PROYECTO DE GRADO

Ingeniería en Informática

UCASAL

UNIVERSIDAD CATÓLICA DE SALTA

DISEÑO E IMPLEMENTACIÓN DE HONEYPOTS PARA LA DETECCIÓN DE CIBERATAQUES

Autor/ Alumno:

BAIRO BRAVO JULIO ENRIQUE

Director de Tesis:

APPENDINO SERGIO DANIEL

Ingeniero de Sistemas

Docente Universitario, Auditor de Sistemas de Información (CISA) y Perito Informático

Presidente de la Red UNIF de Universidades con Informática Forense

Salta - Argentina

2021

TÍTULO

Ingeniero en Informática

PROYECTO

"Diseño e Implementación de Honeypots para la Detección de Ciberataques"

ALUMNO

Julio Enrique Bairo Bravo Firma: 

PROFESOR GUÍA

Ing. Sergio Daniel Appendino Firma: 

TRIBUNAL EVALUADOR

Jurado: _____ Firma: _____

Jurado: _____ Firma: _____

Jurado: _____ Firma:_____

FECHA DE EXPOSICIÓN: _____/_____/_____

OBSERVACIONES:

DEDICATORIAS

Este proyecto está dedicado a mis queridos padres *Edgar Bairo Salazar* y *Mirta C. Bravo Araujo* quienes con su amor, paciencia y sacrificio me permitieron llegar a cumplir una de mis metas planteadas. ***Gracias por inculcar en mí, el ejemplo de esfuerzo, valentía y perseverancia****, de no temer a las adversidades, y de mantener la cabeza siempre en alto, muchos de los logros se los debo a ustedes*.

AGRADECIMIENTOS

A mis padres, quienes siempre me apoyaron incondicionalmente en todos mis proyectos, brindándome las fuerzas y los medios suficientes para poder desarrollarme intelectual y moralmente. Gracias por creer y confiar en mí y por haber sido mi soporte principal durante toda mi carrera profesional.

A mis queridos hermanos, por su cariño y apoyo incondicional durante todo este proceso, y por estar conmigo en los momentos más difíciles. Agradezco también a Dios por brindarme salud, fortaleza e inteligencia para desarrollar este trabajo con éxito.

A mi profesor y tutor guía, el Ingeniero Sergio Appendino, por haberme ayudado en todo el proceso de este proyecto, quien desde su experiencia y sabiduría supo guiarme y darme las directrices necesarias para culminar con éxito este trabajo. Agradezco también de manera especial a la Ingeniera Guillermina Nievas, quien desde el momento que llegué a la Universidad supo guiarme, aconsejarme, apoyarme y colaborar desinteresadamente, brindándome todo su conocimiento y orientación durante el desarrollo de mi carrera profesional.

A la Universidad Católica de Salta (UCASAL), directivos y profesores que me dieron la oportunidad de formarme profesionalmente, y a todas las personas que fueron partícipes de este proceso, porque fueron los responsables de realizar su aporte y que el día de hoy se vea reflejado. Hoy puedo decir que después de años de esfuerzo, sacrificios, dedicación y grandes alegrías, llegó el día que mi meta y sueño profesional se hace realidad.

ÍNDICE GENERAL DEL PROYECTO

CAPÍTULO 1 - INTRODUCCIÓN **1**
1.1 ABSTRACT 1
1.2 DESCRIPCIÓN DEL PROBLEMA 2
1.3 MOTIVACIÓN 3
1.4 ORGANIZACIÓN DEL PROYECTO 4

CAPÍTULO 2 - MARCO TEÓRICO **6**
2.1 INTRODUCCIÓN 6
2.2 FUNDAMENTOS DE SEGURIDAD 7
2.2.1 SEGURIDAD DE LA INFORMACIÓN 7
2.2.2 SEGURIDAD INFORMÁTICA 8
2.2.3 CIBERSEGURIDAD 8
2.2.4 ACTIVOS DE INFORMACIÓN 9
2.2.5 CULTURA DE SEGURIDAD 10
2.3 MARCOS DE REFERENCIA 11
2.3.1 NORMA ISO/IEC 27001 11
2.3.2 CONTROLES CIS 11
2.3.3 NIST SP 800-53 13
2.4 TIPOS DE SEGURIDAD 14
2.4.1 SEGURIDAD FÍSICA 14
2.4.2 SEGURIDAD LÓGICA 15
2.4.3 SEGURIDAD A NIVEL DE RED 16
2.5 CIBERSEGURIDAD 17
2.5.1 LOS PILARES FUNDAMENTALES DE LA CIBERSEGURIDAD 17
2.5.2 IMPORTANCIA DE LA CIBERSEGURIDAD 19
2.5.3 SITUACIÓN GENERAL DE LA CIBERSEGURIDAD EN ARGENTINA 20
2.5.4 LEGISLACIÓN ARGENTINA EN CIBERDELITOS 23
2.5.5 CIBERINTELIGENCIA: UN NUEVO PARADIGMA EN LA CIBERSEGURIDAD 24
2.6 AMENAZAS Y ATAQUES INFORMÁTICOS 26
2.6.1 CONCEPTOS ÚTILES 27
2.6.2 TIPOS DE INTRUSOS 28
2.6.3 TIPOS DE ATAQUES 29
2.6.4 ANATOMÍA DE UN ATAQUE INFORMÁTICO 33
2.6.5 MEDIDAS BÁSICAS DE PROTECCIÓN 34
2.6.6 DEFENSA EN PROFUNDIDAD 36

CAPÍTULO 3 - ESTADO DE LA CUESTIÓN **41**
3.1 ANTECEDENTES 41
3.2 HONEYPOTS 42
3.2.1 OBJETIVOS DE LAS HONEYPOTS 43
3.2.2 HISTORIA DE LAS HONEYPOTS 43
3.2.3 CLASIFICACIÓN DE LAS HONEYPOTS 44
3.2.4 LOCALIZACIÓN DE UN HONEYPOT EN LA RED 46
3.2.5 DISTRIBUCIONES DE HONEYPOTS 49
3.2.6 VENTAJAS Y DESVENTAJAS DE HONEYPOTS 53
3.3 HONEYNETS 54
3.3.1 ARQUITECTURA DE LAS HONEYNETS 55
3.3.2 ELEMENTOS BÁSICOS DE UNA HONEYNET 58
3.3.3 HONEYNETS VIRTUALES 60

CAPÍTULO 4 - DEFINICIÓN DEL PROBLEMA **63**
4.1 DEFINICIÓN EXACTA DEL PROBLEMA 63
4.2 OBJETIVO GENERAL 63
4.3 OBJETIVOS ESPECÍFICOS 63
4.4 ALCANCE DEL PROYECTO 64

CAPÍTULO 5 - SOLUCIÓN PROPUESTA **66**
5.1 JUSTIFICACIÓN 66
5.2 ESTUDIO DE FACTIBILIDAD 68
5.3 ANÁLISIS ECONÓMICO-FINANCIERO 69
5.3 METODOLOGÍA DE DESARROLLO 73
5.4 HERRAMIENTAS A UTILIZAR 75

CAPÍTULO 6 - IMPLEMENTACIÓN DE LA SOLUCIÓN **77**
6.1 ANÁLISIS DEL HONEYPOT 77
6.2 DISEÑO DEL HONEYPOT 78
6.2.1 ARQUITECTURA DE VIRTUALIZACIÓN 78
6.2.2 SELECCIÓN DEL HONEYPOT A IMPLEMENTAR 79
6.2.3 ESQUEMA DE LA INFRAESTRUCTURA 83
6.2.4 REQUERIMIENTOS DE HARDWARE Y SOFTWARE 85
6.2.5 CONFIGURACIÓN DE LA RED DISEÑADA 86
6.3 IMPLEMENTACIÓN DEL HONEYPOT 89
6.3.1 FUNCIONAMIENTO DE T-POT 89
6.3.2 INSTALACIÓN DE T-POT 94
6.3.3 CONFIGURACIÓN DE SERVICIOS T-POT 97

6.3.4 USO DE T-POT 99
6.4 ESCENARIOS DE PRUEBAS Y RESULTADOS 102
6.4.1 ESCENARIO-01: ATAQUES RECOPILADOS CON T-POT 102
6.4.2 ESCENARIO-02: ATAQUES CON DENEGACIÓN DE SERVICIOS (DoS) 108
6.4.3 ESCENARIO-03: ATAQUE CON METASPLOIT 111
6.4.4 ANÁLISIS DE RESULTADOS 114
6.4.5 RECOMENDACIONES GENERALES DE SEGURIDAD 116

CAPÍTULO 7 - CONCLUSIONES Y TRABAJOS FUTUROS 117
7.1 CONCLUSIONES 117
7.2 FUTURAS LÍNEAS DE INVESTIGACIÓN 118

CAPÍTULO 8 - REFERENCIAS BIBLIOGRÁFICAS 120

CAPÍTULO 9 - ANEXOS 131
9.1 ANEXO 01: INSTALACIÓN DE VMWARE WORKSTATION 131
9.2 ANEXO 02: INSTALACIÓN Y CONFIGURACIÓN DE VMWARE TOOLS 135
9.3 ANEXO 03: COMPONENTES BÁSICOS DE LA RED VIRTUAL 137
9.4 ANEXO 04: CREACIÓN DE UNA MÁQUINA VIRTUAL 138
9.5 ANEXO 05: INSTALACIÓN DE UN SISTEMA OPERATIVO 144
9.6 ANEXO 06: ADAPTADORES DE RED EN MÁQUINAS VIRTUALES 150
9.7 ANEXO 07: CONFIGURACIÓN DE LA RED EN LAS MÁQUINAS VIRTUALES 152
9.8 ANEXO 08: INSTALACIÓN DE T-POT EN VMWARE WORKSTATION 157
9.9 ANEXO 09: INSTALACIÓN DE T-POT EN UN SERVIDOR VIRTUAL PRIVADO 163
9.10 ANEXO 10: INDICADORES DE CIBERSEGURIDAD ARGENTINA 2020 168
9.11 ANEXO 11: ATAQUES FRECUENTES PARA PRUEBAS DE PENTESTING 170
9.12 ANEXO 12: METASPLOIT CON KALI LINUX 172

CAPÍTULO 10 - GLOSARIO 175

ÍNDICE DE FIGURAS

Figura 01: Seguridad de la información Pág. 07
Figura 02: Ciberseguridad Pág. 09
Figura 03: Pilares fundamentales de la ciberseguridad Pág. 17

Figura 04: Tipos de ataques en ciberseguridad Pág. 29

Figura 05: Modo de operación de un ataque informático Pág. 33

Figura 06: Defensa en profundidad Pág. 36

Figura 07: Estructura de una honeypot Pág. 42

Figura 08: Honeypot en la red interna Pág. 47

Figura 09: Honeypot en la red externa Pág. 47

Figura 10: Honeypot en una zona desmilitarizada (DMZ) Pág. 48

Figura 11: Esquema de una honeynet básica Pág. 55

Figura 12: Honeynet de primera generación Pág. 56

Figura 13: Honeynet de segunda generación Pág. 57

Figura 14: Honeynet de tercera generación Pág. 58

Figura 15: Honeynet virtual autocontenida Pág. 61

Figura 16: Honeynet virtual híbrida Pág. 62

Figura 17: Ciclo deming de mejora continua Pág. 74

Figura 18: Arquitectura de virtualización Pág. 79

Figura 19: Infraestructura de la red para la honeynet Pág. 83

Figura 20: Listado de máquinas virtuales instaladas Pág. 87

Figura 21: Arquitectura del honeypot T-Pot Pág. 90

Figura 22: Herramientas de monitoreo utilizados por T-Pot Pág. 93

Figura 23: Verificación de puertos abiertos en el servidor T-Pot Pág. 99

Figura 24: Verificación de contenedores T-Pot Pág. 100

Figura 25: Estadísticas de los ciberataques capturados por Kibana Pág. 101

Figura 26: Ataques recopilados con T-Pot a nivel mundial Pág. 103

Figura 27: Ataques recopilados con T-Pot a nivel mundial según ciertos parámetros Pág. 104

Figura 28: Ataques recopilados de Argentina Pág. 105

Figura 29: Ataques recopilados de Estados Unidos Pág. 106

Figura 30: Ataques recopilados de Vietnam Pág. 107

Figura 31: Ejecución por línea de comandos de SlowHTTPTest Pág. 108

Figura 32: Funcionamiento del ataque DoS con SlowHTTPTest Pág. 108

Figura 33: Capturador del tráfico de red para el ataque DoS Pág. 109

Figura 34: Estado del servicio de SlowHTTPTest Pág. 109

Figura 35: Ciberinteligencia a la dirección IP del atacante Pág. 110

Figura 36: Pantalla de inicio de Metasploit Pág. 111

Figura 37: Reconocimiento de puertos con Nmap Pág. 111

Figura 38: Ejecución de módulos en Metasploit Pág. 112

Figura 39: Acceso SSH al servidor T-Pot Pág. 113

Figura 40: Verificación del ataque con Metasploit en el servidor T-Pot Pág. 113

ÍNDICE DE TABLAS

Tabla 01: CSIRTS de Argentina Pág. 23

Tabla 02: Costos de los recursos humanos Pág. 69

Tabla 03: Costos de los recursos físicos y tecnológicos Pág. 71

Tabla 04: Costos de los recursos fijos Pág. 72

Tabla 05: Costos totales Pág. 73

Tabla 06: Ventajas y desventajas de las soluciones propuestas Pág. 81

Tabla 07: Comparativa de las soluciones propuestas Pág. 82

Tabla 08: Detalle de las redes implementadas Pág. 84

Tabla 09: Hardware para equipo host (anfitrión) Pág. 85

Tabla 10: Hardware para estaciones de trabajo (workstation) Pág. 85

Tabla 11: Hardware para servidores Pág. 86

Tabla 12: Hardware para el honeypot T-Pot Pág. 86

Tabla 13: Direccionamiento IP de máquinas virtuales Pág. 89

Tabla 14: Puertos utilizados por los honeypots de T-Pot Pág. 91

Tabla 15: Reglas de firewall para Windows Pág. 98

Tabla 16: Reglas de firewall para Google Cloud Platform Pág. 98

CAPÍTULO 1 - INTRODUCCIÓN

1.1 ABSTRACT

Hoy en día se dice que estamos viviendo una cuarta gran revolución industrial, porque con la llegada de Internet y las nuevas tecnologías emergentes se está cambiando la forma en que vivimos, trabajamos y nos relacionamos. Si bien Internet viene democratizando las formas de comunicación convirtiéndose así en el medio global más cotidiano en nuestra vidas, también trajo consigo un amplio desconocimiento de los riesgos que pueden impactar en la seguridad de las personas, tanto en entornos laborales, como en la vida personal.

Normalmente, todas las personas tienden a pensar que a nadie les interesa vulnerar su seguridad y robar cualquier tipo de información que posean, puesto que no tienen nada que ocultar, pero la realidad es totalmente diferente. Si bien existen muchos ciberdelincuentes que están en el constante acecho para robar información, también están aquellos que realizan ataques cibernéticos sin intervención humana, es decir las botnets (redes infectadas con software malicioso) cuyo único objetivo es la de comprometer sus equipos y extraer la mayor cantidad de información posible, que posteriormente serán usados para fines delictivos. Con esto lo que queremos decir, es que la seguridad en el mundo digital se considera tan importante como la seguridad en nuestro entorno físico, por lo que debemos comenzar a tener un nivel mayor de protección, puesto que la tecnología ingresa a todos los ámbitos de nuestras vidas.

Por lo tanto, en base a esta problemática planteada y sabiendo el constante crecimiento que tienen los ciberdelincuentes, este proyecto tiene como objetivo brindar una herramienta de seguridad proactiva de manera que se puedan prevenir los ciberataques antes de que sean explotadas las vulnerabilidades. Para ello se utilizarán los honeypots, un recurso de red que simula ser un objetivo real para que cualquier intruso pueda atacar y de esa manera poder obtener toda información relevante sobre cualquiera de sus ataques y con ello tomar las medidas necesarias para luego poder mitigarlos. Resaltamos además, que los honeypots no persiguen la finalidad de ser una solución de seguridad, sino que funcionan como un complemento a los sistemas de seguridad ya existentes. El proyecto también detalla los aspectos más importantes que se deberán tener en cuenta a la hora de diseñar e implementar un honeypot para nuestra organización, puesto que en el mercado actual existen muchas distribuciones de honeypots, pero saber cuál emplear para nuestra seguridad dependerá solo de los objetivos que se tenga.

De esta manera, con este proyecto lo que se pretende, es comunicar y concientizar a todas las personas y empresas, para que a través del diseño e implementación de un honeypot, será posible garantizar una mejor seguridad en sus redes y de esa forma poder estar totalmente seguros, con la condición de estar alertas a partir de ahora. Por ende, queda en cada uno de nosotros tomar las medidas de seguridad más pertinentes, puesto que somos nosotros quienes visitamos enlaces sospechosos, quienes descargamos archivos desconocidos y quienes ignoramos las advertencias de seguridad de nuestras aplicaciones. Por lo tanto, es realmente imprescindible que todas las personas comprendan que la información que recolectan, procesan y comparten en la red o sus dispositivos puede convertirse en la entrada principal de cualquier ciberatacante.

1.2 DESCRIPCIÓN DEL PROBLEMA

Internet ha revolucionado muchos ámbitos y especialmente el de las comunicaciones de una manera radical hasta el punto de llegar a convertirse en un medio global de comunicación, hoy día cotidiano en nuestras vidas (Zaryn Dentzel, 2013).

Todos somos conscientes de los cambios que ha provocado Internet en nuestras vidas, en términos de facilitar el acceso a la información y la comunicación instantánea. Sin embargo, en esta época de cambios vertiginosos e incesantes de la tecnología, es imprescindible cuidar el valor de la información que publicamos en la red, ya que el potencial que ofrece Internet presenta de igual forma un riesgo cuando un uso inseguro puede poner en peligro nuestra información más privada y confidencial. (Leticia Gonzalez, 2015). Por esta razón, la responsabilidad de proteger la información privada de los usuarios recae en gran parte en las organizaciones, encargadas de su almacenamiento y de los servicios ofrecidos. Esto es así, porque la gran cantidad de información que tienen a su recaudo las hace vulnerables frente a los constantes ataques e intentos de intrusión de los ciberdelincuentes, que ven un valor incalculable en ella, de la cual pueden sacar un beneficio. (José Fernández, 2013).

Por lo tanto, considerando todas estas cuestiones y frente a los constantes ataques y acosos cibernéticos que pueden sufrir las personas y las organizaciones, estamos ante una problemática evidente, y que cada día aumenta con el avance de la tecnología, por ello es necesario tomar medidas y estrategias que permitan mitigar todos estos ataques, si es que no queremos que nuestros datos sean comprometidos eventualmente.

1.3 MOTIVACIÓN

La motivación que me impulsa a realizar el presente proyecto, se centra básicamente en brindar a las personas y a las organizaciones una mayor *comunicación y concientización* sobre temas de protección de datos y seguridad de la información, que en la actualidad juegan un rol muy importante, además del gran aporte que supone al mundo de la ciberseguridad.

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. Dado que la información ha sido desde siempre un bien invaluable, protegerla ha sido una tarea continua y de vital importancia. A medida que se crean nuevas técnicas para la transmisión de la información, se idean otras que permiten acceder a ella sin autorización.

Por esta razón, a la hora de afrontar las amenazas debemos tener en cuenta dos aspectos muy importantes: la seguridad reactiva y la seguridad proactiva.

- *La seguridad reactiva*

  Considera los elementos básicos de seguridad, centrándose en fortalecer las defensas contra los métodos de ataque comunes, esperando señales visibles de intrusión para luego tomar medidas. Estas medidas de seguridad normalmente incluyen firewalls, antivirus, sistema de detección de intrusiones (IDS), filtros de spam, entre otros. (Ciberseguridad, 2016).

- *La seguridad proactiva*

  Implica métodos que se utilizan para prevenir los ciberataques, intentando localizar y corregir las vulnerabilidades de una organización antes de que sean explotadas por los ciberdelincuentes. Entre sus métodos de seguridad se incluye concienciación sobre ciberseguridad organizacional, hacking ético, pentesting, etc. (Ciberseguridad, 2016). Existen muchas técnicas en este tipo de seguridad, pero básicamente analizaremos los honeypots y la ciberinteligencia, debido a la eficacia que tienen.

  La *ciberinteligencia*, consiste en adquirir y analizar la información, para luego identificar, rastrear, predecir y contrarrestar las capacidades, intenciones y actividades de los criminales, y ofrecer cursos de acción, que mejoren la toma de decisiones. Si bien existen diferentes tipos de inteligencia (OSINT, HUMINT, SIGINT, IMINT, ...), cada una de ellas se rigen de muchas normativas legales que normalmente dependen de cuáles sean las áreas de interés y los objetivos. (Marcos Polanco, 2016).

Los honeypots en cambio, son un recurso de red que simula ser un objetivo real, pero destinado a ser atacado, de tal forma que un intruso pueda ingresar y comprometerla. De esa forma, los ataques se efectúan sobre ese sistema sin causar ningún daño al sistema real. *(Lance* Spitzner, 2002*).*

Analizando en detalle, podemos decir que la seguridad reactiva son excelentes herramientas defensivas para reforzar la seguridad de una organización, pero aún así, presentan limitaciones en cuanto a su efectividad, además de que no se pueden adaptar a diferentes patrones de ataque. En el caso de la seguridad proactiva, la ciberinteligencia, es un paradigma muy amplio para analizar y no tiene sentido utilizarlas porque las empresas se ven restringidas desde el punto de vista legal para hacer este tipo de trabajo, además de que se considera un punto muy riesgoso. Mientras que los honeypots, no se rigen de tantas normativas, es una herramienta centrada en algo específico, poseen muchas variantes para poder implementarlos según lo que la organización precise y sirven tanto para posibles atacantes internos como externos. Por tal motivo, utilizar técnicas proactivas de defensa orientadas a la seguridad de redes como son los honeypots es una buena opción para el análisis de este proyecto.

1.4 ORGANIZACIÓN DEL PROYECTO

Este proyecto está estructurado en 10 capítulos, los cuales están organizados de la siguiente forma:

- *Capítulo 1: Introducción*

  Describe el contexto en el cual está inmerso el proyecto de grado.

- *Capítulo 2: Marco teórico*

  Se presentan los aspectos teóricos que son necesarios comprender y donde se sustentará cualquier análisis, experimento o propuesta de desarrollo. Por lo tanto, este capítulo incluye los conceptos relevantes de seguridad, definiciones útiles, modelos y teorías.

- *Capítulo 3: Estado de la cuestión*

  Consiste en una descripción completa, sistemática, objetiva y lo suficientemente clara sobre los honeypots como tema de investigación. De esta manera, la comprensión de esta útil herramienta incluye antecedentes, historia, características, funcionamiento, clasificaciones, etc.

- *Capítulo 4: Definición del problema*

  Se desarrolla un análisis del contexto y la problemática que dan origen al desarrollo del proyecto, estableciendo los objetivos y el alcance que tendrá el proyecto.

— *Capítulo 5: Solución propuesta*

Después de un análisis de seguridad reactivo y proactivo, se procedió a utilizar como herramienta de seguridad los *honeypots*. Este capítulo, constituye la parte central del proyecto, debido a que se especifica de qué manera se resolverá la problemática planteada, estableciendo una metodología de trabajo, herramientas y los diferentes recursos a utilizar. Además se contará con un análisis económico-financiero para la implementación de todo el proyecto.

— *Capítulo 6: Implementación de la solución*

Consiste en diseñar y analizar la infraestructura necesaria para implementar los honeypots en una red virtual, seleccionando el honeypot con el que se trabajará, su configuración correspondiente, los diferentes escenarios de pruebas a lo que se someterá, como así también las diferentes formas que se tiene para mitigarlos.

— *Capítulo 7: Conclusiones y Trabajos Futuros*

Se muestran los resultados obtenidos, junto con las conclusiones finales sobre la implementación de los honeypots. Además, se plantean las posibles mejoras que se pueden realizar al sistema y los trabajos futuros.

— *Capítulo 8: Referencias Bibliográficas*

Aquí aparecen todas las referencias bibliográficas que fueron citadas en este proyecto, siguiendo como base las normas APA con la intención de hacer más comprensibles las lecturas.

— *Capítulo 9: Anexos*

En este capítulo, se mostrarán todos los anexos que son necesarios para el proyecto, con el fin de proporcionar información extra acerca de los honeypots, que incluyen artículos, gráficos, tablas, imágenes, entre otros.

— *Capítulo 10: Glosario*

Este diccionario permitirá al lector identificar y conceptualizar ciertos términos que pueden causar confusión o desconocimiento sobre temas específicos.

CAPÍTULO 2 - MARCO TEÓRICO

2.1 INTRODUCCIÓN

Durante muchos años las empresas se han preocupado por perfeccionar todos los sistemas informáticos, dejando en una prioridad casi nula, la seguridad de la información. En general, la evolución de los sistemas informáticos, Internet y de las comunicaciones han abierto una puerta para que las personas descubran el valor de la información y la facilidad de acceder a los datos. Desafortunadamente, el fácil acceso a la información también permite que personas no autorizadas la utilicen y debido a esto, existen miles de personas y grupos asociados que se dedican a realizar ataques informáticos con la finalidad de obtener información para cometer actos ilícitos, de tal manera que puede llegar a perjudicar a una empresa. [1]

Actualmente es necesario garantizar que en las mejoras realizadas en los sistemas informáticos y en la manipulación de la información física se incluyan criterios de seguridad de la información, pues ésta debe resguardarse y limitarse para evitar exponerla a personas ajenas a la utilización de la misma. Por ello, realizar controles relacionados con la seguridad de la información y de los sistemas informáticos nos permitirá garantizar la confidencialidad, integridad, disponibilidad y el no repudio en los sistemas de procesamiento de datos y en la información utilizada por el personal de las organizaciones. Por lo tanto, es muy importante realizar un análisis de seguridad en los procesos de una empresa, de manera que se puedan detectar vulnerabilidades y amenazas que de materializarse puedan afectar la continuidad del negocio. [2]

De esta manera, lo que se pretende en este capítulo es analizar conceptos relacionados con la seguridad de la información, seguridad informática y ciberseguridad, detallando definiciones útiles, componentes principales, marcos de referencia, amenazas de seguridad, entre otros, los cuales serán necesarios para comprender más a fondo el tema abordado de honeypots.

[1, 2] Kelly G. Bermúdez y Rafael B. Sanchez. (2015). *Análisis en Seguridad Informática y Seguridad de la información basado en la norma ISO/IEC 27001*. (Anteproyecto). Universidad Politécnica Salesiana Sede Guayaquil, Guayaquil, Ecuador.

2.2 FUNDAMENTOS DE SEGURIDAD

2.2.1 SEGURIDAD DE LA INFORMACIÓN

Se entiende por Seguridad de la Información como el *"conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información"*.

De esta forma, la seguridad de la información es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos, puesto que los datos que se manejan son esenciales para el devenir del negocio. Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso. [3]

Sin importar la forma que posea la información, siempre debe protegerse adecuadamente. Por ello, la seguridad de la información debe conformarse siempre de controles, políticas, procedimientos, concientización y entrenamientos que aseguren que todo el mundo tome todas las precauciones necesarias para preservar dicha información. [4]

FIGURA 01 - SEGURIDAD DE LA INFORMACIÓN

FUENTE Elaboración propia en base a *TINGLINK, 2018.*

[3] Tecon. (2018). *La Seguridad de la Información*. Tecon: Soluciones informáticas. [Blog].

[4] Oscar Schmitz. (27 de enero de 2014). *Principios básicos de seguridad de la información*. Oscar Schmitz. [Blog].

2.2.2 SEGURIDAD INFORMÁTICA

Se puede definir Seguridad Informática como la "*disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir que un sistema de información sea seguro y confiable"* (P. Aguilera, 2011). Es decir, ante una eventual amenaza, lo que siempre se busca es proteger la información ya que es el principal activo de toda organización.

De esta manera, la principal tarea de la seguridad informática es la de minimizar los riesgos, que normalmente provienen de muchas partes, ya sean como entrada de datos, medio que transporta la información, hardware utilizado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal será la de minimizar los riesgos para obtener una mejor y mayor seguridad (Martha I. Romero, Grace L. Figueroa, Denisse S. Vera, José E. Álava, Galo R. Parrales, Christian J. Álava, Angel L. Murillo y Miriam A. Castillo, 2018).

Por lo tanto, cuando buscamos proteger el hardware, redes, software, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o bien de ciberseguridad. Mientras que, cuando se incluyen actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concientización, nos referimos a seguridad de la información. (WeLiveSecurity, 2015).

2.2.3 CIBERSEGURIDAD

En la actualidad, un término ampliamente utilizado es ciberseguridad, que puede asociarse con otras palabras como ciberespacio, ciberamenazas, cibercriminales u otros conceptos compuestos. Aunque se tiene una percepción general sobre lo que representa, en ocasiones puede utilizarse como sinónimo de seguridad de la información, seguridad informática o seguridad en cómputo, pero esta idea no es del todo correcta. [5]

Los profesionales de *ISACA*[6] definen básicamente a la ciberseguridad como la "p*rotección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados"*.

[5] WeLiveSecurity. (2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia.*

[6] ISACA es el acrónimo de *Asociación de Auditoría y Control de Sistemas de Información*. Ver Glosario.

También conocida como seguridad de las tecnologías de la información, es la rama de la informática que procura detectar vulnerabilidades que ponen en juego la integridad, disponibilidad, confidencialidad y no repudio de los sistemas informáticos. Es decir, su objetivo principal es resguardar la infraestructura y la información de los usuarios involucrados (ver *Figura 02*), debido a que se constituye como una esfera con distintos protagonistas: empresas que ofrecen servicios asociados, expertos y analistas que investigan nuevas soluciones, desarrolladores de nuevas herramientas, y aquellos usuarios que utilizan diferentes medios preventivos.[7]

FIGURA 02 - CIBERSEGURIDAD

FUENTE Elaboración propia en base a *FREEPIK, 2019.*

De esta manera, decimos que la ciberseguridad tiene como foco principal la protección de la información digital de los sistemas. Por ello, se puede considerar que la ciberseguridad está comprendida dentro de la seguridad de la información y se distingue de ella porque incluye tecnologías o prácticas ofensivas para atacar a sus adversarios, mientras que la seguridad de la información solo debe ser usada para aspectos defensivos.[8]

2.2.4 ACTIVOS DE INFORMACIÓN

Se define Activo como "*cualquier información o elemento relacionado con el tratamiento de la misma (software, hardware, datos, soportes, edificios, ...) que tenga importancia para la organización*". [9]

Por lo tanto, para comenzar a trabajar con activos, es importante realizar un inventario de los mismos, debido a que si no sabemos lo que tenemos, nos será muy complicado gestionarlo correctamente. Este inventario deberá mantenerse actualizado a lo largo del tiempo, por lo que se deberán realizar revisiones periódicas y comunicar los cambios.

[7] NIC Argentina. (2018). *¿Qué es Ciberseguridad?*.

[8] CIC Team. (2016). *Seguridad de la Información y Ciberseguridad ¿es lo mismo?*. CIC Consulting Informático. [Blog].

[9] Agustin López y Javier Ruiz. (2005). Sistema de Gestión de la Seguridad de la Información.

Los activos los podemos separar en dos grandes grupos: tangibles e intangibles. Los activos tangibles son aquellos activos materiales que contienen información, y sobre los que tomaremos medidas preventivas para protegerlos principalmente de riesgos físicos: golpes, agua, fuego, etc. Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno. [10]

2.2.5 CULTURA DE SEGURIDAD

Los autores Rafael Castillo, Alessio Di Mare, Victor Díaz y Horacio Díez (2004), en su trabajo señalan que "*al hablar de seguridad en la información nos encontramos con tres pilares fundamentales que la soportan: la tecnología, los procesos y las personas*." Esta frase refleja la importancia y la necesidad de profundizar un estudio en la implantación de un programa de concientización de los usuarios en lo que a seguridad de la información se refiere, como forma de lograr una adecuada formación educacional orientado al logro de una cultura de seguridad, de las personas que conforman una organización apoyado en las políticas, normas y lineamientos emanados por la misma. Hoy en día, el acelerado desarrollo de las TIC[11], las crecientes interconexiones, y las redes de información abren paso a la continua exposición de un creciente número de amenazas y vulnerabilidades, donde para la mitigación de las mismas se hace necesario tener en cuenta a las personas y considerarlas indispensables para la seguridad dentro de cualquier organización, logrando obtener una mayor conciencia y entendimiento de los aspectos de seguridad. (Reina A. Camacho, 2013).

Este sentido, los autores indican que hasta ahora las empresas se han preocupado por invertir grandes cantidades de dinero y esfuerzos en tecnología de seguridad y definición de procesos, pero han dejado a un lado a las personas y han hecho que ellas se conviertan en el eslabón más débil de la cadena de seguridad dentro de la organización [12].

Por lo tanto, el mejor plan de seguridad puede verse seriamente comprometido sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria o de luchar contra las medidas de seguridad. Es por ello que se requiere la creación de una cultura de seguridad que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia. (Ministerios de Administraciones Públicas, 2006).

---

[10] ISOWin. (2015). *Los Activos de Información en la norma ISO 27001*. ISOWin. [Blog].

[11] TIC es el acrónimo de *Tecnologías de Información y Comunicación*. Ver *Glosario.*

[12] Rafael Castillo, Alessio Di Mare, Victor Díaz y H. Díez. (2004). *Concientización en seguridad de la información.*

2.3 MARCOS DE REFERENCIA

Un marco de referencia en materia de ciberseguridad es un conjunto de procesos documentados que son utilizados para definir políticas, mecanismos y procedimientos en torno a la implementación y gestión de los controles de seguridad informática dentro del ámbito corporativo, con el objetivo de medir el riesgo de robo y/o pérdida de activos y reducir las vulnerabilidades. Es decir, representan una herramienta para que las empresas puedan evaluar su situación actual en seguridad informática respecto de un estándar de buenas prácticas, para así poder plantear un estado objetivo en dicho ámbito, capaz de ser alcanzado a través de la implementación eficiente del marco de referencia seleccionado. Existen distintos tipos de marcos de referencia, los cuales adoptan enfoques similares, pero difieren en el alcance de sus objetivos. Por lo tanto, es tarea de la organización evaluar cuál se adapta mejor a las necesidades y condiciones de la empresa. (Agustín Spinelli Riso, 2018, pág. 24).

Dada la gran variedad de marcos de referencia, detallaremos los más utilizados:

2.3.1 NORMA ISO/IEC 27001

Es una norma internacional que detalla lineamientos de seguridad de la información, los cuales permiten implementar en la gestión de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información, ayudando así a proteger la información de posibles robos. (Dejan Kosutic, 2014). Esta norma, permite disminuir posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información en general manejada por personal de la empresa, además de la mejora de los procesos y servicios prestados, teniendo una mejor organización de los procesos, aumentando la competitividad de la empresa debido a que se demuestra el interés por salvaguardar la integridad, confiabilidad y disponibilidad de la información de los clientes. (Kelly G. Bermúdez y Rafael B. Sanchez, 2015, pág. 10).

2.3.2 CONTROLES CIS

Desarrollados por el Center for Internet Security (CIS), los Controles de Seguridad Crítica de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos. Estas mejores prácticas procesables para la defensa cibernética son formuladas por un grupo de expertos en tecnología de la información utilizando la información obtenida de ataques reales y sus defensas efectivas. Los controles de CIS proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativos. (Cristian Borghello, 2020).

Según Ruben Ramiro (2018), el objetivo de los controles de CIS es describir qué pueden hacer las organizaciones para defender eficazmente sus sistemas de información contra los ataques más comunes y proporcionar un enfoque gradual para implementar una defensa de ciberseguridad más sólida. Por ello, los primeros cinco controles de seguridad crítica de CIS que a menudo se denominan higiene de la ciberseguridad, muestran que su implementación proporciona una defensa muy eficaz contra los ciberataques más comunes (~ 80% de los ataques). Y en un esfuerzo por ayudar a las organizaciones a implementar prácticamente los primeros cinco controles, los objetivos de estos controles se describen claramente a continuación:

1. *Inventario de dispositivos autorizados y no autorizados*

   El objetivo de este control es ayudar a las organizaciones a definir una línea de base de lo que se debe defender. Después de que una organización haya inventariado con precisión sus sistemas, el siguiente paso es evitar que los dispositivos no autorizados se unan a una red: aquí es donde se destaca la implementación de la autenticación a nivel de red. El objetivo inicial no es evitar que los atacantes se unan a la red, sino también comprender qué hay en la red para poder defenderla.

2. *Inventario de software autorizado y no autorizado*

   El objetivo es garantizar que solo se permita la ejecución de software autorizado en los sistemas de información de una organización. Si bien un inventario de software es importante, el control más importante que una organización puede implementar aquí es la inclusión en la lista blanca de aplicaciones, que limita la capacidad de ejecutar aplicaciones solo a aquellas que están aprobadas. Este control a menudo se considera uno de los más efectivos para prevenir y detectar ataques de ciberseguridad, aunque la lista blanca de aplicaciones a menudo no se implementa fácilmente.

3. *Configuraciones seguras de hardware y software en dispositivos*

   Por defecto, la mayoría de los sistemas tecnológicos se instalan con un enfoque en la facilidad de uso y no necesariamente en la seguridad. Los sistemas pueden tener la capacidad de ser protegidos, pero es probable que existan configuraciones que un sistema debe tener para garantizar una alta seguridad. Por ello, es necesario utilizar estándares de configuración o puntos de referencia, como los definidos por el Centro para la Seguridad de Internet, o lo que se encuentran en el Repositorio del Programa de Lista de Verificación Nacional del NIST.

4. *Evaluación continua de la vulnerabilidad y remediación*

   El objetivo de este control es comprender las debilidades técnicas del software que existen en los sistemas de información de una organización y eliminar esas debilidades. Las organizaciones exitosas implementan sistemas de administración de parches que cubren vulnerabilidades tanto de sistemas operativos como de aplicaciones de terceros. Esto permite la instalación automática, continua y proactiva de las actualizaciones para abordar las vulnerabilidades del software.

5. *Uso controlado de privilegios administrativos*

   El objetivo de este control es garantizar que los miembros de la fuerza laboral solo tengan los derechos, privilegios y permisos del sistema que necesitan para realizar su trabajo, ni más ni menos de lo necesario. Desafortunadamente, por razones de velocidad y conveniencia, muchas empresas y organizaciones permiten que el personal tenga un sistema local o incluso derechos de administrador de dominio que son demasiado generosos y abren la puerta a abusos accidentales o de otro tipo. La respuesta simple para este control es eliminar permisos o permisos innecesarios del sistema.

2.3.3 NIST SP 800-53

El Instituto Nacional de Normas y Tecnología (NIST), una agencia perteneciente al Departamento de Comercio de los Estados Unidos, desarrolló este marco voluntario de manera coherente con su misión de promover la innovación y la competitividad en el país. El Cybersecurity Framework de NIST utiliza un lenguaje común para guiar a las compañías de todos los tamaños a gestionar y reducir los riesgos de ciberseguridad y proteger su información. Este marco no provee nuevas funciones o categorías de ciberseguridad, sino recopila las mejores prácticas (ISO, ITU, CIS, NIST, entre otros) y las agrupa según afinidad. Se centra en el uso de impulsores de negocio para guiar las actividades de ciberseguridad y considerar los riesgos cibernéticos como parte de los procesos de gestión de riesgos de la organización. (Giancarlo Gómez Morales, 2019).

Según Mónica M. Jiménez (2021), en su publicación establece que el marco del NIST, por su simplicidad y flexibilidad se adapta a organizaciones de cualquier sector o tamaño, permitiendo entender, gestionar y disminuir la probabilidad de ocurrencia de un riesgo cibernético gracias a la adecuada protección de sus redes y datos. Este marco, también conocido como Cibersecurity Framework (CSF), está compuesto por tres partes:

1. *El núcleo (Framework core)*

   Es un conjunto de actividades para lograr resultados de seguridad cibernética, hace referencia a estándares, directrices y buenas prácticas de la industria. Este núcleo está conformado por cinco funciones, simultáneas y continuas, que deben seguirse para implementar o complementar un buen programa de seguridad de la información. Estas funciones son: identificar, proteger, detectar, responder y recuperar.

2. *Niveles de implementación del marco*

   Ofrecen un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos y programas para gestionarlo. La selección de estos niveles por parte del NIST toma en cuenta prácticas de gestión de riesgos, requisitos legales y reglamentarios, objetivos empresariales, requisitos de seguridad cibernética, entre otros. Según explica, los niveles respaldan la toma de decisiones organizacionales sobre cómo gestionar el riesgo de seguridad cibernética, así como qué dimensiones de la organización son de mayor prioridad y podrían recibir recursos adicionales.

3. *Perfiles del marco*

   Se refiere a la alineación de las funciones, categorías y subcategorías con los requisitos empresariales, la tolerancia al riesgo y los objetivos de la organización. Estos perfiles sirven para describir el estado actual u objetivo de las actividades que se realizan en ciberseguridad. El perfil actual habla de los resultados que se están logrando, mientras que el perfil objetivo muestra los resultados que se requieren para lograr objetivos trazados en la gestión de riesgos cibernéticos.

2.4 TIPOS DE SEGURIDAD

En la actualidad, la gestión de la seguridad se ha convertido en una de las áreas más importantes dentro de una organización; entre sus objetivos principales está diseñar y mantener un buen sistema de seguridad tanto físico como lógico para proteger los componentes y la información manejada en la red, así como las otras áreas para la gestión de redes. (Reina A. Camacho, 2013).

2.4.1 SEGURIDAD FÍSICA

La Seguridad Física consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. (Cristian Borghello, 2001, pág. 17).

A la hora de hablar de seguridad informática en general, la seguridad física es un aspecto olvidado con demasiada frecuencia por todos los administradores; en muchas casos se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de servidores o cuartos de cableados. Hemos de ser conscientes de que la seguridad física es demasiado importante como para ignorarla, porque de no reforzar este aspecto no importará que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que definamos una política de firewall muy restrictiva, sino tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información, no van a servir de nada. (Reina A. Camacho, 2013, pág. 17).

2.4.2 SEGURIDAD LÓGICA

Luego de ver cómo nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada. Así, la seguridad física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. (Cristian Borghello, 2001, pág. 31).

Según Cristian Borghello (2001), podemos definir Seguridad Lógica como la "*aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas para hacerlo*".

La seguridad lógica incluye la protección de la información (datos y software de la red) de posibles incidentes, que van desde la infección de virus hasta el robo o modificación de estos, mediante el uso de medidas y controles como passwords, logins y grupos de usuarios. La seguridad lógica implica también el establecimiento de estrategias de respaldo y recuperación de datos que permitan minimizar el tiempo de restablecimiento de los servicios de la red. Por lo tanto, para lograr un buen nivel de protección en las redes es necesario diseñar e implantar políticas de seguridad que incluyan aspectos tecnológicos y gerenciales. Además, para garantizar que la seguridad de la información sea gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información (SGSI), que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad de la seguridad de la información. (Reina A. Camacho, 2013, pág. 18).

2.4.3 SEGURIDAD A NIVEL DE RED

El principal objetivo de las redes es mantener disponibles todos los equipos, datos y programas para cualquier usuario de la red, sin importar su ubicación geográfica (Jorge W. Trapp, 2009, pág. 20).

De esta manera, las redes en las empresas son los medios que permiten la comunicación de diversos equipos y usuarios y por lo tanto son una prioridad mantener su seguridad debido a la información que por ellas se transmite. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes malintencionadas, que pongan en peligro la disponibilidad, integridad, confidencialidad y el no repudio de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles y que son tan costosos como los ataques intencionados. Dentro de la organización existen redes internas y externas que deben ser protegidas de acuerdo a las amenazas a las que cada una está expuesta, estableciendo mecanismos de seguridad contra los distintos riesgos que pudieran atacarlas. (María G. Hernández, 2006, pág. 125).

Maria G. Hernandez (2006), indica que existen dos aspectos de seguridad a nivel de red a considerar:

- *Seguridad en la red interna*

  La red interna o intranet está formada por el conjunto de computadoras interconectadas a través de un servidor con la finalidad de compartir información y recursos de forma eficiente y rápida dentro de la organización. El riesgo al que está frecuentemente expuesta esta red es el que viene del uso inadecuado del sistema por parte de los propios usuarios. Ya sea por mala fe o descuido, un usuario con demasiados privilegios puede destruir información. Por lo tanto, las medidas de seguridad que requiere la intranet para disminuir el riesgo existente por parte de los usuarios que son quienes hacen uso constante de la red son la encriptación y las contraseñas para validar usuarios.

- *Seguridad en la red externa*

  La red externa más grande que existe es Internet y en la actualidad es desde donde se producen la gran mayoría de ataques por parte de personas que tienen el propósito de destruir o bien de robar datos empresariales causando pérdidas de dinero. La seguridad en Internet es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios de esta red y las organizaciones que los rodean. La seguridad consiste en una protección contra el comportamiento inesperado.

2.5 CIBERSEGURIDAD

2.5.1 LOS PILARES FUNDAMENTALES DE LA CIBERSEGURIDAD

Los profesionales en ciberseguridad normalmente persiguen cuatro principios fundamentales a la hora de valorar la protección de la información, debido al creciente número de ciberataques que ocurren hoy en día, convirtiendo la protección de los datos en una prioridad para cualquier organización. Estos principios básicamente son la confidencialidad, integridad, disponibilidad y el no repudio (ver *Figura 03*).

FIGURA 03 - PILARES FUNDAMENTALES DE LA CIBERSEGURIDAD

FUENTE Elaboración propia.

Según los autores Martha I. Romero, Grace L. Figueroa, Denisse S. Vera, José E. Álava, Galo R. Parrales, Christian J. Álava, Angel L. Murillo y Miriam A. Castillo (2018) en su publicación titulada "*Introducción a la seguridad informática y el análisis de vulnerabilidades*", explican en detalle los pilares fundamentales de la ciberseguridad:

- ***Confidencialidad (Confidentiality)***

  La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo sólo podrá usar los recursos que necesita para ejercer sus tareas. De esta forma, para garantizar la confidencialidad se recurre principalmente a tres recursos:

  — *Autenticación de usuarios:* Sirve para identificar que quién accede a la información es quien dice ser. Es decir, consiste en el acto de probar la identidad de un usuario del sistema informático. Por ejemplo, comparando la contraseña introducida con la almacenada en la base de datos.

- *Gestión de privilegios:* Los usuarios que acceden al sistema pueden operar solo con la información para la cual se les ha autorizado, es decir, se permite solo lo necesario para realizar las actividades rutinarias. Por ejemplo, gestionar permisos de lectura o escritura en función del tipo o rol de usuario.

- *Cifrado de información:* El cifrado de datos consiste básicamente en la conversión de datos de un formato legible a un formato codificado y sólo podrá ser leído o procesado después de haberse descifrado. Además, el cifrado se considera fundamental para la seguridad de datos, debido a que es la forma más simple e importante de impedir que alguien robe información de un sistema informático.

- ***Integridad (Integrity)***

  Consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente. Esto es así, porque el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tomen decisiones equivocadas.

  Para garantizar la integridad de la información se debe considerar:

  1. Monitorear el tráfico de red para descubrir posibles intrusiones.
  2. Auditar los sistemas para implementar políticas de auditorías.
  3. Implementar sistemas de control de cambios.
  4. Utilizar las copias de seguridad, en caso de que se pierda la información.

- ***Disponibilidad (Availability)***

  Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad. De nada sirve que solo el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, por ello, la información para resultar útil y valiosa debe estar disponible para quien la necesita y se deben implementar las medidas necesarias para que tanto la información como los servicios estén disponibles.

  Por ejemplo, un ataque distribuido de denegación de servicio (DDoS) puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar.

- ***No Repudio (Not repudiation)***

  El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que el emisor envió el mensaje. Así mismo, cuando se recibe un mensaje, el emisor puede verificar que el receptor recibió el mensaje. (Gómez Vieites, 2014). Por lo tanto, este pilar consiste en la capacidad de demostrar la participación de las partes (origen y destino), mediante su identificación, en una comunicación determinada. Para garantizar esto, se necesita establecer dos mecanismos: la identificación, proceso que permite identificar a un usuario de un sistema y la autenticación, el cual verifica la identidad o asegura que un usuario es quien dice ser. Además, se suele aplicar a contratos formales establecidos de manera telemática, comunicación entre dos partes, transferencia de datos y acciones de los usuarios en un sistema informático. (UNIR, la Universidad en Internet, 2021)

A través de un ejemplo práctico sobre los principios de la seguridad de la información, el autor Oscar Schmitz (2014) menciona lo siguiente: “Si alguien roba un activo de información, una persona no autorizada podría leer y difundir la información contenida. Desde esta situación podemos aseverar, en principio, que está en peligro la confidencialidad de la información. Ahora si la persona no autorizada, corrompe, modifica o borra la información contenida, impactaría directamente en problemas de integridad. Finalmente, si la información contenida no fue copiada en otro soporte a modo de resguardo, podrían sucederse problemas de disponibilidad, dado que ninguna persona accedería a esta información”. Y para el caso del no repudio, en una firma digital por ejemplo, podemos garantizar que el autor no puede negar haber firmado cierto documento o mensaje.

2.5.2 IMPORTANCIA DE LA CIBERSEGURIDAD

Cada vez es más habitual encontrarnos con noticias de ataques a empresas de todo el mundo, desde el secuestro de computadores que impide el normal funcionamiento de la compañía, hasta el robo de sus bases de datos, lo que implica un enorme problema de seguridad para las mismas.(Legálitas, 2017).

La seguridad de las tecnologías de la información y comunicación (ciberseguridad) se está convirtiendo en una de las principales preocupaciones de los responsables de las empresas, que no dudan en invertir grandes cantidades de dinero en todo tipo de sistemas que les garanticen cubrir las contingencias no deseadas con la mayor solvencia posible (DataDec, 2019). Al igual que buscamos proteger nuestra casa y los objetos de valor con puertas, llaves, cajas fuertes, alarmas e incluso sistemas de video vigilancia, la información de las empresas también se debe proteger con medios que permitan garantizar que no habrá lugar para ataques informáticos.

Solo para crear un contexto de la importancia de la ciberseguridad, el Panorama de Amenazas en América Latina 2021 de Kaspersky, en su informe anual revela un aumento del 24% en ciberataques en la región durante los primeros ocho meses del año, en comparación con el mismo periodo en 2020. El informe toma en cuenta los 20 programas maliciosos más populares, los cuales representan más de 728 millones de intentos de infección en la región—un promedio de 35 ataques por segundo. Los países más atacados son Brasil (más de 5 millones de intentos de ataque este año), Colombia (1,8 millones), México (1,7 millones), Chile (1 millón) y Perú (507 mil). El informe también destaca que Costa Rica (378%), Venezuela (113%) y Argentina (91%) son los países con mayor crecimiento en ataques de RDP (protocolo de escritorio remoto) en comparación al año pasado. Por lo tanto, la conclusión de los especialistas es clara: la seguridad de las tecnologías para el trabajo remoto debe ser prioridad y la piratería, tanto en dispositivos personales como profesionales, debe ser erradicada. (Hernan Diazgranados, 2021).

En esencia, debemos recordar que un correcto nivel de seguridad de una empresa no pasa solamente por contar con los mejores recursos técnicos posibles. También es igual de necesario trabajar con los empleados para involucrarlos de manera positiva y efectiva en todo el proceso de la ciberseguridad. La ciberseguridad ya no es solo responsabilidad de los informáticos, sino de todos. Cada uno de nosotros somos quienes visitamos enlaces sospechosos, quienes descargamos archivos desconocidos y quienes ignoramos las advertencias de seguridad de nuestras aplicaciones. Y, en ese sentido, la importancia de la ciberseguridad y de la autoprotección radica precisamente en ser responsable y cauteloso para evitar riesgos y sorpresas indeseables al estar conectado y desconectado. (DataDec, 2019).

2.5.3 SITUACIÓN GENERAL DE LA CIBERSEGURIDAD EN ARGENTINA

Agustín Spinelli Riso (2018), explica muy detalladamente que la ciberseguridad es un tema que preocupa a nivel global. El Estado tiene la obligación de involucrarse en el despliegue de los mecanismos de difusión de los recaudos que los ciudadanos deben tomar al respecto, como así también establecer medidas de prevención de incidentes informáticos.

Es por ello, que el gobierno ha tomado conciencia de la problemática existente en torno a la seguridad informática y ha comenzado a tomar algunas medidas, creando así el Comité de ciberseguridad que tendrá como principal objetivo desarrollar una estrategia nacional de seguridad informática, enfocada en la mejora de los marcos normativos existentes para abarcar la creciente aparición de ciberincidentes y el desarrollo de medidas técnicas, políticas y procedimientos que permitan establecer una cultura de ciberseguridad en el país.

Por otro lado, el grado de madurez de la ciberseguridad en Argentina puede ser analizado a partir de los diferentes ejes de análisis propuestos por el Observatorio de la Ciberseguridad en América Latina y el Caribe[13]. De esta manera, podremos aproximarnos al contexto actual de la ciberseguridad en Argentina y analizar el escenario que se presenta para el crecimiento de las organizaciones (ver *Anexo 10*). Pero, si analizamos detalladamente los ejes planteados, vemos que aún no existe mucho avance en cuanto a ciberseguridad, por lo tanto queda mucho trabajo por realizar, y esta problemática es un punto central que el Estado debe resolver.

En conclusión, Argentina aún se encuentra en una etapa inicial de concientización y aprendizaje en el ámbito de la ciberseguridad. Dada la complejidad y relevancia del tema abordado, el cual afecta de manera transversal a todos los sectores de la sociedad, resulta necesaria la participación y colaboración conjunta de los distintos actores (sector público, privado y particulares). En este proceso, el rol del Estado adquiere suma trascendencia para demostrar la importancia de su tratamiento. La cooperación entre el sector público y el privado debe ser un paso inicial para compartir experiencias y generar una comunidad en donde se discutan sobre las mejores prácticas en ciberseguridad. Para ello es fundamental la adopción de normas que primero motiven y luego obliguen a las organizaciones a denunciar los ciberincidentes, ya que las compañías se resisten a reportar públicamente estos sucesos.

No obstante, a pesar de todos los esfuerzos que se puedan realizar para crear una cultura de concientización y cooperación, resulta oportuno retomar una de las ideas principales del presente trabajo: la seguridad absoluta no existe y, por lo tanto, lo mejor que se puede hacer es minimizar los riesgos y atenuar el impacto de un eventual ciberincidente.

También hay que tener en cuenta que el crecimiento y la sofisticación de las amenazas informáticas plantean un nuevo panorama en el cual algunos creen que solo es cuestión de tiempo hasta padecer las consecuencias de algún incidente de seguridad, que podría estar relacionado con la información. Dado este escenario de evolución del malware y otras amenazas, cobran relevancia los equipos de respuesta a incidentes de seguridad—CSIRT por las siglas de Computer Security Incident Response Team. (Miguel Ángel Mendoza, 2015).

[13] Inter-American Development Bank. (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020.*

Andrés Cargill Medel (2018), en su artículo define un CSIRT como un "*equipo, interno o externo a la organización, cuyo objetivo principal es minimizar y controlar los daños ante un ciberataque*". Este también cumple las funciones de asesorar, responder y recuperar la normalidad en las operaciones, así como prevenir que ocurran futuros incidentes. Para lograrlo, actúa como coordinador de todas las áreas, individuos y procesos involucrados en un incidente.

En la operación regular de un CSIRT se ejecutan 3 tareas primordiales: la recepción de la información sobre una incidencia de ciberseguridad, el análisis de dicha incidencia y sus posibles ramificaciones, y por último, una respuesta para solucionar el problema.

Por ello, los principales roles de los CSIRT son:

- Revisar arreglos y procedimientos estándar de seguridad.
- Detectar, analizar, responder y prevenir ciberamenazas.
- Priorizar y escalar alertas y tareas.
- Gestionar auditorías y entrenamiento ante nuevas amenazas.
- Realizar estudios forenses sobre los incidentes.
- Investigar nuevas formas de amenazas.
- Desarrollar planes de comunicación para públicos, clientes, trabajadores y directorio.
- Coordinar y ejecutar las estrategias de respuesta.
- Mantener un registro de todas las actividades para referencias futuras.
- Mantener un registro para cumplir normas y regulaciones.
- Gestionar el manejo remoto de la información crítica (contraseñas o configuraciones de red).

En Argentina existen diferentes CSIRT en los que uno puede consultar o bien reportar aspectos sobre incidencias de seguridad, sean estos a nivel gubernamental, provincial, institucional o empresarial. La *Tabla 01* detalla los CSIRTS más importantes existentes en nuestra región.

Todas estas organizaciones tienen como objetivo la gestión y el asesoramiento ante incidentes de ciberseguridad, la difusión de estrategias para su aplicación a nivel individual y empresarial, y la capacitación para prevenir posibles ciberataques. De esta forma, los CSIRT cobran especial importancia en dos situaciones: la primera, cuando la organización está atravesando un cambio estructural, de tecnologías o de procesos—durante los cuales ya es recomendable tener el equipo conformado—y la segunda, cuando considera que su ciberseguridad está en un nivel de riesgo elevado. (Andrés Cargill Medel, 2018).

TABLA 01 - CSIRTS DE ARGENTINA

Centro de Ciberseguridad del Gobierno de la CABA	Organización Host	Gobierno de la Ciudad Autonoma de Buenos Aires
	Comunidad Objetivo	a) Infraestructura del Gob. de CABA b) El ciudadano de la Republica Arg.
	Contacto	(+54) 11 4323 - 9362
	Web Corporativa	www.ba-csirt.gob.ar
NIC Argentina	Organización Host	NIC Argentina
	Comunidad Objetivo	Dominios .AR
	Contacto	(+54 11) 5235 - 1160
	Web Corporativa	https://nic.ar
ArCERT	Organización Host	Gobierno
	Comunidad Objetivo	Gobierno
	Contacto	(+54) 291 - 459 - 5102
	Web Corporativa	www.icic.conicet.gob.ar
CERT Ejército Argentino	Organización Host	Ejército Argentino
	Comunidad Objetivo	Ejército Argentino
	Contacto	(+54) 11 43466100 (int 2203)
	Web Corporativa	https://www.argentina.gob.ar/ejercito
CSIRT-NQN	Organización Host	OPTIC - Gobierno del Neuquén, Argentina
	Comunidad Objetivo	Administración Pública y Empresas del Estado Provincial
	Contacto	-
	Web Corporativa	https://csirt-nqn.neuquen.gov.ar
CSIRT CABASE	Organización Host	CABASE
	Comunidad Objetivo	Miembros asociados a CABASE
	Contacto	(+54 11) 5263 - 7456
	Web Corporativa	www.cabase.org.ar

FUENTE Elaboración propia en base a *LANIC CSIRT.*

2.5.4 LEGISLACIÓN ARGENTINA EN CIBERDELITOS

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones y estafas. Sin embargo, debe destacarse que con el uso de las técnicas informáticas se han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. (Cristian Borghello).

Por lo tanto, se definió como Delito Informático a "*cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos*." (Cristian Borghello).

Agustín Spinelli Riso (2018) indica que en la normativa Argentina, existen tres leyes que encuadran las distintas figuras delictivas del ámbito de la ciberseguridad, las cuales resultan pertinentes enunciar en función de los objetivos planteados en la presente investigación:

- En primer lugar, la Ley de Protección de Datos Personales (Ley 25.326), tal como establece el art. 1, tiene como objetivo la protección integral de los datos personales asentados en archivos, registros, banco de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas.

- En segundo término, la Ley de Propiedad Intelectual (Ley 11.723) establece la protección del derecho de propiedad sobre obras científicas, literarias y artísticas, incluyendo los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto.

- Por último, la Ley de Delito informático (Ley 26.388) que sustituye, modifica e incorpora figuras delictivas a diversos artículos del Código Penal con el fin de regular las nuevas formas de cometer delitos a través de medios tecnológicos.

De esta manera, se establece sanciones por el acceso ilegítimo a los sistemas o datos informáticos, violación de correos electrónicos (email), daño informático y distribución de códigos maliciosos, e interrupción de las comunicaciones.

2.5.5 CIBERINTELIGENCIA: UN NUEVO PARADIGMA EN LA CIBERSEGURIDAD

Constantemente escuchamos acerca de los riesgos a los que estamos expuestos en el ciberespacio y de la relevancia que está tomando la ciberseguridad. Por ello, ante este nuevo contexto de ciberamenazas avanzadas en las cuales están involucrados grupos criminales y hacktivistas con motivaciones políticas y económicas, contar con una estrategia de ciberinteligencia se vuelve un elemento clave para reforzar la estrategia de seguridad de la información. (Marcos Polanco, 2016).

Pero para empezar a hablar de ciberinteligencia, debemos entender primero la inteligencia; definida como la capacidad de razonar, evaluar, interpretar y generar información útil para luego transformarla en conocimiento que nos permitirá resolver problemas y de esa forma tomar decisiones con el menor nivel de incertidumbre. Por lo tanto, con base a esto y teniendo en cuenta el

ciclo de inteligencia[14], aparecen diversos tipos de inteligencia: lingüística, espacial, emocional, territorial, lógica, militar, etc. hasta llegar finalmente a la ciberinteligencia. (Departamento de Comunicaciones INISEG, 2018).

De esta manera, podemos definir el término de ciberinteligencia como la *"adquisición y análisis de información, para identificar, rastrear, predecir y contrarrestar las capacidades, intenciones y actividades de los criminales, y ofrecer cursos de acción, que mejoren la toma de decisiones"*. Con esto, es claro que el viejo paradigma de proteger las redes y sistemas no basta, tenemos que enfocar nuestros esfuerzos en proteger, detectar y actuar. Debemos planear la estrategia y acciones a partir de la premisa de que nuestra red será comprometida, incluso considerar que ya hemos sido comprometidos. Es aquí donde la ciberinteligencia comienza a convertirse en una habilitadora vital para la ciberseguridad. (Marcos Polanco, 2016).

De esta manera, el proceso general para la generación de ciberinteligencia consta de cinco pasos:

1. *Identificación del objetivo*
   Determinar qué es lo que queremos encontrar o qué respuesta es la que queremos responder.

2. *Colección de información*
   Definir las fuentes de información que utilizaremos; pueden ser internas o externas, abiertas o privadas, manuales o automáticas.

3. *Análisis*
   Preparación y análisis de la información, utilizando diversas técnicas y herramientas.

4. *Identificación de hallazgos*
   Encontrar aquellos elementos que son relevantes y que ayuden a confirmar o rechazar las hipótesis planteadas.

5. *Difusión*
   Hacer llegar a las partes interesadas los hallazgos y cursos de acción propuestos.

De acuerdo con US Naval War College, existen varios tipos diferentes de fuentes de inteligencia, cada una de ellas puede ser de mayor o menor utilidad dependiendo de cuáles sean las áreas de interés y los objetivos. Las disciplinas más importantes son:

[14] *Ciclo de inteligencia*: modelo de 6 fases que representa la inteligencia como proceso y se suele utilizar de forma pedagógica para explicar qué es la inteligencia.

— *Inteligencia de código abierto (OSINT)*

Se refiere a una amplia gama de información y fuentes que están disponibles públicamente, incluida la información obtenida de los medios de comunicación (periódicos, radio, televisión, Internet, etc.), registros profesionales y académicos y otros datos públicos. Debido a la gran cantidad de información disponible, determinar la fuente de los datos y su confiabilidad puede ser realmente complicado.

— *Inteligencia humana (HUMINT)*

Es la recopilación de información a través de fuentes humanas. y puede hacerse abiertamente. Por ejemplo, cuando los agentes del FBI entrevistan a testigos o sospechosos. Dentro de los Estados Unidos, la recolección es responsabilidad del FBI.

— *Inteligencia de señales (SIGINT)*

Se refiere a transmisiones electrónicas que pueden ser recolectadas por barcos, aviones, sitios terrestres o satelitales. Por ejemplo, la inteligencia de comunicaciones (COMINT) es un tipo de SIGINT y se refiere a la intercepción de comunicación entre dos partes.

— *Inteligencia de imágenes (IMINT)*

Conocida como inteligencia fotográfica (PHOTINT), tuvo lugar durante la primera y segunda guerra mundial cuando ambos bandos tomaron fotografías desde aviones. En la actualidad, la mayor parte de IMINT es realizada utilizando imágenes satelitales.

— *Inteligencia de mediciones y firmas (MASINT)*

Es una disciplina de recopilación que se refiere a las capacidades de las armas y las actividades industriales. MASINT incluye el procesamiento avanzado y el uso de datos recopilados de los sistemas de recopilación IMINT y SIGINT aéreos.

2.6 AMENAZAS Y ATAQUES INFORMÁTICOS

A pesar de los grandes avances tecnológicos, los sistemas informáticos siguen presentando grandes vulnerabilidades, es decir que poseen determinados aspectos débiles a través de los cuales pueden ser atacados y recibir algún tipo de daño en cualquiera de sus componentes afectando el funcionamiento normal o previsto de dicho sistema informático. En este sentido, la seguridad de un sistema representa el estado de protección que posee el mismo, para evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento. (Daniel Caffaratti y Lorena Holc, 2017).

2.6.1 CONCEPTOS ÚTILES

- *Amenazas informáticas*

  Una amenaza es la posibilidad de realizar un daño a un sistema de información que, en un momento dado, podría ocasionar una violación de seguridad. Por lo tanto, los responsables del sistema tienen el deber de establecer una política de seguridad y realizar un análisis de riesgos para identificar las posibles amenazas y contrarrestarlas. [15]

- *Ataques cibernéticos*

  Un ataque es un intento de destruir, exponer, alterar, inutilizar, robar, acceder o usar de forma no autorizada de un recurso. También se puede describir como la ejecución de una amenaza. [16]

- *Vulnerabilidades*

  Una vulnerabilidad de una manera muy general es un fallo en un sistema que puede ser explotado por un atacante generando un riesgo para la organización o para el mismo sistema. Existen dos tipos de vulnerabilidades: las físicas las cuales van a afectar a la infraestructura de la organización de manera física y las lógicas que afectan directamente la infraestructura y el desarrollo. [17]

- *Riesgo informático*

  El riesgo es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional. Por lo tanto, se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad. [18]

[15, 16] José Fernández. (2013). *Virtual honeynets*. Universidad de Almería (UAL), Almería, España.

[17, 18] Martha I. Romero, Grace L. Figueroa, Denisse S. Vera, José E. Álava, Galo R. Parrales, Christian J. Álava, Angel L. Murillo y Miriam A. Castillo. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Primera edición.

2.6.2 TIPOS DE INTRUSOS

Dependiendo de su forma de actuar, su nivel de conocimiento y los objetivos que persigue un intruso se puede clasificar en alguno de los tipos que se muestran a continuación.

- *Hackers*

  Son personas apasionadas a la informática que invierten esfuerzos más allá de los habituales y convencionales en la tarea que realizan. A pesar de que la palabra hacker está estigmatizada socialmente asociado a algo malo, en realidad un hacker es una persona con un gran sentido de curiosidad, y utilizan esa virtud para detectar vulnerabilidades en los sistemas y evitar que personas maliciosas provoquen daño. (Daniel Caffaratti y Lorena Holc, 2017, pág. 141).

- *Crackers*

  Son personas cuyo objetivo va más allá de la simple investigación. Es una persona con fines malignos, haciendo daño solo por diversión o para demostrar sus habilidades. Según palabras de los propios hackers, estos consideran a los crackers como hackers mediocres, poco brillantes que buscan violar sistemas. (Jorge W. Trapp, 2009, pág. 27).

- *Phreakers*

  *S*on crackers pero de las redes de comunicación, con amplios conocimientos en telefonía. El objetivo principal de estos individuos es engañar a las compañías telefónicas para realizar llamadas gratis. (Jorge W. Trapp, 2009, pág. 27).

- *Script Kiddies*

  Son los aficionados, que prueban todos los programas que llegan a sus manos. Se aprovechan de los conocimientos de otros para presumir. La mayoría de las veces son los responsables de lanzar virus o bombas lógicas por las redes. (Jorge W. Trapp, 2009, pág. 27).

- *Insiders*

  Son individuos pertenecientes al personal de una organización que realizan ataques a los sistemas. Esto es muy alarmante ya que estas personas pueden conocer perfectamente los sistemas incluyendo los puntos débiles de este, pudiendo vulnerarlos más efectivamente que un atacante externo. Los tipos de insiders se pueden definir de acuerdo a la intención que puedan tener, algunos pueden ser: ex-empleado, curioso e intrusos remunerados. (Jorge W. Trapp, 2009, pág. 28).

- *Piratas informáticos*

  Su actividad consiste en la copia ilegal de programas o aplicaciones rompiendo sus sistemas de protección y licencias. Luego se distribuyen los productos por Internet, a través de CDs, DVDs, pendrives, entre otros, para venderlos ilegalmente. (Daniel Caffaratti y Lorena Holc, 2017, pág. 142).

2.6.3 TIPOS DE ATAQUES

Cuando hablamos de ataques (ver *Figura 04*), hay que tener en cuenta que existen dos tipos y que varían en función del modo de actuación. Por un lado tenemos ataques activos, los cuales exigen algún tipo de manipulación o interacción con el flujo de información transmitido a lo largo de un canal y por el otro, tenemos los ataques pasivos, en el cual, el intruso no altera la comunicación entre el origen y el destino, solo escucha y monitoriza el medio de comunicación con el fin de obtener la información que se está transmitiendo. (José Fernández, 2013).

FIGURA 04 - TIPOS DE ATAQUES EN CIBERSEGURIDAD

FUENTE Elaboración propia.

El mismo autor, describe algunas de las técnicas más utilizadas para llevar a cabo ataques informáticos:

1. ***Spoofing***

   Es un ataque o conjunto de técnicas orientadas a realizar acciones de suplantación de identidad con fines maliciosos. El atacante utiliza una dirección de origen falsificada para enviar paquetes a la red. Los ataques de spoofing se pueden clasificar dependiendo del protocolo o tecnología del ataque, por ejemplo: spoofing de correo electrónico, spoofing de IP y smart-spoofing IP.

2. ***Ingeniería social***

   Este ataque consiste en utilizar técnicas o habilidades sociales contra terceras personas para obtener información confidencial o de utilidad. Por ejemplo, un atacante puede usar el teléfono o Internet para engañar a las víctimas, haciéndose pasar por el empleado de su banco para conseguir el número de la tarjeta de crédito y poder usarla con fines fraudulentos. Algunas de las técnicas más utilizadas son: phishing, sextorsión, pretexting, baiting, tailgating, etc.

3. ***Man in the middle (MiTM)***

   El objetivo de este ataque es interceptar, leer o manipular de forma efectiva la comunicación entre la víctima y sus datos sin que nadie se dé cuenta de que hay una tercera persona incluida en la operación. Es decir, es el método por el cual un ciberdelincuente interviene en el tráfico de datos de las dos partes vinculadas, haciéndose pasar por cualquiera de ellas, y haciéndoles creer que se están comunicando entre ellos cuando en realidad es el intermediario quien recibe la comunicación. (Andres Rodríguez, 2019).

4. ***Desbordamiento de búfer***

   Es un error de software que tiene lugar cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande como para contenerlos, sobrescribiendo otras zonas de memoria. Sobrescribir zonas de memoria puede ocasionar resultados impredecibles. Bajo ciertas condiciones, un atacante puede aprovecharse de esta vulnerabilidad para conseguir acceso o control del sistema.

5. ***Cross-Site Scripting (XSS)***

   Los ataques XSS se basan en la posibilidad de ejecutar código de script, como JavaScript o VBScript, en páginas o aplicaciones programadas en HTML. Al igual que ocurriría con los ataques de inyección SQL, los ataques XSS tienen éxito gracias a una validación incorrecta de los datos de entrada que permite ejecutar el código inyectado. La explotación de vulnerabilidades de tipo XSS permiten al atacante robar información sensible del usuario, secuestrar sesiones de usuario o comprometer el navegador, entre muchas otras posibilidades. Las vulnerabilidades de XSS pueden presentarse en dos tipos: directa/persistente, en donde el código es almacenado permanentemente en el servidor destino o bien indirecta/reflejado, el cual consiste en modificar valores que la aplicación web utiliza para pasar variables entre dos páginas, sin usar sesiones.

6. ***Inyección de código SQL***

Los ataques de inyección de código SQL son un tipo específico de ataques por inyección, extensibles a cualquier otro lenguaje de programación. Este ataque consiste en la inserción directa de código en variables especificadas por el usuario que se concatenan con comandos SQL y se ejecutan en un motor de una base de datos. El resultado exitoso de este ataque permite leer información sensible de la base de datos, modificar los registros de la base de datos mediante sentencias SQL (insertar, actualizar, eliminar), ejecutar operaciones de administración sobre la base de datos y, en algunos casos, emitir comandos en el sistema operativo. El origen de esta vulnerabilidad reside en una incorrecta comprobación o filtrado de las variables utilizadas en un sentencia SQL.

7. ***Denegación de servicio (DoS)***

Este tipo de ataque, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o bien una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como a la red informática. (OSI Team, 2018). El autor menciona además, que existen dos técnicas para este tipo de ataques:

- *Denegación de servicio (DoS):* generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones.

- *Denegación de servicio distribuido (DDoS)*: se realizan peticiones o conexiones empleando un gran número de computadoras o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones provienen desde diferentes IPs y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

8. ***Sniffing***

Es un ataque que, utilizando una aplicaciones específicas, permiten capturar la información que está siendo transmitida en un segmento de red. El objetivo es obtener información sensible, tales como usuarios, contraseñas, correos electrónicos, ficheros transmitidos, etc. Existen muchos protocolos que no cifran los datos transmitidos, lo que los hace propensos a este tipo de ataques. Algunos protocolos que no incluyen cifrado de los datos son: HTTP, SMTP, POP, FTP e IMAP.

9. ***Bots***

Un bot suele utilizarse para designar a un tipo determinado de software malicioso que una vez que ingresa en una computadora afecta de manera directa al sistema, convirtiéndola en una especie de robot autómata. Los boots forman parte de las botnets (zombi), redes de computadoras infectadas de todo el mundo que pueden ser controladas de forma remota, utilizadas para distribuir otros tipos de malware, ya que en líneas generales el software bot funciona en muchos casos como un troyano, por lo que hace posible que se descarguen en la computadora infectada todo tipo de software sin el permiso del propietario de la computadora. (Graciela Marker, 2017).

10. Malware

Es un tipo de software cuyo objetivo es dañar un sistema de información sin el consentimiento de su propietario. El éxito del malware es posible gracias a las vulnerabilidades de las que se aprovechan para expandirse, como bugs, errores de los usuarios, debilidades de protocolos, etc. El malware engloba a una gran variedad de aplicaciones maliciosas y son clasificadas según el funcionamiento u objetivo para el que han sido desarrolladas:

- *Virus*. Tiene por objetivo alterar el funcionamiento normal de un sistema de información sin el consentimiento del propietario. Generalmente destruyen o corrompen los datos almacenados en el sistema. Se propagan a través de un software infectado, pero no pueden reproducirse.

- *Gusanos*. Tiene la capacidad de replicarse así mismo y de propagarse a otros sistemas. La propagación la realizan a través de una red, enviando copias de sí mismos a otros sistemas. Pueden generar cientos de copias, lo que puede provocar un colapso de los recursos de red e influir negativamente en la capacidad de procesamiento del mismo.

- *Troyanos*. Es un software que permite la administración remota de un sistema de forma oculta y sin consentimiento de su propietario. Este software intenta aparentar un programa legítimo para conseguir que la víctima lo ejecute, pero esconde un troyano en su interior que infectará al sistema. Existen muchos tipos, como backdoors, downloaders, rootkits, etc.

- *Spyware*. Son aplicaciones que recopilan información sobre las actividades realizadas por una víctima y toda la información es distribuida principalmente a agencias de seguridad u otras organizaciones interesadas a cambio de un beneficio. Generalmente, este tipo de malware accede al sistema víctima a través de páginas webs que incitan a la instalación de complementos en el navegador.

2.6.4 ANATOMÍA DE UN ATAQUE INFORMÁTICO

Empresas y expertos en seguridad informática han establecido cinco fases a las cuales se conocen también como círculo hacker (ver *Figura 05)*. Los atacantes sean estos éticos o no éticos siempre seguirán esta secuencia, pero puede variar las técnicas y herramientas que utilicen. Conocer esto ayudará a las buenas prácticas de la seguridad informática y sobrellevar sus desafíos. (Byron V. Guamán, 2015, pág. 22).

FIGURA 05 - MODO DE OPERACIÓN DE UN ATAQUE INFORMÁTICO

FUENTE Elaboración propia.

Según el autor Byron V. Guamán (2015), el círculo hacker es el esqueleto que comprende una anatomía de un ataque informático. A continuación detallaremos brevemente cada fase:

1. *Reconocimiento*

   El reconocimiento consiste en la investigación de toda la información que se pueda obtener con el uso de herramientas o métodos de la persona, institución o empresa a la cual se va a atacar. Toda información sea muy importante o insignificante que se recopile servirá a la hora del ataque, obteniéndose de una forma activa cuando tenemos una interacción directa con el objetivo o de una manera pasiva cuando no se tiene interacción directa con el objetivo.

2. *Exploración*

   Una vez recopilada la información, se actúa de una manera más activa con el objetivo, siendo necesario tener algún tipo de conexión, para luego realizar la búsqueda de vulnerabilidades en la red. Utilizando el reconocimiento activo se podrán tener más respuestas del objetivo, ya sean hosts accesibles, puertos abiertos, detalles de sistemas operativos y servicios. Las herramientas utilizadas en esta fase se basan en el concepto del protocolo TCP (Protocolo de Control de Transmisión) y el three-way handshake para establecer la comunicación entre dispositivos.

3. *Obtener acceso*

   Es la fase donde verdaderamente se realiza el ataque, y el daño que se ocasione está en función de la información recopilada y de las habilidades del atacante. El ataque puede ser a nivel de

red, aplicación y de sistema, donde no necesariamente puede implicar un acceso. Esta es la fase más importante porque se explotan vulnerabilidades encontradas y se toma el control de la víctima mediante el uso de herramientas, tales como exploits o bugs para lograrlo.

4. *Mantener acceso*

   Consiste en dar continuidad al ataque con el fin de hacer más daño a la víctima, controlando el sistema al que ya se logró acceder. Es la fase más peligrosa para un atacante, debido a que puede lograr robar información tanto personal, empresarial u otra información clave haciendo mucho daño a la víctima. Existen diversas maneras de mantener un acceso, ya sea mediante malware o bien utilizando sniffer, teniendo como principal factor la habilidad del atacante y la forma como quiera mantener el acceso. Esta fase se caracteriza por no solo hacer daño al equipo donde se ingresó, sino también porque puede infectar otros equipos de la misma red.

5. *Borrar huellas*

   La última fase consiste básicamente en eliminar todo tipo de datos, huellas o información que pueda evidenciar que existió algún tipo de ataque. Es aquí donde se marca la diferencia entre un atacante con experiencia (no deja ninguna huella) y un atacante principiante (que simplemente su objetivo es causar daño). Es importante para un atacante destruir la información que lo implicaría, debido a que esto lo ayudaría a seguir manteniendo acceso al objetivo y el administrador de la red nunca tendría ninguna pista de quién pudo haber causado tal daño.

2.6.5 MEDIDAS BÁSICAS DE PROTECCIÓN

Durante la tercera revolución industrial, el principal reto de las empresas fue establecer de forma efectiva la seguridad en Internet, pero en la cuarta revolución industrial, este sigue siendo un elemento crucial para las organizaciones. De esta forma, la ciberseguridad juega un papel crucial, debido a que ayuda a prevenir daños por alteración, interrupción o mal uso de las tecnologías TI. Los daños en cuestión, podrían incluir el deterioro de la disponibilidad de las TI, restricción sobre estas, o la violación de la confidencialidad y/o la integridad de la información almacenada en los entornos TI. Por ello, es de vital importancia que las empresas cuenten con una estrategia integral de ciberseguridad y sepan cuáles son las medidas más adecuadas para proteger su información y recursos. El riesgo cibernético puede y debe ser mitigado aplicando las medidas necesarias y actuando efectivamente. (KPMG México, 2018).

KPMG México plantea una serie de medidas que toda compañía debe tomar en cuenta para poder proteger su información:

1. *Proteger sus activos más importantes*

   En vista de la dificultad que implica proteger toda una organización, la ciberseguridad requiere una atención especial para salvaguardar la información más valiosa de la empresa; hay que identificar qué activos son realmente importantes.

2. *Informar y capacitar a su capital humano*

   Contar con tecnologías para llevar a cabo la protección, identificar a los intrusos y responder a un ataque resulta indispensable para las organizaciones, sin embargo, el ser humano suele ser el eslabón más débil. Por ello, la alta dirección de una empresa debe abordar la ciberseguridad de manera estructural, destinando los recursos necesarios para mantenerla segura.

3. *Complementar las medidas preventivas con las de detección*

   Enfocarse en el monitoreo técnico para analizar y detectar el flujo de información, así como implementar medidas preventivas para evitar incidentes de ciberseguridad.

4. *Enfocarse en la capacidad de respuesta de la empresa*

   Es cuestión de tiempo que una empresa se convierta en víctima de un incidente cibernético. Incluir planes de contingencia contra estos ataques y un protocolo para las comunicaciones durante un suceso de este tipo, debe ser una prioridad para la compañía.

5. *Fomentar la cooperación entre organizaciones*

   Es crucial que las compañías se mantengan actualizadas e informadas sobre amenazas emergentes y aprendan de otras organizaciones las mejores tácticas para reaccionar ante los incidentes. Para facilitar esto, existen organismos cuyo objetivo es ayudar a otras en ese ámbito. También es importante promover la participación activa de la empresa en este tipo de redes; un incidente en otra entidad es, de igual forma, una amenaza potencial para la propia organización.

6. *Invertir con base en los riesgos de la empresa*

   Con el fin de determinar el perfil de riesgo de una empresa, debemos utilizar un modelo que cubra cinco diferentes aspectos. En el ambiente de negocio, hay que identificar cuáles son los mercados en los que se encuentra activa la entidad y cómo se desempeña en los mismos. Tenemos que estar conscientes de las amenazas y vulnerabilidades que podrían explotar los cibercriminales y anticipar a qué grupo de delincuentes cibernéticos le resulta atractiva la compañía y con qué recursos podría desplegar el ataque. Asimismo, teniendo claros qué objetivos podrían estar sujetos a ataques en la organización y qué requisitos legales debemos

cumplir en materia de ciberseguridad, se pueden destinar los recursos pertinentes para mantener protegida a la empresa.

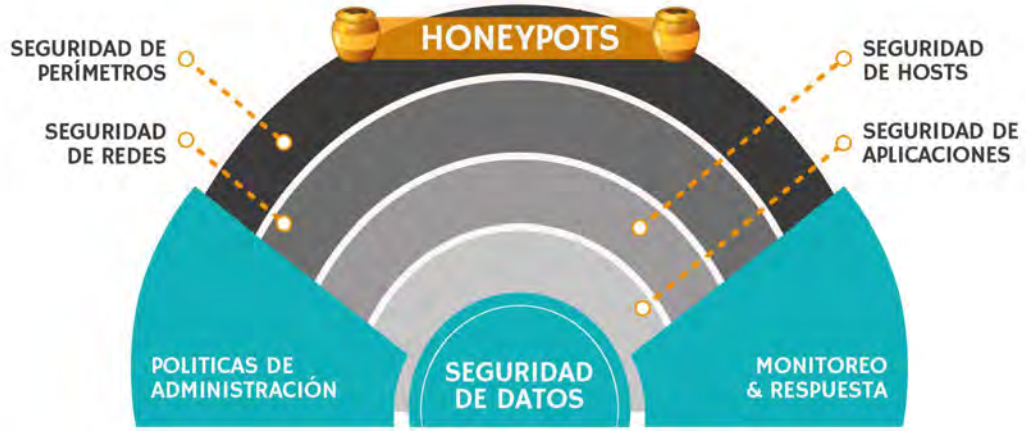
7. *Actualizar el modelo de protección para anticipar amenazas emergentes*
   Las estrategias de ciberseguridad de una compañía tienen que actualizarse constantemente para hacerle frente a nuevas amenazas que surjan. Estas nuevas estrategias deben cubrir las capacidades de respuesta y la integración con otras áreas, tomando como base la inteligencia de amenazas y los activos más importantes para el atacante.

Por lo tanto, toda organización sin una estrategia integral de ciberseguridad está expuesta tanto a la pérdida de recursos como a riesgos a su propia integridad, la de sus clientes y su reputación. Por tal motivo se debe contar con la asesoría especializada en ciberseguridad para seguir las mejores prácticas y así salvaguardar la información más importante, además de capacitar adecuadamente al personal para proteger mejor los activos de la compañía.

2.6.6 DEFENSA EN PROFUNDIDAD

La defensa en profundidad (Defense in Depth), se trata de un modelo que pretende aplicar controles en seguridad para proteger los datos en diferentes capas (ver *Figura 06*).

FIGURA 06 - DEFENSA EN PROFUNDIDAD



FUENTE Elaboración propia en base a *US SIGNAL, 2020.*

Según el CIS (Centro para la Seguridad de Internet), se define Defensa en Profundidad como un enfoque que pretende implementar una serie de mecanismos y controles tecnológicos heterogéneos de forma selectiva para proteger la confidencialidad, integridad y disponibilidad de la red y los datos que esta contiene. Si bien ninguna tecnología o control individual puede contener todas las

amenazas y ataques, juntas brindan mitigaciones frente a una amplia variedad de estas, al tiempo que incorporan diversidad y redundancia en caso de que algún mecanismo o control particular fallara. (Nicolas Raggi, 2021).

Este modelo plantea la concepción de la seguridad como el efecto de una eficiente administración del riesgo, y propone una estructura definida en capas en las cuales se pueden implementar acciones estratégicas para asegurar cada una de estas capas, y en el caso que alguna amenaza logrará filtrar la seguridad de alguna de estas capas, la siguiente capa, contará con sistemas de protección diferente y a otro nivel, logrando así mitigar los riesgos y evitar que el ataque pase a una siguiente etapa. Es importante mencionar, que cada acción de protección tiene un costo, por lo que en cada caso debe evaluarse el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque, y en este sentido planificar las acciones pertinentes para la protección de tal información. (EdwinRSV, 2011).

A su vez, Wendy Cruz (2011), en su artículo explica cada una de las capas de seguridad que tiene el modelo, considerando que este tipo de seguridad es una postura muy efectiva, debido a que emplea múltiples herramientas y técnicas para detener a un atacante. Las capas que se incluyen son:

- *Seguridad física*

  Esta capa debe implementarse correctamente para evitar que cualquier atacante obtenga acceso a la red interna y cause algún tipo de daño. Por ello, la seguridad física es un elemento fundamental en una estrategia de seguridad global, ya que abarca ubicaciones de servidores y/o dispositivos, centro de las bases de datos, acceso a los edificios de la organización, entre otros.

- *Seguridad de perímetros*

  Es el aspecto más importante para detener los ataques externos. Si su perímetro permanece seguro, la red interna estará protegida de ataques externos. Por lo tanto, la organización debe disponer de algún tipo de dispositivo de seguridad para proteger cada punto de acceso a la red y evaluar cada dispositivo para decidir qué tipos de tráfico se permitirán y en base a ello, desarrollar un modelo de seguridad para bloquear el resto del tráfico. Como herramientas en esta capa, se utilizan antivirus, firewalls, IDS, honeypots, anti-malware, entre otros.

- *Seguridad de redes*

  Si dispone de una serie de redes en la organización, debe evaluarse individualmente cada red para asegurarse de que se ha establecido una seguridad apropiada. Es decir, se debe examinar el tráfico admisible, bloquear el que no sea necesario y usar SSL para comunicaciones externas.
- *Seguridad de hosts*

Se debe evaluar cada host del entorno y crear directivas que limiten cada servidor sólo a las tareas que tenga que realizar. De este modo, se crea otra barrera de seguridad que un atacante deberá superar antes de poder provocar algún daño.

- *Seguridad de aplicaciones*

  El refuerzo de las aplicaciones es una parte esencial de cualquier modelo de seguridad. Por lo tanto, es responsabilidad del programador incorporar la seguridad en la aplicación para proporcionar una protección adicional a las áreas de la arquitectura a las que la aplicación puede tener acceso.

- *Seguridad de datos*

  Para muchas empresas, uno de los recursos más valiosos son los datos, debido a que si caen en manos equivocadas, podrían provocar grandes daños. Por ello, los datos deben protegerse y una las formas es incluir sistemas de cifrado y listas de control de acceso en los archivos (ACL).

- *Políticas, procedimientos y concientización*

  Establecen el tono en toda la organización con relación a la protección de los activos, definen los objetivos y actividades de control y proveen un criterio de auditoría para el programa de seguridad. Para ser efectivas, las políticas deben ser debidamente comunicadas a todo el personal de la empresa.

A continuación, se detalla algunas recomendaciones que propone la defensa en profundidad:

— *Antivirus*

  Es la encargada de detectar cuando un archivo, un correo, un proceso o en definitiva cualquier elemento informático del propio sistema intenta ejecutar código malicioso. Es decir, un antivirus solo localiza, y no tendría por qué tener la capacidad de contrarrestarlo, por eso, para detectarlos se cuentan con diferentes bibliotecas de malware, que están una y otra vez consultando para comparar con los elementos activos del sistema. Puesto que el pulso de la industria del crimen va por definición siempre por delante (primero se crea el virus, luego se localiza, y se genera una vacuna para él), cada marca de antivirus desarrolla diferentes técnicas de heurística que le permiten localizar archivos infectados por potenciales malwares (malwares que aún no han sido catalogados) mediante la búsqueda de elementos comunes o habituales en otras tipologías de malware. (Pablo F. Iglesias, 2015).

— *Firewalls (cortafuegos)*

La misión de un firewall es analizar y bloquear cualquier intento de conexión peligrosa con el sistema, habitualmente, desde Internet. El cortafuegos se puede aplicar a nivel de hardware, de software, o mixto, y cumple un papel trascendente en un entorno cada vez más dependiente del mundo online. A diferencia de los antivirus, los firewall funcionan en base a un acotado número de reglas que definen su ámbito de actuación y pueden ser configurados para que por defecto, sean permisivos, o por defecto, sean restrictivos. (Pablo F. Iglesias, 2015).

— *IDS (sistema de detección de intrusos)*

Es una herramienta encargada de detectar intentos de acceso no autorizado a una red o sistema. Su funcionamiento se basa en analizar continuamente los paquetes de comunicación que entran y salen del sistema, con el fin de localizar patrones comúnmente asociados a ataques de diversa índole y bloquearlos, es decir, que al detectar una violación de la política de seguridad, un virus o un error de configuración, un IDS puede expulsar al usuario infractor de la red y enviar una alerta al personal de seguridad. Por ende, mientras el firewall se dedica a analizar el tráfico de entrada y salida de la red, el IDS hace lo propio con lo que está ocurriendo dentro de ella. De ahí que sea habitual que los dos trabajen juntos: el firewall se encarga de bloquear intentos externos de ataque y la inteligencia del IDS protege de posibles fugas de información desde dentro. (Pablo F. Iglesias, 2015).

— *IPS (sistema de protección de intrusos)*

Complementa una configuración de IDS mediante la inspección proactiva del tráfico entrante de un sistema para eliminar solicitudes maliciosas. Una configuración típica de IPS utiliza firewalls de aplicaciones web y soluciones de filtrado de tráfico para proteger las aplicaciones. Además, un IPS evita ataques al descartar paquetes maliciosos, bloquear IPs ofensivas y alertar al personal de seguridad de posibles amenazas. Si bien es eficaz para bloquear los vectores de ataque conocidos, algunos sistemas IPS tienen limitaciones y estos son comúnmente causados por una dependencia excesiva de reglas predefinidas, haciéndolos susceptibles a falsos positivos. (Logitek Ciberseguridad Industrial, 2020)

— *VPN (red privada virtual)*

Una VPN es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet y de esta manera poder acceder a ciertos servicios, ocultando nuestra dirección IP real y enrutando nuestro tráfico a través de un túnel privado y cifrado de forma segura. La comunicación VPN ocurre a través de un software proporcionado por aquellos que administran servicios de VPN, de modo tal que si un usuario quiere utilizar el servicio de VPN simplemente deberá abrir el software, ingresar su nombre de usuario y contraseña y

conectarse. Una vez que complete este proceso de conexión, los servicios a los cuales desea acceder ahora estarán disponibles. (Daniel Cunha Barbosa, 2020).

— *Respuesta a incidentes*

Una respuesta a incidentes es una reacción acelerada a un problema. De esta manera, el incidente es la violación de la seguridad y la respuesta depende de cómo el equipo de seguridad reaccione, qué acciones toman para reducir los daños y cuándo reestablecen los recursos, todo esto mientras intentan garantizar la integridad de los datos. (Red Hat, 2005). Por lo tanto, es necesario contar con un CSIRT dentro las empresas, ya que sus propósitos son específicos y en muchos casos pueden evitar la materialización de amenazas.

CAPÍTULO 3 - ESTADO DE LA CUESTIÓN

3.1 ANTECEDENTES

Para implementar este proyecto, es necesario comprender ciertas investigaciones sobre seguridad de la información, redes informáticas y sistemas de información, de forma tal que nos permita formular unas buenas pautas de seguridad. Algunas de estas investigaciones son:

- *The Cuckoo's Egg* [1]

  El honeypot comenzó en 1991 con la publicación del informático Clifford Stoll, quien desde primera persona cuenta su experiencia atrapando a un cracker, debido a un simple error de contabilidad que logró detectar en el sistema donde trabajaba, y a partir de ahí empieza una cacería constante.

- *The Honeynet Project* [2]

  The Honeynet Project es una organización internacional líder en investigación de seguridad sin fines de lucro, dedicada a investigar los últimos ataques y a desarrollar las herramientas de seguridad de código abierto para mejorar la seguridad de Internet.

- *Honeypots: The Need of Network Security* [3]

  Este paper fue desarrollado en la India en 2014, y centra sus investigaciones en la introducción e importancia que tienen los honeypots hoy en día, y de cómo estos ayudan y mejoran la arquitectura de seguridad de la red de una organización.

- *Honeypot, hacia un protocolo de seguridad más eficiente y competitivo* [4]

  Esta investigación desarrollada por Kevin Martínez en 2018, busca definir de manera clara y concisa lo que es un honeypot, el cual es utilizado como una herramienta dentro del ámbito de la seguridad de la información para extraer y analizar el comportamiento de los atacantes, centrándose en el honeypot KIPPO como prueba experimental.

[1] Clifford Stoll. (2005). *The Cuckoo's Egg*. (1ra Ed.). Estados Unidos: Pocket Books.

[2] Lance Spitzner. (1999). *The Honeynet Project*.

[3] Navneet Kambow, Lavleen K. Passi. (2014). *Honeypots*: The Need of Network Security.

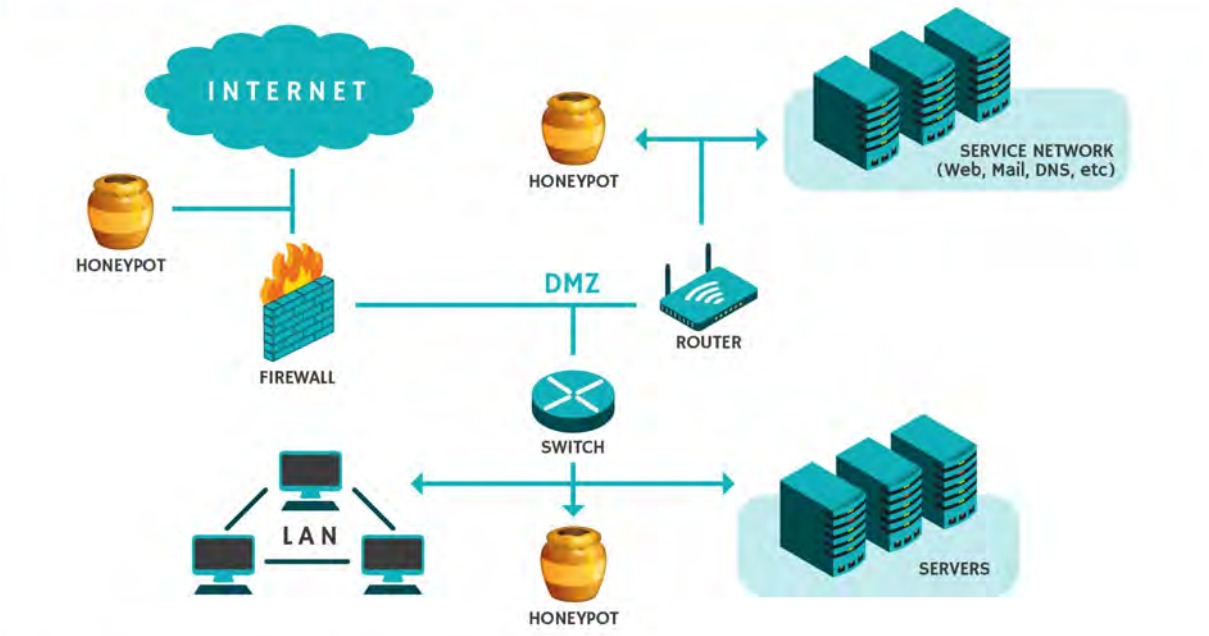
[4] Kevin David Martínez Contreras. (2018). *Honeypot, hacia un protocolo de seguridad más eficiente y competitivo*.

3.2 HONEYPOTS

Un Honeypot es un recurso de red que simula ser un objetivo real, pero destinado a ser atacado, de tal forma que un intruso pueda ingresar, examinarla y comprometerla. Las honeypot no tienen en ningún caso la finalidad de resolver o arreglar fallos de seguridad en nuestra red. Son los encargados de proporcionarnos información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales. *(Lance* Spitzner, 2002*).*

Como menciona Spitzner, un honeypot en ningún momento persigue la finalidad de ser una solución de seguridad, sino que es un complemento a los sistemas de seguridad existentes. Es decir, se encarga de proporcionar información sobre los atacantes que intentan comprometerlo, antes de que comprometan otros sistemas de la red en la que se encuentra. Por ende, nadie (equipo, usuario ni aplicación) debería interactuar con ellos y cualquier comunicación establecida se considera como no autorizada. Por lo tanto, no se tienen casos de falso positivo y los datos recolectados son altamente valiosos al ser siempre producto de intrusiones realizadas. Con estos datos se puede averiguar los medios que utiliza el atacante y, quizás sus motivos, sin el costo de analizar un sistema de producción que haya sido comprometido. Los honeypots constituyen una tecnología altamente flexible y adaptable a cualquier ambiente.

FIGURA 07 - ESTRUCTURA DE UNA HONEYPOT



FUENTE Elaboración propia en base a *CYBER HOOT, 2020.*

La *Figura 07,* muestra la estructura de una Honeypot, donde el recurso para ser atacado puede ser de diversa índole, tales como computadoras con diferentes sistemas operativos, un equipo de red

(router, firewall, etc.), un servicio (correo electrónico, página web, base de datos), entre otros. (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008).

3.2.1 OBJETIVOS DE LAS HONEYPOTS

Los autores Fernando Cócaro, Mauricio García, Maria Rouiller (2008), en su informe final explican que los honeypots no resuelven problemas de seguridad, ni tampoco detienen a los atacantes. *Sus objetivos principales son la captura de ataques a vulnerabilidades, tanto conocidas como desconocidas, además del descubrimiento de riesgos en los sistemas.*

Esto es así, porque tradicionalmente, la detección de ataques ha sido una tarea extremadamente difícil de llevar a cabo. Las tecnologías clásicas como los sistemas de detección de intrusos (IDS) han sido deficientes en el punto de que generan información en cantidades excesivas, con una alta tasa de falsos positivos (reportan como ataques algo que en realidad constituye tráfico normal y autorizado) y no cuentan con la habilidad de detectar nuevos ataques. Mientras que los honeypots no contienen sistemas con valor de producción, con lo cual todo tráfico hacia ellos es considerado producto de un ataque o intrusión.

Es por esta razón que no generan falsos positivos y solo capturan pequeñas cantidades de datos en comparación con los sistemas de detección de intrusos (IDS) y firewalls. Los honeypots son excelentes para ayudar en el análisis de incidencias. Se pueden sacar de la red de forma fácil y rápida para realizar un análisis forense completo sin causar impacto en las operaciones diarias de la organización. Por lo tanto, los honeypots al usar el engaño, pueden confundir fácilmente al atacante y hacerle perder tiempo y recursos. Mientras ese proceso se lleva a cabo, se puede detectar la actividad del atacante y se tiene tiempo para reaccionar y detener el ataque.

3.2.2 HISTORIA DE LAS HONEYPOTS

Lance Spitzner, consultor de tecnologías de la información y experto en seguridad informática, construyó una red con seis computadoras en su propia casa a comienzos del año 2000. Diseñó la red para poder estudiar las metodologías que usaban los hackers en sus ataques y así poder aprender cómo llevaban a cabo sus actividades gracias a la información recopilada en su red de computadoras. Fue uno de los primeros investigadores en adoptar la idea y, en la actualidad, es considerado el mayor experto en honeypots. Sus conocimientos en el campo de la seguridad lo llevaron a crear el proyecto de mayor envergadura sobre honeypots, el denominado *The Honeynet Project*, iniciado en 1999. (Spitzner, 2002). Durante un año, su red estuvo almacenando información sobre los intentos de intrusión y los escaneos realizados desde el exterior, posiblemente mediante herramientas automatizadas, llegando a tener más de 14 alertas al día. Desde entonces, una comunidad de

desarrolladores y colaboradores trabajan aportando herramientas y aconsejando sobre la utilización de estas en el The Honeynet Project. Los intentos por descifrar cómo se realizan los ataques datan de los años 80, se usaban entonces jaulas en sistemas UNIX para intentar obtener un log de la intrusión y un mecanismo de protección que evitará poder obtener mayores privilegios al atacante. (José Fernández, 2013, pág. 15).

3.2.3 CLASIFICACIÓN DE LAS HONEYPOTS

Los honeypots se pueden clasificar de 3 formas distintas, por su funcionalidad (dependientes del objetivo perseguido), según el nivel de interacción que se permita o según nivel de implantación, física o virtual (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008).

- ***Honeypots según su funcionalidad***

  Clasificar un honeypot por funcionalidad se refiere a cuál será el fin de la operativa del mismo. Esta clasificación se divide en dos categorías:

  1. *Honeypots de producción*

     Son usados para asistir a una organización con la protección de su infraestructura IT interna. Son especialmente valiosos para las organizaciones comerciales, ya que ayudan a reducir los riesgos a los que están sometidas. Son útiles para atrapar hackers con intenciones criminales. La implementación y el despliegue de estos honeypots es relativamente más sencilla, debido a que en general tienen menores propósitos y requieren menor cantidad de funciones. Como resultado de esto, proveen menos evidencia acerca de los motivos y patrones de ataque de los intrusos. (Miguel Sanchez, 2015, pág. 25).

  2. *Honeypots de investigación*

     Están diseñados para recolectar tanta información como sea posible acerca de los atacantes y sus actividades. No son especialmente valiosos para una organización. Su misión principal es la de investigar las posibles amenazas a las que una organización pueda estar sometida, como por ejemplo, quiénes son los atacantes, cómo se organizan, qué clase de herramientas utilizan y dónde las obtuvieron. Mientras que los honeypots de producción son como la policía, los honeypots de investigación son como su contraparte de inteligencia y su misión es recopilar información sobre los atacantes. La información obtenida ayudará a la organización a tener una mejor comprensión acerca de los patrones de comportamiento de los hackers, sus motivos y el cómo funcionan. (Miguel Sanchez, 2015, pág. 25).

- ***Honeypots según su nivel de interacción***

  Por interacción se entiende el grado de interacción que el atacante tiene con el sistema. Se definen tres niveles: bajo, medio y alto. A medida que se escala en el nivel de interacción, el riesgo de la red en la que se encuentra implantado también aumenta.

  1. *Honeypots de baja interacción*

     Son los más fáciles de instalar, configurar, desplegar y mantener debido a su diseño simple y funcionalidad básica. Normalmente estas tecnologías meramente emulan una variedad de servicios (HTTP, FTP, TELNET, …) y el atacante se limita a interactuar con estos servicios pre-diseñados. Dado que los honeypots de baja interacción son simples, conllevan el menor grado de riesgo. Tampoco hay sistema operativo con el cual el atacante pueda interactuar, por lo que el honeypot no puede ser usado para atacar o monitorear otros sistemas (Miguel Sanchez, 2015, pág. 26).

  2. *Honeypots de interacción media*

     Son más avanzados que los honeypots de baja interacción, pero no tanto como los de alta interacción. Los honeypots de interacción media tampoco cuentan con un sistema operativo real, pero los servicios que proveen son técnicamente más sofisticados. Aquí los niveles de complejidad del honeypot se vuelven mayores por lo tanto los riesgos también crecen, especialmente en lo que respecta a las vulnerabilidades. (Miguel Sanchez, 2015, pág. 26).

  3. *Honeypots de alta interacción*

     Son soluciones complejas e involucran el despliegue de sistemas operativos y aplicaciones reales. Capturan una extensa cantidad de información mientras permiten a los atacantes interactuar con sistemas reales en los que el alcance total de su comportamiento puede ser estudiado y almacenado. Este tipo de honeypots requieren de mucho tiempo y esfuerzo para su diseño, manejo y mantenimiento. De entre las tres clases de honeypots, estos poseen los mayores niveles de riesgo. Pero la información y evidencia que recopilan para el análisis también es mucho mayor. Con este tipo de honeypots, podemos conocer qué tipo de herramientas los ciberdelincuentes utilizan, de qué tipos de exploits se aprovechan, qué clase de vulnerabilidades normalmente indagan, su capacidad para hackear y abrirse paso a través de los sistemas operativos y cómo y con que interactúan. (Miguel Sanchez, 2015, pág. 26).

- ***Honeypots según su nivel de implantación***

  Una tercera clasificación posible es de acuerdo al nivel de implantación:

  1. *Honeypots físicas*

     Es aquella cuyos nodos son máquinas físicas, todos los elementos en ella son hardware reales y nada en ella se emula. Como es de suponer, implica un costo mayor ya que se debe tener físicamente los equipos que la compongan y al mantenimiento se debe añadir el cuidado de los componentes electrónicos que utilice, además se puede incurrir en costos, ya que con el tiempo el equipo físico puede dañarse y requerir la adquisición de repuestos o contratos de mantenimiento que pueden suponer un impacto presupuestal a considerar de acuerdo al tamaño de la organización donde se implemente. (Miguel Lara y Diana Lopez, 2013, pág. 25).

  2. *Honeypots virtualizadas*

     Estas honeypot consisten en emulaciones de hardware por medio de soluciones como VMware, son menos costosas ya que con un solo equipo de cómputo se pueden simular varios, y de esta forma se reduce la inversión en hardware y el mantenimiento que pueda implicar su instalación. Por supuesto esto también dependerá de la solución que se use para llevar a cabo el aprovisionamiento de los sistemas, ya que el licenciamiento puede ser más costoso en uno u otro. (Miguel Lara y Diana Lopez, 2013, pág. 25).

3.2.4 LOCALIZACIÓN DE UN HONEYPOT EN LA RED

Un honeypot puede situarse en distintos puntos de la red de una organización. Cada localización aporta unas ventajas y desventajas, siendo responsabilidad de los administradores la decisión de implantar la tecnología adecuada en la red. La función de un honeypot es la de recopilar toda la información posible cuando tiene lugar un evento sospechoso, por lo que los datos obtenidos varían en función de la localización del honeypot. A continuación se describen los puntos principales y más adecuados donde ubicar los honeypots. (José Fernández, 2013, pág. 21).

1. ***En la red interna (LAN)***

   En esta posición, el honeypot queda afectado por las reglas de filtrado del firewall. Por un lado tenemos que modificar las reglas para permitir algún tipo de acceso a nuestro honeypot por posibles atacantes externos, y por el otro lado, al introducir un elemento potencialmente peligroso dentro de nuestra red, podemos permitir a un atacante que gane acceso al honeypot un paseo triunfal por nuestra red. La ubicación tras el firewall (ver *Figura 08*) nos permite la detección de atacantes internos así como firewalls mal configurados, máquinas infectadas por gusanos o virus e incluso atacantes externos. (Gabriel Verdejo, 2003, pág. 127).

FIGURA 08 - HONEYPOT EN LA RED INTERNA (LAN)

FUENTE Elaboración propia en base a *FWHIBBIT, 2016.*

Dentro de la red interna (LAN), existirán redes separadas en función de su propósito, localización geográfica o propiedad, y además se puede utilizar un segmento de red dedicado donde desplegar uno o varios honeypots. Esta separación de redes facilita la administración de la mismas, pero también permite a los honeypots identificar ataques internos, ya que el tráfico del resto de las redes internas de la organización no debería interactuar con ellos, considerando en tal caso una actividad sospechosa, posiblemente ocasionada por algún usuario o por malware que esté infectando a los sistemas de la organización. (José Fernández, 2013, pág. 23).

2. ***En la red externa***

Esta localización (ver *Figura 09*) permite evitar el incremento del riesgo inherente a la instalación del honeypot. Como este se encuentra fuera de la zona protegida por el firewall, puede ser atacado sin ningún tipo de peligro para el resto de nuestra red. De esta manera, nos permite tener un acceso directo a los atacantes, puesto que el firewall ya se encarga de filtrar una parte del tráfico peligroso o no deseado, obteniendo trazas reales de su comportamiento y estadísticas muy fiables sobre la cantidad y calidad de ataques que puede recibir nuestra red.

FIGURA 09 - HONEYPOT EN LA RED EXTERNA

FUENTE Elaboración propia en base a *FWHIBBIT, 2016.*

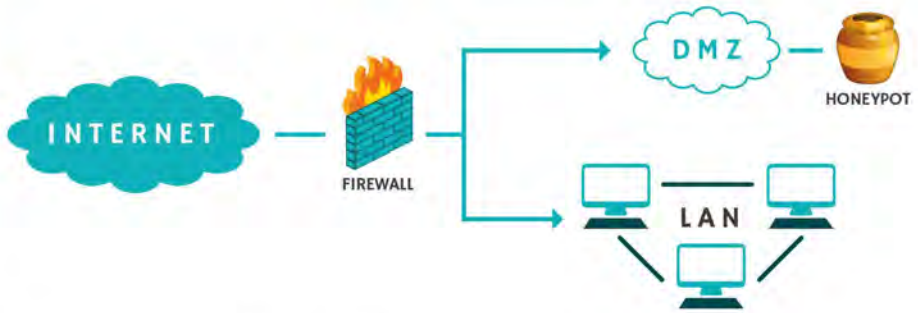
Además con esta configuración evitaremos las alarmas de otros sistemas de seguridad de nuestra red (IDS) al recibir ataques en el honeypot. Sin embargo, existe el peligro de generar mucho tráfico debido precisamente a la facilidad que ofrece el honeypot para ser atacado.

Cualquier atacante externo será lo primero que encuentre y esto generará un gran consumo de ancho de banda y espacio en los ficheros de log. Por otro lado, esta ubicación nos evita la detección de atacantes internos. (Gabriel Verdejo, 2003, pág. 127).

3. *En la zona desmilitarizada (DMZ)*

La zona desmilitarizada es quizás la mejor opción para una organización en la cual ubicar un honeypot (ver *Figura 10*), ya que gran parte de los recursos de red y servicios se sitúan en ella. Es la arquitectura más difícil de implantar debido a que son servicios expuestos a Internet y a la red interna y por lo tanto, el nivel de seguridad aplicado debe de ser crítico. Un honeypot en la DMZ permite recopilar información y alertar sobre ataques externos, generalmente basados en aplicativos web, ya que si el firewall de la DMZ está bien configurado, tan solo permitirá conexiones, a priori confiables, como consultas HTTP, FTP, DNS, etc. (José Fernández, 2013, pág. 23).

FIGURA 10 - HONEYPOT EN UNA ZONA DESMILITARIZADA (DMZ)



FUENTE Elaboración propia en base a *FWHIBBIT, 2016.*

Esta arquitectura nos permite tener la posibilidad de detectar ataques externos e internos con una simple reconfiguración de nuestro sistema de firewall puesto que se encuentra en la zona de acceso público. La detección de atacantes internos se ve algo debilitada, puesto que al no compartir el mismo segmento de red que nuestra LAN, un atacante local no podrá acceder al honeypot. Sin embargo, desde la red local sí que es posible acceder al honeypot, con lo que un atacante interno que intente atacar nuestros servidores públicos u otros sistemas externos (un gusano por ejemplo) muy probablemente acabe siendo detectado. (Gabriel Verdejo, 2003, pág. 130).

3.2.5 DISTRIBUCIONES DE HONEYPOTS

Los honeypots aquí nombrados son algunos de los más conocidos y utilizados, ya que existe una inmensa lista, pudiéndose encontrar honeypots para distintas áreas, teniendo honeypots para base de datos, data mining, correos electrónicos, servicios, Internet de las cosas (IoT), desarrollo, servidores, entre otros. Por ello, el uso de cada una de estas herramientas dependerá del área de aplicación a implementar y los objetivos que se quiera alcanzar. A continuación detallaremos los honeypot más populares:

1. *Honeypot: ManTrap*

   ManTrap es un honeypot comercial de alta interacción, que fue creado, mantenido y distribuido por Recourse Technologies. ManTrap crea un entorno operativo altamente controlado con el cual un atacante puede interactuar. Crea un sistema operativo completamente funcional el cual alberga jaulas en lugar de un sistema operativo limitado. Estas jaulas son entornos lógicamente controlados de los cuales un atacante no puede salir y atacar al sistema que lo alberga (host). Sin embargo, en lugar de crear una jaula vacía y llenarla con ciertas funcionalidades preestablecidas, ManTrap crea jaulas que son copias espejadas del sistema operativo maestro. De esta manera, cada jaula es un sistema operativo plenamente funcional que tiene las mismas capacidades que de una instalación de producción. Este acercamiento crea una solución muy poderosa y flexible. Cada jaula es su propio mundo virtual con pocas limitaciones. Un administrador puede personalizar cada caja de la misma manera que lo haría con un sistema físicamente separado. Puede crear usuarios, instalar aplicaciones, ejecutar procesos, e incluso compilar sus propios archivos binarios. Cuando un intruso ataca y logra obtener acceso a una jaula, para él, ésta se ve como si fuese un verdadero sistema físico separado e ignora completamente el hecho de que en realidad se encuentra en un entorno aislado en el que cada acción que realiza está siendo registrada. (Miguel Sanchez, 2015, pág. 28).

2. *Honeypot: Back Officer Friendly*

   BackOfficer Friendly (conocido por sus siglas BOF), es una simple solución honeypot de licencia libre desarrollada por Marcus Ranum y de baja interacción. Es extremadamente simple de instalar, fácil de configurar así también como de muy bajo mantenimiento, pero esta simplicidad trae asociado un costo, debido a que sus capacidades están severamente limitadas. Cuenta con un pequeño conjunto de servicios que simplemente escuchan en puertos, con capacidades de emulación notablemente reducidas. Funciona creando sockets abiertos que se enlazan a distintos puertos y detectan cualquier conexión que se intente a los mismos. Cuando se realiza una conexión al puerto, estos sockets en modo escucha establecen una conexión TCP completa,

guardan el intento en un log, generan una alerta, y luego cierran la conexión, dependiendo de cómo el servicio haya sido configurado. Todo lo que BOF hace ocurre en el espacio de usuario. No genera ni personaliza ningún paquete cuando responde a conexiones. A causa de este simple modelo, BOF se puede correr en cualquier plataforma Windows, incluyendo Windows 95 y Windows 98. (Miguel Sanchez, 2015, pág. 28).

3. *Honeypot: Specter*

   Specter es un honeypot comercial de baja interacción desarrollado, soportado y distribuido por NetSeg. Sin embargo, Specter cuenta con capacidades y funcionalidades mucho mayores que BOF. No sólo puede emular más servicios, sino que puede emular diferentes sistemas operativos y vulnerabilidades. También posee extensas capacidades de alerta y registro. Como Specter sólo emula servicios de interacción limitada, es de bajo riesgo, fácil de desplegar y de mantener. Sin embargo, comparado con honeypots de interacción media o alta, es limitado en cuanto a la cantidad de información que es capaz de recopilar. Specter es ante todo un honeypot de producción y comparte las mismas limitaciones que BOF. Específicamente, no puede escuchar o monitorear un puerto que previamente se encuentre tomado por otra aplicación, sino que solo lo puede hacer con puertos libres. La emulación de distintos sistemas operativos la puede efectuar cambiando el comportamiento de los servicios que emula, de manera que imiten el sistema seleccionado. (Miguel Sanchez, 2015, pág. 29).

4. *Honeypot: Modern Honey Network (MHN)*

   Este tipo de honeypot, es un software de código abierto en su totalidad, que provee un manejo de grado empresarial del software, desde su seguro despliegue hasta el agregado de miles de eventos, haciendo que el manejo de honeypots sea una tarea extremadamente simple. MHN facilita la confección de una honeynet de una forma rápida y sencilla, ofreciendo una amplia variedad de sensores para desplegar en la misma. Posee una consola gráfica de administración y soporta el despliegue de forma distribuida y en gran escala de honeypots internos y externos y para ello, utiliza el estándar HPFeeds y honeypots de baja interacción para mantener la efectividad y seguridad a nivel de grado empresarial. (Miguel Sanchez, 2015, pág. 30).

   Es importante entender, que el sensor es una aplicación externa al administrador de MHN, ya que se puede instalar en el propio servidor, o bien ir desplegando sensores en otros servidores remotos; de esta forma vamos a poder desplegar tantos honeypot como queramos y todos los datos se van a cruzar en la consola de administración central, pudiendo filtrar no solo la procedencia y el tipo de ataque que reciben los sensores, sino que además podremos filtrar por destinos. En el caso de instalar sensores en varios servidores virtuales por diferentes países,

también vamos a tener una idea de qué países o proveedores de redes son los más susceptibles a ser atacados y no solo eso, también la información de que tipo de ataques se hacen en cada zona geográfica, aparte de que tipo de ataques son más comunes dependiendo de la procedencia de los mismos. (Joan, 2014).

5. *Honeypot: Honeyd*

   Honeyd es desarrollado y mantenido por Niels Provos de la Universidad de Michigan y fue lanzado por primera vez en Abril de 2002. Está diseñado como una solución de baja interacción; no hay ningún sistema operativo destinado a que los atacantes accedan al mismo, sólo cuenta con servicios emulados. Está diseñado primariamente como un honeypot de producción, usado para detectar ataques o actividad no autorizada.

   Honeyd funciona bajo el principio de que cuando detecta un intento de conexión hacia un sistema que no existe, éste asume que la conexión es hostil, muy probablemente un sondeo, escaneo o un ataque y cuando recibe tráfico de estas características, éste adopta una dirección IP y corre un servicio emulado para el puerto que la conexión está probando. Una vez que el servicio emulado se inicia, éste interactúa con el atacante y captura toda su actividad. Cuando el atacante termina y se retira, el servicio emulado también se cierra. Entonces Honeyd continúa a la espera de más tráfico e intentos de conexión hacia sistemas que no existen. Este método es sumamente eficiente. A medida que Honeyd recibe más ataques, repite el proceso descrito tantas veces como ataques perciba. Puede emular múltiples direcciones IP e interactuar con diferentes atacantes todos al mismo tiempo. (Miguel Sanchez, 2015, pág. 29).

6. *Honeypot: T-Pot*

   T-Pot es un desarrollo de código abierto que combina honeypots de baja y alta interacción en un único sistema. Su implementación es bastante sencilla y provee una interfaz gráfica para visualizar la información generada. Si bien lo ideal es crear un honeypot personalizado con los mismos servicios que se prestan en nuestra red y nada más, T-Pot es una forma más rápida y sencilla de desplegar un honeypot si no poseemos el tiempo o los recursos para desarrollar uno propio. Además, puede ser configurado de acuerdo con las necesidades específicas de la organización. (Alan Warburton, 2020).

   Es decir, T-Pot es una plataforma de honeypots que tiene como base una distribución Linux Debian, la cual incluye una gran variedad de honeypots ya preparados, configurados y listos para entrar en funcionamiento. Algunos de estos honeypots y herramientas que incluye son: Conpot, Cowrie, Dionaea, Elasticpot y EMobility. Por otro lado, tiene una web central de gestión, desde la

cual el posible atacante tendría acceso a todos los nodos de carga de la falsa infraestructura. La gran ventaja de esta distribución T-Pot es que los integra todo es una misma instalación (mismo servidor) y todos virtualizados con Docker[5] . Además, al tener cada honeypot su entorno dockerizado, es muy sencillo su mantenimiento, gestión y personalización. (Chema Alonso, 2017).

7. *Honeypot: Kippo*

   Kippo es un tipo de honeypot SSH, de interacción media, el cual fue diseñado para el monitoreo de ataques de fuerza bruta, y la interacción dentro de la Shell por parte del atacante. Tiene una curva de aprendizaje de instalación baja, lo cual es importante a la hora de su implementación, lo que indica que puede ser estudiado y configurado acorde a los objetivos de quien lo utiliza.

   Como características principales, posee un sistema de fichero falso agregado a la shell, el cual le da capacidad al atacante de agregar y/o eliminar archivos; puede agregar contenido de ficheros falsos, para que el atacante perciba una interacción real con el contenido y posee la capacidad de monitorear en tiempo real las ejecuciones del atacante y de registrar las pulsaciones y acciones del atacante desde el momento en que comienza con el ataque. (Kevin David Martínez Contreras, 2018).

8. *Honeypot: Deception Toolkit (DTK)*

   Deception Toolkit es un tipo de honeypot de bajo nivel de interacción, open source, el cual se basa en simular servicios. Básicamente se trata de un conjunto de scripts Perl diseñados para emular una variedad de vulnerabilidades conocidas, las cuales pueden ser configuradas para dar respuestas falsas (archivos, peticiones, etc.). Un objetivo peculiar de DTK es que sus desarrolladores intentan hacer que este sea fácil de detectar. Esto lo hacen porque la idea del sistema se basa en el supuesto de que si un atacante identifica la instalación en la red que desea comprometer, desistirá de su intento y buscará otro blanco (decepción). Está orientado a desahuciar al atacante, intentando vencerlo psicológicamente. (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008, pág. 28).

9. *Honeypot: Glastopf*

   Glastopf (Glaspot v3) desarrollado en Python con licencia GPL es un completo honeypot creado en 2009 por Lukas Rist, quien es miembro de Honeynet Project. Este honeypot está específicamente diseñado para aplicaciones web, y es capaz de emular miles de vulnerabilidades

[5] Docker: Permite empaquetar una aplicación y sus dependencias en un contenedor muy ligero. Ver *Glosario*.

web con el objetivo de recolectar una gran información de ataques remotos como por ejemplo inyección SQL, inserción remota de archivos, inserción local de archivos, vulnerabilidades XSS y de elevación de privilegios entre otras muchas. El software trabajará como un servidor web normal, cuando un cliente envía peticiones al servidor web serán procesadas y el servidor enviará la información que se le ha pedido, pero si la petición no es correcta, se mostrará una página de error e internamente se almacenarán todos los datos de la solicitud y del solicitante. Ahora, si el atacante envía una petición maliciosa con el fin de comprometer la seguridad del servidor web, el honeypot procesa la petición como si realmente el servidor fuera vulnerable. (Sergio De Luz, 2015).

10. *Honeypot: Google Hack Honeypot (GHH)*

    Este honeypot está diseñado para detectar a los atacantes que utilizan los motores de búsqueda como herramienta de hacking contra diferentes recursos. El funcionamiento es muy sencillo, emula vulnerabilidades de aplicaciones web y permite que sus páginas sean indexadas por los motores de búsqueda. Estas no son visibles a usuarios comunes de la web, sino que están diseñadas para ser encontradas por motores de búsqueda mediante los llamados enlaces transparentes. Estos permiten reducir falsos positivos y evitan además dejar la huella digital del señuelo. Este enlace se coloca en páginas web ya existentes ya que no afecta su funcionamiento.

    Por lo tanto, GHH consiste en explotar la gran capacidad de almacenamiento de información de Google, buscando información específica que ha sido añadida a las bases de datos del buscador. Si las búsquedas están orientadas a ciertas palabras claves, es posible encontrar información o puntos de entrada sensibles a posibles ataques. (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008, pág. 33).

3.2.6 VENTAJAS Y DESVENTAJAS DE HONEYPOTS

Según Gabriel Verdejo (2003), las ventajas y desventajas que tienen los honeypots son:

Ventajas

- Genera un volumen pequeño de datos, al contrario que los sistemas clásicos de seguridad que generan cientos de megas de ficheros de logs con todo tipo de información, las honeypots generan muy pocos datos y de altísimo valor, recogen pequeñas cantidades de información sólo cuando el atacante interactúa con ellas.

- Necesita unos recursos mínimos, a diferencia de otros sistemas de seguridad, las necesidades de un honeypot son mínimas. No consume ni ancho de banda ni memoria o CPU extra. No necesita complejas arquitecturas, cualquier computadora conectada a la red lo puede realizar.

- Universalidad, este tipo de sistemas sirven tanto para posibles atacantes internos como externos. De esta forma, obviamente, se ha de evitar poner a las máquinas nombres como honeypot o attack-me. Su objetivo es pasar desapercibidas en una red como una máquina más.

- Simplicidad, uno de los puntos más importantes a favor de las honeypot es su sencillez. No utilizan complicados algoritmos de análisis, ni rebuscados métodos para registrar la actividad de los intrusos. Por el contrario, sólo hay que instalarlos y esperar. Algunos sistemas trampa de desarrollo pueden poseer mayor nivel de complejidad, pero no comparable a otros enfoques.

Desventajas

- Fuente potencial de riesgo, debido a la atracción de atacantes, se debe tener cuidado en la configuración, y convertirlo en un entorno cerrado y controlado, para evitar que se utilice como fuente de ataque a otras redes e incluso a la propia.

- No resuelven fallos de seguridad, las honeypot son herramientas empleadas para el análisis de ataques, son usadas para la búsqueda de mejoras y soluciones a los posibles problemas que presenten los métodos de seguridad implementados en una red.

- No detienen a un atacante, al contrario, lo atraen con el fin de permitir estudiar sus técnicas de ataque para un posterior análisis.

3.3 HONEYNETS

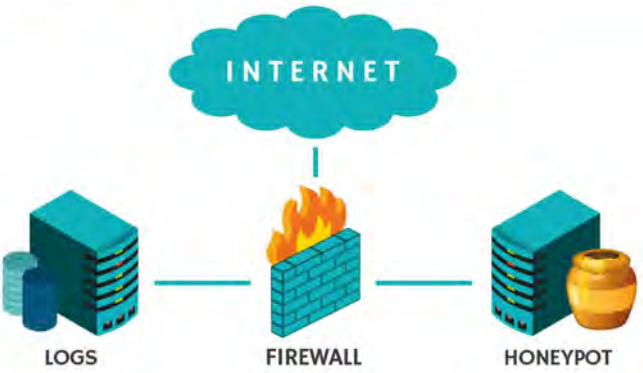
Una honeynet es una arquitectura de red compuesta por una red de honeypots, dispositivos de red y herramientas de seguridad. Los honeypots de una honeynet son sistemas operativos reales, es decir, son honeypots de alta interacción (José Fernández, 2013, pág. 61). Cuando los sistemas de una honeynet son atacados, la honeynet registra toda la información sobre las actividades que están ocurriendo (Lance Spitzner, 1999). Para ello, cuenta con una serie de componentes comunes:

- Router: Enruta el tráfico a los distintos dispositivos de la honeynet.
- Firewall: Restringe el tráfico de entrada y salida a la honeynet.
- IDS/IPS: Permiten analizar con mayor detalle el tráfico y el contenido de los paquetes de red.
- Servidor: La información recolectada por honeypots se envían a un servidor centralizado de logs.

La *Figura 11* muestra un esquema de una honeynet básica, compuesta por honeypots, un mecanismo de control y captura de datos (firewall) y un repositorio que almacena los datos obtenidos de los ataques recibidos por los distintos componentes. Un factor clave es que la red ha sido diseñada para ser comprometida, por lo que proporciona un gran atractivo para el atacante. Como todo el tráfico

que entra a una honeynet se considera un ataque, cualquier tráfico saliente es indicador de que la honeynet fue comprometida y puede tratarse de un ataque a sistemas o computadores externos (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008, pág. 24).

FIGURA 11 - ESQUEMA DE UNA HONEYNET BÁSICA



FUENTE Elaboración propia en base a *PROYECTO HONEYPOTS, 2008.*

3.3.1 ARQUITECTURA DE LAS HONEYNETS

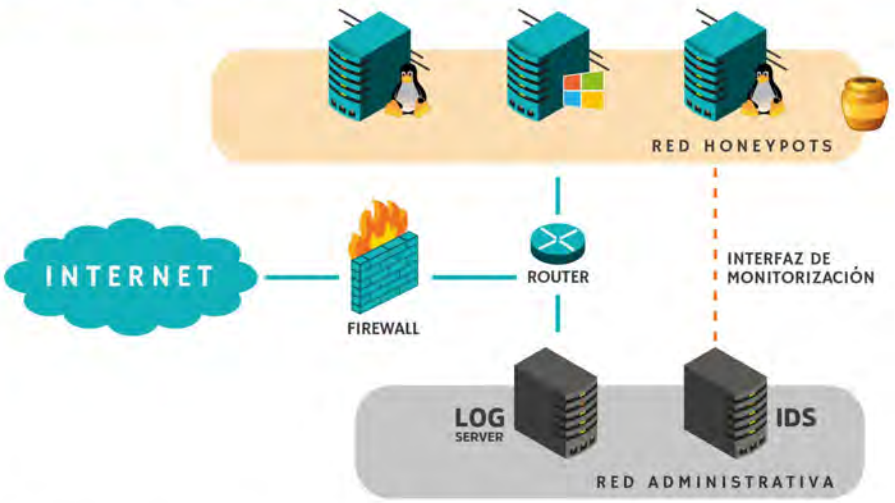
Hasta ahora, no existe un modelo cerrado de arquitectura de honeynet. Para su desarrollo, hay absoluta libertad a la hora de seleccionar tanto su topología como las herramientas a utilizar para realizar las tareas de control, registro y análisis de las acciones del intruso en su interior. A pesar de esto, si bien es cierto que no hay una estandarización clara, las distintas propuestas del Honeynet Project han venido marcando el modelo a seguir desde la aparición de esta herramienta de seguridad (Juan García, 2009).

Por lo tanto, con el pasar del tiempo las honeynets han ido mejorando progresivamente, dando lugar a lo que los autores llaman generaciones de honeynets, cada una incorporando nuevas características y funcionalidades (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008).

- ***Honeynets de primera generación (Gen. I)***

  Las honeynets de primera generación fueron las primeras en ser implementadas por The Honeynet Project desde sus orígenes hasta el año 2001 aproximadamente. Esta arquitectura (ver *Figura 12*) se creó para dar solución a los problemas de control sobre el atacante y a la captura de información dentro de una red. Los dispositivos que componen una honeynet primera generación son: router, firewall, IDS y un servidor de logs (José Fernández, 2013, pág. 61).

FIGURA 12 - HONEYNETS DE PRIMERA GENERACIÓN



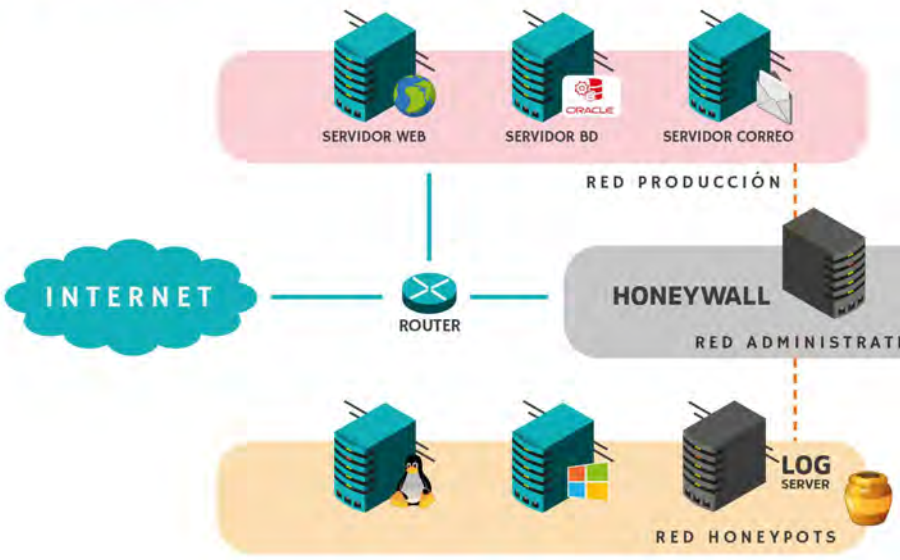
FUENTE Elaboración propia en base a *VIRTUAL HONEYNETS, 2013.*

Desarrollada en 1999, consiste en la instalación de un elemento con capacidad de control de acceso entre una red y otra (dicho dispositivo puede ser un firewall). De esta manera, cada paquete de datos que llega a la honeynet debe pasar por el firewall y el router. La tarea del firewall es permitir que ingrese todo el contenido, pero controlar lo que sale, y el router brinda soporte para esta función y enmascara la existencia del firewall. Se cuenta también con un IDS que monitorea el comportamiento de la red y analiza el tráfico, y finalmente el sistema termina por completarse con una última máquina sobre la cual se almacenarán los registros de las actividades que se lleven a cabo por el sistema y el usuario. Su desventaja es que no resultan atractivos para atacantes experimentados porque los sistemas que lo componen son sistemas operativos básicos y debido a sus fallas a nivel de control de datos, los atacantes avanzados pueden detectarlos fácilmente (Miguel Lara y Diana Lopez, 2013).

- ***Honeynets de segunda generación (Gen. II)***

  Las honeynets de segunda generación (ver *Figura 13*) se empezaron a desplegar a partir del año 2002. Son una evolución de las honeynets de primera generación, aportando una mayor capacidad de control sobre el intruso, mejores herramientas para la recopilación de información y la posibilidad de integrar las honeynets de segunda generación en una red corporativa de producción, disminuyendo los riesgos. (José Fernández, 2013, pág. 63).

FIGURA 13 - HONEYNETS DE SEGUNDA GENERACIÓN



FUENTE Elaboración propia en base a *VIRTUAL HONEYNETS, 2013.*

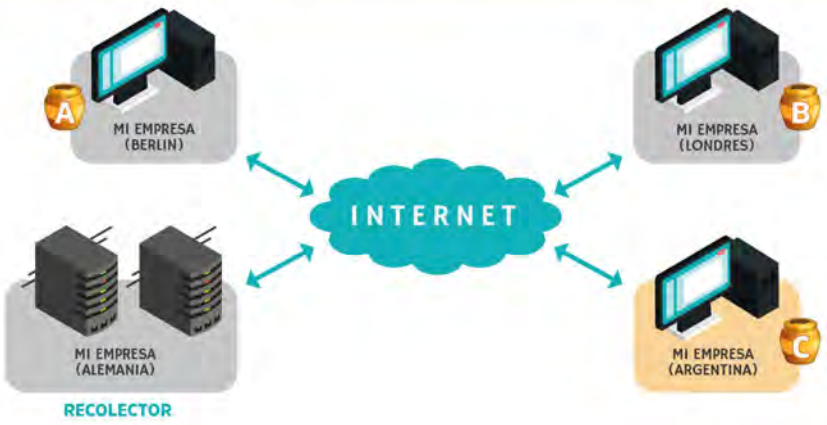
La principal diferencia en esta arquitectura respecto a la primera generación, es la incorporación de un elemento que actúa como gateway de la honeynet llamado honeywall, un dispositivo que incorpora las funciones de firewall y de IPS en el mismo equipo (José Fernández, 2013, pág. 63).

El honeywall es un dispositivo de red de capa 2 que es invisible para el posible atacante que se conecte a la honeypot, y su misión es la de separar el tráfico que viaja a la o las honeypots, del tráfico de la red de producción y de esta manera, todo el tráfico que transite por la red hacia los honeypots deberá pasar a través de él. El honeywall debe ser capaz de implementar control de datos, captura de datos, análisis de datos y recolección de datos. Cada uno de ellos es clave y obligatorio, ya que tienen como fin minimizar el riesgo y capturar la información que genere el atacante sin que él mismo tenga idea de lo que está sucediendo. Si bien a simple vista parece un modelo simple en comparación con la primera generación, las opiniones de expertos indican que su instalación es más complicada y su mantenimiento más costoso (Miguel Lara y Diana Lopez, 2013).

- ***Honeynets de tercera generación (Gen. III)***

  Las honeynets distribuidas se dieron a conocer en el año 2004 y se clasifican como honeynets de tercera generación, ya que cumplen los requisitos de control, captura y análisis de datos, además de la recolección de datos y la implementación de herramientas de administración remota. El conjunto de varias honeynets repartidas a lo largo de la red y bajo la misma administración, recibe el nombre de honeynet distribuida (ver *Figura 14*).

FIGURA 14 – HONEYNETS DE TERCERA GENERACIÓN



FUENTE Elaboración propia en base a *VIRTUAL HONEYNETS, 2013.*

Este sería el caso particular de una organización que quiere estudiar posibles ataques informáticos a su infraestructura entre diferentes delegaciones en su distribución geográfica. Lo ideal es que todas las honeynets sean gestionadas por un administrador desde su puesto de trabajo localizado, evitando los desplazamientos hasta la ubicación física de cada honeynet, así como el hecho de tener que conectar con el honeywall de cada una de ellas para supervisarlas individualmente. Su funcionamiento en sí, consiste en que cada honeynet envía la información recopilada a un sistema central responsable de recibir y almacenar toda la información, de modo que el estado de todas las honeynet pueda ser monitoreado y analizado desde un único punto, simplificando la gestión y el mantenimiento (José Fernández, 2013, pág. 69).

3.3.2 ELEMENTOS BÁSICOS DE UNA HONEYNET

Debido a la arquitectura de las honeynets de primera generación, no es posible realizar un control exhaustivo sobre ellas, por ello evolucionaron a honeynets de segunda y tercera generación, las cuales son redes altamente controladas, donde cada paquete que entra y sale de ellas es monitorizado, capturado y analizado. Por lo tanto, para realizar esto, las honeynets requieren la implementación de métodos que permitan analizar toda la actividad que ocurre en la honeynet, estos métodos son: control, captura, análisis y recolección de datos (José Fernández, 2013, pág. 67).

1) *Control de datos*

   El control de datos permite a un intruso realizar actividades maliciosas dentro de la honeynet, manteniendo un equilibrio entre la libertad y la contención de sus acciones. Por ende, hay que proporcionar al intruso un entorno en el que pueda realizar actividades con cierta libertad, pero sin que pueda comprometer sistemas externos (José Fernández, 2013, pág. 68). Aquí se debe

llegar a un equilibrio entre nivel de interacción que se va a permitir a los atacantes y los riesgos a que se van a exponer los sistemas. Para ello se pueden aplicar distintas estrategias, como por ejemplo, limitar el tráfico y conexiones salientes, limitar el ancho de banda, limitar rangos de direcciones IP entrantes. Estas estrategias disminuyen el riesgo sin llegar a eliminarlo por completo (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008, pág. 25).

2) *Captura de datos*

El propósito de la captura de datos es registrar toda la información que se genera en la honeynet debido a la actividad de los atacantes. La captura de datos es el principal requisito que fundamenta el uso de una honeynet, cuyo objetivo es recopilar toda la información posible sobre un ataque.

El autor José Fernández (2013) explica que en las honeynets de segunda y tercera generación se identifican tres capas o niveles de captura de datos:

- Registros del firewall: El log de las conexiones del firewall permite obtener las conexiones de entrada y salida que atraviesan el honeywall. Estos registros proporcionan información sobre el origen y destino de un ataque, así como de las conexiones que realizan las herramientas instaladas por el atacante o malware.

- Registros del tráfico de red. En este nivel se capturan todos los paquetes que entran o salen de la honeynet y se almacenan en un fichero para su posterior análisis, por ejemplo, mediante la herramienta Wireshark.

- Registros de actividad del sistema. La captura de información en los honeypots es cada vez más complicada, debido a que hace unos años los atacantes utilizaban protocolos sin cifrar, como FTP, HTTP o TELNET para realizar sus actividades, por lo que los comandos que enviaban se podían capturar. Pero hoy en día, apenas se usan estos protocolos, siendo sustituidos por protocolos cifrados como SSH para realizar conexiones con las máquinas remotas. Por lo tanto, sabiendo que el uso de protocolos cifrados impide obtener información relevante analizando el tráfico de red, es necesario realizar capturas de la información en los honeypots.

3) *Análisis de datos*

Toda la información recopilada por la honeynet carece de valor si no se interpreta correctamente. Con el fin de analizar los sucesos ocurridos en la honeynet, se puede hacer uso de herramientas de terceros que faciliten la labor de representación y comprensión de la información. Ejemplos de algunas de estas herramientas son: Snort, Sebek, Wireshark, Snorby, Tripwire, por nombrar algunos (José Fernández, 2013, pág. 69).

4) *Recolección de datos*

La recolección de datos no es un requisito obligatorio en una organización que solo administra una honeynet. Este requisito sólo tiene sentido cuando se administran varias honeynets distribuidas en distintas localizaciones. El propósito de la recolección de datos es centralizar toda la información capturada en cada honeynet en un único punto, donde se puede analizar de forma conjunta. Cuando se envía información a través de redes externas hay que tener en cuenta una serie de factores: asignar nombres únicos a cada honeynet, cumplir con los principios de confidencialidad, integridad, disponibilidad y no repudio de los datos transmitidos y la posibilidad de implementar un sistema de anonimato para datos de carácter confidencial en un entorno determinado. Por ejemplo, aplicar un sistema de cifrado a los datos antes de ser transmitidos por un medio de comunicación inseguro (José Fernández, 2013, pág. 69).

3.3.3 HONEYNETS VIRTUALES

Uno de los problemas más graves a los que se enfrenta cualquier administrador de redes y por tanto el grupo de seguridad, es el de la disponibilidad de recursos. Las arquitecturas presentadas (GenI y GenII) cada vez demandan más máquinas y recursos, lo que puede llevar a la paradoja de tener dos servidores de producción y cuatro computadoras en una Honeynet. Obviamente, este punto es algo exagerado, sin embargo puede pasar que mucha gente descarte las honeynets porque no tiene los recursos necesarios o porque estos son iguales o superiores a las máquinas de producción (Gabriel Verdejo, 2003, pág. 144).

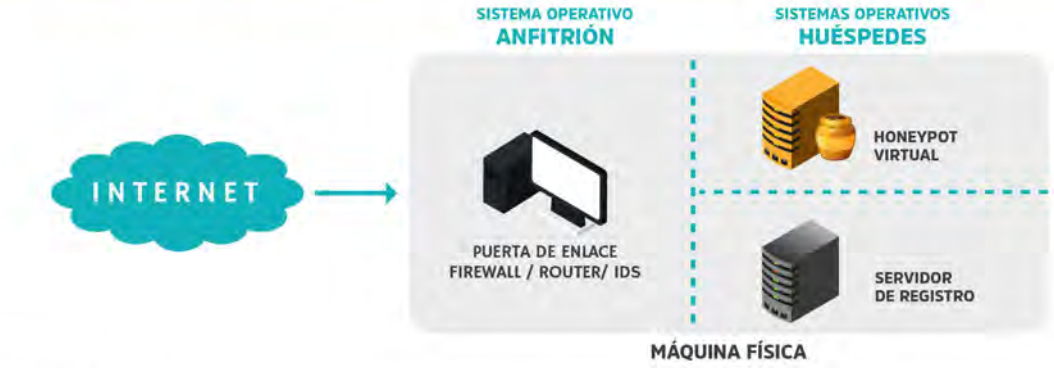
El concepto de honeynet virtual se puede definir como la solución que permite implantar el esquema de Honeynet utilizando un único ordenador. El adjetivo virtual viene dado porque todos los sistemas operativos que existen en la honeynet aparentemente tienen su propia máquina, aunque realmente se ejecutan en el mismo hardware. (Lance Spitzner, 2002).

Las honeynet virtuales pueden clasificarse en:

1. ***Honeynet virtual autocontenida***

   Está implementada en una única máquina física mediante virtualización (ver *Figura 15*), incluyendo todos los honeypots y los dispositivos que la componen. (José Fernández, 2013). Cada sistema operativo contenido dentro de ella actúa independientemente. Su mayor ventaja es el ahorro de costes al minimizar la inversión en recursos físicos . (Edgar A. Maya y Tatiana A. Vinueza, 2013).

FIGURA 15 - HONEYNET VIRTUAL AUTOCONTENIDA



FUENTE Elaboración propia en base a *HONEYNET VIRTUAL HÍBRIDA, 2013.*

Consideraciones de esta honeynet:

- Fácilmente transportable, especialmente si se instala en un equipo portátil.
- Es barata y ocupa poco espacio.
- Rápida puesta en funcionamiento (instalación y configuración sencilla).
- Si falla el hardware, la honeynet entera podría dejar de funcionar.
- Tiene mucha dependencia del software virtual.

2. ***Honeynet virtual híbrida***

   Es una combinación de una honeynet virtual con una física (ver *Figura 16*). Aquí, los honeypots se ejecutan sobre máquinas virtuales en una misma máquina física, pero los dispositivos básicos (IDS, router, etc.) se implementan en una máquina física independiente. Esta implementación disminuye la carga de memoria y de CPU del equipo de virtualización. Además, supone una mejora de seguridad, ya que disminuye las probabilidades de que la honeynet completa sea comprometida por un atacante (José Fernández, 2013, pág. 66).

FIGURA 16 - HONEYNET VIRTUAL HÍBRIDA

FUENTE Elaboración propia en base a *HONEYNET VIRTUAL HÍBRIDA, 2013.*

Consideraciones de esta honeynet:

- El único peligro sería que el atacante accediera a otros honeypots.
- Mayor flexibilidad a la hora de utilizar software para el control y captura de datos de la red.
- Al implicar a más de una máquina, la movilidad es más reducida.
- Es más cara y ocupa más espacio que la honeynet autocontenida.

CAPÍTULO 4 - DEFINICIÓN DEL PROBLEMA

4.1 DEFINICIÓN EXACTA DEL PROBLEMA

El presente proyecto tiene como finalidad ofrecer a particulares y organizaciones un diseño de seguridad para poder aplicarse a sistemas virtuales, utilizando como herramienta informática los honeypots, haciéndoles creer a cualquier ciberdelincuente que es un objetivo legítimo y de esa manera poder obtener información sobre cualquier sus ataques y en base a ello tomar las medidas necesarias.

El constante aumento de aplicaciones web y servicios de cloud hace que diariamente se generen nuevos vectores de ataque y vulnerabilidades explotables, por ello, el uso de honeynets es una infraestructura que cada vez más tiene que ser implementada por las organizaciones como medida de seguridad (José Fernández, 2013). Sin embargo, debido al constante acecho y auge constante que realizan estos ciberdelincuentes para vulnerar sistemas, muchas empresas y organizaciones que empezaron a utilizar sistemas virtuales para realizar sus diferentes actividades, aún no tienen en cuenta el otro lado de la moneda: la seguridad. Por lo tanto, con este proyecto lo que se pretende, es comunicar y concientizar a todos, que a través de un diseño de honeypot bien implementado, será posible garantizar una mejor seguridad en sus redes y así poder estar totalmente seguros momentáneamente, con la condición de estar alertas a partir de ahora.

4.2 OBJETIVO GENERAL

El objetivo general de este proyecto consiste principalmente en diseñar una infraestructura que permita implementar honeypots en una red virtual, de tal forma que nos permita analizar, detectar y obtener información sobre cualquier tipo de ataque informático, para que posteriormente se tomen las medidas de seguridad necesarias. El honeypot utilizado en este proyecto está enfocado a fines académicos, de investigación y desarrollo.

4.3 OBJETIVOS ESPECÍFICOS

- Evaluar, instalar y configurar una distribución de honeypot como herramienta de seguridad para que pueda ser implementado dentro de una red interna (LAN), una zona desmilitarizada (DMZ), o una red externa, de manera que figuren como señuelos legítimos en los ciberataques.

- Diseñar la infraestructura de una honeynet adecuada y funcional que nos permita proteger, analizar y monitorear la red en cuestión.

- Implementar los sistemas operativos y el software necesario, para poder capturar y recopilar información en un ambiente virtualizado, que luego nos permitirán tomar ciertas estrategias de seguridad.

- Recopilar toda la información acerca de los principales tipos de ataques que afectan a las organizaciones y crear los escenarios de ataque a los que estará expuesto el honeypot.

- Realizar ataques informáticos mediante herramientas de software libre con el fin de comprobar la funcionalidad y desempeño del honeypot utilizado.

4.4 ALCANCE DEL PROYECTO

Como se mencionó en el objetivo general, este proyecto consiste en el diseño de una infraestructura que permitirá la implementación honeypots en redes virtuales para la detección de ciberataques, el cual, al ser utilizado como una herramienta de seguridad nos permitirá recolectar todo tipo de información sobre los ciberdelincuentes, monitorear sus actividades dentro de nuestra red y de esa forma tomar las estrategias de seguridad más óptimas para poder mitigarlos.

Para su desarrollo, emplearemos una computadora personal (portátil), en donde simularemos una infraestructura de red virtual para implementar el honeypot, utilizando Windows 10 Pro como sistema operativo base para la administración de toda la red. Utilizaremos además virtualización para poder montar nuestra honeynet haciendo uso de la herramienta VMware en su última versión estable, permitiéndonos alojar y configurar muchas máquinas virtuales, teniendo de esa forma una red más eficiente y con una fácil administración centralizada, ahorrando en costos de hardware, electricidad y mantenimiento.

Dentro de la infraestructura virtual creada, se harán uso de honeypots de alta y baja interacción. Para ello se configurarán cuatro redes internas que alojarán diferentes máquinas virtuales, donde cada red LAN tendrá sus propias estaciones de trabajo, sus propios servicios (DNS, FTP, MAIL, ...) y activos necesarios. Por lo tanto, con todo esto se podrán crear y simular los escenarios de ataque necesarios para que luego se pueda comprobar la funcionalidad y el desempeño del honeypot utilizado.

El diseño de redes honeypots permitirá principalmente:

- Proteger la red de ataques externos e internos.
- Monitorear los accesos a la red no autorizados o posibles ataques.
- Engañar a los posibles intrusos mediante redes falsas simuladas.
- Determinar de dónde provienen los cibercriminales y el modus operandi que utilizan.

Y se hará especial énfasis en que los honeypots no comprenden:

- Ser por sí mismo, una solución que garantice la seguridad de toda la red.
- Corregir todos los fallos que puedan surgir durante un ataque.
- Evitar ataques cibernéticos contra la red.
- Reemplazar los firewalls que tiene una computadora o una red.

Como limitaciones se tiene que los honeypots:

- No persiguen la finalidad de ser una solución de seguridad, sino que básicamente funcionan como un complemento a los sistemas de seguridad existentes.
- No son herramientas de tipo correctivo ante un ataque, sino que su objetivo es solo el análisis de los ataques informáticos como base para la posterior toma de decisiones.

Este proyecto básicamente se implementará en una infraestructura virtual controlada y creada con fines académicos e investigativos, el cual también podrá ser adaptado para cualquier PyME u organización con características similares. A medida que el tamaño de la red crezca, más complejo será la implementación, por ello es indispensable saber que tipo de honeypot se utilizará, cuál será su modo de interacción y donde estará ubicado, para que de esa forma se pueda hacer frente a cualquier ciberataque que se presente.

CAPÍTULO 5 - SOLUCIÓN PROPUESTA

5.1 JUSTIFICACIÓN

Dado que la información ha sido desde siempre un bien invaluable, protegerla es una tarea continua y de vital importancia, y esto es así, porque a medida que se crean nuevas técnicas para la transmisión de la información, se idean otras que permitan acceder a ella sin autorización. Por ello, la seguridad no es sólo una aplicación de un nuevo programa capaz de proteger un sistema, se trata también de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Por lo tanto, es necesario apropiarse del concepto de seguridad para que en cada labor que se desempeñe, se aplique de manera adecuada o se mejore la existente. (Atreyi Kankanhalli, Hock-Hai Teo, Bernard C.Y. Tan y Kwok-Kee Wei, 2003).

Por tal razón, como mencionamos en el capítulo 1, a la hora de afrontar las amenazas debemos tener en cuenta dos aspectos importantes: seguridad reactiva y seguridad proactiva. Para la seguridad reactiva, actualmente contamos con herramientas complementarias para reforzar la seguridad informática tales como el Firewall, Antivirus, IPS y Antispyware que brindan un mayor soporte a las empresas, pero aún presentan algunas limitaciones: cada herramienta tiene técnicas de detección limitadas, presentan dudas en cuanto a su efectividad, son herramientas defensivas y no se adaptan a los diferentes patrones de ataque. (Iván Florez y Jesús Quintana, 2018). Mientras que para la seguridad proactiva se busca principalmente prevenir ciberataques, intentando localizar y corregir las vulnerabilidades de una organización antes de que sean explotadas por los ciberdelincuentes. Y si bien existen muchas técnicas en este tipo de seguridad, podemos destacar como herramientas principales a analizar a los honeypots y a la ciberinteligencia, debido a su gran uso y eficacia.

Por tal motivo, es pertinente la necesidad de utilizar técnicas proactivas de defensa orientadas a la seguridad de redes como son los honeypots, debido a que no se rigen de tantas normativas, es una herramienta centrada en algo específico, poseen muchas variantes para poder implementarlos según lo que la organización precise y sirven tanto para posibles atacantes internos como externos. Para este proyecto no se utilizará la ciberinteligencia porque es un paradigma muy amplio para analizar y no tiene sentido utilizarlas pues las empresas se ven restringidas desde el punto de vista legal para hacer este tipo de trabajo, además de que se considera un punto muy riesgoso.

De esta manera, el objetivo de los honeypots, es mostrar a los atacantes un sistema virtual que aparente el sistema real, con la intención de atraer a los atacantes simulando ser sistemas débiles o con fallas de seguridad, para atraerlos y monitorear todas las actividades que se realizan, de esa

manera los ataques se efectuarán sobre ese sistema sin causar ningún daño al sistema real además de obtener información sobre las actividades ilícitas que realiza el atacante. (Iván Florez y Jesús Quintana, 2018).

El presente proyecto propone una nueva alternativa para la detección de intrusos basado en honeypots, brindando información de las actividades de los intrusos que ingresen a la red, lo cual facilitará la toma de medidas preventivas sobre futuros atacantes, además de poder actualizar las políticas de seguridad para evitar réplicas o ataques con patrones similares, facilitando de forma eficiente y eficaz la gestión de la seguridad de la información que se transporta tanto interna como de manera externa por una red de datos.

Los autores Iván Florez y Jesús Quintana (2018), indican que cualquier implementación de honeypots conlleva una cantidad de beneficios para las organizaciones, entre lo que se pueden destacar:

- *Beneficios económicos*

  Porque utiliza diversos tipos de software libre, como parte de un todo, algunos de ellos cobijados bajo licencias GPL, lo cual implica que se encuentran a total disposición sin costo alguno. Además, la información guardada en los honeypot para atraer a los atacantes no afecta a las organizaciones, por tanto, no genera pérdidas económicas para estas.

- *Beneficios sociales*

  Aporta un beneficio social porque, en primer lugar, contiene posibles ataques verdaderamente peligrosos; en segundo lugar, porque entretiene y desgasta al atacante haciéndole perder el tiempo; y en tercer lugar, porque analiza los reportes de los ataques para detectar posibles nuevas formas de ataque que se estén llevando a cabo en el sector.

- *Beneficios académicos*

  Porque permitirá conocer los resultados del desarrollo de un sistema de detección basado en honeypots, para poder examinar ataques informáticos, nuevas herramientas y tipos de ataques a intrusos. Además de incentivar a las empresas a dedicar sus recursos a estudiar nuevas tendencias de ciberseguridad empresarial, analizar las últimas estrategias de cibercrimen y, en definitiva, poder proteger la seguridad informática de su compañía de una manera mucho más efectiva.

5.2 ESTUDIO DE FACTIBILIDAD

5.2.1 FACTIBILIDAD TÉCNICA

Esta factibilidad consiste en describir principalmente los componentes, tanto de hardware como de software que serán necesarios para el desarrollo de este proyecto. De esta manera, se especificarán los componentes necesarios para poder montar el servidor principal y las estaciones de trabajo, además del software a utilizar, ya sean sistemas operativos, virtualizadores o algunas herramientas útiles.

5.2.2 FACTIBILIDAD OPERATIVA

Para implementar una honeypot o bien una honeynet no se requiere un alto nivel en tecnología, pero sí será necesario contar con profesionales y expertos en el campo IT con sólidos conocimientos de redes informáticas, sistemas operativos, seguridad informática y ramas afines, para poder realizar todas las operaciones de la mejor manera. En esta etapa además se identificarán todas las actividades que son de vital importancia para lograr el objetivo planteado, y se evaluará y determinará todo lo necesario para implementar el proyecto de tal manera que se pueda determinar en qué medida el análisis de vulnerabilidad propuesto es el apropiado. Además, a medida que se desarrolla la infraestructura, es necesario ir capacitando a los profesionales IT quienes serán los responsables de las operaciones, el monitoreo y el mantenimiento de la honeynet.

5.2.3 FACTIBILIDAD ECONÓMICA

Esta factibilidad puede ser analizada tanto si la infraestructura es implementada de manera física como de manera virtual. Pero teniendo en cuenta que este proyecto no supone la utilización de equipos físicos ni la adquisición de nuevas tecnologías, su realización se llevará a cabo en un entorno totalmente virtual, empleando hardware esencial y herramientas de software gratuitas, de manera de ahorrar costos de licencia. Todo el análisis económico y financiero se puede ver en detalle en este mismo capítulo.

5.2.4 FACTIBILIDAD LEGAL

Si bien los honeypots nos permiten identificar vulnerabilidades dentro del sistema, estas se consideran una de las herramientas de seguridad más utilizadas entre los analistas y expertos de seguridad, por lo que el proyecto no ocasionará inconvenientes legales. Por otro lado, todas las pruebas de seguridad se realizarán a través de un entorno de simulación controlado para verificar la funcionalidad del honeypot, utilizando en la mayoría de los casos herramientas de software libre.

5.3 ANÁLISIS ECONÓMICO-FINANCIERO

El análisis de estados financieros, también conocido como el análisis económico-financiero, análisis de balances o análisis contable, es un conjunto de técnicas estudiadas para diagnosticar la situación y perspectivas de la empresa con el fin de poder tomar decisiones adecuadas. (Oriol Amat, 2008).

Debido a que este proyecto se puede ejecutar tanto de manera física como virtual, realizaremos ambos análisis a fin de comprender en detalle qué implementación es la más óptima a realizar, puesto que la finalidad es determinar los montos de los recursos necesarios para poder ejecutar el proyecto. Además sabiendo que la moneda en nuestro país (Argentina) es fluctuante, lo cual llevaría a que todos los precios puedan variar considerablemente, tomaremos un valor de dólar estimativo a $200 ARS correspondiente al año 2021. De esta manera, se considera que realizar este tipo de análisis es realmente fundamental, tanto para este proyecto como para cualquier otro, puesto que nos permitirá evaluar distintos aspectos vinculados al proyecto y su correspondiente evolución.

Como observamos, la *Tabla 02* nos muestra todos los recursos humanos que serán necesarios para la infraestructura, sea esta física o virtual. Por ello, siempre es necesario contar con expertos en el campo IT para poder realizar todas las actividades según el rol asignado. Además, la cantidad de estos recursos dependerá siempre del tamaño de la red diseñada, por lo cual, cuanto más grande sea la infraestructura mayor será el costo de inversión.

TABLA 02 - COSTOS DE LOS RECURSOS HUMANOS

INFRAESTRUCTURA FÍSICA	DISPONIBILIDAD	CANT.	HONORARIOS USD	TOTAL USD
Lider de Proyecto	Presencial	1	840,00	840,00
Analista / Consultor de ciberseguridad	Presencial	1	725,00	725,00
Administrador de redes y comunicaciones	Presencial	2	686,00	1.372,00
Soporte / Técnico en Hardware	Presencial	1	289,00	289,00
Penetration Tester	Presencial	2	2.150,00	4.300,00
			COSTOS TOTALES	$7.526,00

INFRAESTRUCTURA VIRTUAL	DISPONIBILIDAD	CANT.	HONORARIOS USD	TOTAL USD
Lider de Proyecto	Presencial/Remoto	1	840,00	840,00
Analista / Consultor de ciberseguridad	Presencial/Remoto	2	923,00	1.846,00
Soporte / Técnico en Hardware	Presencial/Remoto	1	289,00	289,00
Penetration Tester	Presencial/Remoto	1	2.150,00	2.150,00
			COSTOS TOTALES	$5.125,00

Los honorarios confeccionados en esta tabla están basados en los salarios promedios e indicativos que todo profesional IT debería cobrar tomando como referencias fuentes del COPAIPA (Consejo Profesional de Agrimensores, Ingenieros y Profesionales Afines) y Glassdoor (portal web de empleos,

sueldos y opiniones sobre empresas IT). Asimismo, cabe resaltar que al montar una infraestructura física de este tipo, la inversión de recursos humanos será de unos USD $7.526 ($1.505.200 ARS), mientras que los recursos humanos en una infraestructura virtual sólo exigirá USD $5.125 ($1.025.000 ARS), teniendo así una diferencia de USD $2.401 ($480.200 ARS). De esta forma, podremos evaluar qué infraestructura montar, debido a que si tuviéramos una pequeña PyMES implementarla de manera virtual sería la mejor opción, resultando en un ahorro realmente significativo.

Por otro lado, la *Tabla 03* nos muestra los costos de los recursos físicos y tecnológicos que tendremos en el proyecto, siendo uno de los aspectos más importantes a considerar. En gran parte, la tabla describe toda la factibilidad técnica que tendrá este proyecto, especificando todo el hardware y software que será necesario a la hora de implementar el proyecto, ya sea de manera física o virtual. De esta manera, para saber qué elementos básicos e indispensables de hardware y software se deben considerar, previamente será necesario efectuar un croquis o un bosquejo del diseño de la infraestructura (ver *Figura 19*) que montaremos, debido a que esto nos permitirá saber la disposición de los elementos y así poder conocer a fondo todo el funcionamiento de la red implementada. En cuanto al hardware, se deberá contar con equipos servidores, estaciones de trabajo, dispositivos de conectividad, accesorios útiles y todo software que nos permita las comunicaciones entre ellos. Por ello, como mencionamos en la *Tabla 02,* tener profesiones y expertos en el campo IT nos serán de mucha utilidad, puesto que ellos determinarán los elementos más adecuados para la tareas que estemos por realizar.

La inversión considerada en esta etapa será de unos USD $26.728 ($5.345.600 ARS) para montar una infraestructura física, mientras que para la virtual tendremos unos USD $8.688 ($1.737.600 ARS). De esta manera vemos que montar una infraestructura virtual es mucho más efectiva que una física, debido a que se se ve un ahorro de más del 50%, es decir, monetariamente se puede ahorrar unos USD $18.040 ($3.608.000 ARS).

Resaltamos además que, cuando hablamos de infraestructura virtual no significa que toda la empresa se instalará en la nube de Internet, sino que nos referimos a que la infraestructura se acomodará de otra manera a fin de optimizar los recursos que posee, y en donde ciertos dispositivos, equipos, utilitarios, entre otros ya no se precisarán de manera física (tangible), pero sí estarán presente de manera virtual, lo cual no significa que no tengan un costo asociado.

TABLA 03 - COSTOS DE LOS RECURSOS FÍSICOS Y TECNOLÓGICOS

INFRAESTRUCTURA FÍSICA	TIPO	CANT.	PRECIO USD	TOTAL USD
HPE ProLiant DL180 Gen10 Server	Físico	6	2.500,00	15.000,00
Computadora de escritorio (estaciones de trabajo)	Físico	10	350,00	3.500,00
Computadora de escritorio (estaciones de soporte)	Físico	3	350,00	1.050,00
Router Cisco RV Series RV345 Black 100V / 240V	Físico	2	248,00	496,00
Switch Cisco Sg250-26p 24p Giga + Poe + 2p Combo	Físico	2	315,00	630,00
Rack Server/Router/Switch GLC-RACKP-40U-600	Físico	3	350,00	1.050,00
APC Easy UPS SRV3000 SRV3KI-AR 3000VA	Físico	2	630,00	1.260,00
Accesorios Cables UTP / Patchcord / Conectores ...	Físico	1	379,00	379,00
Software Windows 10 Pro 64 bits	Licencia	7	234,00	1.638,00
Software Linux (Distribuciones varias)	Licencia	10	0,00	0,00
Software Windows Server 2019 Essentials	Licencia	3	325,00	975,00
Otros gastos + Imprevistos	Físico	1	750,00	750,00
			COSTOS TOTALES	$26.728,00

INFRAESTRUCTURA VIRTUAL	TIPO	CANT.	PRECIO USD	TOTAL USD
Equipo anfitrión (uso de portatil para este proyecto)	Físico	1	1.400,00	1.400,00
Servidor Cloud (AWS/ Azure/ Digital Ocean/ ...)	Virtual	6	250,00	1.500,00
Computadora de escritorio (estaciones de trabajo)	Físico	10	350,00	3.500,00
Computadora de escritorio (estaciones de soporte)	Virtual	3	0,00	0,00
Router Cisco RV Series RV345 Black 100V / 240V	Virtual	2	0,00	0,00
Switch Cisco Sg250-26p 24p Giga + Poe + 2p Combo	Virtual	3	0,00	0,00
Rack Server/Router/Switch GLC-RACKP-40U-600	Físico	-	0,00	0,00
APC Easy UPS SRV3000 SRV3KI-AR 3000VA	Físico	-	0,00	0,00
Accesorios Cables UTP / Patchcord / Conectores ...	Físico	-	0,00	0,00
Software VMware Workstation 16 PRO	Licencia	1	250,00	250,00
Software Windows 10 Pro 64 bits	Licencia	7	234,00	1638,00
Software Linux (Distribuciones varias)	Licencia	10	0,00	0,00
Software Windows Server 2019 Essentials (incluido en Cloud)	Licencia	3	0,00	0,00
Otros gastos + Imprevistos	Físico	1	400,00	400,00
			COSTOS TOTALES	$8.688,00

Por último, la *Tabla 04* nos muestra los costos de recursos fijos que tendremos en el proyecto. Este tipo de costos son fijos y no hay forma de no considerarlos, ya que a partir de estos podremos calcular de forma directa los ingresos y egresos que tendrá nuestro proyecto si optamos por realizar después un análisis de CashFlow (flujo efectivo o de caja). La ventaja de una implementación virtual, es que para nuestro proyecto, podremos ahorrarnos en costos de alquiler, cableado de red y adaptación de los cuartos de servidores, debido a que ahora todo esto se implementará en la nube (Internet) y de esa forma algunos de los gastos fijos se reducirán a más de la mitad o directamente desaparecerán. De esta manera, al ser virtual tendremos un ahorro de USD $3.660 ($732.000 ARS).

TABLA 04 - COSTOS DE LOS RECURSOS FIJOS

INFRAESTRUCTURA FÍSICA	TIPO	PRECIO USD	TOTAL USD
Alquiler de oficina (depende de la organizacion)	Fisico	2.250,00	2.250,00
Adaptación del cuarto de servidores	Fisico	450,00	450,00
Cableado + Configuración de toda la red	Fisico	400,00	400,00
Impuestos varios (AFIP/ Rentas/ Tasa Provincial/ ...)	Fisico	1.000,00	1.000,00
Internet 1000MB	Virtual	35,00	35,00
Gastos de oficina	Fisico	200,00	200,00
Servicios básicos (Luz/ Gas/ Agua/ ...)	Fisico	250,00	250,00
Otros gastos + Imprevistos	Fisico	400,00	400,00
		COSTOS TOTALES	$4.985,00

INFRAESTRUCTURA VIRTUAL	TIPO	PRECIO USD	TOTAL USD
Alquiler de oficina (depende de la organizacion)	Fisico	0,00	0,00
Adaptación del cuarto de servidores	Fisico	0,00	0,00
Cableado + Configuración de toda la red	Fisico	0,00	0,00
Impuestos varios (AFIP/ Rentas/ Tasa Provincial/ ...)	Fisico	1.000,00	1.000,00
Internet 500MB	Virtual	25,00	25,00
Gastos de oficina	Fisico	100,00	100,00
Servicios básicos (Luz/ Gas/ Agua/ ...)	Fisico	0,00	0,00
Otros gastos + Imprevistos	Fisico	200,00	200,00
		COSTOS TOTALES	$1.325,00

Finalmente, concluyendo con este análisis económico, tenemos la *Tabla 05* el cuál nos muestra los costos totales que tendría el proyecto si queremos implementarla de manera física o virtual.

Como se observa, el total de los gastos económicos necesarios para una implementación física es de unos **USD $39.239 ($7.847.800 ARS)**, donde si bien el proyecto podría ser económicamente factible o no, implicaría gastos realmente a considerar y más aún sabiendo que la moneda en nuestro país (Argentina) es muy fluctuante. Mientras que si la implementación de la infraestructura se hace de manera virtual, se reducen considerablemente estos gastos, teniendo de esta manera una inversión monetaria de unos **USD $15.138 ($3.027.600 ARS)**, lo cual simplifica mucho de los gastos por las mismas tareas, razón por la cual, la implementación adecuada para este proyecto es hacerla virtualmente. Con todo esto detallado, la elección por un tipo de implementación solo dependerá de nosotros, de que tan óptimo sea la infraestructura al momento de ejecutarse y del soporte que tendremos por parte de nuestro equipo al momento de surgir inconvenientes o de qué tan eficaz sea la comunicación y el acceso a la información en un red física o virtual. Por ende, en base a todo este análisis, realizaremos el proyecto virtualmente.

Por otro lado, también hay que saber discriminar bien estos dos aspectos de implementación física y virtual, debido a que el hecho de que sea virtual, no significa que la implementación sea más sencilla o requiera menos trabajo, sino que al contrario, ejecutar hoy en día una infraestructura virtual puede considerarse en ocasiones mucho más complejo de lo que parece (en comparación de una física), debido a que se requiere de ciertas habilidades tecnológicas y técnicas que no todos poseen, por tal razón, el contar con profesionales en el campo IT es realmente importante.

TABLA 05 - COSTOS TOTALES

INFRAESTRUCTURA FÍSICA	TOTAL USD
Costo de recursos humanos	7.526,00
Costo de los recursos físicos y tecnológicos	26.728,00
Costo de los recursos fijos	4.985,00
COSTOS TOTALES EN DOLARES	$39.239,00
COSTOS TOTALES EN PESOS	$ 7.847.800,00

INFRAESTRUCTURA VIRTUAL	TOTAL USD
Costo de recursos humanos	5.125,00
Costo de los recursos físicos y tecnológicos	8.688,00
Costo de los recursos fijos	1.325,00
COSTOS TOTALES EN DOLARES	$15.138,00
COSTOS TOTALES EN PESOS	$3.027.600,00

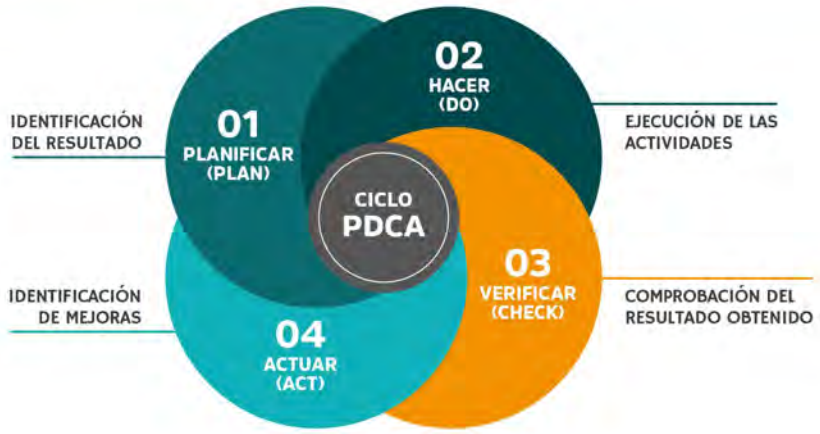
5.3 METODOLOGÍA DE DESARROLLO

Para el desarrollo de este proyecto se utilizará como metodología el *Ciclo PDCA (Plan, Do, Check, Act)*, conocido también como el Ciclo Deming (ver *Figura 17*), en la cual se podrán aplicar todos los procesos que abarca el Sistema de Gestión de la Seguridad de la Información (SGSI). Esta metodología, es una herramienta para la mejora continua basada en un ciclo de cuatro pasos, efectuadas en orden secuencial y comenzando por la fase de Plan (planificar), Do (hacer), Check (verificar) y Act (actuar).

El ciclo PDCA (o en español PHVA), es un ciclo dinámico que puede ser empleado dentro de los procesos de una organización, puesto que es una herramienta de simple aplicación, y que cuando se la utiliza adecuadamente, puede ayudar mucho en la realización de las actividades de una manera organizada y eficaz. A través de este ciclo la organización planea, estableciendo objetivos, definiendo los métodos para alcanzar los objetivos y definiendo indicadores para verificar que en efecto, éstos fueron logrados. Luego, la organización implementa y realiza todas sus actividades según los procedimientos y conforme a los requisitos de los clientes y a las normas establecidas, comprobando,

monitoreando y controlando la calidad de los productos y el desempeño de todos los procesos clave. Se mantiene esta estrategia de acuerdo a los resultados obtenidos, haciendo girar de nuevo el ciclo PDCA mediante la realización de una nueva planificación que permita adecuar la política y los objetivos de la calidad, así como ajustar los procesos a las nuevas circunstancias del mercado. (Camilo Leon y Maria Bonilla, 2017, pág. 38).

FIGURA 17 - CICLO DEMING DE MEJORA CONTINUA (PDCA/PHVA)



FUENTE Elaboración propia en base a *ARETE GESTIONA, 2017.*

A continuación, se detalla cada uno de los pasos y cómo será implementado en este proyecto:

1. *Plan (Planificar)*

   Se establecen todos los objetivos y procesos necesarios para obtener los resultados esperados, establecidos por las partes interesadas y por las políticas de la organización. De esta manera, se comienza realizando un relevamiento de información sobre los temas asociados a seguridad informática, redes informáticas, ataques, vulnerabilidades, y principalmente honeypots, dentro del cual se analizarán: concepto, estructura, diseño, implementación, configuración, y parámetros de instalación. De este modo se establecen los procesos relacionados con el objeto de este proyecto.

2. *Do (Hacer)*

   Se procede a implementar los procesos para alcanzar los objetivos, según el plan establecido. En esta etapa, entra en funcionamiento el honeypot escogido, el cual es integrado a la infraestructura diseñada, para que posteriormente se configuren los elementos necesarios, y a partir de ello poder hacer el análisis de los datos capturados.

3. *Check (Verificar)*

   Se realiza un seguimiento y se miden los procesos y los productos en relación con las políticas, los objetivos y los requisitos, reportando los resultados alcanzados. En esta etapa se realizan pruebas funcionales y se verifica que todos los procesos estén cumpliendo con su objeto.

4. *Act (Actuar)*

   Por último se realizarán acciones para promover la mejora del desempeño de los procesos. El ciclo PDCA significa actuar sobre el proceso, resolviendo continuamente las desviaciones a los resultados esperados. El mantenimiento y la mejora continua de la capacidad del proceso pueden lograrse aplicando el concepto de PDCA en cualquier nivel de la organización, y en cualquier tipo de proceso, ya que está asociado con la planificación, implementación, control y mejora del desempeño de los procesos. Es aplicable tanto en los procesos estratégicos de alta dirección como en actividades operacionales simples. Finalmente, en esta etapa se opta por dar solución a las inconformidades halladas en la verificación, se ejecuta toda acción correctiva que diera lugar y a partir de ello se establecen planes de mejoramiento.

5.4 HERRAMIENTAS A UTILIZAR

A continuación describiremos algunas de las herramientas más frecuentes que vamos a utilizar a lo largo de este proyecto:

1. *VMware Workstation*

   Es un hipervisor[1] que se ejecuta en computadoras de arquitectura x86-64 que permite a los usuarios configurar una o más máquinas virtuales (VM) en una única máquina física, y utilizarlas de forma simultánea junto con la máquina real. Cada máquina virtual puede correr su propio sistema operativo, incluyendo las versiones de Microsoft Windows, Linux, BSD, y MS-DOS entre otros. (Miguel Sanchez, 2015, pág. 143).

2. *Kali-Linux*

   Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Kali Linux trae preinstalados más de 600 programas para pruebas de penetración, escaneo de redes, password crackers, pruebas de vulnerabilidades y otras herramientas afines. (Miguel Sanchez, 2015, pág. 140).

[1] Hipervisor: Pieza de software, firmware o hardware que crea y ejecuta máquinas virtuales. Ver *Glosario*.

3. *Nmap*

   Es un escáner de seguridad utilizado para descubrir hosts y servicios en una red, creando así un mapa de la misma. Para lograr su objetivo, Nmap envía paquetes especialmente construidos hacia el host objetivo y luego analiza sus respuestas. (Miguel Sanchez, 2015, pág. 141).

4. *Honeypot T-Pot*

   Es una herramienta de seguridad informática de código abierto que combina honeypots de baja y alta interacción en un único sistema, permitiendo que se tengan varios tipos de honeypots dentro de una sola máquina virtual. Su implementación es bastante sencilla y provee una interfaz gráfica para visualizar la información generada. La gran ventaja de esta distribución es que al incluir una gran variedad de honeypots, estos ya vienen todos preparados, configurados y listos para entrar en funcionamiento.

5. *Google Cloud Platform*

   Es una plataforma que ofrece grandes posibilidades para trabajar en la nube y aprovechar los datos obtenidos de una manera estratégica. Provee los servicios necesarios para montar la infraestructura de TI completamente en la nube así como también para desarrollo, inteligencia artificial, analítica, almacenamiento, bases de datos y seguridad. Todos se utilizan de manera personalizada, elástica y a demanda, según las necesidades de cada empresa o profesional. (Pronectis, 2021).

6. *Metasploit Framework*

   Es un proyecto de código abierto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración. Es una herramienta para desarrollar y ejecutar exploits contra una máquina remota. (José Fernández, 2013, pág. 151).

7. *Wireshark*

   Se trata de un potente sniffer de red de software libre, que nos permite capturar y monitorizar todos los paquetes de red que pasan por nuestro equipo con el solo hecho de poner nuestra tarjeta de red a escuchar en modo promiscuo, es decir, diciéndole a nuestra tarjeta que capture todo el tráfico que pase por ella. Por ejemplo, si nuestra conexión a Internet está muy lenta y no sabemos cuál es la razón, con este sniffer podremos observar si en nuestro equipo se está generando tráfico no deseado (red infectada por un troyano u otra actividad maliciosa). (Blog SEAS, 2013).

CAPÍTULO 6 - IMPLEMENTACIÓN DE LA SOLUCIÓN

6.1 ANÁLISIS DEL HONEYPOT

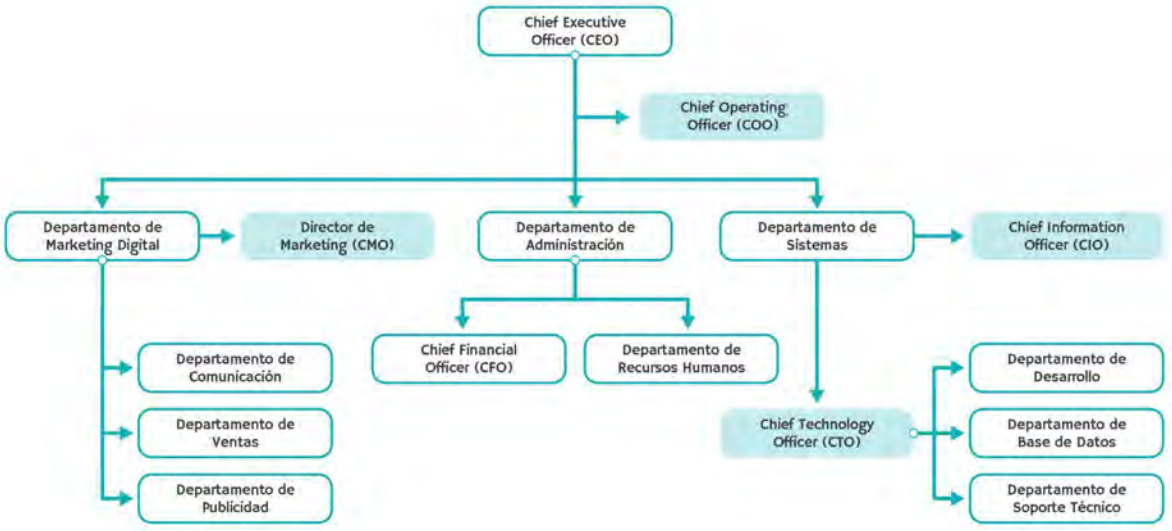
Para dar inicio con el proyecto de forma efectiva, el primer paso es realizar un análisis sobre la primera fase de la metodología PDCA[1] utilizada, es decir la planificación. Por lo tanto, se tomará como referencia una empresa ficticia de término medio para realizar un relevamiento adecuado de toda su información, brindando aspectos generales sobre su seguridad, estado de sus redes informáticas, entre otros, con el fin de establecer los objetivos y los procesos necesarios para posteriormente obtener los resultados esperados.

— *Empresa*

La empresa tecnológica PACHA+KOM cuenta con una sede principal en la capital salteña de la República Argentina, ofreciendo principalmente desarrollo de sistemas informáticos y marketing digital. Si bien no es una empresa muy grande, cuenta con un total de 20 empleados y con la misión presente de ofrecer servicios de alta calidad, agregando valor a los proyectos de software y soluciones integrales que crean día a día.

— *Organigrama*

Para apreciar un poco mejor a la empresa, la siguiente imagen muestra cómo está compuesta la empresa en cuestión, detallando todos sus departamentos y responsables de área.



[1] PDCA: Conocido como ciclo deming, es una herramienta de mejora continua que consta de 4 pasos Plan, Do, Check y Act.

— *Infraestructura*

La empresa está conformada principalmente por cuatro subredes, en donde se tiene dos redes LAN para estaciones de trabajo (workstation), una red DMZ y por último una red de servidores para dar soporte a toda la empresa, que normalmente son empleados para dar servicios Web, Mail y DNS.

— *Seguridad*

En lo que respecta a su seguridad, la empresa aún no posee especialistas en ciberseguridad, ni tampoco cuenta con documentos de políticas de seguridad, plan de seguridad, análisis de riesgos o respuesta ante incidentes. De esta manera, se observa que la empresa analizada solo cuenta con una seguridad del tipo reactiva donde solamente consideran los elementos básicos de seguridad (firewalls, VPN, antivirus, etc.)[2], fortaleciendo solo las defensas contra los métodos de ataque más comunes. Por lo tanto, implementar un tipo de seguridad proactiva con honeypots es indispensable, y sobre todo teniendo en cuenta la cantidad de datos que manejan de sus clientes.

6.2 DISEÑO DEL HONEYPOT

6.2.1 ARQUITECTURA DE VIRTUALIZACIÓN

Como mencionamos anteriormente, para este proyecto estaremos implementando una infraestructura virtual, a fin de optimizar los recursos que posee, y en donde ciertos dispositivos, equipos, utilitarios, entre otros ya no se precisarán de manera física (tangible), pero sí estarán presente de manera virtual.

Si bien para virtualizar existen muchas aplicaciones, en este proyecto nos limitaremos a utilizar como hipervisor el VMware Workstation (ver *Anexo 01* para su instalación) en su última versión estable, debido a que posee una gran versatilidad y muchas funcionalidades. Además, al montar la infraestructura, se deberá utilizar una honeynet virtual autocontenida. Esto es así, porque la virtualización autocontenida nos permitirá hacer uso de una única máquina física (anfitrión), incluyendo así todos los honeypots y dispositivos que la componen. El diseño de esta virtualización se lo puede ver en la *Figura 18*, donde el honeypot será una máquina virtual alojada en el equipo físico (anfitrión) y si es necesario, el mismo se utilizará para atacar el honeypot en la red, ahorrando así el uso de otros equipos o máquinas virtuales.

[2] Para conocer más acerca de estos elementos, consultar el Capítulo 3: *Defensa en profundidad.*

FIGURA 18 - ARQUITECTURA DE VIRTUALIZACIÓN

FUENTE Elaboración propia.

La idea de virtualizar un sistema permitirá reducir los costos por requerimiento de dispositivos, puesto que, entre más grande es la honeynet, más dispositivos y espacio físico se necesitará. De esta forma, utilizando honeynet virtuales podremos tener todos los recursos en una sola máquina física y en el caso de querer aumentar más dispositivos virtuales (ver *Anexo 04*), bastará con mejorar todo el hardware del equipo anfitrión.

En cuanto a limitaciones, tenemos el hardware necesario de la máquina que alberga a la honeynet, y el software que es usado para virtualizar, puesto que si el atacante toma el poder de nuestra máquina anfitrión, tendría control sobre toda la honeynet y sería un peligro para los sistemas reales. (Carlos M. Heredia Terán, 2015, pág. 23).

6.2.2 SELECCIÓN DEL HONEYPOT A IMPLEMENTAR

Una de las decisiones más importantes de este proyecto es la elección del honeypot a implementar en nuestra infraestructura. Por esta razón, como se vió en todo el *Capítulo 3*, antes de elegir el honeypot más adecuado, deberemos evaluar ciertos aspectos que consideramos son importantes.

- *Funcionalidad*

  En cuanto a su funcionalidad, se decidió utilizar *honeypots de investigación*, debido a que podremos recolectar toda la información posible acerca de los ciberdelincuentes, ayudando a nuestra empresa o organización a tener una mejor comprensión acerca de sus patrones de comportamiento. Además, como su propósito es ser atacado, nos servirá como herramienta didáctica para aprender a proteger nuestros sistemas ante futuras amenazas.

- *Nivel de interacción*

  En lo que respecta a su nivel de interacción (grado en el que se compromete a la red real), se utilizarán *honeypots de alta interacción*, porque tienen la capacidad de capturar una extensa cantidad de información mientras permiten a los atacantes interactuar con sistemas reales en

los que el alcance total de su comportamiento puede ser estudiado y almacenado. Si bien, estos honeypots, requieren de mucho tiempo y esfuerzo para su diseño, manejo y mantenimiento, podremos conocer a fondo el tipo de herramientas que los ciberdelincuentes utilizan.

— *Arquitectura*

Para su arquitectura, se optará por emplear *honeypots de tercera generación,* puesto que cumplen con los requisitos de control, captura y análisis de datos, muy útil cuando la infraestructura se encuentra en diferentes locaciones, es decir cuando se cuenta con varias honeynets repartidas a lo largo de la red y bajo la misma administración.

De esta manera, para poder elegir una distribución o un tipo de honeypot correcto, se deberán tener todos estos aspectos analizados, lo que no quita que cualquier particular o empresa pueda elegir otro, dependiendo siempre del área de aplicación a implementar y los objetivos que se quiera alcanzar. Además, antes de poder seleccionar el honeypot del proyecto estudiaremos previamente cuáles son las ventajas y desventajas que nos ofrecen las diferentes distribuciones de honeypots (consideradas como posibles soluciones) y una comparativa general de las mismas, a fin de evaluar correctamente todo y elegir el honeypot más óptimo y adecuado para este proyecto.

- ***Ventajas y desventajas de las soluciones propuestas***

  A continuación analizaremos algunas de las distribuciones de honeypots que consideramos son posibles soluciones mostrando sus ventajas y desventajas más relevantes. Esto lo hacemos con el fin de analizar en detalle cada honeypot para de esa forma tener un criterio más razonable sobre la elección de un honeypot sobre otro. Todos los detalles se analizan en la *Tabla 06*.

TABLA 06 - VENTAJAS Y DESVENTAJAS DE LAS SOLUCIONES PROPUESTAS

TIPO DE HONEYPOT	VENTAJAS	DESVENTAJAS
Honeyd	Fue creado como un honeypot de producción para detectar cierto tipo de ataques. Puede emular múltiples direcciones IP e interactuar con diferentes atacantes y todos al mismo tiempo.	No posee ningún sistema operativo destinado para que los atacantes interactúen. Su interfaz está basado mediante linea de comandos y archivos de configuraciones.
Specter	Puede emular muchos servicios, entre ellos emulación de diferentes sistemas operativos. Es de bajo riesgo, fácil de desplegar y de mantener.	Solo puede monitorear puertos libres y no aquellos tomados por otras aplicaciones. Limitado en cuanto a informacion que puede recopilar.
Glastopf	Diseñado para aplicaciones web, con capacidad de emular miles de vulnerabilidades web. La emulación de los tipos de ataque más populares ya está implementada.	La configuración es compleja, por lo que se debe tener un buen dominio de Linux. La aplicación puede resultar muy lenta y complicada.
Modern Honey Network (MHN)	Facilita la creación de una honeynet de forma rápida y sencilla y ofrece una amplia variedad de sensores. La visualización de todos los datos recolectados se muestran siempre en tiempo real.	Al estar implementado con tecnologías nuevas pueden fallar e introducir errores. La instalación es compleja al ser todo por línea de comandos, además de que solo es compatible con tres sistemas Linux.
Black Officer Friendly (BOF)	Puede correr en cualquier plataforma Windows/ Unix y es fácil instalar, configurar y mantener. Funciona creando sockets abiertos y detectan cualquier conexión que se intente a los mismos.	Su simplicidad trae asociado un costo, debido a que sus capacidades están limitadas. No permite que los logs remotos, alertas o configuraciones sean personalizadas.
T-POT	Posee dashboards de monitorización en tiempo real, para visualizar todos los eventos de seguridad. Incluye una gran variedad de honeypots preparados, configurados y listos para entrar en funcionamiento. Proporciona toda herramientas y documentación necesaria para construir su propio sistema honeypot.	El hardware que utiliza varía en función de si se quiere activar todos los honeypots y herramientas. Los honeypot instalados en T-POT tienen que ser redireccionados hacia el honeypot desde nuestro firewall o router.

FUENTE Elaboración propia.

- ***Comparativa de las soluciones propuestas***

  Sabiendo que existe una lista inmensa de honeypots a utilizar, sean estos empleados para base de datos, data mining, correos electrónicos, desarrollo, servidores, entre otros, la elección de un honeypot como solución para nuestro proyecto deberá de cumplir con los aspectos ya analizados (funcionalidad, nivel de interacción y arquitectura). De esta manera, y teniendo en cuenta las ventajas y desventajas ofrecidas por cada tipo de honeypot, realizaremos una comparativa con las características más relevantes que poseen estas distribuciones y que además podrían ser utilizadas en este proyecto. Esta comparativa se muestra en la *Tabla 07.*

TABLA 07 - COMPARATIVA DE LAS SOLUCIONES PROPUESTAS

DISTRIBUCIONES DE **HONEYPOT**

CARACTERISTICAS	Honeyd	Specter	Glastopf	MHN	BOF	T-POT
Nivel de interacción	Baja	Alta	Media	Alta	Baja	Baja / Alta
Datos obtenidos	Limitado	Extensivo	Limitado	Extensivo	Limitado	Extensivo
Instalación	Fácil	Difícil	Fácil	Difícil	Fácil	Media
Mantenimiento	Fácil	Complejo	Fácil	Complejo	Fácil	Complejo
Riesgo	Bajo	Alto	Bajo	Alto	Bajo	Bajo
Emulación de S.O.	No	Si	Si	Si	No	Si
App / Complementos extra	No	No	No	Si	No	Si

*MHN: Modern Honey Network *T-POT: Honeypot hive, all in one *BOF: Black Officer Friendly

- ***Selección óptima del honeypot***

  Finalmente, después de todo el análisis realizado y de una evaluación exhaustiva de las diferentes distribuciones de honeypots, se decidió optar como solución del presente proyecto al honeypot *T-Pot*. El motivo principal de utilizar este honeypot es básicamente porque cumple con todos los aspectos que justificamos anteriormente correspondiente a la funcionalidad, nivel de interacción y arquitectura y por el amplio abanico de características funcionales que presenta.

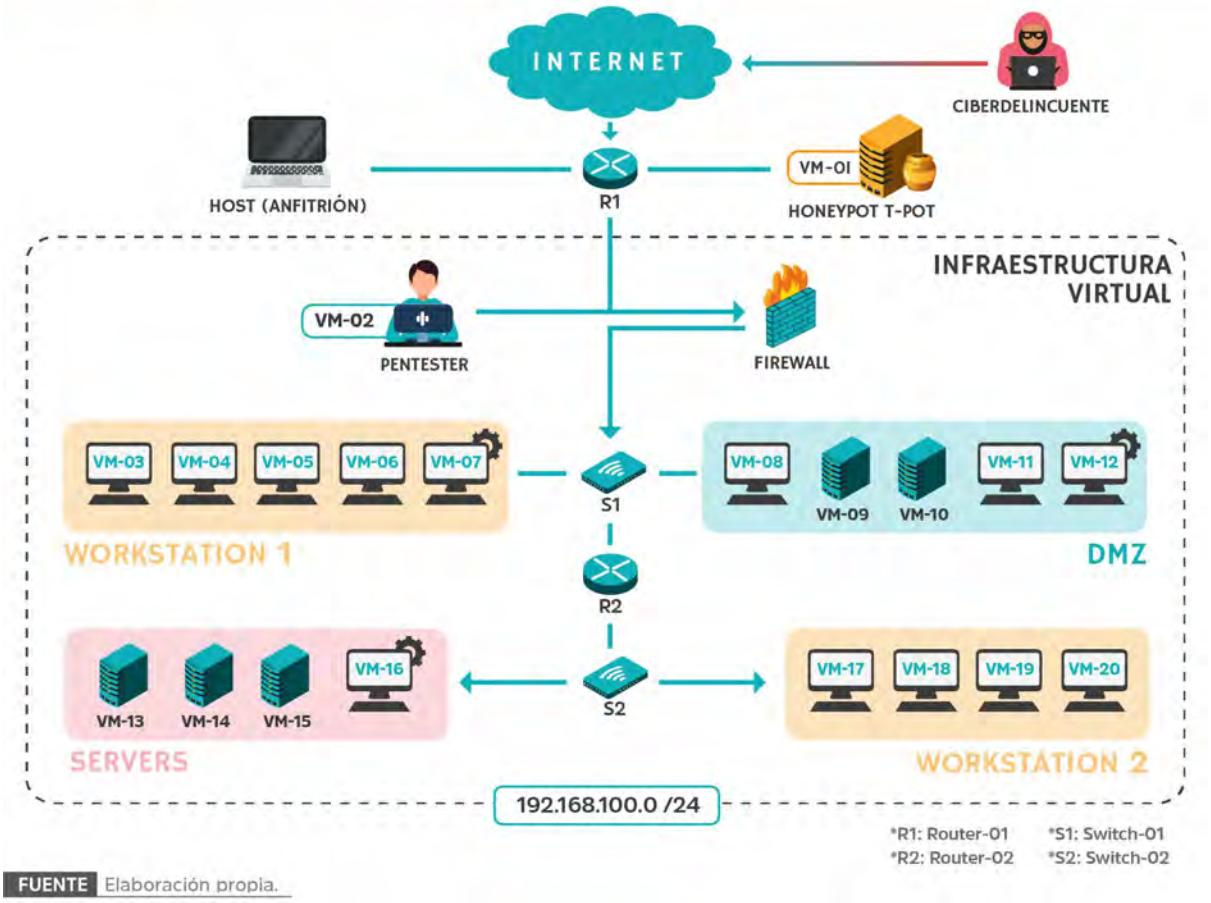
  T-Pot es un desarrollo de código abierto que combina honeypots de baja y alta interacción en un único sistema y se podría traducir básicamente como una gran colmena de honeypots todo en uno, permitiendo que se tengan varios tipos de honeypots dentro de una sola máquina virtual. La gran ventaja de esta distribución es que al incluir una gran variedad de honeypots (conpot, cowrie, dionaea, heralding, tanner, etc.), estos ya vienen todos preparados, configurados y listos para entrar en funcionamiento, y con la particularidad de que vienen virtualizados con docker, haciendo más fácil su mantenimiento, gestión y personalización.

  Además, T-Pot incluye una serie de herramientas (Kibana, Suricata, Cockpit, Spiderfoot, entre otros) muy útiles, las cuales nos permitirán analizar mejor toda la información de los ciberatacantes que disponemos y con ello saber cómo actuar adecuadamente. En cuanto a su implementación, esta es bastantante sencilla, puesto que nos ofrece diferentes formas de instalación según las necesidades específicas que requiera la organización, es de bajo riesgo porque el dashboard de monitorización posee toda la información necesaria, y cuenta con un mantenimiento complejo por la gran cantidad de herramientas que se debe analizar, pero no por esto es complicado su uso. Por lo tanto, con base a todo esto, el honeypot T-Pot es el mejor candidato y una excelente solución que se tiene para poder implementar en este proyecto.

6.2.3 ESQUEMA DE LA INFRAESTRUCTURA

Finalmente en esta etapa se diseña y planifica la arquitectura de red donde se implementará el honeypot que seleccionamos, es decir el *T-Pot*. El esquema de esta infraestructura se basa principalmente en la disposición de los elementos de comunicación (routers, firewalls, switches, equipos, etc.) que la empresa utilizará, además de la ubicación estratégica donde se instalará el honeypot seleccionado.

FIGURA 19 - INFRAESTRUCTURA DE LA RED PARA LA HONEYNET



FUENTE Elaboración propia.

Si observamos, la *Figura 19* muestra en detalle el esquema general de la infraestructura propuesta para este proyecto. En ella podremos ver de manera clara y precisa toda la disposición de equipos que se tiene, el honeypot utilizado (en este caso T-Pot) y la comunicación que existe entre las diferentes redes. Además, en caso de que la empresa PACHA+KOM quisiera expandirse, este esquema nos permitirá tener un mejor criterio a la hora de analizar los nuevos dispositivos o redes a implementar en cuanto a su seguridad se refiere.

Por otro lado, en la infraestructura diseñada se incorporan cuatro equipos adicionales, teniendo así:

- *1 host de pentesting:* Este equipo será destinado para realizar los diferentes tipos de pruebas tanto en la red interna como en la red externa. Es decir, el profesional a cargo determinará el alcance de los fallos de seguridad del sistema, y todo esto con el fin de mantener una seguridad activa y con ello evaluar diariamente como se encuentra la seguridad en la empresa.

- *3 host de soporte:* Estos equipos básicamente funcionarán como equipos de respaldo instalados dentro de algunas redes de la empresa. El objetivo final será que a futuro estos equipos puedan operar como honeypots o bien alojar ciertas herramientas de seguridad, de modo que el atacante tenga más equipos señuelos con los cuales interactuar y no comprometer nuestra red.

Si bien este esquema está estructurado con cuatro redes, en este proyecto solo nos limitaremos a analizar dos redes, evaluando de esta forma una red de estaciones de trabajo y la de servidores, es decir, la red 1 y la red 3 respectivamente. Este alcance se debe básicamente por la falta de recursos con el que contamos actualmente, pero para los fines del presente proyecto, el análisis de estas redes será más que suficiente. Por otro lado, para que la infraestructura diseñada no resulte confusa, la *Tabla 08* muestra en forma general algunas de las características que posee cada red.

TABLA 08 - DETALLE DE LAS REDES IMPLEMENTADAS

RED	TIPO DE RED	MAQUINA VIRTUAL	FUNCIÓN DEL EQUIPO	SISTEMA OPERATIVO
	LAN Externa	VM-01	Honeypot T-POT	Debian v10 (buster)
	LAN Interna / Externa	VM-02	Pentesting/ Hacking Ético	Kali Linux 2021 v3a
Red - 01	LAN Workstation	VM-03	Equipo de trabajo/ Office	Windows 10 Pro x64 v20H1
	LAN Workstation	VM-04	Equipo de trabajo/ Office	Windows 10 Pro x64 v20H1
	LAN Workstation	VM-05	Equipo de trabajo/ Office	Windows 10 Pro x64 v20H1
	LAN Workstation	VM-06	Equipo de trabajo/ Office	Windows 10 Pro x64 v20H1
	LAN Workstation	VM-07	Equipo de soporte	Ubuntu v18. 04. 6
Red - 02	LAN DMZ	VM-08	Servidor de backup	Windows Server 2019
	LAN DMZ	VM-09	Servidor de base de datos	Windows Server 2019
	LAN DMZ	VM-10	Administrador DMZ	Ubuntu v18. 04. 6
	LAN DMZ	VM-11	Administrador DMZ	Ubuntu v18. 04. 6
	LAN DMZ	VM-12	Equipo de soporte	Ubuntu v18. 04. 6
Red - 03	LAN Servers	VM-13	Servidor DNS	OpenSUSE Leap v15. 3
	LAN Servers	VM-14	Servidor WEB	OpenSUSE Leap v15. 3
	LAN Servers	VM-15	Servidor MAIL	Windows Server 2019
	LAN Servers	VM-16	Equipo de soporte	Ubuntu v18. 04. 6
Red - 04	LAN Workstation	VM-17	Equipo de trabajo/ Office	Windows 10 Pro v20H1
	LAN Workstation	VM-18	Equipo de trabajo/ Office	Windows 10 Pro v20H1
	LAN Workstation	VM-19	Equipo de trabajo/ Office	Ubuntu v18. 04. 6
	LAN Workstation	VM-20	Equipo de trabajo/ Office	Ubuntu v18. 04. 6

*Red 01: Workstation (Estaciones de trabajo) *Red 02: DZM (Zona Desmilitarizada)
*Red 03: Servers (Servidores) *Red 04: Workstation (Estaciones de trabajo)

6.2.4 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

Para este proyecto, se deberán tener en cuenta ciertos requisitos para los equipos que montaremos en la infraestructura diseñada. Cada uno de los requerimientos en cuanto a hardware y software se refiere, son los elementos mínimos con los que se deben contar. Estos requerimientos son muy importantes, puesto que nos van a garantizar el correcto funcionamiento de la honeynet virtual autocontenida.

- *Requerimientos para el equipo host (anfitrión)*

  Nuestra infraestructura al ser implementada virtualmente, solo dispondrá de un solo equipo host, el cual podrá ser un portátil o bien un equipo de escritorio, por lo tanto, en este proyecto, se utilizará un equipo portátil, el cual se especifica en la *Tabla 09.* En cuanto al software, se utilizará como sistema operativo base Windows 10 Professional, el hipervisor VMware Workstation para emular las diferentes máquinas virtuales de la infraestructura diseñada y ciertas herramientas gratuitas, que a medida se necesiten se irán instalando.

TABLA 09 - HARDWARE PARA EQUIPO HOST (ANFITRION)

TIPO / MODELO	Notebook 13.3" / HP Spectre x360 v2020
Microprocesador	Intel (R) Core i7-1065G7 CPU @ 1.50 GHZ, 8MB Cache, 4 Núcleos
Memoria RAM	8GB LPDDR4 3200MHZ
Almacenamiento	SSD M2 PCIe NVMe 512 GB
Tipo de Sistema	Sistema Operativo de 64 bits

- *Requerimientos para las estaciones de trabajo (workstation)*

  La empresa dispone de varias estaciones de trabajo destinadas principalmente a trabajos de oficina y administración, las cuales se especifican en la *Tabla 10*. Respecto al software, solo serán instalados herramientas que tengan que ver con el labor de la empresa, por lo que cualquier otro aplicativo que se necesite deberá ser consultado previamente y aprobado por el departamento IT.

TABLA 10 - HARDWARE PARA ESTACIONES DE TRABAJO (WORKSTATION)

Microprocesador	Intel Core i3 o AMD Ryzen 3 de 2.2 MHZ o superior, 2 núcleos
Memoria RAM	8GB DDR4 2133MHZ o superior
Almacenamiento	500GB o 1TB SATA 6GBs (SATA3) 5.4K RPM
Fuente de alimentación	550W 80 Plus Bronze
Interfaz de red	Tarjeta de red Ethernet 10/100/1000 Gigabit
Periféricos	Pantalla LED 22" / Kit teclado+mouse / Tarjeta Wireless /...

- *Requerimientos para servidores*

  Estos servidores son de mucha utilidad para la empresa, puesto que se utilizan para responder y almacenar peticiones de backup, base de datos, correo electrónico, entre otros. Para el software, algunos equipos contarán con sistemas operativos Linux debido a que son más estables, mientras que otros operarán solo con Windows Server. La *Tabla 11* detalla en concreto los componentes necesarios para estos servidores, sean estos implementados de manera física o virtual.

TABLA 11 - HARDWARE PARA SERVIDORES

MODELO	HPE DL180 GEN10
Microprocesador	Intel Xeon Silver 4208 8-Core 2.10GHZ, 11MB
Memoria RAM	16GB RDIMM 2933MHZ
Almacenamiento	HP 2TB 3.5-inch (LPc) SATA 6GB/s 7.2K RPM
Interfaz de red	HPE Embedded 1GbE Dual Port 332i
Fuente de alimentación	HPE 500W Flex Slot Platinum Hot Plug

- *Requerimientos para el honeypot*

  El honeypot T-Pot para poder instalarse adecuadamente requiere de ciertos requisitos, los cuales permitirán que funcione lo más óptimo posible. Por ello, cuanto más recursos tenga este equipo, mejor performance tendrá para emplear los distintos dashboard de monitorización, herramientas de seguridad y el despliegue de honeypots que posee. En cuanto al software, se usará el sistema operativo Debian, el cual alojará el sistema T-Pot con todas sus funcionalidades. La *Tabla 12* detalla el hardware necesario para este equipo.

TABLA 12 - HARDWARE PARA EL HONEYPOT T-POT

REQUISITOS	MINIMOS	RECOMENDADOS
Microprocesador	2 Procesadores con 2 o 4 Núcleos	
Memoria RAM	8GB	16GB
Almacenamiento	128GB	256GB
Interfaz de red	Tarjeta de Red ethernet 10/ 100/ 1000 gigabit	
Fuente de alimentación	Fuente de 500W. 80 Plus Bronze	
Periféricos	Pantalla LED 22" / Kit teclado + mouse/ Tarjeta Wireless	

6.2.5 CONFIGURACIÓN DE LA RED DISEÑADA

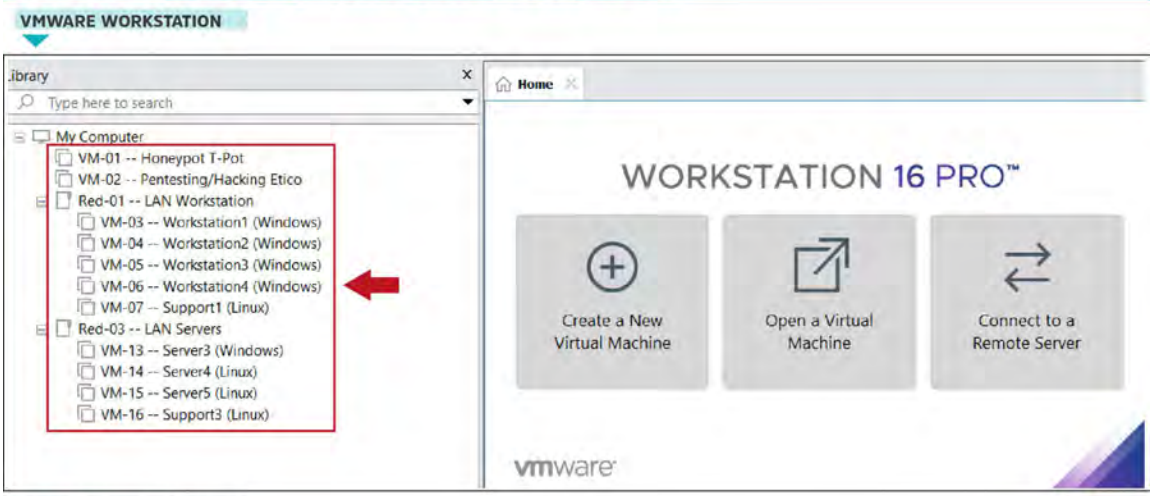
Una vez definida y diseñada la infraestructura con la cual se trabajará en este proyecto, lo que resta es configurar la red virtual. Para ello y según el alcance definido, utilizaremos nuestro equipo host junto con el hipervisor VMware para configurar las redes, los equipos y los dispositivos con los que se trabajará. Por lo tanto, los siguientes pasos explicarán en detalle la configuración más adecuada:

1. *Creación e instalación de máquinas virtuales*

Como primer paso, se deberán de crear todas las máquinas virtuales con las que se trabajará en el proyecto y luego instalar sus respectivos sistemas operativos previamente definidos. Si se sigue el esquema de la infraestructura diseñada (ver *Figura 19*), tendremos que instalar un total aproximado de 20 equipos (hosts), los cuales tendrán usos variados, y la implementación dependerá siempre del alcance definido. Para la creación correcta de máquinas virtuales en el hipervisor VMware consultar el *Anexo 04*, y posteriormente el *Anexo 05* para su respectiva instalación de los sistemas operativos (sean estos Windows o Linux).

Como resultado final, la *Figura 20* nos muestra el listado de máquinas virtuales que instalamos en el equipo anfitrión, además se especifica la red a la que pertenece cada máquina, el sistema operativo empleado y el honeypot principal evaluará la red diseñada. Para este proyecto, el equipo destinado para el honeypot T-Pot será implementado en un servidor privado en la nube (VPS).

FIGURA 20 - LISTADO DE MAQUINAS VIRTUALES INSTALADAS



FUENTE Elaboración propia.

2. *Configuración del adaptador de red en las máquinas virtuales*

Por defecto, cada una de las máquinas virtuales que instalamos tienen configurado el modo de red como NAT(Network Address Translator), lo cual es bueno, debido a que nos ayudará a preservar mejor el espacio de direcciones IPv4, nos proporcionará mayor seguridad en la red y, por lo tanto, mejorará la confiabilidad y flexibilidad de la interconexión con la red global.

Es decir, a través del protocolo NAT[3], cuando salgamos a Internet, nuestras direcciones IPs privadas se convertirán en direcciones IPs públicas, lo cual nos hace una red medianamente segura ante cualquier incidente que se presente.

El sistema NAT es solo uno de los cinco modos de red que tenemos para configurar en VMware, y todo dependerá de cuál será nuestro objetivo final en la empresa. Por ello, para conocer más sobre los adaptadores de red consultar el *Anexo 06*.

3. ***Asignación de direcciones IPs a las máquinas virtuales***

Finalmente lo que resta es configurar la asignación de direcciones IPs de nuestra red. Por lo tanto, como solo vamos a trabajar con dos redes: la red 1, la cual incluye los equipos de trabajo y la red 3 que posee los servidores de la empresa, tendremos que configurar ahora los rangos de red, la asignación de IPs correspondientes para los host virtuales y ciertos parámetros que consideremos.

Para esto, es necesario definir previamente el adaptador de red NAT a utilizar y luego otorgar las direcciones IPs a las redes analizadas mediante el protocolo DHCP[4] utilizando una cantidad de IPs limitadas, puesto que la empresa es pequeña. Toda esta configuración de red se puede consultar en detalle en el *Anexo 07*.

De esta manera, como se pudo observar en el anexo anterior, el direccionamiento IP es de suma importancia dentro de las redes de cualquier tipo, debido a que sin estas direcciones IPs (sean versiones IPv4 o bien IPv6), sería imposible detectar los equipos. Por ello al tener toda nuestra red direccionada, podemos identificar fácilmente nuestros host implementados (virtuales o físicos), y más en un caso tan importante como es la ciberseguridad, donde debemos tener todo controlado para monitorear los accesos no autorizados.

Entonces, con base a toda esta configuración y de forma resumida, la *Tabla 13* muestra cómo se configuraron las redes de la infraestructura diseñada. Además, la tabla muestra las interfaces de cada red, la dirección IP asignada, función del equipo y puerta de enlace.

[3] NAT es el acrónimo que hace referencia a la traducción de direcciones de red. Ver *Glosario*.
[4] DHCP es el acrónimo que hace referencia al protocolo de configuración dinámica de host. Ver *Glosario*.

TABLA 13 - DIRECCIONAMIENTO IP DE MAQUINAS VIRTUALES

MAQUINA VIRTUAL	INTERFACE	DIRECCIÓN IP	FUNCIÓN DEL EQUIPO	PUERTA DE ENLACE
VM-01	1 NAT	34.125.199.232:64294	Administrador del servidor T-Pot	34.125.199.1
	1 NAT	34.125.199.232:64295	Administrador del servidor mediante SSH	34.125.199.1
	1 NAT	34.125.199.232:64297	Dashboard de monitorización T-Pot	34.125.199.1
VM-02	1 NAT	192.168.100.13/ 24	Pentesting/ Hacking Ético	192.168.100.1
VM-03	1 NAT	192.168.100.18/ 24	Equipo de trabajo/ Office	192.168.200.1
VM-04	1 NAT	192.168.100.19/ 24	Equipo de trabajo/ Office	192.168.200.1
VM-05	1 NAT	192.168.100.20/ 24	Equipo de trabajo/ Office	192.168.200.1
VM-06	1 NAT	192.168.100.21/ 24	Equipo de trabajo/ Office	192.168.200.1
VM-07	1 NAT	192.168.100.22/ 24	Equipo de soporte	192.168.200.1
VM-13	1 NAT	192.168.100.23/ 24	Servidor DNS	192.168.200.1
VM-14	1 NAT	192.168.100.24/ 24	Servidor WEB	192.168.200.1
VM-15	1 NAT	192.168.100.25/ 24	Servidor MAIL	192.168.200.1
VM-16	1 NAT	192.168.100.26/ 24	Equipo de soporte	192.168.200.1

6.3 IMPLEMENTACIÓN DEL HONEYPOT

En la segunda etapa de la metodología PDCA, entra en funcionamiento el honeypot escogido, el cual es integrado a la infraestructura diseñada (ver *Figura 19*), para que posteriormente configuremos los elementos necesarios, y a partir de ello poder hacer el análisis de los datos capturados. De esta forma, se analizará el funcionamiento del honeypot T-Pot, los requerimientos necesarios y su correspondiente instalación y configuración.

6.3.1 FUNCIONAMIENTO DE T-POT

Como mencionamos anteriormente, en este proyecto utilizaremos el *Honeypot T-Pot* como herramienta de seguridad proactiva. Esta útil herramienta básicamente consiste en una plataforma de honeypots que tiene como base una distribución Debian que incluye una gran variedad de honeypots dockerizados listos para desplegar. Cada uno de estos honeypots se ejecuta sobre un contenedor de docker distinto, lo que permite tener una mayor facilidad para simular ser elementos individuales y reales de la red. (Joel Pérez Pregal, 2020). Por otro lado, T-Pot cuenta con una implementación bastante sencilla, puede ser configurado de acuerdo con las necesidades específicas de la organización y al ofrecer una plataforma central de gestión, el posible atacante podrá tener acceso a todos los nodos de carga de una falsa infraestructura con los cuales interactuar. (Chema Alonso, 2017).

A continuación explicaremos los aspectos claves con los que trabaja T-Pot, comprendiendo primero su arquitectura, los diferentes tipos de honeypots que se despliegan y las distintas herramientas de monitorización:

— ***Arquitectura***

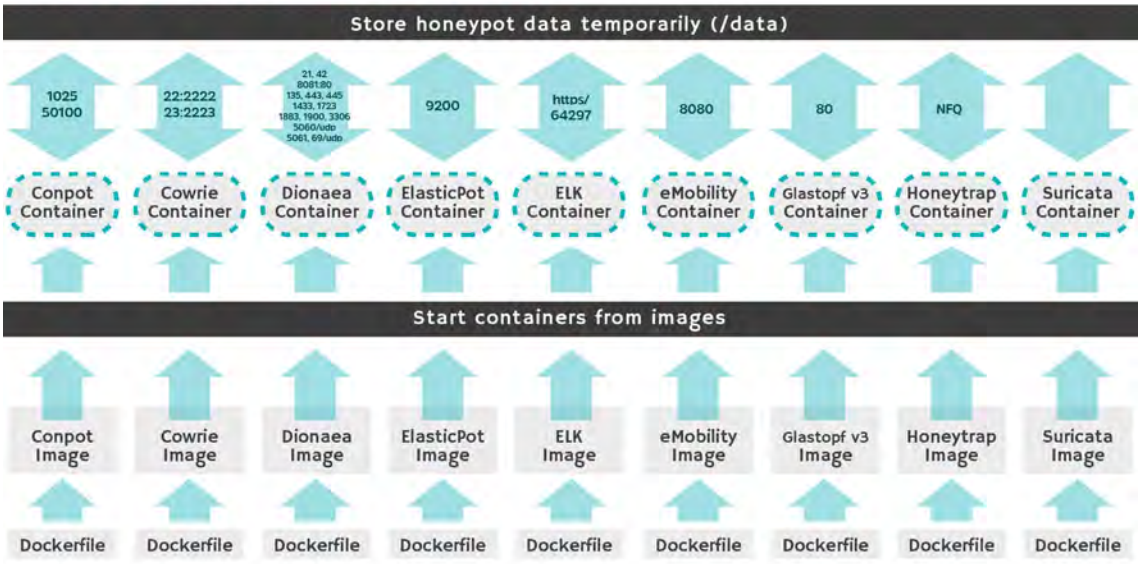
Como T-Pot está basado en docker, su arquitectura es básicamente la misma, siendo un sistema cliente-servidor, en donde un cliente (*DockerClient*) puede comunicarse con los diferentes demonios (*DockerService*) de un contenedor y en donde cada uno de estos demonios del honeypot, así como otros componentes de soporte que se utilizan se han virtualizado todos mediante docker. Con esto, se permite tener en ejecución múltiples demonios de honeypot en la misma interfaz o tarjeta de red sin problemas, lo que hace que todo el sistema sea de bajo mantenimiento. (Telekom-Security).

Básicamente, lo que sucede cuando se inicia el sistema es lo siguiente:

- Inicia el sistema host.
- Inician todos los servicios necesarios (es decir, docker-motor).
- Inician todos los contenedores docker (honeypots, nms, elk).

De esta manera, cuando se logra combinar todos los tipos de honeypots e integrarlos en una misma instalación, los diferentes paneles de monitorización que nos ofrece T-Pot, nos permitirá visualizar fácilmente todos los eventos capturados y con ello, analizar la información para posteriormente tomar las medidas de seguridad más pertinentes. Todos estos detalles se pueden observar en la *Figura 21*, donde además se muestran los puertos que ejecuta cada honeypot.

FIGURA 21 - ARQUITECTURA DEL HONEYPOT T-POT



FUENTE Un informático en el lado del mal, Chema Alonso, 2017

En T-Pot, los puertos de los diferentes honeypots deberán de ser redireccionados hacia el honeypot desde nuestro firewall o router si fuera necesario. Se podrán enviar tantos puertos

TCP como se desee, ya que el honeypot enlaza dinámicamente cualquier puerto TCP que no esté cubierto por los otros demonios honeypot. La *Tabla 14* muestra los puertos que usan los honeypots más comunes, y en donde el número de puerto y la disponibilidad pueden variar según su ubicación geográfica.

TABLA 14 - PUERTOS UTILIZADOS POR LOS HONEYPOTS DE T-POT

SERVICIO	PROTOCOLO	PUERTOS
Conpot	TCP	81, 102, 502
	UDP	161
Cowire	TCP	22
Dionaea	TCP	21, 42, 135, 443, 445, 1433 3306, 5060, 5061, 8081
	UDP	161

SERVICIO	PROTOCOLO	PUERTOS
Elasticpot	TCP	9200
Emobility	TCP	8080
Glastopf	TCP	80
Honeytrap	TCP	25, 110, 139, 3389, 4444 4899, 5900, 21000

FUENTE Un informático en el lado del mal, Chema Alonso, 2017

— ***Honeypots desplegados***

La gran ventaja de utilizar T-Pot es que al ser una plataforma multi-honeypot permite tener varios honeypot dockerizados en un mismo sistema operativo logrando de esta manera tener servicios de red de detección de intrusos y un motor de seguimiento. Según el autor Hernán J. León Loja (2021), algunos de los honeypots más utilizados por T-Pot incluyen a:

- Conpot: Se define como un honeypot que posee un nivel de interacción baja el cual permite emular una infraestructura industrial compleja, siendo de fácil implementación, modificación y extensión. Su objetivo principal es recopilar información sobre los motivos y métodos de los adversarios que apuntan a los sistemas de control industrial (ICS).
  https://github.com/mushorg/conpot

- CitrixHoneypot: Este honeypot crea un sitio web falso sobre el protocolo HTTPS en donde los posibles atacantes tratarán de ingresar al sistema usando una forma de autenticación para vulnerar la seguridad de la página.
  https://github.com/MalwareTech/CitrixHoneypot

- Cowrie: Simula ser un servidor SSH y TELNET con una interacción media a alta diseñado para registrar ataques de fuerza bruta, además de registrar las formas en que actúa un atacante para intentar penetrar el sistema. Cowrie permite a los atacantes acceder al honeypot usando un cliente TELNET o SSH emulado, siendo capaz de registrar toda la información de la sesión que realiza el atacante en formato JSON para luego ser utilizado por otras herramientas.
  https://github.com/cowrie/cowrie

- Dionaea: Es un honeypot de carácter general diseñado para simular vulnerabilidades de red y servicios como HTTP, FTP, o MySQL, entre otros. Fue diseñado para atrapar el malware que explota las vulnerabilidades publicadas por los servicios red, con el objetivo final de obtener una copia del malware utilizado por el atacante.
  https://github.com/DinoTools/dionaea

- Honeytrap: Es una herramienta que se centra en observar los ataques contra los servicios TCP y UDP. En este caso, todos los atacantes serán engañados y enviarán respuestas a un proceso del servidor honeytrap.
  https://github.com/armedpot/honeytrap/

- Mailoney: Simula ser un servicio de correo electrónico que al utilizar el protocolo SMTP por el puerto 25, nos permitirá registrar los diferentes emails enviados cuando el servicio se configure como open relay, además registra las credenciales usadas en los intentos de inicios de sesión.
  https://github.com/phin3has/mailoney

- Rdpy: Fue desarrollado en Python para simular un servicio de protocolo de escritorio remoto (RDP) de Microsoft, funcionando como un MiTM (Man in the middle) para registrar la sesión.
  https://github.com/citronneur/rdpy

- Heralding**:** Es un honeypot simple que únicamente recoge información de inicio de sesión o credenciales utilizados en los diferentes protocolos de red como FTP, HTTPS, SSH, SMTP, etc.
  https://github.com/johnnykv/heralding

- Honeysap: Está centrado en la investigación específica para servicios SAP. Principalmente busca aprender las técnicas y motivaciones detrás de los ataques contra los sistemas SAP.
  https://github.com/SecureAuthCorp/HoneySAP

Otros honeypots dockerizados que incluye este T-Pot para sus estadísticas son:

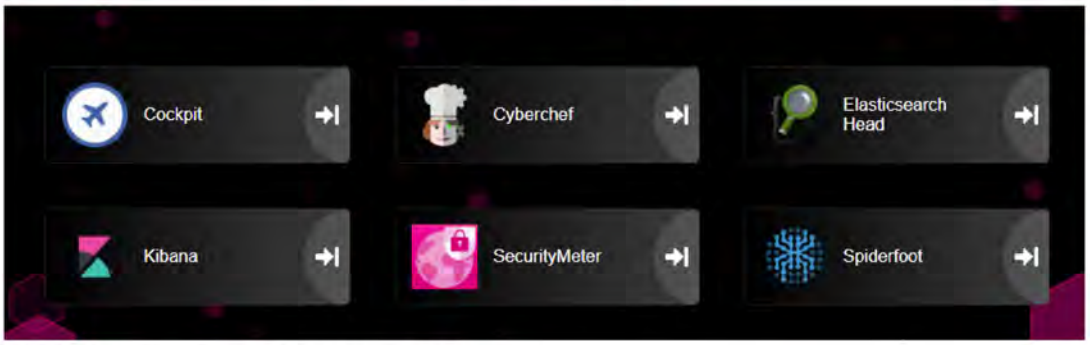
- adbhoney https://github.com/huuck/ADBHoney
- ciscoasa https://github.com/Cymmetria/ciscoasa_honeypot
- ddospot https://github.com/aelth/ddospot
- dicompot https://github.com/nsmfoo/dicompot
- elasticpot https://gitlab.com/bontchev/elasticpot

- endlessh https://github.com/skeeto/endlessh
- glastopf https://github.com/mushorg/glastopf
- glutton https://github.com/mushorg/glutton
- hellpot https://github.com/yunginnanet/HellPot
- honeypy https://github.com/foospidy/HoneyPy
- ipphoney https://gitlab.com/bontchev/ipphoney
- medpot https://github.com/schmalle/medpot
- redishoneypot https://github.com/cypwnpwnsocute/RedisHoneyPot
- snare https://github.com/mushorg/snare
- tanner https://github.com/mushorg/tanner

- ***Herramientas de monitorización (dashboards)***

Estas herramientas sirven para monitorear en tiempo real los diferentes honeypots que utiliza T-Pot, permitiendo recoger datos de la interacción de los atacantes para luego mostrarlos en los diferentes dashboard que utilicemos. Estos aplicativos son ejecutados sobre contenedores docker.

FIGURA 22 - HERRAMIENTAS DE MONITOREO UTILIZADOS POR T-POT



FUENTE Elaboración en base a Telekom-Security, 2021.

- *Cockpit*: Permite a los administradores de sistemas Linux gestionar fácilmente sus servidores y realizar tareas sencillas, como administrar el almacenamiento del sistema, verificar registros, iniciar o detener servicios, actualizar e instalar aplicaciones, entre otros. (ProgrammerClick, 2018).

- *CyberChef*: Es una aplicación web para realizar encriptación, codificación, compresión y análisis de datos, permitiendo a los analistas manipular los datos de manera compleja sin tener que lidiar con herramientas complejas. (Joel Pérez Pregal, 2020).

- *Elasticsearch Head:* Es un motor de analítica y análisis distribuido, abierto para todo los tipos de datos estructurados o no estructurados. Elasticsearch es el componente principal

de Elastic Stack, un conjunto de herramientas gratuitas para el almacenamiento y análisis de visualización de datos, usada para indexar varios tipos de contenidos tales como búsqueda de aplicaciones, búsqueda de sitios web, analitica de seguridad, entre otros. (Hernán J. León Loja, 2021).

- *Kibana*: Es el aplicativo más importante para visualizar datos. Estos datos se generan mediante la combinación de las herramientas elasticsearch, logstash y kibana, conocida como ELK Stack. Logstash proporciona un flujo de datos de entrada a elasticsearch para el almacenamiento y la búsqueda, y Kibana accede a esos datos para realizar las visualizaciones desde la interfaz web. (Joel Pérez Pregal, 2020).

- *Security Meter*: Se encarga de medir constantemente la temperatura de los ataques, es decir, funciona como un radar en tiempo real detectando todos los ataques que están ingresando a nuestro equipo, y el cual es alimentado a través de un protocolo particular que envía toda la información completamente anónima. Es decir, esta herramienta funciona de manera similar a las plataformas web de ciberinteligencia que usan las grandes empresas de ciberseguridad.

- *SpiderFoot*: Es una herramienta OSINT que facilita el proceso para recoger información a través de Internet, al realizar la agregación de diversas fuentes, como por ejemplo shodan,bing o google, entre otras, sobre las que permite realizar una búsqueda a través de su propia interfaz web. (Joel Pérez Pregal, 2020). Además podremos obtener diversa información sobre objetivos relacionados, como subdominios de sitios web, direcciones de correo electrónico, versiones de servidores web, etc. La sencilla interfaz permite iniciar el escaneo después de la instalación; simplemente se debe configurar el nombre de dominio de destino del escaneo y habilitar el módulo de escaneo. (ProgrammerClick, 2018).

6.3.2 INSTALACIÓN DE T-POT

La instalación del honeypot T-Pot es realmente sencilla, puesto que este sistema podrá ser montado en cualquier máquina virtual, ya sea de forma local en VMware o bien en algún servicio VPS[5] de la nube. Básicamente se hará uso de un servidor principal, el cual se encargará de desplegar los distintos tipos de honeypots que posee la herramienta, montado sobre el sistema operativo Debian (o Ubuntu).

[5] VPS es el acrónimo que hace referencia a un servidor privado virtual. Ver *Glosario*.

Una vez instalado el honeypot, después se podrán ir instalando nuevos aplicativos y servicios según se requiera y se tenga los recursos necesarios para correrlos adecuadamente. Los requisitos y especificaciones para este equipo ya fueron especificadas anteriormente (ver *Tabla 12*).

Elementos necesarios

- Tener creado una máquina virtual con las especificaciones indicadas (ver *Anexo 04*).
- Tener instalado en la máquina virtual el sistema operativo base, es decir Debian (ver *Anexo 05*)
- Haber configurado previamente las interfaces de red (ver *Anexo 07*)
- Tener descargado la imagen ISO del sistema de: https://github.com/telekom-security/tpotce

Si bien la instalación de este honeypot no es compleja, su éxito dependerá en gran medida de tener una buena conexión a internet y de los recursos del equipo, caso contrario la instalación podría fallar. Por lo tanto, como primer paso hay que decidir cómo obtendremos el sistema T-Pot que vamos a instalar. Este sistema puede ser descargado como imagen ISO desde el repositorio de Github, puede ser creado por uno mismo, es decir, una imagen ISO totalmente personalizada según lo que necesitemos o bien se puede instalar el sistema T-Pot después de haber instalado previamente un sistema Debian. Posterior a todo esto, lo que resta es determinar en donde se ejecutará, y si será en un equipo con hardware físico o en una máquina virtual, pero para este proyecto, la implementación será totalmente virtual.

Los métodos de obtención del sistema T-Pot e instalación son:

1. ***Imagen ISO prediseñada***

   Este tipo de imagen se descarga del repositorio oficial de T-Pot y es una imagen prediseñada, es decir, cuando lo instalamos este ya viene predeterminado con ciertas herramientas y aplicaciones, con lo cual nos ahorra mucho tiempo de descargar componentes adicionales. Por lo tanto, esta opción solo es factible si la usamos con un hipervisor (VMware por ejemplo). Toda la instalación de este tipo de imagen se detalla en el *Anexo 08*.

2. ***Imagen ISO personalizada***

   Aquí podremos instalar el sistema T-Pot en base a ciertos aplicativos, servicios y herramientas que queremos que tenga nuestra imagen ISO. Pero básicamente se utiliza este método por razones de transparencia, seguridad del usuario y los objetivos que se tenga.

   Requisitos para crear la ISO:

   - Debian 10 como sistema host.
   - 4GB de memoria RAM/ 32GB de almacenamiento en disco.
   - Una conexión a Internet estable.

Para instalar, seguir estos pasos:

a. Clonar el repositorio y luego entrar en la carpeta clonada.

```
git clone https://github.com/telekom-security/tpotce
cd tpotce
```

b. Ejecutar el script *makeiso.sh* para crear la imagen ISO. Este script será el encargado de descargar e instalar las dependencias necesarias para construir la imagen en la máquina que invoca.

```
sudo ./makeiso.sh
```

c. Después de que se compile, encontrará la imagen ISO con el nombre *tpot.iso*.

3. ***Después de una una instalación posterior***

En este caso será necesario instalar previamente el sistema operativo Debian 10 (Buster) por nuestra cuenta y una vez realizada esta acción, descargar del repositorio de Telekom-Security el instalador universal T-Pot el cual actualizará e instalará todas las dependencias necesarias. Para instalar correctamente un sistema con Linux consultar el *Anexo 05*.

Para instalar, seguir estos pasos:

```
git clone https://github.com/telekom-security/tpotce
cd tpotce/iso/installer/
./install.sh --type=user
```

Esta instalación es la que emplearemos en este proyecto, puesto que la instalación del sistema operativo Debian podrá ser instalado localmente en VMware o bien en cualquier VPS alojado en la nube, contemplando siempre los requisitos necesarios. La instalación del honeypot T-Pot en un VPS se detalla en el *Anexo 09*.

Luego de haber instalado correctamente el honeypot T-Pot por medio de la imagen ISO, ya lo tendremos activado y funcionando en nuestro equipo, solo resta configurar ciertos parámetros. Por lo tanto, cuando ejecutemos el sistema T-Pot tendremos tres puertos con lo cuales podremos gestionar eficientemente la monitorización, administración y configuración de la máquina virtual y sus contenedores:

- **64294: Administración del servidor T-Pot** https://34.125.199.232:64294

  En esta interfaz podremos realizar la gestión y el mantenimiento de los distintos contenedores de T-Pot, monitorizar el consumo de recursos de la máquina virtual, o monitorizar registros del

sistema, entre otras tareas de gestión. Accedemos mediante la dirección IP asignada e iniciamos sesión con las credenciales que especificamos durante la instalación. Por defecto el usuario del servidor es *tsec*. (Joel Pérez Pregal, 2020).

- **64295: Administración del servidor mediante SSH** https://34.125.199.232:64295
  Aquí se podrá realizar el desarrollo y el despliegue de nuevos honeypots para implementar en la arquitectura que se ha definido, así como la modificación de ciertos honeypots ya existentes para adaptarlos al funcionamiento deseado. Mediante el acceso SSH a la máquina virtual T-Pot, entre otras cosas, se crearán los nuevos archivos de docker necesarios para el despliegue de los nuevos honeypots y se aplicarán las configuraciones necesarias en el sistema de registro de eventos. (Joel Pérez Pregal, 2020).

- **64297: Dashboard de monitorización T-Pot:** https://34.125.199.232:64297
  Esta interfaz, permite al usuario acceder a una gran variedad de herramientas para realizar la monitorización y gestión de los datos procedentes de los diversos honeypots de la máquina T-Pot. Para acceder a esta interfaz, nos dirigimos a la dirección IP asignada y nos logueamos con el usuario y contraseña que establecimos durante la instalación. (Joel Pérez Pregal, 2020).

6.3.3 CONFIGURACIÓN DE SERVICIOS T-POT

Una vez que instalamos nuestro T-Pot, configuraremos ahora ciertos servicios y parámetros que serán necesarios antes de usar las direcciones IPs que nos otorga el honeypot. Toda esta configuración nos permitirá redirigir todo el tráfico de nuestra red a la dirección IP del honeypot, de forma que cuando un atacante intente comprometer nuestra red, éste se dirija automáticamente al honeypot configurado y de esa manera poder controlar todos los accesos que realizan los atacantes en nuestro sistema.

Hay que tener en cuenta que la instalación realizada del T-Pot cambió muchas cosas, entre ellas se movió el puerto SSH predeterminado al puerto 64295 para hacerlo mucho más atractivo para los delincuentes, por lo que deberemos conectarnos a ese puerto para poder acceder a la máquina virtual, ya que el puerto 22 se asignará al honeypot SSH. Es decir, como en nuestra configuración de máquina virtual, solo tenemos el puerto 22 expuesto a Internet, esto no es suficiente para que nuestro honeypot funcione correctamente, por ende necesitamos exponer todos los puertos.

Por lo tanto, para solucionar este problema solo basta con agregar ciertas reglas de seguridad en nuestro firewall para exponer todos los puertos a Internet. Esta configuración de firewall dependerá de donde esté instalado el T-Pot, para ver si se configura en el sistema anfitrión o en algún VPS.

1. ***Configuración del firewall en Windows (útil para VMware)***

Si tenemos instalado T-Pot en una máquina virtual por medio del hipervisor VMware deberemos de agregar ciertas reglas de seguridad en el firewall de nuestro equipo host (anfitrión) para poder enviar todos los puertos TCP/ UDP a la máquina virtual T-Pot. Por otro lado, si además tenemos una red DMZ, también deberíamos de asignarle la dirección IP otorgada por el honeypot. Es decir hay que configurarlo con el fin de que cada atacante ingrese al honeypot y no a nuestra red.

TABLA 15 - REGLAS DE FIREWALL PARA WINDOWS

Reglas de entrada						
Nombre	Perfil	Protocolo	Puerto local	Dirección local	Dirección remota	Acción
Firewall tpot 2	Todo	TCP	64294, 64295, 64297	Cualquiera	Cualquiera	Permitir
Firewall tpot 1	Todo	TCP	Cualquiera	Cualquiera	Cualquiera	Permitir
KMS Emulator Port	Público	TCP	1688	Cualquiera	Cualquiera	Permitir
KMS Emulator: KMSELDI.exe	Público	TCP	Cualquiera	Cualquiera	Cualquiera	Permitir

2. ***Configuración del firewall en un VPS (útil para Google Cloud Platform)***

En este caso, al tener nuestro honeypot instalado en la nube, es decir en un servidor privado virtual (VPS) como DigitalOcean, Amazon Web Services, Google Cloud Platform, entre otros, solo bastará con agregar las siguientes reglas de entrada en el firewall y en algunos casos configurar que solo nosotros tengamos acceso. Para Google Cloud Platform, esta configuración se encuentra dentro de la opción de *Red VPC>Firewall.*

TABLA 16 - REGLAS DE FIREWALL PARA GOOGLE CLOUD PLATFORM

Nombre	Tipo	Filtros	Protocolos/puertos	Acción	Prioridad
tpot-access-dashboard	Entrada	Intervalos de IP: 186.136.192.106/32	tcp:64297	Permitir	1000
tpot-access-ports	Entrada	Intervalos de IP: 0.0.0.0/0	all	Permitir	1000
tpot-access-ssh	Entrada	Intervalos de IP: 186.136.192.106/32	tcp:64295	Permitir	1000
default-allow-icmp	Entrada	Intervalos de IP: 0.0.0.0/0	icmp	Permitir	65534
default-allow-internal	Entrada	Intervalos de IP: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Permitir	65534
default-allow-rdp	Entrada	Intervalos de IP: 0.0.0.0/0	tcp:3389	Permitir	65534
default-allow-ssh	Entrada	Intervalos de IP: 0.0.0.0/0	tcp:22	Permitir	65534

Como recomendaciones generales, antes de instalar este honeypot en la máquina virtual, será necesario establecer estas reglas de firewall, puesto que durante la instalación pueden llegar a surgir errores o bien cuando se ejecute el servidor no funcionar correctamente.

3. ***Verificación de puertos***

   Luego de configurar la capa de seguridad en el firewall, verificamos los puertos que tiene abierto el servidor. Si todo está bien, la herramienta *nmap* nos mostrará un listado con el estado general de esos servicios. De esta manera, ahora podremos ingresar de manera segura a las direcciones URL otorgadas por el honeypot T-Pot. Para verificar estos puertos tipear en consola *nmap <nuestra IP>.*

FIGURA 23 - VERIFICACIÓN DE PUERTOS ABIERTOS EN EL SERVIDOR T-POT

```
Host is up (0.28s latency).
Not shown: 141 closed ports
PORT      STATE SERVICE
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
80/tcp    open  http
```

FUENTE Elaboración propia.

Finalmente, cuando concluimos con estas configuraciones y ejecutamos el sistema T-pot, los resultados comenzarán a llegar en cuestión de minutos y de esa manera podremos observar todos los ataques que vamos a ir recibiendo. De esta forma, al verificar las diferentes herramientas y paneles de monitorización que posee el T-Pot podremos analizar mejor toda la información y con ello poder tomar las mejores decisiones para proteger nuestra red o la red de cualquier organización.

6.3.4 USO DE T-POT

A continuación se explicará brevemente algunos de los usos más frecuentes que podemos realizar con el honeypot. Los comandos utilizados fueron ejecutados desde el servidor mediante SSH.

1. *Verificar estado del servicio T-Pot*

   Nos permitirá saber en qué estado se encuentra el honeypot, es decir si está en ejecución o inactivo. Además podrá darnos información sobre algún error específico. Para verificar esto solo deberemos de tipear *system status tpot* o bien verificar con *nmap (*ver *Figura 23).*

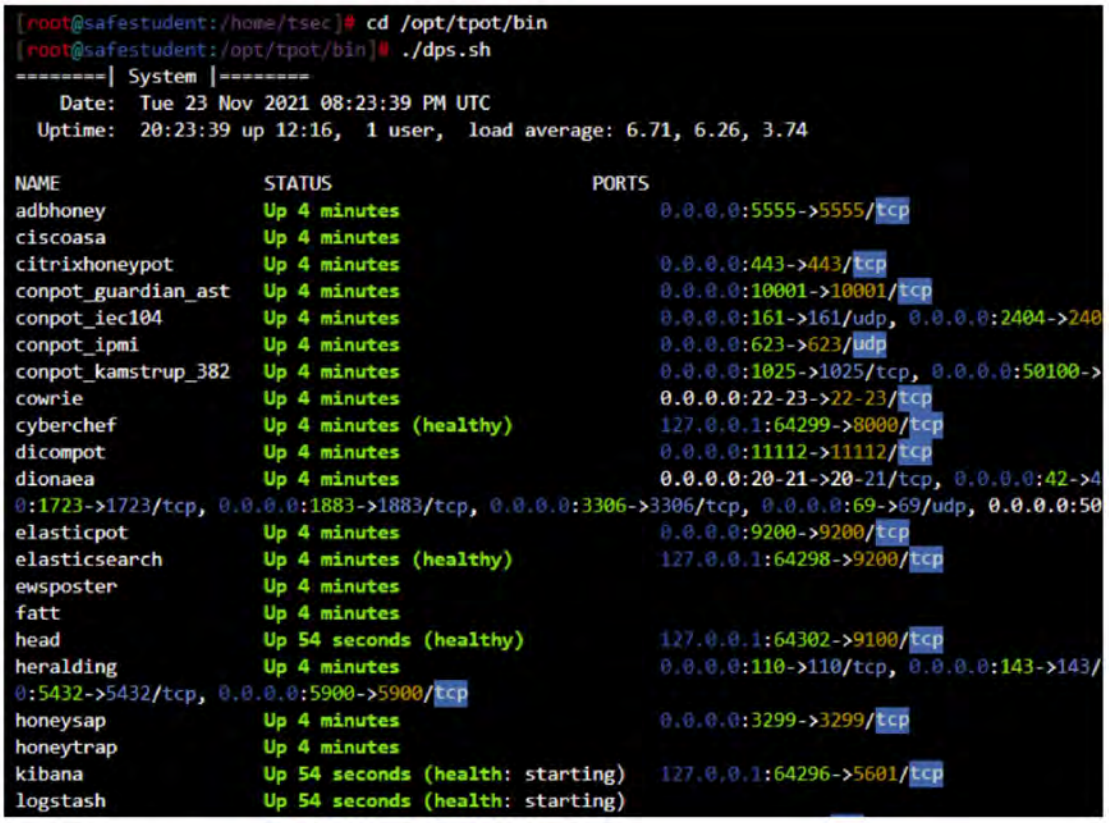
2. *Verificar estado del servicio T-Pot*

   Consiste en saber qué puertos están ocupados. Para ello, primero debemos de detener el servicio de T-Pot con el comando *systemctl stop tpot* y luego ejecutar *netstat -tulpen*. Luego de realizar estas acciones, volvemos a encender el honeypot, para ello ejecutamos *systemctl start tpot.* Para todas estas acciones tenemos que estar logueados en modo root.

3. *Verificar contenedores T-Pot*

   Para poder ver el estado actual de los contenedores que contienen los honeypots, nos dirigirnos a la carpeta */opt/tpot/bin* y escribimos *./dps.sh.* La pantalla básicamente nos muestra el estado de dicho honeypot, y su puerto. Otra forma de acceder es utilizando Docker como *docker ps*.

FIGURA 24 - VERIFICACIÓN DE CONTENEDORES T-POT



FUENTE Elaboración propia en base al sistema T-Pot.

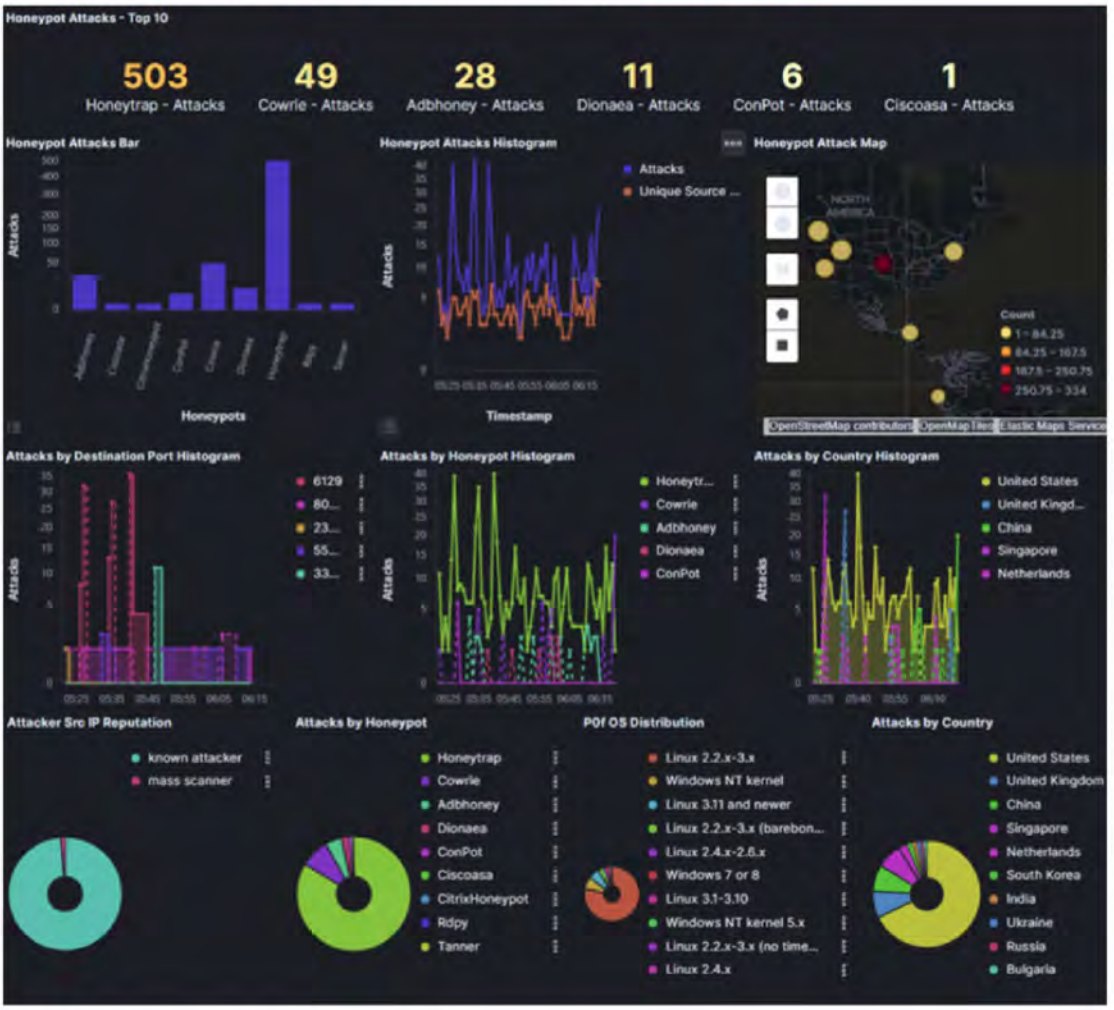
4. *Monitorización mediante los aplicativos de T-Pot*

   Para poder monitorear de manera efectiva los ataques recibidos en la máquina virtual, T-Pot cuenta con varias herramientas *(*ver *Figura 22)* que nos permitirán gestionar todos los datos procedentes de los diversos honeypots de la máquina T-Pot.

   Para esto, solo basta con ingresar la dirección IP que nos otorgó el honeypot durante su instalación (https://34.125.199.232:64297) y una vez logueados, la interfaz web nos mostrará los aplicativos instalados, entre ellos Cockpit, Cyberchef, Elasticsearch Head, Kibana, SecurityMeter y Spiderfoot, con los cuales podremos evaluar, y hacer varios análisis de las métricas que consideremos, según la información que estemos buscando o se requiera.

Si no vamos a la herramienta *Kibana*, observamos que cada honeypot proporciona datos diferentes, sin embargo, todos tienen una base común de datos que se utiliza para obtener algunas métricas genéricas. Lo bueno de esta herramienta es que la mayoría de los paneles de monitorización que utiliza T-Pot son interactivos y en tiempo real, dando la posibilidad de filtrar datos para obtener información sobre ataques concretos, ataques según una localización o dirección IP específica, top de ataques más comunes, entre otros (ver *Figura 25*).

FIGURA 25 - ESTADISTICAS DE LOS CIBERATAQUES CAPTURADOS POR KIBANA



FUENTE Elaboración propia en base al sistema T-Pot.

Y como mencionamos anteriormente, T-Pot posee muchos tipos de honeypots, cada uno en su rol específico y mostrando información realmente valiosa para los expertos de TI. Por ende, con todas las herramientas que nos ofrece T-Pot se tiene un gran abanico de recursos que serán de mucha utilidad para los expertos en ciberseguridad, ya que además, cada aplicativo utiliza otras fuentes para poder certificar aún más la información y de esa forma nos permite hacer una ciberinteligencia a un nivel casi tan detallado como OSINT. Es decir, identificando la dirección IP

de nuestro atacante, podremos saber qué tan comprometido está esa IP ya sea simplemente accediendo a esa dirección por medio de Kibana o bien evaluando la IP en Spiderfoot o Elasticsearch Head (ver *Figura 26*).

Sin duda alguna, la empresa Telekom-Security dueño del proyecto T-Pot ha hecho un gran trabajo al armar esta herramienta de seguridad, ya que al utilizar diferentes paneles frontales de monitoreo, brindan al usuario un excelente método estructurado y relevante para encontrar patrones en los ataques y generar vistas poderosas y visuales de la primera línea de Internet. Además, T-Pot es una excelente oportunidad de aprendizaje para aquellos que quieran comenzar a utilizar herramientas de seguridad informática a un nivel no tan sofisticado, pero con muchos recursos útiles.

6.4 ESCENARIOS DE PRUEBAS Y RESULTADOS

Finalmente llegamos a la tercera etapa de la metodología PDCA, es decir la verificación (check). Esta fase es quizás, la más importante, puesto que se realizarán las pruebas funcionales con el honeypot y se verificará el cumplimiento de los objetivos planteados. Básicamente, mediante los diferentes escenarios de pruebas que realicemos, podremos detectar y registrar todas las actividades maliciosas que suceden en la red diseñada, obteniendo así una gran cantidad de información sobre los atacantes, ya sea lugar de procedencia, proveedor de Internet utilizado o los métodos empleados para vulnerar el sistemas. De esta manera, al quedar todo registrado, los diferentes paneles de monitorización que emplea T-Pot nos otorgará información realmente relevante y certera, permitiendo así tomar las mejores decisiones en cuanto a seguridad se refiere.

A continuación vamos a explicar algunos escenarios de pruebas contra el honeypot T-Pot, de forma que se puedan registrar cualquier ataque malicioso con el fin de obtener datos suficientes para analizarlos. Si bien hay un sin fin de herramientas y metodologías para realizar ciberataques, vulnerando ya sea la red o un host específico, en este proyecto nos limitaremos a los ataques más típicos. Para conocer algunos de los ataques que emplearemos, consultar el *Anexo 11*.

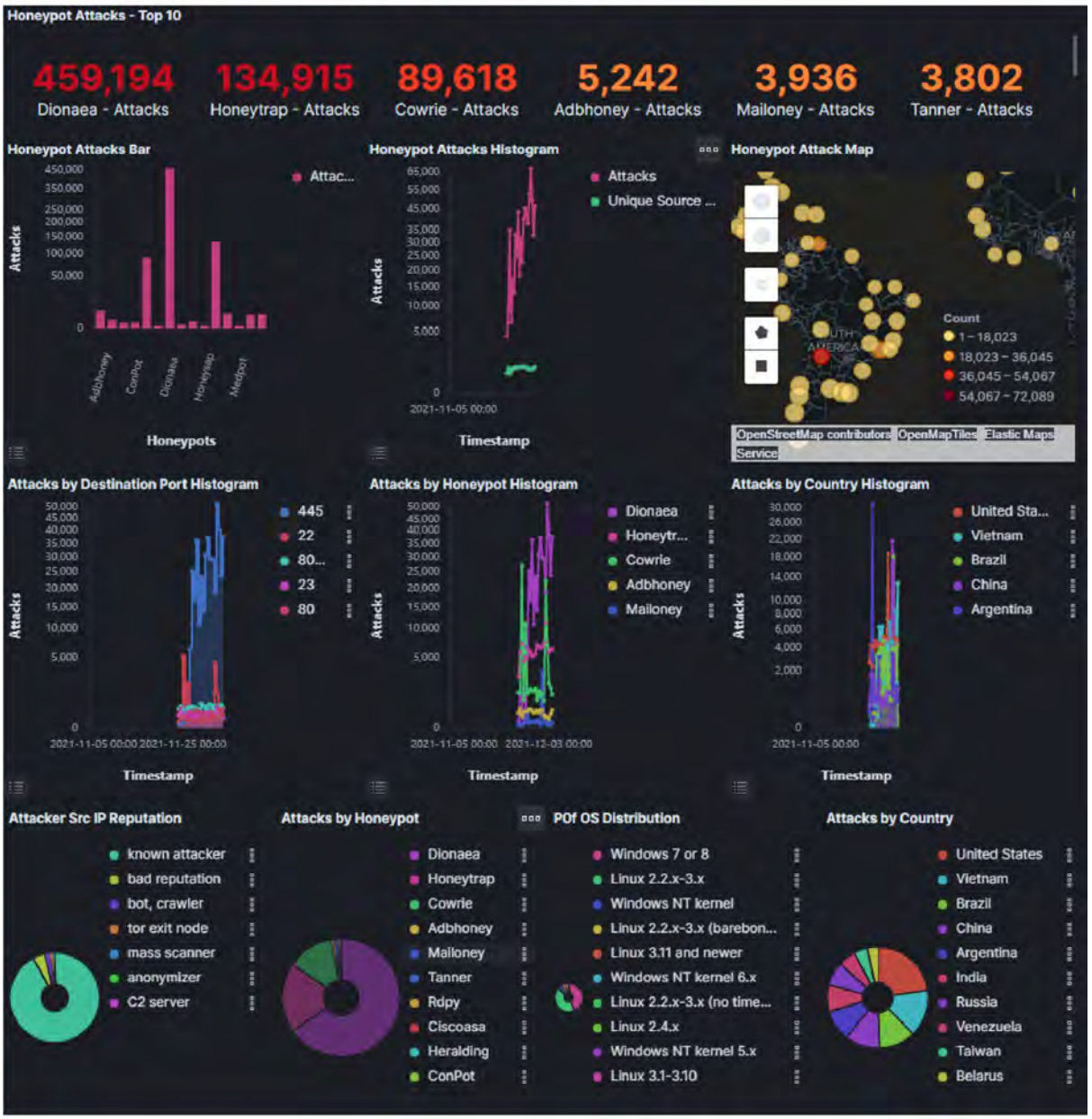
6.4.1 ESCENARIO-01: ATAQUES RECOPILADOS CON T-POT

Este escenario es quizás el más básico, pero a su vez el más efectivo, puesto que cuando el servidor T-Pot está activo, los ataques empezarán a llegar en cuestión de minutos. Esto es así, ya que ahora este equipo es un nodo señuelo y un host atractivo dentro de la red de redes para cualquier atacante. Por lo tanto, si a partir de ahora entramos a los diferentes paneles de monitorización (dashboard) que nos ofrece T-Pot observaremos rápidamente una gran cantidad de datos recopilados sobre los atacantes y con los cuales podremos hacer ciberinteligencia. Por ello, cuanto más tiempo

estén ejecutándose los diferentes tipos de honeypots que emplea T-Pot, mayor será la cantidad de información que habrá que evaluar.

De forma general, las siguientes figuras, muestran en detalle los ataques continuos que fue recibiendo nuestro honeypot durante aproximadamente 40 horas activas, plasmados en diferentes histogramas y gráficos estadísticos, dando un total de 40.000 ataques, mientras que en un lapso de una semana, el ataque llegó a unos 450.000. La actualización de ataques es siempre en tiempo real.

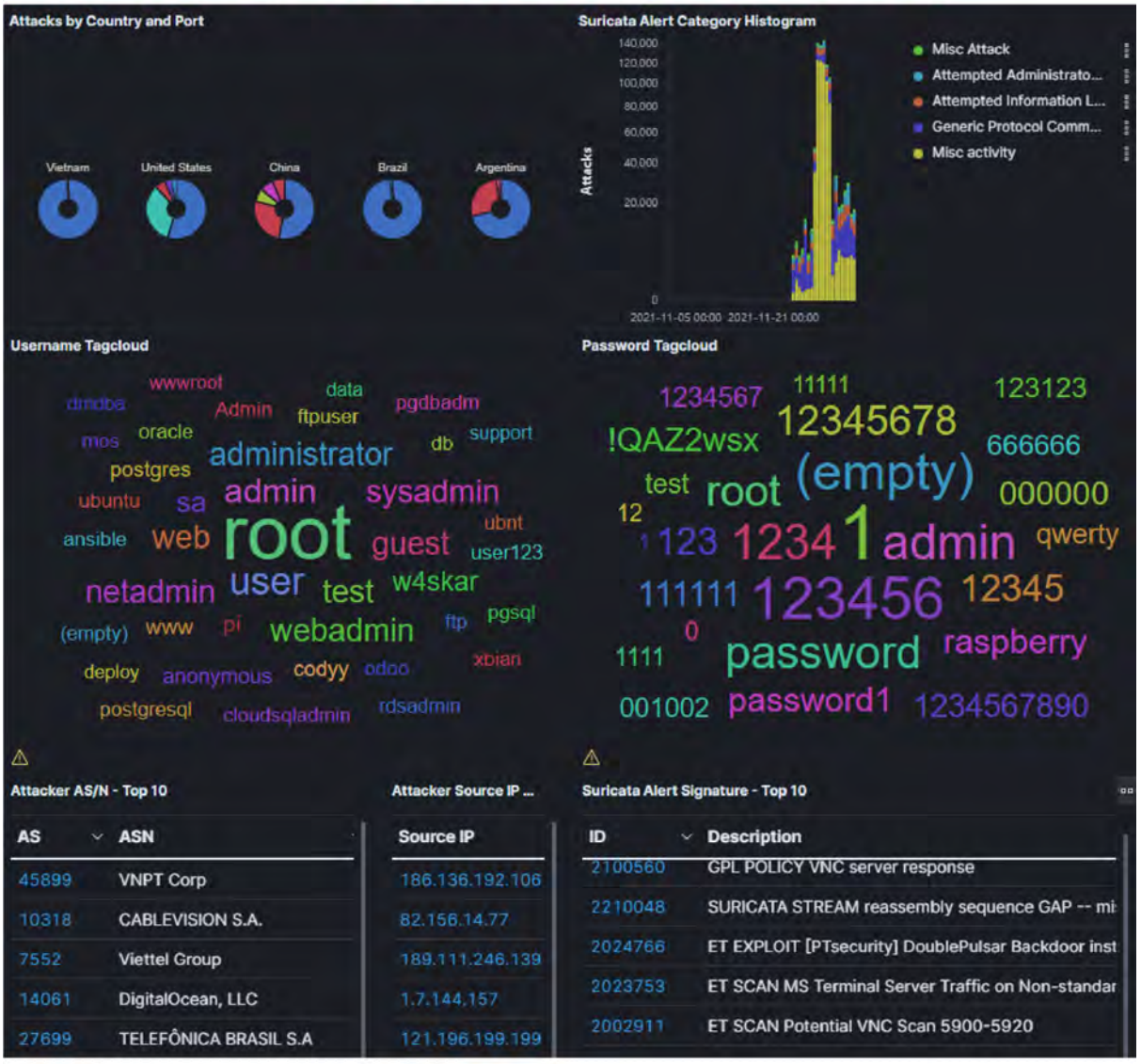
FIGURA 26 - ATAQUES RECOPILADOS CON T-POT A NIVEL MUNDIAL



FUENTE Elaboración propia en base al sistema T-Pot.

En la actualidad los honeypots son una fuente de información realmente útil e importante para cualquier organización, puesto que con ellos podemos registrar todos los métodos que utilizan los ciberatacantes y luego verificar la información de forma clara y detallada en los diferentes dashboard que tenemos (ver *Figura 27*), sin que esto llegue a comprometer de alguna forma nuestra red.

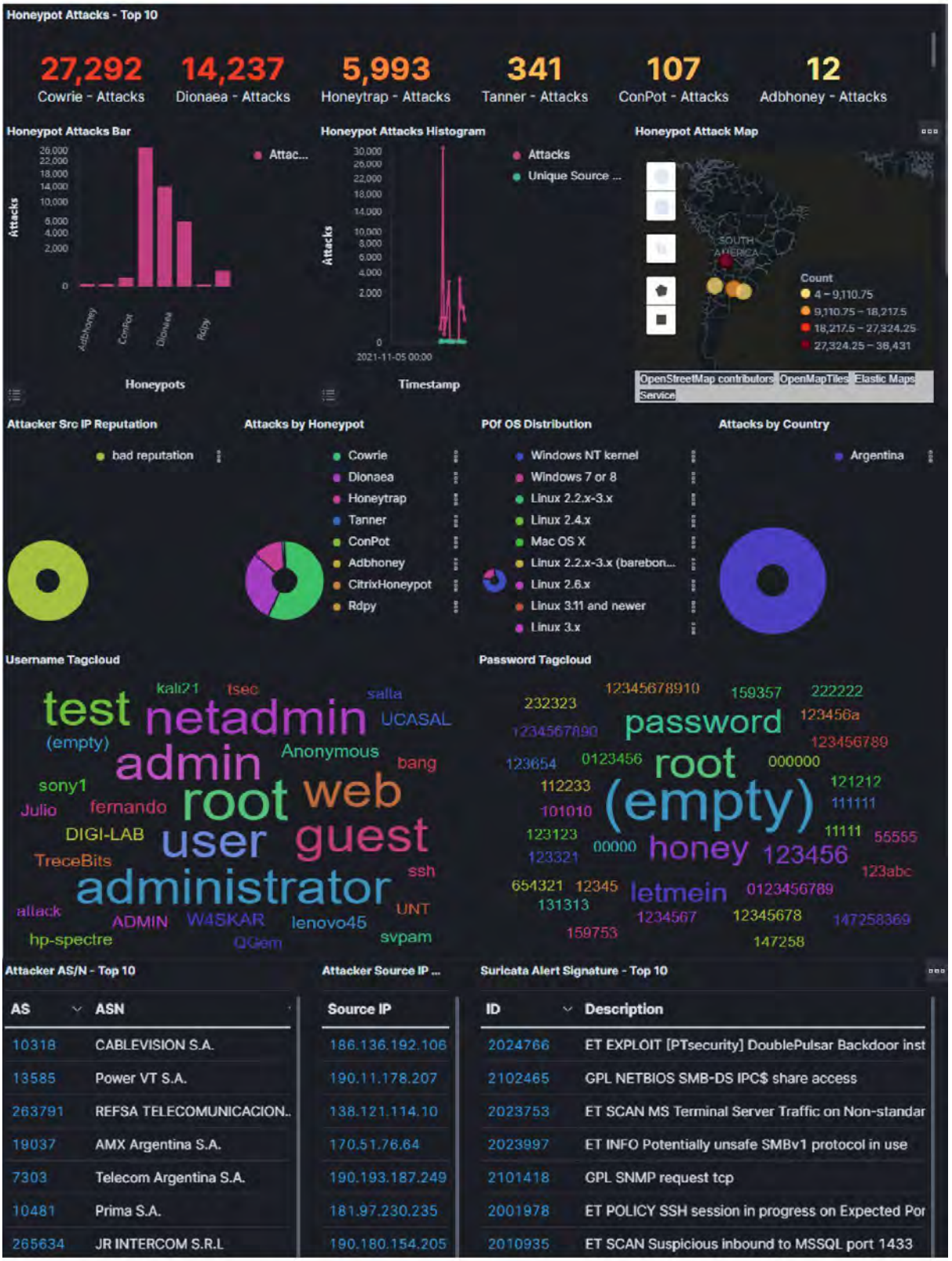
FIGURA 27 - ATAQUES RECOPILADOS CON T-POT A NIVEL MUNDIAL SEGUN CIERTOS PARÁMETROS



FUENTE Elaboración propia en base al sistema T-Pot.

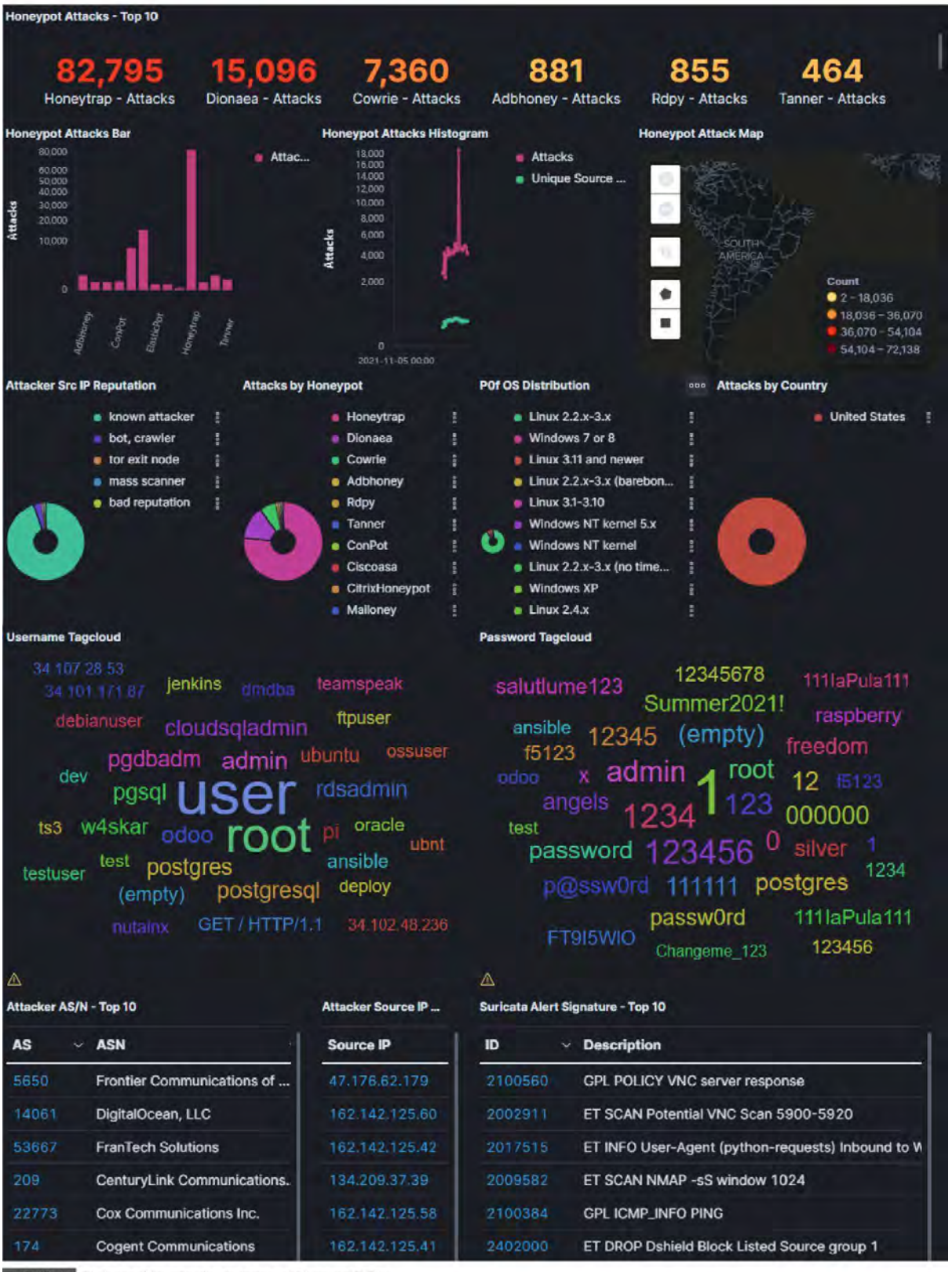
La característica más relevante de T-Pot es que podremos filtrar los ataques por su localización, para que se pueda observar en detalle el tipo de ataque empleado, el puerto más comprometido o los proveedores de Internet más usados. Para este proyecto compararemos además datos recopilados de Argentina, Estados Unidos y Vietnam, puesto que son los que lideran el top de ataques. Para el caso de Argentina, los datos fueron provistos por alumnos, compañeros y colegas informáticos, con accesos al sistema mediante el protocolo SSH.

FIGURA 28 - ATAQUES RECOPILADOS DE ARGENTINA



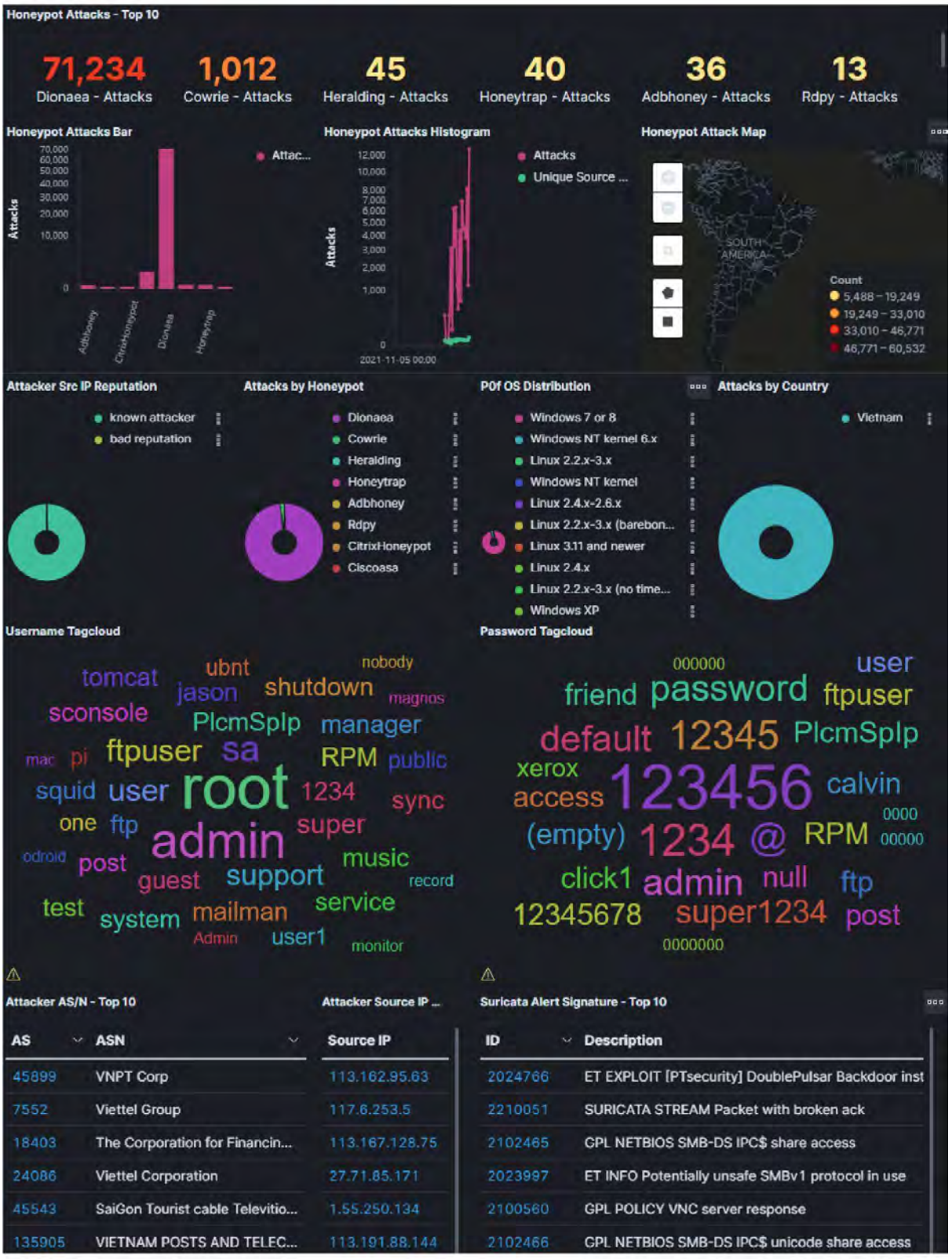
FUENTE Elaboración propia en base al sistema T-Pot.

FIGURA 29 - ATAQUES RECOPILADOS DE ESTADOS UNIDOS



FUENTE Elaboración propia en base al sistema T-Pot.

FIGURA 30 - ATAQUES RECOPILADOS DE VIETNAM



FUENTE Elaboración propia en base al sistema T-Pot.

6.4.2 ESCENARIO-02: ATAQUES CON DENEGACIÓN DE SERVICIOS (DoS)

En este caso, se llevará a cabo un ataque DoS, que no es más que una gran cantidad de solicitudes a una dirección IP específica, por lo que el servidor no podrá procesar todas las solicitudes recibidas, dando como resultado errores del sistema y la detención o reinicio del servicio, dejando además que el servidor esté inaccesible por un determinado tiempo. Para realizar este ataque, vamos a utilizar la herramientas *SlowHTTPTest* que ya viene instalada por defecto en Kali Linux.

1. Para trabajar con la herramienta, primero vamos a tener que asignarle varios parámetros, los cuales incluyen el número de peticiones que quiero (-c), los segundos en los cuales se envía las conexiones (-i), las conexiones enviadas por segundos (-r) y la dirección URL objetivo (-u). Ver *Figura 31*.

FIGURA 31 - EJECUCIÓN POR LINEA DE COMANDOS DE SLOWHTTPTEST

```
┌──(root💀kali)-[/home/w4skar]
└─# slowhttptest -c 2010 -H -i 10 -r 500 -l 600 -u https://34.125.199.232
```

FUENTE Elaboración propia.

2. Cuando ejecutamos el comando especificado, el ataque empezará a funcionar de manera automática. Si observamos la *Figura 32*, nos indica el que el servicio aun esta disponible (*service available*).

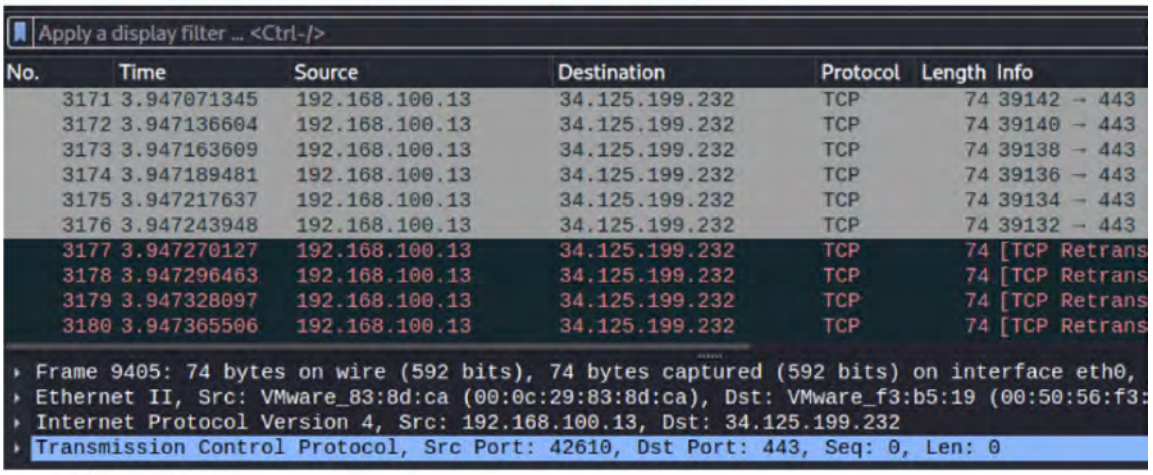
FIGURA 32 - FUNCIONAMIENTO DEL ATAQUE DOS CON SLOWHTTPTEST

```
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            2010
URL:                              https://34.125.199.232/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          68
interval between follow up data:  10 seconds
connections per seconds:          500
probe connection timeout:         5 seconds
test duration:                    600 seconds
using proxy:                      no proxy

Sat Dec  4 19:03:16 2021:
slow HTTP test status on 0th second:

initializing:        0
pending:             1
connected:           0
error:               0
closed:              0
service available:   YES
```

FUENTE Elaboración propia.

3. Todos estos ataques lo podemos ver fácilmente con *Wireshark,* de esta manera, podremos observar todo el tráfico que hay, en donde se ve continuamente el envío de paquetes TCP desde nuestro host virtual de pentesting (192.168.100.13) a la dirección IP objetivo del honeypot (34.125.199.232). En ocasiones, antes de realizar este tipo de ataque, siempre será conveniente ocultar nuestra dirección IP para evitar ser detectados, ya sea utilizando otras herramientas de Kali Linux o bien alguna VPN.

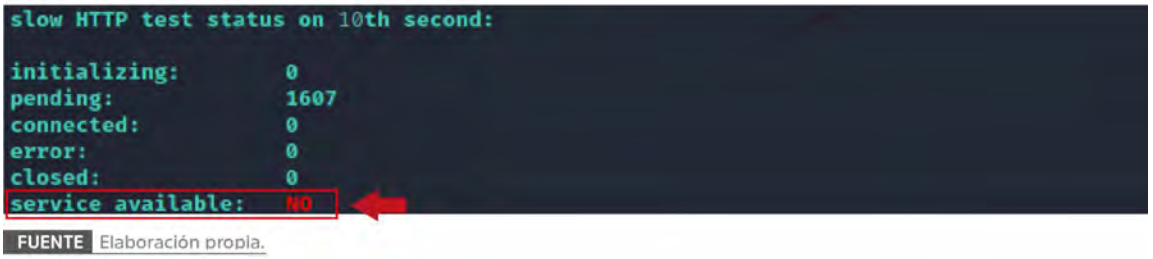
FIGURA 33 - CAPTURADOR DEL TRÁFICO DE RED PARA EL ATAQUE DOS



FUENTE Elaboración propia.

4. Después de un par de minutos, el servicio de *SlowHTTPTest* cambió a no disponible, lo cual significa que el servidor de esa dirección IP ahora empezará a caerse de a poco, esto lo iremos notando ya que cuando queremos navegar por nuestra interfaz del honeypot, esta empezara a andar muy lenta o no responderá con fluidez en las consultas que realicemos, hasta que directamente llegará un punto en el que no haya acceso. Para que el servidor esté realmente caído, la cantidad de peticiones debe ser grande, en este caso es poco, para cuestiones demostrativas, pero en promedio la conexiones enviadas debería ser arriba de 50.000.

FIGURA 34 - ESTADO DEL SERVICIO DE SLOWHTTPTEST



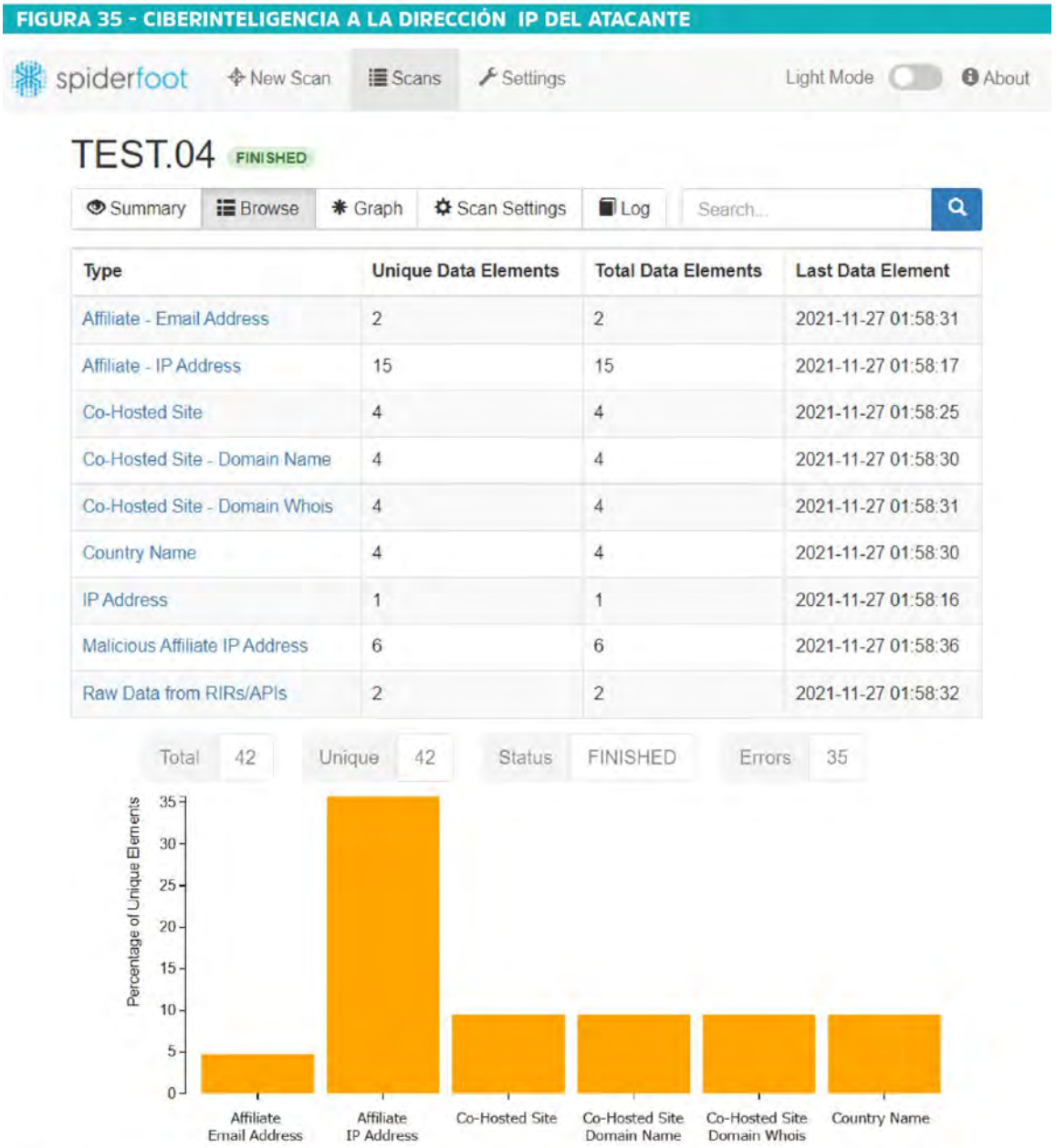
FUENTE Elaboración propia.

5. De esta manera habremos aplicado un ataque por denegación de servicio (DoS). Y para el caso en que ya no queramos seguir enviando peticiones al servidor, simplemente cancelamos la aplicación en Kali Linux con las teclas *Ctrl+C.*

6. Si nos vamos ahora al aplicativo de Kibana, podremos saber que la dirección IP de la cual realizamos el ataque quedó registrado en el sistema T-Pot. Por lo tanto, si deseamos tener más información, podemos hacer una ciberinteligencia de esa IP. Además, para complementar aún más, se puede usar el aplicativo Spiderfoot para tener así un reconocimiento más detallado sobre esa IP.

   Para hacer esto, simplemente especificamos el objetivo del cual queremos investigar, es decir, la dirección IP del atacante, que en este caso es 192.168.100.13. Luego, SpiderFoot recopilará todos los datos necesarios para poder comprender mejor toda la información relacionada.

FIGURA 35 - CIBERINTELIGENCIA A LA DIRECCIÓN IP DEL ATACANTE



Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Email Address	2	2	2021-11-27 01:58:31
Affiliate - IP Address	15	15	2021-11-27 01:58:17
Co-Hosted Site	4	4	2021-11-27 01:58:25
Co-Hosted Site - Domain Name	4	4	2021-11-27 01:58:30
Co-Hosted Site - Domain Whois	4	4	2021-11-27 01:58:31
Country Name	4	4	2021-11-27 01:58:30
IP Address	1	1	2021-11-27 01:58:16
Malicious Affiliate IP Address	6	6	2021-11-27 01:58:36
Raw Data from RIRs/APIs	2	2	2021-11-27 01:58:32

FUENTE Elaboración propia en base al sistema T-Pot.

6.4.3 ESCENARIO-03: ATAQUE CON METASPLOIT

En este escenario lo que vamos a realizar es un ataque de fuerza bruta a un servicio SSH. Para ello vamos a utilizar la herramienta de *Metasploit* para realizar la acción y posteriormente todo el ataque lo veremos reflejado en los dashboard de monitorización del honeypot T-Pot. Para conocer más sobre metasploit, modo de uso e instalación consultar el *Anexo 12*.

1. Como primer paso, abrimos una consola en Kali Linux y ejecutamos la herramienta metasploit. Verificamos previamente si la herramienta está instalada y luego tipeamos *msfconsole*.

FIGURA 36 - PANTALLA DE INICIO DE METASPLOIT

```
       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
```

FUENTE Elaboración propia.

2. Ahora realizamos un reconocimiento de puertos para poder determinar de forma efectiva si el host que estamos tratando de vulnerar tiene puertos abiertos. Para ello vamos a emplear la herramienta *nmap* con ciertos parámetros para luego obtener información detallada sobre sus puertos. Como ya sabemos la dirección IP de nuestra víctima, resultará un poco más fácil la implementación, es decir, es la dirección IP de nuestro servidor T-Pot (34.125.199.232).

FIGURA 37 - RECONOCIMIENTO DE PUERTOS CON NMAP

```
msf6 > nmap -v -sV 34.125.199.232
[*] exec: nmap -v -sV 34.125.199.232

Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-27 04:24 EST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 04:24
Scanning 34.125.199.232 [4 ports]
Completed Ping Scan at 04:24, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:24
Completed Parallel DNS resolution of 1 host. at 04:24, 0.07s elapsed
Initiating SYN Stealth Scan at 04:24
Scanning 232.199.125.34.bc.googleusercontent.com (34.125.199.232) [1000 ports]
Discovered open port 21/tcp on 34.125.199.232
Discovered open port 443/tcp on 34.125.199.232
Discovered open port 110/tcp on 34.125.199.232
Discovered open port 25/tcp on 34.125.199.232
Discovered open port 22/tcp on 34.125.199.232
Discovered open port 3389/tcp on 34.125.199.232
Discovered open port 23/tcp on 34.125.199.232
```

FUENTE Elaboración propia.

3. Luego que detectamos que el puerto 22 correspondiente al protocolo SSH está abierto, utilizaremos un módulo de metasploit para su acceso. Para llevar a cabo la enumeración de usuarios SSH en una máquina remota utilizaremos el módulo ssh que se encuentra en *auxiliary/scanner/ssh/ssh_login*.

   Con esto no solo podremos probar un conjunto de credenciales en un rango de direcciones IP, sino que también se podrá realizar intentos de inicio de sesión por fuerza bruta. Una vez dentro del módulo ssh_login, le pasaremos un archivo al módulo que contiene contraseñas. Luego cargaremos el módulo del escáner en metasploit y configuramos otros parámetros para que apunte a nuestra lista de credenciales. Por defecto en este ataque probaremos con usuario root, que normalmente es el se asigna por defecto a cualquier servidor. (ver *Figura 38*). El archivo que usa metasploit también podría tener nombres de usuario, pero aquí decidimos optar solo por las contraseñas.

FIGURA 38 - EJECUCIÓN DE MÓDULOS EN METASPLOIT

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/passwords.txt
PASS_FILE => /root/passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 34.125.199.232
RHOSTS => 34.125.199.232
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/ssh/ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name              Current Setting      Required  Description
  ----              ---------------      --------  -----------
  BLANK_PASSWORDS   false                no        Try blank passwords for all users
  BRUTEFORCE_SPEED  5                    yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false                no        Try each user/password couple stored in the current
                                                   database
  DB_ALL_PASS       false                no        Add all passwords in the current database to the lis
                                                   t
  DB_ALL_USERS      false                no        Add all users in the current database to the list
  PASSWORD                               no        A specific password to authenticate with
  PASS_FILE         /root/passwords.txt  no        File containing passwords, one per line
  RHOSTS            34.125.199.232       yes       The target host(s), see https://github.com/rapid7/me
                                                   tasploit-framework/wiki/Using-Metasploit
  RPORT             22                   yes       The target port
  STOP_ON_SUCCESS   false                yes       Stop guessing when a credential works for a host
  THREADS           1                    yes       The number of concurrent threads (max one per host)
  USERNAME          root                 no        A specific username to authenticate as
  USERPASS_FILE                          no        File containing users and passwords separated by spa
                                                   ce, one pair per line
  USER_AS_PASS      false                no        Try the username as the password for all users
  USER_FILE                              no        File containing usernames, one per line
  VERBOSE           false                yes       Whether to print output for all attempts
```

FUENTE Elaboración propia.

4. Luego ejecutamos con el comando *run* para que empiece a trabajar. De esta forma irá probando varias contraseñas por fuerza bruta hasta dar con el indicado. Una vez que se encuentra el password indicado salimos del metasploit y podremos acceder por SSH.

FIGURA 39 - ACCESO SSH AL SERVIDOR T-POT

FUENTE Elaboración propia.

5. Finalmente, podremos realizar todas las operaciones en modo root al tener acceso SSH. Lo que resta es verificar este acceso en nuestro honeypot T-Pot. Para ello nos dirigimos al aplicativo Kibana y verificamos la dirección IP del atacante, en este caso 192.168.100.13. En las estadísticas, si buscamos por el nombre usuario, podremos ver todos las contraseñas con las que se accedió al servidor, el proveedor de Internet utilizado, cantidad de ataques recibidos, puerto utilizado, entre otros. Además, en la sección de discover, todos los comandos que realizó el atacante figurará registrado ahí, por lo que sí accediendo al servidor creamos una carpeta, esta acción también se verá reflejada en el discover del T-Pot. Por lo tanto este ataque se realizó correctamente.

FIGURA 40 - VERIFICACIÓN DEL ATAQUE CON METASPLOIT EN EL SERVIDOR T-POT

FUENTE Elaboración propia.

6.4.4 ANÁLISIS DE RESULTADOS

En esta sección, vamos a presentar los análisis de los diferentes escenarios de pruebas que realizamos anteriormente. Las herramientas de sistema T-Pot que nos ayudaron a interpretar los datos obtenidos y determinar estas conclusiones fueron principalmente Kibana, SecurityMeter y Spiderfoot, puesto que nos ofrecieron una gran cantidad de información sobre los atacantes.

- ***Escenario-01***

  Como se pudo observar, los ataques que recibió el honeypot de forma general fueron muy grandes en tan solo 40 horas continuas y sin dar ningún tipo de error durante la recopilación. Luego, al filtrar los datos y realizar una comparativa específica entre los ataques procedentes de Argentina, Estados Unidos y Vietnam, se pudo comprobar que por lo general la mayoría de los ataques realizados se centran en el puerto 22 (protocolo SSH) y el puerto 8088 (puerto TCP/UDP), ya que los mismos, son servicios conocidos y con vulnerabilidades conocidas. Por otro lado, el origen con mayor demanda de ataques provienen mayormente de Rusia, Estados Unidos y China, sabiendo que estos ataques se van originando aleatoriamente, puesto que dependen de la situación geográfica del servidor.

  La inmensa mayoría de ataques malware que fuimos recibiendo en esta prueba fueron de Cowrie y Honeytrap, destinados a simular servidores SSH y servicios TCP/ UDP respectivamente. También se pudo observar, que los sistemas operativos desde los cuales se recibieron los ataques son en su mayoría Linux seguidos después por Windows NT y Windows 7/8. El uso de estos sistemas se debe a que gran parte de los mismos fueron infectados o añadidos a una red de botnets. En cuanto a las nombre de usuarios y contraseñas utilizadas para el logueo al sistema, se ve que la mayoría utiliza contraseñas numéricos y en otros, se observa ciertos patrones con expresiones regulares, además de que atacantes prueban constantemente nombres de usuarios típicos, tales como root, admin, mysql, puesto que estos en algunas ocasiones están por defecto en los servidores.

- ***Escenario-02***

  Uno de los activos más importantes para muchas empresas, en cualquier rubro, es su página web, por eso, es que muchos ciberdelincuentes ven aquí una buena oportunidad de vulnerar el sistema. En las pruebas realizadas, se optó por una ataque DoS (denegación de servicio), pero sin causar graves consecuencias en el sistema objetivo.

  Si bien el ataque DoS es algo que puede ocurrir con frecuencia, cuando se lleva a cabo logran que el sistema quede inactivo pero sólo en el honeypot implementado, puesto que el mismo es

solo un señuelo atractivo para los ciberdelincuentes, dándonos la oportunidad a nosotros como empresa de tomar medidas que eviten esa situación.

En los paneles de monitorización de T-Pot, los ataques que se registraron se contemplan como uno, ya que al enviar tantas peticiones TCP y todas desde la misma IP, el sistema detecta una única IP pero con múltiples accesos. Además, en este tipo de ataque, el único encargado de detectar estas anomalías es el honeytrap, debido a su versatilidad de observar los ataques contra los servicios TCP y UDP. Los atacantes siempre serán engañados y enviarán todas sus respuestas a un proceso de servidor honeytrap y luego todo estos serán recopilados por T-Pot.

- ***Escenario-03***

  Durante las pruebas realizadas se pudo observar que al utilizar un ataque de fuerza bruta mediante SSH empleando metasploit, se pudo vulnerar fácilmente el servidor y tener el control del honeypot. Por tal motivo, todas las organizaciones deben estar alertas, puesto qué herramientas de este tipo hay muchas y cada vez se van perfeccionando.

  Si bien el atacante pudo acceder al servidor mediante SSH, a su vez, el honeypot también nos da una ventaja de tener un gran abanico de recursos y herramientas para recopilar todo tipo de información sobre él. Es decir, si accedemos al aplicativo web de Kibana, tendremos la posibilidad de hacer ciberinteligencia sobre ese ataque, sabiendo de antemano lugar de procedencia (aunque no siempre es certero, puesto que puede ser una red de botnets), el tipo de ataque realizado, el cual es registrado por el honeypot suricata, conocer cuántas veces tuvo acceso al sistema, con que sistema operativo fue realizado el ataque, las credenciales de acceso que utilizó, entre otros. Todos estos datos lo pudimos visualizar fácilmente en los dashboard del T-Pot, permitiéndonos de esta manera saber que acciones tomar a futuro para poder mitigarlas.

  Por otro lado, al detectar la IP del atacante provisto por T-Pot, si quisiéramos profundizar en detalle con más información, se puede realizar una ciberinteligencia con el aplicativo Spiderfoot, ya que esta herramienta al pertenecer a OSINT nos permitió obtener datos recopilados de Internet, como así también de otros medios. Pero en forma general, gracias a T-Pot pudimos saber la reputación detallada de esa dirección IP, además de saber en qué servidores estuvo comprometida, el tiempo de actividad, lugares por los que pasó, entre otros.
  Des esta manera, tuvimos acceso a una gran cantidad de información, lo que nos da pie para concluir que si no hubiéramos implementado este honeypot, la red de nuestra organización o de cualquier otra hubiese sufrido un ataque realmente comprometedor, por eso, la idea de contar con una seguridad proactiva es muy importante.

6.4.5 RECOMENDACIONES GENERALES DE SEGURIDAD

En base a toda la información que nos entrega constantemente el honeypot T-Pot, podemos saber de antemano sobre los diferentes tipos de ataques que podríamos llegar a sufrir si nuestra red es vulnerada, por tal motivo, para disminuir estos intentos de ataques será necesario tomar ciertas medidas. A continuación detallamos algunos recomendaciones formales a tener en cuenta:

- Los profesionales y expertos en ciberseguridad deben utilizar un lenguaje fácil de entender para establecer una comunicación eficaz en toda la organización.
- Los altos directivos y los empleados de cualquier organización deben estar siempre al tanto de los problemas de ciberseguridad que pueden llegar a ocurrir, de forma tal, que se puedan prevenir futuros robos o divulgación de información.
- Utilizar herramientas proactivas de seguridad como lo son los honeypots o cualquier otra, toman un valor indispensable en la actualidad, puesto que si bien no mitigan la amenaza por completo, ayudarán a prevenir futuros patrones de ataques.
- Se deben de crear políticas de seguridad y planes de contingencias efectivas, que contemplen en lo posible los marcos más indispensables de la norma 27001, empleando además buenas prácticas de seguridad.
- Todos los equipos y dispositivos tecnológicos que se utilizan en la empresa, tanto en hardware como en software deben ser actualizados con regularidad, ya que todos estamos expuestos ante posibles ataques informáticos.

Por lo tanto, en base a los resultados de las pruebas obtenidas en este proyecto, hay que resaltar que ***un honeypot en ningún momento persigue la finalidad de ser una solución de seguridad***, sino que es un complemento a los sistemas de seguridad existentes. Es decir, se encarga de proporcionar información sobre los atacantes que intentan comprometerlo, antes de que comprometan otros sistemas de la red en la que se encuentra. Por ello, en cada una de las pruebas realizadas como lo son los ataques con denegación de servicios (DoS), metasploit o cualquier otro tipo de ataque, estos serán detectados en la plataforma del honeypot T-Pot, lo cual nos permitirá obtener gran cantidad de información sobre los atacantes, tomar las medidas de seguridad necesarias y con ello utilizar otras herramientas de seguridad como ser SIEM (Security Information and Event Management) el cual nos proporcionará una respuesta rápida y precisa para solucionar cualquier amenaza sobre los sistemas informáticos. Las recomendaciones aquí detalladas son algunas de las cuestiones que se debe de tener presente para así evitar futuros ataques y tener protegida la seguridad de cualquier empresa.

CAPÍTULO 7 - CONCLUSIONES Y TRABAJOS FUTUROS

7.1 CONCLUSIONES

Como se pudo observar, a lo largo del desarrollo de todo este proyecto, se pudo evidenciar los cambios que ha provocado Internet en nuestras vidas. Por tal motivo, debido a este constante avance tecnológico, las actividades maliciosas (malware, bots, spoofing, ingeniería social, sniffing etc.) también fueron evolucionando, por esta razón es imprescindible cuidar el valor de la información que publicamos en la red, y adoptar un nuevo tipo de seguridad proactiva para prevenir de esta forma cualquier tipo de ataque informático. Por ende, para solucionar esta problemática es que se propuso emplear honeypots.

En líneas generales, se logró cumplir con los objetivos planteados en este proyecto. Es decir, que tras varias investigaciones, aportes, pruebas, errores y análisis comparativos realizados a los diferentes tipos de distribuciones de honeypots, se logró presentar una solución concreta a la problemática planteada, implementado así el honeypot más óptimo, que en este caso fue T-Pot. Esta solución fue implementada en una infraestructura totalmente virtual (lo que no quita que pueda ser implementada físicamente) diseñada con el propósito de experimentar con ella, realizando además diferentes tipos de ataques para comprometerla con el fin de ver su comportamiento y obtener datos valiosos para que posteriormente se pueden realizar análisis y así tener una mejor toma de decisiones en futuros ataques cibernéticos.

En base a esto, hemos podido comprender fácilmente el funcionamiento de un honeypot, ayudándonos a mejorar la seguridad de cualquier organización o incluso nuestra propia seguridad. También se ha visto como la mayoría de los ciberatacantes, cuando deciden comprometer una sistema, una red o un equipo concreto, no se valen de ataques complejos ni avanzados, sino que principalmente intentan buscar el eslabón más débil, es decir, las personas.

En un principio, también fue necesario explicar en detalle ciertos conceptos sobre seguridad informática, para que luego podamos adentrarnos a fondo a todo el mundo de honeypots. La razón principal se debe al hecho de que cuando se implemente, configure y mantenga el honeypot no se presenten problemas. Por lo tanto, si bien la instalación y configuración del honeypot seleccionado T-Pot fue sencilla, para otros usuarios esto puede resultar complejo y tedioso, puesto que no se tuvo en claro los objetivos, conceptos y estructura de red.

Por otro lado, la implementación del honeypot T-Pot que se montó de manera virtual se pudo lograr con éxito gracias al hipervisor VMware que empleamos. Además durante el desarrollo, aplicarlo nos ayudó a incorporar un conocimiento más profundo y detallista sobre el funcionamiento de las diferentes máquinas virtuales que analizamos, comprendiendo así su instalación, configuración y mantenimiento. Si bien la red que montamos fue acotada, su manipulación hizo que nos familiarizamos aún más con términos, acrónimos y herramientas sobre conectividad de redes.

En cuanto a las pruebas y análisis realizados, llegamos a la conclusión que el honeypot T-Pot funciona de manera adecuada, logrando detectar e identificar cualquier intruso en la red propuesta. Si bien el honeypot en ningún momento persigue la finalidad de ser una solución de seguridad, logra ser un complemento realmente muy útil a los sistemas de seguridad existentes. Además, con todo este tipo de análisis se pudo observar en detalle los diferentes informes que emiten los dashboard de monitorización del T-Pot, mostrando así diferentes tipos de alertas, direcciones IPs involucradas en los ataques, puertos vulnerados, honeypot desplegado, etc., con lo cual se cumplen los objetivos que indicamos en este proyecto.

Con lo anterior expuesto podemos asegurar que, establecer una seguridad total como tal, no existe, puesto que los ciberdelincuentes crecen al mismo ritmo que Internet o de las nuevas tecnologías emergentes. Por tal motivo, lo que sí podemos garantizar es dar una protección gradual de nuestros activos principales, ya sea que nos anticipemos mediante diferentes controles de seguridad o bien utilizando herramientas proactivas de seguridad (como los honeypots), asegurando de esa forma que toda nuestra información pueda estar segura. Por lo tanto, vuelvo a mencionar, que es sumamente importante brindar a las personas y a las organizaciones una mayor comunicación y concientización sobre temas de protección de datos y seguridad de la información, puesto que en la actualidad juegan un rol importante, quedando en cada uno de nosotros tomar las medidas de seguridad más pertinentes, además del gran aporte que supone al mundo de la ciberseguridad.

7.2 FUTURAS LÍNEAS DE INVESTIGACIÓN

Como líneas futuras para el presente proyecto y en base al diseño e implementación de honeypots que realizamos como herramienta proactiva de seguridad informática, podemos mencionar que:

- Resultaría muy interesante realizar un estudio más profundo y detallado sobre los otros tipos de honeypots con los que cuenta T-Pot, puesto que de esta forma se podrían recabar más datos para analizar, ya que cada honeypot que se despliega del T-Pot tienen características y funcionalidades diferentes según los objetivos que se persiga.

- Para la infraestructura diseñada, quedaría pendiente hacer una implementación con otros tipos de honeypots o bien implementar otras herramientas de seguridad proactivas en los equipos virtuales de soporte, puesto que estos equipos no se utilizaron en el proyecto. Por ello, además de tener el T-Pot implementado, contar con otros honeypots (distintos a los que emplea T-Pot) nos daría más información para recabar y así tener una mejor toma de decisiones.

- Si bien los honeypots han ayudado a los profesionales de ciberseguridad a recabar información realmente valiosa en cuanto a las actividades maliciosas se refiere, también han generado problema cuando se trata de analizar grandes cantidades de datos, siendo una tarea muy tediosa y de mucho tiempo. Por lo tanto, para ayudar y facilitar este proceso sería necesario implementar en una futura investigación el *Machine Learning* para poder analizar los datos recopilados por los honeypots. Esto lo consideramos clave, debido a que las botnets últimamente están empezando a implementar IA (inteligencia artificial) en muchos de sus ataques cibernéticos.

- Crear e implementar honeypots que estén orientados exclusivamente a cualquier dispositivo móvil, puesto que en la actualidad el uso de estos dispositivos inteligentes representa aproximadamente un 48% de la población a nivel mundial. Por lo tanto, cubrir este tipo de seguridad es realmente primordial, y más en un mundo tan conectado.

- Quedaría por realizar también, un manual de políticas de seguridad basado en la norma ISO 27001 con las mejores prácticas y en donde se detallen de forma clara y precisa todos los controles de seguridad acorde a las necesidades actuales de la empresa, además de proveer una concienciación adecuada a todos los directivos y personal de la empresa, como así también el monitoreo continuo, asegurando de esa forma una seguridad activa y constante.

- El proyecto hasta aquí realizado también abre un conjunto de ideas y proyecciones sobre las cuales se puede continuar la investigación. Algunas de ellas no han sido abordadas por estar fuera de los objetivos planteados, pero sabiendo la creciente expansión de la ciberseguridad en estos tiempos, serán muy necesarios cubrir a futuro.

CAPÍTULO 8 - REFERENCIAS BIBLIOGRÁFICAS

[1] Zaryn Dentzel. (2013). *El impacto de Internet en la vida diaria*. BBVA. Recuperado el 02 de abril de 2021 de https://www.bbvaopenmind.com/articulos/el-impacto-de-Internet-en-la-vida-diaria/

[2] Leticia González. (27 de mayo de 2015). La importancia de la ciberseguridad. Metrópolis. [Blog]. Recuperado el 02 de abril de 2021 de https://metropoliscom.com/la-importancia-de-la-ciberseguridad/

[3] José Fernández. (2013). *Virtual honeynets*. (Proyecto de Grado). Universidad de Almería (UAL), Almería, España. Recuperado el 02 de abril de 2021 de http://repositorio.ual.es/bitstream/handle/10835/2643/Trabajo.pdf?sequence=1&isAllowed=y

[4] Ciberseguridad. (2016). *Seguridad reactiva frente a proactiva: ¿cuál es mejor?*. Recuperado el 02 de abril de 2021 de https://ciberseguridad.com/guias/seguridad-reactiva-proactiva/

[5] Julio C. Matus Chan. (2017). *Análisis e implementación de una solución honeypot para un entorno experimental*. (Trabajo de Tesis). Universidad de Quintana Roo, Chetumal, Quintana Roo, México. Recuperado el 07 de abril de 2021 de http://risisbi.uqroo.mx/bitstream/handle/20.500.12249/1966/QA76.9.A25.2017-1966.pdf?sequence=1

[6] Kelly G. Bermúdez y Rafael B. Sanchez. (2015). *Análisis en Seguridad Informática y Seguridad de la información basado en la norma ISO/IEC 27001*. (Anteproyecto). Universidad Politécnica Salesiana Sede Guayaquil, Guayaquil, Ecuador. Recuperado el 07 de abril de 2021 de https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

[7] Tecon. (2018). *La Seguridad de la Información*. Tecon: Soluciones informáticas. [Blog]. Recuperado el 07 de abril de 2021 de https://www.tecon.es/la-seguridad-de-la-informacion/

[8] Oscar Schmitz. (27 de enero de 2014). *Principios básicos de seguridad de la información*. Oscar Schmitz. [Blog]. Recuperado el 07 de abril de 2021 de https://www.oscarschmitz.com/2014/01/principios-basicos-de-seguridad-de-la.html

[9] P. Aguilera. (2011). *Redes seguras (Seguridad informática)*. Madrid, España: Editex. Recuperado el 07 de abril de 2021.

[10] Martha I. Romero, Grace L. Figueroa, Denisse S. Vera, José E. Álava, Galo R. Parrales, Christian J. Álava, Angel L. Murillo y Miriam A. Castillo. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Primera edición. Recuperado el 09 de abril de 2021 de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[11] UNIR Revista. (04 de febrero de 2021). *No repudio, ¿qué significa en seguridad informática?.* UNIR, la Universidad en Internet. [Blog]. Recuperado el 09 de abril de 2021 de https://www.unir.net/ingenieria/revista/no-repudio-seguridad-informatica/

[12] WeLiveSecurity. (2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia.* Recuperado el 09 de abril de 2021 de https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia

[13] NIC Argentina. (2018). *¿Qué es Ciberseguridad?.* Recuperado el 09 de abril de 2021 de https://nic.ar/es/enterate/novedades/que-es-ciberseguridad

[14] CIC Team. (2016). *Seguridad de la Información y Ciberseguridad ¿es lo mismo?*. CIC Consulting Informático. [Blog]. Recuperado el 09 de abril de 2021 de https://www.cic.es/seguridad-de-la-informacion-y-ciberseguridad-es-lo-mismo/

[15] Agustin López y Javier Ruiz. (2005). *Sistema de Gestión de la Seguridad de la Información*. Recuperado el 09 de abril de 2021 de https://www.iso27000.es/index.html

[16] ISOWin. (2015). *Los Activos de Información en la norma ISO 27001*. ISOWin. [Blog]. Recuperado el 13 de abril de 2021 de https://isowin.org/blog/activos-ISO-27001/

[17] Rafael Castillo, Alessio Di Mare, Victor Díaz y Horacio Díez. (2004). *Concientización en seguridad de la información*. Recuperado el 13 de abril de 2021 de http://www.criptored.upm.es/guiateoria/gt_m142r.htm

[18] Reina A. Camacho. (2013). *Diseño e implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) para la protección de los activos informáticos de la Universidad Central de Venezuela*. (Proyecto Especial de Grado). Universidad Central de Venezuela , Caracas, Venezuela. Recuperado el 13 de abril de 2021 de https://mendillo.info/seguridad/tesis/Camacho.pdf

[19] Ministerios de Administraciones Públicas. (2006). MAGERIT Versión 2. *Methodology for Information Systems Risk Analysis and Management*. Recuperado el 16 de abril de 2021 de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[20] Agustín Spinelli Riso. (2018). *Ciberseguridad en PyMES de la industria de retail farmacéutico: estudio de los casos Zona Vital y FarmaBelén*. (Trabajo de Graduación). Universidad de San Andrés, Buenos Aires, Argentina. Recuperado el 16 de abril de 2021 de https://repositorio.udesa.edu.ar/jspui/bitstream/10908/16720/1/%5BP%5D%5BW%5D%20T.%20G.%20A.%20y%20C.%20Spinelli%20Riso,%20Agust%C3%ADn.pdf

[21] Cristian Borghello. (23 de diciembre de 2020). *¿Qué son los controles de CIS*?. Segu-Info. [Blog]. Recuperado el 16 de abril de 2021 de https://blog.segu-info.com.ar/2020/12/que-son-los-controles-de-cis.html?m=0

[22] Ruben Ramiro. (18 de julio de 2018). *Guía práctica para implementar los controles críticos de seguridad*. Ciberseguridad.Blog. [Blog]. Recuperado el 16 de abril de 2021 de https://ciberseguridad.blog/guia-practica-para-implementar-los-controles-criticos-de-seguridad/

[23] Giancarlo Gómez Morales. (2019). *¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?*. Recuperado el 16 de abril de 2021 de https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

[24] Mónica M. Jiménez. (22 de enero de 2021). *Conoce el Marco de Ciberseguridad del NIST.* Pirani. [Blog]. Recuperado el 21 de abril de 2021 de https://www.piranirisk.com/es/blog/marco-ciberseguridad-nist-que-es

[25] Dejan Kosutic. (2014). *The basic logic of ISO 27001: How does information security work.* 27001 Academy. Recuperado el 21 de abril de 2021 de http://www.iso27001standard.com/blog/2014/05/05/the-basic-logic-of-iso-27001-how-does-information-security-work/#

[26] Cristian Borghello. (2001). *Seguridad Informática: Implicancias e implementación.* (Tesis Licenciatura en Sistemas). Universidad Tecnológica Nacional, Buenos Aires, Argentina. Recuperado el 21 de abril de 2021 de https://www.segu-info.com.ar/tesis/tesis-borghello-full.zip

[27] Jorge W. Trapp. (2009). *ICIHONEY: Diseño e Implementación de una Red Trampa en el Instituto de Informática de la Universidad Austral de Chile*. (Tesis). Universidad Austral de Chile, Valdivia, Chile. Recuperado el 21 de abril de 2021 de http://cybertesis.uach.cl/tesis/uach/2009/bmfcit774i/doc/bmfcit774i.pdf

[28] María G. Hernández. (2006). *Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial*. (Tesis de Grado). Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador. Recuperado el 21 de abril de 2021 de https://core.ac.uk/download/pdf/12401004.pdf

[29] Rodrigo Mariano Díaz. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad*. Boletín FAL No. 382. Recuperado el 24 de abril de 2021 de https://repositorio.cepal.org/bitstream/handle/11362/46275/1/S2000679_es.pdf

[30] Legálitas. (2017). *La ciberseguridad y su importancia actualmente*. Recuperado el 24 de abril de 2021 de https://www.legalitas.com/actualidad/La-ciberseguridad-y-su-importancia-actualmente

[31] Consultor DataDec. (27 de febrero de 2019). *La ciberseguridad también es cosa de los empleados*. DataDec. [Blog]. Recuperado el 24 de abril de 2021 de https://www.datadec.es/blog/ciberseguridad-tambien-es-cosa-de-los-empleados

[32] KeepCoding Team. (29 de enero de 2020). *Por qué es importante la Ciberseguridad para empresas*. KeepCoding. [Blog]. Recuperado el 24 de abril de 2021 de https://keepcoding.io/blog/importancia-ciberseguridad-para-empresas/

[33] Inter-American Development Bank. (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020.* Recuperado el 26 de abril de 2021 de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[34] Miguel Ángel Mendoza. (18 de mayo de 2015). *¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?.* WeLiveSecurity. [Blog]. Recuperado el 26 de abril de 2021 de https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

[35] Andrés Cargill Medel. (06 de agosto de 2018). *Entendiendo los CSIRT: responsabilidades, roles y diferencias respecto a un SOC y CERT.* LinkedIn. [Blog]. Recuperado el 26 de abril de 2021 de https://www.linkedin.com/pulse/entendiendo-los-csirt-responsabilidades-roles-y-respecto-cargill-1f/?originalSubdomain=es

[36] Cristian Borghello. *Legislación y Delitos Informáticos - La Información y el Delito.* Recuperado el 26 de abril de 2021 de https://www.segu-info.com.ar/legislacion/?id=legislacion

[37] Marcos Polanco. (21 de abril de 2016). *La ciberinteligencia como habilitador de la ciberseguridad*. Magazcitum. [Blog]. Recuperado el 26 de abril de 2021 de https://www.magazcitum.com.mx/?p=3205

[38] Departamento de Comunicaciones INISEG. (20 de diciembre de 2018). *Ciberinteligencia: la inteligencia en el ciberespacio.* INISEG. [Blog]. Recuperado el 26 de abril de 2021 de https://www.iniseg.es/blog/ciberseguridad/ciberinteligencia/

[39] US Naval War College. *Intelligence Studies: Types of Intelligence Collection*. Recuperado el 28 de abril de 2021 de https://usnwc.libguides.com/c.php?g=494120&p=3381426

[40] Daniel Caffaratti y Lorena Holc. (2017). *Forensia Informática aplicada a PC con sistema operativo Windows y Linux*. (Proyecto de Tesis de Grado). Instituto Universitario Aeronáutico, Córdoba, Argentina. Recuperado el 26 de abril de 2021 de https://rdu.iua.edu.ar/bitstream/123456789/844/1/Proyecto%20de%20Grado%20-%20Caffaratti%20-%20Holc.pdf

[41] Andres Rodríguez. (24 de octubre de 2019). *¿Qué es un ataque Man in the Middle?*. GoDaddy. [Blog]. Recuperado el 26 de abril de 2021 de https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/

[42] OSI Team. (21 de agosto de 2018). *¿Qué son los ataques DoS y DDoS?*. OSI Oficina de Seguridad del Internauta. [Blog]. Recuperado el 28 de abril de 2021 de https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

[43] Graciela Marker. (2017). *¿Qué es bot? ¿Qué es una red de bots?.* Tecnología fácil. [Blog]. Recuperado el 28 de abril de 2021 de https://tecnologia-facil.com/que-es/que-es-bot-que-es-una-red-de-bots/

[44] Byron V. Guamán. (2015). *Anatomía de un ataque informático*. (Anteproyecto). Universidad de Azuay, Cuenca, Ecuador. Recuperado el 28 de abril de 2021 de http://dspace.uazuay.edu.ec/handle/datos/5046#:~:text=Para%20lograr%20mitigar%20riegos%20de,autorizaci%C3%B3n%20y%20esquematizando%20sus%20pasos.

[45] KPMG México. (2018). *Siete medidas básicas para proteger a su empresa.* Recuperado el 28 de abril de 2021 de https://assets.kpmg/content/dam/kpmg/mx/pdf/2018/04/ciberseguridad-servicios.pdf

[46] Nicolas Raggi. (26 de marzo de 2021). *Defensa en profundidad: cómo implementar esta estrategia de ciberseguridad.* WeLiveSecurity. [Blog]. Recuperado el 28 de abril de 2021 de https://www.welivesecurity.com/la-es/2021/03/26/defensa-profundidad-que-es-como-implementar-estrategia-ciberseguridad/

[47] EdwinRSV. (2011). *Modelo de seguridad en profundidad.* GuardNET. [Blog]. Recuperado el 30 de abril de 2021 de https://guardnet.wordpress.com/2011/06/08/modelo-de-seguridad-en-profundidad/

[48] Wendy Cruz. (8 de junio de 2011). *Estrategia de defensa en profundidad.* Seguridad en redes. [Blog]. Recuperado el 30 de abril de 2021 de https://seguridadprofundadenredes.blogspot.com/2011/06/estrategia-de-defensa-en-profundidad.html

[49] Pablo F. Iglesias. (2015). *Qué diferencia a un antivirus de un firewall y de un IDS.* PabloYglesias. [Blog]. Recuperado el 30 de abril de 2021 de https://www.pabloyglesias.com/antivirus-firewall-e-ids/#:~:text=De%20ah%C3%AD%20que%20sea%20habitual,fugas%20de%20informaci%C3%B3n%20desde%20dentro.

[50] Logitek. (8 de julio de 2020). *IDS vs IPS ¿Cuál es la diferencia?.* Logitek Ciberseguridad Industrial. [Blog]. Recuperado el 30 de abril de 2021 de https://www.ciberseguridadlogitek.com/ids-vs-ips-cual-es-la-diferencia/

[51] Daniel Cunha Barbosa. (19 de mayo de 2020). *Para qué sirve una VPN.* WeLiveSecurity. [Blog]. Recuperado el 30 de abril de 2021 de https://www.welivesecurity.com/la-es/2020/05/19/para-que-sirve-vpn/

[52] Clifford Stoll. (2005). *The Cuckoo's Egg*. (1ra Ed.). Estados Unidos: Pocket Books. Recuperado el 03 de mayo de 2021.

[53] Lance Spitzner. (1999). *The Honeynet Project.* Recuperado el 03 de mayo de 2021 de https://www.honeynet.org

[54] Navneet Kambow, Lavleen K. Passi. (2014). Honeypots: The Need of Network Security. *International Journal of Computer Science and Information Technologies, 5* (5), 6098-6101. Recuperado el 03 de mayo de 2021 de https://ijcsit.com/docs/Volume%205/vol5issue05/ijcsit2014050521.pdf

[55] Kevin David Martínez Contreras. (2018). *Honeypot, hacia un protocolo de seguridad más eficiente y competitivo*. (Anteproyecto). Universidad Nacional Abierta y a Distancia (UNAD), Bogotá, Colombia. Recuperado el 03 de mayo de 2021 de https://repository.unad.edu.co/bitstream/handle/10596/17369/1103111366.pdf

[56] Lance Spitzner. (2002). *Honeypots: Tracking Hackers*. Estados Unidos: Addison-Wesley Professional. Recuperado el 04 de mayo de 2021.

[57] Fernando Cócaro, Mauricio García y Maria Rouiller. (2008). *Proyecto Honeypots*. (Grupo de Seguridad Informática, Facultad de Ingeniería, Universidad de la República). Recuperado el 04 de mayo de 2021 de https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/3114/1/tg-cocaro.pdf

[58] Lance Spitzner. (2002). Know *your enemy: Defining Virtual Honeynets*. (2da Ed.). Estados Unidos: Addison-Wesley Professional. Recuperado el 05 de mayo de 2021 de http://www.sane.nl/events/sane2002/papers/honeynet.PDF

[59] Miguel Lara y Diana Lopez. (2013). *Honeypot virtualizado para ambientes académicos y de investigación*. (Proyecto de Grado). Universidad Piloto de Colombia, Bogotá, Colombia. Recuperado el 08 de mayo de 2021 de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2584/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

[60] Miguel Sanchez. (2015). *Implementación de una honeynet para la Ciberdefensa de Infraestructuras Críticas*. (Proyecto Final de Grado). Universidad de la Defensa Nacional, Córdoba, Argentina. Recuperado el 08 de mayo de 2021 de https://rdu.iua.edu.ar/bitstream/123456789/1143/1/Trabajo%20Final%20de%20Grado%20-%20Miguel%20E%20Sanchez%20-%20(Versi%C3%B3n%20Final).pdf

[61] Gabriel Verdejo. (2003). *Seguridad en redes IP*. (Doctorado en Informática). Universidad Autónoma de Barcelona, Barcelona, España. Recuperado el 11 de mayo de 2021 de https://issuu.com/2dmadafakas/docs/seguridadip

[62] Lance Spitzner. (10 de octubre de 2001). *The Value of Honeypots, Part One: Definitions and Values of Honeypots*. Recuperado el 11 de mayo de 2021 de https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=a8da0d16-65ae-405a-abeb-325af33a393d&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[63] Joan. (14 de noviembre de 2014). *Modern HoneyPot Network: dejando un tarro de miel en Internet.* Joan es Marti. [Blog]. Recuperado el 11 de mayo de 2021 de https://joanesmarti.com/modern-honeypot-network-dejando-un-tarro-de-miel-en-Internet/

[64] Alan Warburton. (30 de julio de 2020). *Qué es un honeypot y cómo implementarlo en nuestra red.* WeLiveSecurity. [Blog]. Recuperado el 11 de mayo de 2021 de https://www.welivesecurity.com/la-es/2020/07/31/que-es-honeypot-como-implementarlo-nuestra-red/

[65] Chema Alonso. (26 de julio de 2017). *T-Pot: Una colmena de Honeypots para atraparlos a todos.* Un informático en el lado del mal. [Blog]. Recuperado el 15 de mayo de 2021 de https://www.elladodelmal.com/2017/07/t-pot-una-colmena-de-honeypots-para.html

[66] Sergio De Luz. (29 de septiembre de 2015). *Glaspot: Conoce este honeypot de aplicaciones web de código abierto.* RZ Redes Zone. [Blog]. Recuperado el 15 de mayo de 2021 de https://www.redeszone.net/2015/09/29/glaspot-conoce-este-honeypot-de-aplicaciones-web-de-codigo-abierto/

[67] Gabriel Verdejo. (2003). Honeypots y Honeynets. *Seguridad en redes IP.* (p. 113-149). Bellaterra, Barcelona, España. Recuperado el 15 de mayo de 2021 de https://www.cs.upc.edu/~gabriel/files/DEA-es-4HoneypotsyHoneynets.pdf

[68] Edgar A. Maya y Tatiana A. Vinueza. (2013). *Honeynet Virtual Híbrida en el entorno de red de la Universidad Técnica Del Norte de la ciudad de Ibarra*. (Tesis de pregrado). Universidad Técnica del Norte (UTN), Ibarra, Ecuador. Recuperado el 15 de mayo de 2021 de http://repositorio.utn.edu.ec/bitstream/123456789/1058/2/04%20RED%20013%20-%20ART_TECNICO_HONEYNET_UTN.pdf

[69] Eibin Acosta y Miguel Chaparro. (2013). *Diseño e implementación de un honeypot para la empresa SoluConstruccion SAS*. (Proyecto de Grado). Universidad Piloto de Colombia, Bogotá, Colombia. Recuperado el 20 de mayo de 2021 de http://polux.unipiloto.edu.co:8080/00000807.pdf

[70] Atreyi Kankanhalli, Hock-Hai Teo, Bernard C.Y. Tan, Kwok-Kee Wei. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*, 139-154. Recuperado el 20 de mayo de 2021 de http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/KankanhalliEtAl2003IJIM23_ISSecEffectiveness.pdf

[71] Iván Florez y Jesús Quintana. (2018). *Sistema de detección de ataques informáticos a redes de datos empresariales soportado en honeypots*. (Anteproyecto). Universidad de Cartagena, Cartagena, Colombia. Recuperado el 20 de mayo de 2021 de https://repositorio.unicartagena.edu.co/bitstream/handle/11227/8498/TESIS%20FLOREZ-%20MANQUINTANA.pdf?sequence=1&isAllowed=y

[72] Camilo Leon y Maria Bonilla. (2017). *Análisis de ataques informáticos mediante honeypots para el apoyo de actividades académicas en la Universidad Distrital Francisco José de Caldas.* (Proyecto de Grado). Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. Recuperado el 22 de mayo de 2021 de https://repository.udistrital.edu.co/bitstream/handle/11349/7509/Le%C3%B3n%20Cuervo%20Camilo%20Andr%C3%A9s%20-%20Bonilla%20D%C3%ADaz%20Mar%C3%ADa%20Alejandra%202017.pdf?sequence=1&isAllowed=y

[73] Admin. (14 de julio de 2007). *El ciclo PHVA Planear-Hacer-Verificar-Actuar*. Top Punto Com. [Blog]. Recuperado el 22 de mayo de 2021 de https://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

[74] Ruben B. Sanchez. (2005). *Seguridad en redes.* (Proyecto de Grado). Universidad Autónoma del Estado de Hidalgo, Hidalgo, México. Recuperado el 26 de mayo de 2021 de http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/165/Seguridad%20en%20redes.pdf?sequence=1&isAllowed=y

[75] Biblioteca Médica Nacional. (24 de julio de 2013). *¿Qué son las TICs?.* Recuperado el 26 de mayo de 2021 de http://www.bmns.sld.cu/que-son-las-tic

[76] INCIBE. (18 de mayo de 2021). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*. INCIBE. [Blog]. Recuperado el 26 de mayo de 2021 de https://www.incibe.es/protege-tu-empresa/blog/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[77] Hernan Diazgranados. (31 de agosto de 2021). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021.* Kaspersky Daily. [Blog]. Recuperado el 30 de septiembre de 2021 de https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

[78] Oriol Amat. (2008). *Análisis de Estados Financieros*. (8va Ed.) Ediciones Gestion 2000. Barcelona. Recuperado el 11 de octubre de 2021 de https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxnYW5pcm9wYXVwdGFlYnBuZmFkbXxneDo0MmE0ZGExNDBjYWE4Nzcz

[79] Carlos M. Heredia Terán. (2015). *Diseño e Implementación de una Honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre.* (Proyecto de Grado). Universidad Nacional de Loja, Loja, Ecuador. Recuperado el 27 de octubre de 2021 de https://dspace.unl.edu.ec/jspui/bitstream/123456789/11676/1/Heredia%20Ter%C3%A1n%2C%20Carlos%20Mauricio.pdf

[80] Victor M. Galán Pozuelo. (2015). *Tipos de conexiones de red en software de virtualización: VirtualBox y VMware*. Recuperado el 06 de noviembre de 2021. https://www.ticarte.com/sites/su/users/7/file/tipos-de-redes-en-virtualbox-y-vmware.pdf

[81] Luigy. (2016). *Cómo configurar el tipo de conexión de red en Máquina Virtual VMware WorkStation.* Tu Informática Fácil. [Blog]. Recuperado el 06 de noviembre de 2021 de https://www.tuinformaticafacil.com/virtualizacion/vmware/como-configurar-el-tipo-de-conexion-de-red-en-maquina-virtual-vmware-workstation

[82] Telekom-Security. (2021). *Guia de instalación y configuración del honeypot T-Pot.* Recuperado el 15 de noviembre de 2021 de https://github.com/telekom-security/tpotce

[83] Eduardo Zepeda. (18 de diciembre de 2020). *¿Qué es Docker y para qué sirve? Explicación. Dev.* [Blog]. Recuperado el 17 de noviembre de 2021 de https://dev.to/silicosis/que-es-docker-y-para-que-sirve-explicacion-5h2n

[84] Joel Pérez Pregal. (2020). *Diseño y despliegue de una campaña de engaño (deception campaign) en una red corporativa, basado en soluciones de código abierto.* (Proyecto Fin de Máster). Universidad de Vigo (UVIGO), España. Recuperado el 18 de noviembre 2021 de http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/534/TFM%20Joel%20P%C3%A9rez%20Pregal.pdf?sequence=1&isAllowed=y

[85] Hernán J. León Loja. (2021). *Despliegue de honeypot en la nube privada como primer perímetro de seguridad.* (Proyecto de Grado). Universidad Politécnica Salesiana Sede, Cuenca, Ecuador. Recuperado el 20 de noviembre 2021 de https://dspace.ups.edu.ec/handle/123456789/21307

[86] Ongi Etorri Gure. (27 de enero de 2021). *Los mejores honeypots: ejemplos, tipos, características y configuración*. Humedal Informatik. [Blog]. Recuperado el 20 de noviembre de 2021 de https://www.humedalinformatik.com/blog/los-mejores-honeypots-ejemplos-tipos-caracteristicas-y-configuracion

[87] ProgrammerClick. (2018). *T-Pot: Revolución de la plataforma multi-honeypot*. Recuperado el 20 de noviembre de 2021 de https://programmerclick.com/article/50621952610/

[88] David. (18 de septiembre de 2018). *¿Qué es Metasploit Framework?.* Hardsoft Security. [Blog]. Recuperado el 24 de noviembre de 2021 de https://hardsoftsecurity.es/index.php/2018/09/18/que-es-metasploit-framework/

[89] Zaher Talab. (20 de mayo de 2021). *11 herramientas de ataque de fuerza bruta para pruebas de penetración*. GeekFlare. [Blog]. Recuperado el 25 de noviembre de 2021 de https://geekflare.com/es/brute-force-attack-tools/

CAPÍTULO 9 - ANEXOS

9.1 ANEXO 01: INSTALACIÓN DE VMWARE WORKSTATION

VMware Workstation Pro es un hipervisor alojado que se ejecuta en versiones de 64 bits de los sistemas operativos Windows y Linux. Este un hipervisor permite a los usuarios configurar una o más máquinas virtuales en una única máquina física, y utilizarlas simultáneamente con la máquina host.

Cada máquina virtual puede correr su propio sistema operativo, incluyendo las versiones de Microsoft Windows, Linux, BSD, y MS-DOS entre otros. Lo bueno de usar este software es que admite la conexión de adaptadores de red de host existentes y el uso compartido de unidades de disco físico (CD-ROM) y dispositivos USB con una máquina virtual.

Requisitos mínimos

- 2GB de memoria RAM.
- Procesadores Intel Atom basados en la microarquitectura Bonnell.
- Sistemas con procesadores Intel Atom basados en la microarquitectura Saltwell.
- Sistemas con procesadores AMD basados en las microarquitecturas Llano y Bobcat.
- Sistemas operativos host (64 bits) Ubuntu 15/ CentOS 7/ Windows 7 o superiores.
- Compatibilidad con más de 200 sistemas operativos.

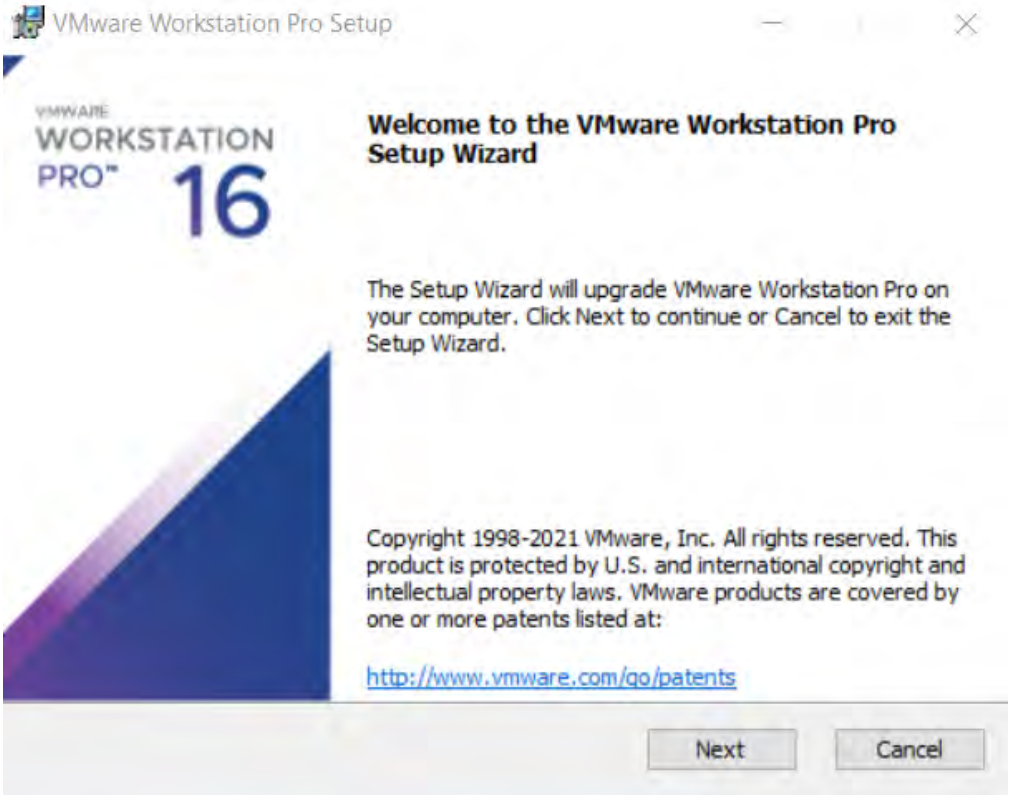
Activación de virtualización en BIOS/ UEFI

Este paso es fundamental y necesario para crear máquinas virtuales de 64 bits. Para ello se deberá activar una opción de virtualización que tienen los motherboards, permitiendo así que la máquina host destine físicamente parte de los recursos de hardware a las máquinas virtuales. Por lo tanto, debemos entrar a la BIOS de nuestro sistema, y activar el VT-x o bien el AMD-V para procesadores Intel o AMD respectivamente. En el caso de motherboards actuales, si se tiene UEFI, simplemente se activa mediante la opción de Virtualization Technology.

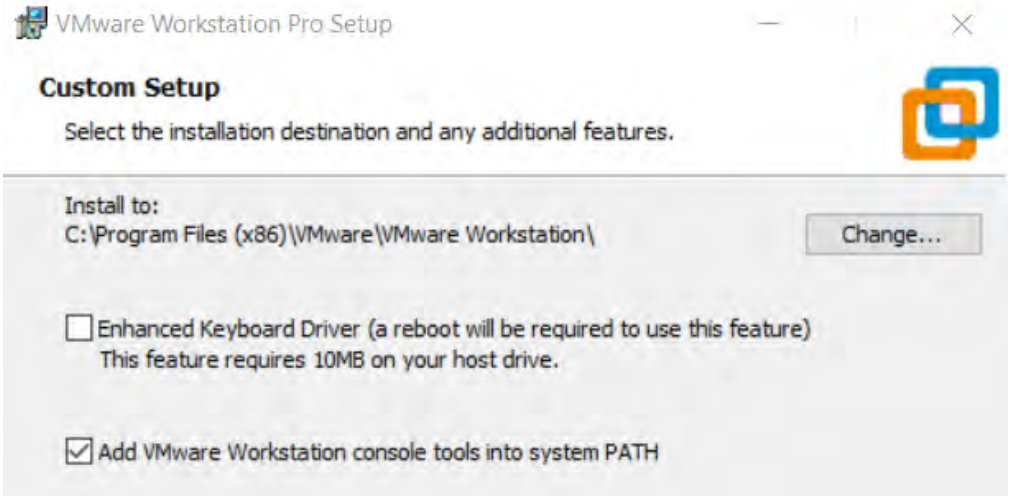
Proceso de instalación

1. Descargar desde la web oficial de VMware el software para Windows (o Linux según lo precise): https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

2. Una vez descargado el archivo lo ejecutamos para continuar con la instalación, mostrando en pantalla el asistente de configuración de VMware Workstation. Cabe resaltar, que la instalación es relativamente sencilla pues se trata de un simple wizard.

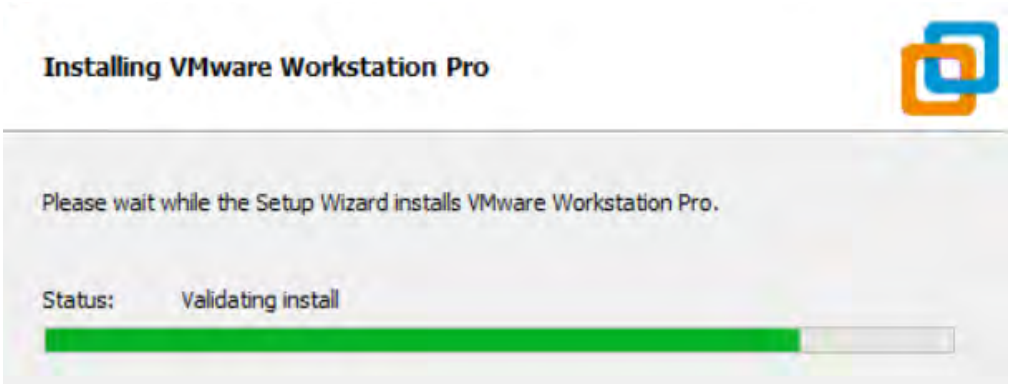


3. Aceptamos los términos del acuerdo de licencia y en las opciones de configuración personalizada seleccionamos la carpeta donde instalaremos la aplicación. Por lo general, se deja por defecto la ubicación que aparece, que normalmente será *Archivos de programa/VMware.*

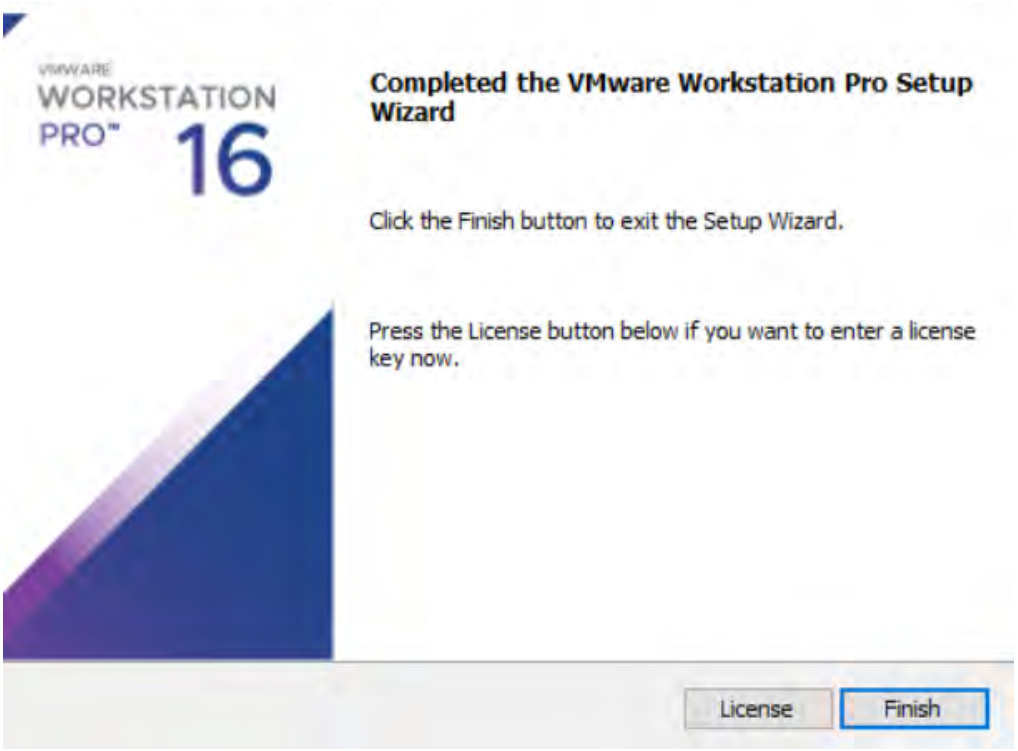


4. En este paso se selecciona el lugar donde se colocarán los accesos directos para iniciar la aplicación de VMware. La ubicación por lo general es en el escritorio y el menú de inicio.

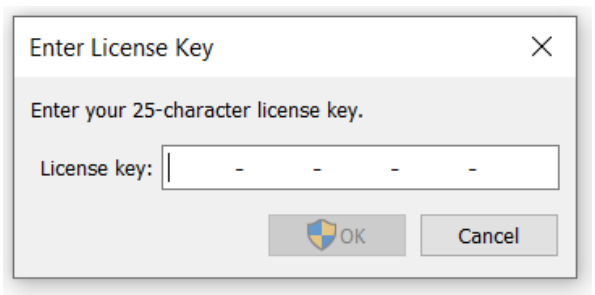
5. Una vez completados los pasos anteriores comienza el proceso de instalación. Esperamos a que la instalación se complete, el cual tardará unos pocos minutos.



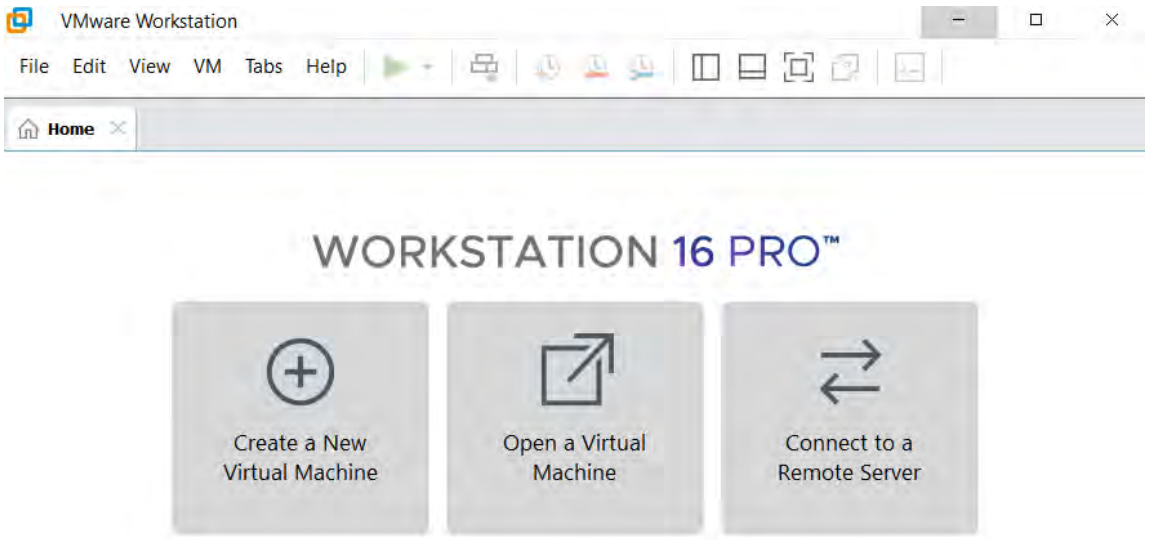
6. Ahora nos aparecerá la ventana de instalación completa. Hacemos clic en finalizar para terminar el proceso de instalación.



7. Una vez completada la instalación, ejecutamos el aplicativo VMware desde su acceso directo en el escritorio. Al ejecutar, el programa nos solicitará la clave de licencia, la ingresamos y continuamos con la apertura del programa.



8. Ahora ya tenemos nuestro VMware Workstation activado e instalado correctamente en nuestro equipo. La siguiente imagen nos muestra la ventana principal del programa.



9. Lo último que queda es empezar a crear las diferentes máquinas virtuales que queramos tener, asignando para cada máquina virtual los recursos necesarios.

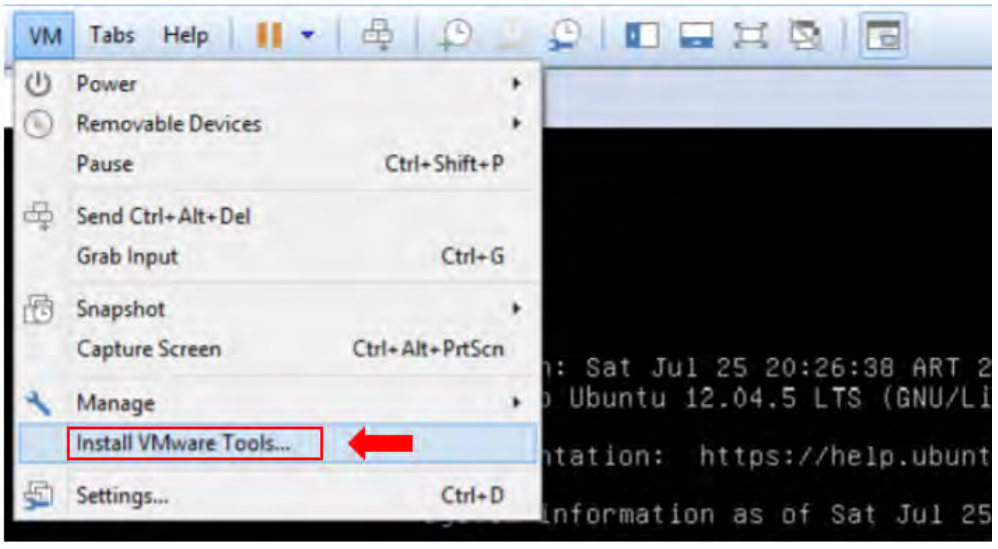
9.2 ANEXO 02: INSTALACIÓN Y CONFIGURACIÓN DE VMWARE TOOLS

Las VMware Tools es un conjunto de controladores del hardware virtual que es recomendable instalar en cualquier máquina virtual creada con VMWare. Las ventajas de instalar las VMware Tools pasan por la optimización del uso del hardware virtual por parte del sistema operativo de la máquina virtual y la mayor integración entre el anfitrión y el sistema operativo virtualizado. (Miguel Sanchez, 2015).

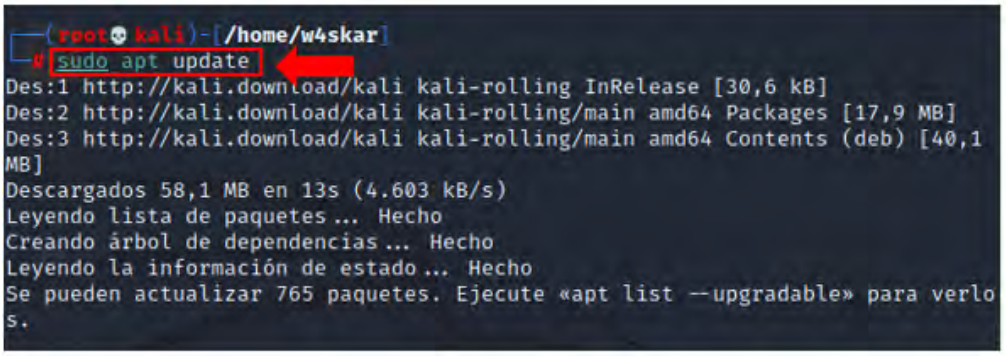
Proceso de instalación

1. Este controlador deberá ser instalado en cada sistema operativo virtual que configuremos. Verificar previamente que no esté cargado ninguna imagen ISO en la unidad virtual CD/DVD.

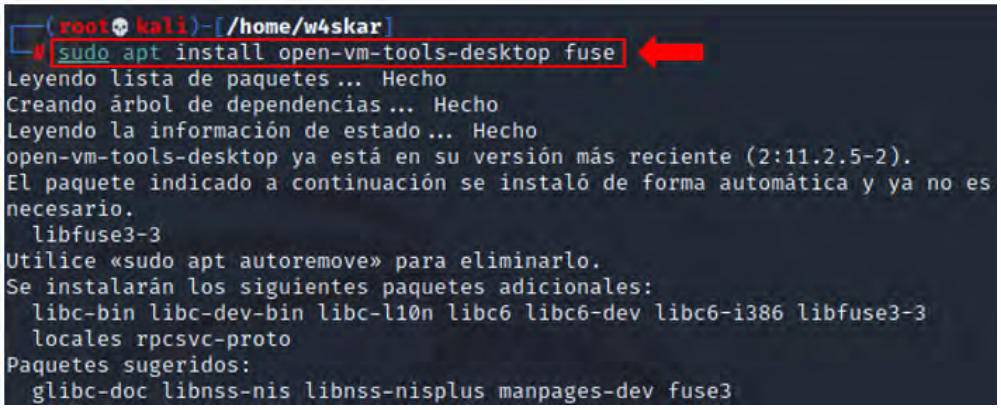
2. Para el caso de Kali Linux o cualquier sistema Linux, encendemos nuestra máquina virtual y luego en la propia ventana del VMware nos dirigimos al menú y seleccionamos *VM>Install VMware Tools.* Con esto, lo que hemos logrado es cargar en nuestra unidad virtual la imagen ISO correspondiente a las VMware Tools.



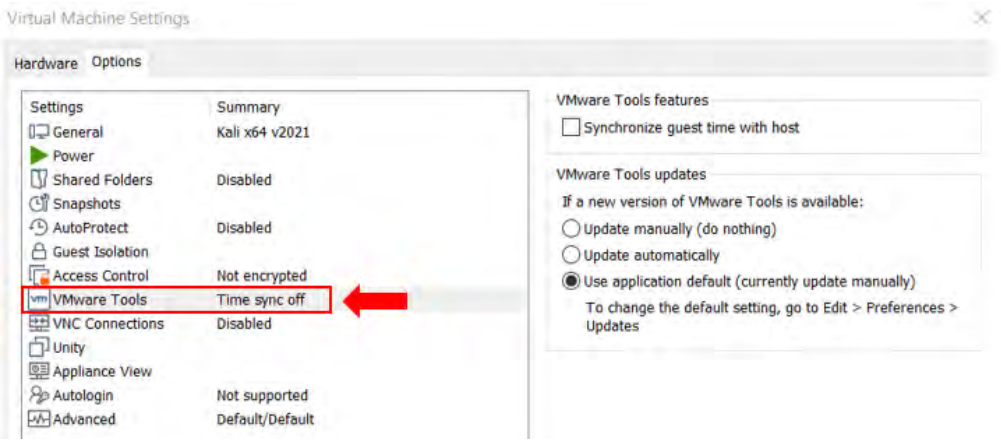
3. Para instalar el VMware Tools montado en nuestro sistema, abrimos una consola y como usuario root (*sudo su*) actualizaremos nuestro sistema Linux. Para ello tipeamos: *sudo apt update*



4. Ahora resta instalar VMware Tools tipeando: *sudo apt install open-vm-tools-desktop fuse.* Luego de esto, simplemente reiniciamos el sistema virtual.



5. Para verificar que está correctamente instalado VMware Tools, nos dirigimos a la configuración de la máquina virtual y en la solapa *Options* nos debería de salir las características de VMware Tools.



6. Listo. Con esto ya tenemos funcionando VMware Tools.

9.3 ANEXO 03: COMPONENTES BÁSICOS DE LA RED VIRTUAL

Los componentes que posee una red virtual normalmente incluyen switches virtuales, adaptadores de red virtual, servidor DHCP virtual y el dispositivo NAT (Luigy, 2015).

- *Switches virtuales*

  Funcionan igual que un switch físico, conectando así los componentes de red. Los switches virtuales, que son también referidos como redes virtuales, se nombran con VMnet0, VMnet1, VMnet2, ... y así sucesivamente. Lo bueno de VMware es que se pueden crear hasta 10 switches virtuales en un host Windows, conectando un número ilimitado de dispositivos, mientras que en un host Linux se pueden crear hasta 255 switches con un máximo de 32 dispositivos. Normalmente, en los sistemas host Linux, los nombres de los switches son en minúsculas, por ejemplo, vmnet0, vmnet1, etc.

Tipo Red	Nombre Switch
Bridged	VMnet0
NAT	VMnet1
Host-Only NetWork	VMnet2

- *Adaptadores de red virtuales*

  Cuando se utiliza el asistente para crear una nueva máquina virtual, el asistente crea una adaptador virtual de red para la máquina virtual. Este adaptador aparece en el sistema operativo guest y puede ser empleado de cinco modos diferentes (para mayor detalle consultar el *Anexo 06*). Además con las versiones VMware 6.0 o superiores se pueden tener hasta 10 adaptadores de red virtuales.

- *Servidor DHCP Virtual*

  El servidor DHCP virtual proporciona direcciones IP a las máquinas virtuales en configuraciones que no sean bridged o una red externa. Por ejemplo, el servidor DHCP virtual asigna direcciones IP a las máquinas virtuales configuradas en modo Host-Only y NAT.

- *Dispositivo NAT*

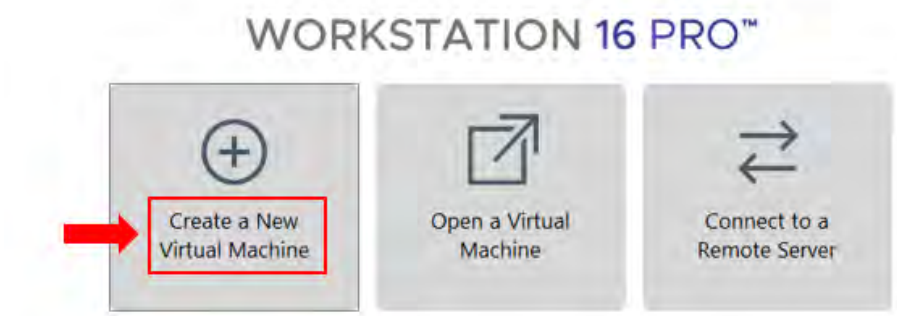
  En una configuración NAT, el dispositivo NAT pasa datos entre una o más máquinas virtuales y la red externa, identifica los paquetes de datos entrantes destinados a cada máquina virtual y los envía a al destino correcto.

9.4 ANEXO 04: CREACIÓN DE UNA MÁQUINA VIRTUAL

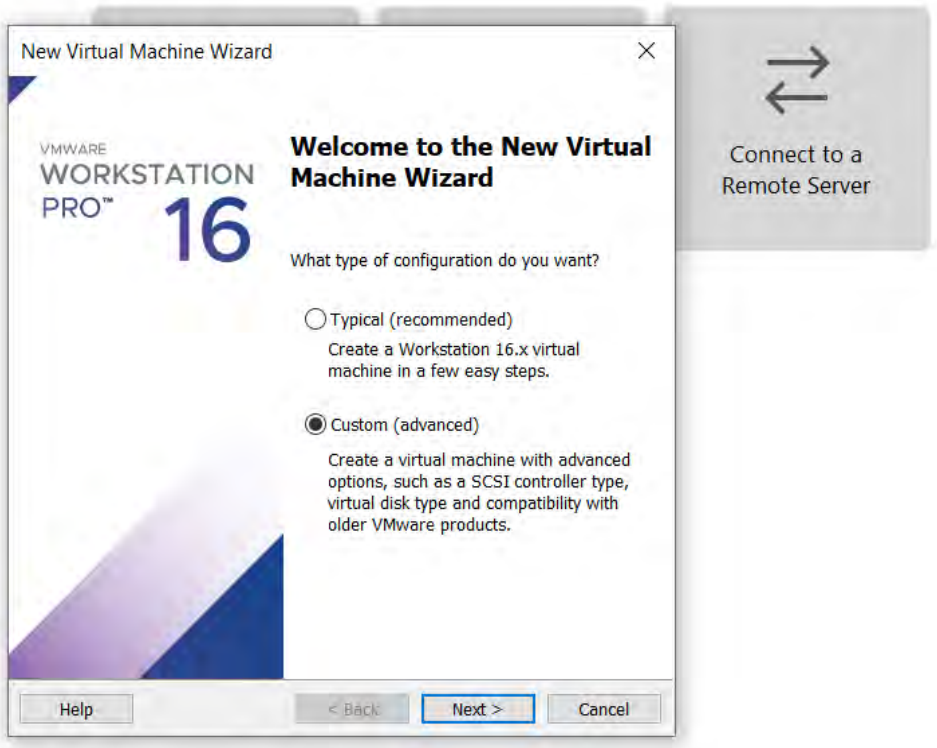
En términos generales, una máquina virtual (VM) es un software que permite emular el funcionamiento de una computadora dentro de otra computadora. Es decir, es un entorno virtual que funciona como sistema informático virtual con su propia CPU, memoria, interfaz de red y almacenamiento, pero se crea en un sistema de hardware físico (equipo host).

Proceso de instalación

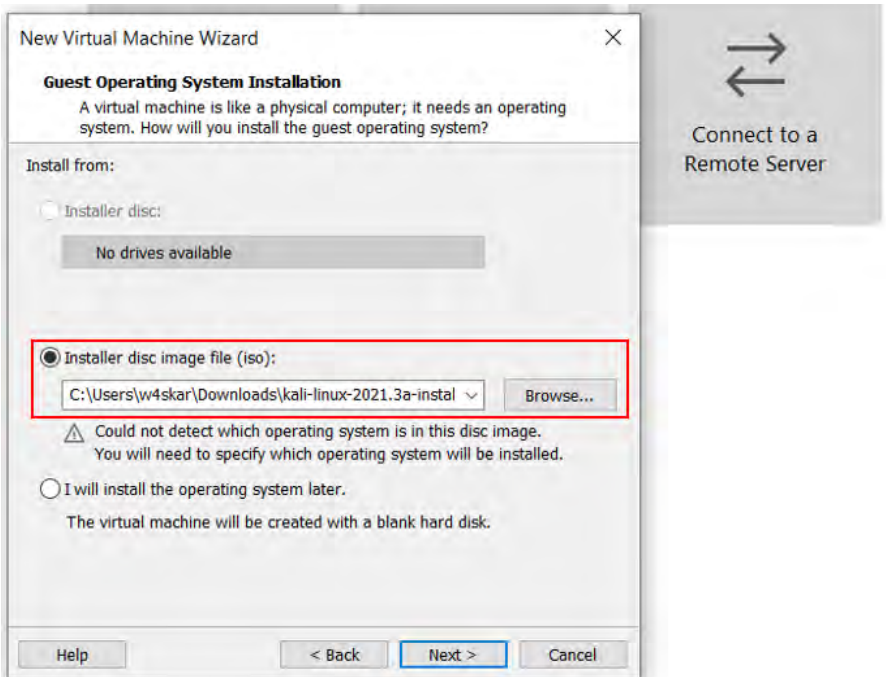
1. Abrimos el software VMware Workstation y en la pantalla principal que nos aparece seleccionamos *Create a New Virtual Machine* o bien hacemos clic en *Files>New Virtual Machine*



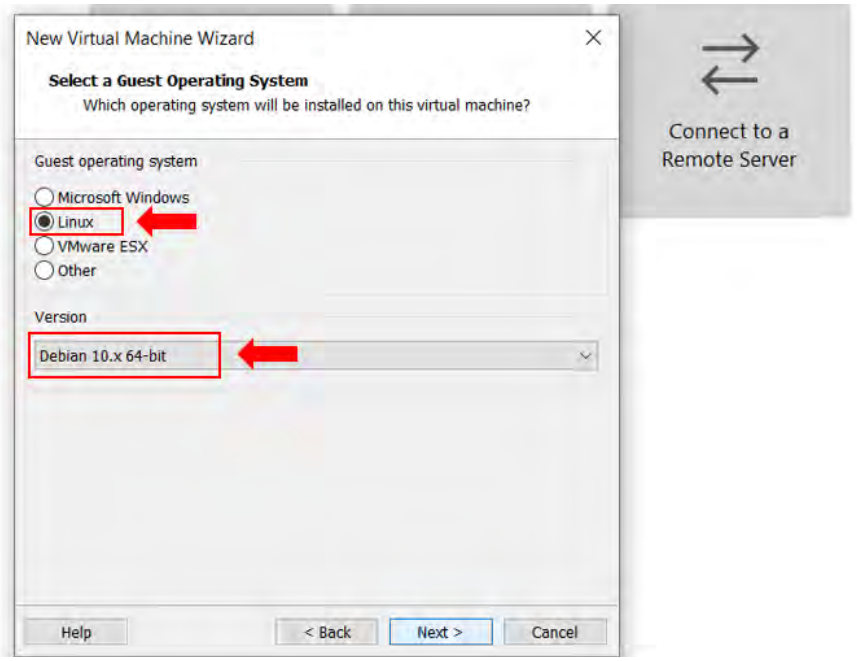
2. Luego en la ventana que nos aparece seleccionaremos la opción que mejor se ajuste a nosotros. Por lo tanto, seleccionaremos por una configuración personalizada (custom).



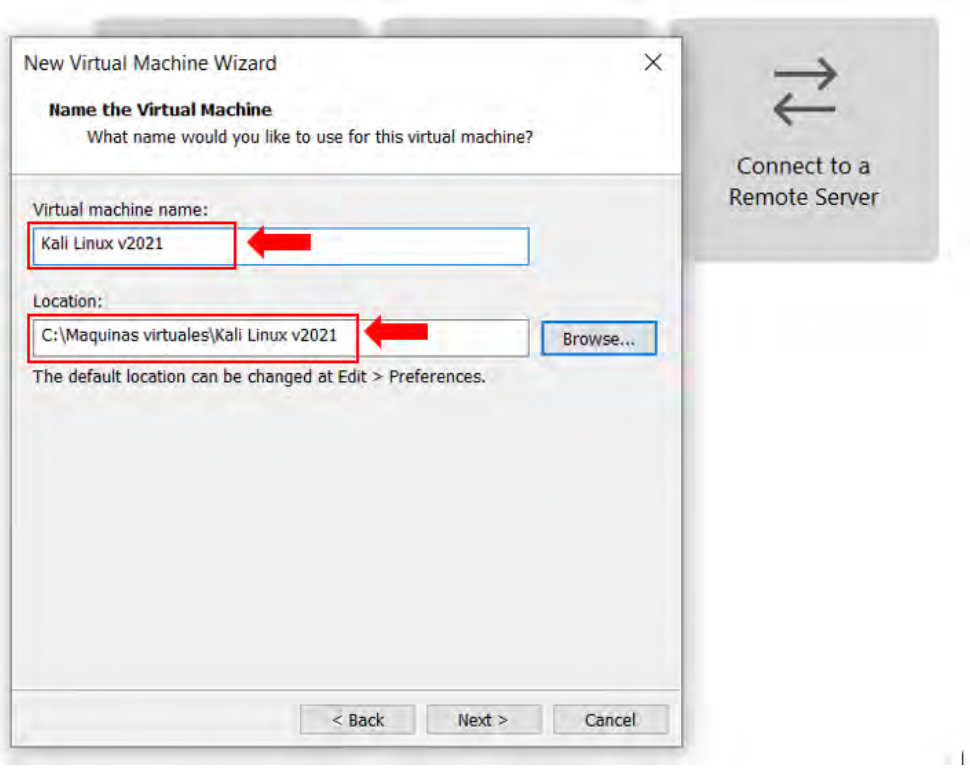
3. En esta ventana, si ya tenemos la imagen ISO de nuestro sistema operativo que queremos instalar tendremos que seleccionar la opción que dice *Installer disc image file (iso)* y luego buscar la imagen ISO de dicho sistema (en este caso Kali Linux). Caso contrario, cargamos la imagen ISO más adelante.



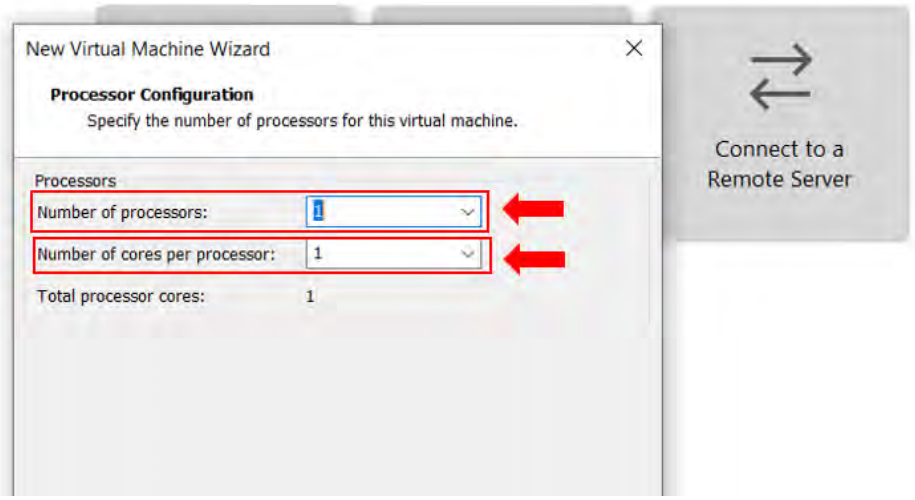
4. Sabiendo el tipo de sistema operativo que vamos a instalar (sean distribuciones Windows o Linux), ahora se deberá especificar el tipo de plataforma y versión que alojará la máquina virtual.



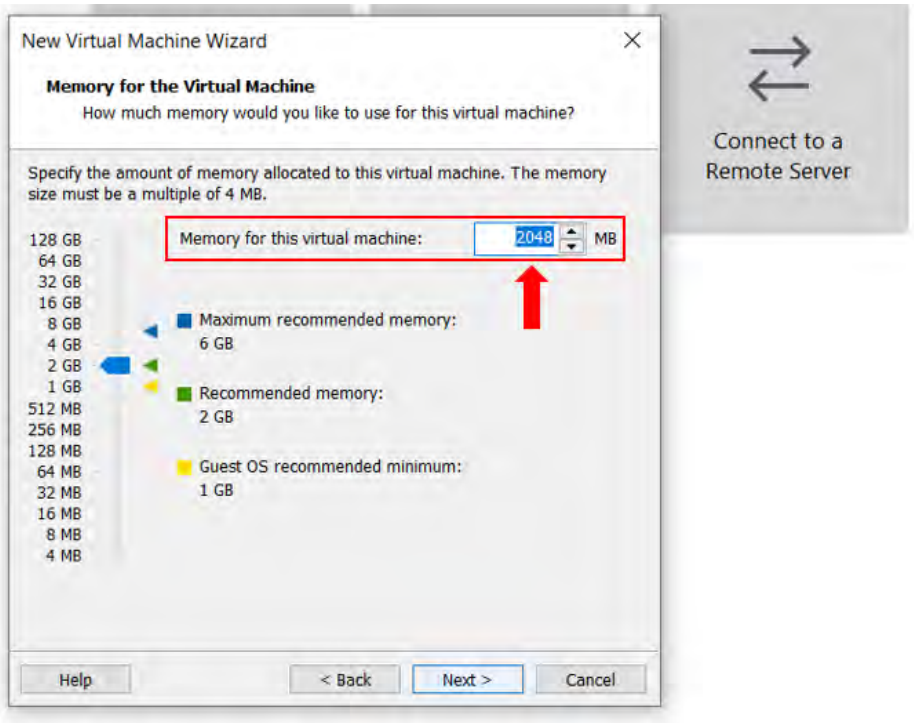
5. Ahora colocamos un nombre para identificar la máquina virtual. También podemos modificar la ubicación donde se instalará la máquina virtual o bien dejarlo por defecto. Para nuestro caso, vamos a instalarla en una carpeta específica para allí tener ordenadas todas las máquinas virtuales creadas.



6. En esta ventana configuraremos la cantidad de procesadores y núcleos que tendrá nuestra máquina virtual. Tener en cuenta que esta asignación dependerá del hardware de nuestro host anfitrión.



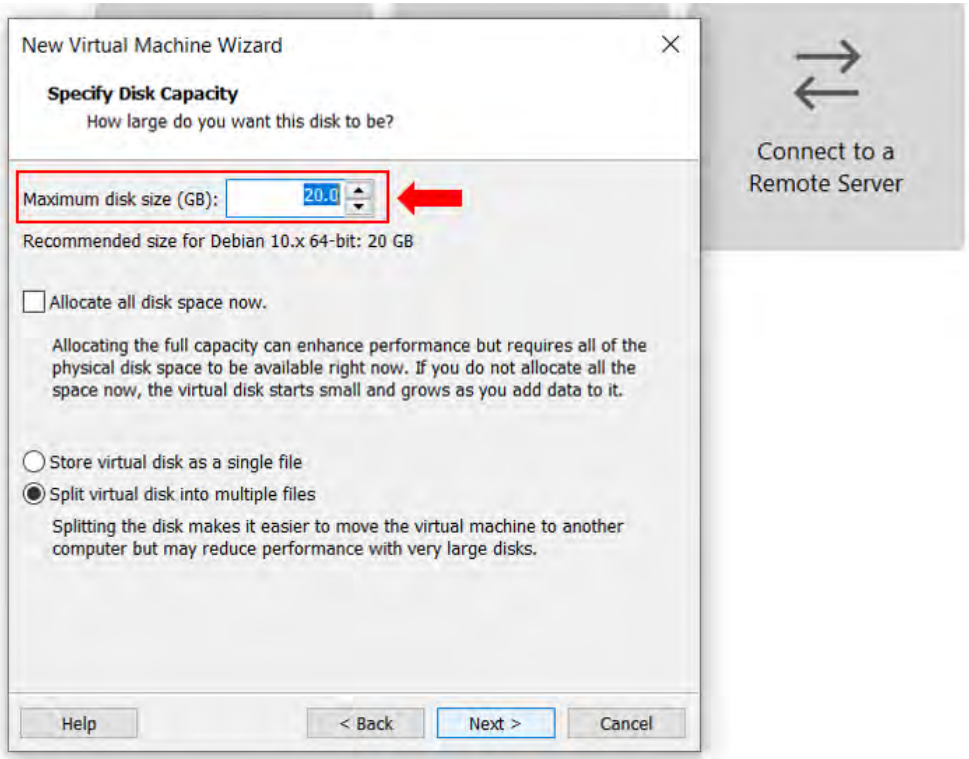
7. También vamos a configurar la memoria RAM del sistema, que según lo que fuimos configurando, el propio VMware asignará una memoria mínima (y una recomendada), para que a partir de ella podamos modificarla a gusto si así lo deseamos. Obviamente que cuanto menor sea la memoria, menos performance va a tener esa máquina virtual.



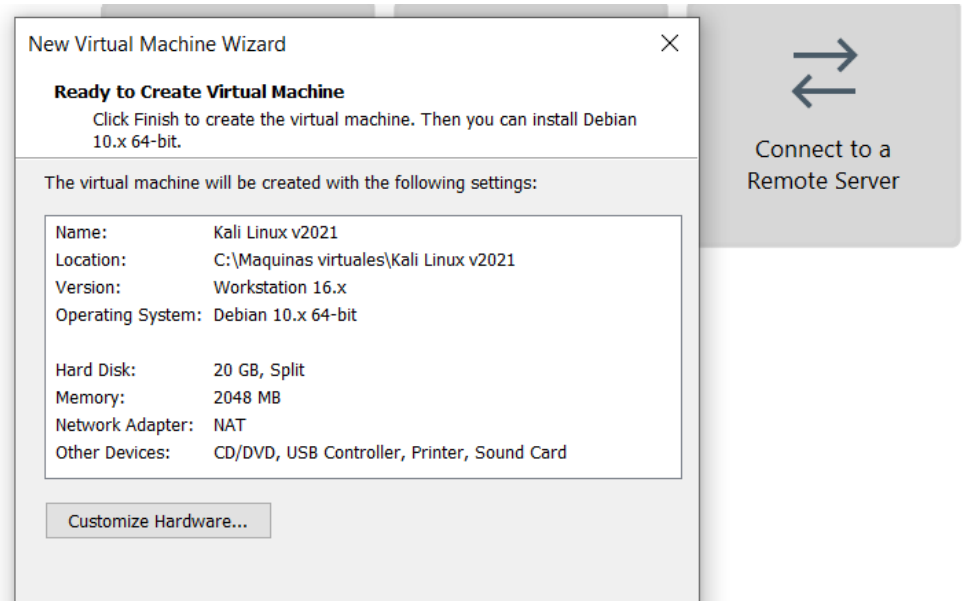
8. Otros de los parámetros a configurar serán el tipo de red, tipo de controlador de entrada/ salida y el tipo de disco virtual. Todo esto dependerá siempre del tipo de máquina que queremos montar y lo que se hará con ella. Normalmente estos parámetros se los deja por defecto.

9. También habrá que configurar la capacidad máxima del disco. Esto determinará el espacio total que tendremos en nuestra máquina virtual para almacenar datos. El espacio quedará determinado por la capacidad de almacenamiento que tengamos en nuestro anfitrión, y por ende no se podrá asignar más de lo que se tiene. En cuanto a las opciones, si el disco virtual será de tamaño fijo o variable dependerá de nosotros y del objetivo de esa máquina virtual.

   Por ejemplo, si nuestra máquina virtual estará destinada para ser explotada, colocar la opción de almacenamiento en un único disco (*store virtual disk as a single file*) evitará que se produzca mucha fragmentación, pero con la desventaja de que la asignación (de 20GB por ejemplo) se reserva por completo, a pesar de no usarse todo. Mientras que en el otro caso, el *split virtual disk into multiple files* el disco aumentará de tamaño a medida que se requiera.

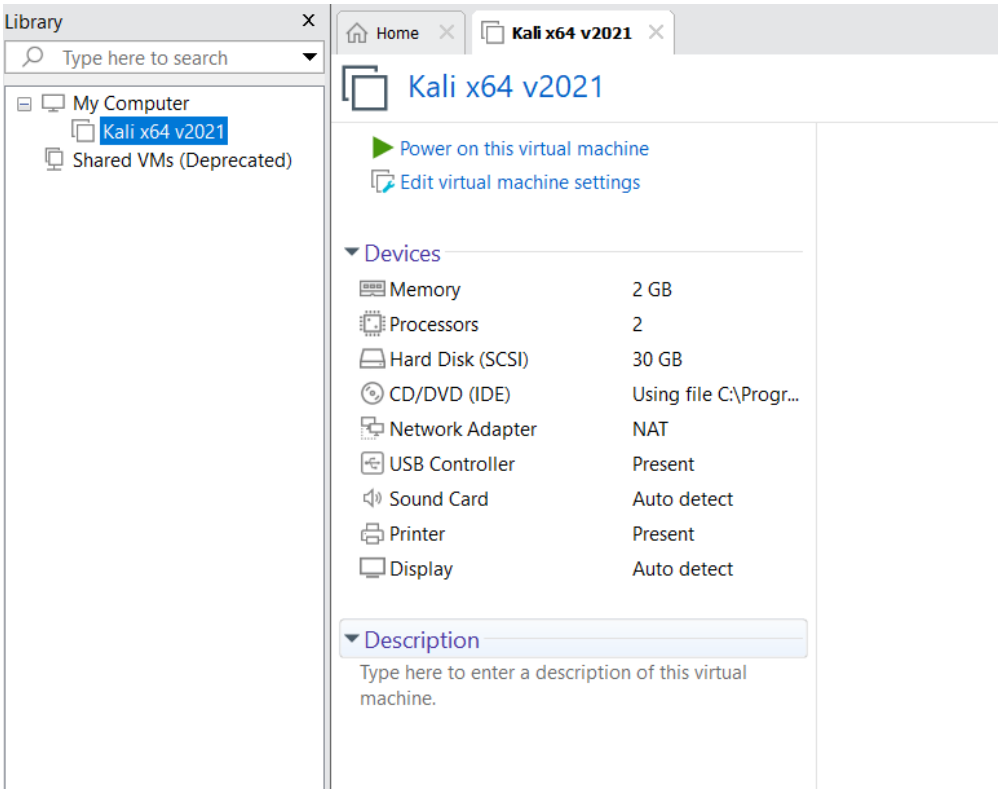


10. Finalmente la última pantalla nos muestra un resumen detallado de todas las configuraciones que hicimos. Si quisiéramos modificar algún parámetro solo hacemos clic en *Customize Hardware* para modificar o agregar lo se necesite.



11. Con todos estos parámetros configurados, ya tenemos listo nuestra máquina virtual, solo resta instalar el sistema operativo que queramos. Cabe destacar que todo este proceso es válido para cualquier máquina, sea Windows o Linux, lo que variará serán solo algunos aspectos de hardware.

Por ejemplo, la siguiente imagen muestra la máquina virtual que se creó para alojar al sistema operativo Kali Linux, teniendo como elementos de hardware asignado 2GB para la memoria RAM, un procesador de dos núcleos, tipo de red NAT y un almacenamiento en disco de 30GB. Si bien estos parámetros ya están definidos, se pueden modificar tranquilamente, siempre y cuando la máquina virtual esté apagada.



9.5 ANEXO 05: INSTALACIÓN DE UN SISTEMA OPERATIVO

A continuación se explicará cómo poder instalar un sistema operativo en una máquina virtual. El sistema a instalar podrá ser tanto Windows como Linux y válido para sistemas actuales de 64 bits, pero en sí, los procedimientos a realizar son los mismos. En este anexo básicamente ejemplificaremos la instalación de sistemas operativos Linux, puesto que los sistemas Windows son más intuitivos y fáciles de instalar.

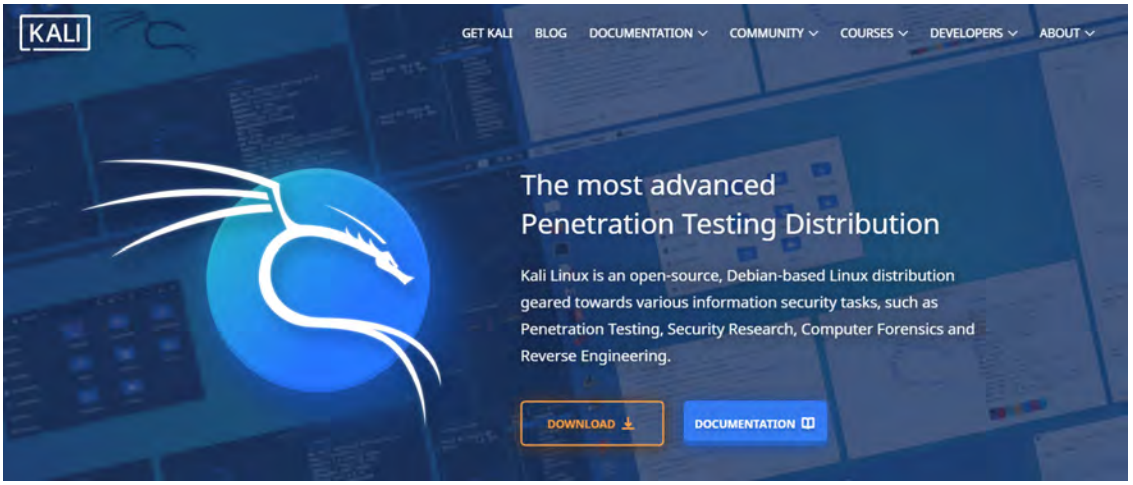
La instalación de cualquier distribución Linux en una máquina virtual muchas veces puede parecer compleja para algunos usuarios, pero una vez que se entienda el proceso, la instalación será realmente sencilla. En este caso vamos a considerar la instalación del sistema operativo Kali Linux en su última versión estable. Como se sabe, Kali Linux es una distribución de Linux basada en Debian y desarrollada por Offensive Security para pruebas de penetración y auditorías de seguridad. Este sistema operativo consta de muchas características, entre las que podemos mencionar que tiene más de 300 herramientas gratuitas para realizar tareas de pentesting, amplio apoyo para los dispositivos inalámbricos permitiendo que funcionen correctamente, enteramente personalizable, de código abierto, y un sistema totalmente confiable por la seguridad de paquete firmados que posee.

Requisitos mínimos

- 1GB de memoria RAM.
- 8GB de almacenamiento en disco.
- Procesador Intel i386 o AMD64.

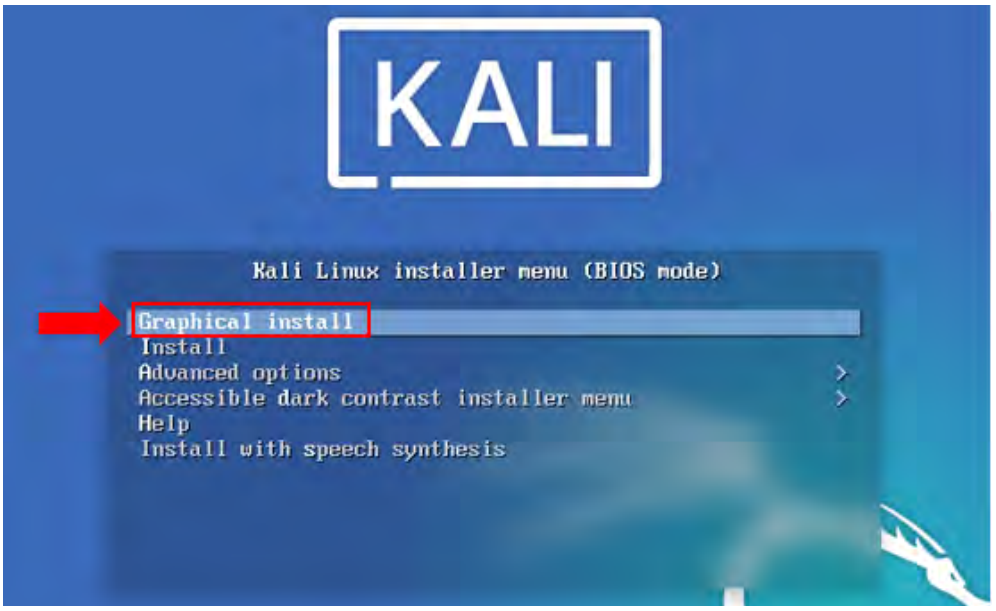
Proceso de instalación

1. Descargar desde la web oficial de Kali Linux (https://www.kali.org/) la imagen ISO adecuada.

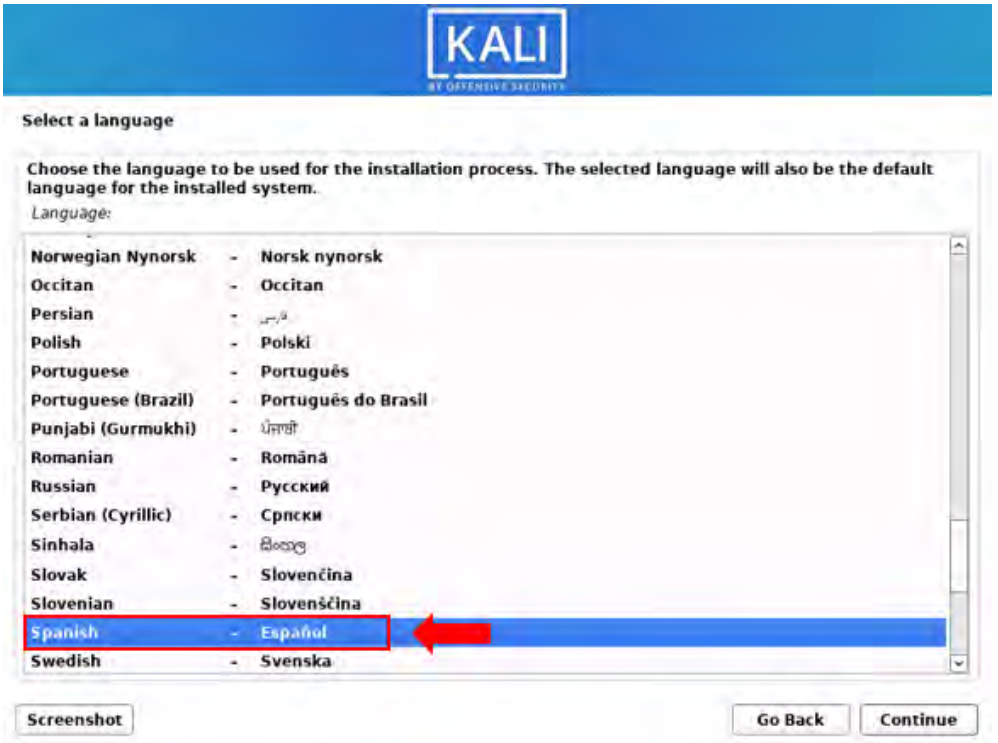


2. En VMware crearemos una máquina virtual el cual alojará nuestro sistema operativo Kali Linux. Para saber cómo se crea una máquina virtual en VMware consultar el *Anexo 04.*

3. Con la máquina virtual ya creada y configurada, cargamos ahora la imagen ISO de Kali Linux para dar inicio a la instalación. Tras arrancar, elegir el modo de instalación gráfico (Graphical install).



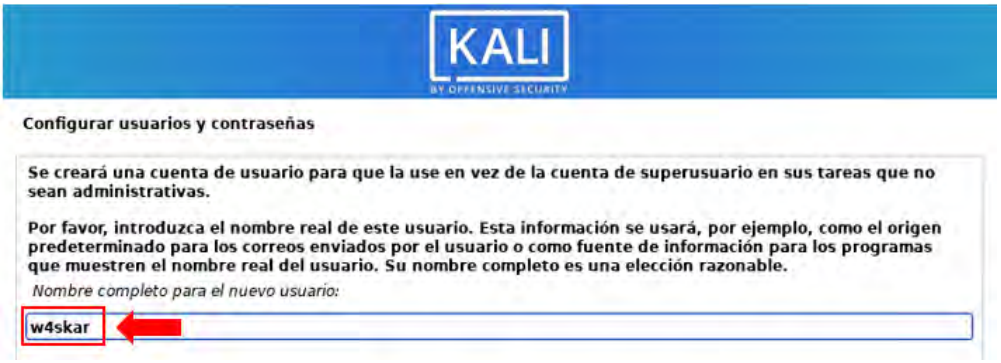
4. A partir de ahora nos aparecerán una serie de pantallas donde deberemos ir configurando nuestro lenguaje, ubicación y el tipo de teclado a utilizar.



5. Luego configuraremos la red asignando un nombre a la máquina en cuestión. Por lo general, este hostname se lo deja por defecto con el nombre *kali*.

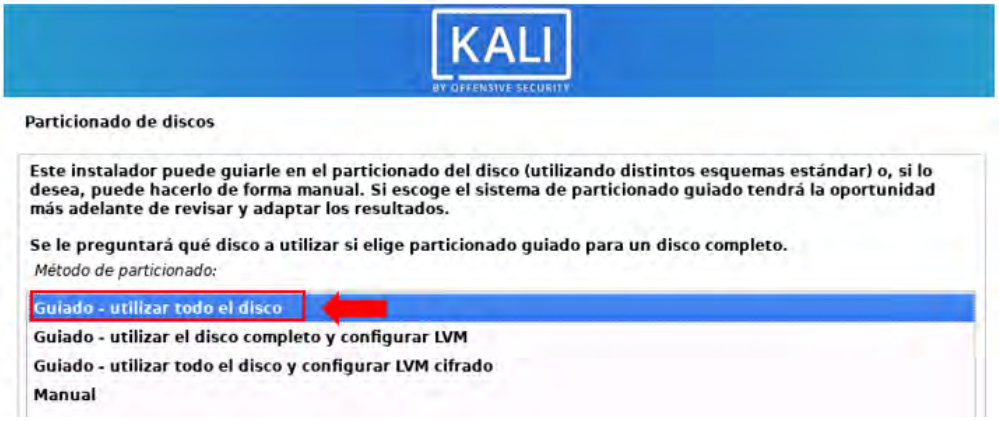
6. El nombre de dominio también lo dejamos por defecto (es decir en blanco), puesto que aún no necesitamos ninguno en concreto. En caso que se necesite, se configura más adelante cuando el sistema ya esté instalado.

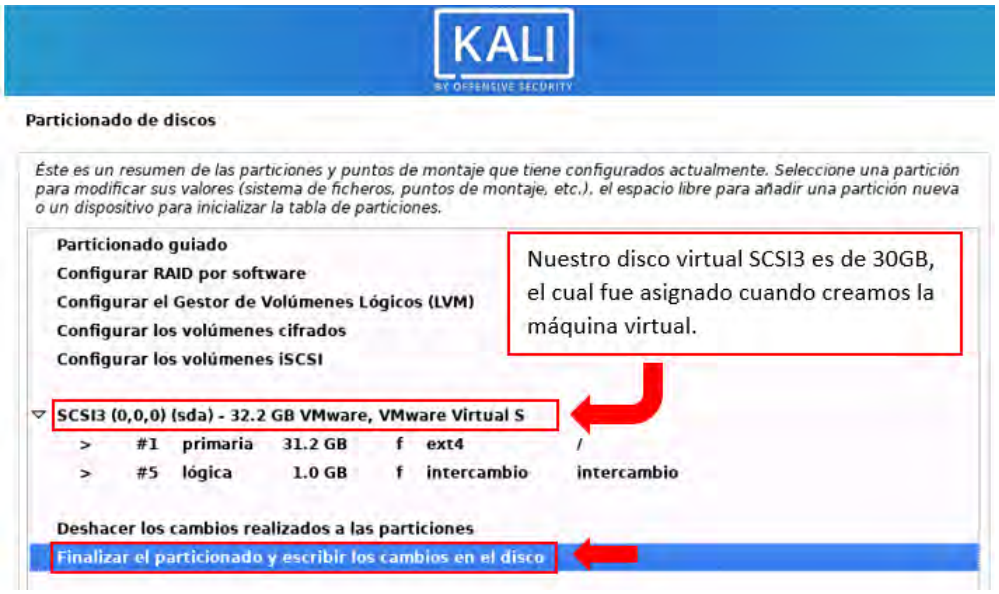
7. Ahora asignaremos un nombre de usuario y contraseña para utilizar en el sistema. Para fines de este proyecto usaremos el pseudónimo *w4skar* y el cual podrá tener privilegios root.

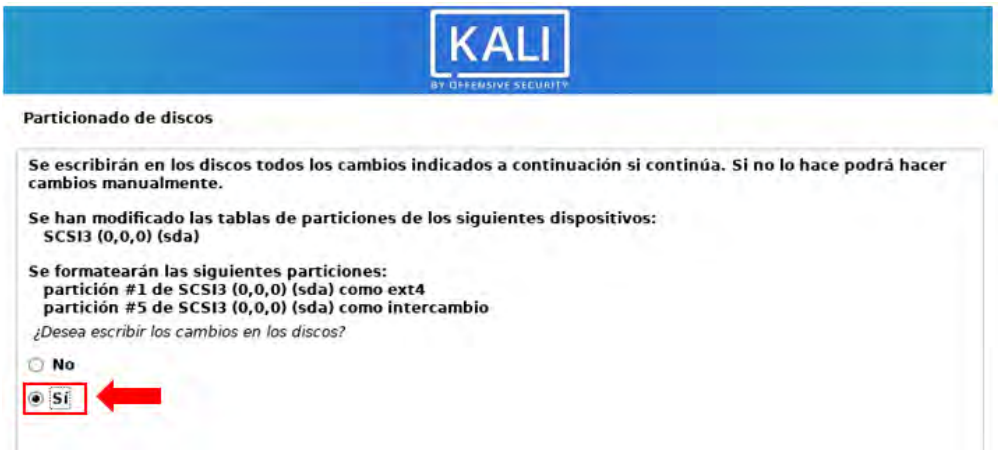


Para mayor seguridad, la contraseña debe contener como mínimo 8 caracteres alfanuméricos. Además, esta clave será la que usaremos para loguearnos en el sistema.

8. Realizamos ahora las particiones del disco. Puesto que solo vamos a almacenar un solo sistema operativo en esta máquina, lo lógico es seleccionar una instalación guiada utilizando todo el disco virtual. Para usuarios avanzados, se pueden crear tantas particiones como sean necesarias.

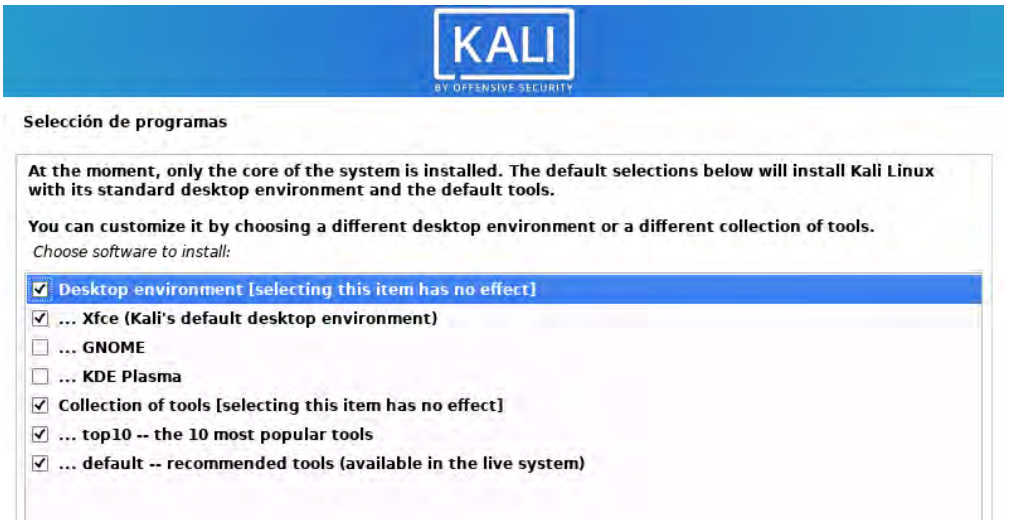






9. Tras confirmar las configuraciones de las particiones que realizamos en los pasos anteriores comenzará a instalarse el sistema base.

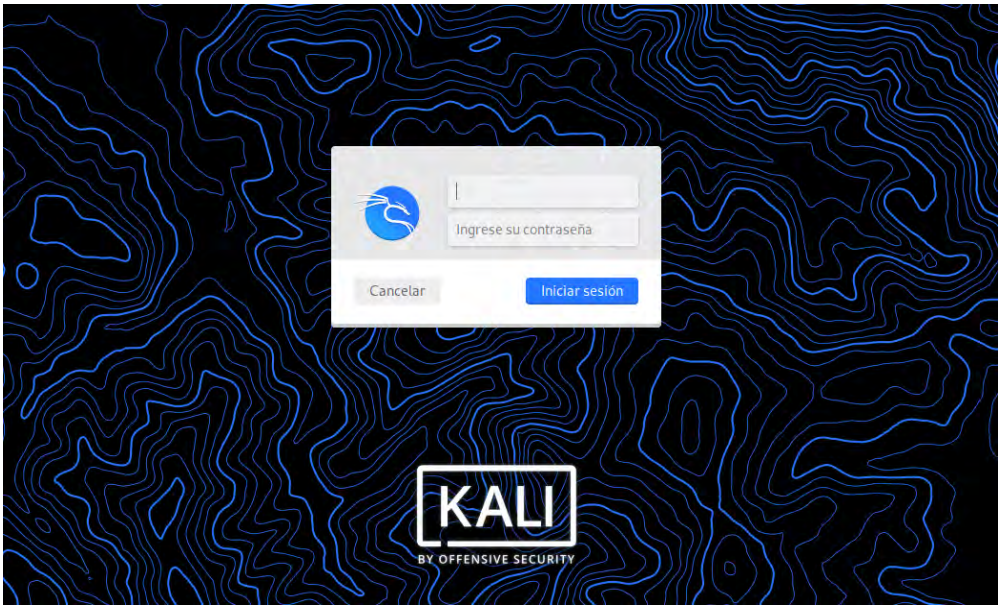
10. Luego el wizard nos pedirá que seleccionemos algunos programas, pero dejaremos por defecto los que aparecen seleccionados.



11. Ahora queda instalar el GRUB de arranque múltiple. Si bien este gestor es ideal cuando tenemos varios sistemas operativos, no está mal tenerlo instalado para futuros sistemas.

12. Finalmente con todas estas configuraciones se termina la instalación. La última ventana nos indicará que todo salió bien y se reiniciará el equipo ejecutando el sistema operativo Kali Linux.

Una vez iniciado el sistema, solo restará loguearnos con las credenciales correspondientes.

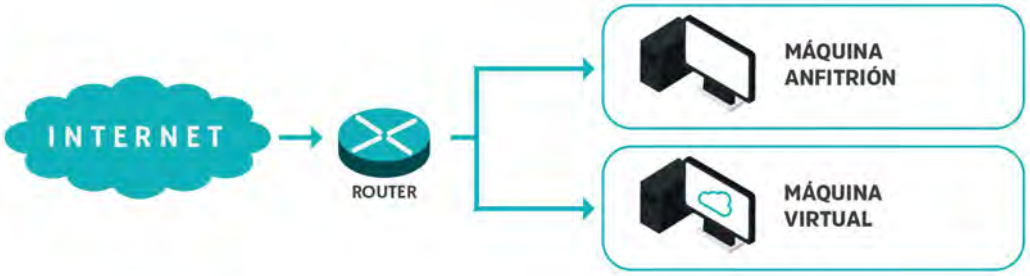


9.6 ANEXO 06: ADAPTADORES DE RED EN MÁQUINAS VIRTUALES

A continuación se mostrarán y explicarán las diferentes formas en las que podemos configurar la red en una máquina virtual, ya que dependiendo de cómo se conecten se utilizarán de una forma o de otra, y para ello utilizaremos el hipervisor VMware Workstation. Según el autor Victor M. Galán Pozuelo (2015), los distintos tipos de conexiones de red que se tiene son:

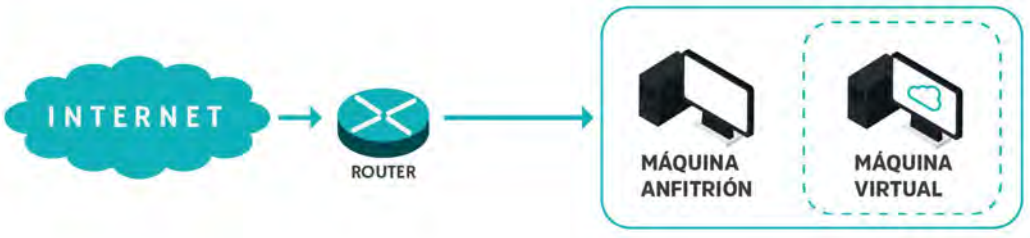
1. *Modo Bridge*

   Bridge es la configuración por defecto cuando creamos una máquina virtual, ya que es la forma más sencilla de otorgar acceso a la red a una máquina virtual. Cuando está en modo bridge, tu red local es extendida hacia tu máquina virtual. Aunque tu equipo se conecte a tu red local usando el hardware de tu ordenador físico, la máquina virtual será totalmente independiente de la red. Del mismo modo, todo PC físico u otra máquina virtual que esté conectada de la misma forma, podrá usar los recursos de la máquina virtual como si fuera un equipo físico en la misma red. De esta forma si tu equipo físico está configurado para recibir una dirección IP por un servidor DHCP, tu máquina virtual recibirá una IP del mismo servidor DHCP.



2. *Modo Host-Only*

   Host-Only como su propio nombre indica solo se conecta con el host físico. Cuando está en modo host-only, la máquina virtual está totalmente aislada de la red de área local ya que la red de la máquina virtual está dentro del propio equipo y es invisible e inaccesible para cualquier equipo de la red del equipo.

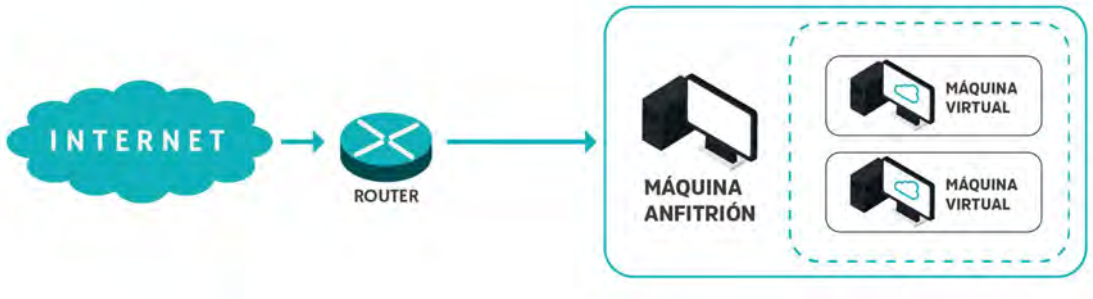


3. *Modo NAT (Network Address Translator)*

   NAT es un modo de conexión fácil de utilizar pero algo complicado de entender. Fue pensado para solucionar el problema de la escasez de las direcciones IP de forma tal que las redes de computadoras utilicen un rango de direcciones especiales (IP privadas) y se conecten a Internet usando una única dirección IP (IP pública), de esta forma varios PCs se conectan a Internet con una única IP. En las máquinas virtuales lo que sucede es que esta recibirá una dirección IP de un servidor DHCP virtual, sin embargo el que pide la IP será el firewall dentro de la aplicación de virtualización, que sustituye a tu máquina virtual. Así, el que se encarga de comunicarse con la red fuera de tu equipo será tu firewall, no tu máquina virtual.

4. *Modo Red Interna*

   Red interna es una forma de conectar varias máquinas virtuales entre ellas creando una red privada, de esta forma, las máquinas virtuales no podrán ver al PC anfitrión ni viceversa. Con esta opción podemos crear más de una red interna de forma sencilla, de esta forma se puede trabajar con varias redes internas de forma muy sencilla.



5. *Modo No Conectado*

   Esta opción indica que hay una tarjeta de red instalada pero no está conectada a ningún otro lugar. Esta configuración se utiliza para que no se pierda la configuración, ya que aunque esté en modo no conectado, la tarjeta de red guarda la configuración especificada. Después de explicar las opciones llevémoslo a la práctica, para ello vamos a utilizar dos máquinas virtuales con un sistema operativo Ubuntu (Cliente 1 y Cliente 2) y un ordenador anfitrión con sistema operativo Windows 8.

9.7 ANEXO 07: CONFIGURACIÓN DE LA RED EN LAS MÁQUINAS VIRTUALES

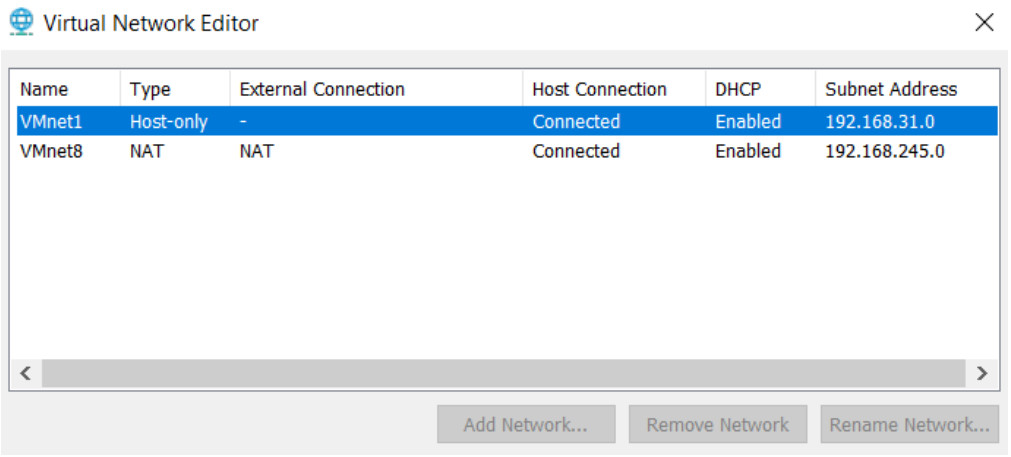
Para poder asignar correctamente las direcciones IPs en nuestras máquinas virtuales, se deberá tener en cuenta los rangos de direcciones para redes privadas ya establecidas por IANA . Estas direcciones podrán ser de tres clases:

- Para redes grandes usamos Clase A: 10.0.0.0 a 10.255.255.255
- Para redes medianas usamos Clase B: 172.16.0.0 a 172.31.255.255
- Para redes pequeñas usamos Clase C: 192.168.0.0 a 192.168.255.255

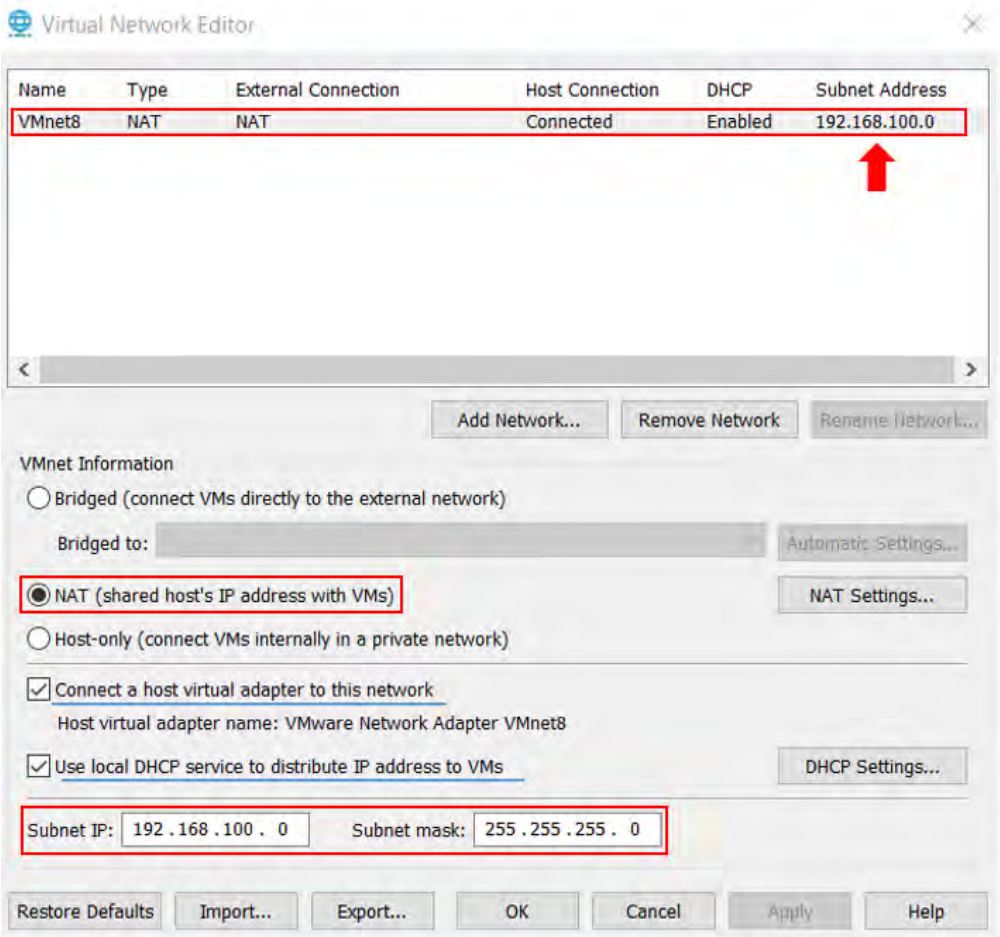
Por ende, en la infraestructura de este proyecto podremos usar cualquiera de estas clases, puesto que estos rangos están sin coordinación con IANA. Entonces, sabiendo que la empresa analizada no es muy grande, trabajaremos con redes privadas de clase C debido a que se tendrá menos de 256 equipos, pero llegado el momento, si la empresa se expande superando estos equipos, se podrá optar por emplear direcciones clase B o clase A. Con esto, lo que queremos decir es que las direcciones en este espacio de direcciones solo son únicas dentro nuestra red privada, y fuera de estos rangos se consideran públicas.

Proceso de configuración

1. Toda la configuración entre todas las máquinas virtuales se hace mediante el editor virtual de redes. Para ello, abrimos el hipervisor VMware y seleccionamos *Edit>Virtual Network Editor*. Por defecto nos muestra dos adaptadores de red correspondientes a host-only y NAT. Podemos usar los mismos y configurarlos con lo que necesitemos o bien eliminarlos y comenzar una configuración nueva. Si observamos las direcciones IPs de las subredes que muestra el editor son clase C, puesto que son direcciones asignadas automáticamente en base a nuestro host.



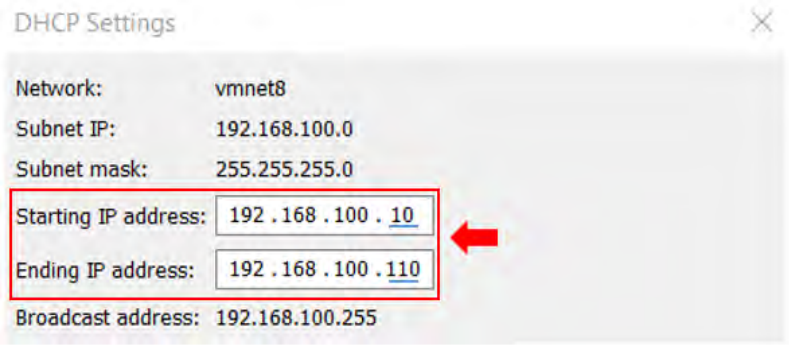
2. Lo que sigue ahora es definir el adaptador de red que tendrán las máquinas virtuales y el rango de red que tendrán los equipos, por lo tanto, usaremos el VMnet8 para el modo de red NAT. También se deberá marcar que el host se conecte a un adaptador virtual y que la asignación de IPs sea por DHCP. Por lo tanto, asignamos la red en 192.168.100.0/24 y aplicamos los cambios.



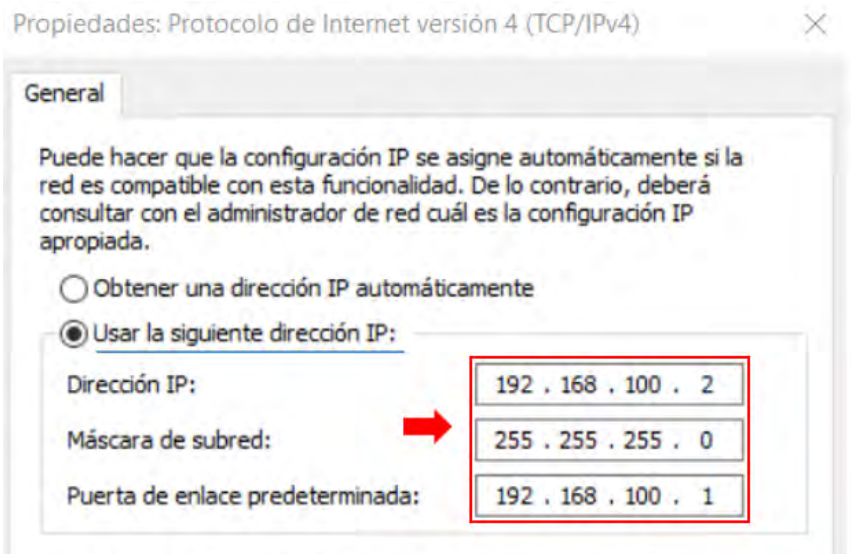
3. También se deberá de configurar los parámetros de NAT Y DHCP:
   - Para el caso de NAT, la puerta de enlace (Gateway IP) será 1 debido a que es la que se usa por defecto, es decir, se deberá asignar 192.168.100.1.

   - En el caso la configuración de DHCP, limitaremos la asignación de direcciones IPs a 100 hosts, ya que no hay muchos equipos, sabiendo que se debe descontar las direcciones asignadas para el gateway, broadcast y el adaptador virtual de VMware en el host anfitrión.

De esta forma, DHCP irá asignando direcciones IPS empezando desde la 10 a la 110 únicamente.

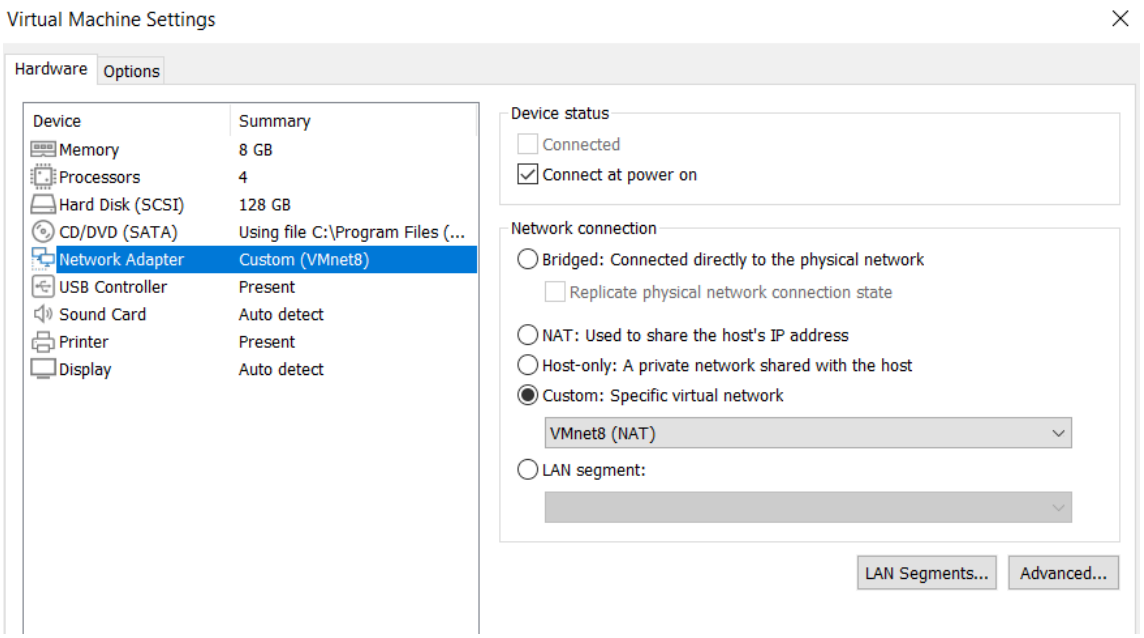


4. Guardamos los cambios y con esto ya tendremos configurado el adaptador NAT. Ahora nos dirigimos a nuestro equipo host y configuraremos el *Adaptador de Red Virtual de VMware VMnet8.* Para ello nos vamos al *Panel de control>Redes e Internet>Conexiones de red,* y luego en el adaptador de red seleccionamos sus propiedades y posteriormente propiedades del *Protocolo de Internet versión 4 (TCP/IPv4)*. Posteriormente configuraremos la IP estática, su máscara de subred y la puerta de enlace, y como paso opcional agregaremos los DNS de Google, puesto que son muy seguros.

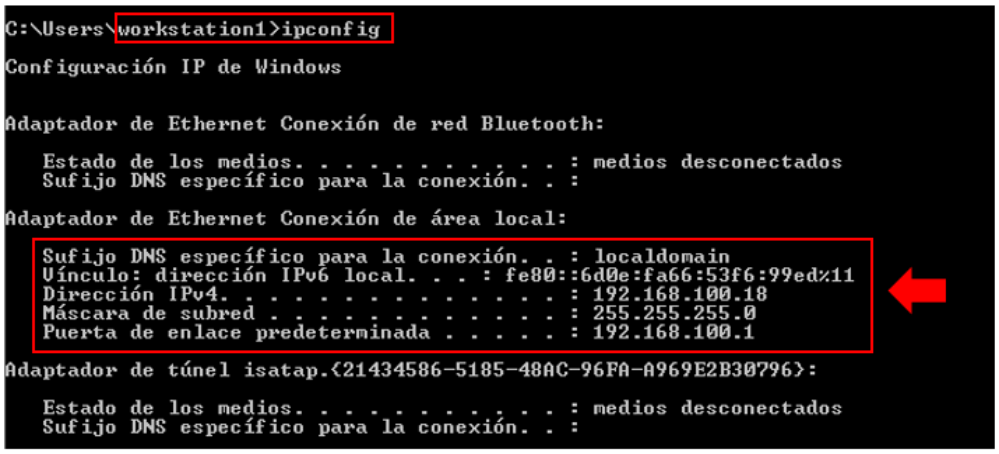


5. Ahora debemos asignar a cada máquina virtual el adaptador de red configurado para que se asignen las direcciones IPs correspondiente, es decir, cada máquina tendrá que ser conectada al adaptador de red VMnet8 de NAT. Para esto, nos situamos en cualquier máquina virtual y luego accedemos a sus propiedades y en las opciones de hardware marcaremos el adaptador de red (Network Adapter) y posteriormente buscaremos la red virtual VMnet8 (NAT), es decir Custom.

Guardamos los cambios y con esto ya estaría vinculado el adaptador de red. Repetimos todo este proceso para cada una de las máquinas virtuales que tengamos.

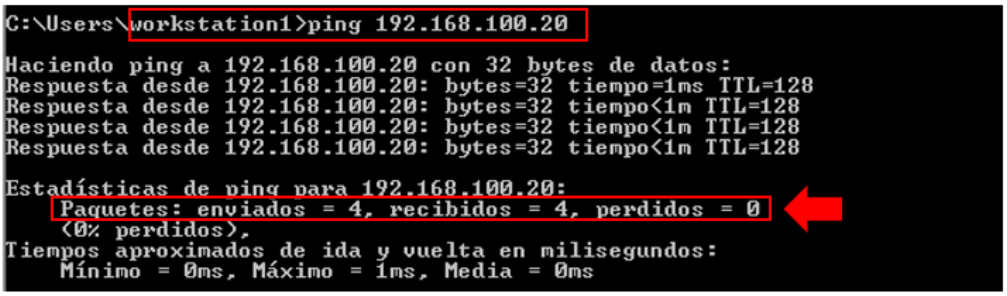


6. Listo con esto ya quedo todo configurado, ahora solo resta verificar las direcciones IPs asignadas a las máquinas virtuales y su conectividad con los otros equipos de la red. Para ejemplificar esto de una manera rápida y sencilla, tomaremos de la red 1, el primer equipo (osea la workstation1) y a partir de este host veremos como quedó configurado. Si observamos la siguiente imagen vemos que las direcciones IPs que aparecen son las que definimos en nuestro VMware, tanto de la red como del host asignado por DHCP. Por lo tanto la asignación está bien configurada.

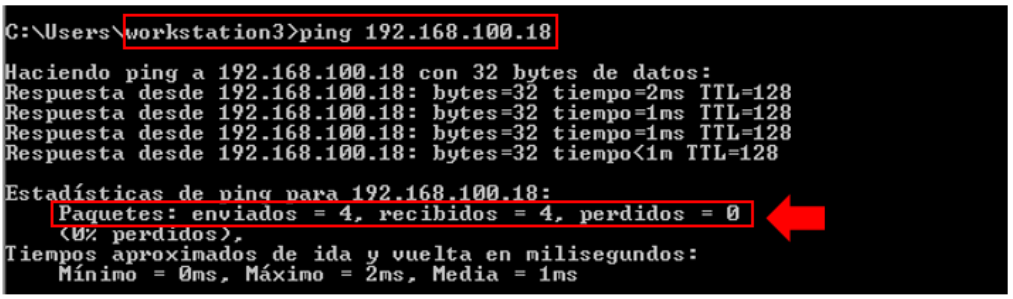


Luego, para ver la conectividad de este equipo (workstation1) con el resto de los equipos, tanto en su misma red como con la red 3 de servidores se deberá utilizar el comando *Ping* seguido de la dirección IP a la que queremos llegar. Las siguiente imágen muestra la verificación:

De la red 1 (workstation1) nos vamos a la misma red (workstation3):



Si hacemos el proceso inverso, también tenemos conexion:



Repetimos el proceso para todas las máquinas virtuales. De esta forma podemos concluir que todos los hosts de la red tienen conexión, es decir el equipo workstation1 de la red 1 se puede comunicar con el resto de equipos en su misma red y con los equipos servidores de la red 3. Y si tomamos cualquier otro equipo, sea workstation4, server2 u otros pasará lo mismo, todas tendrán conexión.

En un caso particular, si dentro de la red quisiéramos que solo un equipo tenga acceso a Internet y el resto solo tenga comunicación, el proceso es medianamente fácil. Para esto, solo un equipo se configura con NAT y el resto de equipos se cambia el adaptador de red por un host-only. Toda esta configuración como vimos en este anexo, se hace mediante el editor de redes virtuales.

9.8 ANEXO 08: INSTALACIÓN DE T-POT EN VMWARE WORKSTATION

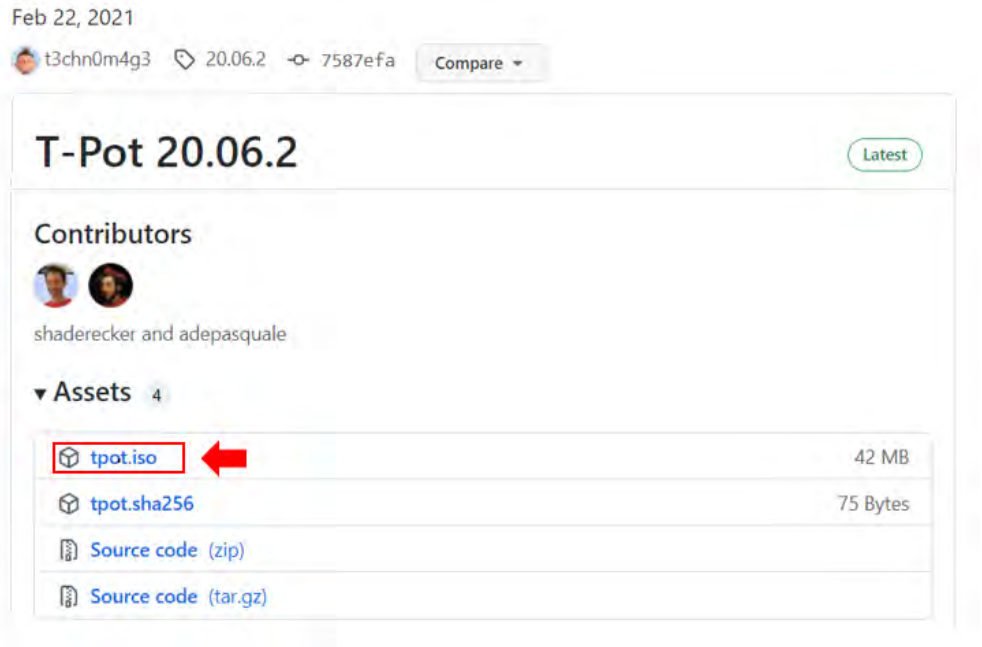
T-Pot es un programa de instalación de red basado en Linux, específicamente en Debian, que posee un sin fin de características y funcionalidades que lo hacen destacar del resto. Durante la instalación se verá que T-Pot ofrece 3 tipos o modos de instalación, y según lo que uno necesite o los objetivos que desee cumplir, se seleccionará uno u otro sistema.

Requisitos mínimos

- 8GB de memoria RAM.
- 128GB de almacenamiento en disco.
- Procesadores Intel o AMD con doble núcleo.

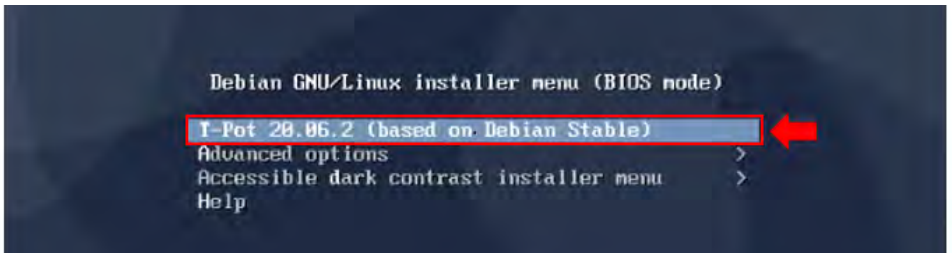
Proceso de instalación

1. Descargamos desde el repositorio oficial de *Telekom-Security* la imagen ISO en su última versión estable del honeypot T-Pot. Dentro de este repositorio, nos dirigimos a la sección de release y descargamos la imagen ISO https://github.com/telekom-security/tpotce/releases/tag/20.06.2.

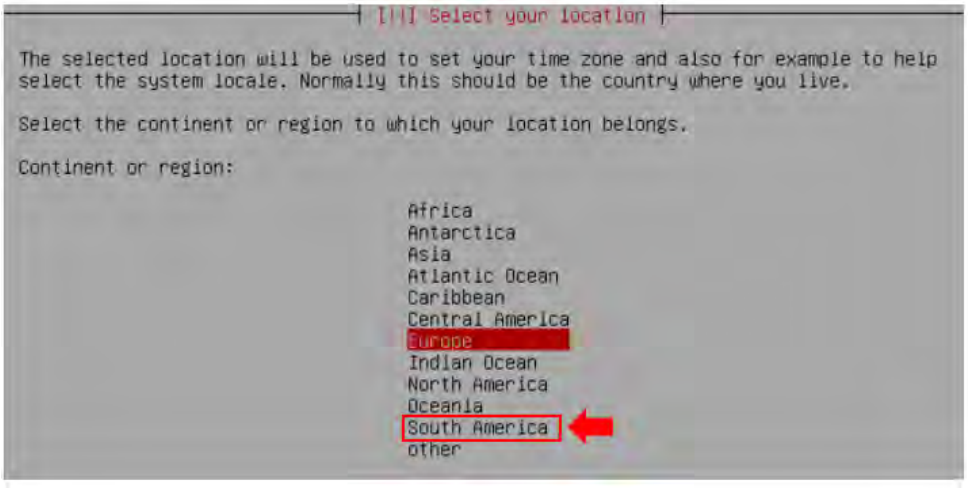


2. Luego preparamos nuestra máquina virtual el cual alojará nuestro honeypot. Además, esta máquina virtual deberá ser creada según los requerimientos de hardware y software que establecimos para este honeypot. Cuando creemos la máquina virtual, esta debe estar basada en Debian o bien en alguna distribución de Ubuntu para evitar posibles errores durante la instalación.

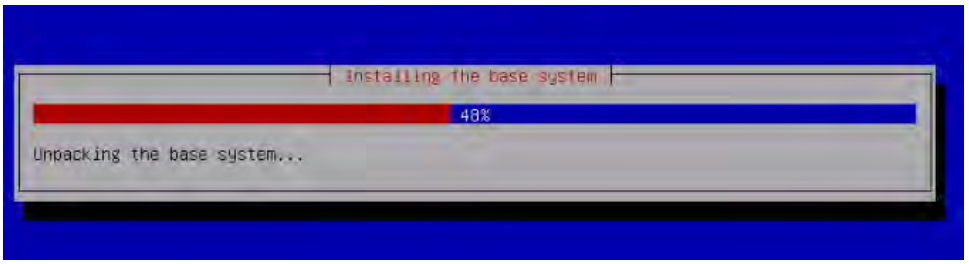
3. Ejecutamos nuestra máquina virtual con la imagen ISO de T-Pot previamente cargada. En el grub que nos aparece seleccionamos la primera opción.



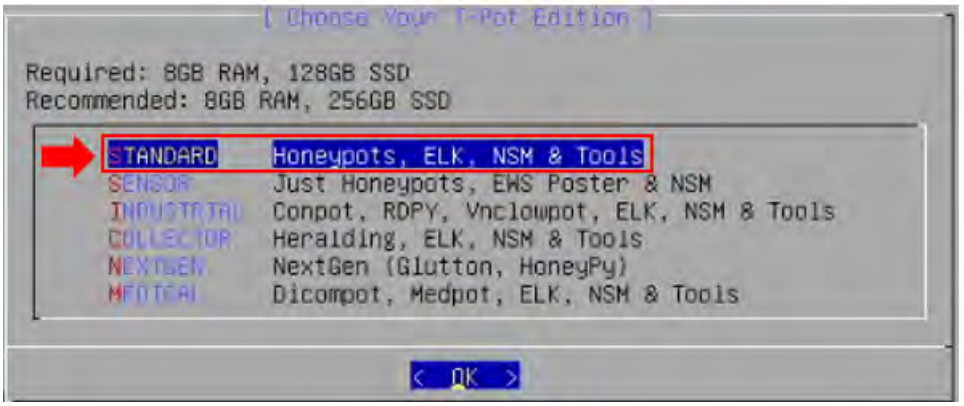
4. A partir de ahora, configuraremos una serie de pantallas que tienen que ver con nuestra ubicación, lenguaje, zona horaria e idioma de nuestro teclado.



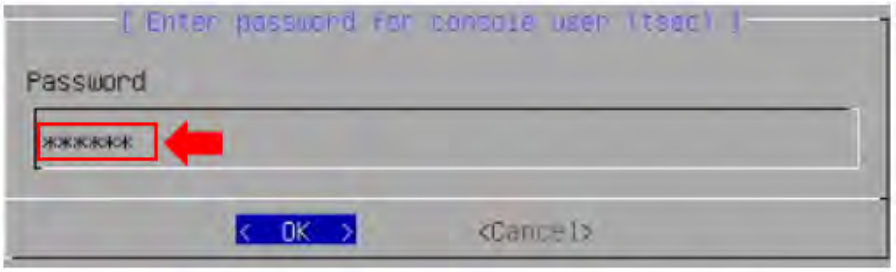
5. Luego nos pedirá cierta configuración acerca del servidor Debian y si se utilizará algún proxy. Pero por ahora dejamos todo por defecto. Una vez configurado, empezará a instalar el sistema base y ciertos componentes que necesita.



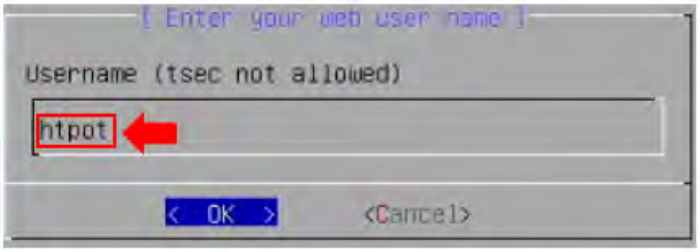
6. En esta pantalla debemos elegir el modo o tipo de instalación que queremos según los objetivos que tengamos. Como se observa podremos seleccionar entre cinco tipos de instalación, cada uno con las herramientas que trae de base y además nos indica los requisitos necesarios, por lo que si no cumplimos con esto, la instalación se cancelará automáticamente. Para este proyecto solo basta con una instalación *Standard.*

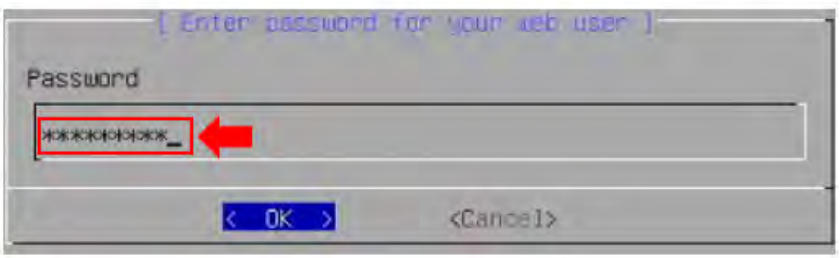


7. Este honeypot contará con dos usuarios, uno es *tsec* un usuario que ya viene por defecto con el sistema y que solo deberemos generar una contraseña y otro usuario que deberemos generar nosotros, también con su respectiva contraseña de acceso. Anotar bien las claves y nombres de acceso de estos usuarios, ya que sin ellos no podremos hacer nada.



El usuario *tsec* básicamente nos servirá para administrar todas las configuraciones nativas que tiene el honeypot T-Pot, como por ejemplo ver los servicios que tiene habilitado, las aplicaciones disponibles, el almacenamiento del sistema, redes con las que está conectada, etc. Mientras que el nuevo usuario (en este caso *htpot*) solo nos permitirá ingresar a la plataforma web (dashboard) para ver todos los paneles de administración.





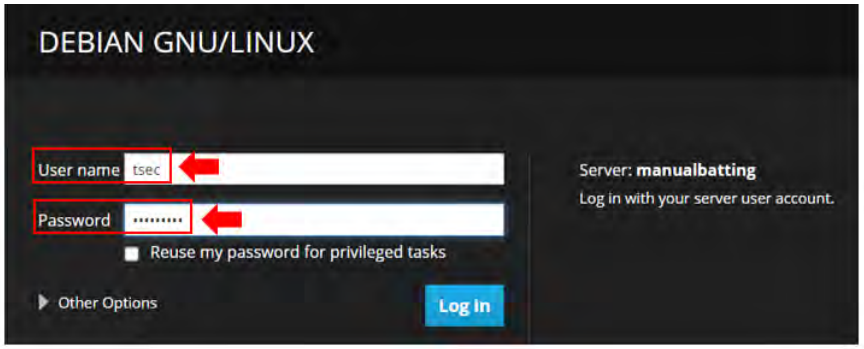
8. Finalmente ahora empieza el proceso detallado de la instalación del honeypot. Este proceso podría durar aproximadamente 30 minutos, dependiendo siempre del buen funcionamiento de internet y de los recursos que tengamos en nuestro equipo. Luego la máquina se reiniciará cuando la instalación finalice.

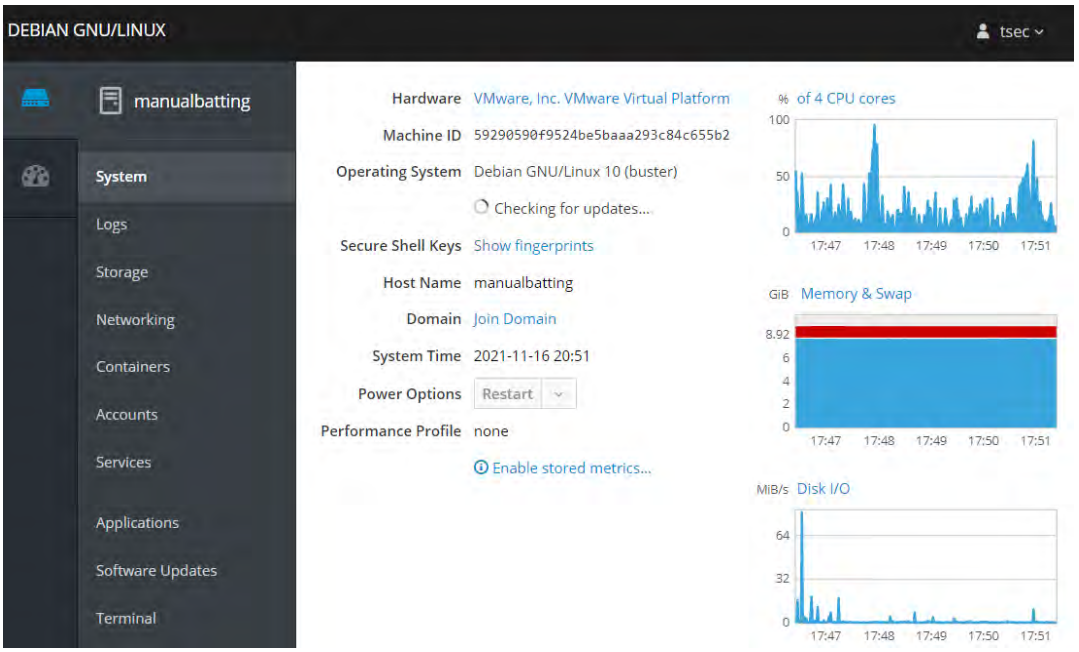
9. Una vez instalado, nos aparecerá la pantalla de consola con el servidor activo del honeypot T-Pot. La pantalla mostrará la versión del honeypot y las direcciones IPs correspondientes para poder ingresar a los diferentes paneles de administración. Una vez que está activo el T-Pot, también deberemos de loguearnos con el usuario tsec, puesto que si no lo hacemos, no podremos ingresar al consola de configuración del T-Pot.

10. Con esto ya tenemos activo y funcionando nuestro honeypot T-Pot y para acceder a cualquiera de sus administradores web, solo basta con ingresar con las direcciones IPs que nos otorgó el sistema.

    a. *Administración y configuración del servidor T-Pot:* https://192.168.100.11:64294

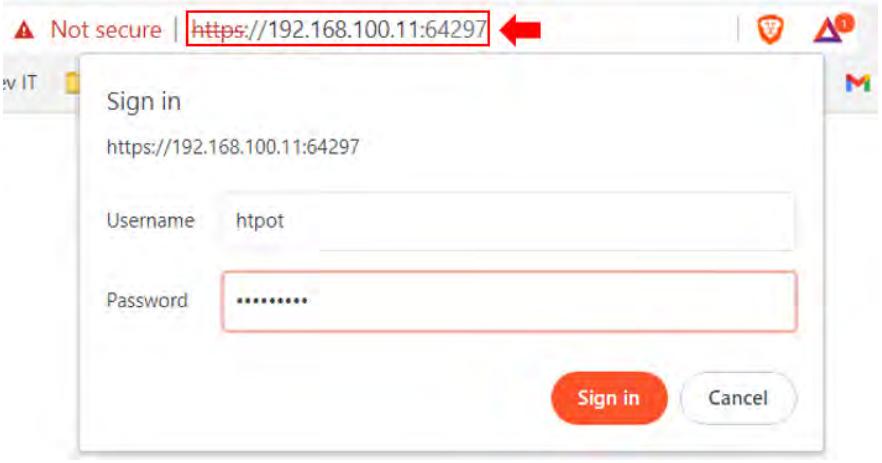
    Aquí se podrá gestionar de manera general varios aspectos del servidor en relación al sistema, los logs, almacenamiento, servicios, aplicaciones, despliegue de honeypots, entre otros. Por lo tanto, este es un aspecto que se debe configurar previamente antes de su uso.



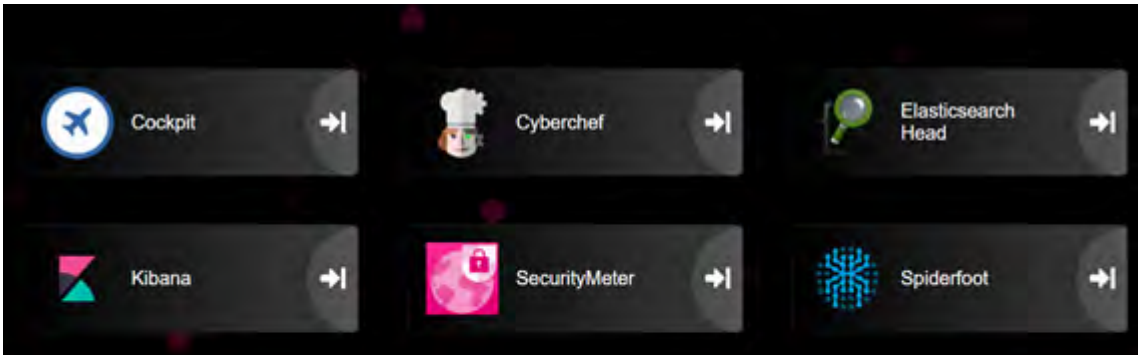


    b. *Administrador web (dashboard) T-Pot:* https://192.168.100.11:64297

    Por otro lado, esta plataforma web, nos ofrece muchos aplicativos y servicios con los cuales podremos trabajar. Muchos de estos aplicativos ya vienen preinstalados, mientras que otros podrán ser instalados cuando se configure el servidor T-Pot que explicamos anteriormente. Aquí nos logueamos con el usuario que creamos durante la instalación del honeypot.



La interfaz que se presenta es muy amigable y fácil de entender. Se tiene muchos dashboards y paneles de monitorización en los cuales se podrá analizar todos los datos recabados de los ciberdelincuentes y lo bueno es que todos estos análisis y ataques realizados se pueden ver en tiempo real, mostrando mucho información realmente relevante para el profesional IT, para que en base a ello, se puedan tomar las mejores decisiones para la mitigación de ataques.



9.9 ANEXO 09: INSTALACIÓN DE T-POT EN UN SERVIDOR VIRTUAL PRIVADO

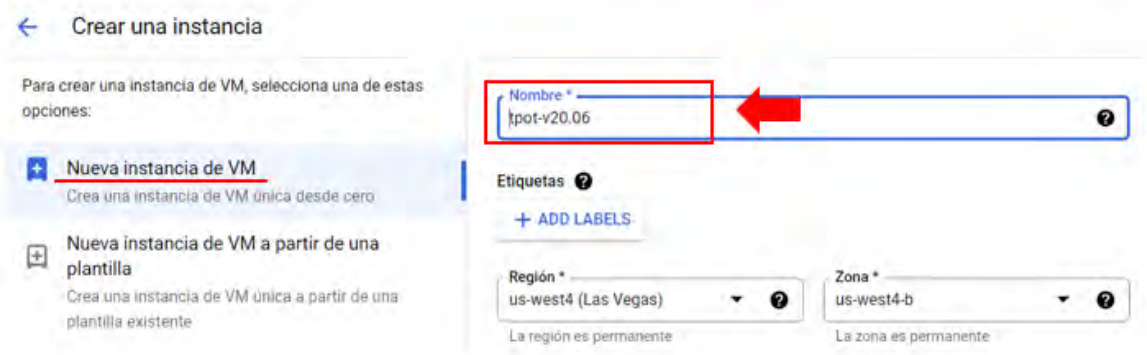
Para este tipo de instalación, las configuraciones no cambian mucho en comparación al *Anexo 08*, donde instalamos el honeypot en el hipervisor VMware. En este caso, vamos a utilizar un VPS de Google Cloud Platform por las prestaciones que nos ofrece, aunque se puede utilizar cualquier otro proveedor. Si bien los precios de Google Cloud pueden resultar caros para algunos, lo bueno es que al hacerlo se dispondrá de una suite de herramientas, lo cual será muy fructífero para futuros proyectos, pero todo queda en manos del usuario o de la empresa en cuestión.

Requisitos mínimos

- 8GB de memoria RAM.
- 128GB de almacenamiento en disco.
- Procesadores Intel o AMD con doble núcleo.

Proceso de instalación

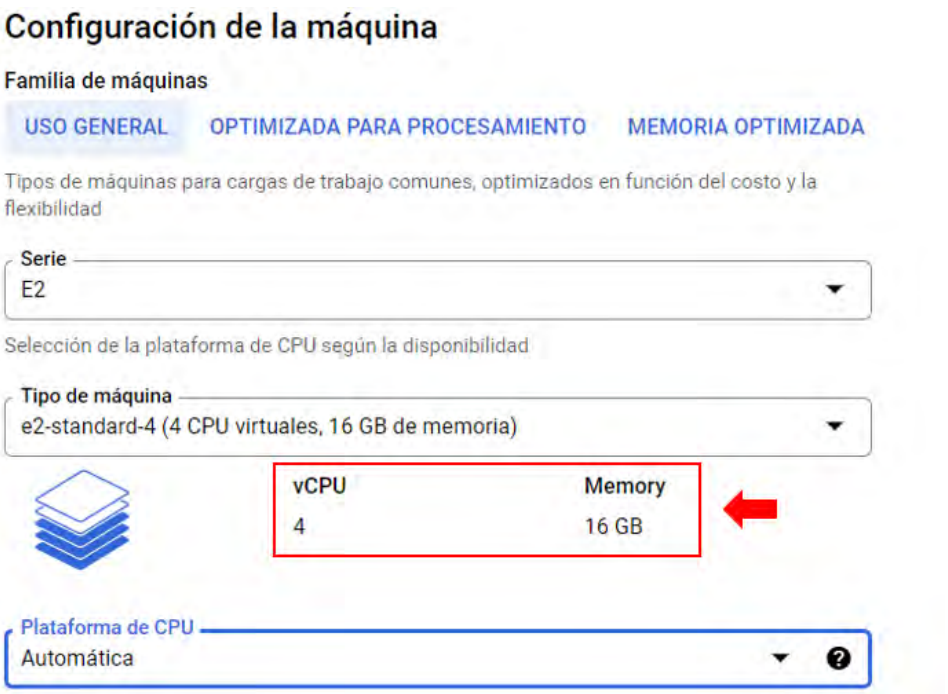
1. Dentro de la plataforma de Google Cloud Platform crearemos previamente una máquina virtual en un servidor Debian 10, o en su defecto en Ubuntu. Para ello, dentro de la plataforma nos dirigimos a la opción de *Compute Engine>Crear una instancia de VM.* Le asignamos un nombre para identificar el servidor que contendrá el honeypot, y en las opciones de región y zona lo dejamos por defecto.



2. Antes de proceder, es conveniente configurar el firewall de este VPS, puesto que si no lo hacemos podrán llegar a presentarse algunos errores irreversibles. Solo bastará con agregar las siguientes reglas de entrada en el firewall y en algunos casos configurar que solo nosotros tengamos acceso. Esta configuración se encuentra dentro de la opción de *Red VPC>Firewall.*

Nombre	Tipo	Destinos	Filtros	Protocolos/puertos	Acción	Prioridad
tpot-access-dashboard	Entrada	Aplicar a todas	Intervalos de IP: 186.136.192.106/32	tcp:64297	Permitir	1000
tpot-access-ports	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	all	Permitir	1000
tpot-access-ssh	Entrada	Aplicar a todas	Intervalos de IP: 186.136.192.106/32	tcp:64295	Permitir	1000
default-allow-icmp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	icmp	Permitir	65534
default-allow-internal	Entrada	Aplicar a todas	Intervalos de IP: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Permitir	65534
default-allow-rdp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:3389	Permitir	65534
default-allow-ssh	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:22	Permitir	65534

3. Ahora, se deberá especificar los requisitos de hardware que tendrá el servidor T-Pot. Si bien en los requisitos mínimos ya especificados con 8GB de memoria RAM era suficiente, aquí el hardware va a cambiar, puesto que Google Cloud Platform ofrece otras configuraciones, por lo que elegiremos la opción más próxima.

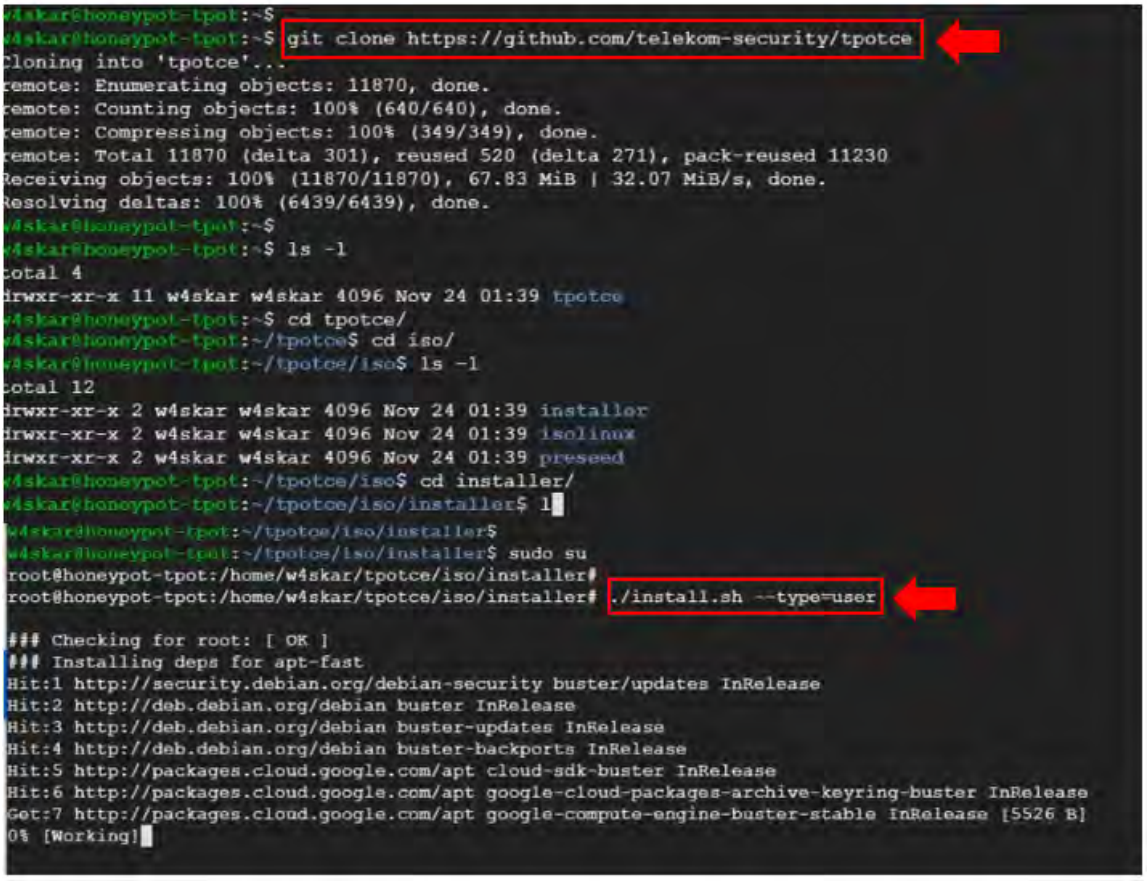


4. Por último, la opción de *Identidad y acceso a la API* lo dejamos con los valores por defecto. Solo en el firewall tildamos las dos opciones, para poder permitir el tráfico de HTTP y HTTPS. Finalmente creamos la máquina virtual.

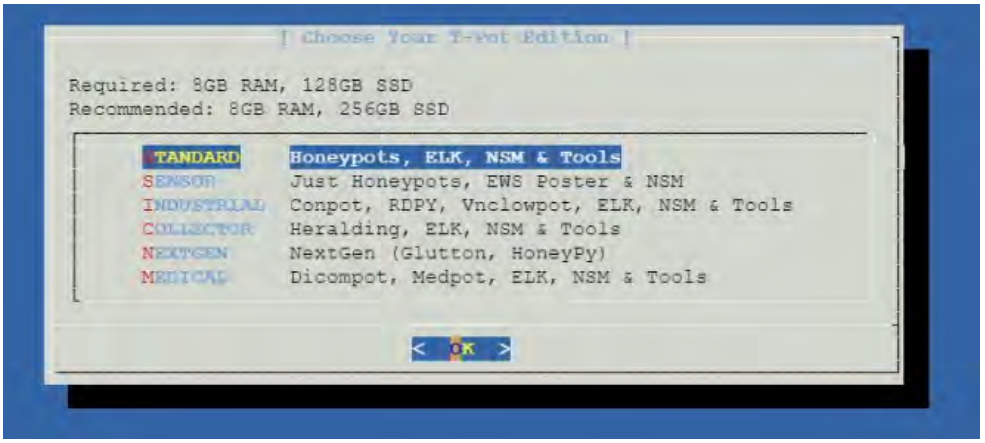
Nombre	Zona	Tipo de máquina	IP interna	IP externa
tpot-honeypot	us-west4-b	e2-standard-4	10.182.0.6 (nic0)	34.125.199.232

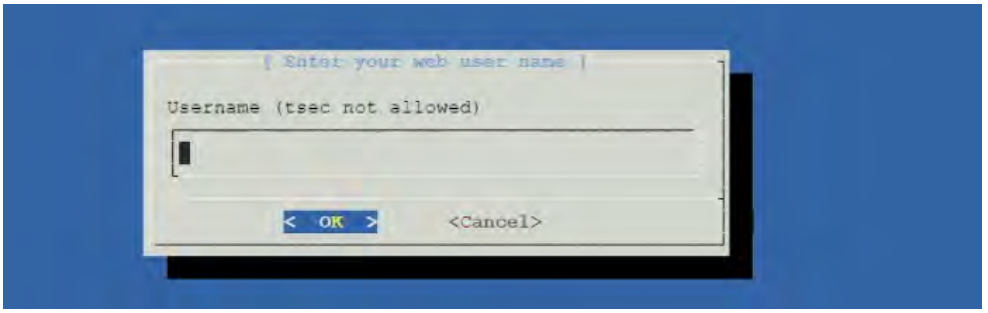
5. Ahora instalaremos el honeypot. Para ello, desde la consola de Google Cloud Platform accedemos al SSH del servidor. Para este caso, no hace falta tener la ISO de T-Pot, ya que al mismo lo bajaremos de Internet mediante su repositorio. Antes de continuar con la instalación deberemos de actualizar los repositorios, paquetes e instalar github, mediante sus comandos respectivos.

6. Si todo esto está listo, procedemos con la instalación del honeypot. El instructivo de los comandos de T-Pot que se emplearán se encuentra en la web oficial de Telekom-Security.

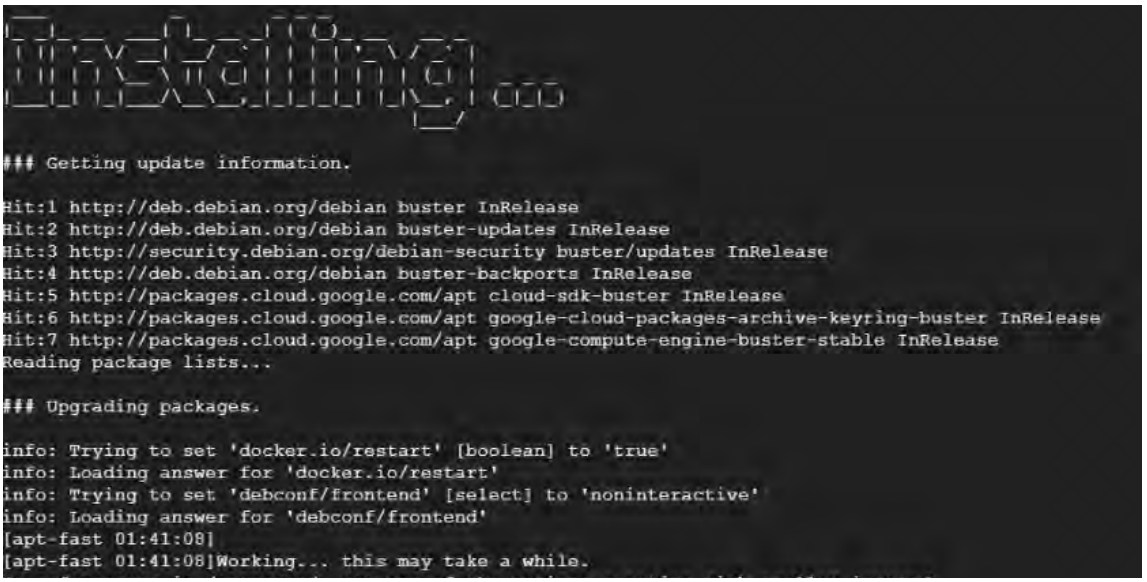


7. Durante la instalación, nos pedirá que seleccionemos el tipo de honeypot a instalar, en este caso seleccionaremos *standard* y tambien nos pedira que generemos los datos de logueo (nombre de usuario y contraseña) para que posteriormente cuando concluya la instalación podamos acceder a los diferentes administradores del honeypot



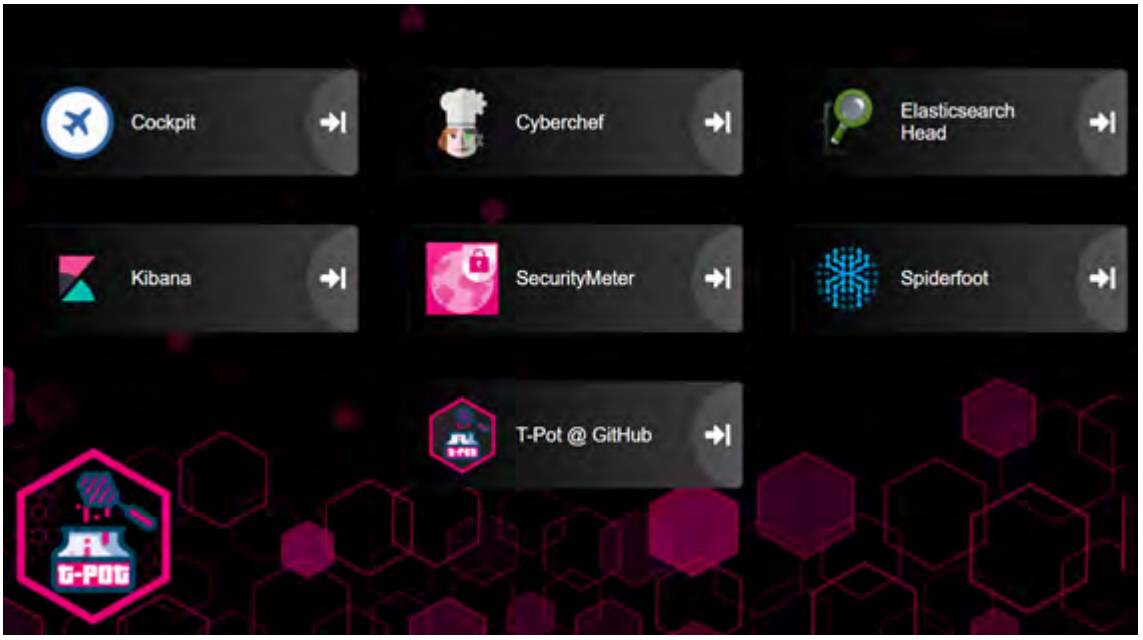


8. Ahora empieza a realizarse la instalación del honeypot en cuestión. Esta acción puede demorar alrededor de 20 a 40 minutos.



9. Una vez instalado, ya estaremos en condiciones de acceder al honeypot. Para ello nos dirigimos a un navegador y accedemos a la IP que nos otorgó el servidor virtual, es decir 34.125.199.232.

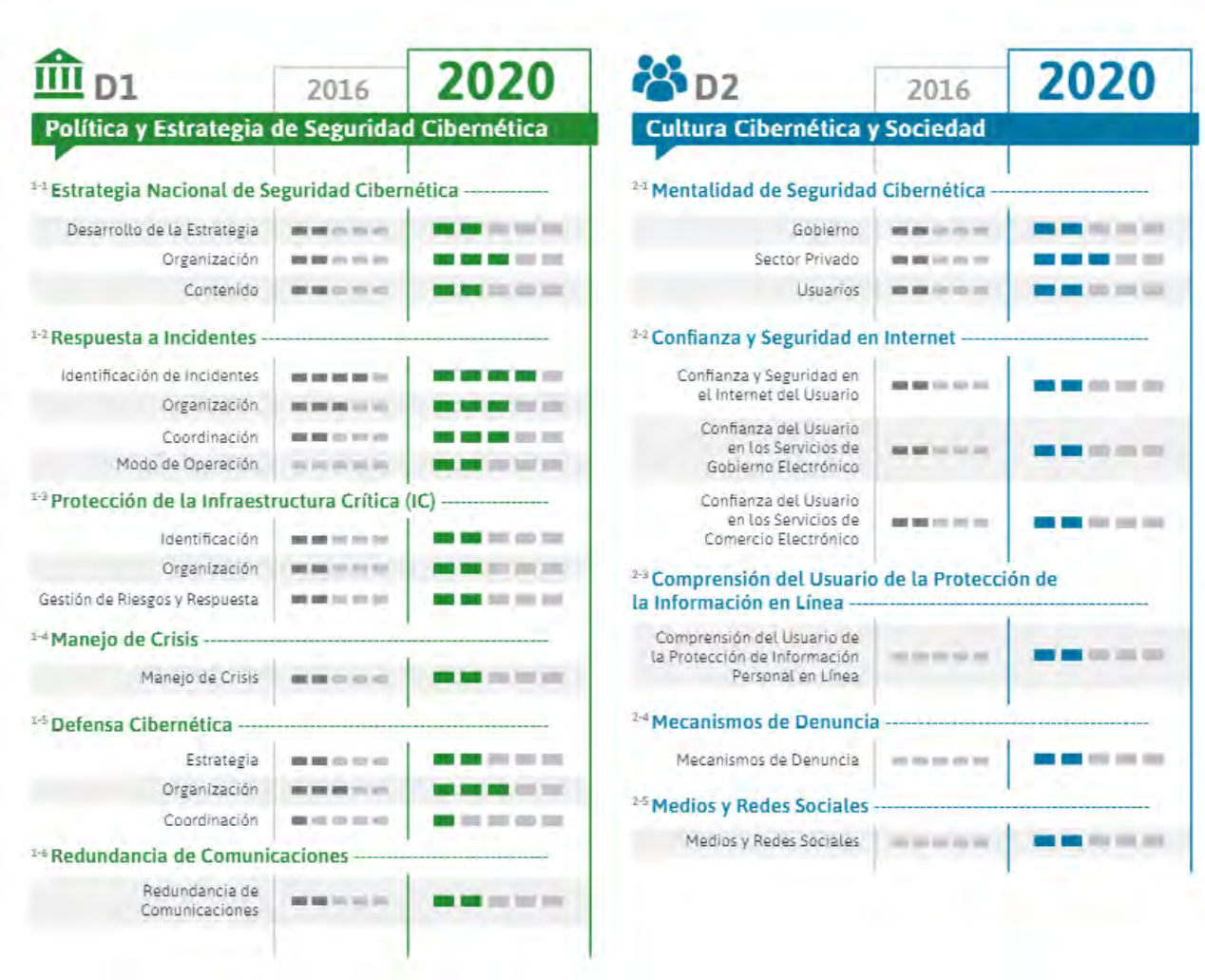
Los puertos de T-Pot siempre serán los mismos, puesto que ya están definidos por la empresa Telekom-Security, lo único que cambiará es nuestra dirección IP. Para acceder nos logueamos con los datos que pusimos durante la instalación y listo, ya tenemos funcionando el honeypot.



10. Como configuración final, en la plataforma de Google Cloud, deberemos de establecer la dirección IP que utiliza T-Pot a fija, ya que sino cada que reiniciemos se obtendrá una IP distinta, y esto puede resultar muy tedioso. Lo mejor es especificar una que ya quede fija.

9.10 ANEXO 10: INDICADORES DE CIBERSEGURIDAD ARGENTINA 2020

Este reporte fue realizado por el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos, brindando de esta forma un panorama detallado y actualizado de las políticas y prácticas de ciberseguridad en Argentina, ofreciendo una perspectiva sobre el progreso alcanzado desde su primera edición en 2016.




D3
2016
2020
Formación, Capacitación y Habilidades de Seguridad Cibernética
3-1 Sensibilización
Programas de Sensibilización
Sensibilización Ejecutiva
3-2 Marco para la Formación
Provisión
Administración
3-3 Marco para la Capacitación Profesional
Provisión
Apropiación
D4
2016
2020
Marcos Legales y Regulatorios
4-1 Marcos Legales
Marcos Legislativos para la Seguridad de las TIC
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
Legislación Sobre Protección de Datos
Protección Infantil en Línea
Legislación de Protección al Consumidor
Legislación de Propiedad Intelectual
Legislación Sustantiva Contra el Delito Cibernético
Legislación Procesal Contra el Delito Cibernético
4-2 Sistema de Justicia Penal
Fuerzas del Orden
Enjuiciamiento
Tribunales
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
Cooperación Formal
Cooperación Informal
D5
2016
2020
Estándares, Organizaciones y Tecnologías
5-1 Cumplimiento de los Estándares
Estándares de Seguridad de las TIC
Estándares en Adquisiciones
Estándares en el Desarrollo de Software
5-2 Resiliencia de la Infraestructura de Internet
Resiliencia de la Infraestructura de Internet
5-3 Calidad del Software
Calidad del Software
5-4 Controles Técnicos de Seguridad
Controles Técnicos de Seguridad
5-5 Controles Criptográficos
Controles Criptográficos
5-6 Mercado de Seguridad Cibernética
Tecnologías de Seguridad Cibernética
Seguro Cibernético
5-7 Divulgación Responsable
Divulgación Responsable

9.11 ANEXO 11: ATAQUES FRECUENTES PARA PRUEBAS DE PENTESTING

1. *Hydra*

   Es una herramienta de descifrado de contraseña de fuerza bruta de código abierto desarrollada por el conocido grupo de hackers THC, que puede descifrar múltiples contraseñas en línea, y se ha incluido en plataformas de infiltración como Backtrack y Kali Linux. Puede descifrar uno o una lista de nombres de usuario/ contraseñas mediante el método de fuerza bruta. (ProgrammerClick, 2017).

2. *Metasploit*

   Es un proyecto de código abierto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración. Esta herramienta, no solo puede verificar vulnerabilidades, administrar evaluaciones de seguridad y aumentar la conciencia de seguridad, sino que también puede ayudar a los equipos de seguridad a hacer más. (Codetd, 2020).

3. *Ncrack*

   Esta herramienta de crackeo de autenticación en red de alta velocidad, fue construida para ayudar a las compañías a proteger sus redes probando todos sus hosts y dispositivos de red contra las contraseñas débiles. Los profesionales de la seguridad también confían en Ncrack al auditar a sus clientes. Fue diseñado utilizando un enfoque modular, una sintaxis de línea de comandos similar a nmap y un motor dinámico que puede adaptar su comportamiento basado en la retroalimentación de la red. Las características de Ncrack incluyen una interfaz muy flexible que otorga al usuario un control total de las operaciones de la red, permitiendo ataques muy sofisticados, plantillas de temporización para facilitar su uso, interacción en tiempo de ejecución similar a nmap y muchos más. (SecurityHackLabs, 2018).

4. *Burp Suite*

   Es un conjunto de herramientas esencial para los pentesters, ya que viene con funciones rápidas y confiables. Está diseñado por las funciones de prueba de seguridad manuales y semiautomatizadas de los expertos. Es una herramienta diseñada realmente para probar servicios, no para piratear, como muchos otros. Por lo tanto, registra secuencias de autenticación complejas y escribe informes para que los usuarios finales los utilicen directamente y los compartan. (Zaher Talab, 2021).

5. *Hashcat*

   Es la utilidad de recuperación de contraseñas más rápida y avanzada del mundo, compatible con 5 modos únicos de ataque para más de 200 algoritmos de hash altamente optimizados. Admite CPU, GPU y otros aceleradores de hardware en Linux, Windows y macOS, y además tiene instalaciones para ayudar a habilitar el descifrado de contraseñas distribuidas. (Ethical Hacking Group, 2019).

6. *Secure Shell Bruteforcer (SSB)*

   Es una de las herramientas más rápidas y sencillas para servidores SSH de fuerza bruta. El uso de SSB le brinda una interfaz adecuada, a diferencia de otras herramientas que descifran la contraseña de un servidor SSH. (Zaher Talab, 2021).

7. *SlowHHTPTest*

   Este tipo de ataques se basan en que el protocolo HTTP, que por diseño, requiere que las peticiones que le llegan sean completas antes de que puedan ser procesadas. Si una petición HTTP no es completa o si el ratio de transferencia es muy bajo el servidor mantiene sus recursos ocupados esperando a que lleguen el resto de datos. Si el servidor mantiene muchos recursos en uso podría producirse una denegación de servicio (DoS). Estos tipos de ataque son fáciles de ejecutar debido a que una sola máquina es capaz de establecer miles de conexiones a un servidor y generar miles de peticiones HTTP sin terminar en un período muy corto de tiempo utilizando un ancho de banda mínimo. (Segu-Info, 2016).

8. *Pydictor*

   Es otra gran herramienta poderosa para piratear diccionarios. Cuando se trata de pruebas largas y de seguridad de contraseñas, puede sorprender tanto a los principiantes como a los profesionales. Es una herramienta que los atacantes no pueden distribuir en su arsenal. Además, tiene un exceso de funciones que le permiten disfrutar de un rendimiento realmente sólido en cualquier situación de prueba. (Zaher Talab, 2021).

9.12 ANEXO 12: METASPLOIT CON KALI LINUX

Un Metasploit es un conjunto de herramientas con las que un pentester puede desarrollar y ejecutar exploits y lanzarlos contra máquinas para comprobar la seguridad de estas. Esta herramienta incluye una gran colección de exploits, siendo utilizada en gran parte por los auditores de seguridad debido a su fácil implementación con otras herramientas tales como nmap, escáneres de vulnerabilidades, entre otros. Es una infraestructura que puede ser personalizada y utilizada para necesidades específicas. (David, 2018).

Además el autor en su artículo explica que, para comprender mejor el Metasploit, es necesario conocer y tener bien en claro las siguientes definiciones:

- *Exploit*: Es un código escrito con el fin de aprovechar un error de programación y con la intención de conseguir ciertos privilegios en el sistema o software vulnerado. Normalmente con el uso de los exploits se busca tomar control de la máquina víctima. Un ejemplo de cómo usar un exploit de Metasploit, para explotar la vulnerabilidad que utilizaba la NSA para tener acceso a los equipos.

- *Payload*: Es la carga de un exploit la cual se encarga de realizar la parte maliciosa de la intrusión, es decir, es el código remoto que se ejecutará en la máquina vulnerada, así creando una secuencia de actividades maliciosas.

- *0-day exploit*: Es un código malicioso que permite al atacante tener control total sobre un sistema vulnerable, el problema o ventaja de estos exploits es que no son conocidos por los usuarios o por los fabricantes, es decir que quedan completamente expuestos al ataque. Normalmente existe un tiempo de corrección desde que se descubre hasta que se soluciona.

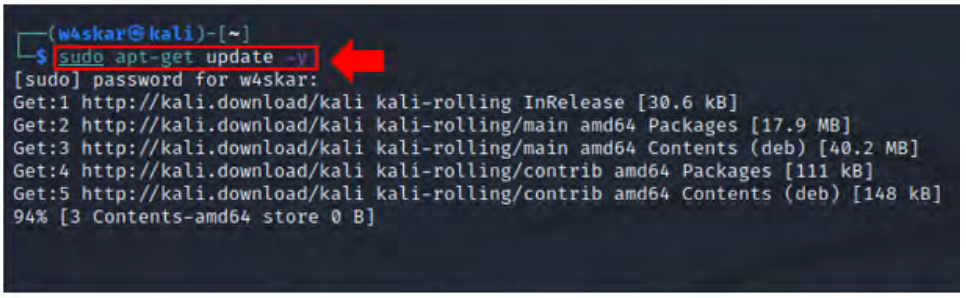
- *Módulos*: Es un conjunto de funcionalidades que hacen que sean más sencillas de utilizar. Como podría ser un exploit o un escaneo. Existen diferentes tipos de módulos.

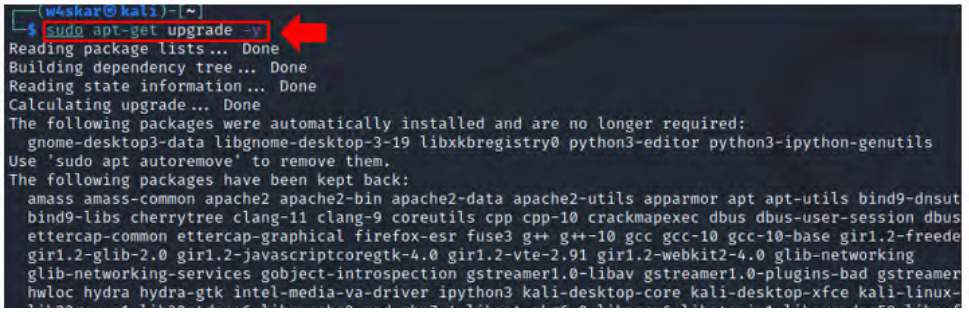
    - Auxiliary: Proporciona herramientas externas tal como escáneres o sniffers.
    - Exploits: Este es el más conocido, se encuentran todos los exploits.
    - Payloads: Almacena los distintos códigos maliciosos a implementar con los exploits.
    - Msfpayload: Generar shellcodes para inyectar junto a los exploits o junto a un software.
    - Msfencode: Se encarga de ocultar el código malicioso a los IDS, antivirus, etc.
    - Msfvenom: Facilita la tarea de generar una shell y ocultarla desde una misma consola.

Proceso de instalación

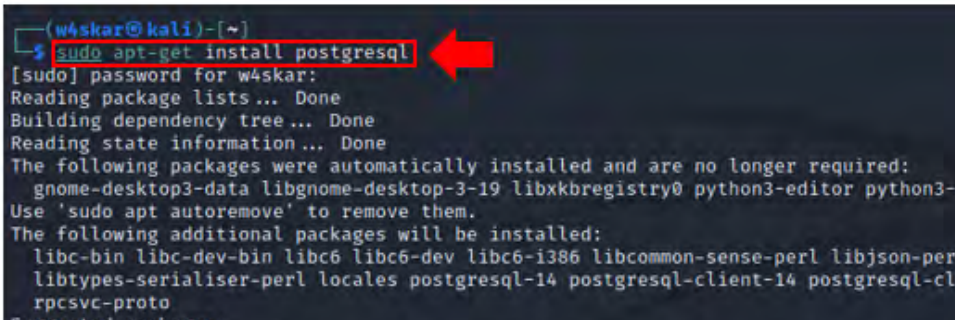
Como ya mencionamos en el proyecto, todas las herramientas de seguridad que estén destinadas para realizar pruebas de pentesting se llevarán a cabo en el equipo ya especificado para tal fin, es decir la máquina virtual VM-02. Este equipo cuenta además con el sistema operativo Kali Linux y solo este será apto para realizar cualquier tipo de prueba.

1. Dentro de Kali Linux, abrimos una consola y actualizamos el sistema y todos los repositorios con los comandos de *update* y *upgrade*.

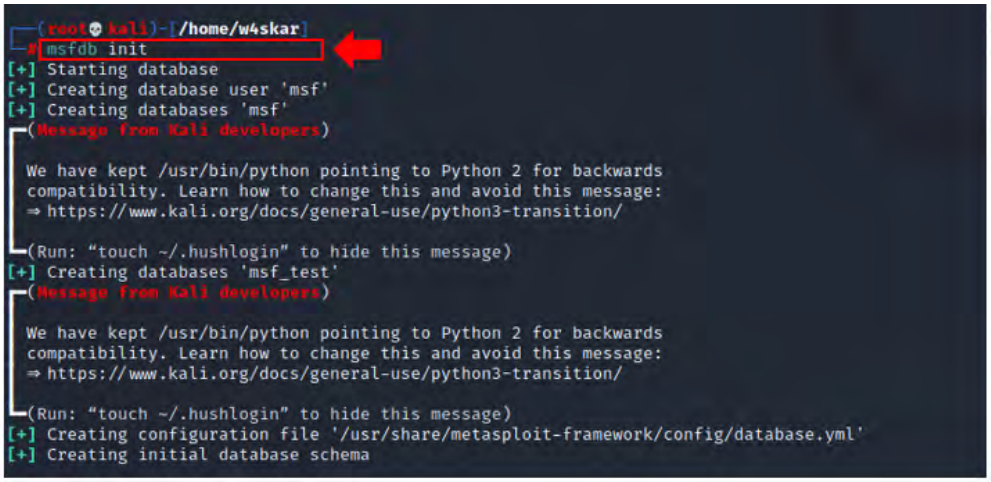




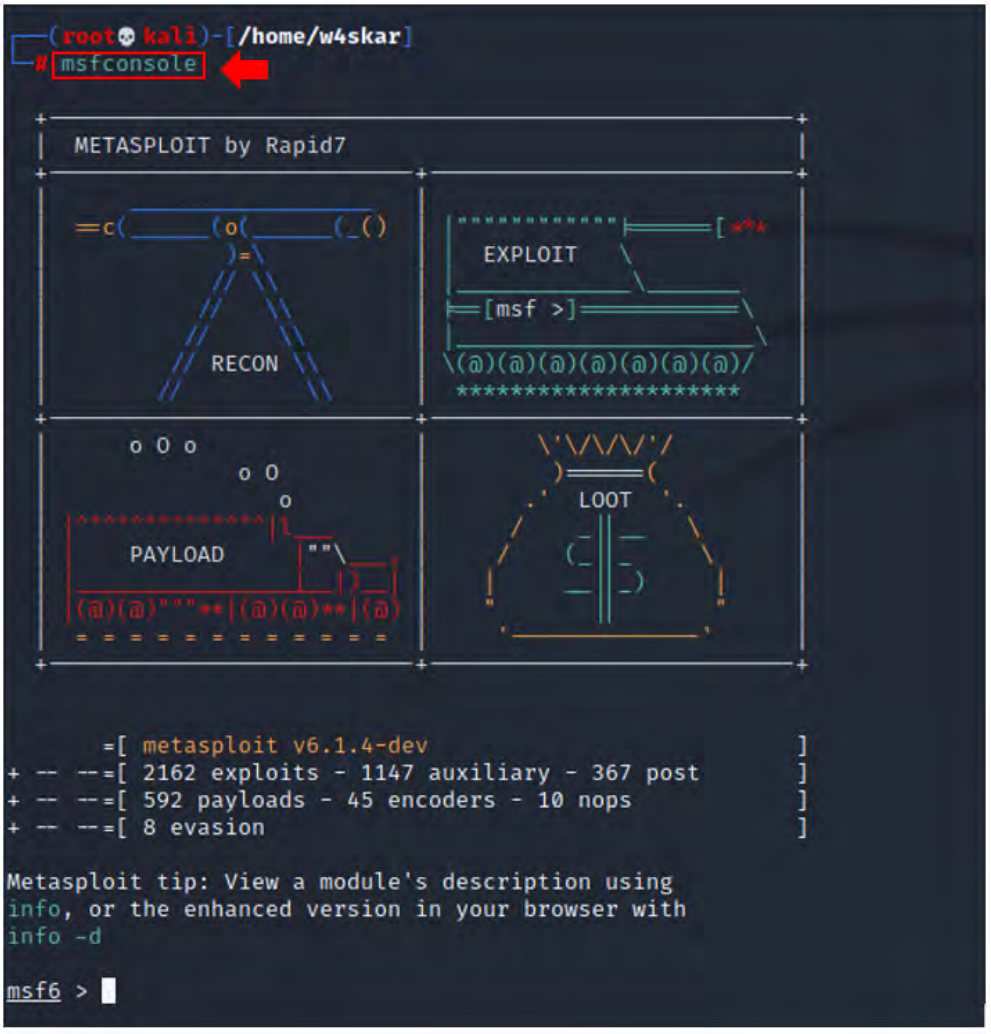
2. Instalamos la base de datos *postgresql.*



3. Luego iniciamos la base de datos para que el metasploit pueda utilizarla. Para ello escribimos en consola *msfdb* para que nos muestre el listado de opciones de la base de datos de postgresql y luego seleccionamos *init* para iniciar tipeando *msfdb init*. Para estas acciones deberemos estar logueado como root o bien ser usuario con privilegios de administrador.



4. Con toda estas configuraciones ya tenemos instalado el metasploit en nuestro sistema, ahora solo queda ejecutarlo en nuestra terminal. A partir de ahora ya podemos empezar a utilizarlo buscando el equipo víctima que vamos a explotar.



CAPÍTULO 10 - GLOSARIO

A.

ACL (Access Control List)

Lista mantenida por un router para controlar el acceso desde o hacia un router para varios servicios. Por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router.(Ruben B. Sanchez, 2005).

Antivirus

Programa encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca. Para realizar este labor existen muchos programas que comprueban los archivos para encontrar el código de virus en su interior. (Cristian Borghello, 2001).

B.

Backup

Copia de seguridad que se realiza con el fin de mantener los datos en forma segura. Es decir, permite tener disponible e íntegra la información para cuando sucedan accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre. (Cristian Borghello, 2001).

Bot

Es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. Forman parte de una red de máquinas infectadas, conocidas como botnet. A las máquinas infectadas también se les conoce por el nombre de zombis. (José Fernández, 2013).

Botnets

Red de computadoras infectadas con software malicioso y que cuenta con funciones de backdoor que permite al atacante controlar dichas máquinas de forma remota. (José Fernández, 2013).

Bug

Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo. (Cristian Borghello, 2001).

C.

Ciberataque

Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para realizar actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema. (INCIBE, 2021).

Ciberdefensa

Es el conjunto de acciones de defensa activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos (Miguel Sanchez, 2015).

Ciberdelincuente

Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos mediante robo, filtración de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos. (INCIBE, 2021).

D.

DHCP (Dynamic Host Configuration Protocol)

Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después. (El blog de Claudio).

DMZ (Demilitarized Zone)

Consiste en una red aislada que se encuentra dentro de la red interna de la organización. Por lo general, una DMZ permite las conexiones procedentes tanto de Internet como de la red local de la empresa, pero las conexiones que van desde la DMZ a la red local no están permitidas. Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad. (INCIBE, 2021).

DNS (Domain Name Service)

Se refiere tanto al servicio de nombres de dominio, como al servidor que ofrece dicho servicio. Su función es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple. (INCIBE, 2021).

Docker

Es una herramienta que permite empaquetar una aplicación y sus dependencias en un contenedor muy ligero. Es decir, nuestra aplicación funcional puede ser transportada sin problema a cualquier otro servidor con Docker instalado para seguir siendo desarrollada o para hacer deploy. Por lo tanto, Docker nos permite correr nuestras aplicaciones en contenedores, cada una con su propia función, sistema operativo y recursos. (Eduardo Zepeda, 2020).

DoS ((Denial of Service)

El ataque de denegación de servicios es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios leegítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o, sobrecarga de los recursos computacionales del sistema de la víctima. (José Fernández, 2013).

E.

Exploit

Es un programa código utilizado con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. No es un código malicioso en sí mismo, generalmente se utiliza para otros fines como permitir el acceso a un sistema no autorizado o como parte del método de propagación del malware. (José Fernández, 2013).

F.

Firewall

La misión de un firewall o cortafuegos es analizar y bloquear cualquier intento de conexión peligrosa con el sistema, habitualmente, desde Internet. Para ello, utiliza un procedimiento de seguridad programado entre una red segura y una red insegura. (Cristian Borghello, 2001).

FTP (File Transfer Protocol)

Protocolo del nivel de usuario para la transferencia de archivos entre computadoras. También pueden hacer referencia a la aplicación que permite transferir archivos de una computadora a otra usando el mismo protocolo. (Cristian Borghello, 2001).

Fuerza bruta

Un ataque de fuerza bruta es un intento de descifrar una contraseña o un nombre de usuario, de buscar una página web oculta o de descubrir la clave utilizada para cifrar un mensaje, que consiste en aplicar el método de prueba y error con la esperanza de dar con la combinación correcta. Se trata de un antiguo método de ataque, pero sigue siendo eficaz y goza de popularidad entre los hackers. (Kaspersky, 2018).

G.

Gateway (Default Gateway)

Un gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. Además, gestiona toda la comunicación de datos que se enruta interna o externamente desde la red. (Puerta de enlace).

H.

Hackers

Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet, pero también incluye a aquellos que depuran y arreglan errores en los sistemas. Son personas que disfrutan explorando los detalles de las computadoras y de cómo extender sus capacidades. (José Fernández, 2013).

Hipervisor

También llamado monitor de máquina virtual (VMM) es una pieza de software, firmware o hardware que crea y ejecuta máquinas virtuales. Un equipo en el que un hipervisor está ejecutando una o más máquinas virtuales se define como una máquina anfitrión o host. El hipervisor presenta los sistemas operativos invitados con una plataforma operativa virtual y gestiona la ejecución de los sistemas operativos invitados. Varias instancias de una variedad de sistemas operativos pueden compartir los recursos de hardware virtualizados. (Miguel Sanchez, 2015).

Host

Un host no es más que un nodo, una computadora o un conjunto de ellos, que ofrecen servicios, datos... al resto de las computadoras conectados a la red, sea esta local o global como Internet. En el caso de redes locales, el host suele coincidir con la computadora central que controla la red. (Sistemas Master).

I.

IANA (Internet Assigned Numbers Authority)

Es un acrónimo de la autoridad de números asignados en Internet, una de las instituciones más antiguas de Internet. Es la responsable de administrar la zona raíz del sistema de nombres de dominio (DNS), coordinar la asignación mundial de las direcciones del protocolo de Internet (IP), y gestionar los sistemas de numeración IP. Por lo tanto, IANA se encarga de mantener y administrar las funciones técnicas que posibilitan que Internet opere sin problemas. (Dynadot).

Internet

Es un sistema de redes de computación ligadas entre sí, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias. (Cristian Borghello, 2001).

IP (Internet Protocol)

Es el encargado de proporcionar una dirección IP a todos los equipos conectados a una red, ya sean hosts cliente, servidores o incluso el propio router. Opera en la capa de red OSI o de Internet en TCP/IP y es un protocolo no orientado a conexión, por lo que en definitiva se encarga de llevar los datos de un punto a otro. (Profesional Review, 2020).

ISACA (Information Systems Audit and Control Association)

Es una asociación internacional que apoya y patrocina el mejor conocimiento sobre cómo conseguir que los sistemas de información sirvan a las necesidades del negocio con seguridad, eficacia y economía. Por lo tanto, ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase. Desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales en gobierno, control, seguridad y auditoría de la información. (ISACA).

ISO (International Organization for Standarization)

Organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia OSI y protocolos estándares para varios niveles de este modelo. (Cristian Borghello, 2001).

L.

LAN (Local Area Network)

Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. (Cristian Borghello, 2001).

Log

Es un registro oficial durante un periodo de tiempo en particular de eventos generados por sistemas y dispositivos. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué ocurre un evento. (Fernando Cócaro, Mauricio García y Maria Rouiller, 2008).

N.

NAT (Network Address Translator)

El acrónimo NAT hace referencia a la traducción de direcciones de red y se desarrolló principalmente para resolver la falta de direcciones IP con el protocolo IPv4. Este sistema permite que se conecten a Internet las redes privadas (no registradas), convirtiendo direcciones IPs privadas de nuestra red interna en direcciones IP públicas, antes de que se envíen todos los paquetes a la red. (CISCO México).

O.

Open source

Es un software cuyo código fuente ha sido escrito con el afán de que cualquiera lo pueda inspeccionar, modificar, mejorar y redistribuir el código libremente. Es decir, los programadores que tienen acceso al código pueden mejorarlo, añadiendo funciones, optimizando su código o arreglando errores o bugs que podrían haber quedado de versiones anteriores. (Platzi, 2018).

P.

Phishing

Es un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. (José Fernández, 2013).

Política de Seguridad

Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información. (INCIBE, 2021).

Protocolo

Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información). (Cristian Borghello, 2001).

R.

Root

El usuario root puede hacer lo que quiera en el sistema operativo, así que cuando se utilice se debe tener mucho cuidado porque podríamos llegar a dejar nuestro sistema inutilizable. Es decir, con root se tiene acceso total y sin restricciones al sistema. (Cristian Borghello, 2001).

Rootkit

Programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. (José Fernández, 2013).

Router

Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los routers envían paquetes de una red a otra en base a la información de la capa de red. (Cristian Borghello, 2001).

S.

Script

Los scripts son un grupo de lenguajes de programación que son típicamente interpretados y pueden ser tecleados directamente desde el teclado. Los scripts pueden estar embebidos en otro lenguaje para aumentar las funcionalidades de este, como es el caso de los scripts PHP o Javascript en código HTML. (José Fernández, 2013).

SGI (Information Security Management System)

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. (INCIBE, 2021).

SMTP (Simple Network Management Protocol)

Protocolo de mensajería empleado para mandar un email de un punto A (servidor saliente) a un punto B (servidor entrante). Y sin importar dónde tengas tu dirección de correo electrónico (gmail, hotmail, zoho, aol, gmx, etc.), este procedimiento es imprescindible en cualquier proceso de envío de emails masivo y siempre es complementado por un servidor SMTP. (Beatriz Redondo, 2020).

Sniffer

Es un software utilizado para capturar tramas de una red de computadoras, ya sea que éstas estén dirigidas a él o no cuando la interfaz de red escucha en un medio compartido por varios dispositivos. El sniffer pone la interfaz de red en modo promiscuo de manera de no descartar las tramas no destinadas a su dirección MAC y así capturar todo el tráfico de la red. Son utilizados con fines (legítimos o maliciosos) muy diversos como: monitoreo de redes para detectar y analizar fallos, detección de intrusos, captura de contraseñas, intercepción de mensajes, espionaje, etc. (Miguel Sanchez, 2015).

SQL (Structured Query Language)

El lenguaje de consulta estructurada (SQL), es un lenguaje gestor para el manejo de información en una base de datos relacional. Es muy popular por su facilidad de uso y efectividad para convertir grandes volúmenes de datos en información útil. Además, SQL es empleado para escribir scripts de integración de datos y para configurar y ejecutar consultas analíticas.(CoderHouse, 2021).

SSH (Secure Shell)

Es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación. Es decir, proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el TELNET sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada. (Hostinger, 2019).

SSL (Secure Sockets Layers)

Protocolo que provee una conexión segura entre dos hosts. SSL proporciona un canal de comunicaciones seguro entre los servidores web y los clientes (los navegadores), pero su uso no se limita a la transmisión de páginas web. Al encontrarse entre los niveles de transporte y de aplicación, potencialmente SSL puede servir para securizar otros servicios, como FTP, SMTP, TELNET, etc. (Cristian Borghello, 2001).

Switch

Dispositivo que opera en la capa de enlace de datos del modelo OSI. Dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar. (Cristian Borghello, 2001).

T.

TCP (Transmission Control Protocol)

Este Protocolo de Control de Transmisión es un protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de éstos. (Cristian Borghello, 2001).

TCP/IP (Transfer Control Protocol/Internet Protocol)

Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundida en la actualidad, por ser la base de Internet. (Cristian Borghello, 2001).

TELNET

Protocolo estándar utilizado para realizar un servicio de conexión desde una terminal remota. Es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un equipo remoto en la red, de la misma forma que si se tratara de una terminal real directamente conectado al sistema remoto. (Cristian Borghello, 2001).

TIC (Tecnologías de Información y Comunicación)

Son todas aquellas herramientas y programas que tratan, administran, transmiten y comparten la información mediante soportes tecnológicos. La informática, Internet y las telecomunicaciones son las TIC más extendidas, aunque su crecimiento y evolución están haciendo que cada vez surjan cada vez más modelos. (Biblioteca Médica Nacional, 2013).

U.

UDP (User Datagram Protocol)

Este protocolo permite el envío de datagramas sin necesidad de establecer previamente una conexión, tan solo es necesario tener abierto un socket en el destino para que acepte los datagramas del origen. UDP es un protocolo no orientado a conexión, es decir, no ocurre como en TCP donde hay una fase de establecimiento de conexión, aquí directamente se envían sin establecimiento previo y no garantiza que los datagramas sean entregados en destino. (Redes Zone).

V.

VPN (Virtual Private Network)

Se utiliza para conectar una o más computadoras a una red privada utilizando Internet y de esta manera poder acceder a ciertos servicios, ocultando nuestra dirección IP real y enrutando nuestro tráfico a través de un túnel privado y cifrado de forma segura. (Daniel Cunha Barbosa, 2020).

VPS (Virtual Private Server)

Este servidor virtual es un servicio de alojamiento web que se obtiene dividiendo un servidor físico en varios servidores virtuales, haciendo que cada uno de ellos cuente con recursos dedicados y esté aislado de los demás. A nivel operativo, un VPS funciona igual que otros servicios de hosting web, ofreciendo un espacio conectado a internet de forma permanente al que podemos subir los contenidos de nuestra web para que otras personas puedan acceder a ellos. (Web Empresa, 2018).