Análisis de las vulnerabilidades de seguridad informática en ecosistemas IoT por medio de un honeypot que simule un dispositivo inteligente para alertar y prevenir ataques en la red

Hernández Cueva, Bryan Andrés

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

Ing. Alulema Flores, Darwin Omar, PhD.

8 de febrero de 2023

Informe de originalidad

NOMBRE DEL CURSO
Trabajo de titulación

NOMBRE DEL ALUMNO
BRYAN ANDRES HERNANDEZ CUEVA

NOMBRE DEL ARCHIVO
BRYAN ANDRES HERNANDEZ CUEVA - Documento sin título

CREACIÓN DEL INFORME
24 ene 2023

Resumen

Pasajes marcados	0	0 %
Pasajes citados/entrecomillados	0	0 %

Firmado electrónicamente por:
DARWIN OMAR ALULEMA FLORES

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Certificación

Certifico que el trabajo de titulación: "**Análisis de las vulnerabilidades de seguridad informática en ecosistemas IoT por medio de un honeypot que simule un dispositivo inteligente para alertar y prevenir ataques en la red**" fue realizado por el señor **Hernández Cueva, Bryan Andrés**; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 8 de febrero de 2023

Firmado electrónicamente por:
DARWIN OMAR ALULEMA FLORES

.....

Ing. Alulema Flores, Darwin Omar, PhD

C. C. 1002493334

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Hernández Cueva, Bryan Andrés**, con cédula de ciudadanía n° 172444920-0, declaro que el contenido, ideas y criterios del trabajo de titulación: **Análisis de las vulnerabilidades de seguridad informática en ecosistemas IoT por medio de un honeypot que simule un dispositivo inteligente para alertar y prevenir ataques en la red** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 8 de febrero de 2023

Hernández Cueva, Bryan Andrés

C.C.: 172444920-0

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Autorización de Publicación

Yo **Hernández Cueva, Bryan Andrés**, con cédula de ciudadanía n° 172444920-0, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Análisis de las vulnerabilidades de seguridad informática en ecosistemas IoT por medio de un honeypot que simule un dispositivo inteligente para alertar y prevenir ataques en la red** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 8 de febrero de 2023

Hernández Cueva, Bryan Andrés

C.C.: 172444920-0

Dedicatoria

Este trabajo está dedicado a mi familia por todo su amor, trabajo y sacrificio a lo largo de todos estos años, de no ser por ustedes no habría llegado hasta aquí. Son el motor que me empuja a esforzarme cada día ya que de ustedes he aprendido que todo lo que nos propongamos es posible con tiempo, dedicación y trabajo duro.

A todas las personas que me han apoyado a lo largo de mi vida universitaria y en especial para aquellos que me han brindado de su ayuda y conocimiento para poder realizar con éxito este trabajo.

Agradecimiento

Agradezco a mi familia por confiar y creer en este proceso, por ayudarme a superar las adversidades a lo largo de mi vida y estar dispuestos a siempre darme la mano.

A mis amigos de la universidad con los que pasamos gratos momentos a lo largo de estos años y de quienes también he podido aprender bastante.

También quiero expresar mi agradecimiento a la Universidad de las Fuerzas Armadas ESPE y a todos los profesores que me compartieron su conocimiento y experiencias. Su dedicación y esfuerzo nos motivan a ser buenos profesionales.

Índice de contenido

Índice de Tablas

Índice de Figuras

Resumen

Hoy en día los constantes avances tecnológicos y la interconexión global de dispositivos a través de Internet han abierto un mundo de oportunidades para que las personas realicen tareas que hace algunos años eran impensables. A medida que el tiempo transcurre los dispositivos inteligentes van tomando mayor aceptación y generan mayor utilidad al ser humano, abarcando tanto sectores industriales como domésticos. En consecuencia, nuevas técnicas de intrusión van apareciendo, generando nuevas vulnerabilidades de seguridad informática.

Los dispositivos IoT en la actualidad pueden utilizarse como agentes para difundir ataques informáticos a pequeña y gran escala. Evidentemente, es necesario afrontar estos nuevos retos de seguridad cibernética en los productos y servicios del Internet de las Cosas creando medidas para prevenir y detectar ciberataques en estos entornos. El propósito del presente trabajo es realizar el análisis de vulnerabilidades de seguridad informática en entornos IoT a través de honeypots. Para lo cual, se implementó un MHN (Modern Honey Network) el cual es un servidor centralizado para la administración y recopilación de datos de honeypots. Mediante una honeynet virtual autocontenida y una Raspberry pi se instalaron tres señuelos diferentes. Los honeypots instalados simulan servicios atractivos e intencionalmente expuestos para ser atacados por un ciberdelincuente. Estos señuelos están implementados dentro de un escenario real de un invernadero inteligente y se harán pasar como servidores de producción dentro de la red IoT. Con este escenario de prueba se comprobará la capacidad de detección de los honeypots. La finalidad es obtener un sistema que pueda identificar las técnicas utilizadas por los cibercriminales en ataques internos o externos a las redes del Internet de las Cosas.

Palabras clave: honeypot, ciberseguridad, IoT, vulnerabilidad, auditoría de seguridad informática.

Abstract

Nowadays, constant technological advances and the global interconnection of devices through the Internet have opened up a world of opportunities for people to perform tasks that were unthinkable a few years ago. As time goes by, smart devices are becoming more accepted and more useful to humans, covering both industrial and domestic sectors. As a result, new intrusion techniques are emerging, creating new computer security vulnerabilities.

IoT devices can nowadays be used as agents to spread small- and large-scale cyber-attacks. Clearly, it is necessary to address these new cyber security challenges in Internet of Things products and services by creating measures to prevent and detect cyber-attacks in these environments. The purpose of this work is to perform the analysis of cyber security vulnerabilities in IoT environments through honeypots. For this purpose, a MHN (Modern Honey Network) was implemented, which is a centralized server for the administration and collection of honeypot data, and by means of a self-contained virtual honeynet and a Raspberry Pi, three different decoys were installed. The installed honeypots simulate attractive and intentionally exposed services to be attacked by a cybercriminal. These decoys are implemented within a real scenario of a smart greenhouse and will masquerade as production servers within the IoT network. This test scenario will be used to test the detection capability of the honeypots. The aim is to obtain a system that can identify the techniques used by cybercriminals in internal or external attacks on Internet of Things networks.

Keywords: honeypot, cybersecurity, IoT, vulnerability, IT security audit.

Capítulo I: Marco Metodológico

Antecedentes

En la última década la tecnología ha crecido exponencialmente no solamente en calidad si no también en cantidad, lo que ha dado hincapié a la aparición de nuevos dispositivos inteligentes conectados a Internet. A este conjunto de dispositivos se les denomina Internet de las Cosas y con ellos aparecieron nuevos ataques y delitos informáticos. De esta manera cada vez más los adversarios emplean más recursos para irrumpir en estos entornos. En el trabajo realizado conjuntamente entre la industria y academia “Understanding the Mirai Botnet” (Antonakakis, y otros, 2017) se habla de uno de los ataques más gigantescos a IoT. La botnet nombrada Mirai es un malware que inició en septiembre de 2016. Consecuentemente tras la liberación de este malware decenas de miles de dispositivos IoT mal configurados fueron capturados por criminales informáticos. Como resultado, los dispositivos esencialmente cámaras IP, routers y grabadoras digitales se convirtieron en elementos controlados a distancia. Es así que esta infección a dispositivos IoT con falencias de seguridad terminó por consumar un ataque de denegación de servicio distribuido en contra del proveedor de servicios de nombres de dominio Dyn. Tal es el caso que afectó a importantes sitios web a nivel global.

A partir de la liberación del código fuente del malware Mirai, han aparecido variantes tales como Satori, Masuta, Okiru, etc. Una de las últimas variantes es la potente botnet IoTrooper la cual atacó a entidades gubernamentales y bancos de Países Bajos. Según (Howell, 2018) los ataques que se produjeron a finales de enero de 2018 detuvieron temporalmente servicios bancarios en línea de ABN Amor, ING y Raboban, así como los sistemas de la oficina nacional de impuestos de Países Bajos.

En la primera mitad del año 2019 (Kaspersky Lab, 2019) mediante sus honeypots detectó más de 100 millones de ataques a dispositivos del Internet de las Cosas provenientes de 276 000 direcciones IP únicas. Los datos registrados por los honeypots indican que las

regiones que más sufren ataques a estos entornos son China con el 30%, Brasil 19% y Egipto 12%. Los adversarios cibernéticos están aumentando los intentos de instaurar y monetizar redes de bots con dispositivos IoT.

Según reportes del portal de estadística alemán (Statista, 2021), se estima que para 2030 habrá alrededor de 25.44 billones de dispositivos de Internet de las cosas (IoT) conectados alrededor del mundo, más del doble de los 11.57 billones de dispositivos estimados para 2022. De acuerdo a (Statista, 2021) en el segmento de consumidores se concentra la mayor cantidad de dispositivos conectados con un 60 por ciento y lo restante corresponde a principales derivaciones de la industria.

Finalmente, en un estudio realizado por (Kaspersky, 2022) se evidencia que el 43% de las empresas no protege por completo sus redes IoT. El 46% de las empresas creen que las soluciones de ciberseguridad afectan el rendimiento de los dispositivos IoT. Otra de las razones con el 30% es que las herramientas de seguridad son costosas, lo que también se asocia a que no se pueda justificar la inversión de la misma. Consecuentemente, los riesgos de seguridad cibernética asociados a los dispositivos IoT son vistos por el 57% de las empresas que se declinan por no implementar este tipo de soluciones.

Motivación

Actualmente los dispositivos del Internet de las Cosas se encuentran implementados en varios ecosistemas de ámbito empresarial y también en entornos domésticos. De acuerdo a la base de datos de Gartner Machina, el empleo de tecnología IoT está incrementado en la mayoría de industrias. Se tiene proyectado un total de 18 mil millones de dispositivos IoT en entornos empresariales para el 2030. A partir de lo indicado nace este proyecto, el fin es descubrir y analizar las diferentes variantes de amenazas y vulnerabilidades informáticas que abarcan e infectan a millones de dispositivos IoT.

De acuerdo con (Netscout Systems, Inc., 2019) los dispositivos IoT fueron objetos de algún tipo de ataque los primeros cinco minutos tras haber sido conectados a Internet. Los adversarios y autores de malware aprovechan las vulnerabilidades de los dispositivos inteligentes para crear botnets de IoT para atacar nuevas áreas. Únicamente en el año 2020 según el informe Nokia Threat Intelligence Report (Nokia, 2020) los ataques consumados a dispositivos IoT ha crecido drásticamente. De modo que, un 100% de dispositivos IoT han sido comprometidos respecto al año 2019.

En su mayoría los fabricantes y desarrolladores de dispositivos IoT no crean medidas de seguridad robustas en los artefactos lanzados al consumo. Las debilidades en el apartado de software o hardware de estos equipos crean pivotes de ataque manipulados por criminales informáticos. La confidencialidad, integridad y disponibilidad se deja de lado ya que actualmente se toman pocas consideraciones en el desarrollo de software orientado a dispositivos del Internet de las Cosas. En suma, la seguridad en IoT es diminuta o totalmente nula en gran cantidad de dispositivos del Internet de las Cosas, provocando que este sea un sector cada vez más expuesto y vulnerable. Lo preocupante es que, en la actualidad, desde equipamiento médico hasta sistemas automovilísticos y domóticos, utilizan tecnología IoT. Conforme al informe de amenazas de IoT de (Palo Alto Networks, 2020) el 72% de las VLAN de atención hospitalaria se componen de dispositivos IoT y TI, permitiendo así la propagación de malware desde las terminales de usuarios a dispositivos IoT explotables dentro de la misma red informática. Adicionalmente, el 41% de los exploits ejecutan las vulnerabilidades de los dispositivos, esto debido a que los ataques propagados a través de TI examinan todos los terminales conectados a la red con el fin de utilizar las vulnerabilidades más comunes.

Por esta razón se necesita aplicar acciones y mecanismos para robustecer la seguridad informática en los ecosistemas IoT. En este trabajo se implementará una Honeynet híbrida en una red IoT la misma que permitirá alertar al administrador de red de probablemente ataques

que busquen vulnerar y explotar debilidades de los elementos de red. Por tanto, el administrador tomará las acciones necesarias para mitigar el riesgo. Adicionalmente, se estudiarán las vulnerabilidades más comunes que atentan a los dispositivos del Internet de las Cosas, acortando la seguridad de los datos y operación de redes en estos entornos. Mediante la implementación de herramientas de seguridad en la red se logra aplacar e impedir que las amenazas exploten vulnerabilidades en dispositivos inteligentes.

Importancia

El revelar las principales amenazas que quebrantan la seguridad de las redes e información en entornos IoT es de gran relevancia. Actualmente existe una gran cantidad de dispositivos IoT desplegados en hogares, ciudades inteligentes e industria. Por tal motivo, una herramienta que sea capaz de encontrar y clasificar vulnerabilidades dentro de sistemas IoT se vuelve de gran envergadura. Algunos de los hallazgos claves que menciona (Team, 2018) indican que los desarrolladores de bonets para IoT están implementando cada vez mayor énfasis en la explotación de vulnerabilidades vinculadas con tecnología IoT en su arsenal, además del enrutamiento común de ataques de fuerza bruta. En ciertos casos, los atacantes complementan este tipo de ataques con intrusiones mediante vulnerabilidades conocidas. Adicionalmente, se identifica que las vulnerabilidades vinculadas a tecnología del Internet de las Cosas son vectores de ataque funcionales durante mayor periodo de tiempo dado la dificultad y el lento ritmo de parchear dispositivos IoT. Es así que se requiere garantizar un entorno IoT más seguro, íntegro y que permita vigilar las técnicas, tácticas y procedimientos que utilizan los adversarios para infiltrarse en la red.

Con este trabajo se pretende cubrir estas falencias de seguridad y proporcionar a los sistemas IoT emergentes de instrumentos de supervisión y prevención de irrupciones. Para avalar el trabajo que ejecutarán los distintos Honeypots, se plantean los principales tipos de vulnerabilidades y riesgos asociados a las redes y dispositivos del Internet de las Cosas. Por

consiguiente, a manera de ejemplificar la importancia de la seguridad en las principales industrias, se implementará un escenario de prueba enfocado al sector de la agricultura. La gran ventaja de esta arquitectura de red es que es aplicable a cualquier campo que despliegue o abarque tecnologías emergentes IoT. La gestión del ciclo de vida de IoT es un reciente desafío para las instituciones. Es así que, al contar con estas soluciones de seguridad, se permite a las entidades descubrir e identificar dispositivos IoT y proporcionarles un perfil de riesgo a cada uno de estos.

Existe una obligación ascendente de emprender acciones de seguridad proactivas que puedan ser puestas en marcha por distintas partes interesadas dentro de una institución. En tal sentido, se identificarán los principales vectores de ataque en este tipo de ecosistemas y se indicarán las mejores prácticas que se pueden implementar para salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas IoT.

Estado del arte

Mapeo Sistemático de la Literatura

Las estrategias de Seguridad Informática dentro de ecosistemas IoT son escasas y no existe un nivel de concientización sobre la importancia de las mismas para salvaguardar la integridad de la red y las tecnologías emergentes. En primer lugar, existe un crecimiento y desarrollo acelerado de dispositivos inteligentes debido a la demanda actual y al aumento de acceso de los usuarios a Internet. Por tal motivo la academia y la industria se centran en investigar nuevas aplicaciones con tecnologías emergentes para simplificar las labores humanas. Sin embargo, la seguridad de los dispositivos y la red en la que trabajan se deja en segundo plano. Consecuentemente, hallar una explotación dentro de estos sistemas de información por parte de adversarios, bots o amenazas desconocidas puede desembocar en una pérdida sustancial. De hecho, la pérdida puede ser productiva, financiera e inclusive reputacional para una organización. De tal manera, podría significar la exfiltración de datos y

material sensible de los usuarios, desembocando en problemas no solo a nivel de infraestructura tecnológica sino a niveles legales de acuerdo a la normativa nacional.

Por tal motivo, se realizará un mapeo sistemático de literatura o SMS (Systematic Mapping Studies, por sus siglas en inglés) que permita comprender de mejor manera las herramientas disponibles para el desarrollo de soluciones de seguridad informática. Haciendo hincapié en mecanismos para proteger entornos del Internet de las Cosas.

Este mapeo sistemático de literatura se realiza con el fin de trazar una línea de ruta con una vasta base de entendimiento para el desarrollo adecuado del presente proyecto.

En la actualidad existen algunos trabajos sobre la implementación de soluciones de seguridad informática para ecosistemas del Internet de las Cosas. Sin embargo, estas herramientas son de carácter investigativo y no ofrecen una implementación viable en la mayoría de redes.

A continuación, mediante el mapeo sistemático de literatura se indaga en los trabajos y propuestas que se están desarrollando alrededor del mundo. De tal manera se determinará si estos pueden ser aplicables a entornos de tecnologías emergentes reales, analizando los resultados alcanzados por parte de los investigadores. El empleo del SMS surge de acuerdo a la cantidad de investigaciones realizadas en el marco nacional e internacional.

Definición de las preguntas de investigación. Para analizar los resultados obtenidos producto de la búsqueda de información, se categorizó los trabajos obtenidos procurando responder las preguntas de investigación realizadas. La utilización del SMS permitirá verificar el nivel de estudio de los temas investigados. Por tal motivo, se han definido preguntas de investigación para conocer qué herramientas de seguridad informática existen para entornos del Internet de las Cosas.

Tabla 1

Preguntas de investigación del SMS

Pregunta de Investigación	Motivación
P1: ¿Cuánta relevancia ha tomado la seguridad informática en tecnologías emergentes como el Internet de las cosas en los últimos años?	Conocer la importancia de proteger una red informática diseñada a partir de tecnologías emergentes como IoT.
P2: ¿Cuáles son los principales problemas de seguridad informática a los que están expuestos los ambientes basados en tecnologías emergentes?	Conocer las falencias de seguridad más notorias dentro de entornos que utilicen tecnologías emergentes.
P3: ¿Existen soluciones de seguridad cibernética que permita monitorear, capturar y catalogar las amenazas presentes en la red?	Conocer las herramientas de seguridad informática existentes en la actualidad y el estado de desarrollo de las mismas.
P4: ¿Qué limitaciones de hardware y/o software tienen los dispositivos del Internet de las Cosas?	Conocer las falencias de dispositivos inteligentes para escoger una solución de seguridad apropiada para reducir los vectores de ataque.

Criterios de búsqueda de información. Se seleccionó la base de datos Web of Science (WOS, por sus siglas en inglés) como motor de búsqueda de información. Este es un servicio que cuenta con una base amplia de información científica. Resultado de esta primera fase se pretende abarcar trabajos de científicos donde se descubra la tecnología actual.

Dado la gran cantidad de información que existe, se emplea una búsqueda preliminar para conseguir un primer borrador. De esta búsqueda preliminar se debe aclarar que algunas de las consultas no se emplearán en el presente trabajo debido a que no representan gran importancia para el desarrollo del mismo.

Mediante los siguientes términos de consulta se construye la estructura de búsqueda del mapeo sistemático de la literatura. Estos términos se basan en las preguntas de investigación planteadas en el presente capítulo:

Tabla 2

Términos para construir la estructura de búsqueda del SMS

Término Principal	**Términos alternativos**
Tools	Instrument, device, mechanism
Cybersecurity	Information security, Infosec, Cybersec, security
Internet of things	IoT, IoT Network, IoT Technology

En base a los términos principales se formula la estructura de la consulta para el desarrollo del SMS:

- *Tools* OR *instrument* OR *device* OR *mechanism* + *Cybersecurity* OR *Information security* OR *infosec* OR *cybersec* OR *security* + *Internet of Things* OR *IoT* OR *IoT Network* OR *IoT Technology*

Criterios de incorporación y exclusión. A lo largo de la búsqueda fueron considerados todos los trabajos científicos que han sido publicados hasta septiembre de 2022 donde se concluye la fase del SMS. De acuerdo a los resultados obtenidos se procede a realiza una revisión sistemática de la literatura.

Para catalogar la información relevante los trabajos que serán considerados al menos deben cumplir con los siguientes parámetros:

- Trabajos científicos completos.
- Pertenecientes a los campos de “Computer Science Information Systemas”, “Telecommunications”, “Engineering Electrical Electronic”
- Publicaciones hasta septiembre de 2022.
- Expongan estándares y/o soluciones de seguridad para sistemas informáticos.

De igual manera se descartaron trabajos que cumplen con uno de estos parámetros:

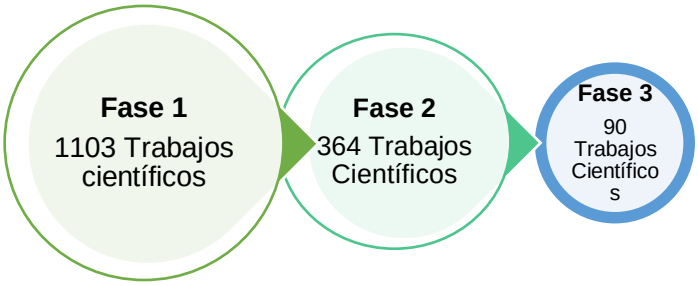
- Trabajos que no abordan mecanismos de seguridad informática.
- Artículos, tesis o documentos incompletos.
- Trabajos repetidos, de acceso anticipado.

Clasificación de los trabajos científicos. Para el proceso de categorización de trabajos se empleó tres fases que se explican a continuación:

1. A partir de las estructuras de consultas armadas se realizó un primer barrido de información. No se aplicó ningún filtro dentro de la petición, como resultado de esta primera fase se obtuvo un total de 1103 resultados.
2. En esta fase se toman en cuenta los criterios de incorporación y exclusión descritos anteriormente en este capítulo. Adicionalmente se empleó la misma estructura de consulta utilizada en la primera fase, se obtuvieron un total de 364 resultados.
3. Finalmente, para la tercera fase se empleó la misma estructura y consideraciones que en la fase 2, adicionalmente se consideraron los trabajos más relevantes y de utilidad para el desarrollo de una solución de seguridad informática. Por tal motivo el filtrado es más preciso y se obtuvieron 90 trabajos de interés.

Figura 1

Trabajos científicos extraídos en cada fase del SMS

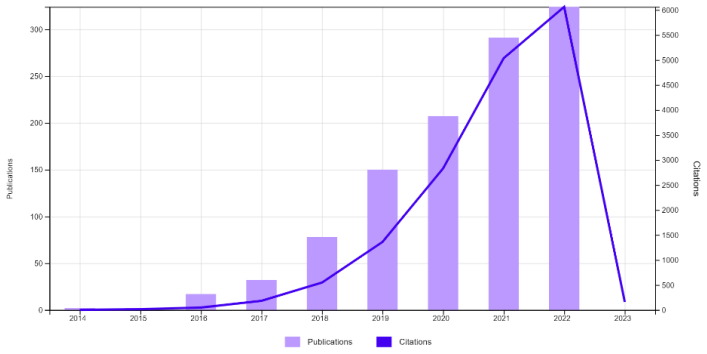


Resultados. El mapeo sistemático de la literatura concluye con la obtención de 90 trabajos relevantes. De la primera fase de clasificación de trabajos se aprecia que en los últimos años el tema de seguridad informática para tecnologías emergentes ha tomado gran relevancia. Es así que en el año 2014 se registran 2 publicaciones, mientras que para 2021 son 291 y para 2022 son 324 las publicaciones que abordan estos temas. De la data obtenida se aprecia que los campos que más abarcan publicaciones son los de *Computer Science Information Systems* con 643 (58.296%), *Engineering Electrical Electronic* tiene 484 (43.880%), *Telecommunications* con 365 (33.092%) y *Computer Science Theory Methods* con 281 publicaciones (25.476%).

Para la segunda fase de la clasificación se obtuvo un total de 364 trabajos científicos de los cuales 87 fueron publicados en el 2021 y 99 en el 2022 manteniendo la tendencia de la primera fase en cuanto a número de publicaciones por año. Los campos con más publicaciones siguen siendo *Computer Science Information Systems* con 270 (74.176%), *Engineering Electrical Electronic* con 249 (68.407%) y *Telecommunications* con 177 (48.626%). La diferencia con respecto a la primera fase es que *Computer Science Theory Methods* es desplazado al sexto lugar de campos con más publicaciones y toma su antigua posición *Instruments Instrumentation* con 62 publicaciones (17.033%).

Figura 2

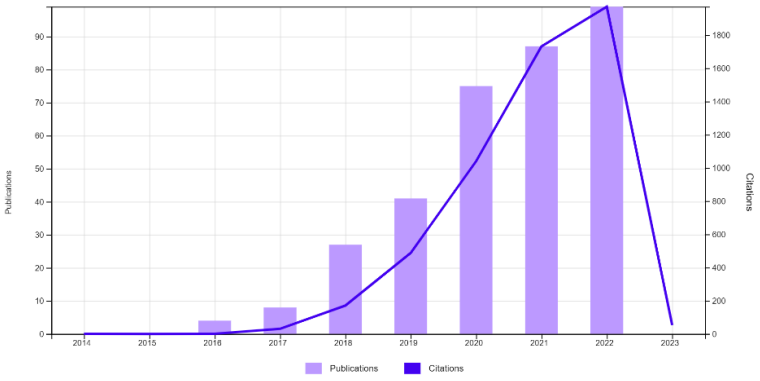
Publicaciones por año de la fase 1 del SMS



Nota. Número de publicaciones vs citas por año sobre Seguridad Informática en entornos con tecnologías emergentes conocidos en la fase 1 del SMS, resultados obtenidos de la base de datos Web of Science.

Figura 3

Publicaciones por año de la fase 2 del SMS

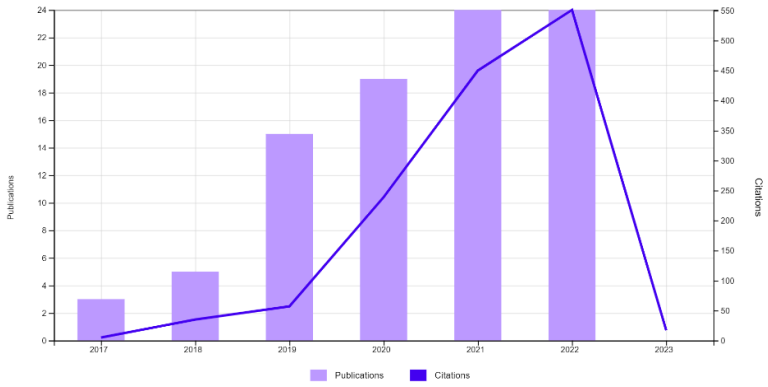


Nota. Número de publicaciones vs citas por año sobre Seguridad Informática en entornos con tecnologías emergentes conocidos en la fase 2 del SMS, resultados obtenidos de la base de datos Web of Science.

La tercera fase del mapeo sistemático de la literatura arrojó 90 trabajos científicos del interés, como se aprecia en la Figura 4 la cantidad de publicaciones es igual para el año 2021 y 2022 con un total de 24. El campo de estudio que más aborda publicaciones relacionadas a soluciones de seguridad en sistemas informáticos con tecnologías emergentes es *Engineering Electrical Electronic* con 68 (75.556%) seguido de *Computer Science Information Systems* con 65 (72.222%).

Figura 4

Publicaciones por año de la fase 3 del SMS

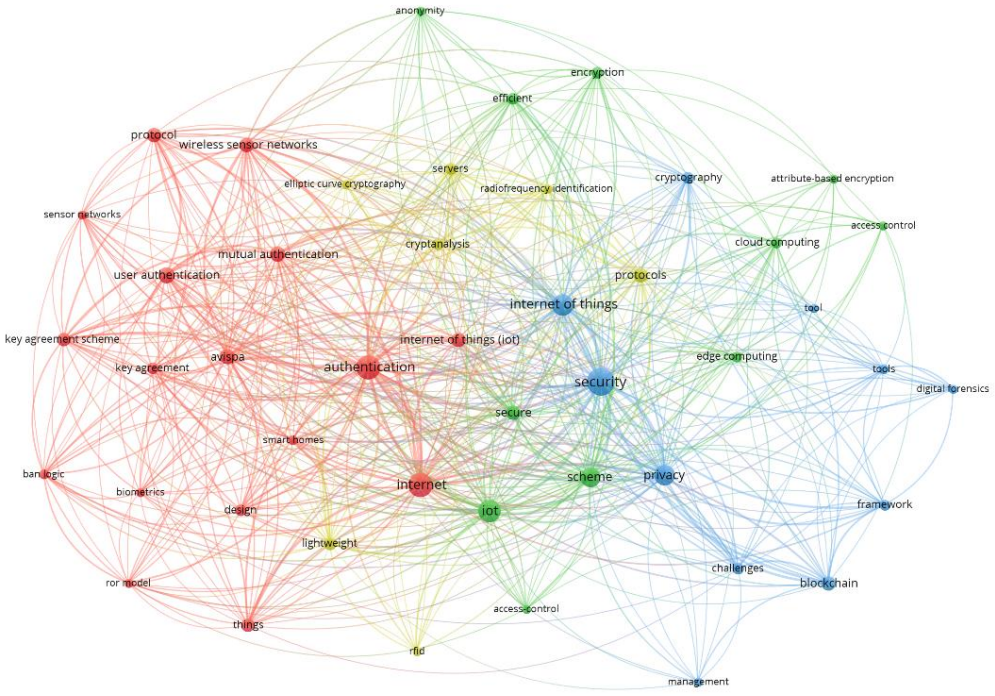


Nota. Número de publicaciones vs citas por año sobre Seguridad Informática en entornos con tecnologías emergentes conocidos en la fase 3 del SMS, resultados obtenidos de la base de datos Web of Science.

Por último, mediante VOSviewer la cual es una herramienta que permite el análisis y la visualización de trabajos científicos a través de redes bibliométricas se procederá a indicar las palabras claves más recurrentes encontradas en la última fase del SMS. Dentro de VOSviewer se han definido 46 términos en 4 clusters de los que destacan palabras clave como: *security, privacy, internet of things, authentication, design, tool.* De acuerdo a los parámetros de filtrado en la fase 3 los términos encontrados son los más adecuados, security y tool son términos que cuentan con varias relaciones dentro de la base de información obtenida.

Figura 5

Términos clave en WOS correspondiente a la fase 3 del SMS



Nota. Red Bibliométrica realizada en VOSviewer a partir de los datos obtenidos de la Web of Science y que corresponden a las relaciones de las palabras claves de las publicaciones encontradas en la fase 3 del SMS.

Conclusiones. Las preguntas de investigación planteadas para el SMS se han resuelto gracias al proceso de búsqueda y selección de las publicaciones dentro de WOS. Seguidamente se da respuesta las preguntas planteadas:

P1: ¿Cuánta relevancia ha tomado la seguridad informática en tecnologías emergentes como el Internet de las cosas en los últimos años?

Como se aprecia en los resultados obtenidos en la primera fase de la clasificación de publicaciones en los últimos años las investigaciones de soluciones sobre seguridad informática en entornos IoT ha incrementado notoriamente. En 2014 se registraron únicamente

2 publicaciones relacionadas, mientras que en 2022 ya se han publicado 324 trabajos. La tendencia se mantiene si se aplican filtros más exhaustivos como se evidencia en la fase 3. Estos resultados indican la relevancia que ha tomado la ciberseguridad para tecnologías emergentes.

P2: ¿Cuáles son los principales problemas de seguridad informática a los que están expuestos los ambientes basados en tecnologías emergentes?

En el SMS se pudo deducir que el campo que más abarca investigaciones en esta temática es *Computer Science Information Systems* con 643 (58.296%). Dentro de este campo se exponen trabajos sobre soluciones para el firmware IoT, problemas de privacidad en la arquitectura de la red que alberga a estas tecnologías, así como en los dispositivos per se. Otro campo es *Telecommunications* con 365 (33.092%) publicaciones que abordan problemas de seguridad y privacidad en los protocolos de transporte de información desde o hacia los dispositivos de red.

P3: ¿Existen soluciones de seguridad cibernética que permita monitorear, capturar y catalogar las amenazas presentes en la red?

En la fase 2 del SMS las publicaciones abordan la investigación e implementación de soluciones de seguridad basadas en arquitecturas especializadas. Las estrategias para mitigar los ciberataques abarcan tecnologías como una granja virtual de honeypots, la implementación de herramientas como IDS/IPS a través de Raspberry Pi, aplicación de protocolos seguros. Adicionalmente se aprecian soluciones incluso más sofisticadas y específicas como una herramienta para monitorear la seguridad en áreas de control de vehículos. También se aprecian esquemas de encriptación y aplicación de administradores de identidad y autenticación de dispositivos.

P4: ¿Qué limitaciones de hardware y/o software tienen los dispositivos del Internet de las Cosas?

La principal temática que se aborda en las investigaciones es el bajo nivel de madurez en los diseños actuales de las arquitecturas de red que albergan ecosistemas IoT. Sobre los principales riesgos de seguridad generado por debilidades en el hardware que tienen los dispositivos IoT se aprecia que los componentes utilizados son de bajas prestaciones. Consecuentemente esto desemboca en ataques de denegación de servicio, inclusive ataques de interferencia. En cuanto a riesgos debido al software se observan investigaciones centradas en el robustecimiento de sistemas de autenticación y control de acceso. La falta de métodos de encriptación robustos y las limitaciones impuestas en el firmware del dispositivo también son abordados dentro de la literatura obtenida en el SMS.

Revisión Sistemática de la Literatura

Una vez culminada la etapa del mapeo sistemático de la literatura es necesario profundizar en las herramientas de seguridad informática para entornos emergentes disponibles en la actualidad. Acorde a los trabajos científicos obtenidos en el SMS las investigaciones cubren una amplia variedad de soluciones para mejorar la ciberseguridad de estos entornos. Es por esto que se ejecutará una revisión sistemática de la literatura o SLR (Systematic Literature Review, por sus siglas en inglés).

El SLR permite abarcar de forma más específica un tema de investigación, mediante este se recopila los resultados más apropiados de los diversos estudios realizados en el SMS. De manera análoga, en la revisión sistemática de la literatura se emplea un proceso ordenado para su realización similar al proceso del SMS.

El objetivo principal de este SLR es averiguar las herramientas, métodos y soluciones de seguridad informática existentes y disponibles para entornos que incorporen tecnologías

emergentes como IoT, con el fin de obtener directrices para la protección de estos entornos. De la misma forma se estima encontrar trabajos que permitan conocer de primera mano la efectividad y viabilidad de las distintas soluciones.

Es necesario la realización de un SLR dada la gran cantidad de información encontrada en el SMS. Como consecuencia a la necesidad de la industria y la academia de cubrir la creciente demanda de sistemas y arquitecturas para la protección ante las amenazas cibernéticas.

Definición de las preguntas de investigación. Para conocer las herramientas, métodos y soluciones existentes para entornos que incorporen tecnologías emergentes se plantearon las siguientes preguntas:

Tabla 3

Preguntas de investigación del SLR

Pregunta de Investigación	**Motivación**
P1: ¿Qué soluciones de seguridad informática existen para monitorear, capturar y catalogar las amenazas presentes en redes del Internet de las Cosas?	Conocer las herramientas de seguridad informática existentes en la actualidad y el estado de desarrollo de las mismas para entornos IoT.
P2: ¿Qué trabajos existen centrados en analizar el malware presente en entornos IoT?	Encontrar todas las publicaciones científicas que aborden el análisis de malware en redes IoT (en el caso que hubiesen).
P3: ¿Existen herramientas de ciberseguridad que ocupen bajos recursos de hardware para su funcionamiento?	Conocer las soluciones de seguridad informática que limiten los recursos de hardware para su correcto funcionamiento.

Pregunta de Investigación	Motivación
P4: ¿Qué métodos y/o técnicas de intrusión están afectando más los entornos IoT en la actualidad?	Conocer los métodos y/o técnicas que explotan las vulnerabilidades de los entornos del Internet de las Cosas.

Criterios de búsqueda de información. Se emplearán criterios semejantes a los ya utilizados para el mapeo sistemático de la literatura sin embargo lo que se busca con el SLR es dar mayor fondo en cuanto a métodos, técnicas y tecnología de seguridad informática. Por tal motivo se prescindirá de publicaciones como artículos de revisión, de acceso anticipado, papeles de procedimiento o trabajos que tengan un enfoque únicamente de divulgación científica. El motor de búsqueda es la base de datos de la Web of Science el cual cuenta con una amplia base de publicaciones y ya fue utilizado en el SMS.

La estructura de búsqueda empleada en el SLR ha sido determinada en base a las preguntas de investigación planteadas:

Tabla 4

Términos para construir la estructura de búsqueda del SLR

Término Principal	Términos alternativos
Tools	Instrument, device, mechanism
Cybersecurity	Information security, Infosec, Cybersec, security
Malware	Malicious software, badware, malign code
Low-resource software	Architecture, protocol, framework, platform, system
Internet of things	IoT, IoT Network, IoT Technology

En base a los términos principales se formula la estructura de la consulta para el desarrollo del SLR:

- *Tools* OR *instrument* OR *device* OR *mechanism* + *Cybersecurity* OR *Information security* OR *infosec* OR *cybersec* OR *security* + *malware* OR *malicious software* OR *badware* OR *malign code* + *Low-resource software* OR *architecture* OR *protocol* OR *framework* OR *platform* OR *system* + *Internet of Things* OR *IoT* OR *IoT Network* OR *IoT Technology*

Criterios de incorporación y exclusión. Para esta etapa del SLR se han considerado todas las publicaciones indexadas a la base de la Web of Science hasta octubre de 2022. Se valoró la relevancia de cada trabajo científico para determinar la importancia de su inclusión en el presente trabajo.

Para catalogar la información relevante los trabajos que serán considerados al menos deben cumplir con los siguientes parámetros:

- Trabajos científicos completos.
- Pertenecientes a los campos de “Computer Science Information Systemas”, “Telecommunications”, “Engineering Electrical Electronic”
- Publicaciones hasta octubre de 2022.
- Expongan estándares y/o soluciones de seguridad para sistemas informáticos.

De igual manera se descartaron trabajos que cumplen con uno de estos parámetros:

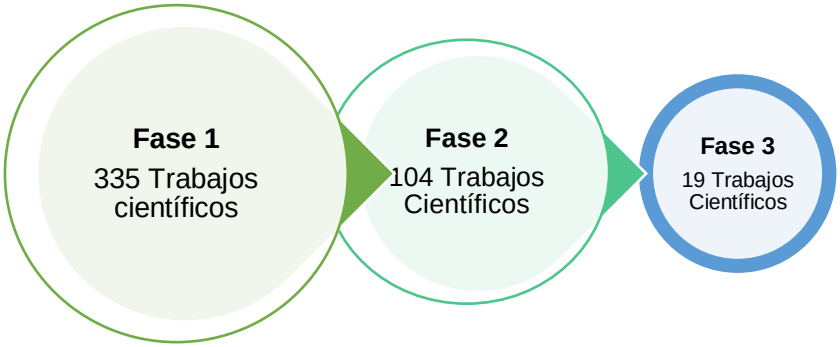
- Trabajos que no abordan mecanismos de seguridad informática.
- Artículos, tesis o documentos incompletos.
- Trabajos repetidos.
- Artículos de revisión, de acceso anticipado y papeles de procedimiento.

Clasificación de los trabajos científicos. De similar manera que en el SMS se utilizó tres fases para catalogación de las publicaciones de la WOS:

1. Para esta primera fase se identificaron todas las publicaciones encontradas con la estructura de búsqueda definida para el SLR. Se obtuvieron un total de 335 publicaciones.
2. En la segunda fase se empleó los criterios de incorporación y exclusión definidos anteriormente además de los criterios de la primera fase. Se consiguieron 104 artículos.
3. Finalmente se aplican filtros más exactos para conocer únicamente los trabajos de interés y que provean de una herramienta de seguridad informática en base a las necesidades especificadas a lo largo del SLR. Se obtuvieron 19 resultados de interés.

Figura 6

Trabajos científicos extraídos en cada fase del SLR

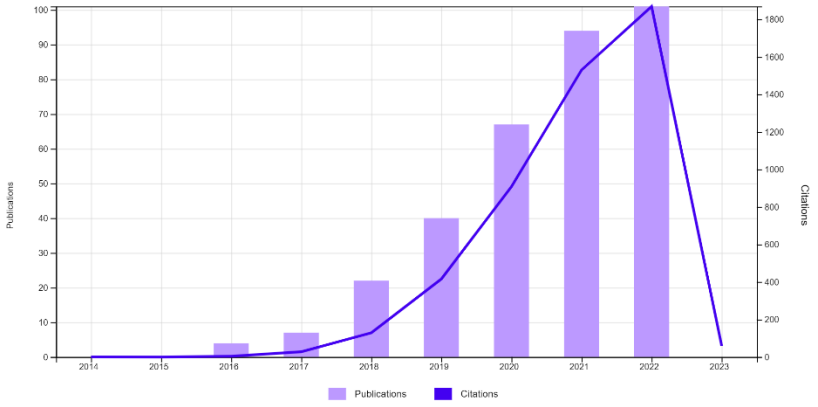


Resultados. En esta etapa se analizarán los trabajos científicos encontrados en la fase de clasificación. Tras aplicar la metodología descrita se pudo obtener en la tercera fase un total de 19 artículos de interés. Como consecuencia de esto se indicarán datos relevantes para el estudio.

En la primera fase de catalogación de información se aprecia que la tendencia de publicaciones de seguridad informática para ecosistemas IoT es creciente en el año 2022 se registra un total de 101 publicaciones seguido de 94 artículos registrados en 2021. El 73.433% de las publicaciones encontradas en esta primera fase corresponden al campo *Computer Science Information Systems.*

Figura 7

Publicaciones por año de la fase 1 del SLR

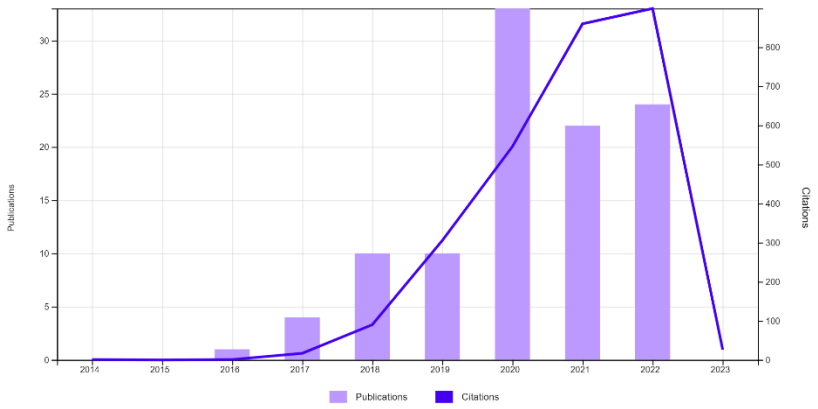


Nota. Número de publicaciones vs citas por año sobre Soluciones de seguridad Informática en entornos del Internet de las Cosas conocidos en la fase 1 del SLR, resultados obtenidos de la base de datos Web of Science.

Para la segunda fase de clasificación se registra una variación en la tendencia. Se evidencia que al aplicar filtros más exhaustivos las publicaciones de interés en su mayoría han sido publicadas a partir del 2020 y de hecho en este año se registran 33 publicaciones del total encontrado en esta fase. De similar manera el campo que más aborda estos temas es el de *Engineering Electrical Electronic* con el 74.038%.

Figura 8

Publicaciones por año de la fase 2 del SLR



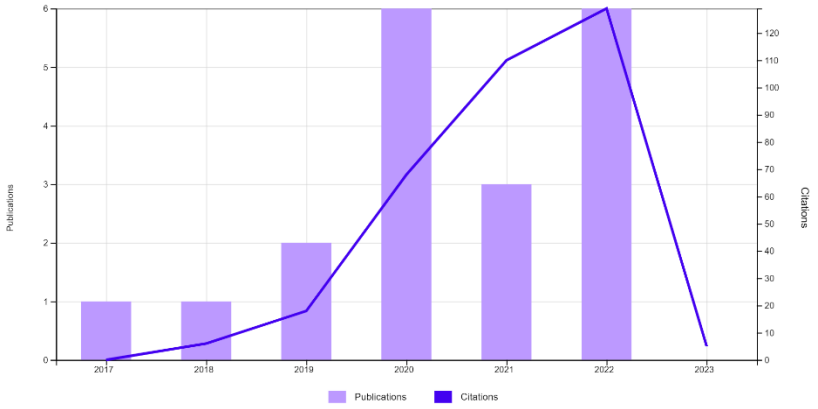
Nota. Número de publicaciones vs citas por año sobre Soluciones de seguridad Informática en entornos del Internet de las Cosas conocidos en la fase 2 del SLR, resultados obtenidos de la base de datos Web of Science.

En la última fase donde se toma en consideración parámetros más exhaustivos de búsqueda se aprecia que 6 de los trabajos de interés se han publicado en 2022. En la Figura 9 también se aprecia que las citas en trabajos de investigación aumentan con el pasar del tiempo debido a la necesidad de protección de estos entornos ante las amenazas actuales. Nuevamente el campo con más participación dentro de las publicaciones es *Computer Science Information Systems* con el 78.947%.

Finalmente, como se realizó en el mapeo sistemático de la literatura se emplea la herramienta VOSviewer para determinar las palabras clave encontradas en la fase 3. Consecuentemente se requiere constatar que el filtrado se realizó de manera correcta y este se alinea al objetivo principal del SLR el cual es dar respuesta a las preguntas de investigación. Como se aprecia en la Figura 10, las palabras más frecuentes encontradas son: *security, internet of things, intrusión detection, malware, botnet, honeypot, attacks, anomaly detection.*

Figura 9

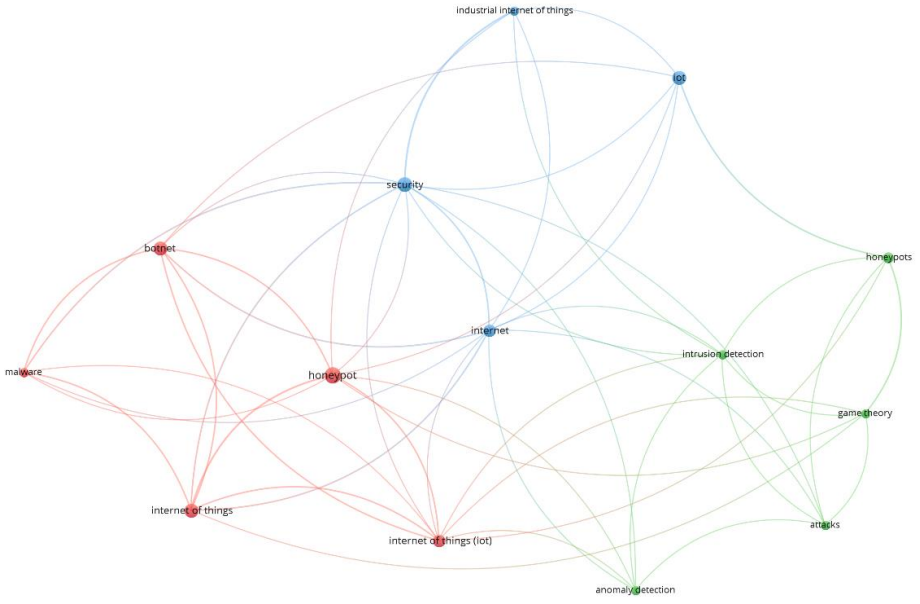
Publicaciones por año de la fase 3 del SLR



Nota. Número de publicaciones vs citas por año sobre Soluciones de seguridad Informática en entornos del Internet de las Cosas conocidos en la fase 3 del SLR, resultados obtenidos de la base de datos Web of Science.

Figura 10

Términos clave de WOS correspondiente a la fase 3 del SLR



Conclusiones. La finalidad de la ejecución del SLR es dar respuestas a las preguntas de investigación planteadas, las cuales se indican a continuación:

P1: ¿Qué soluciones de seguridad informática existen para monitorear, capturar y catalogar las amenazas presentes en redes del Internet de las Cosas?

Dentro de los principales trabajos recabados se identifican soluciones basadas en sistemas de detección de intrusiones (IDS, por sus siglas en inglés), sistemas de prevención de intrusiones (IPS, por sus siglas en inglés), granjas de honeypots o también llamados Honeynets. También se evidencia el uso de servidores especializados para la autenticación y administración de claves. Adicionalmente existen modelos y marcos de trabajo que emplean tecnologías como Machine Learning, Blockchain y herramientas de analítica especialmente diseñados para entornos del Internet de las Cosas.

P2: ¿Qué trabajos existen centrados en analizar el malware presente en entornos IoT?

Acorde a las publicaciones encontradas en el SLR, gran parte buscan soluciones orientadas a capturar y analizar el tráfico malicioso en las redes de los ecosistemas IoT. Los trabajos analizan las familias de malware existentes mediante repositorios abiertos de información para clasificarlas y estructurar ambientes para la protección de los sistemas. También se aprecia que las investigaciones utilizan tecnologías como redes neuronales, métodos de detección basados en características estáticas, detección inteligente, análisis dinámico entre otras.

P3: ¿Existen herramientas de ciberseguridad que ocupen bajos recursos de hardware para su funcionamiento?

Dentro de los trabajos científicos obtenidos en la fase de clasificación no se obtuvo de manera específica evidencia de herramientas de seguridad informática que funcionen con

pocos recursos. Sin embargo, en las investigaciones se indicaba herramientas altamente configurables y adaptables que cumplen con este principio. Por tal motivo algunas de las soluciones se basan en mecanismos de detección de intrusiones como los IDS e IPS también se abordan herramientas como honeypots, sniffers, firewalls, infraestructuras de clave pública entre otras.

P4: ¿Qué métodos y/o técnicas de intrusión están afectando más los entornos IoT en la actualidad?

En la actualidad las amenazas automatizadas han sido la principal causa de estudio por parte de los investigadores. El uso de botnets para la ejecución de ataques de denegación de servicios han puesto en alerta al entorno del internet de las cosas. También se encontraron métodos de escaneo masivo por parte de bots creados por redes de delincuentes informáticos. Como se aprecia las falencias en los sistemas IoT son aprovechadas principalmente por este tipo de programas informáticos como son los bots. Las publicaciones científicas indican que la ejecución de procesos automáticos como los escaneos a través de la red ayudan a los delincuentes informáticos a detectar de manera más eficiente entornos vulnerables.

Alcance

El presente trabajo propone abarcar temas de seguridad informática sobre ecosistemas IoT. En resumen, se analizará las vulnerabilidades mediante el uso de una Honeynet híbrida como instrumento de detección de intrusos. De esta manera el administrador de red puede identificar y tomar medidas ante posibles ataques a la red interna, mitigando el riesgo de usar a los dispositivos IoT como agentes de ataque a redes informáticas. Cabe señalar que los honeypots que conforman esta Honeynet híbrida están implementados sobre ordenadores de diferentes prestaciones. Consecuentemente, resulta ventajoso al momento de la elección del honeypot más idóneo para la red en caso de que no se cuente con un capital elevado para el despliegue de toda la solución de seguridad propuesta. Al emplear una Raspberry Pi para la

instalación de uno de los Honeypots disminuye enormemente la complejidad del proyecto y ofrece al usuario una solución económica. Pero se ofrece una solución más completa en caso de contar con infraestructura con mejores prestaciones. La finalidad de este trabajo no es solo entregar un sistema de seguridad de entornos IoT, además se pretende que el mismo sea adaptable, escalable y costeable para cualquier entorno informático.

Objetivos

General

Evaluar las vulnerabilidades de seguridad informática en ecosistemas IoT por medio de un honeypot que simule un dispositivo inteligente para alertar y prevenir ataques en la red.

Específicos

- Investigar normativa y recomendaciones en el marco de seguridad informática y seguridad para la Internet de las Cosas.
- Identificar los principales ataques informáticos que se podría perpetrar a ecosistemas del Internet de las Cosas.
- Desplegar un escenario de prueba donde el honeypot físico pudiese detectar y recabar información de las amenazas en una red IoT.
- Implementar un honeypot físico a través de una Raspberry Pi que simule un dispositivo IoT para ser el objeto de un posible ataque informático.
- Analizar los resultados que se obtienen con la integración de un honeypot en un entorno IoT.

Capítulo II: Marco Conceptual

Vulnerabilidad

Existen distintas definiciones para referirse a una vulnerabilidad, la (ISO/IEC, 2013) indica que una vulnerabilidad es una debilidad de un activo o control que puede ser explotada por una o varias amenazas. También se puede indicar que una vulnerabilidad es la cualidad de una red o infraestructura para ser comprometida negativamente por diferentes amenazas.

CVSS – Common Vulnerability Scoring System

Es un sistema de puntaje utilizado para estimar el impacto causado por las vulnerabilidades identificadas dentro del campo de TI. Permite cuantificar la severidad que representan las vulnerabilidades, siendo uno de los estándares para la gestión de riesgos.

CVE – Common Vulnerabilities and Exposures

Corresponde a una lista de vulnerabilidades de seguridad registradas. En esta lista se identifica, define y cataloga las vulnerabilidades divulgadas de manera pública. Las vulnerabilidades y exposiciones comunes forman un catálogo de fallas de seguridad informática. Los CVE se encuentran supervisados por MITRE Corporation con la financiación del Departamento de Seguridad Nacional de los Estados Unidos. (Red Hat, 2020)

Amenaza

Es la propiedad de causar de una o diferentes maneras daño sobre un activo. (ISO/IEC, 2013) define la amenaza como un motivo potencial de un suceso no deseado, mediante el cual se puede originar daño a una infraestructura o a una organización.

Exploit

Son programas o códigos especialmente diseñados para explotar una vulnerabilidad identificada o no de software, generalmente debido a fallas en el esquema de seguridad del sistema atacado. De acuerdo con (AVG Technologies, 2020) son creados para apuntar

debilidades concretas ya sea de un programa de software o un componente de hardware, los exploits abarcan definiciones desde aplicaciones de software hasta sucesiones de comandos.

Payload

También denominado carga útil, son partes de código malicioso o repertorio de instrucciones que se ejecutan para causar un daño y explotar una vulnerabilidad en un sistema víctima. Estos códigos permiten realizar tareas como ejecución de código remoto y apropiación de máquinas, conexiones a botnets, despliegue de malware, carga y descarga de archivos.

Clasificación de Ataques

De acuerdo al Marco Técnico de Aseguramiento de la Información (IATF, por sus siglas en inglés) los ataques de seguridad informática están clasificados en 5 categorías: pasivos, activos, de proximidad, internos y de distribución. (National Security Agency, 2002)

Ataques Pasivos

Este tipo de ataques suelen ser los más difíciles de detectar debido a que el adversario no interactúa directamente con la máquina física. Consisten en interceptar, supervisar y analizar el tráfico de la red víctima, recabando la mayor información posible de las máquinas objetivos, sin alterar los datos interceptados. Con este tipo de ataque se puede obtener información sin autorización del propietario.

Algunos de los principales ejemplos de ataques pasivos son:

- Footprinting
- Sniffing
- Eavesdropping
- Descifrado de tráfico con bajo nivel de cifrado
- Análisis del tráfico de red
- Captura de credenciales transmitidas en texto claro

Ataques Activos

Los ataques activos se caracterizan por malograr las características de protección, inyectar código malicioso, modificar e interrumpir información en tránsito y robar datos de objetivos de una red. Aquí los ataques buscan penetrar e infectar una red víctima y establecer conexiones remotas para comprometer la seguridad informática del sistema. Los ataques que se ejecutan son más propensos a ser detectados por una herramienta de seguridad debido a la alta interacción entre el atacante y el objetivo.

Algunos de los principales ejemplos de ataques activos son:

- Ataques de Denegación de Servicio – DoS
- Elución de mecanismos de protección
- Ataques de malware (Virus, gusanos, ransomware)
- Ataques de suplantación
- Ataques de diccionario, fuerza bruta
- Ataques de intermediario
- Ataques de IDS y Firewall
- Ejecución de código arbitrario, etc.

Ataques de Proximidad

Se realizan cuando el atacante físicamente se encuentra próximo al usuario o sistema objetivo. Los ataques de proximidad se caracterizan por recoger la mayor cantidad de información posible o quebrantar la seguridad de los accesos sean lógicos o físicos. Este tipo de ataques se originan principalmente por una falencia de seguridad física en los métodos de acceso al sistema. Algunos de los métodos empleados en este ataque se basan en ingeniería social.

Ataques Internos

Se originan por personas pertenecientes a la organización y con acceso a información confidencial que intencionalmente espía, roba o daña información con diferentes fines. Un ataque interno puede saltarse gran cantidad de barreras de seguridad. Al contar con accesos privilegiados los atacantes se vuelven sumamente peligrosos para la organización ya que pueden afectar directamente a la confidencialidad, disponibilidad e integridad de los activos de información.

Los ataques internos también pueden ser no maliciosos, sin embargo, igual de severos que los maliciosos. Un ataque interno no malicioso se puede producir por descuido, falta de capacitación o por acciones intencionales con fines no maliciosas del personal por cumplir con las tareas encargadas.

Ataques de Distribución

Suceden cuando los adversarios modifican ya sea el hardware o software antes de la instalación del mismo. Esta modificación puede ocurrir desde su origen o cuando el mismo está en tránsito. Principalmente se apoyan de puertas traseras para ganar acceso sin la autorización del usuario final, logrando introducirse a la red y comprometer la información de los elementos de la misma.

OWASP Top 10 Internet of Things 2018

OWASP es un proyecto sin fines de lucro que trabaja para robustecer la seguridad del software en diferentes ámbitos. El proyecto de Internet de las Cosas de OWASP se diseñó especialmente para determinar los problemas de seguridad vinculados con el Internet de las Cosas IoT. Ayuda a los fabricantes, desarrolladores y usuarios finales a entender dichos problemas. (OWASP Foundation, Inc., 2018) A continuación de indican las 10 principales prácticas que se deben evitar al momento de construir, implementar o administrar ecosistemas del Internet de las Cosas:

Tabla 5

OWASP Internet of Things Top 10

OWASP IoT Top 10	Descripción
1. Contraseñas débiles, predecibles o codificadas	Credenciales disponibles públicamente o no modificables o empleo de credenciales de fácil deducción. Puertas traseras en firmware o en el software del usuario que permiten el acceso no autorizado al sistema implementado.
2. Servicios de red inseguros	Servicios de red que se ejecutan en los dispositivos y que carecen de métodos robustos de seguridad para exponerse a Internet. Comprometen la confidencialidad, integridad y disponibilidad de la información o generan puertas de acceso remoto.
3. Interfaces de ecosistemas inseguros	Se generan debido a web inseguras, API back-end, nube o interfaces móviles con las cuales se administra los dispositivos y comprometen la seguridad del ecosistema. Los principales problemas es la carencia de autenticación, la falta de cifrado robusto y no contar con un filtrado de paquetes de entrada y salida.
4. Carencia de mecanismos de actualización seguros	No cuentan con una forma segura de actualizar el dispositivo. No existe una notificación de cambios de seguridad por actualizaciones.
5. Utilización de componentes inseguros u obsoletos	Uso de componentes de software descontinuados e inseguros que pueden hacer vulnerable al dispositivo y a la red que los alberga.

OWASP IoT Top 10	Descripción
6. Falta o poca protección de privacidad	Los dispositivos almacenan internamente o en sus ecosistemas información personal del usuario de manera insegura, incorrecta e inclusive sin permiso.
7. Transferencia y almacenamiento de datos de manera insegura	No existe una encriptación robusta y hay una falta de control de acceso a los datos en el ecosistema, a través del ciclo de vida de los mismos.
8. Carencia de gestión de dispositivos	Los dispositivos implementados en producción no cuentan con soporte de seguridad. Incluyendo procesos como la gestión de activos, actualizaciones, desmantelamiento seguro, monitoreo y capacidad de respuesta ante posibles intrusiones.
9. Configuración predeterminada insegura	Los fabricantes entregan dispositivos con configuraciones predeterminadas de manera insegura. No permiten a los operadores modificar las configuraciones de fábrica de los dispositivos IoT.
10. Falta de robustecimiento físico en los dispositivos	No existen medidas de refuerzo físico sobre los dispositivos, facilitando la exfiltración de información por parte de atacantes.

Nota. Datos obtenidos de la matriz de riesgo para el Internet de las Cosas. Tomado de *OWASP Internet of Things*, por OWASP Foundation Inc, 2018.

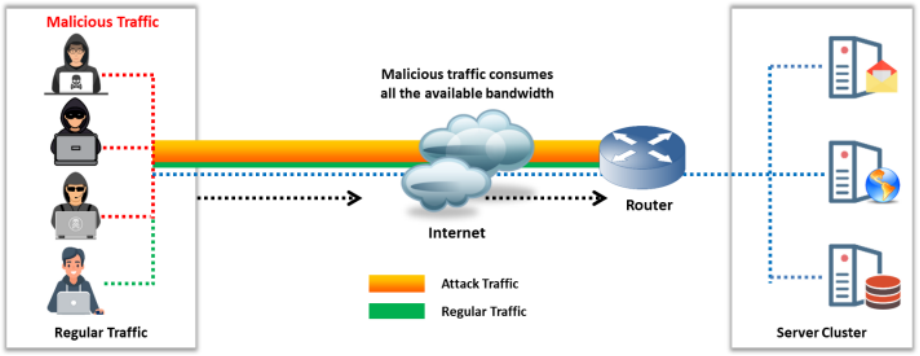
Denegación de Servicio DoS

El principal objetivo de este tipo de ataque es inhabilitar a los usuarios de servicios a los que normalmente tienen acceso. Estos ataques se dirigen a un objetivo específico para

saturarlos de una gran cantidad de peticiones falsas, provocando que el servicio no funcione de manera correcta y rechazando inclusive las peticiones legítimas. (Wang & Kissel, 2015) Este ataque se puede generar desde una simple computadora o incluso formar un grupo más grande de computadoras distribuidas en el Internet. Si el ataque de denegación de servicio se realiza de manera conjunta desde varios computadores a un mismo objetivo se trata de un ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés).

Figura 11

Esquema General de un ataque de Denegación de Servicio (DoS)



Nota. La figura indica el esquema de un ataque DoS. Tomado de *Ethical Hacking Essentials*, por EC-Council, 2021.

Botnets

Un bot es un sistema comprometido por un ciberdelincuente el cual tiene control sobre este a través de Internet. La botnet es el conjunto o red de sistemas controlados con la finalidad de realizar un ataque de denegación de servicio o el envío masivo de spam sobre objetivos definidos por los atacantes. La gran mayoría de botnets se forman a partir de malware como troyanos ocultos en software aparentemente correcto. (Escrivá, Romero, Ramada, & Onrubia, 2013)

Ataque de Diccionario

Es una técnica de descubrimiento de contraseñas en la que el atacante emplea un diccionario para ir probando todas las palabras que contiene el mismo. Generalmente las palabras que contiene este diccionario recaban las principales contraseñas utilizadas de manera determinada por los fabricantes de equipos y sistemas operativos. Este tipo de ataques es más efectivo que uno de fuerza bruta. Una estrategia para contrarrestar estos ataques es configurar una contraseña compuesta por mayúsculas, minúsculas, números y caracteres especiales. Los ataques de diccionario son poco efectivos con contraseñas robustas ya que debido a la complejidad no suelen ser incluidas en los diccionarios. Una desventaja es el tamaño que ocupan estos diccionarios ya que dependiendo de la cantidad de palabras el tamaño aumenta. (Chicano, 2015)

Inyección SQL

Este ataque consiste en emplear el lenguaje de consulta estructurado SQL con el fin de realizar consultas concatenadas a las bases de datos de los servidores objetivos. Se puede inyectar scripts malintencionados simples hasta secuencias de comandos más complejas que permiten la interacción con el sistema operativo. El atacante busca obtener acceso a la base de datos sin autorización alguna, para obtener información sensible de esta. (Arroyo, Gayoso, & Hernández, 2020)

Tipos de Auditoría de Seguridad Informática

Caja Blanca

En la auditoría de caja blanca la organización provee información específica del ataque a realizarse o el objetivo que se requiere evaluar. La información que se entrega al auditor corresponde a topologías de red, información de valoración e inclusive información de ubicación física del objetivo. El auditor cuenta con toda la información necesaria para llevar a cabo la evaluación de seguridad del sistema o aplicación.

Caja Gris

Consiste en otorgarle al auditor un rol de empleado sin privilegios o incluirlo dentro de la red como invitado. El auditor se comporta como un insider malintencionado para comprobar la seguridad de las aplicaciones de la organización auditada. El auditor al encontrarse en la misma red de los empleados puede verificar la conectividad con otros equipos de red y obtener información de la red interna. El objetivo más común de este tipo de auditoría es encontrar vulnerabilidades y escalar privilegios a partir de un rol de empleado común.

Caja Negra

Es la auditoría más completa y complicada que existe debido a que sitúa al auditor como un agente externo. Consecuentemente el auditor no cuenta con ningún conocimiento interno de la organización o su infraestructura de red. El principal objetivo es evaluar el nivel de seguridad de la organización y determinar hasta qué nivel puede llegar un atacante externo y el nivel de daño que este podría provocar a la compañía. Esta auditoría minimiza los falsos positivos, pero para ejecutarla se debe contar con un personal altamente capacitado.

Fases de una Prueba de Penetración en Seguridad Informática

Normalmente se emplea una metodología ordenada para determinar todas las vulnerabilidades de las redes auditadas. Inicialmente se crea un proyecto donde se ubica el espacio de trabajo y se almacenan datos. El espacio dependerá de la cantidad de redes y subredes a auditar.

Fase de Pre-Ataque

Information Gathering. Es la primera fase donde se recolecta toda la información pública disponible. Conocida de igual manera como Footprinting. En esta fase se emplean un conjunto de métodos y procesos donde los auditores recogen información relevante de los objetivos mediante fuentes abiertas en Internet. (Wren, Reilly, & Berry, 2010) Mediante el

empleo de diferentes herramientas de auditoría de seguridad se puede conseguir información útil para desarrollar las siguientes fases de manera eficaz, algunas de estas herramientas son:

- Google hacking: Mediante sentencias avanzadas en el motor de búsqueda de Google se puede acceder a información sensible o útil de organizaciones que no tengan asegurada óptimamente su información.
- Bing hacking: De manera análoga que Google hacking solo que utilizando estas sentencias en Bing.
- Shodan: Es un motor de búsquedas de dispositivos, activos y servidores conectados a Internet con una mala configuración y puertos abiertos. Se puede detectar dispositivos por región y por servicios expuestos.
- FOCA: Herramienta con funcionalidades de examinación de metadatos.

En una auditoría interna esta fase no es de relevancia y se la realiza de manera superficial debido a que la información interna generalmente no se encuentra filtrada por Internet. En las auditorías de seguridad web y perimetral si es de gran importancia ya que al tratarse de auditorías de caja negra toda la información recabada del objetivo es de suma utilidad.

Fingerprinting. Consiste en el proceso de recolectar información más específica sobre los objetivos descubiertos y analizados en la fase de footprinting. En base a la información recolectada se procede a encontrar vulnerabilidades propias de los sistemas objetivos. Entre la información más relevante que se puede obtener de este proceso sería:

- Sistema operativo de ordenadores remotos.
- Recolección de elementos de protección presentes entre el auditor y el elemento de red objetivo, como Firewalls, IDS, IPS, etc.
- Puertos y servicios abiertos en los sistemas.

- Versiones de software de los servicios que se ejecutan sobre los puertos abiertos.

Existen dos tipos de fingerprinting, el pasivo y el activo. El fingerprinting pasivo emplea herramientas que son configuradas con la finalidad de analizar y escuchar el tráfico en una red, con el fin de identificar ordenadores y servicios expuestos sin interactuar directamente con estos. En el fingerprinting activo las herramientas empleadas provocan una interacción directa entre la máquina del auditor y el objetivo, generando una respuesta por parte de este último.

Análisis de vulnerabilidades. En este paso se analizan todas las vulnerabilidades encontradas en los procesos de fingerprinting. A través de herramientas con bases de datos de vulnerabilidades se determina los exploits pertinentes para cada servicio expuesto en la máquina objetivo. La finalidad es seleccionar los procesos y herramientas más apropiadas a emplearse en las siguientes fases de la auditoría. A nivel de vulnerabilidades de red y web las principales herramientas son:

- Nessus
- BurpSuite
- IBM Security QRadar
- Qualys

Fase de Ataque

Explotación de vulnerabilidades. En esta fase se emplean las herramientas y procesos determinados en fases anteriores para explotar las vulnerabilidades encontradas en los hosts objetivos. A través de frameworks como Metasploit se puede realizar diferentes tipos de explotación, algunas se listan a continuación:

- Escalamiento de privilegios a través de una explotación local de vulnerabilidades.
- Creación de sesiones remotas con conectividad directa entre la máquina objetivo y el auditor.

- Explotación con ataques Client-Side.
- Instalación de backdoors para mantener la conexión sin conocimiento del administrador de la red objetivo.
- Carga de payloads.
- Ataques de denegación de servicio.
- Ataques de desbordamiento de buffer.
- Ataques de hombre en el medio (Men in the Middle Attack).
- Carga y transferencia de archivos con información sensible.

Fase de Post-Ataque

Generación de Informes. Finalmente, en todo proceso de auditoría se debe documentar adecuadamente todos los hallazgos y los resultados obtenidos. Generalmente se presentan dos tipos de informes:

- El informe ejecutivo destinado a todas las líneas de negocio pertinentes y responsables de los procesos vulnerables encontrados, con los hallazgos a alto nivel y recomendación de mitigación de riesgos de ser el caso.
- El informe técnico donde se indica la metodología empleada y datos más precisos del alcance de la auditoría. Se entrega información relevante de los sistemas vulnerables y está dirigido a personal técnico de la compañía auditada.
- Dependiendo del alcance de la auditoría contratada, también se suele entregar una carta de indicaciones donde se exponen las principales falencias y los puntos a mejorar a alto nivel por parte de la compañía.

Figura 12

Fases de una prueba de penetración de seguridad informática

Nota. La figura representa las fases de una prueba de penetración de seguridad informática. Tomado de *Metasploit,* por Rapid7 Inc, 2022.

Nmap

Es una herramienta de análisis de red, servicios y puertos, especialmente útil para evaluar la seguridad de los sistemas informáticos. Nmap emplea paquetes de IP sin procesar para diagnosticar que host se encuentran habilitados en la red, los servicios que prestan estos hosts indicando nombre y versión de la aplicación, que sistemas operativos y la versión del mismo se encuentran corriendo, el tipo de filtros de paquetes/firewall en uso, etc. (Gordon Lyon, 2022)

Entre las funcionalidades y ventajas principales de Nmap se encuentran las siguientes:

- Acepta varias técnicas avanzadas para identificar sistemas llenos de filtros IP, firewalls, routers y otros obstáculos. Permite la detección de sistemas operativos, versiones, barridos de peticiones ping, así como escaneos de puertos en TCP y UDP.

- Se puede auditar redes de gran cantidad de máquinas, que albergan miles de elementos.
- Ofrece una amplia gama de comandos y conjuntos avanzados para auditorías de red, además se puede emplear líneas de comando tradicionales y básicas para su funcionamiento.
- Existe una gran variedad de manuales, documentos técnicos, tutoriales y libros actualizados para el uso de la herramienta.
- Es software open source y se encuentra disponible para la mayoría de sistemas operativos ya que la herramienta es compatible. Se puede utilizar por líneas de comandos o por interfaz gráfica.

Metasploit

Es una herramienta de validación y explotación de vulnerabilidades en sistemas informáticos. Permite realizar auditorías y pruebas de penetración con ayuda de un flujo de trabajo configurable de acuerdo a las necesidades del auditor. (Rapid7 Inc, 2022) Mestasploit es un proyecto open source que alberga más de 900 exploits distintos. Entre las funcionalidades principales se pueden destacar las siguientes:

- Permite realizar un escaneo de descubrimiento para recabar información, además de admitir la importación de datos existentes de redes previamente auditadas.
- Mediante herramientas integradas como Nmap se puede identificar sistemas activos con servicios, descubriendo las posibles fallas sobre el objetivo escaneado.
- Permite la visualización y administración de los datos del host objetivo mediante vistas a alto nivel de los elementos de red incorporados en el proyecto.
- Admite la ejecución de un análisis de vulnerabilidades para determinar las diferentes debilidades de seguridad que la herramienta puede aprovechar y explotar. Expone las

vulnerabilidades detectadas en el host y publicadas en la lista de información de vulnerabilidades de ciberseguridad CVE.

- Explota las vulnerabilidades conocidas mediante la ejecución de exploits especialmente diseñados para los fallos identificados. Con una explotación exitosa se consigue acceso a los sistemas objetivos y se puede obtener información útil como hashes y archivos con información sensible.
- Posibilita instalar puertas traseras mediante el módulo de payloads. Además, se puede realizar la técnica de fuzzing para diagnosticar las fallas de un sistema o programa en materia de seguridad.
- Metasploit incorpora herramientas y métodos para eliminar las huellas producidas en una prueba de penetración.

Hping3

Es una herramienta que permite el análisis y envío de paquetes personalizados ICMP, TCP o UDP. Funciona de manera similar como una petición ping con respuestas ICMP. Posibilita el diseño de paquetes manipulando el cuerpo, tamaño y velocidad de transmisión de los mismos. Permite realizar distintas pruebas de detección sobre Firewallas, IDS (Intrusion Detection System), determina el rendimiento de la red con el uso de diferentes protocolos y genera la ruta del paquete enviado a través de su función avanzada de traceroute. Hping3 se maneja a través de línea de comandos y cuenta con parámetros avanzados para todas sus distintas funcionalidades. (OffSec Services Limited, 2022)

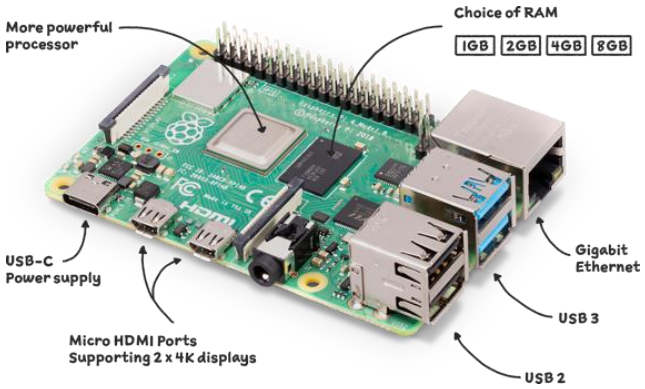
Raspberry Pi

Es una computadora de placa reducida de bajo costo, al igual que una computadora de escritorio puede hacer uso de hojas de cálculo, procesadores de texto y soportar diferentes sistemas operativos desarrollados específicamente para este modelo de ordenadores. (López, 2017) La Raspberry Pi emplea un microprocesador con arquitectura ARM, una GPU o tarjeta

gráfica y una memoria RAM en un solo chip, lo que indica que es un sistema SoC (System on a Chip). Existen diferentes configuraciones de RAM a la hora de adquirir el ordenador, partiendo de una configuración de 1GB hasta una de 8GB para la Raspberry Pi 4 modelo B. La placa no incluye un sistema de almacenamiento por lo que se debe hacer uso de una unidad de almacenamiento externa como una tarjeta SD. La placa dispone de diferentes conectores para su utilización, el modelo B de la Raspberry Pi 4 dispone de una ranura de tarjetas SD, un puerto USB-C para la alimentación, 2 puertos micro HDMI con soporte para monitores 4K, un conector Gigabit Ethernet, cuatro puertos USB dos 2.0 y dos 3.0 respectivamente.

Figura 13

Componentes de una Raspberry Pi



Nota. En la figura se aprecia la composición de una Raspberry Pi. Tomado de *Raspberry Pi*, por Raspberry Pi Foundation, 2022.

Internet de las Cosas

El Internet de las Cosas engloba todo tipo de ecosistemas que albergan objetos, artefactos, ordenadores, equipos médicos, etc., que en su estructura tengan incorporados componentes electrónicos, software y sensores con los cuales pueda obtener información constante de sus entornos y puedan transferir hacia otros sistemas o dispositivos de ser necesario. (Arroyo, Gayoso, & Hernández, 2020)

Honeypot

Los honeypot o señuelos son un recurso de seguridad utilizado como trampa para atraer a los delincuentes informáticos. Es una computadora diseñada de manera intencionada con vulnerabilidades para motivar al posible atacante y que este explote las fallas. El honeypot está diseñado de tal manera que captura información de relevancia de los ataques recibidos. Usualmente el señuelo simula sistemas que albergan información confidencial o crítica y que pueden ser ventajosas para los ciberdelincuentes. (Buchanan, Prasad, Chandramouli, & Benslimane, 2021)

Algunas de las razones para la implementación de un honeypot como solución de seguridad pueden ser:

- Permite identificar y estudiar las vulnerabilidades del propio sistema, esto si el honeypot es una copia del sistema real.
- Captura de diversos exploits realizados por los atacantes.
- Se puede desarrollar y comprobar las defensas contra exploits incluso antes de implementar en un sistema real.
- Permite crear un programa de inteligencia de amenazas y estudiar los diferentes eventos registrados por el honeypot.
- Detecta ataques internos si es que el honeypot se coloca de manera estratégica en la red interna.

Un señuelo permite la interacción con el adversario a diferentes niveles. Puede colocarse en diferentes partes de la red, dentro de la LAN, detrás de un router o detrás de un Firewall. Dependiendo de su ubicación se puede obtener un registro de operaciones completo del router o Firewall, detallando las pruebas realizadas por el cibercriminal y los puertos atacados. (Díaz, Alzórriz, Sancristóbal, & Castro, 2014)

Para hacer más atractivo al honeypot, se debe configurar un nombre de interés y llamativo que insinúa contener información valiosa de una organización. Se debe configurar adecuadamente para que el registro de logs no sea accesible para el atacante.

Tipos de Honeypot

Honeypot de producción

Son soluciones de seguridad que se colocan en arquitecturas de red en producción para encontrar vulnerabilidades o ataques internos que se presenten en el ecosistema. La principal razón de la implementación de estos señuelos es desviar la atención de los atacantes de sistemas realmente críticos. Con la exposición de servicios intencionalmente vulnerables se puede detener y contrarrestar el accionar del adversario o tomar acciones para evitar la paralización de las actividades cotidianas de la red de producción y no afectar al negocio.

Honeypot de investigación

Se diseñan para ser atacados y así poder estudiar el comportamiento de los atacantes. Son señuelos de alta interacción que generalmente se sitúan dentro de una red aislada y son expuestos a internet con el objetivo de contener las amenazas en el honeypot. Emulan sistemas operativos de organizaciones de alto perfil como departamentos gubernamentales, militares o empresas de alto renombre para atraer la mayor cantidad de atacantes. Principalmente son desarrollados e implementados por centros de investigación académicos, compañías de seguridad privadas y organizaciones gubernamentales de defensa.

Honeypot de baja interacción

Son señuelos que proporcionan funcionalidades básicas, por tal motivo son sencillos de instalar y configurar. Los honeypots de baja interacción emulan una cantidad limitada de servicios con los cuales el atacante puede interactuar. Al no ser honeypots tan sofisticados necesitan menos prestaciones de hardware para funcionar. El principal valor de estos honeypots es que sirven para detectar escaneos de puertos e intentos no autorizados de

conexión desde IPs extrañas. (Díaz, Alzórriz, Sancristóbal, & Castro, 2014) La información capturada por los honeypots es limitada ya que solo están diseñados para registrar comportamientos conocidos y no para descubrir nuevas técnicas o procedimientos de intrusión.

Honeypot de interacción media

Son sistemas trampa que están diseñados para tener una mayor interacción con el atacante sin llegar al nivel de los honeypots de alta interacción. Pueden simular el comportamiento de algunos de los principales servicios y vulnerabilidades conocidas. Están configurados para capturar más información de las técnicas y herramientas utilizadas por el adversario. Incluso se puede obtener el código utilizado, el procedimiento de acceso y elevación de privilegios que empleó el atacante. Al simular partes de sistemas o subsistemas de manera realista persuaden al atacante para que piense que se encuentra en un servidor de alta importancia.

Honeypot de alta interacción

Este tipo de señuelos proporcionan características más complejas y una mayor interacción con el atacante. Permite exponer un sistema real con diversas aplicaciones vulnerables para la interacción directa con el adversario. Por tal motivo los honeypots de alta interacción representan un mayor riesgo cuando es implementado en un entorno de producción. La mala configuración o supervisión de esta clase de honeypots genera riesgos a la red que los alberga. Los atacantes pueden usar este sistema como un nuevo agente malicioso para infectar o realizar ataques a otros sistemas de utilidad. A diferencia de sistemas reales convencionales, los honeypots de alta interacción no almacenan información relevante o sensible ya que están diseñados para ser comprometidos.

Honeynet

Es una arquitectura de seguridad sofisticada compuesta por dos o más honeypots. Está diseñada para registrar información de ataques que se realicen a los diferentes sensores que la

componen. Es una solución avanzada que puede ser integrada con otras herramientas de seguridad como Firewalls, sistemas de detección de intrusiones (IDS, por sus siglas en inglés) e incluso sistemas de gestión de eventos y seguridad informática (SIEM, por sus siglas del inglés) para relacionar los eventos registrados por los diferentes honeypots.

La honeynet es una arquitectura administrable y cuenta con un servidor centralizado para administrar cada sensor que la integra. Es una red completa compuesta por diferentes sistemas trampas diseñados para ser atacados. Dependiendo de la configuración de la honeynet se puede replicar redes completas emulando la de cualquier organización. Esta solución cuenta con herramientas que permiten detectar y filtrar el tráfico entrante. Determina los puertos, servicios y honeypots más atacados, todo de manera pasiva para que el adversario no note que está siendo supervisado.

Entre las principales funciones de la honeynet se detallan las siguientes.

- Control del adversario. Se debe contener los ataques realizados sobre la arquitectura del honeypot dentro de este. Se controla que las conexiones realizadas por el atacante repercutan solo sobre equipos de la honeynet.
- Registro de datos. Debe estar configurada para recolectar la mayor cantidad de datos e información de los ataques como sea posible. Esto con el fin de poder procesar estos datos y estudiarlos para fortalecer las redes y sistemas reales.
- Centralización de información. Para gestionar de mejor manera la información capturada por los distintos honeypots se debe disponer de un servidor centralizado de almacenamiento. Con esto se logra un registro más ordenado y se puede interrelacionar los eventos de cada señuelo.

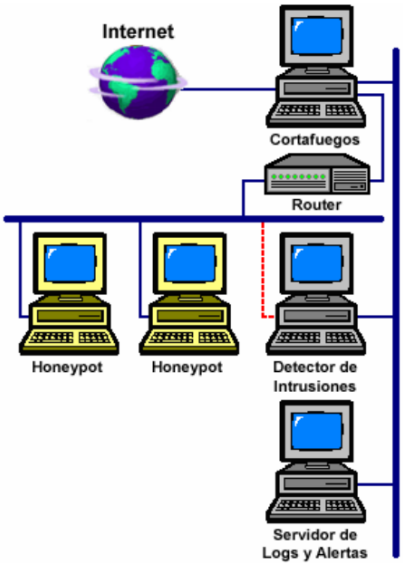
Tipos de Honeynets

Honeynet de Primera Generación

La primera generación de Honeynets se identifica por implementar mecanismos esenciales de control de flujo de datos y registro de datos. Físicamente esta generación es representada mediante una arquitectura de tres subredes conformadas por la Honeynet, la red de producción y la Internet todas separadas por un Firewall. El trabajo de control del adversario se realiza con ayuda del Firewall y el router. El Firewall filtra todos los paquetes entrantes o salientes de la red y segmenta la red, separando los honeypots del servidor de logs y el sistema de detección de intrusiones. La Honeynet junto al Firewall están configurados para permitir cualquier intento de conexión desde internet hacia los honeypots. Para ello se debe establecer un umbral de conexiones con el objetivo de bloquear las conexiones desde internet después de superar el mismo. (Gallego & López, 2004)

Figura 14

Arquitectura general de una honeynet de primera generación



Nota. La figura muestra la arquitectura de una honeynet de primera generación. Tomado de *Honeynets: Aprendiendo del Atacante*, por Gallego & López, 2004.

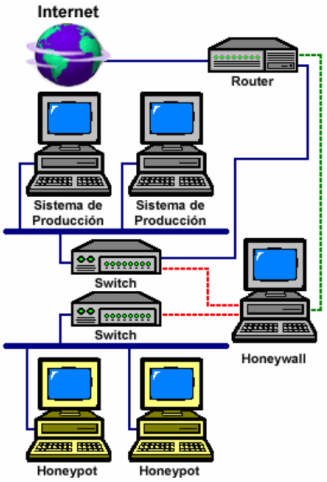
El router se coloca con la finalidad de ofuscar la presencia del Firewall con respecto a la red de honeypots, así el intruso al realizar una búsqueda del Gateway del sistema comprometido se encontrará con un router y no con el Firewall. La principal desventaja de este tipo de soluciones es que tiene una gran limitación con el control del adversario. Ya que si se permite un cierto umbral de conexiones pueden que todas de estas se consumen en un ataque exitoso y las medidas de contención implementadas no sirvan.

Honeynet de Segunda Generación

A diferencia de la generación anterior, la Honeynet de segunda generación combina el control del adversario, el registro de datos y la recolección de información en una única entidad, facilitando su implementación y administración. También acuñado Honeywall, este es un dispositivo de capa 2 que tiene la posibilidad de transmitir paquetes tipo puente. Esta cualidad permite que envíe los paquetes de extremo a extremo. Este dispositivo no genera ningún tipo de tráfico lo cual es beneficioso en caso de que el atacante quiera observar.

Figura 15

Arquitectura general de una honeynet de segunda generación



Nota. La figura muestra la arquitectura de una honeynet de segunda generación. Tomado de *Honeynets: Aprendiendo del Atacante*, por Gallego & López, 2004.

Honeynet de Tercera Generación

Mantiene la misma arquitectura y características que la Honeynet de segunda generación con la mejora en el apartado de registro de datos. Se implementan herramientas para catalogar de mejor manera eventos registrados por los honeypots. En esta generación se combinan los datos generados por las herramientas de registro de datos, permitiendo determinar la trazabilidad de las conexiones realizadas por los atacantes desde el administrador de honeypots.

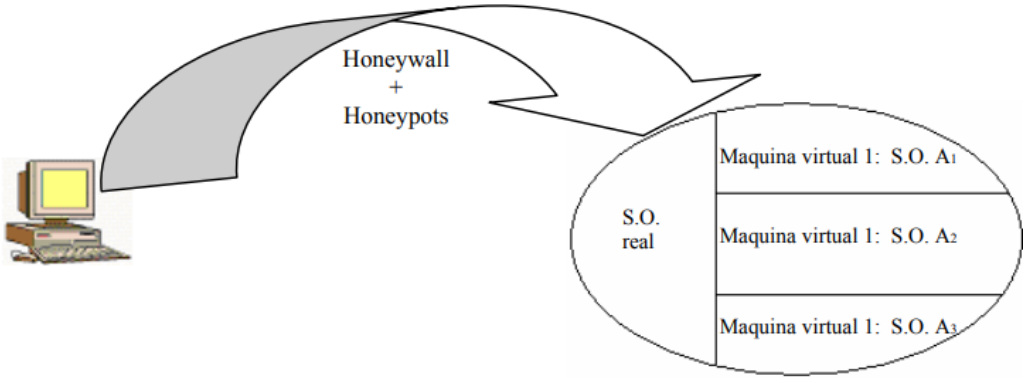
Dentro del Honeywall se despliega información segmentada de cada uno de los sensores, donde se reflejan datos capturados relevantes y estadísticas de conexiones.

Honeynet Virtual Autocontenida

En este tipo de arquitecturas todo el software de los diferentes honeypots corren sobre un mismo servidor. El honeywall y los honeypots se encuentran dentro del servidor. La ventaja de esta solución es el apartado económico ya que se necesita un único ordenador que contenga el sistema operativo anfitrión y el software de virtualización. (Verdejo, 2003)

Figura 16

Honeynet autocontenida



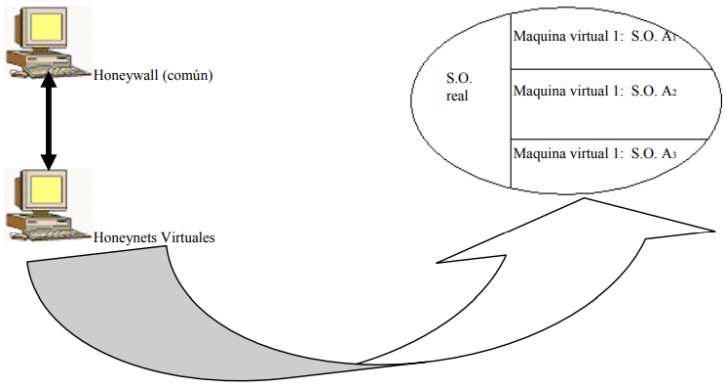
Nota. La figura muestra una honeynet virtual autocontenida. Tomado de *Seguridad en Redes IP*, por Verdejo, 2003.

Honeynet Híbrida

Este diseño como solución de seguridad implica que el Honeywall y los honeypots implementados se encuentren separados. Esta arquitectura supone una ventaja ya que se disminuye el peligro de que el adversario tenga acceso al resto de Honeynets. Es ideal para implementar diferentes modelos de Honeynets con ayuda de otros ordenadores y diseñar una solución más real que permita una interacción alta con los distintos atacantes. La Honeynet híbrida permite almacenar los registros fuera de la Honeynet virtual. Además, permite el escalamiento de la Honeynet de acuerdo a los recursos y necesidades del proyecto.

Figura 17

Honeynet Híbrida



Nota. La figura muestra una honeynet híbrida. Tomado de *Seguridad en Redes IP*, por Verdejo, 2003.

Directrices de Seguridad y Privacidad para el Internet de las Cosas

ITU X. 1361

La Unión Internacional de Telecomunicaciones propone un Marco de seguridad para el Internet de las cosas en el cual se estudian las amenazas y los principales problemas de seguridad informática presente en estos ecosistemas. Mediante este marco se abordan las

capacidades con las que se puede reducir las amenazas IoT y resolver las falencias de estos sistemas. (UIT-T, 2018)

El marco de seguridad estudia las principales amenazas de seguridad a la que están sujetas los sensores/dispositivos IoT. Se distinguen cuatro grupos de amenazas presentes en IoT.

- Amenazas de seguridad propias del sensor/dispositivo
  - Captura de dispositivo: Se origina cuando un sensor es afectado físicamente o cuando se desaparecen sus claves.
  - Ataque de sumidero: En este caso el dispositivo objetivo atrae todo el tráfico de comunicación. En este ataque el adversario utiliza los dispositivos para lanzar otros ataques.
  - Ataque Sybil: Busca disminuir la efectividad de los mecanismos tolerantes a fallos mediante un dispositivo malicioso que toma la forma de múltiples identidades.
  - Ataque por inundación: Es una variante de un ataque de denegación de servicios, el ciberdelincuente envía una secuencia de paquetes a un dispositivo para consumir recursos y no pueda responder a ataques legítimos.
  - Ataque de retransmisión selectiva: El nodo atacado retransmite paquetes recibidos al nodo subsecuente.
  - Suplantación de sensor/dispositivo: Un adversario se hace pasar por un dispositivo genuino.
- Amenazas propias de pasarela
  - Acceso no autorizado: Este ataque puede desembocar en la exfiltración, modificación o eliminación de datos de los sistemas.

  - Pasarela maligna: Los adversarios tienen la capacidad de implementar su propia pasarela maligna esto provoca que los dispositivos IoT puedan conectarse y poner en riesgo la información y la operación del sistema.
  - Ataque de denegación de servicio: Provoca una disminución abrupta en el servicio o la anulación completa del mismo.
- Amenazas propias de red
  - Acceso no autorizado: El acceso no autorizado a una red inalámbrica provoca un riesgo en la disponibilidad de los servicios y robo de información confidencial.
  - Rastreo de paquetes: Cuando la red de sensores IoT no posee la capacidad de encriptar la comunicación se vuelve fácil para los adversarios escuchar y capturar el tráfico de toda la red.
  - Bluejacking: Ataque dirigido a dispositivos Bluetooth.
  - Bluesnarfing: Mediante una conexión Bluetooth los atacantes pueden obtener de manera no autorizada información del objetivo.
- Amenazas propias de plataformas/servicios
  - Elaboración de perfiles utilizando información de plataformas y servicios del Internet de las Cosas.
  - Negación de servicio.
  - Ejecución de código remoto: El atacante ejecuta códigos maliciosos para afectar al sistema objetivo y provocar el fallo de sus recursos o también con el fin de utilizar al dispositivo como pivote de ataque.
  - Elevación de privilegios.
  - Inyección de lenguaje estructurado de consulta SQL para aprovechar vulnerabilidades en la configuración de la aplicación y extraer información confidencial de bases de datos.
  - Sniffing: Ataque que consiste en escuchar sigilosamente el tráfico de la red.

- Acceso no autorizado.
- Ataques de fuerza bruta: El atacante prueba todas las claves posibles hasta llegar a la exacta.
- Ataque de diccionario: El atacante prueba todas las claves seteadas en un diccionario especialmente diseñado para el sistema objetivo.
- Uso de credenciales por defecto.
- Contraseñas débiles.

El marco de seguridad de la UIT especifica los requisitos generales de seguridad con el que debe contar un ecosistema IoT. Entre estas capacidades generales la arquitectura IoT debe contar con las siguientes:

- Brindar una comunicación segura.
- Gestión de claves segura.
- Capacidad de gestión de datos de forma segura.
- Autenticación.
- Autorización.
- Gestión y monitorización de los accesos a los recursos del ecosistema.
- Prestación de servicios con seguridad.
- Capacidad de integración segura con diferentes políticas y herramientas de ciberseguridad.
- Gestión de Identidades y accesos.
- Análisis de vulnerabilidades.
- Enrutamiento multitrayecto.
- Capacidad de configuración segura.
- Cualidad de resistencia ante ataques de canal paralelo.

La capacidad de proteger los ecosistemas IoT abarca varias aristas. Se habló de las medidas generales que se deben considerar para proteger la arquitectura de estas redes. A continuación, se exponen las necesidades que deberían incorporar los sensores y dispositivos del Internet de las Cosas:

- Negociación de algoritmo criptográfico.
- Encriptación de datos, al igual que en los casos donde exista datos de plano de señalización.
- Asegurar la integridad de los datos transmitidos a través de redes inalámbricas.
- Proporcionar autenticación de la procedencia de los datos y de las identidades de cada sensor IoT y administradores de la red respectivamente.
- Gestión de parches y actualizaciones seguras.
- Incorporación de protocolos seguros.
- Administración y control de accesos.
- Prevención y/o localización de posibles alteraciones.
- Cualidad de protegerse contra irrupciones de canal paralelo.
- Capacidad de Firewall, detección y/o protección de intrusos.
- Control del tráfico de la red.
- Contar con un esquema que permita realizar configuraciones seguras sobre los dispositivos.

La seguridad de pasarelas también es primordial, es así que las medidas y capacidades con las que se debe contar incluye muchos de los puntos ya indicados para las otras aristas vistas. Se agrega a todas estas directrices la capacidad de tener la capacidad de disponibilidad sobre la red. Gestionando, conteniendo y mitigando posibles ataques de denegación de servicio, realización de pruebas de vulnerabilidad o pruebas de análisis de código seguro. Adicionalmente se debe contar con un plan de responsabilización de dispositivos IoT.

Finalmente, pero no menos importante, se presenta las cualidades necesarias con las que los ecosistemas deben contar para proteger las plataformas y/o servicios IoT:

- Modificación de credenciales de usuario administrador por defecto.
- Aplicación de políticas de contraseñas y control de accesos.
- Modificación de puertos no necesarios, habilitación o inhabilitación.
- Configuración segura.
- Protección ante infecciones de código maligno.
- Política de implementación de parches.
- Gestión de vulnerabilidades.
- Gestión de claves para la transferencia de mensajes de manera segura.
- Capacidad de disponibilidad ante posibles intrusiones.
- Monitorización de la red.
- Seguridad a nivel de aplicación.
- Apoyo para mitigar ataques de interferencia.

Como se observó la Unión Internacional de Telecomunicaciones describe varias capacidades con las que debe contar los ecosistemas IoT para protegerse en la actualidad. Las directrices de seguridad que debe tener la red no se incluyen y quedan fuera del alcance de la presente recomendación.

ISO/IEC 27002

Es una norma que agrupa las directrices relacionadas a la Seguridad de la Información. La referencia nace como pauta para que las organizaciones puedan seleccionar controles de seguridad para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Al mismo tiempo, esta norma puede utilizarse en el desarrollo de directrices de gestión

de seguridad de la información propias dentro de organizaciones e industrias tomando en cuenta sus entornos de riesgo. (ISO/IEC, 2013)

De esta normativa se seleccionan las directrices concernientes a las capacidades de protección de la red que recomendaciones como la de seguridad y privacidad de IoT de la UIT no incluyen. En tal sentido se exponen únicamente las siguientes medidas de seguridad:

- Seguridad física y del entorno
  - Perímetro de seguridad física.
  - Controles físicos de entrada.
  - Seguridad en instalaciones.
  - Protección contra las amenazas ambientales y externas.
  - Ubicación y protección de equipos.
  - Protección contra fallo en instalaciones de suministro.
  - Seguridad del cableado.
  - Mantenimiento de equipos.
  - Protección contra eliminación de activos.
  - Reutilización o eliminación segura de equipos.
- Seguridad de las comunicaciones
  - Controles de red.
  - Seguridad en los servicios de red.
  - Segmentación en las redes.

Capítulo III: Diseño

Este capítulo contiene el diseño completo de la Honeynet la cual es una solución de seguridad informática. La finalidad de esta solución es salvaguardar la integridad de red y servir como una herramienta versátil de detección y estudio de las principales técnicas empleadas por amenazas informáticas. Se requiere implementar esta solución para distraer a posibles adversarios externos o internos que intenten corromper la operatividad normal de los sistemas de información. El diseño cubre las principales características que todo entorno informático debe tener de acuerdo a los lineamientos de seguridad y privacidad de datos indicados por los organismos reguladores más relevantes a nivel mundial.

Planteamiento del escenario

Un arquitecto de red requiere adaptar una solución de seguridad informática que le permita detectar y monitorear amenazas dentro de la red de producción de su organización. Para validar la eficacia de su diseño el arquitecto de red implementó una solución de un invernadero inteligente basado en tecnología del Internet de las Cosas. Consecuentemente, este ecosistema está compuesto por diferentes sensores y actuadores para el control del riego automatizado y los sistemas de climatización. El invernadero inteligente consta de sensores para monitorear la temperatura en tiempo real y sensores para evaluar la humedad del suelo de manera periódica. Adicionalmente, existen sistemas de electroválvulas y ventiladores accionados de manera automática en respuesta a los datos recopilados por los sensores. Por último, todos estos sistemas se comunican por protocolo MQTT por lo que se cuenta con un servidor físico que aloja el bróker MQTT de la red IoT. Ante el incremento de ataques cibernéticos que han sufrido las empresas por la incorporación de nuevas tecnologías como IoT el arquitecto de red decidió diseñar e incorporar a su red una Honeynet híbrida. La implementación de esta solución permitirá al arquitecto de red monitorear, evaluar y capturar posibles amenazas dentro de su red. Se diseño la Honeynet para que pueda ser empleada en

diferentes tipos de sistemas informáticos que se basen en tecnologías emergentes o arquitecturas típicas sensibles a ataques. Para implementar esta herramienta de monitoreo emplea el uso de dos servidores físicos. El primero se trata del servidor de registro que se encarga de capturar, recopilar y almacenar los eventos registrados por los honeypots. Además, se configura una Honeynet virtual autocontenida dentro de este para incorporar a la arquitectura más señuelos que emulan diferentes servicios. El segundo servidor contendrá un honeypot físico, este dispositivo puede adaptarse a las necesidades específicas de hardware para garantizar el correcto funcionamiento del honeypot. Por consiguiente, en el diseño se consideran los honeypots que van a utilizarse y las especificaciones de hardware necesarias para la operabilidad y almacenamiento de la información capturada. La herramienta de seguridad se basa en software libre para reducir costes adicionales por uso de licencias. Asimismo, el arquitecto decide segmentar la red para aislar completamente los sistemas trampa. En consecuencia, evita exponer innecesariamente los equipos de producción. Una vez adecuada la solución de seguridad y la red IoT de producción se procederá a realizar una auditoría informática. De esta manera, el arquitecto de red puede evaluar la eficacia de la solución ante el monitoreo de amenazas cibernéticas.

Directrices de seguridad implementadas

En base a las recomendaciones y normativa vista sobre la seguridad y privacidad del Internet de las Cosas, se definen las directrices que se pretenden cubrir con esta solución de seguridad informática. Seguidamente se expone cada directriz con una breve explicación que justifique la necesidad de proteger cada arista de un ecosistema del Internet de las Cosas.

- Orientaciones generales
    - Comunicación segura: Dentro de la arquitectura propuesta, los honeypots cifran todos los datos y se envían a la Honeynet. Adicionalmente la ventaja de

implementar un broker MQTT recae cuando se utiliza el puerto 8883 para cifrar la comunicación mediante SSL/TLS.

- Autenticación de dispositivos: La honeynet maneja una clave única para identificar los sensores desplegados y conectados dentro de la solución.
- Capacidad de auditoría: El servidor de registros MHN recolecta toda la información captada por los sensores. Esta información es almacenada y mediante la misma se puede verificar el acceso o los intentos de acceso a los sistemas donde se encuentra implementada la herramienta.
- Integración segura: El servidor MHN permite integrarse con otras herramientas de seguridad para monitorear los eventos en la red como un SIEM.
- Gestión de identidades: Dentro del servidor de registros se puede configurar y agregar nuevos usuarios para administrar el mismo. Adicionalmente los routers utilizados dentro de la arquitectura permiten la creación de cuentas de usuarios con diferentes perfiles para la administración y configuración de los diferentes parámetros del dispositivo.
- Análisis de vulnerabilidades: El MHN analiza y cataloga las vulnerabilidades conocidas registradas por cada sistema trampa.

- Orientaciones de seguridad de pasarelas
  - Detección de intrusos: El MHN cumple las funciones de una herramienta de detección de intrusos (IDS).
  - Control de Acceso: Solo los usuarios con las credenciales de administrador pueden acceder a los diferentes elementos de red y a la información almacenada en los registros de eventos.

- Orientaciones de seguridad en la red
    - Perímetro de seguridad física: Los servidores físicos donde se aloja la solución se encuentran custodiados.
    - Seguridad en instalaciones: Solo el personal autorizado puede acceder a las instalaciones donde se encuentra desplegada la solución de seguridad.
    - Protección contra las amenazas ambientales y externas: Los servidores de la solución de seguridad no se encuentran desplegados en un ambiente hostil. Mientras tanto la solución IoT por su naturaleza está únicamente expuesta a un entorno previamente estudiado.
    - Seguridad del cableado: Todas las conexiones en las diferentes subredes de la arquitectura se encuentran debidamente protegidas.
    - Protección contra eliminación de activos: El servidor MHN al igual que cada uno de los servidores que contienen los honeypots se encuentran debidamente configurados para impedir el acceso a personal no autorizado.
    - Controles de red: El ecosistema IoT cuenta con controles de monitoreo y registro de eventos para descubrir posibles acciones que puedan corromper la seguridad de la información.
    - Segmentación en las redes: En la arquitectura propuesta se segmenta la red de producción IoT y la solución de seguridad de manera física.

Arquitectura

El apartado fundamental de esta solución de seguridad se centra en la ubicación y el tamaño de la Honeynet a utilizar, así como los servicios y puertos expuestos. El fin es lograr una arquitectura robusta y que permita registrar toda la actividad anómala de la red. En la Figura 18 se muestra el esquema de red de la Honeynet y del ecosistema IoT.

Como se evidencia la red se encuentra claramente segmentada, por un lado, se cuenta con un segmento donde se encuentra la solución de seguridad y por otro, un segmento que compone la red IoT. Esta decisión se toma con el objetivo de contrarrestar problemas asociados a ataques de intercepción como es el Sniffing. Al tener la red segmentada el administrador puede tener más control de los activos que pertenecen a cada subred de la arquitectura de la empresa. Si bien esta solución está siendo ejemplificada para una arquitectura pequeña, el principio de segmentación es aplicable a redes más grandes y complejas.

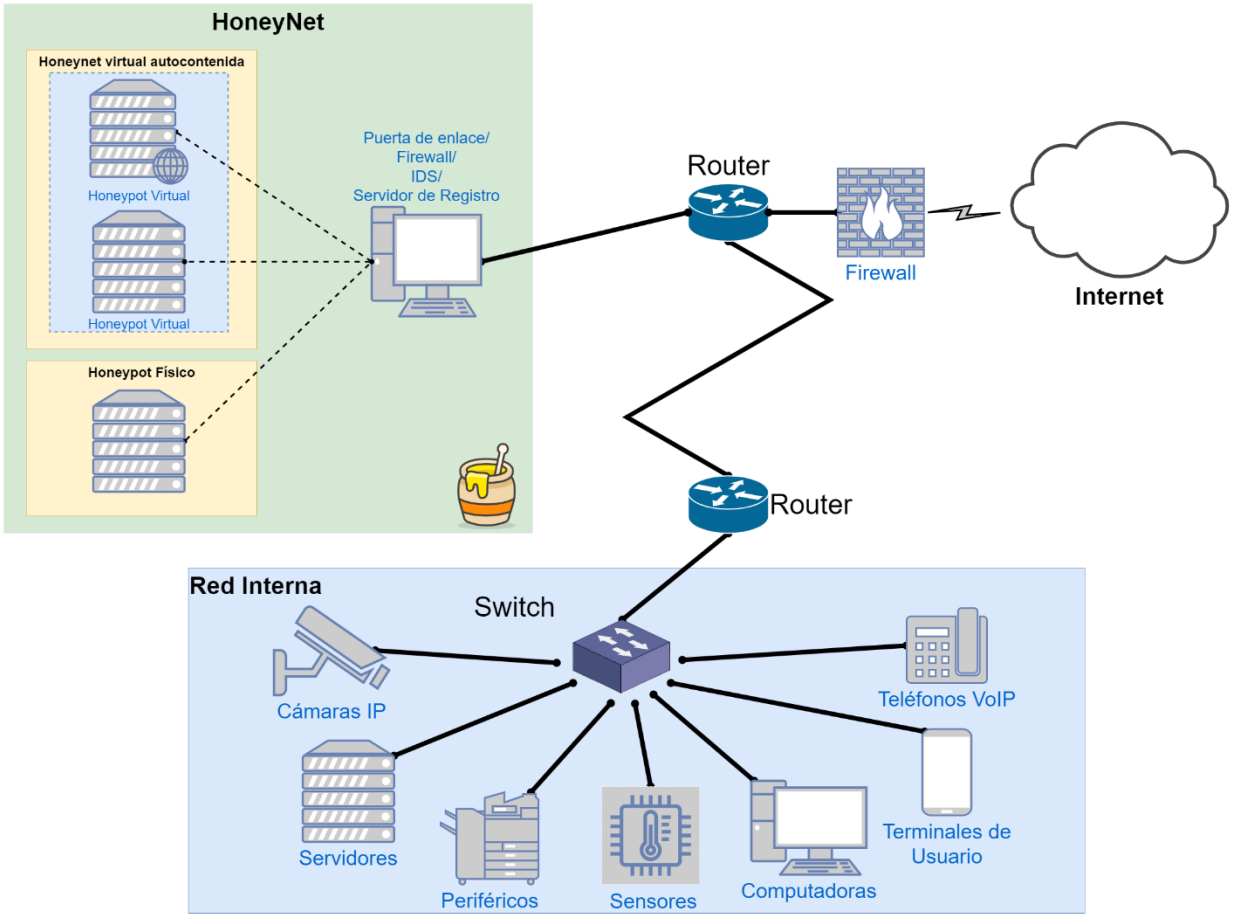
El arquitecto de red puede controlar la cantidad de equipos conectados a cada sub red de manera precisa. Consecuentemente los problemas asociados a ataques de suplantación también se contrarrestan. Para contar con una buena administración de activos, se debe identificar las direcciones MAC y las IP asociadas a cada elemento de red.

La arquitectura propuesta cumple con el principio de escalabilidad que los sistemas y redes hoy en día requieren. Permitiendo ampliar el tamaño de la Honeynet o incorporando a la red organizacional nuevas subredes de producción. También se puede crear nuevas subredes cada una con una solución diferente de Honeynet de acuerdo a la información que contengan los servidores. Inclusive esta arquitectura es totalmente migrable a ecosistemas basados en la Nube.

El firewall representado en la arquitectura propuesta por lo general está integrado dentro de la terminal de red óptica (ONT, por sus siglas en inglés) que entrega el proveedor de servicios de Internet (ISP, por sus siglas en inglés). Dentro del firewall es recomendable configurar listas de control de acceso, donde se definan reglas y se creen listas negras. El objetivo de crear listas negras es controlar y contener posibles ataques de ciertos dominios o IPs maliciosas ya conocidas. La configuración del Firewall debe impedir los principales intentos de conexión a causa de bots que escanean todas las redes con conexión a Internet.

Figura 18

Arquitectura de la solución de seguridad informática



Honeynet

El diseño de la solución de seguridad se basa en una Honeynet de tercera generación debido a la ventaja que supone el apartado de administración de datos. Los registros son almacenados y catalogados de una mejor manera. El sistema se compone por una Honeynet virtual autocontenida que a su vez está compuesta por dos honeypots instalados en servidores virtuales. Adicionalmente se incorpora a la Honeynet un honeypot físico instalado sobre un ordenador Raspberry Pi 4 del cual se hablará más adelante.

La Honeynet se encuentra ubicada detrás del firewall dentro de la red LAN de la organización con el fin de detectar ataques internos principalmente. Al ser una red de producción el objetivo es evitar que atacantes externos puedan ingresar. En caso de que los atacantes logren traspasar el Firewall la Honeynet implementada los distraerá hasta el momento en que el administrador pueda tomar medidas correctivas.

Es importante recalcar que la Honeynet no está diseñada para tener salida a Internet ya que el objetivo primordial es brindar una herramienta de protección y no una solución únicamente para investigación que es donde más sentido haría esta conexión. La Honeynet debe recabar información y técnicas de agentes nocivos que atenten contra la red de producción con el fin de mejorar continuamente su esquema de seguridad. En ningún momento se busca poner intencionalmente la red de producción en peligro exponiendo la Honeynet. Un posible fallo de configuración puede provocar movimientos laterales por parte de la amenaza y logrando que esta pueda llegar a afectar la red de producción.

Honeypots

Los señuelos utilizados deben primordialmente detectar ataques automatizados generalmente producidos por redes de bots que escanean activamente todos los sistemas conectados a internet para detectar posibles vulnerabilidades y aprovecharse de estas. Por tal motivo la elección más apropiada para cumplir con esta tarea sin acudir a una gran inversión de hardware es utilizar honeypots de baja interacción.

Al utilizar un ordenador de placa reducida como la Raspberry Pi se limitan las capacidades de cómputo de los sistemas, el honeypot de baja interacción es ideal para este tipo de equipos. La ventaja es que no se necesita un nivel de interacción alto con la amenaza el objetivo primordial va a ser captar las anomalías de la red. Para los servidores virtuales se puede implementar un honeypot que simule una base de datos y otro señuelo que simule un servidor de aplicación. Estos entornos son cotidianos en la mayoría de empresas alrededor del

mundo ya que por lo general tienen aplicativos que controlan ciertos procesos productivos. Se optará por un señuelo de interacción media en el servidor que simula la aplicación diseñada con el fin de crear un poco más de interacción con el posible atacante.

Red Interna

De manera general se ejemplifica la composición de la red interna de las organizaciones, estas a su vez contienen diferentes subredes. Por tal razón la solución de seguridad informática está diseñada para proteger cualquier tipo de estos entornos ya que la misma se encuentra ubicada fuera de esta. La red interna puede estar compuesta por subredes de cámaras IP, granjas de servidores, conjunto de teléfonos VoIP, subredes mixtas que alberguen dispositivos de usuario final como computadores, terminales de usuario y periféricos. También pueden estar compuesta por dispositivos como sensores y actuadores como es el caso de ecosistemas del Internet de las Cosas. En cualquiera de estos escenarios la solución garantiza su correcto funcionamiento siempre y cuando se realicen las configuraciones adecuadas para cada caso.

Capítulo IV: Implementación

Hardware

Para la implementación de esta solución de seguridad informática se ha utilizado diferentes elementos de red, cada uno de ellos se explica a continuación:

Tabla 6

Elementos de la red implementada

Cantidad	Elemento de red	Descripción
1	*Raspberry Pi*	Es un ordenador de bajo costo el cual alojará un honeypot físico. Características: • RAM: 2 GB • Procesador: Broadcom BCM2711
1	*Computador Asus*	Computador con altas capacidades para el alojamiento de parte de la honeynet así como el servidor de registro. Características: • RAM: 16 GB • Almacenamiento: 512 GB Estado Sólido. • Sistema Operativo: Windows 10 • Procesador: Intel Core i7
1	*Optical Network Terminal*	Es el router que generalmente el ISP entrega al momento de la instalación de un servicio de Internet por fibra óptica.

Cantidad	Elemento de red	Descripción
1	*Router Inalámbrico*	Se seleccionó uno de acuerdo a las necesidades de cobertura de la red IoT y dependerá también de la frecuencia que trabajen los elementos de red a los que de servicio.

Configuración del Raspberry Pi

Dado que el ordenador no cuenta con una memoria de almacenamiento este no tiene un sistema operativo instalado de fábrica. Por tal motivo con la ayuda de otro ordenador se debe descargar la imagen de la página oficial de Raspberry Pi. Dada la arquitectura propuesta y de acuerdo a los requerimientos de sistema operativo para ejecutar el honeypot. Se debe elegir el sistema operativo Raspberry Pi OS (Legacy) disponible en la siguiente dirección web https://www.raspberrypi.com/software/operating-systems.

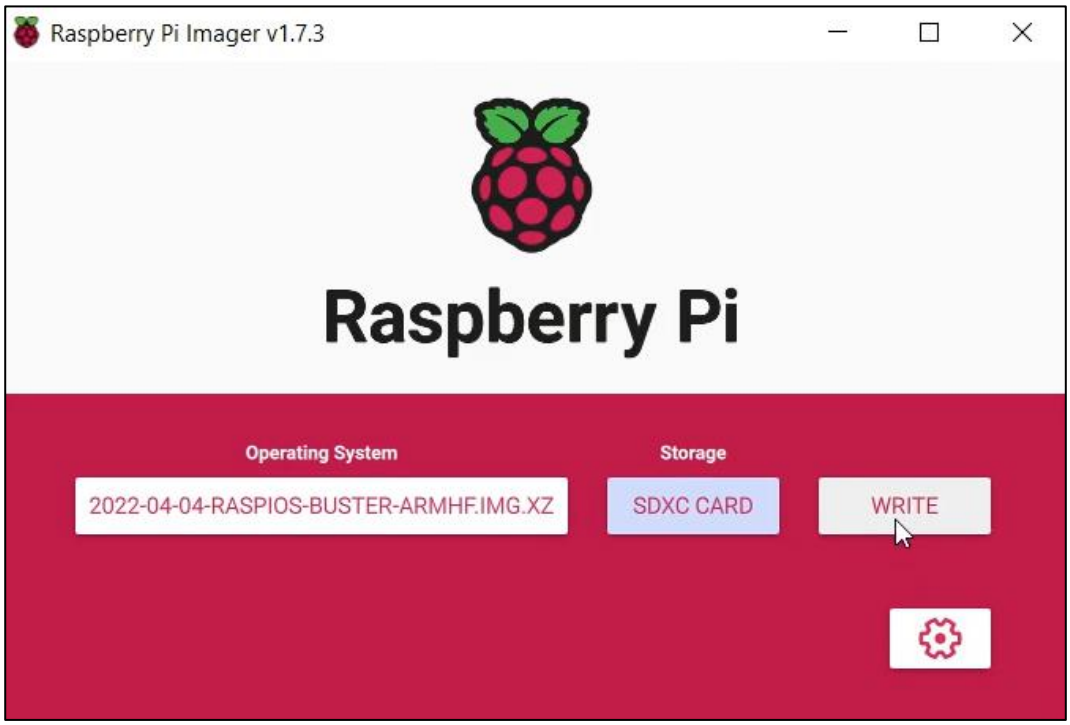
Para poder cargar la imagen en una unidad de almacenamiento se necesita de una tarjeta SD y se requiere descargar un software adicional que permite realizar este procedimiento. La herramienta que se emplea se llama Raspberry Pi Imager la cual se encuentra en el siguiente enlace https://www.raspberrypi.com/software. Una vez instalado el Imager se debe insertar la tarjeta SD al ordenador, cargar el sistema operativo, seleccionar la unidad de almacenamiento y escoger la opción escribir para que comience el procedimiento como se indica en la Figura 19.

Realizado los pasos anteriores se extrae la tarjeta SD y se inserta en la Raspberry Pi. Posteriormente se procede a encender el ordenador, se inicia el sistema operativo con una pantalla de bienvenida. Enseguida se debe configurar el idioma, el país y la zona horaria. Continuando con la configuración se debe crear un usuario dentro del sistema operativo, por lo que en este apartado se debe ingresar un usuario y contraseña. Por último, se debe

seleccionar una conexión de red WiFi, para el sistema propuesto se va a conectar mediante puerto LAN la Raspberry Pi por lo que este paso se salta. Una vez que se configura todos estos parámetros se debe reiniciar el ordenador.

Figura 19

Interfaz Raspberry Pi Imager



Software de Virtualización

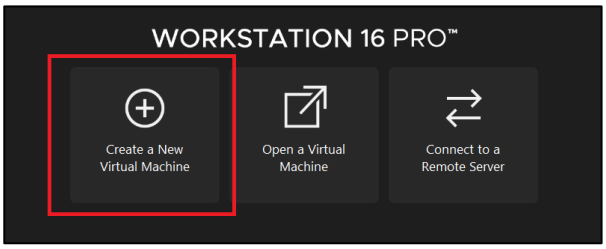
Para la virtualización de los honeypots y el servidor de registro se utilizó el hipervisor VMware Workstation, mediante el cual se pudo crear y administrar tres máquinas virtuales las cuales conforman parte de la red de honeypots propuesta incluyendo el servidor de administración de la Honeynet. Adicionalmente sobre todas las máquinas virtuales creadas se ejecuta el sistema operativo Ubuntu 18.04 LTS el cual es una distribución de Linux basada en Debian GNU/Linux.

Configuración de la máquina virtual

Para implementar el servidor centralizado para la gestión y recopilación de eventos de los honeypots se crea una máquina virtual en el hipervisor VMware Workstation

Figura 20

VMware Workstation 16



Se selecciona la opción de Create a New Virtual Machine, por practicidad se selecciona la configuración típica recomendada por el desarrollador.

Figura 21

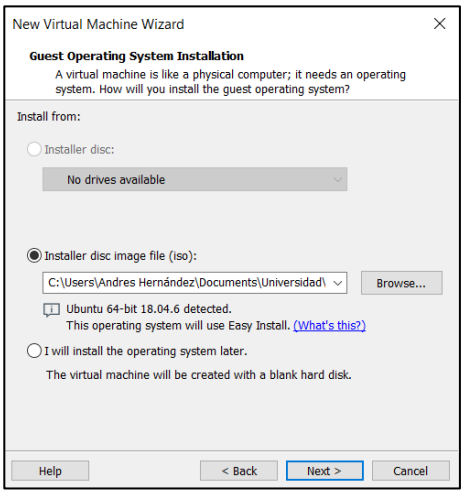
Creación de una máquina virtual en VMware

Nota. Creación de una nueva máquina virtual en VMware Workstation 16 Pro seleccionando la configuración típica.

Previamente se debe tener descargado la imagen ISO del sistema operativo que se va a ejecutar en la máquina virtual, en este caso ese sistema operativo es Ubuntu 18.04 LTS el mismos que se encuentra en la página oficial https://releases.ubuntu.com. Se escoge la segunda opción para utilizar la imagen descargada e instalar el sistema operativo, como se indica a continuación:

Figura 22

Instalación del sistema operativo anfitrión

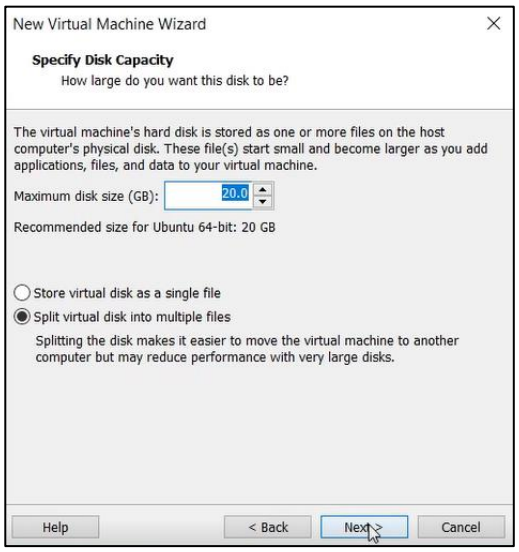


Nota. Selección de la imagen ISO que contiene el sistema operativo del servidor.

Se personaliza el nombre y se agrega las credenciales del usuario, en el presente trabajo se optó por simplificar las credenciales de este administrador. Pero si este ecosistema se pretende implementar en un ambiente de producción empresarial se recomienda personalizar el usuario y crear una contraseña compleja que contenga al menos 12 caracteres, al menos una mayúscula, una minúscula, un número y un carácter especial. Esto con el fin de robustecer la arquitectura propuesta. Posteriormente, se asigna un nombre a la máquina virtual, aquí se recomienda seguir la política de identificación que la empresa cuente para diferenciar claramente este servidor, en caso de no contar con una política se debe asignar un nombre distintivo. Además, se debe especificar la capacidad de disco de la máquina virtual creada.

Figura 23

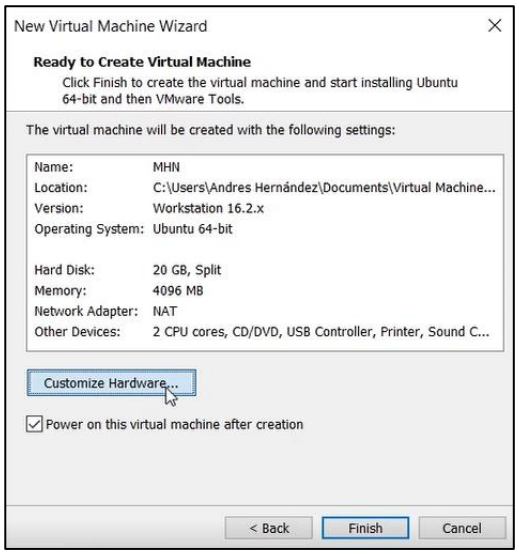
Configuración de la capacidad



Por último, se indicará un resumen de las configuraciones que tendrá la máquina virtual creada. Se debe seleccionar la pestaña de modificar hardware para configurar la cantidad de memoria RAM asignada, el número de procesadores y el adaptador de red que va a utilizarse.

Figura 24

Personalización de la máquina virtual



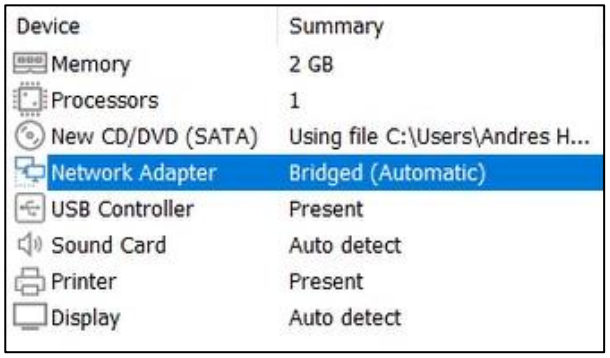
Como se indica en la imagen, se configuró de la siguiente manera:

- **Software de virtualización:** VMware Workstation 16.2.4
- **Procesadores:** 1 núcleo
- **RAM:** 2 GB
- **ROM:** 20 GB
- **Adaptador de red:** Bridged (Automatic)

El adaptador de red de las máquinas virtuales se configura en modo puente con el fin de que los servidores virtualizados formen parte del mismo segmento de red donde se ubica la Raspberry Pi. Posteriormente modificado estos parámetros se selecciona la opción de finalizar y automáticamente se encenderá la máquina virtual después de la creación.

Figura 25

Especificaciones de la máquina virtual creada

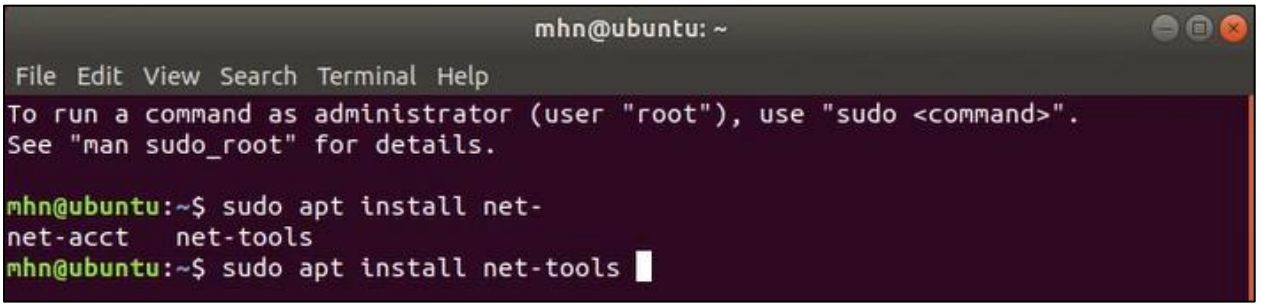


Nota. Asignación de recursos para la máquina virtual creada, configuración de RAM, adaptador de red y número de procesadores.

Una vez creada y ejecutada correctamente la máquina virtual, se abre una terminal para visualizar la dirección IP asignada dentro de la red. Primeramente, se debe instalar el paquete net-tools para poder utilizar el comando ifconfig y observar la información que se necesita.

Figura 26

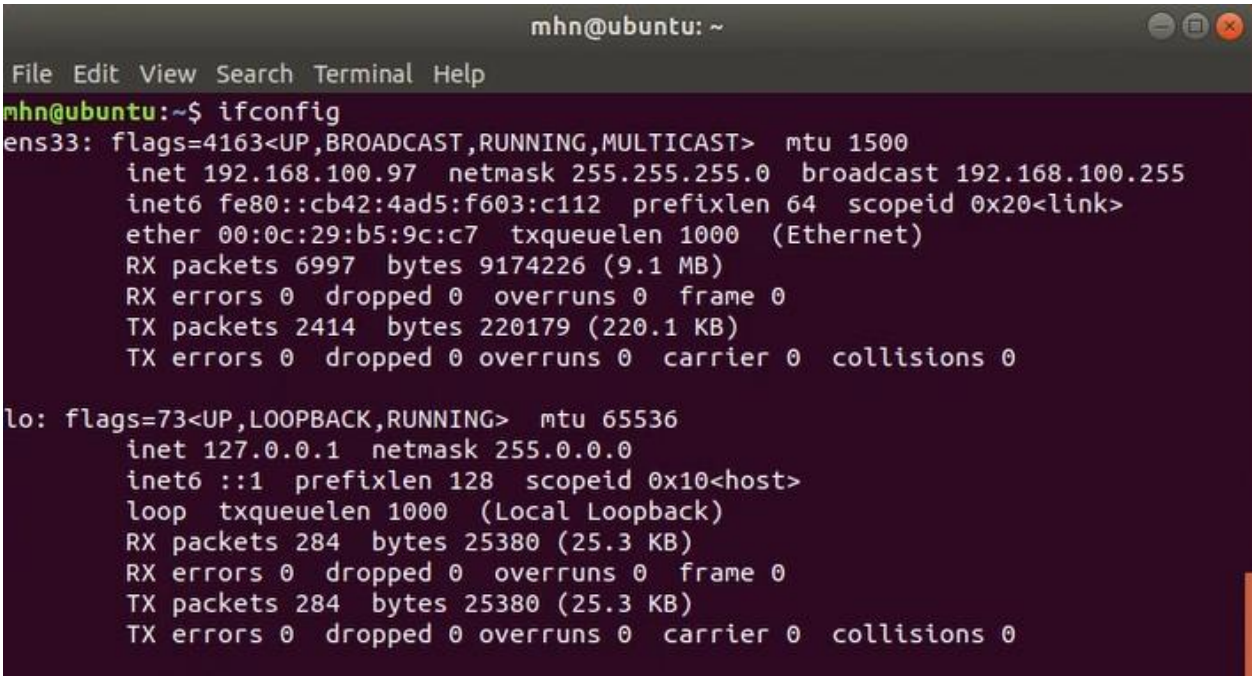
Instalación del paquete net-tools



Una vez realizado se evidencia a continuación que la IP asignada al administrador de eventos es la 192.168.100.97.

Figura 27

Visualización de la dirección IPv4



Nota. Ejecución del comando ifconfig dentro de una terminal de Ubuntu para verificar la dirección IPv4 asignada a la máquina virtual.

Modern Honey Network

Es el servidor centralizado para la administración y recolección de los datos registrados por los honeypots implementados. A continuación, se detallan algunas de las ventajas que presenta este servidor:

- Permite la implementación de diferentes señuelos de forma rápida.
- Configura automáticamente la conexión entre servidor de administración y sistema trampa.
- Cuenta con diferentes tecnologías de honeypot, incluyendo las más comunes.
- Posee una interfaz gráfica web.
- Existe una comunidad que constantemente está resolviendo posibles fallos de la solución.
- Software de código abierto.
- Existe amplia documentación sobre la herramienta.
- Permite la integración con herramientas de seguridad como el SIEM.
- Cuenta con un gran catálogo de reglas de seguridad definidas de manera nativa.
- Recopila toda la información de los diferentes sensores implementados.
- Almacena toda la data de manera sigilosa, centralizada y automáticamente.

Los honeypots no son admitidos como una solución de defensa en la mayoría del sector empresarial menos aún para soluciones del Internet de las Cosas. Esto se debe a la complejidad que conlleva la configuración e instalación de los mismos. Con la presente solución de seguridad se pretende dotar y ampliar de herramientas de seguridad informática a entornos emergentes como la industria IoT. Esta herramienta simplifica la instalación y mantenimiento de los honeypots a la vez que ofrece una interfaz amigable para el monitoreo de amenazas.

Para proceder con la instalación del administrador se debe contar con el paquete Git para la cual se ejecuta la siguiente instrucción:

sudo apt install git -y

Realizado el paso anterior se cambia de directorio con el comando

cd /opt/

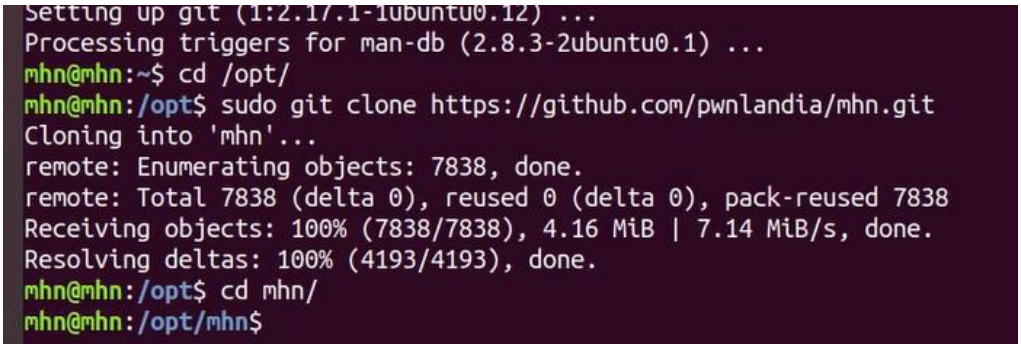
Se clona del repositorio de MHN la herramienta y se ingresa en el directorio descargado

sudo git clone https://gituhub.com/pawlandia/mhn.git

cd mhn/

Figura 28

Clonación del repositorio del MHN



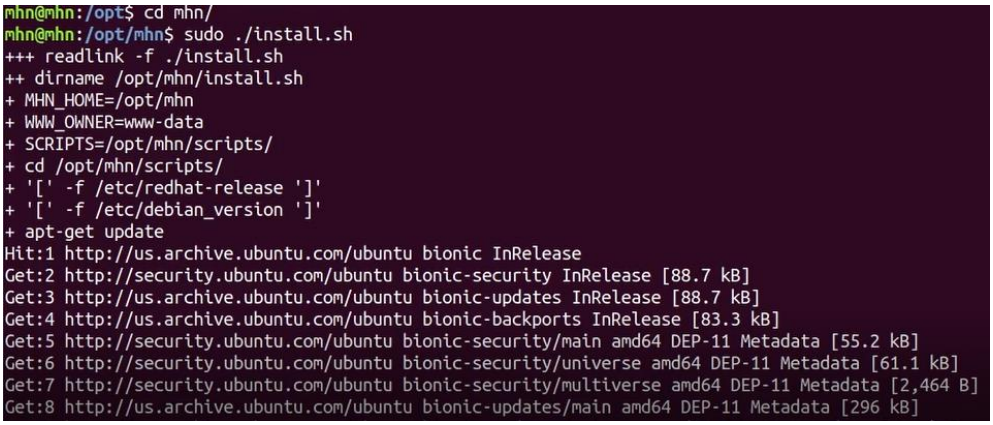
Nota. En la figura se indica el proceso de clonación de la herramienta MHN dentro de la máquina virtual a través de una terminal de usuario.

Una vez realizado este paso se ejecuta la siguiente instrucción para instalar el administrador de eventos en el servidor.

sudo ./install.sh

Figura 29

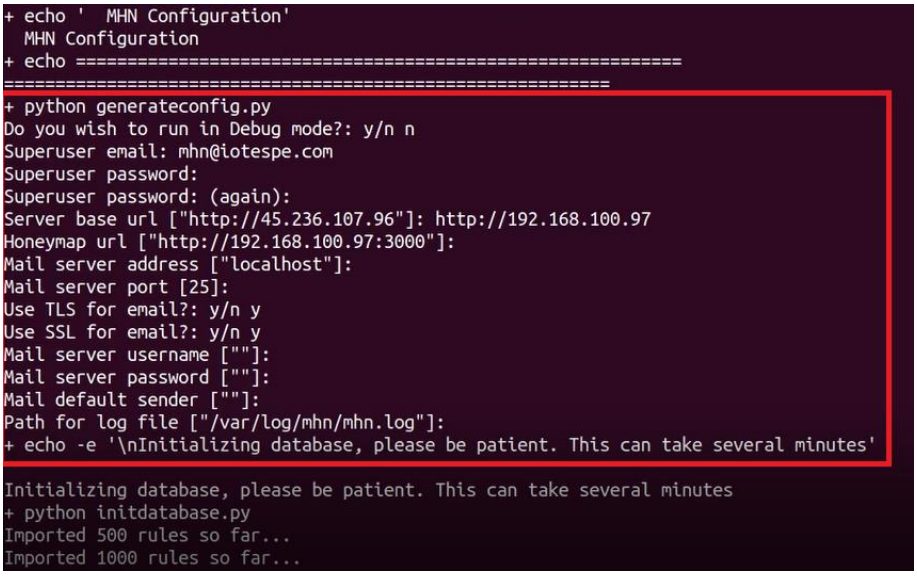
Instalación del MHN



La instalación se realiza de manera automática, suele demorar entre 15 y 20 minutos. Mientras se ejecuta el script se solicitará cierta información para realizar la configuración del administrador. Se debe especificar el correo y credenciales del administrador, la IP del servidor donde se alberga y parámetros que debido a la arquitectura propuesta se puede pasar por alto, la configuración recomendada se indica a continuación:

Figura 30

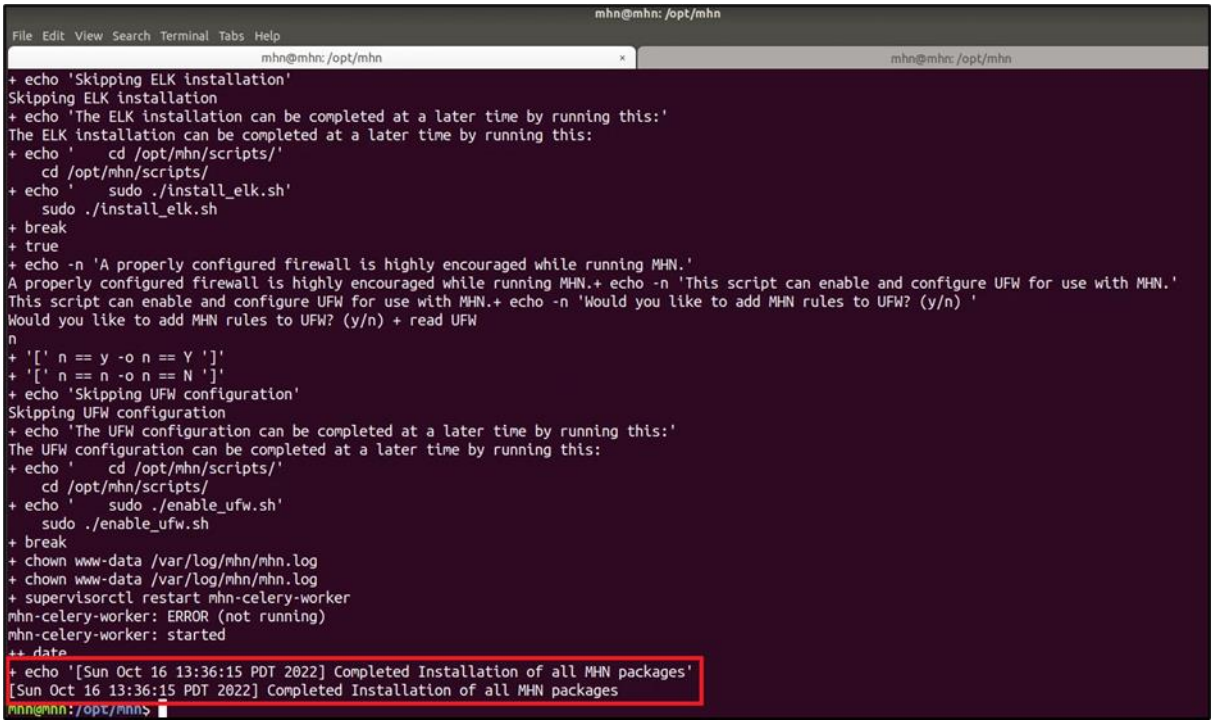
Configuración del MHN



Después de configurar estos parámetros se empezarán a importar las reglas del servidor. En las preguntas donde se indique si se desea instalar ELK y agregar las reglas del MHN al UFW se selecciona la opción no. La instalación finaliza con el mensaje de que todos los paquetes del MHN han sido instalados.

Figura 31

Instalación finalizada del MHN



Nota. En la imagen se aprecia el mensaje de instalación satisfactoria de todos los paquetes de la herramienta MHN.

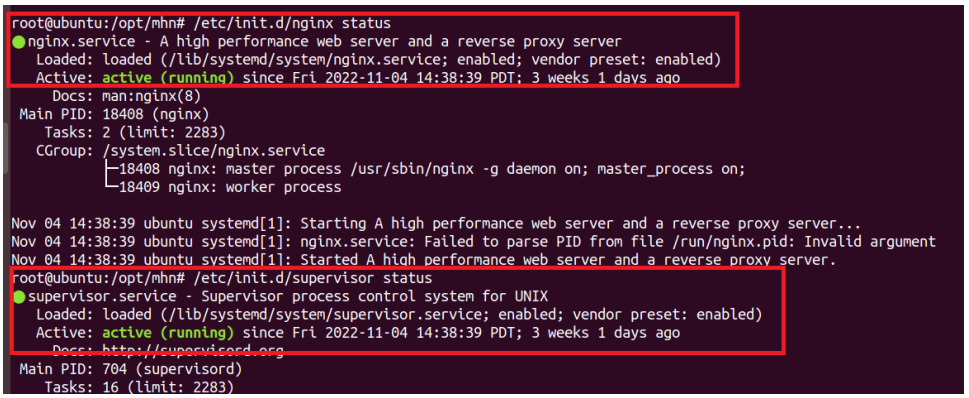
Se procede a verificar que el servicio web se encuentre levantado y el funcionamiento sea el adecuado, con perfil de root se procede a comprobar mediante terminal los servicios que se están ejecutando en el servidor con las siguientes instrucciones:

/etc/init.d/nginx status

/etc/init.d/supervisor status

Figura 32

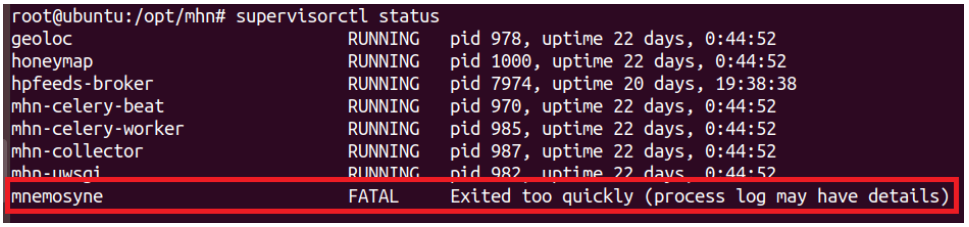
Verificación de los servicios levantados



supervisorctl status

Figura 33

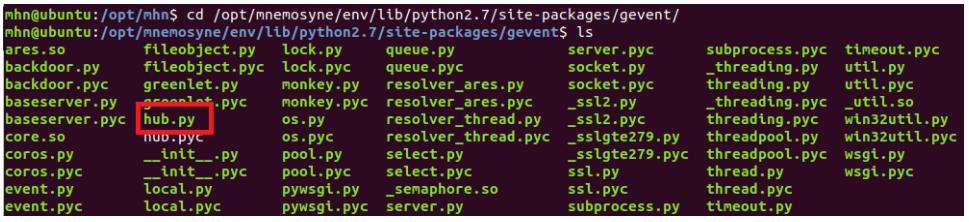
Procesos ejecutándose en la máquina virtual



Debido a que el servicio mnemosyne no se está ejecutando, se debe remover la sección de greenlet_version del fichero hub.py. Este fichero se encuentra en el siguiente path /opt/mnemosyne/env/lib/python2.7/site-packages/gevent/

Figura 34

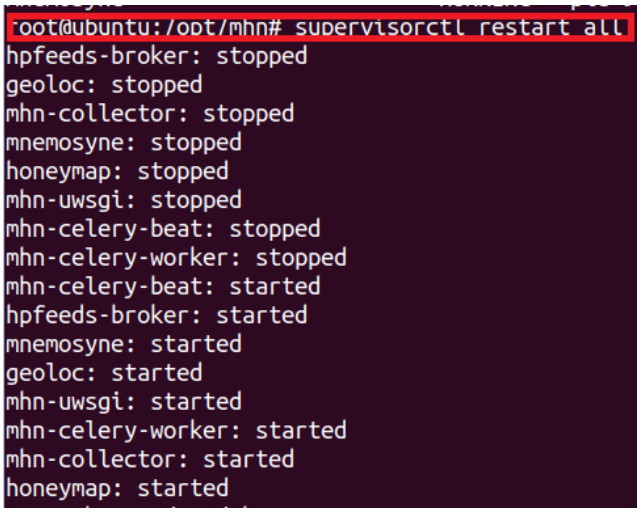
Listado de ficheros en la carpeta gevent



Una vez realizada esta acción se debe guardar el fichero con todos los cambios indicados y reiniciar todos los servicios que se estaban ejecutando con el objetivo de comprobar si ahora el servicio mnemosyne marcha de manera correcta.

Figura 35

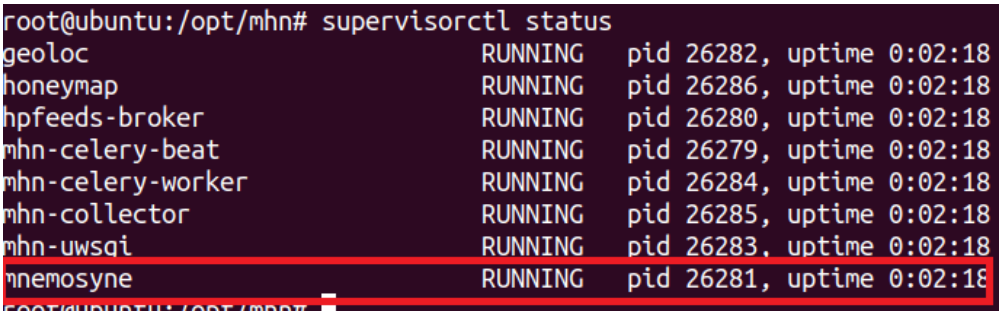
Reinicio de todos los procesos en MHN



Al comprobar que todos los servicios se inician correctamente visualizamos el estado de cada uno de ellos y efectivamente el servidor MHN ya se encuentra funcionando correctamente.

Figura 36

Estado de los procesos del MHN

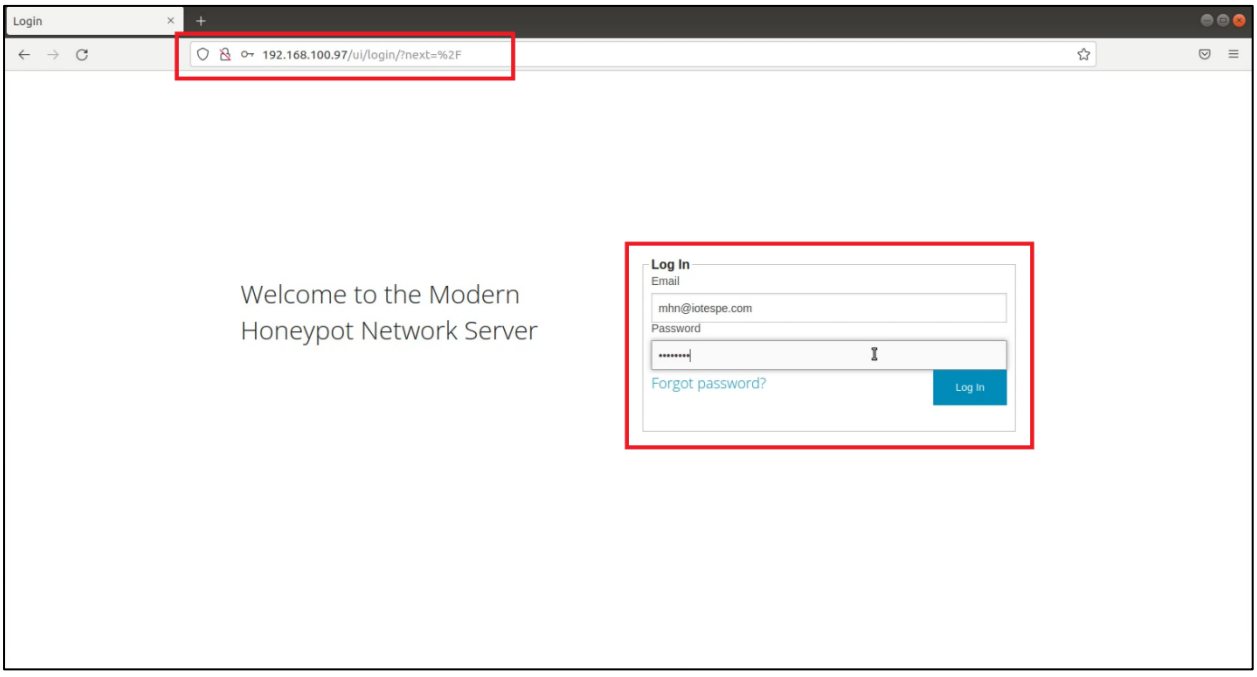


Nota. El proceso mnemosyne ya se encuentra ejecutándose con normalidad con el PID 26281.

Se verifica que todos los servicios están corriendo por lo que a continuación, se abre el navegador web y se digita la IP del servidor. Se desplegará la pantalla de inicio en la cual se debe ingresar las credenciales del usuario administrador que previamente se habían configurado.

Figura 37

Interfaz Web MHN

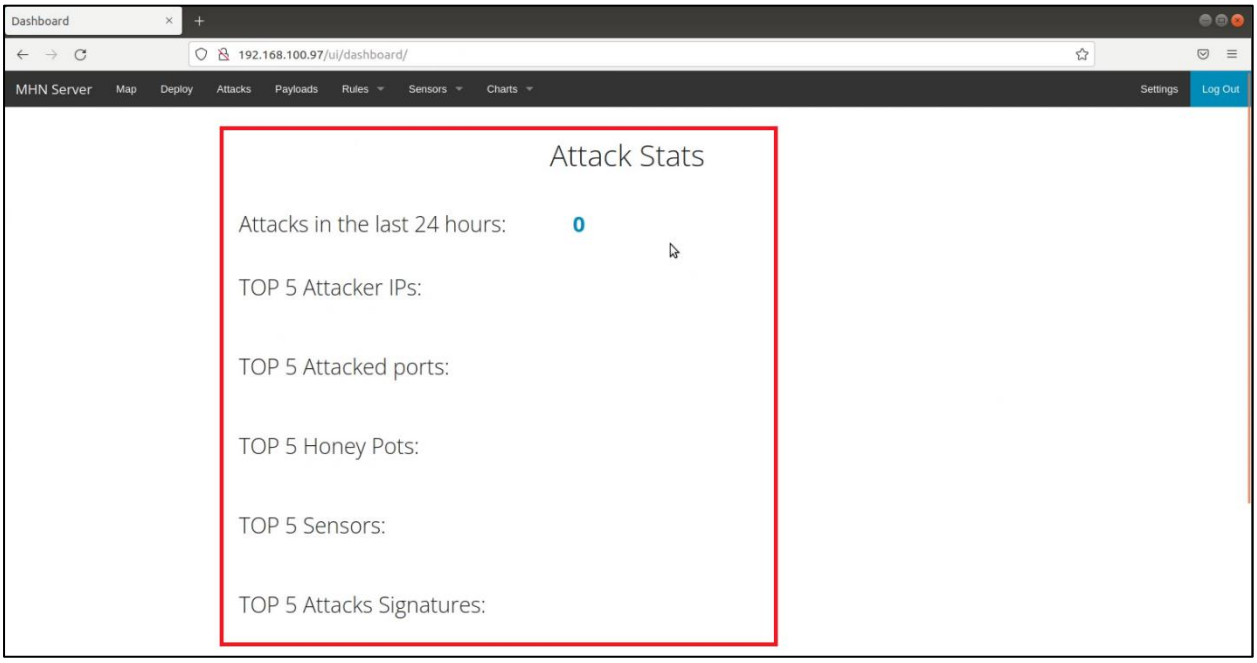


Nota. En la figura se muestra la pantalla de inicio de sesión que tiene la herramienta MHN dentro de la cual se deben ingresar las credenciales configuradas en la instalación.

Una vez iniciada sesión se visualiza el tablero general del administrador y sus diferentes pestañas. De manera general muestra información de los ataques realizados las últimas 24 horas, las IPs con más ataques registrados, los honeypots más atacados, los diferentes señuelos más atacados y desplegados, por último, se indican las 5 firmas de ataques más empleadas.

Figura 38

Dashboard del MHN



A continuación, se presenta una tabla donde se describe cada una de las pestañas del servidor de eventos implementado.

Tabla 7

Opciones del servidor MHN

Opción	Descripción
Map	Permite visualizar un mapa global de los diferentes países de donde provienen las IPs atacantes.
Deploy	Permite observar y configurar los parámetros para desplegar los diferentes honeypots disponibles y soportados por el servidor MHN.
Attacks	A través de esta opción se puede determinar el número de ataques realizados a cada uno de los honeypots.

Opción	Descripción
Payloads	Se observan las cargas útiles registradas por cada sensor.
Rules	Detalle de todas las reglas configuradas en el servidor de eventos.
Sensors	Permite visualizar todos los señuelos implementados y administrados por el servidor, así como información relevante de cada uno de ellos.
Charts	Permite obtener gráficos de los eventos registrados por ciertos honeypots.

Nota. Esta tabla especifica las diferentes opciones que tiene el servidor MHN.

Honeypot Drupot

Generalmente las compañías incorporan servicios web en sus arquitecturas de red internas con el objetivo de manejar las distintas bases de datos y aplicaciones. Drupot es diseñado de tal manera que simule una de estas interfaces web que permiten la configuración de dichos sistemas. Cumpliendo la premisa de atraer al atacante y desviar su atención de sistemas críticos, la interfaz gráfica del honeypot implementado busca imitar un servidor de administración.

Drupot es un honeypot de interacción media, el mismo fue seleccionado debido a que permite detectar los principales ataques a los que están expuestos las aplicaciones web. Ataques de Cross-Site scripting, Inyección SQL, Denegación de servicios son detectados por este sistema trampa. El servidor web contiene una interfaz atractiva e informativa relacionada a sistemas de sensado. La información de la página es valiosa e incita al atacante a ganar más privilegios para llegar a sistemas más sensibles. Dentro de la interfaz gráfica se encuentra un módulo de inicio de sesión, donde el atacante puede acceder y realizar ataques sobre este. El módulo registra todas las entradas que el atacante realice y las almacena en un archivo log. Adicionalmente con cada entrada se registran datos relevantes del ataque como fecha y hora de la solicitud, ip de origen del ataque, incluso se captura todas las instrucciones empleadas

por el atacante. Se puede determinar de manera específica las tácticas y el procedimiento que emplea el delincuente.

A continuación, se presenta un resumen con los puntos más destacables que convierten al honeypot Drupot en parte de la solución de este ecosistema de seguridad:

- Honeypot de interacción media.
- Emula servicios web.
- Posee una interfaz web atractiva.
- Permite detectar ataques de inyección de código.
- Registra todas las conexiones entrantes al sistema.
- Bloquea a los robots de spam.
- Fácil configuración e integración dentro de una arquitectura de red.
- Existen manuales disponibles para su correcta configuración.
- Fácil administración y mantenimiento.

Es preciso aclarar que a pesar que el señuelo detecta ataques de denegación de servicio (DoS) no es una solución orientada a contener o responder a este tipo de ataques, para eso existen otras herramientas como Imperva, NetScout, FortiDDoS, entre otras.

Una vez configurada la máquina virtual con el sistema operativo Ubuntu 18.04 LTS como se indicó anteriormente se debe comprobar que exista conexión directa con el servidor MHN. Para comprobar la comunicación se procede a realizar una petición ICMP con el comando ping seguido de la IP 192.168.100.97 correspondiente al servidor MHN.

Después de comprobar que existe comunicación hay que dirigirse al servidor MHN y seleccionar la opción Deploy en donde se debe seleccionar el script correspondiente al Honeypot Drupot.

Figura 39

Verificación de conexión

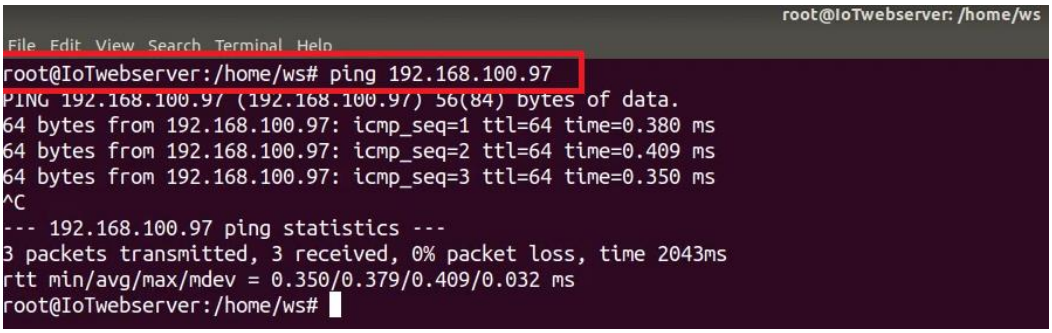
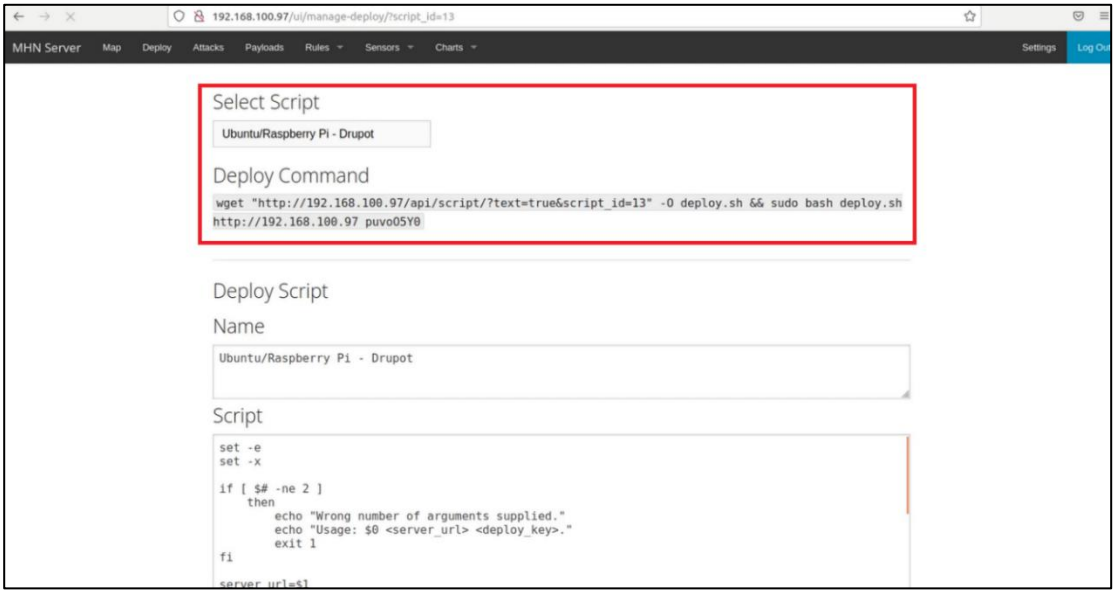


Figura 40

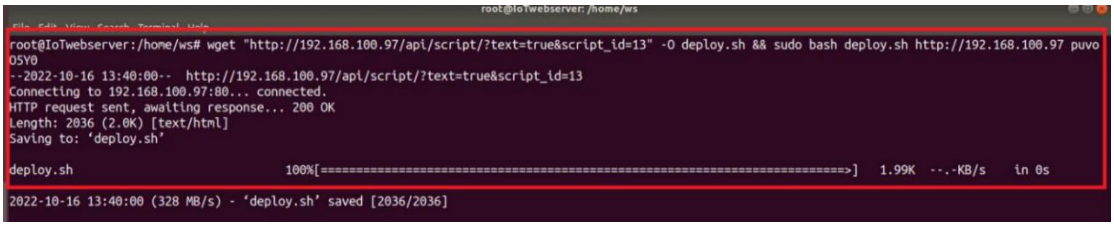
Script del honeypot Drupot



Se copia el comando de despliegue indicado. De regreso en el servidor que aloja el Honeypot Drupot se abre una terminal de usuario. A la misma se debe acceder con permisos de usuario root con el comando sudo su. Hay que pegar el comando de despliegue y comenzará con la ejecución del script.

Figura 41

Ejecución del script del honeypot Drupot



La configuración se realiza de manera automática y finaliza cuando ocurre el reinicio de todas las aplicaciones del servidor como se observa a continuación:

Figura 42

Inicialización del honeypot Drupot

En el servidor MHN se debe verificar que el honeypot instalado aparezca en la sección de sensores con la IP adecuada y sin ningún ataque registrado.

Figura 43

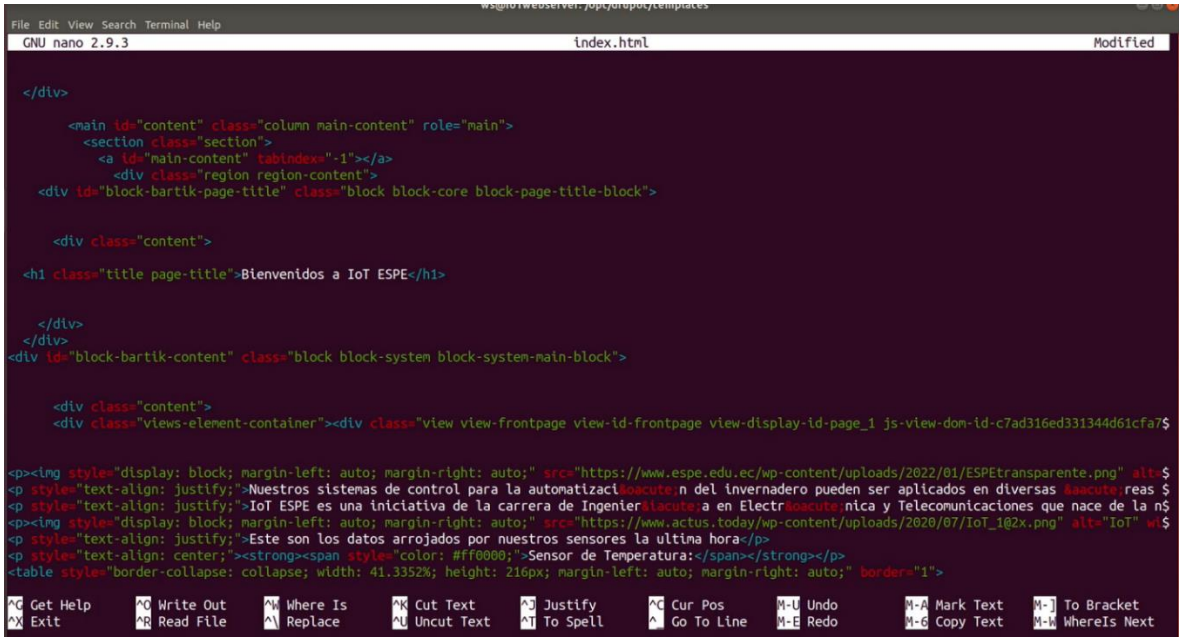
Vinculación del honeypot Drupot en el MHN

Nota. Se aprecia que el sensor Drupot se encuentra vinculado con el servidor de registro, adicionalmente se especifica parámetros como el nombre del servidor, la dirección IPv4, el nombre del honeypot y el número de ataques que registra hasta el momento.

Dado que se trata de un honeypot web se debe configurar el front de la página levantada. El fin es obtener una interfaz gráfica que emule un servicio web de producción en una red IoT, esto con el objetivo de ser atacado. Primeramente, se debe configurar el fichero index.html el cual contendrá la interfaz gráfica de la página y se encuentra en la siguiente ruta /opt/drupot/templates y el mismo está escrito en lenguaje html. Con la instrucción sudo nano index.html se puede modificar el código a conveniencia del administrador de seguridad.

Figura 44

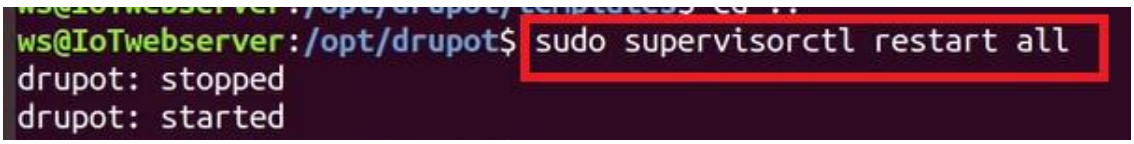
Modificación de la interfaz web de Drupot



Una vez realizada las configuraciones pertinentes se guarda el archivo modificado y se reinician las aplicaciones del servidor.

Figura 45

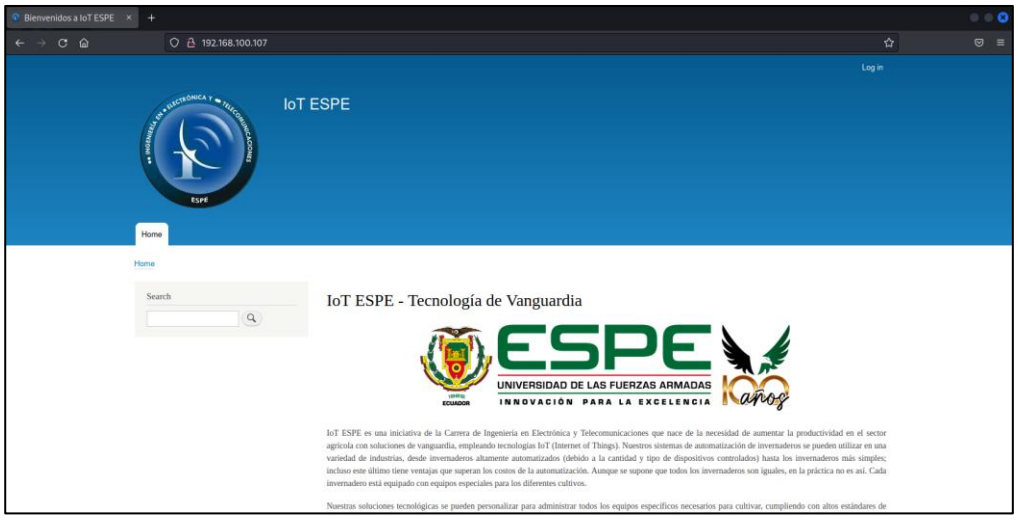
Reinicio de todos los procesos en Drupot



Se verifica que los cambios realizados sean correctos y la aplicación web se encuentre levantada.

Figura 46

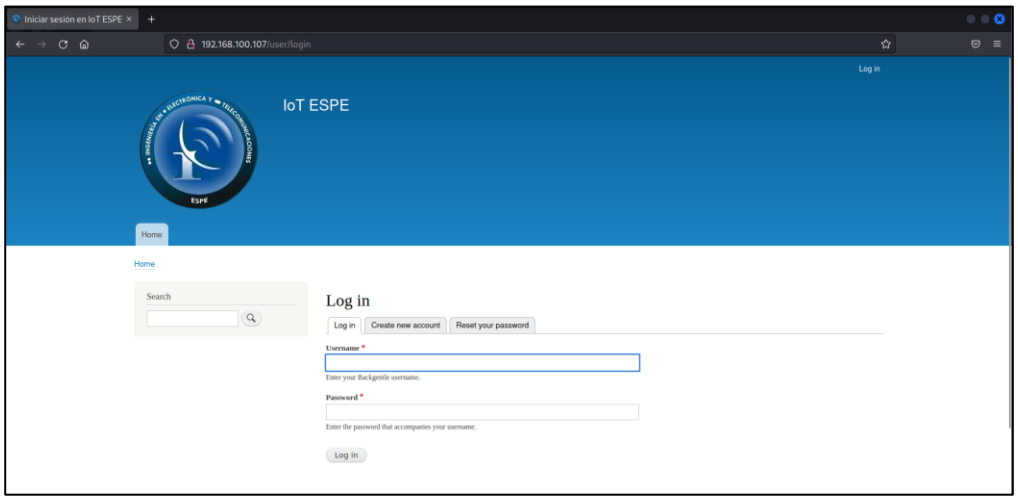
Interfaz web de inicio en Drupot



Nota. En la figura se aprecia la pantalla principal del honeypot Drupot

Figura 47

Interfaz web de sesión en Drupot



Nota. Se evidencia la pantalla de inicio de sesión dentro del servidor web Drupot.

Como se observa el servidor fue configurado de tal manera que aparenta ser una aplicación web de un sistema IoT, el mismo cuenta con una sección de ingreso de credenciales que generalmente se encuentran en este tipo de servicios y las mismas pueden llegar a sufrir diferentes tipos de ataques.

Honeypot Amun

Amun es un señuelo de baja interacción y de muy fácil implementación. Una de las principales cualidades de este honeypot es que posee atractivos módulos de vulnerabilidad. Estos forman servicios emulados que atraen al malware de propagación automática para iniciar exploits. Al ser un honeypot de baja interacción los servicios se emulan únicamente hasta el punto que permita activar un exploit determinado. Los servicios expuestos no pueden utilizarse ni interactuar de forma real ofreciendo una funcionalidad limitada. Este diseño es especialmente útil para detectar ataques automáticos y también debido a que los requerimientos de hardware para su implementación son mínimos.

Toda la información registrada por el sistema trampa se almacena en diferentes subdirectorios dentro de la carpeta de instalación de Amun.

Tabla 8

Registros de información de Amun

Archivo ".log"	**Descripción**
amun_server	Abarca información general, mensajes y errores del servidor
amun_request_handler	Comprende información acerca de exploits no reconocidos y etapas no coincidentes de exploits
analysis	Incluye información sobre el análisis del shellcode (análisis manual)

Archivo ".log"	**Descripción**
downloads	Información de los módulos de descarga como ftp, tftp entre otros.
exploits	Contiene la afirmación de exploits producidos.
shellcode_manager	Abarca información y errores del administrador de Shellcode
submissions	Información de descargas únicas.
successfull_downloads	Tiene información sobre los malware descargados.
unknown_downloads	Contiene información acerca de métodos de descarga no reconocidos
vulnerabilities	Información de algunos módulos de vulnerabilidad.

Las características de funcionalidad más relevantes de este sistema trampa se detallan a continuación:

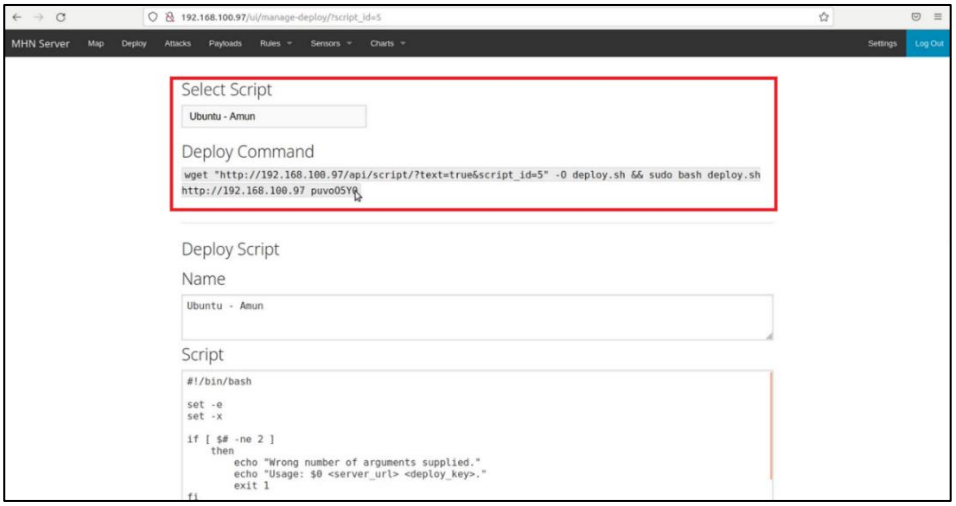
- Honeypot de interacción baja.
- Emula servicios atractivos como ftp, telnet, smtp, entre otros.
- Desarrollado en Python.
- Permite registrar malware de propagación automática.
- Fácil instalación y configuración.
- Fácil administración y mantenimiento.
- Cataloga toda la información registrada en diferentes módulos.
- Proporciona información detallada del ataque.

Para el servidor que contiene el Honeypot Amun se realiza los mismos pasos descritos para el Honeypot Drupot comprobando inicialmente si existe comunicación con el servidor MHN

a través de una simple petición ICMP. Mediante la venta de Deploy se selecciona el script Ubuntu – Amun y se copia el comando de despliegue indicado en la pantalla.

Figura 48

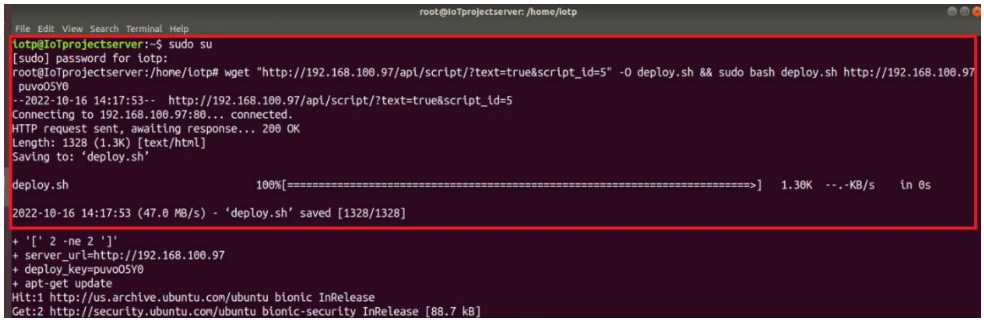
Script del honeypot Amun



En el servidor recién configurado con el sistema operativo Ubuntu 18.04 LTS y que aloja el Honeypot Amun se ejecuta el comando de despliegue copiado dentro de una terminal, se debe realizar esta ejecución con rol de administrador.

Figura 49

Ejecución del script del honeypot Amun

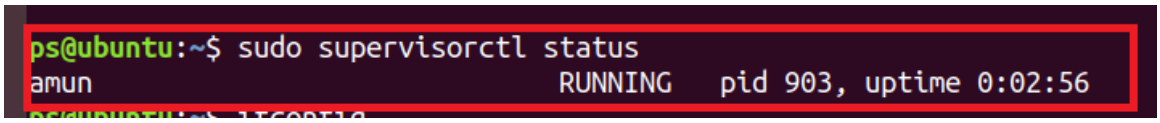


Nota. Ejecución del script para la instalación del honeypot Amun dentro de una terminal con permisos de super usuario.

Una vez completada la instalación, se debe verificar que el Honeypot se encuentre ejecutando correctamente con el comando sudo supervisorctl status, se aprecia que Amun está corriendo con el PID 903.

Figura 50

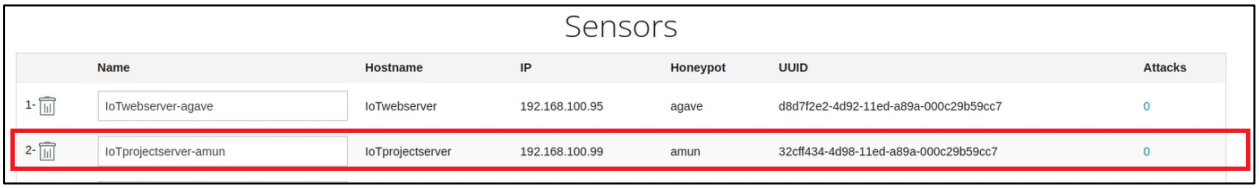
Estado del honeypot Amun



Por último, se verifica que se haya enlazado satisfactoriamente con el administrador de registros MHN.

Figura 51

Vinculación del honeypot Amun en el MHN



Nota. Se evidencia que el sensor Amun se encuentra vinculado con el MHN, adicionalmente se visualiza parámetros como el nombre del servidor, dirección IPv4, nombre y número de ataques que registra hasta el momento el honeypot.

Honeypot Dionaea

Este honeypot está diseñado para emular diferentes servicios y permite ejecutar instrucciones basadas en Intel x86. Este señuelo es de baja interacción y simula la existencia de hosts sobre una red, proporcionando al servidor el espectro completo de direcciones IPv4. Estas características lo hacen idóneo para instalarlo sobre la Raspberry Pi ya que los requerimientos de este hardware son suficientes para ejecutarlo sin problemas.

Se selecciona el honeypot Dionaea debido a que este sistema soporta rutinas no bloqueantes. Esta cualidad permite acrecentar de manera considerable el funcionamiento general del señuelo y admite efectuar varias operaciones de escritura y lectura sobre uno o diferentes sockets sin obligación de aguardar una confirmación por parte del receptor. Adicionalmente utiliza diferentes librerías para peticiones DNS no bloqueantes y receptar notificaciones acerca de varios tipos de eventos en el ecosistema de red respectivamente.

Este honeypot posee diferentes características y funcionalidades propicias para cumplir las necesidades de la solución, las mismas se detallan a continuación de manera general:

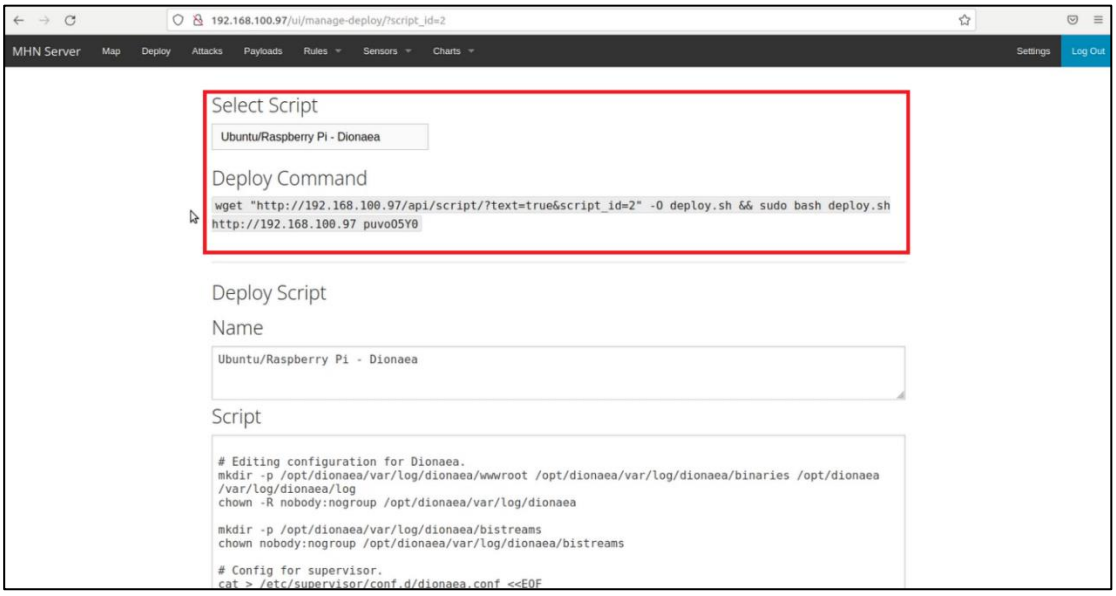
- Honeypot de interacción baja.
- Diseñado para atrapar malware dirigido a servicios de red.
- Publica servicios como FTP, SMB, Base de Datos, MQTT, etc.
- Soporta rutinas no bloqueantes.
- Fácil instalación y configuración.
- Fácil administración y mantenimiento.
- Permite levantar diferentes módulos y servicios vulnerables.
- Guarda una copia de los shellcodes y registra los métodos utilizados por el atacante durante la fase de explotación.

La instalación de este honeypot se realizará sobre un ordenador Raspberry Pi 4 el cual corre con un sistema operativo Raspberry Pi OS (Legacy). El objetivo es tener un señuelo de bajo costo y que se adecue a la necesidad de las redes del Internet de las Cosas siendo compacto y de fácil implementación sobre cualquier ecosistema.

Con el tercer servidor configurado se selecciona el comando de despliegue del Honeypot Dionaea indicado en el servidor MHN.

Figura 52

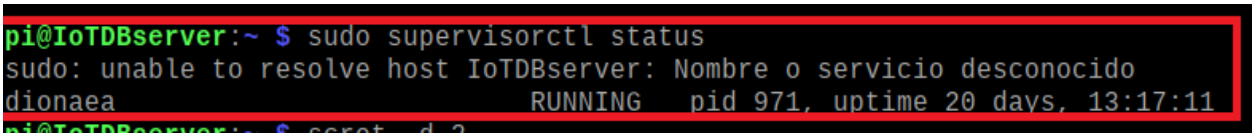
Script del honeypot Dionaea



Dado que toda la solución de seguridad IoT se configuró adecuadamente para que todos los elementos de la misma se encuentren dentro de un segmento de red específico debe existir comunicación entre la Raspberry Pi y el servidor MHN. Basta con transcribir el comando de despliegue y ejecutarlo en el ordenador mediante la terminal de usuario y con permisos root. Al momento de finalizar la instalación se debe corroborar que el proceso del Honeypot Dionaea esté corriendo.

Figura 53

Estado del honeypot Dionaea



Para finalizar, se verifica la integración con el servidor MHN al igual que los demás sensores desplegados.

Figura 54

Vinculación del honeypot Dionaea en el MHN

Sensors

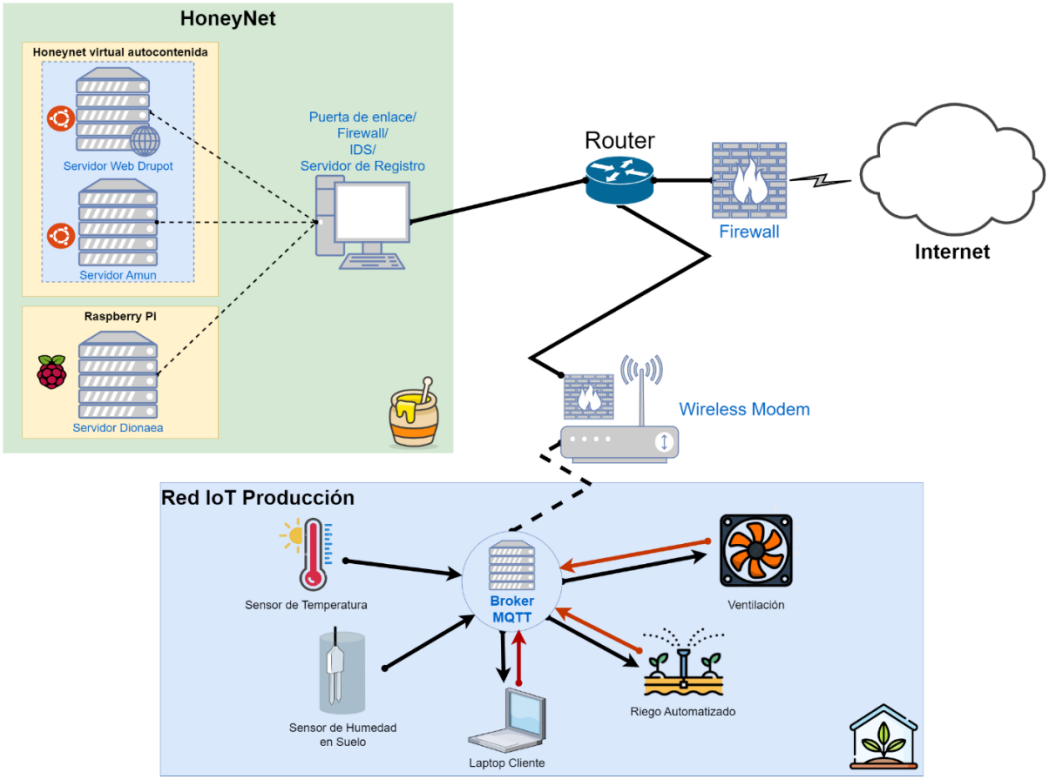
	Name	Hostname	IP	Honeypot	UUID	Attacks
1-	IoTwebserver-agave	IoTwebserver	192.168.100.95	agave	d8d7f2e2-4d92-11ed-a89a-000c29b59cc7	0
2-	IoTprojectserver-amun	IoTprojectserver	192.168.100.99	amun	32cff434-4d98-11ed-a89a-000c29b59cc7	0
3-	IoTdbserver-dionaea	IoTdbserver	192.168.100.79	dionaea	0cd1052e-4d99-11ed-a89a-000c29b59cc7	0

Topología de red implementada

En base a las especificaciones y criterios indicados en este capítulo se bosqueja la arquitectura de red basado en un ecosistema IoT de un invernadero inteligente y una Honeynet híbrida como herramienta trampa para monitoreo y detección de posibles amenazas en la red.

Figura 55

Arquitectura de la red implementada



Capítulo V: Pruebas de validación

Pruebas de auditoría

Como se ha visto en capítulos anteriores, la auditoría de seguridad informática es una metodología para verificar los mecanismos de seguridad y evaluar las medidas adoptadas por una entidad de cara a un ataque informático.

Al ser una metodología, esta se realiza siguiendo un orden lógico con el fin de aprovechar todo lo descubierto en fases anteriores. Como las pruebas de auditoría de seguridad se van a realizar a un escenario totalmente emulado y no supone un riesgo para una organización real, se seguirá una metodología de auditoría interna de caja negra. Se parte de que el atacante o el auditor informático en este caso se encuentra dentro de la red de la organización. A continuación, se detalla las fases del proceso de la auditoría de seguridad realizada.

Máquina atacante

Para atacar la red se utilizó una máquina virtual Kali Linux la cual se encuentra en el mismo segmento de red que la Honeynet Híbrida y del AP (Access Point) del ecosistema IoT.

Especificaciones técnicas

- **Software de virtualización:** Se utilizó VMware Workstation 16.2.4
- **Procesadores:** 4 núcleos
- **RAM:** 4 GB
- **ROM:** 80 GB
- **Adaptador de red:** Bridged

Sistema Operativo

Con el comando uname -a se descubre la versión del kernel, arquitectura, sistema operativo y hardware de la máquina.

Figura 56

Información del sistema operativo

```
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64 GNU/Linux
```

Datos de red

Con el comando ifconfig se identifica la información básica de las interfaces de red de la máquina, este comando es para sistemas operativos basados en Linux.

- **IPv4:** 192.168.100.100
- **Máscara:** 255.255.255.0
- **Broadcast:** 192.168.100.255
- Clase C

Figura 57

Información del dispositivo de red

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::abcb:1454:a51a:221f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:16:1d:65  txqueuelen 1000  (Ethernet)
        RX packets 821112  bytes 1193372037 (1.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 254575  bytes 18486870 (17.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1593  bytes 581997 (568.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1593  bytes 581997 (568.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Footprinting y Fingerprinting

En la fase de footprinting se recolecta toda la información posible del objetivo que va a ser atacado, se utilizan varias técnicas para recolectar información. Al tratarse de una auditoría

interna y la red implementada es emulada únicamente con el fin de ser perpetrada, no se utilizarán fuentes públicas para la recolección de datos. Teniendo en claro los puntos anteriores se comienza con la fase fingerprinting.

Escaneo de red

Se realiza un escaneo ARP para identificar los equipos dentro de la red con el comando arp-scan y parámetro -l. A partir de este punto se utilizará niveles de superusuario para tener acceso completo a las herramientas.

Figura 58

Escaneo de red por comando

El atacante identifica los equipos dentro de la red, con este comando se obtiene la dirección IPv4, la dirección MAC y el nombre del proveedor del Host identificado.

Con los datos obtenidos el atacante puede bosquejar una arquitectura de red y entender de mejor manera el entorno de ataque.

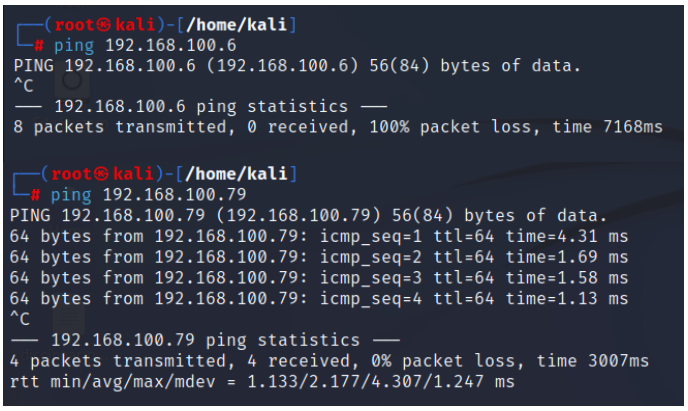
Verificación de conexión

Mediante el protocolo ICMP el auditor verifica si los hosts identificados anteriormente son accesibles desde la máquina atacante. Para corroborar esto se utilizará el comando ping seguido del elemento de red que se quiere comprobar.

De las peticiones ICMP realizadas a todos los elementos de red, los únicos objetivos que rechazaron la conexión fueron el 192.168.100.6 y el 192.168.100.88. Los demás elementos de red son accesibles desde la máquina atacante.

Figura 59

Verificación de conexión con elementos de la red auditada



A continuación, se presenta un resumen de los datos obtenidos hasta el momento.

Tabla 9

Parámetros de los elementos de la red implementada

Dirección IPv4	Dirección MAC	Fabricante	Descripción	Accesible desde la máquina atacante
192.168.100.1	---	HUAWEI TECHNOLOGIES CO.,LTD	Dirección reservada al router.	No se realizó la petición.
192.168.100.6	---	ASUSTek COMPUTER	Máquina Asus	NO

Dirección IPv4	Dirección MAC	Fabricante	Descripción	Accesible desde la máquina atacante
192.168.100.79	---	(Unknown)	No se ha identificado al elemento de red.	SI
192.168.100.88	---	(Unknown)	No se ha identificado al elemento de red.	NO
192.168.100.97	00:0c:29:b5:9c:c7	VMware, Inc.	Corresponde posiblemente a una máquina virtualizada.	SI
192.168.100.107	00:0c:29:3b:cb:b4	VMware, Inc.	Corresponde posiblemente a una máquina virtualizada.	SI
192.168.100.108	00:0c:29:b7:80:80	VMware, Inc.	Corresponde posiblemente a una máquina virtualizada.	SI

Nota. En la tabla se muestra todos los parámetros de relevancia dentro de la primera fase de la auditoría como direcciones IPv4, MAC, nombre de fabricante del dispositivo y una breve descripción.

Escaneo de puertos y sistemas operativos a elementos de red

Para este paso se procede a escanear únicamente los hosts accesibles desde la máquina atacante. El objetivo es descubrir los servicios, puertos abiertos y sistemas operativos de los elementos de red. Mediante la herramienta Nmap se logrará el objetivo, utilizando el comando:

nmap -O -Pn -p- dirección_IP_a_evaluar

Tabla 10

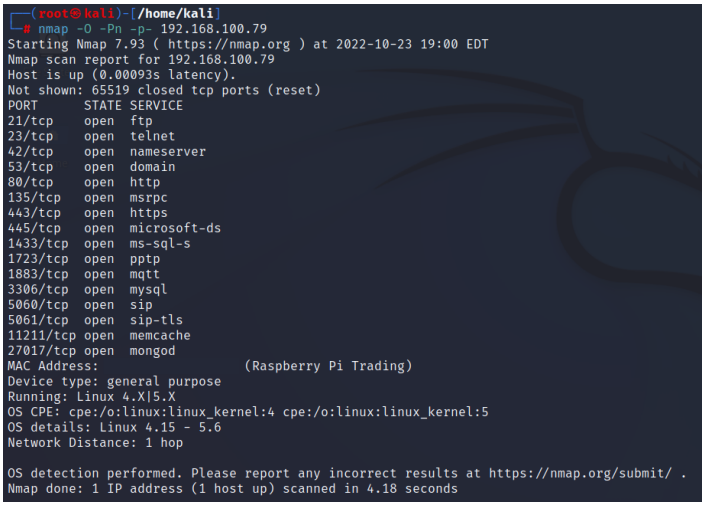
Parámetros para escanear puertos y sistemas operativos con Nmap

Parámetro	Descripción
-O	Activa la detección del sistema operativo
-Pn	No realiza peticiones ICMP. Analiza directamente los puertos
-p-	Analiza todos los puertos

- 192.168.100.79

Figura 60

Resultados del escaneo a la dirección 192.168.100.79



Este elemento de red corre sobre un sistema operativo Linux 4.X|5.X. De acuerdo a los resultados obtenidos se puede evidenciar que la máquina fue desarrollada por la compañía Raspberry Pi. A continuación, se presenta una descripción de los puertos detectados.

Tabla 11

Puertos abiertos detectados en la IP 192.168.100.79

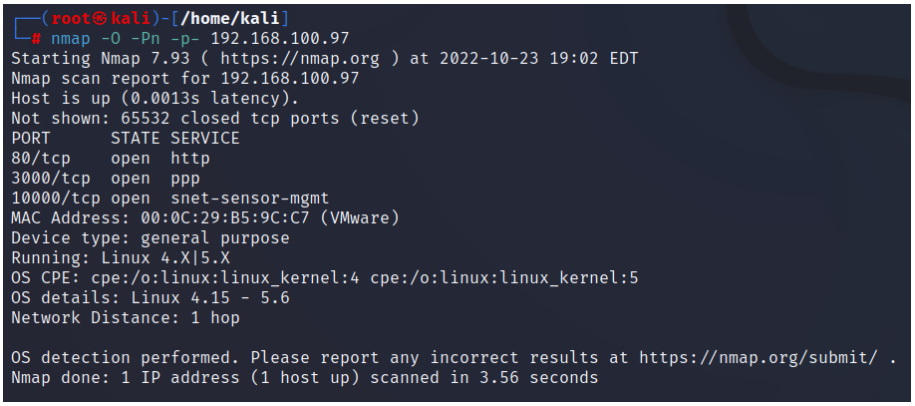
Puerto	Estado	Servicio	Descripción
21	Abierto	ftp	Protocolo que permite la transferencia de archivos a través de la red.
23	Abierto	telnet	Sirve para instaurar una conexión remotamente con otro equipo.
42	Abierto	nameserver	Puerto TCP, Host Name Server
53	Abierto	domain	Domain Name System
80	Abierto	http	Navegación web no segura
135	Abierto	msrpc	Puerto tcp, dirige el tráfico hasta el epmap (Endpoint Mapper) de la RPC
443	Abierto	https	Navegación web segura
445	Abierto	Microsoft-ds	Protocolo SMB
1433	Abierto	Ms-sql-s	Permite conexiones remotas a la base de datos SQL
1723	Abierto	pptp	Protocolo VPN
1883	Abierto	mqtt	Protocolo MQTT
3306	Abierto	mysql	Puerto por defecto de MySQL
5060	Abierto	sip	Permite conexión a servidores SIP
5061	Abierto	Sip-tls	Protocolo de inicio de sesión a través de TLS

Puerto	Estado	Servicio	Descripción
11211	Abierto	memcache	Servicio de memoria de cache
27017	Abierto	mongod	Puerto por defecto MongoDB

- 192.168.100.97

Figura 61

Resultados del escaneo a la dirección la IP 192.168.100.97



A continuación, se presenta una descripción de los puertos detectados en este elemento de red que corre sobre un sistema operativo Linux.

Tabla 12

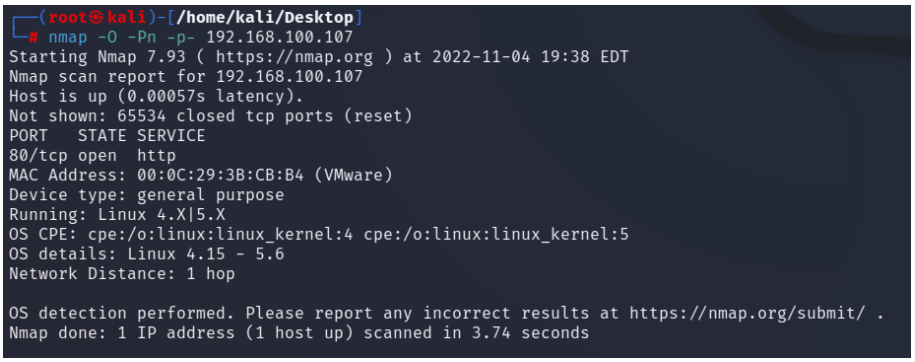
Puertos abiertos detectados en la IP 192.168.100.97

Puerto	Estado	Servicio	Descripción
80	Abierto	http	Navegación web no segura
3000	Abierto	ppp	Protocolo punto a punto
10000	Abierto	Snet-sensor-mgmt	Protocolo TCP

- 192.168.100.107

Figura 62

Resultados del escaneo a la dirección 192.168.100.107



El servidor auditado corre sobre un sistema operativo Linux. A continuación, se presenta una descripción del puerto detectado:

Tabla 13

Puertos abiertos detectados en la IP 192.168.100.107

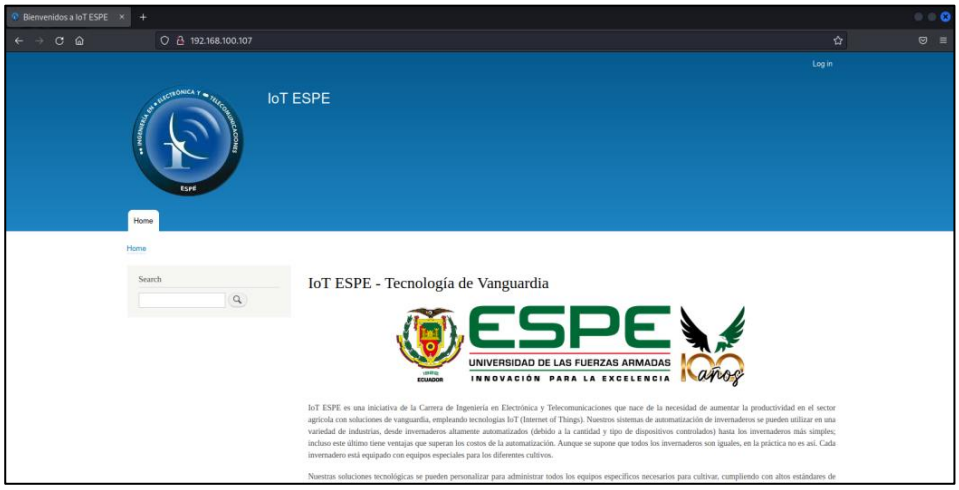
Puerto	Estado	Servicio	Descripción
80	Abierto	http	Navegación web no segura

Al tener únicamente abierto este puerto se realiza una conexión a esta IP a través de un navegador para comprobar si tiene un servicio web levantado o se procede a descartar este objetivo para una posible intrusión.

Como se aprecia existe un servicio web levantado, por lo que para este objetivo se realizará una auditoría de seguridad web y así poder obtener las vulnerabilidades de este servidor.

Figura 63

Interfaz web de la IP 192.168.100.107



- 192.168.100.108

Figura 64

Resultados del escaneo a la dirección 192.168.100.108

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O -Pn -p- 192.168.100.108
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-04 19:44 EDT
Nmap scan report for 192.168.100.108
Host is up (0.00071s latency).
Not shown: 65484 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
80/tcp    open  http
105/tcp   open  csnet-ns
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
587/tcp   open  submission
617/tcp   open  sco-dtmgr
1023/tcp  open  netvenuechat
1025/tcp  open  NFS-or-IIS
1080/tcp  open  socks
1111/tcp  open  lmsocialserver
1581/tcp  open  mil-2045-47001
1900/tcp  open  upnp
2101/tcp  open  rtcm-sc104
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2380/tcp  open  etcd-server
2555/tcp  open  compaq-wcp
2745/tcp  open  urbisnet
2954/tcp  open  ovalarmsrv-cmd
2967/tcp  open  symantec-av
2968/tcp  open  enpp
3127/tcp  open  ctx-bridge
3128/tcp  open  squid-http
3268/tcp  open  globalcatLDAP
3372/tcp  open  msdtc
3389/tcp  open  ms-wbt-server
3628/tcp  open  ept-machine
5000/tcp  open  upnp
5168/tcp  open  scte30
5554/tcp  open  sgi-esphttp
6070/tcp  open  messageasap
6101/tcp  open  backupexec
6129/tcp  open  unknown
7144/tcp  open  unknown
7547/tcp  open  cwmp
8080/tcp  open  http-proxy
9999/tcp  open  abyss
10203/tcp open  unknown
27347/tcp open  unknown
38292/tcp open  landesk-cba
41523/tcp open  unknown
MAC Address: 00:0C:29:B7:80:80 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:lin
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect
Nmap done: 1 IP address (1 host up) scanned in 3.87
```

El servidor tiene un sistema operativo Linux. A continuación, se presenta una descripción de los puertos detectados en este elemento de red, para las siguientes fases se debe analizar y escoger los puertos más relevantes para la vulneración de los mismos.

Tabla 14

Puertos abiertos detectados en la IP 192.168.100.108

Puerto	Estado	Servicio	Descripción
21	Abierto	ftp	Protocolo que permite la transferencia de archivos a través de la red.
23	Abierto	telnet	Sirve para instaurar una conexión remotamente con otro equipo.
25	Abierto	smtp	Usado para servicio de correo electrónico
42	Abierto	nameserver	Puerto TCP, Host Name Server
80	Abierto	http	Navegación web no segura
105	Abierto	csnet-ns	Protocolo de nombre del servidor CCSO
110	Abierto	pop3	Usan gestores de correo electrónico para hacer conexiones con el protocolo POP3
135	Abierto	msrpc	Puerto tcp, dirige el tráfico hasta el epmap (Endpoint Mapper) de la RPC
139	Abierto	netbios-ssn	Utilizado por servicios de archivo de Microsoft Windows.
143	Abierto	imap	Protocolo utilizado por IMAP
443	Abierto	https	Navegación web segura
445	Abierto	Microsoft-ds	Protocolo SMB
554	Abierto	rtsp	Real Time Streaming Protocol
587	Abierto	submission	Utilizado por SMTP

Puerto	Estado	Servicio	Descripción
617	Abierto	sco-dtmgr	Servidor de administración de escritorio SCO
1023	Abierto	netvenuechat	Puerto TCP reservado
1025	Abierto	NFS-or-IIS	Puerto TCP reservado
1080	Abierto	socks	Servidor Proxy
1111	Abierto	lmsocialserver	Puerto TCP, Servidor LM Social
1581	Abierto	mi-2045-47001	Puerto TCP
1900	Abierto	upnp	Protocolo SSDP
2101	Abierto	rtcm-sc104	Puerto TCP, protocolo de aplicación MSMQ-DC
2103	Abierto	zephyr-clt	Puerto TCP, protocolo de aplicación MSMQ-RPC
2105	Abierto	eklogin	Puerto TCP, protocolo de aplicación MSMQ-RPC
2107	Abierto	msmq-mgmt	Puerto TCP, protocolo de aplicación MSMQ-Mgmt
2380	Abierto	etcd-server	Puerto TCP, sin asignación
2555	Abierto	compaq-wcp	Compaq WCP
2745	Abierto	urbisnet	Puerto TCP, URBISNET
2954	Abierto	ovalarmsrv-cmd	Puerto TCP, OVALARMSRV-CMD
2967	Abierto	symantec-av	Administración remota entre el servidor y el cliente para Symantec
2968	Abierto	enpp	ENPP
3127	Abierto	ctx-bridge	Puerto CTX Bridge
3128	Abierto	squid-http	Cachés web para Squid
3268	Abierto	globalcatLDAP	Puerto usado por protocolos de AD y comunicaciones de ID
3372	Abierto	msdtc	Puerto TCP

Puerto	Estado	Servicio	Descripción
3389	Abierto	ms-wbt-server	Microsoft Terminal Server
3628	Abierto	ept-machine	Interfaz EPT Machine
5000	Abierto	upnp	Interoperabilidad de dispositivos de red de Windows
5168	Abierto	scte30	Conexión SCTE30
5554	Abierto	sgi-esphttp	SGI ESP HTTP
6070	Abierto	messageasap	Puerto TCP, Messageasap
6101	Abierto	backupexec	Puerto TCP
6129	Abierto	Desconocido	Desconocido
7144	Abierto	Desconocido	Desconocido
7547	Abierto	cwmp	Puerto utilizado para escucha de paquetes MC (Misfortune Cookie)
8080	Abierto	http-proxy	Puerto de prueba para servidores web
9999	Abierto	abyss	Puerto TCP
10203	Abierto	Desconocido	Desconocido
27347	Abierto	Desconocido	Desconocido
38292	Abierto	landesk-cba	Puerto TCP
41523	Abierto	Desconocido	Desconocido

Enumeración de servicios y versión

Empleando la herramienta Nmap y modificando los argumentos de la petición, se procede a enumerar los servicios con su respectiva versión. Con esto se obtiene una visión más profunda de los puertos detectados en el paso anterior. Se utilizará el siguiente comando:

nmap -Pn -sV dirección_IP_a_evaluar

Tabla 15

Parámetros para enumerar servicios con Nmap

Parámetro	Descripción
-Pn	No realiza peticiones ICMP. Analiza directamente los puertos
-sV	Identifica la versión de los servicios

Figura 65

Enumeración de servicios a la dirección 192.168.100.79

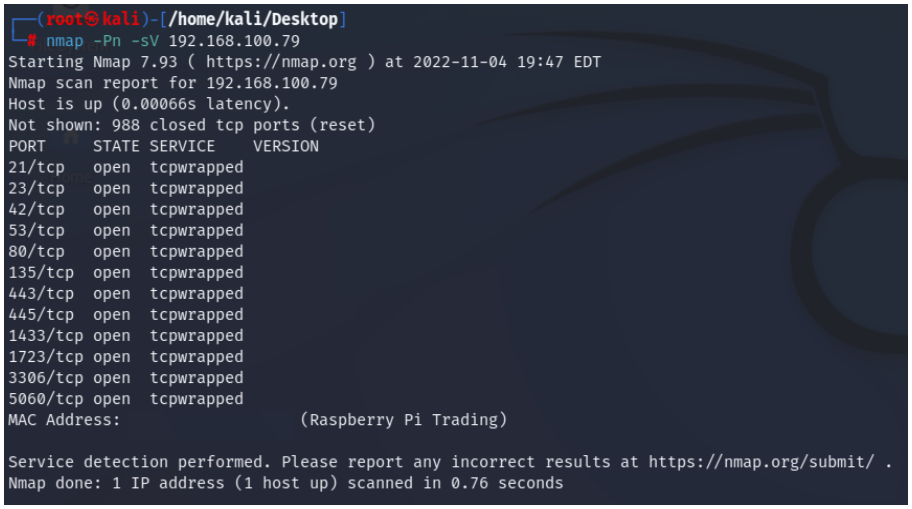


Figura 66

Enumeración de servicios a la dirección 192.168.100.97

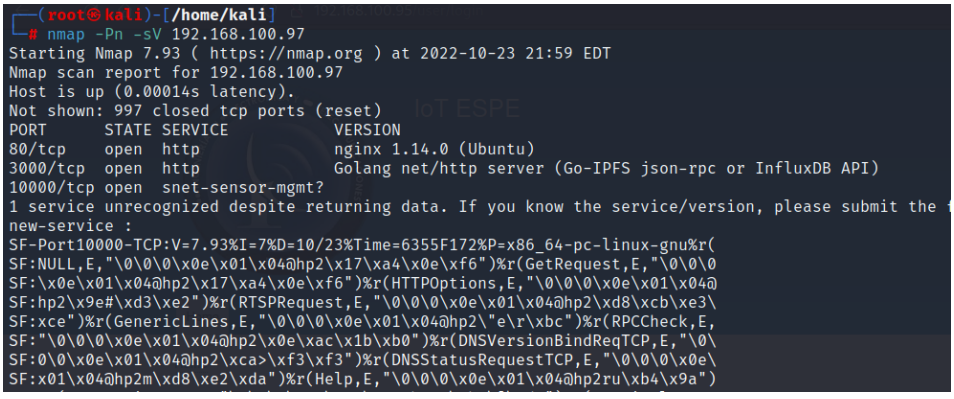


Figura 67

Enumeración de servicios a la dirección 192.168.100.107

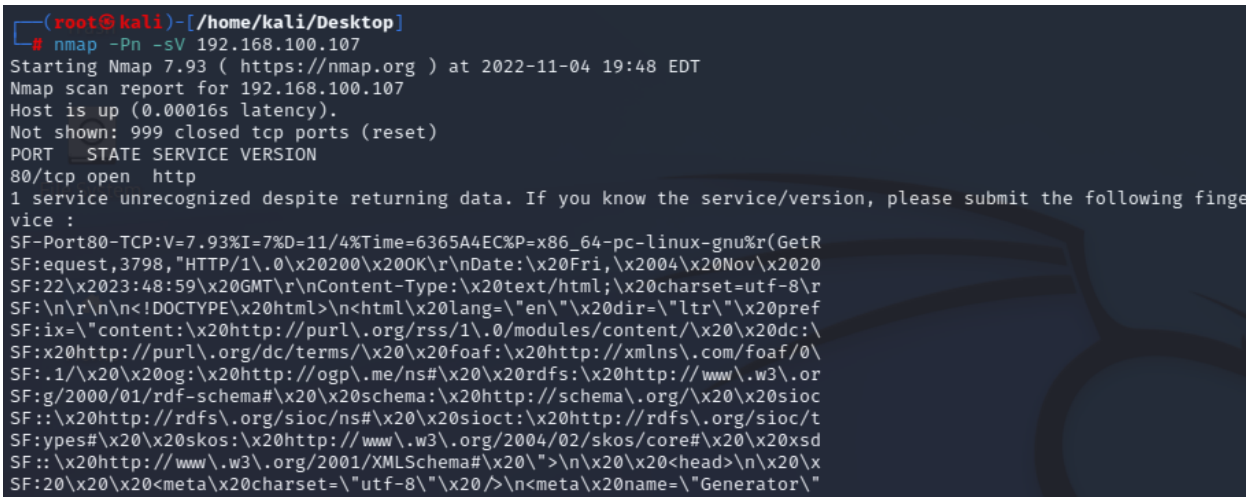
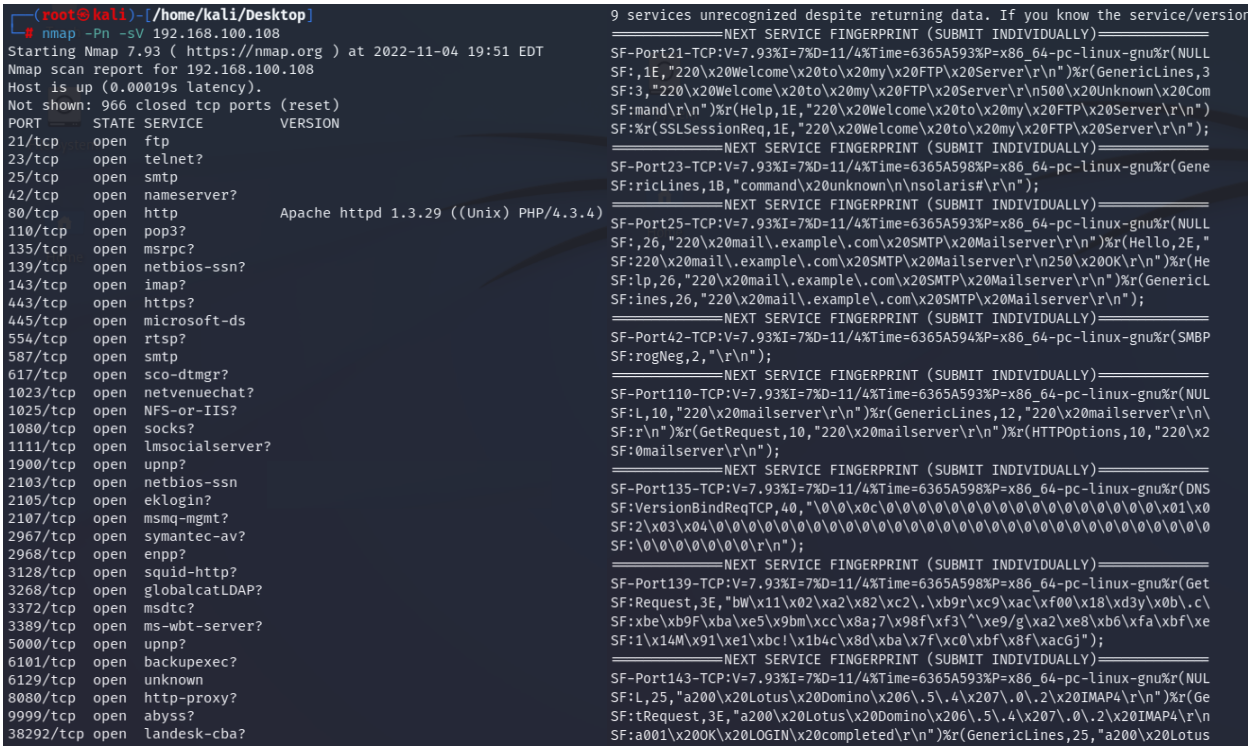


Figura 68

Enumeración de servicios a la dirección 192.168.100.108



Análisis y explotación de vulnerabilidades

Los datos recogidos en los pasos anteriores permitirán tener un mejor entendimiento de los servicios que se requieren explotar. Para esta sección se seleccionará los hosts que presentan mayor riesgo sobre la red auditada.

Elección de objetivos de ataque

En base a los problemas de seguridad hallados en la fase de fingerprinting, se seleccionó los servidores que puedan suministrar una mayor tasa de éxito en la fase de intrusión.

Tabla 16

Servidores a ser evaluados

Nombre	IP	Número de puertos detectados
Servidor A	192.168.100.79	16
Servidor B	192.168.100.107	1
Servidor C	192.168.100.108	51

Como se observa los servidores seleccionados tienen una gran cantidad de puertos expuestos por lo que se elegirán los puertos más sensibles y que permitan alcanzar las metas establecidas anteriormente. De lo indicando, el servidor B si bien tiene un único puerto abierto, a diferencia de los otros elementos de red, este levanta una página web por ello la elección del mismo.

Puerto 21

Como se había indicado el puerto 21 corresponde al protocolo FTP el cual permite intercambiar archivos entre computadoras dentro de la red. Con estos antecedentes se tratará

de establecer comunicación a través de este protocolo, si el puerto no tiene un usuario configurado el servicio FTP sería de acceso público.

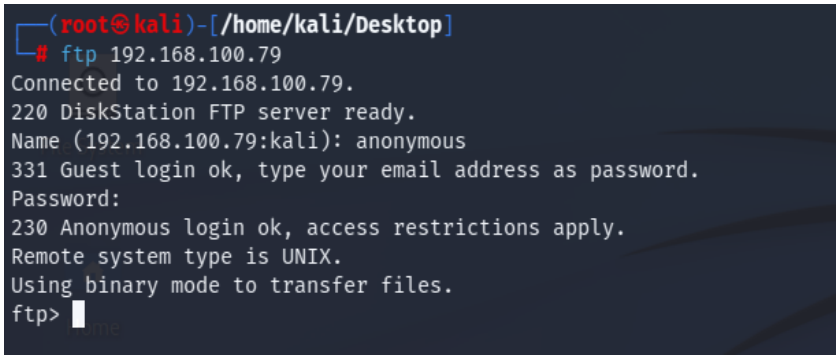
Mediante el comando ftp seguido de la dirección a evaluar se intentará establecer la conexión.

- 192.168.100.79

Al momento de ingresar el comando se solicitará autenticación por parte del usuario, se ingresará las credenciales por defecto del servicio FTP para usuario y contraseña las cuales son “anonymous”. Se logra acceder al directorio FTP del Servidor A, se lista los archivos dentro de este directorio sin resultados. En caso de que el acceso fuese incorrecto se debería hacer un ataque de fuerza bruta para probar las claves por defecto más comunes y así lograr una autenticación exitosa.

Figura 69

Conexión mediante ftp a la IP 192.168.100.79

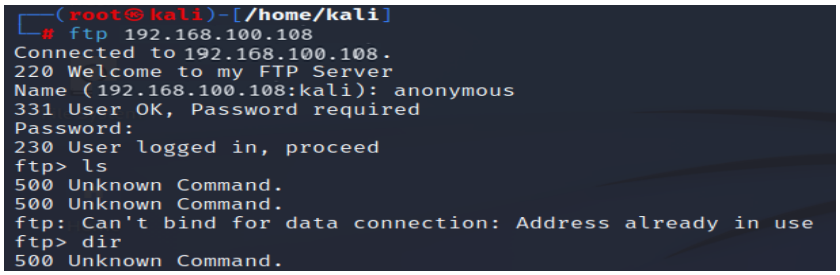


- 192.168.100.108

  Se repite el procedimiento para el Servidor C, se logra el mismo nivel de acceso. Sin embargo, no reconoce los comandos utilizados para listar archivos tanto para Linux como para sistemas basados en Linux.

Figura 70

Conexión mediante ftp a la IP 192.168.100.108



Puerto 23

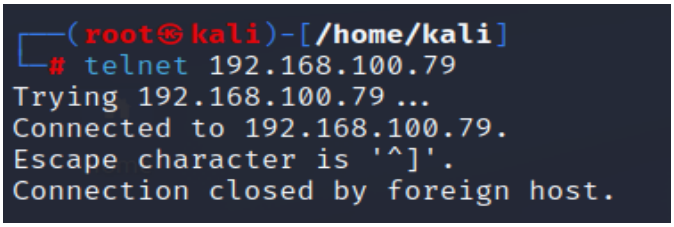
Este puerto permite acceder remotamente a una máquina a través de la red, permitiendo al usuario remoto controlar completamente el sistema a través de líneas de comando. Al identificar que el Servidor A y C tiene este puerto abierto, se procederá a la explotación del servicio. Con el comando telnet seguido de la dirección IP se probará establecer la conexión.

- 192.168.100.79

  El servidor A rechazo la conexión.

Figura 71

Conexión mediante telnet a la IP 192.168.100.79



- 192.168.100.108

EL servidor C si acepto la conexión. Se puede visualizar que la máquina remota trabaja sobre Solaris, al tratar de verificar la versión de Solaris instalada no reconoce el comando.

Figura 72

Conexión mediante telnet a la IP 192.168.100.108

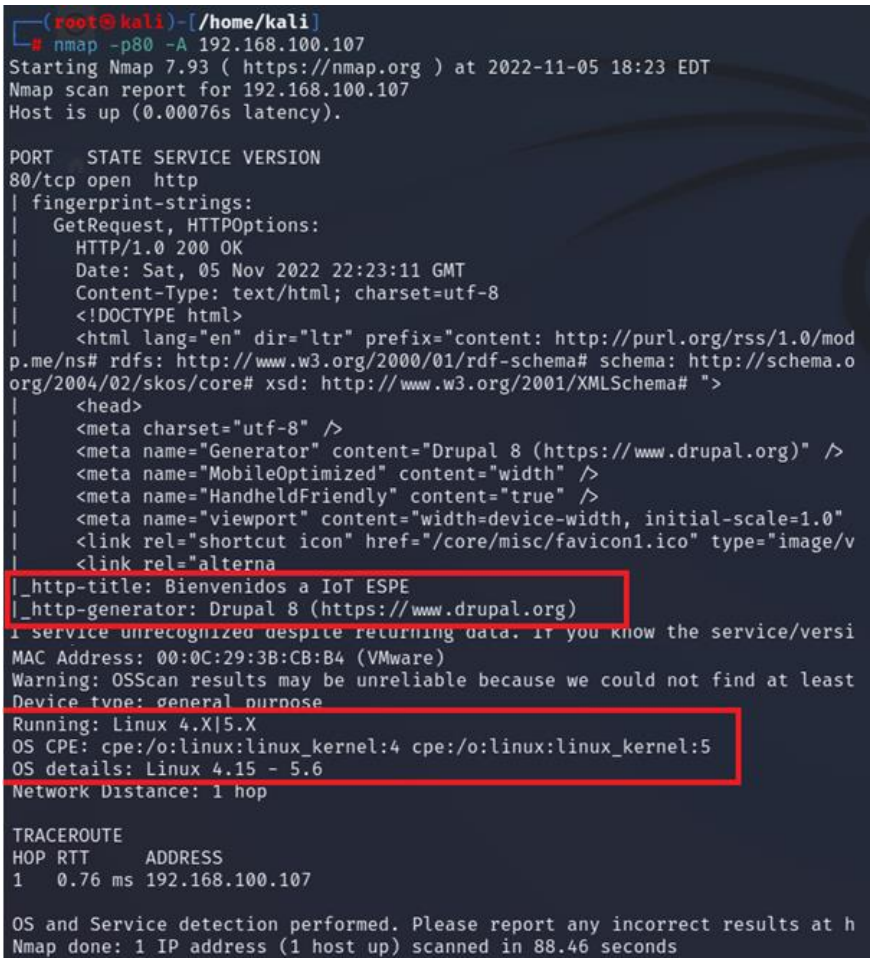
Puerto 80

Este es el puerto asignado al protocolo de transferencia de hipertexto HTTP, si bien los tres servidores tienen este puerto expuesto, el análisis se volcará sobre el servidor B. En la fase de recolección de información se constató que el servidor B tiene una página web levantada, con información relevante sobre el giro de negocio de la red que se está evaluando. Por tal motivo, se hace necesario verificar la parte de seguridad web sobre esta página. Al trabajar la página sobre el protocolo HTTP se sabe de primera instancia que la comunicación entre el cliente y el servidor web no está cifrada, lo que es un problema de seguridad en caso que se maneje información sensible o se requiera un inicio de sesión como en este el caso.

Como se había mencionado con anterioridad para obtener un ataque más efectivo se necesita recabar toda la información posible del sistema. Con Nmap se recolectará mayor información del servicio web.

Figura 73

Resultados de escaneo del puerto 80 en la IP 192.168.100.107

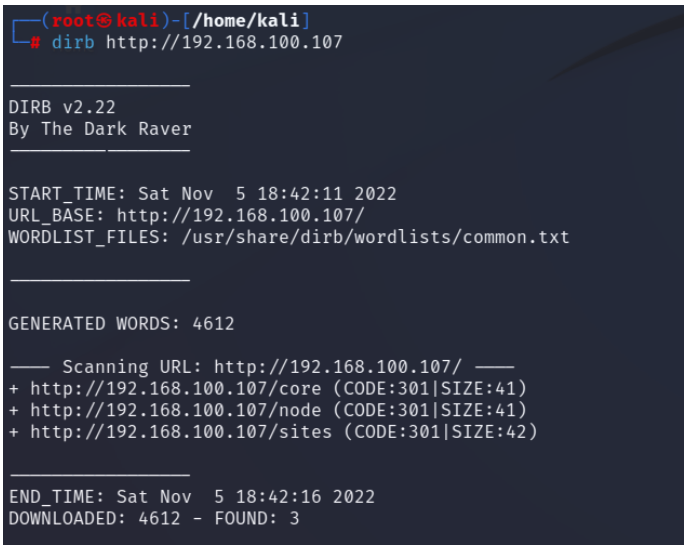


Se puede evidenciar que el servidor corre sobre sistema operativo Linux y utiliza un sistema de gestión de contenidos multipropósito como Drupal, la versión de este CMS es la número 8.

Descubrimiento de archivos en el servidor web. La herramienta dirb es un web fuzzer que básicamente permite verificar las rutas activas de un sitio web, esto con el objetivo de encontrar posibles vulnerabilidades de seguridad. Se emplea esta herramienta para encontrar todos los archivos web ocultos de esta página, para ejecutar el web fuzzer en la máquina atacante se ingresa el comando dirb seguido de la dirección de la página web.

Figura 74

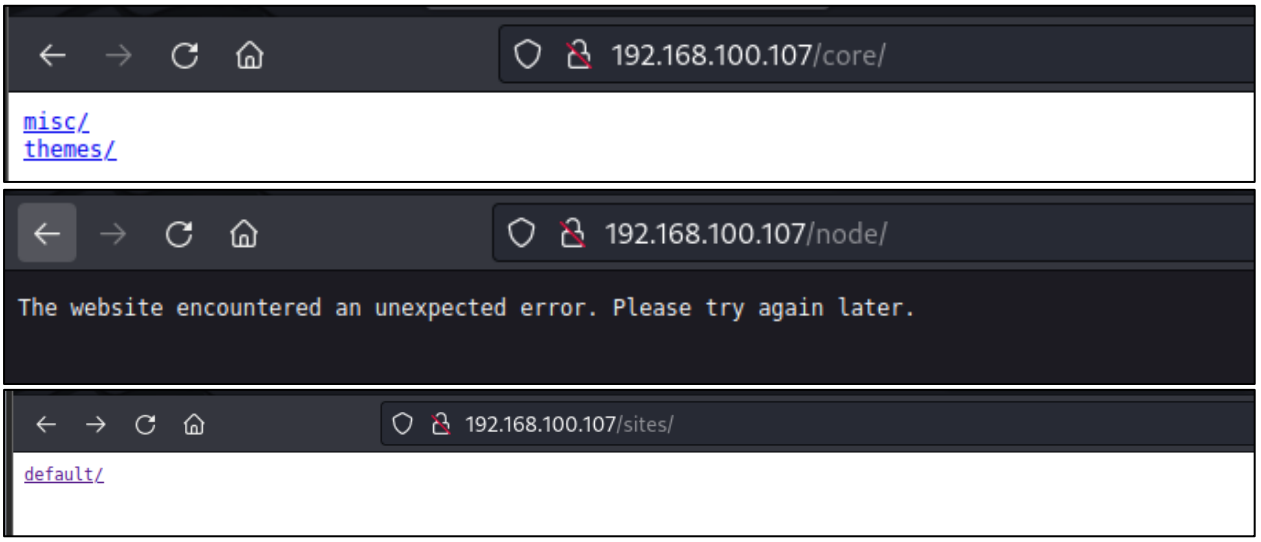
Escaneo de contenido web con dirb



Se tiene 3 objetos encontrados dentro de esta página web, se procede a acceder a cada uno de ellos para verificar si la información es relevante para la auditoría web.

Figura 75

Ficheros de la página web de la IP 192.168.100.107



Como resultados en el sitio http://192.168.100.107/core se obtiene los recursos que la página web utiliza como images, codígos .css, iconos, etc. El sitio http://192.168.100.107/sites tiene los archivos de programción .js y .css de la página web.

Ataque de Denegación de Servicios. Como se estudió anteriormente un ataque de denegación de servicio consiste en la inundación de peticiones a servidores objetivos con el fin de provoccar una sobrecarga en el sistema y que este deje de funcionar de manera normal o correcta. Para realizar este ataque se utiliza la herramienta hping3, configurando correctamente la instrucción se puede enviar paquetes personalizados y mostrar respuestas en el host destino. El objetivo es enviar la mayor cantidad de paquetes al servidor B con el fin de empeorar su servicio, para lo cual se envía la siguiente instrucción:

```
hping3 --rand-source -d 1000 -p 80 --flood 192.168.100.107
```

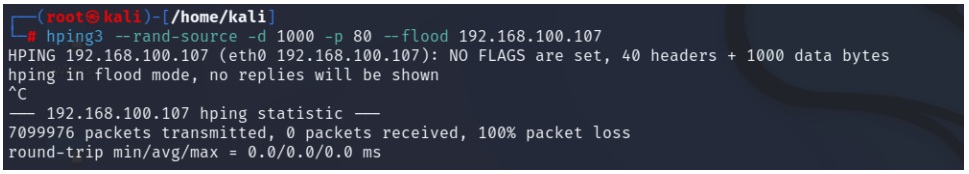
Tabla 17

Parámetros de la herramienta hping3

Parámetro	Descripción
--rand-source	Modo de dirección de fuente aleatorio
-d	Especifica el tamaño del dato
-p	Puerto de destino
--flood	Se encarga de enviar la mayor cantidad de paquetes como sea posible.

Figura 76

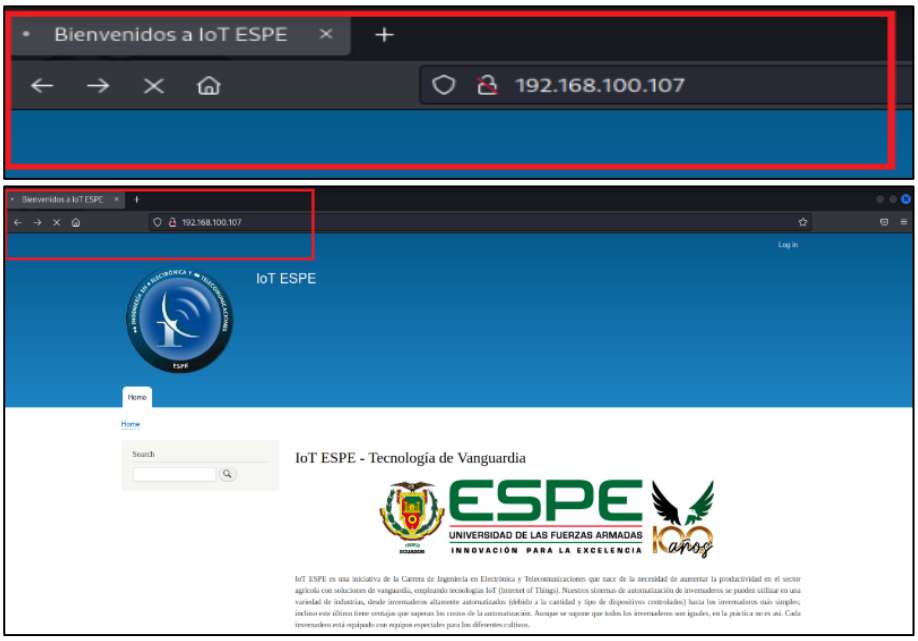
Ejecución de un ataque de denegación de servicio



Con la ejecución de esta instrucción se enviaron más de 7 millones de paquetes al servidor B, al comprobar la funcionalidad de la página la misma disminuyó en los tiempo de carga, por lo que se observa que el objetivo se cumple.

Figura 77

Afectación en la página web atacada



Puerto 135

Cuando se hacen conexiones al puerto 135, el tráfico se envía al Endopoint Mapper (Asignador de puntos finales) de la RPC. Se sabe que el Endopoint Mapper es explotado por virus, las constantes conexiones hacia este puerto provocan que el host se recargue. El ataque más empleado a este puerto es la DoS o ataque de Denegación de Servicio.

- 192.168.100.79

Para la explotación de esta vulnerabilidad se utilizará la herramienta Metasploit la cual contiene el exploit específico para el puerto 135. El exploit es el MS03_026_DCOM el cual hace un desbordamiento de pila sobre el servicio RPCSS y afecta sistemas operativos Windows 2000, XP y 2003.

Para iniciar la herramienta Metasploit se ejecuta el comando msfconsole, una vez se haya cargado la herramienta se ingresará el siguiente comando:

use exploit/windows/dcerpc/ms03_026_dcom

Se configura un shell inverso mediante la siguiente instrucción para tener acceso remoto a la máquina vulnerable.

set payload windows/meterpreter/reverse_tcp

Se establece el Listener Host que es la máquina atacante, en este caso la 192.168.100.100 con el siguiente comando

set LHOST 192.168.100.100

Y la máquina objetivo (servidor A) con la siguiente instrucción

set RHOST 192.168.100.79

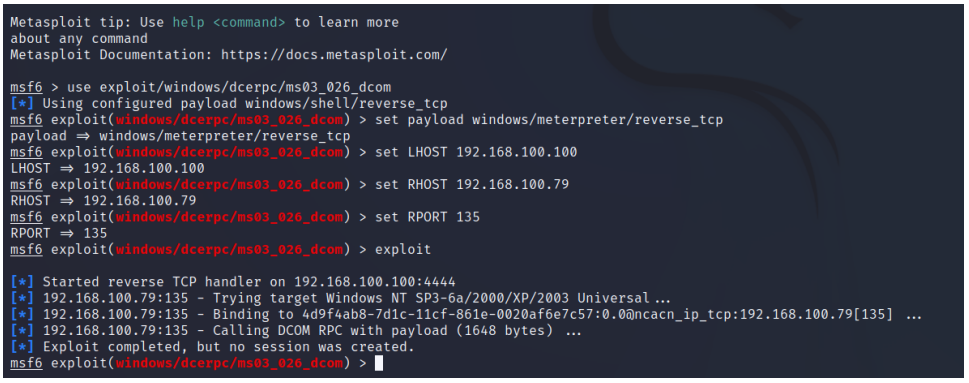
Se establece el puerto donde se realizará la carga

set RPORT 135

Con el comando exploit se inicia el proceso de vulneración.

Figura 78

Ataque al puerto135 de la IP 192.168.100.79



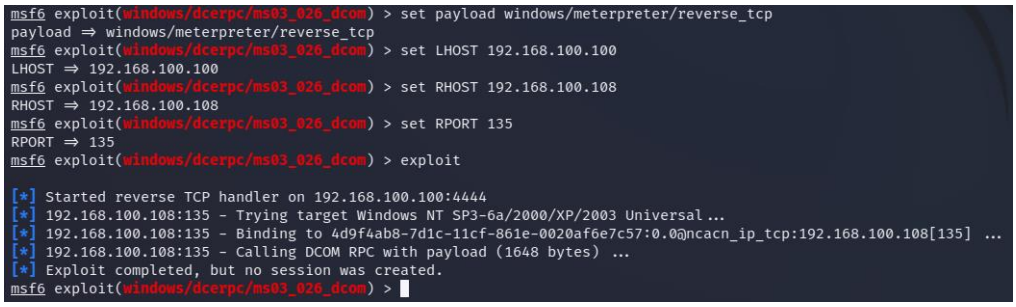
El resultado indica que el exploit se completó, pero como se observa la sesión no fue creada.

- 192.168.100.108

Se repite el proceso anterior, únicamente cambiando el RHOST en este caso la IP es la 192.168.100.108 que corresponde al servidor C.

Figura 79

Ataque al puerto135 de la IP 192.168.100.108



Nuevamente el exploit se completa, pero sin establecer una sesión entre la máquina atacada y el atacante.

Puerto 445

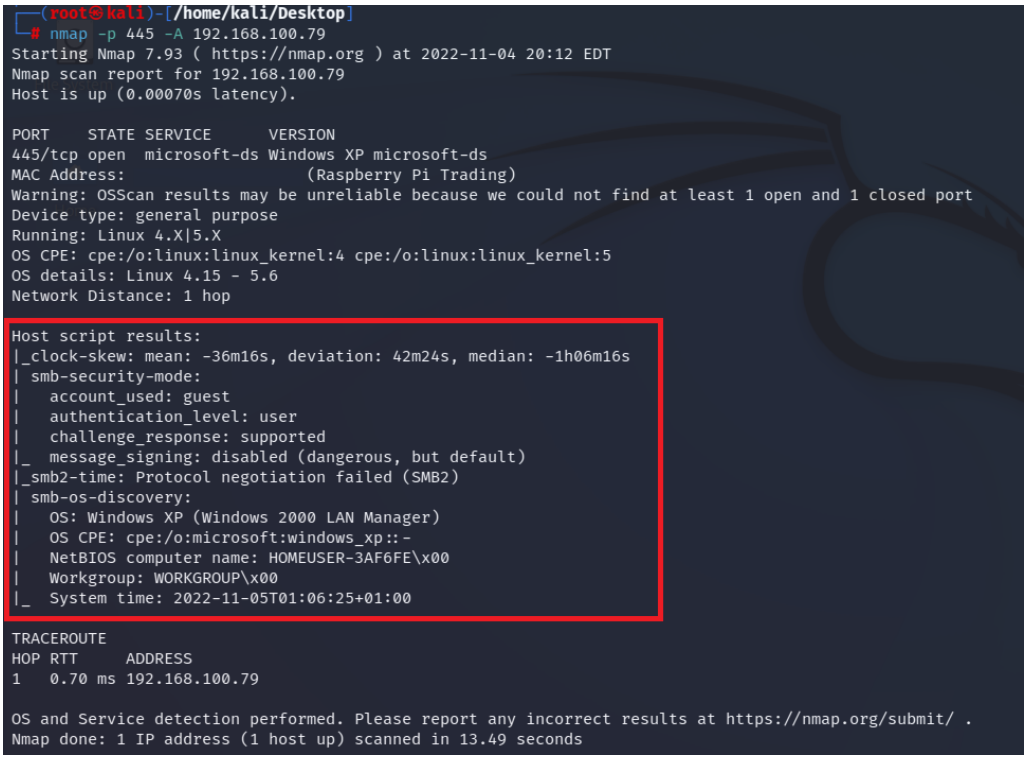
Este puerto es uno de los más usuales y fácilmente propensos para ataques informáticos. El mismo al ser un puerto TCP permite compartir archivos SMB de Microsoft-DS.

- 192.168.100.79

Para identificar apropiadamente el puerto a vulnerar, se realiza la enumeración SMB, para lo cual se utiliza la herramienta Nmap, con el comando nmap -p 445 -A ip_servidorA se obtienen la información del sistema operativo, nombre de la computadora y de la NetBIOS y el modo de seguridad SMB.

Figura 80

Resultados de escaneo del puerto 445 en la IP 192.168.100.79



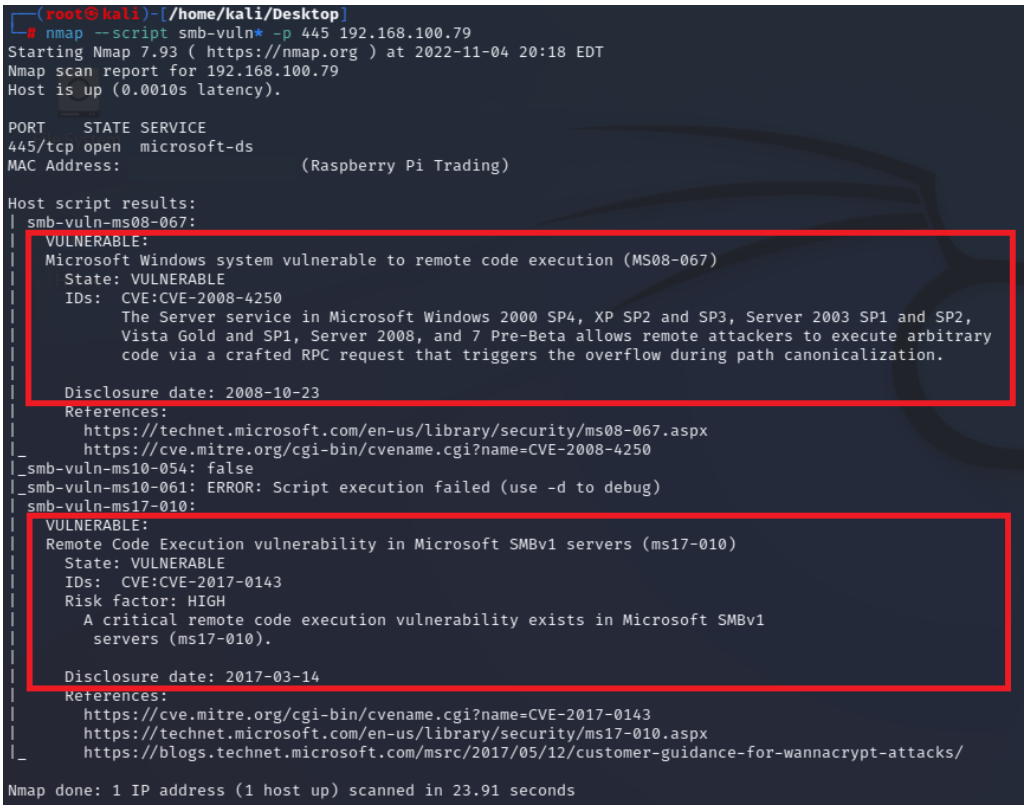
Una vez realizada la enumeración, se procederá a verificar si el servicio detectado es vulnerable o el mismo ya se encuentra parchado. Nuevamente utilizando Nmap se puede descubrir el estado vulnerable de un servicio SMB que tiene una máquina destino.

nmap --script smb-vuln* -p 445 192.168.100.79

En la Figura 81 se identifica que la máquina atacada es vulnerable a MS17-010 para servidores Microsoft SMBv1 y también es vulnerable a ejecución de código remoto MS08-067. De acuerdo a la notación de vulnerabilidades comunes y explotaciones, el Servidor A es vulnerable al CVE-2017-0143 y al CVE-2008-4250.

Figura 81

Vulnerabilidades detectadas en el puerto 445 en la IP 192.168.100.79



Nota. En la imagen se enmarcan las vulnerabilidades encontradas sobre el puerto 445 del servidor con la IP 192.168.100.79, también se indica el nivel de riesgo y la fecha en que la vulnerabilidad fue descubierta.

Sabiendo que la máquina es vulnerable a MS17-010 se utilizara Metasploit para atacar el servidor A. Se inicia la herramienta con msfconsole. Se establece la IP del servidor A y se ejecuta la explotación

Como se observa en la Figura 82 a pesar de que en la fase de análisis de vulnerabilidades sobre el puerto 445 se indica que el servicio es vulnerable a MS17_010, el exploit no llego a establecer la conexión remota con la máquina atacante.

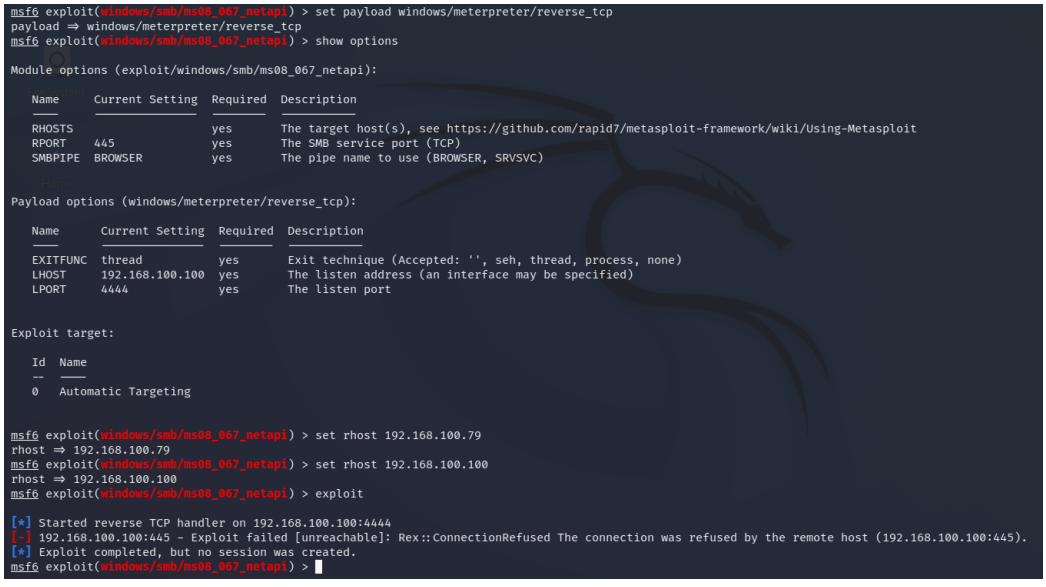
Figura 82

Ataque utilizando el payload ms17_010_eternalblue

También se conoce que la máquina es vulnerable a MS08_067 se utilizara Metasploit nuevamente para atacar el servidor A. Se inicia la herramienta con msfconsole, se configura el payload ms08_067_netapi y se indica la IP del servidor A.

Figura 83

Ataque utilizando el payload ms08_067_netapi



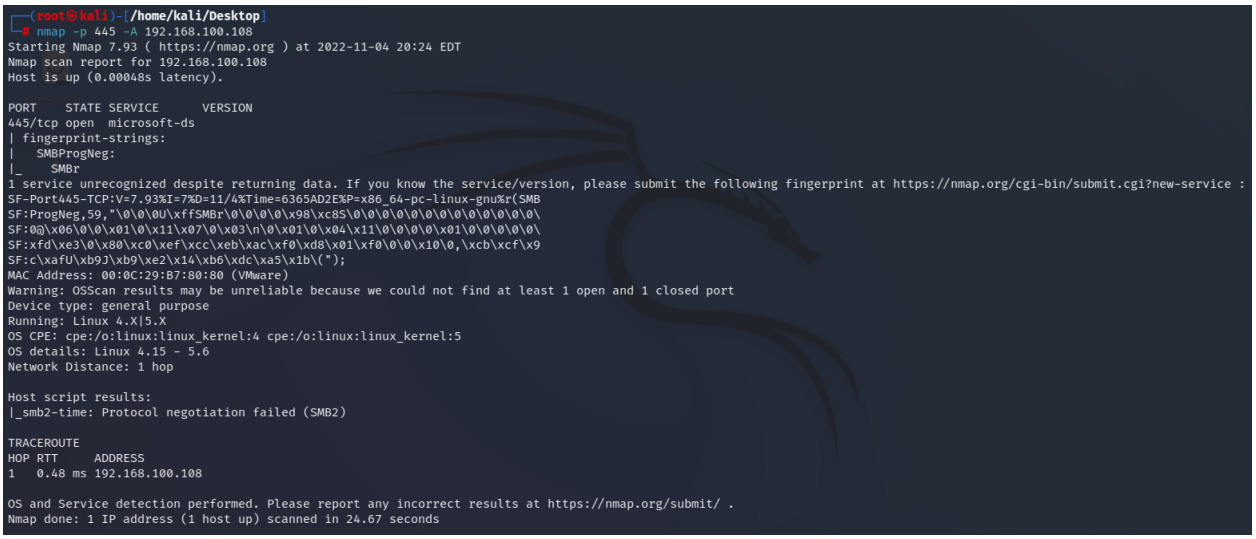
Nota. En la figura se aprecia que la sesión remota entre la máquina víctima y el del atacante no se crea.

- 192.168.100.108

Al tener el mismo puerto expuesto que el servidor A. Se procederá de la misma manera para el Servidor C, en la fase de enumeración se obtienen los siguientes resultados.

Figura 84

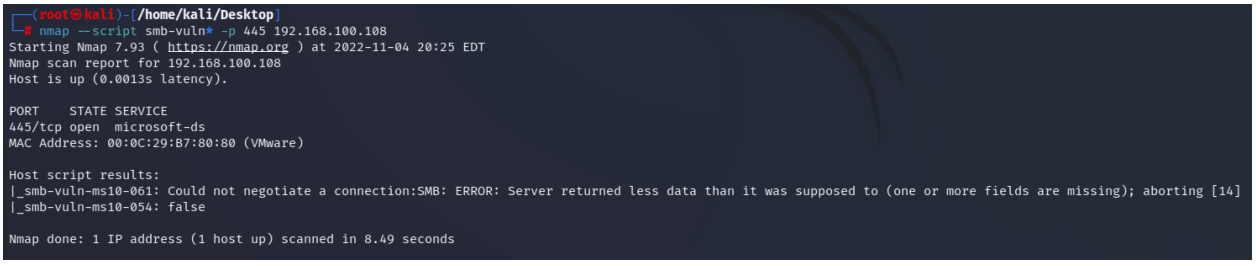
Resultados de escaneo del puerto 445 en la IP 192.168.100.108



A pesar de que la negociación con el protocolo SMB fallo, se procederá a intentar detectar a que es vulnerable el servicio SMB de la IP 192.168.100.108.

Figura 85

Vulnerabilidades detectadas del puerto 445 en la IP 192.168.100.108



En el resultado se indica que no puede negociar una conexión con la vulnerabilidad MS10-061 y tampoco con la MS10-054.

Puerto 1883

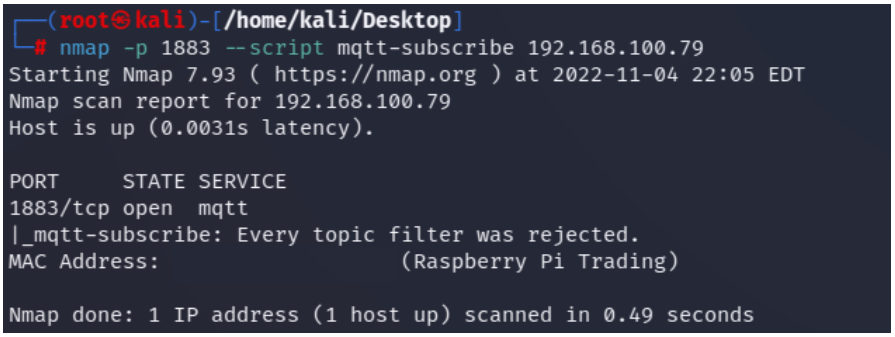
Este es el puerto predeterminado para el protocolo de mensajería/suscripción MQTT. Como se observa el servidor A cuenta con este puerto abierto, por lo que se procederá a explotarlo. Para esto se realizará un ataque de fuerza bruta, debido a que en el protocolo MQTT la autenticación es opcional y a pesar de que se implementen las credenciales, estas no son cifradas y se envían en texto claro. Teniendo en cuenta lo indicado también se podría realizar un ataque de hombre en el medio para obtener las contraseñas si se necesitase, pero como se mencionó anteriormente en la mayoría de aplicaciones IoT hay una falencia de mecanismos de limitación de velocidad y la autenticación está mal implementada.

En primera instancia se utilizará la herramienta Nmap para intentar establecer una conexión con un agente MQTT e intentar suscribirse a los temas predeterminados configurados por esta herramienta para tener información del sistema y todos los mensajes de diferentes clientes. Se emplea el siguiente código:

nmap -p 1883 --script mqtt-subscribe 192.168.100.79

Figura 86

Ejecución del script mqtt-subscribe sobre la IP 192.168.100.79



No hubo respuesta favorable a esta petición, se indica que todos los tópicos filtrados fueron rechazados. Se procede a realizar un ataque de fuerza bruta con la herramienta Metasploit, a través de un diccionario configurado se intentará obtener acceso al bróker MQTT.

Se utiliza el siguiente módulo:

use auxiliary/scanner/mqtt/connect

Se configura el diccionario de contraseñas, usuarios y el objetivo del ataque:

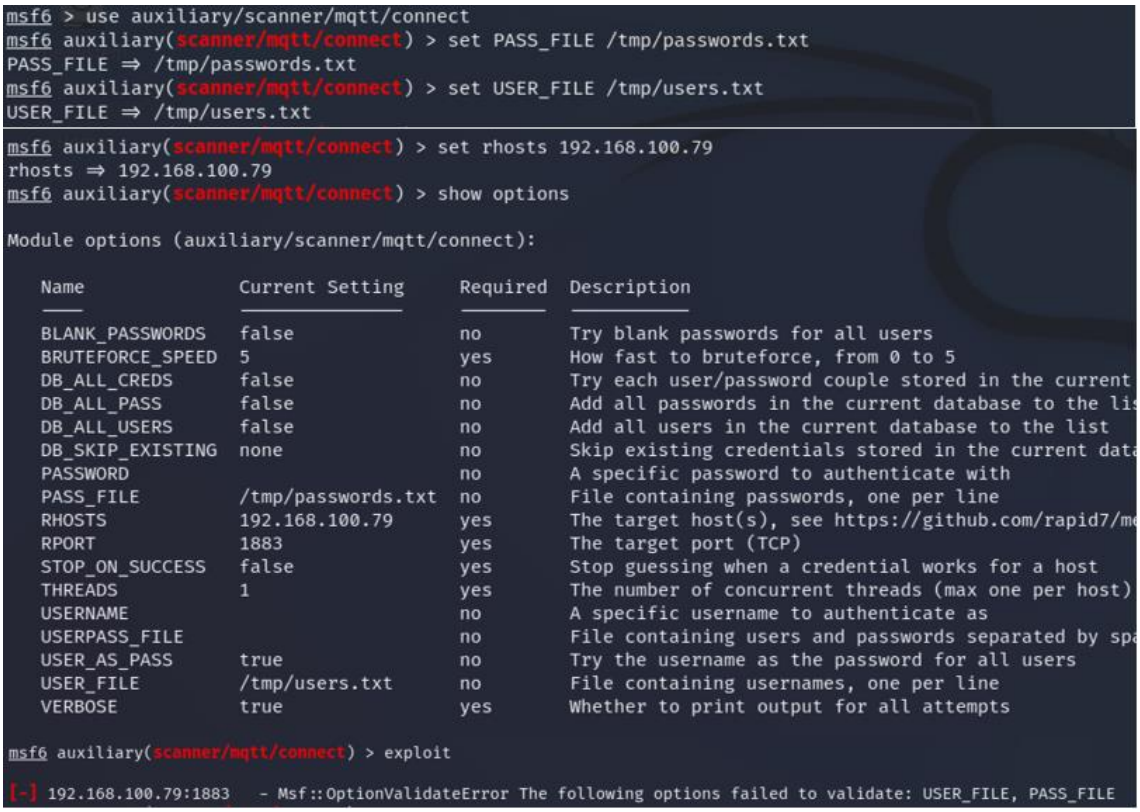
set PASS_FILE /tmp/passwords.txt

set USER_FILE /tmp/users.txt

set rhosts 192.168.100.79

Figura 87

Ataque de fuerza bruta sobre la IP 192.168.100.79



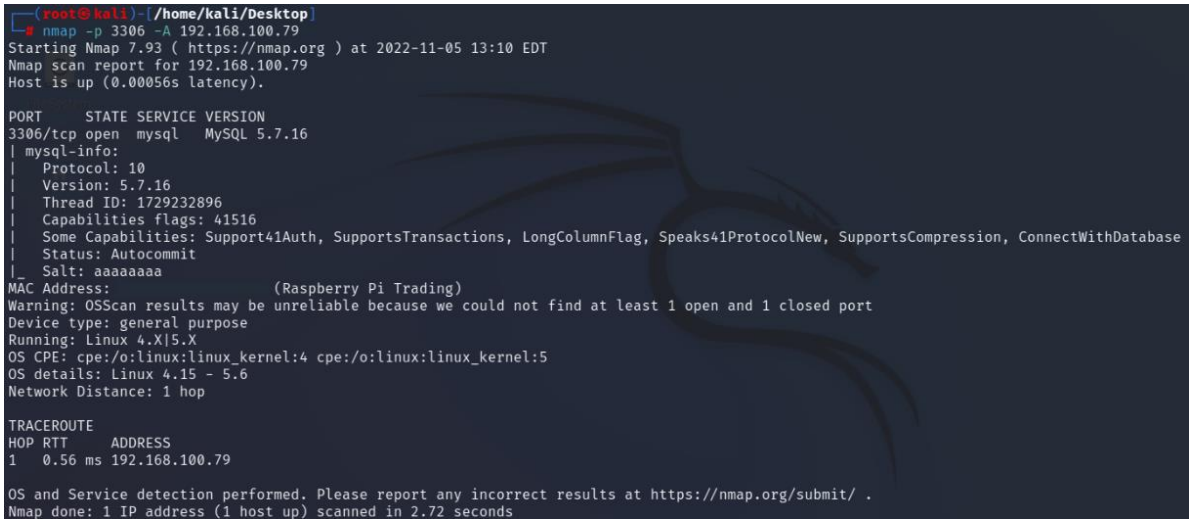
Si bien el puerto 1883 está abierto, no existe un bróker MQTT trabajando, tras estas pruebas se evidencia que no hay tópicos publicados por este puerto, en la fase de reconocimiento y en la fase de explotación no se logra establecer conexión.

Puerto 3306

MySQL es un sistema de gestión de base de datos relacional, el mismo que corre sobre el puerto 3306 por defecto, en el servidor A este puerto se encuentra abierto por lo que se pudo observar en la primera fase de recopilación activa de información, ahora nuevamente con la ayuda de la herramienta Nmap se escaneara solo el puerto 3306 para descubrir más información solo de este puerto y verificar si el mismo es explotable.

Figura 88

Resultados de escaneo del puerto 3306 en la IP 192.168.100.79



El servidor MySQL maneja la versión 5.7.16, al ser una versión antigua la misma es vulnerable a ataques de ejecución de código remoto. Como se observa en la Figura 89 mediante un ataque de fuerza bruta podemos obtener las credenciales para acceder a esta consola y poder ejecutar comandos con privilegios elevados desde la terminal del atacante. En primera fase con el módulo --script=mysql-brute de la herramienta Nmap se encontrará los nombres de usuario con credenciales válidas.

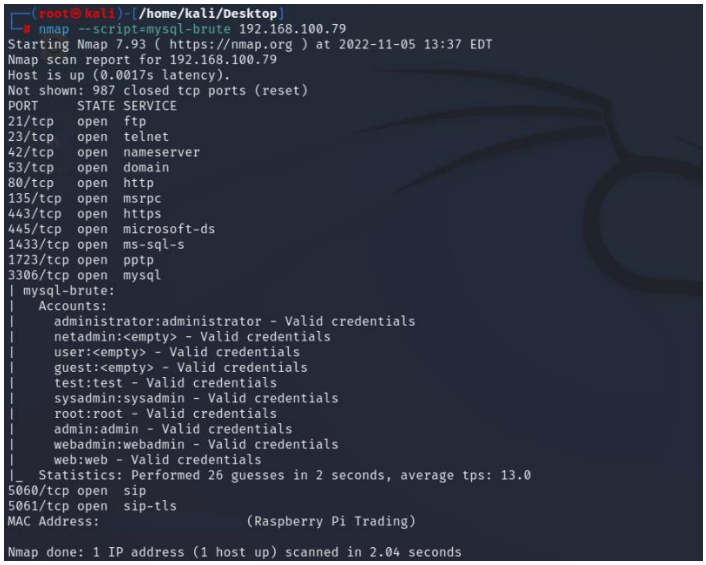
Tabla 18

Credenciales válidas detectadas en el servicio MySQL

Usuario	Contraseña
administrator	administrator
netadmin	<vacío> (No necesita contraseña solo el nombre de usuario)
user	<vacío> (No necesita contraseña solo el nombre de usuario)
guest	<vacío> (No necesita contraseña solo el nombre de usuario)
test	test
sysadmin	sysadmin
root	root
admin	admin
webadmin	webadmin
web	web

Figura 89

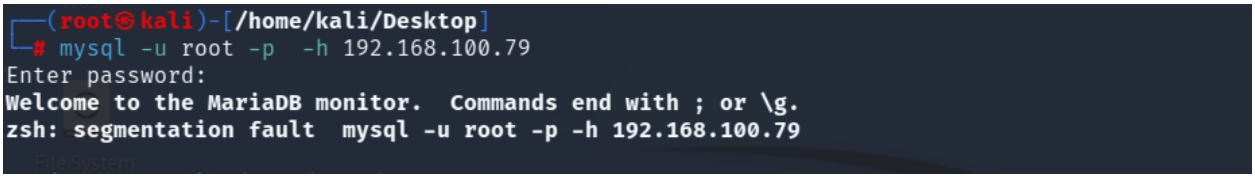
Ataque de fuerza buta al servicio MySQL



Con esta información se procede a explotar el puerto con las credenciales antes indicadas, se realizará la prueba con el usuario root.

Figura 90

Ingreso a la base de datos mediante terminal



Cuando se introducen las credenciales de root el servidor de base de datos si permite el acceso, pero el proceso se detiene y se bloquea debido a una falla de segmentación, se valida que el mismo inconveniente sucede con todas las credenciales listadas anteriormente.

Puerto 3389

Este puerto es generalmente utilizado para iniciar una conexión de escritorio de forma remota (RDP, por sus siglas en inglés), este protocolo ha sido blanco de varios tipos de ataques. A pesar que la comunicación es a través de un canal cifrado, la falta de una configuración correcta, los ataques de fuerza bruta y las vulnerabilidades de seguridad permiten que sea un objetivo atractivo para un atacante. Con la ayuda de la herramienta Hydra se realizará un ataque de fuerza bruta sobre el servidor C, para lo cual se debe emplear los diccionarios de usuarios y contraseñas de Metasploit.

A continuación, se utilizará los siguientes los siguientes parámetros para realizar un ataque dirigido y eficiente al objetivo. Partiendo que queremos explotar este servicio con privilegios elevados se busca una clave útil para el usuario admin.

hydra -s 3389 -l admin -P unix_passwords.txt 192.168.100.108 rdp

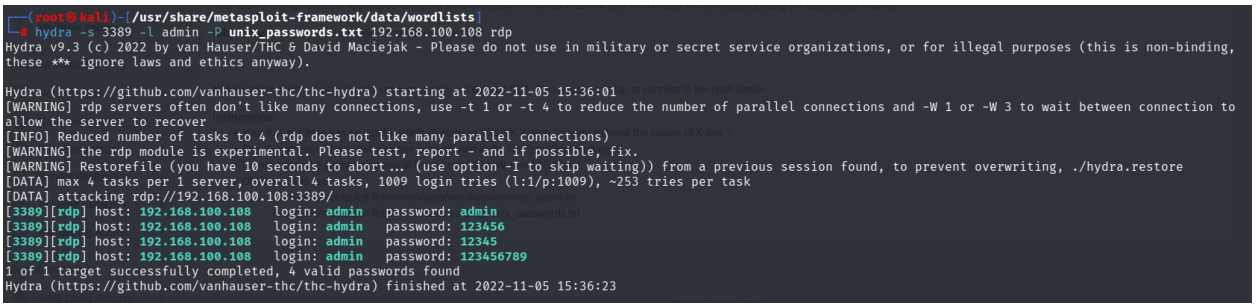
Tabla 19

Parámetros utilizados por hydra

Parámetro	Descripción
-s	Especifica el puerto
-l	Para configurar un nombre de usuario conocido
-P	Para especificar un diccionario de contraseñas a evaluar
rdp	El servicio a crackear, este servicio trabaja sobre el puerto 3389

Figura 91

Resultados obtenidos de un ataque de diccionario



Se encontraron 4 contraseñas válidas para el usuario admin, las cuales son:

Tabla 20

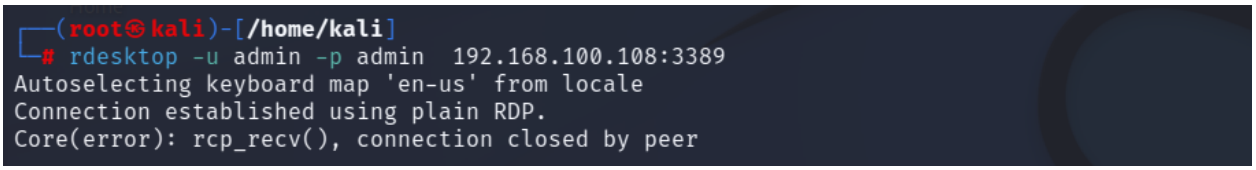
Credenciales válidas del servicio RDP en la IP 192.168.100.108

Usuario	Contraseña
admin	admin
admin	123456
admin	12345
admin	123456789

Para validar estas credenciales se establecerá una conexión remota entre el atacante y la víctima, para lo cual se utiliza la instrucción rdesktop seguido de las credenciales, la ip y el puerto del elemento de red objetivo.

Figura 92

Conexión RDP a la IP 192.168.100.108



Se establece la conexión con la máquina victima usando el protocolo RDP, a pesar que en el ataque de diccionario se identificaron las credenciales del servicio la conexión se demora en establecer y al final se cierra. Se valida con todas las credenciales encontradas, obteniendo el mismo resultado.

Pruebas de funcionamiento de los Honeypots

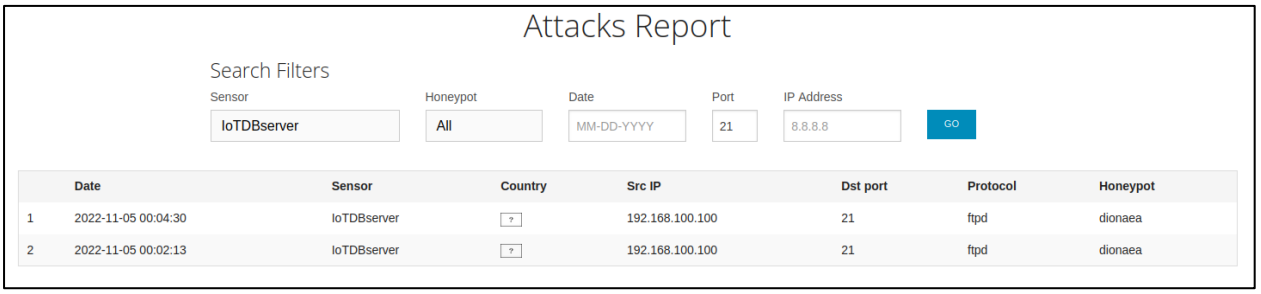
Dionaea

El sensor Dionaea es el que más registros de ataque posee. El servidor de la Honeynet está configurado de tal manera que detecte el más mínimo intento de intrusión así sea una simple instrucción de verificación de comunicación como un ping. Esto permitirá detectar cualquier intento de intrusión y ofrecer al administrador de red un reporte de las novedades que se susciten. El administrador de la red tendrá que descartar posibles falsos positivos o de lo contrario asumir el riesgo y levantar una regla en el administrador de registros. Lo más óptimo es identificar y descartar manualmente este tipo de peticiones. Si la red se encuentra debidamente segmentada y todos los elementos de red identificados, se crearía una regla que excluya aquel o aquellos dispositivos que por sus funciones realicen actividades de reconocimiento sobre la red IoT.

A continuación, se indica un extracto de las conexiones entrantes que se realizaron al sensor el 5 de noviembre de 2022 a las 00:04 desde una IP interna 192.168.100.100. La máquina intrusa intenta explotar el servicio ftp del honyepot, estos logs son exportados al servidor de registro:

Figura 93

Reporte de ataques al puerto 21 del honeypot Dionaea

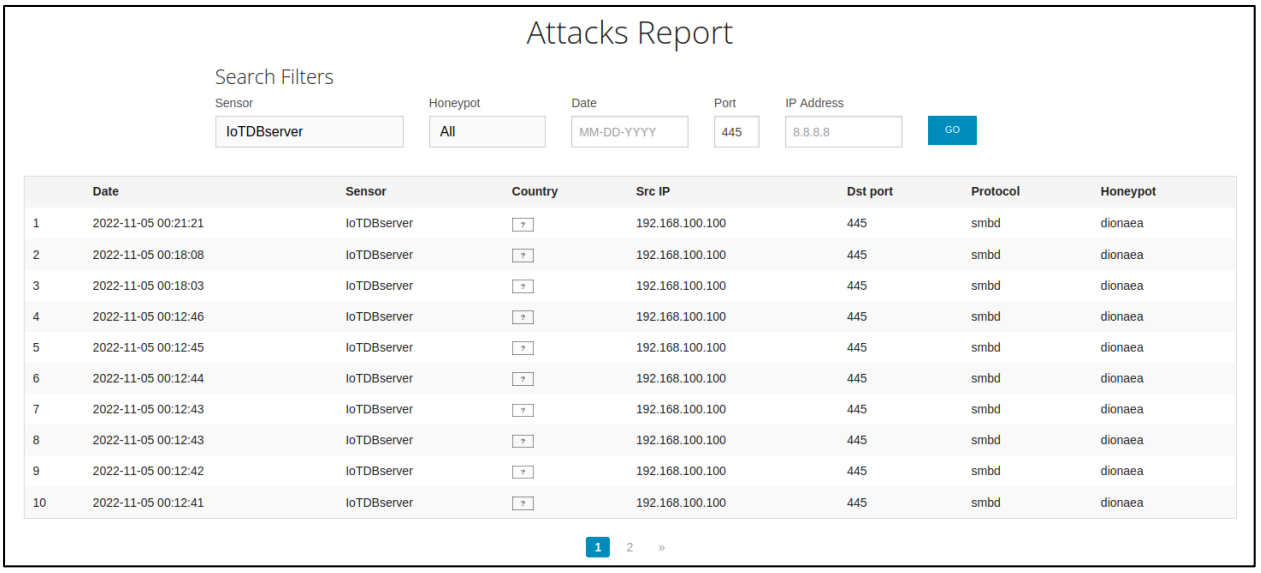


	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2022-11-05 00:04:30	IoTDBserver	?	192.168.100.100	21	ftpd	dionaea
2	2022-11-05 00:02:13	IoTDBserver	?	192.168.100.100	21	ftpd	dionaea

En el servidor de registro también se detectaron peticiones e intentos de explotación sobre el puerto 445 desde la ip 192.168.100.100:

Figura 94

Reporte de ataques al puerto 445 del honeypot Dionaea



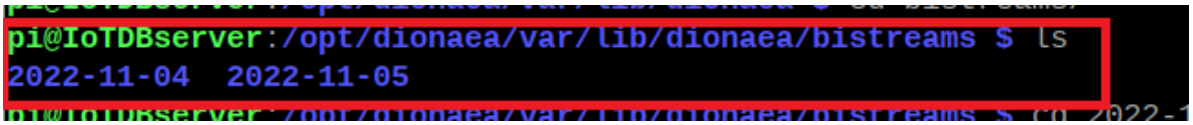
	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2022-11-05 00:21:21	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
2	2022-11-05 00:18:08	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
3	2022-11-05 00:18:03	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
4	2022-11-05 00:12:46	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
5	2022-11-05 00:12:45	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
6	2022-11-05 00:12:44	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
7	2022-11-05 00:12:43	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
8	2022-11-05 00:12:43	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
9	2022-11-05 00:12:42	IoTDBserver	?	192.168.100.100	445	smbd	dionaea
10	2022-11-05 00:12:41	IoTDBserver	?	192.168.100.100	445	smbd	dionaea

1 2 »

Todos los intentos de explotación también son almacenados localmente por el Honeypot, los eventos registrados por el sensor son almacenados en una carpeta diferente dependiendo el día en que son detectados. Estos datos se encuentran en la siguiente ruta:

Figura 95

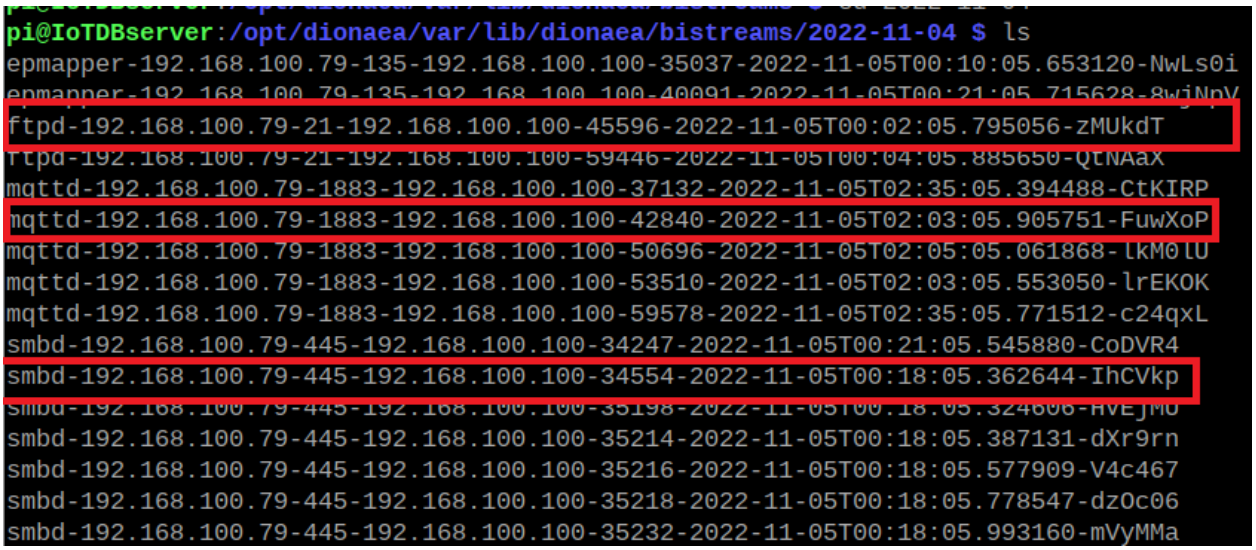
Ruta donde se almacenan los registros de ataques de Dionaea



A continuación, se presenta un extracto de los eventos registrados el 4 de noviembre de 2022, entre los servicios atacados se encuentran los protocolos ftp, mqtt, smb.

Figura 96

Logs generados por día en el honeypot Dionaea



Drupot

Al ser un servidor web tiene únicamente levantado el puerto 80, el servidor de logs registro 4789 ataques provenientes de la IP 192.168.100.100 como se indica a continuación:

Figura 97

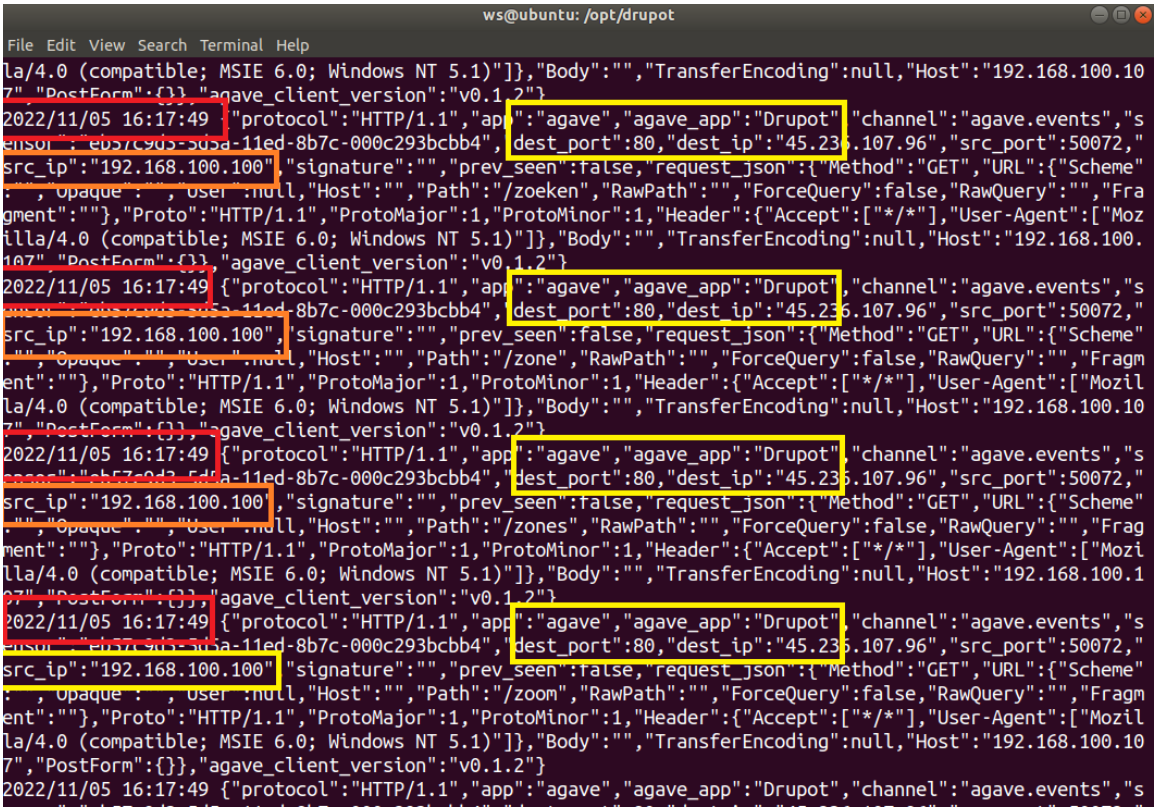
Resumen de ataques generados en el honeypot Drupot

	Name	Hostname	IP	Honeypot	UUID	Attacks
1-	IoTWserver-agave	IoTWserver	192.168.100.107	agave	81229a8c-5c80-11ed-9153-000c29b59cc7	4789

Del archivo **drupot.out** se obtienen todos los logs que registró el servidor web durante su funcionamiento, como se puede dar cuenta el 5 de noviembre de 2022 se realizaron múltiples conexiones entrantes de la IP antes indicada. Estas peticiones se realizan en intervalos de tiempos cortos. Debido a la gran cantidad de solicitudes detectadas se presenta un compendio de solicitudes, estas solicitudes quedan como evidencia de un ataque de Denegación de servicio DoS desde la IP atacante 192.168.100.100.

Figura 98

Logs generados de los ataques en el honeypot Drupot

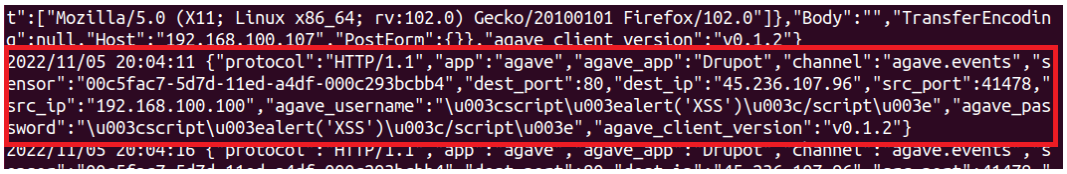


Además, ese mismo día a las 20 horas con 4 minutos se registra un intento de explotación de la vulnerabilidad XSS (Cross-site scripting) que permite a los adversarios inyectar código en la página web. Se observa que se realiza un script a través de los campos de inicio de sesión, el fin es generar un popup dentro del navegador con la palabra XSS. En el registro todos los campos se ingresan en el sistema de codificación Unicode.

<script>alert("XSS")</script>

Figura 99

Detección de un ataque Cross-Site scripting



El 26 de noviembre de 2022 se detecta una petición maliciosa en el servidor web del Honeypot Drupot, la IP 192.168.100.100 realiza una inyección SQL. El atacante intenta omitir la autenticación que la página web tiene mediante una instrucción diseñada para modificar la consulta SQL en el parámetro Login. La instrucción es la siguiente:

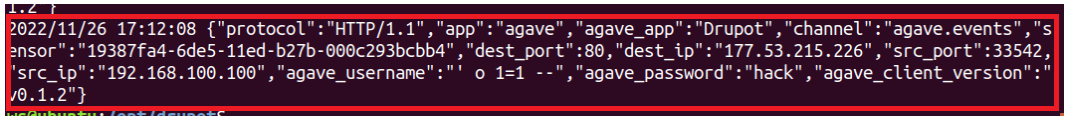
' o 1=1 –

Esta instrucción al final contiene una secuencia de comentarios (--) que provoca que se ignore el resto de la consulta haciendo una equivalencia con la consulta:

SELECT * FROM users WHERE username = ' ' OR 1=1

Figura 100

Detección de un ataque de inyección SQL

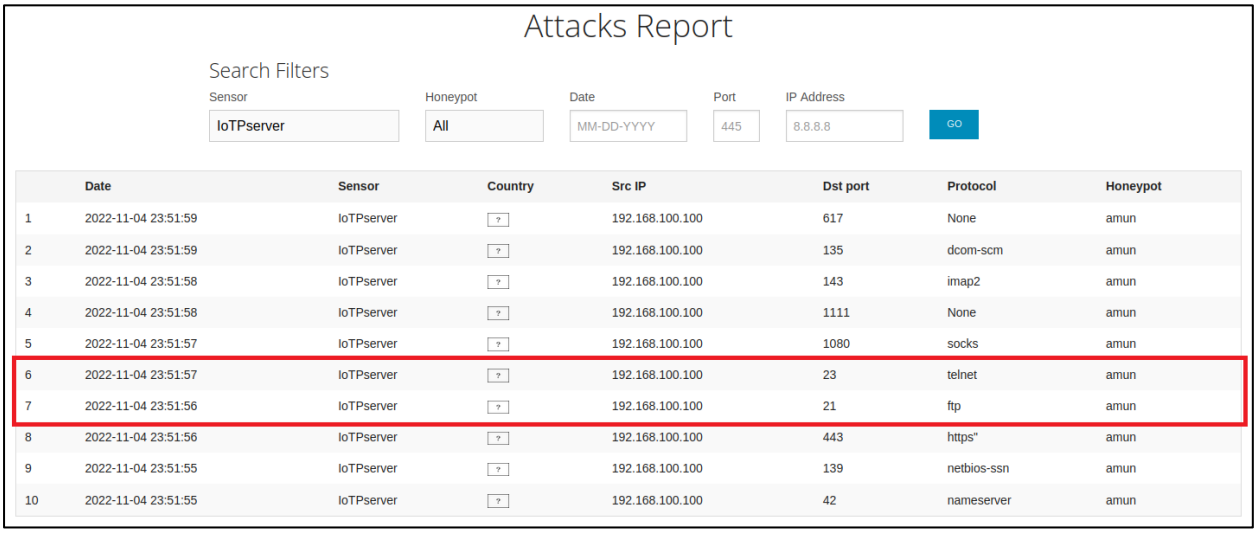


Amun

El señuelo Amun también registró ataques a diferentes servicios, el 4 de noviembre de 2022 a partir de las 23 horas y 51 minutos empieza a sufrir diversos ataques en distintos puertos vulnerables. Los servicios que más llaman la atención son los puertos 21 y 23 que corresponden a protocolo ftp y telnet respectivamente. Se observa que todos los ataques provienen de la IP 192.168.100.100 la cuál teniendo en cuenta la topología de la red implementada, el adversario se encuentra dentro del ecosistema.

Figura 101

Reporte de ataques del honeypot Amun



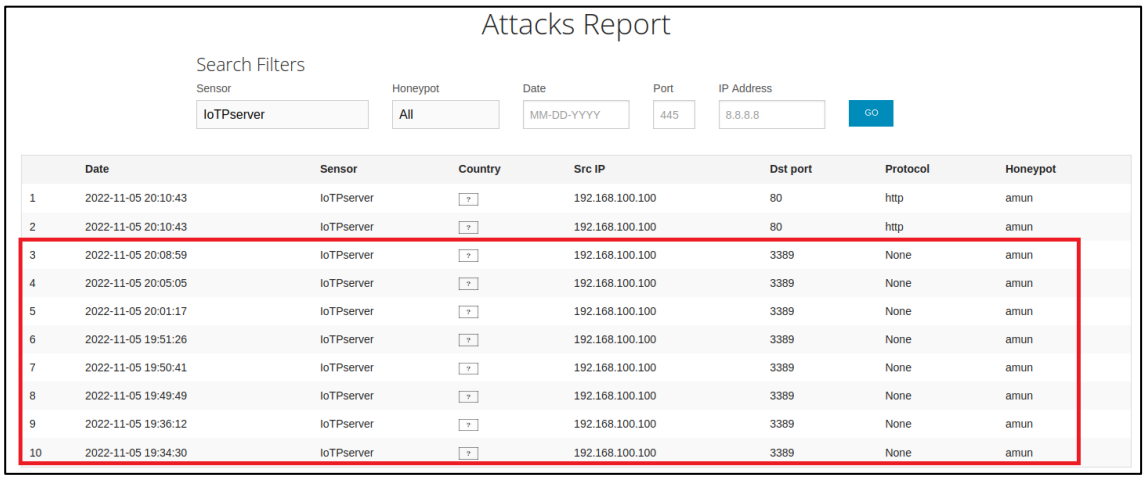
	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2022-11-04 23:51:59	IoTPserver	?	192.168.100.100	617	None	amun
2	2022-11-04 23:51:59	IoTPserver	?	192.168.100.100	135	dcom-scm	amun
3	2022-11-04 23:51:58	IoTPserver	?	192.168.100.100	143	imap2	amun
4	2022-11-04 23:51:58	IoTPserver	?	192.168.100.100	1111	None	amun
5	2022-11-04 23:51:57	IoTPserver	?	192.168.100.100	1080	socks	amun
6	2022-11-04 23:51:57	IoTPserver	?	192.168.100.100	23	telnet	amun
7	2022-11-04 23:51:56	IoTPserver	?	192.168.100.100	21	ftp	amun
8	2022-11-04 23:51:56	IoTPserver	?	192.168.100.100	443	https"	amun
9	2022-11-04 23:51:55	IoTPserver	?	192.168.100.100	139	netbios-ssn	amun
10	2022-11-04 23:51:55	IoTPserver	?	192.168.100.100	42	nameserver	amun

Nota. En la figura se aprecia el reporte de ataques generados el 4 de noviembre de 2022 sobre el honeypot Amun, se evidencia algunos de los protocolos atacados y la dirección de la IPv4 atacante.

Se presenta un extracto de los últimos ataques captados por el Honypot Amun en donde el principal protocolo a atacar es el 3389. Se evidencia que este puerto es muy atractivo para el atacante ya que si se logra consumar el ataque puede iniciar una conexión remota a la máquina y apropiarse del sistema.

Figura 102

Reporte de ataques al puerto 3389 del honeypot Amun



	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2022-11-05 20:10:43	IoTPserver	?	192.168.100.100	80	http	amun
2	2022-11-05 20:10:43	IoTPserver	?	192.168.100.100	80	http	amun
3	2022-11-05 20:08:59	IoTPserver	?	192.168.100.100	3389	None	amun
4	2022-11-05 20:05:05	IoTPserver	?	192.168.100.100	3389	None	amun
5	2022-11-05 20:01:17	IoTPserver	?	192.168.100.100	3389	None	amun
6	2022-11-05 19:51:26	IoTPserver	?	192.168.100.100	3389	None	amun
7	2022-11-05 19:50:41	IoTPserver	?	192.168.100.100	3389	None	amun
8	2022-11-05 19:49:49	IoTPserver	?	192.168.100.100	3389	None	amun
9	2022-11-05 19:36:12	IoTPserver	?	192.168.100.100	3389	None	amun
10	2022-11-05 19:34:30	IoTPserver	?	192.168.100.100	3389	None	amun

En la ruta /opt/amun/logs se guardan todos los registros recopilados por el honeypot, estos registros indican información más detallada de los distintos ataques realizados a este señuelo. En los archivos amun_request_handler.log se guardan todas las solicitudes receptadas, se presenta un extracto de logs generados el 4 de noviembre de 2022, podemos apreciar que la IP atacante 192.168.100.100 está realizando un ataque con la herramienta Nmap al puerto 8080, se aprecia la cabecera y cuerpo correspondiente al payload ejecutado con esta herramienta.

Figura 103

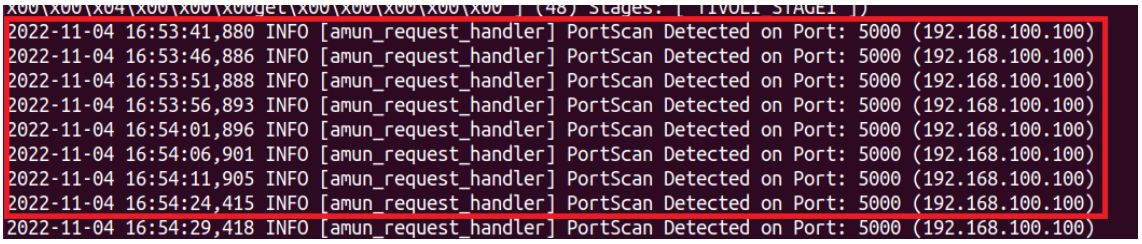
Logs generados después de un ataque en el honeypot Amun

Nota. En la imagen se evidencia la herramienta utilizada para realizar el ataque además de la fecha y hora que se ejecutó el mismo.

Se observa un extracto en el cual se visualiza diferentes ataques de escaneo de puertos desde una misma IP al puerto 5000 del señuelo, se registra la fecha y hora exacta del ataque, el señuelo está en la capacidad de diferenciar el tipo de ataque realizado a su infraestructura.

Figura 104

Logs generados por el honeypot Amun



Conclusiones

El diseño de la solución de seguridad informática propuesta en el presente trabajo busca ser aplicable para la mayor cantidad de entornos basados en tecnologías de la información y comunicación. Si bien la arquitectura implementada se basa en un entorno del Internet de las Cosas, los honeypots pueden ser reemplazados en la fase de diseño para cubrir otras aristas y vectores de ataques dependiendo el ecosistema que se pretenda proteger. Así, se obtiene una arquitectura útil y configurable, lo que representa una ventaja hoy en día con el crecimiento tan acelerado de nuevas técnicas de intrusión y los procesos automatizados de ejecución de ataques.

La principal fortaleza de la honeynet diseñada es su escalabilidad, permite incrementar el número de sensores (honeypots) de acuerdo a los requerimientos de seguridad, capacidad de infraestructura, espacio físico y presupuesto económico de la organización. De hecho, este último punto se puede aprovechar aún más ya que el software de los honeypots es libre y como ventaja adicional hoy en día aún siguen dando soporte y actualizaciones a librerías con las que funcionan estos señuelos. Con el surgimiento de la industria 4.0, el Internet de las Cosas y la

migración de los sistemas core a la nube por parte de las empresas alrededor del mundo es útil esta arquitectura de seguridad para incrementar la estructura de seguridad de la información a la que se rigen las organizaciones.

La honeynet híbrida propuesta permite repartir los señuelos en diferentes servidores creando redundancia en la arquitectura física de la solución. Se diseñó así con la finalidad de mantener totalmente operativa la red de señuelos. Al segregar los señuelos en diferentes servidores, se puede garantizar la operabilidad de la solución pese a alguna razón de mala configuración o ataque contra la integridad física de uno de estos sistemas. La honeynet híbrida seguirá recolectando y monitoreando los eventos de los honeypots que sigan funcionando correctamente.

El enfoque que se pretende cubrir con la implementación realizada es la detección de ataques automatizados y dirigidos a redes IoT que por su naturaleza se vuelven atractivas para atacantes, bots y amenazas desconocidas en la actualidad. Al utilizar honeypots de baja interacción se obtiene un sistema que atrae principalmente a bots configurados para detectar vulnerabilidades sobre entornos informáticos. Cabe indicar que el diseño no pretende generar una alta interacción con el atacante, si la finalidad fuese esta se seleccionará otro tipo de honeypots como los de interacción alta o inclusive de interacción media. Por este motivo esta solución de seguridad no será capaz de detectar ataques de día cero. Sin embargo, el diseño se puede acoplar para diferentes fines desde la protección de sistemas reales hasta entornos de investigación donde se pretenda recolectar técnicas más avanzadas utilizadas por ciberdelincuentes.

El sistema fue sometido a pruebas de validación mediante una metodología de auditoría de seguridad informática. El fin de esta implementación fue garantizar la recolección de eventos perjudiciales que se generen a nivel de red. Consecuentemente las técnicas para validar el funcionamiento de estos señuelos son elementales. Como se mencionó anteriormente la

arquitectura desplegada la componen principalmente señuelos de baja interacción como Dionaea, Amun aunque también se utiliza un honeypot que permite más interacción como Drupot. Estos señuelos son eficaces para detectar amenazas como bots que suelen ser programas informáticos que se encargan de la detección de vulnerabilidades de manera automática. Sin embargo, para ataques más sofisticados o ataques dirigidos esta elección de honeypots no es la más apropiada.

La configuración de la honeynet y la interconexión de los honeypots permitieron monitorear todos los eventos anómalos dentro de la red. Esta herramienta faculta al arquitecto de red la supervisión de dichos eventos y tomar mediadas proactivas mediante la caza de amenazas. La concentración de todos los registros en una base de datos facilitó el análisis de los logs generados. La interfaz web del servidor centralizado permitió obtener estadísticas en tiempo real de los eventos registrados y al estar todo catalogado se pudo identificar las direcciones IP de las principales amenazas.

Se pudo apreciar que la solución implementada detecta ataques de escaneo de puertos, ataques sobre servicios específicos, inyecciones de código, ataques de denegación de servicio, entre otros. Adicionalmente, mediante el análisis de estos eventos se pudo determinar las técnicas utilizadas por la amenaza, como los scripts específicos utilizados para vulnerar cada honeypot, las peticiones empleadas y los hashes coincidentes de los exploits detectados. Esta herramienta cuenta con una biblioteca amplia de firmas que permiten reconocer y catalogar los ataques registrados. La solución implementada cubre las principales disposiciones y recomendaciones expuestas en normativas internacionales para la seguridad informática en el Internet de las Cosas.

La solución de seguridad es de fácil implementación y mantenimiento por lo que no requiere personal altamente calificado para la instalación de los señuelos y monitoreo de los eventos. Sin embargo, si se cuenta con un equipo de seguridad apropiado se puede

interconectar este sistema con otras herramientas de correlación de eventos como un SIEM (Security Information and Event Management). Por consecuencia si la organización cuenta con un programa de seguridad se puede reforzar el esquema existente con el diseño propuesto. El servidor de registro MHN cuenta con un gran número de reglas implementadas, pero posibilita crear nuevas reglas a partir de los hallazgos de los eventos recolectados y las nuevas amenazas descubiertas.

El hardware disponible para la implementación de la herramienta resultó ser apropiado y no limitó los requerimientos de operabilidad establecidos en su diseño. La Raspberry Pi es un excelente ordenador de placa reducida para la puesta en marcha de honeypots de baja interacción. Además de ser altamente portable y configurable reduce significativamente los costos de ejecución de la solución de seguridad. La limítate de utilizar señuelos de baja interacción es que en ataques realizados por un ciberdelincuente este puede reconocer que se trata de un sistema trampa.

Recomendaciones

Antes de la implementación de la herramienta se debe realizar una evaluación de las necesidades de seguridad de la red donde se pretenda instalar la solución. Existen diversos tipos de honeypots que pueden ser adaptados y cada uno está diseñado para emular servicios específicos que probablemente sean de mayor utilidad en ciertas redes.

El mantenimiento y la configuración del sistema de seguridad es sencillo sin embargo es aconsejable evaluar periódicamente el rendimiento de los dispositivos físicos que contienen la solución. Una política de mantenimiento de infraestructura y equipos tecnológicos puede ayudar a conservar totalmente operativa la herramienta.

La gran cantidad de datos generados a causa de la recolección de logs provoca un uso alto de capacidad de memoria. En consecuencia, es recomendable contar con una política de

respaldos para determinar la utilidad de los datos y almacenar la información generada de manera eficiente.

Para la implementación de la herramienta se hace necesario revisar los manuales de configuración de cada honeypot así como del servidor de registro centralizado. Esto dará un panorama claro de las utilidades y limitaciones de cada señuelo y permitirá definir el alcance del proyecto.

Trabajos futuros

Implementación de otras herramientas de seguridad que complementen la funcionalidad de la solución de seguridad. Se puede abordar seguridad en redes inalámbricas con el uso de honeypots WiFI o también conocidos como hotspot para distraer y monitorear accesos no autorizados en redes WiFi.

Despliegue de la solución de seguridad en otros sistemas de última generación. Se puede adaptar el diseño para entornos basados en la nube, Smart Cities, sistemas robóticos industriales y entornos domóticos basados en IoT. Esto permitirá obtener un espectro más amplio del panorama de amenazas que afecta a cada uno de estos ecosistemas.

Creación de una herramienta mediante aprendizaje automático que permita captar e interpretar los datos recolectados por la Honeynet para ejecutar acciones de protección de manera autónoma sobre la red.

Utilización de honeypots de alta interacción diseñados específicamente para emular un sistema real de una organización, evitando la exposición de documentación sensible. Sirviendo de base para descubrir ataques de día cero (Zero-day Attack), nuevas técnicas, tácticas y procedimientos empleados actualmente por los ciberdelincuentes. El fin es obtener una honeynet de investigación basada en un modelo real de una organización como una entidad

financiera, una institución del estado o centros de salud que suelen ser los más atractivos y propensos a sufrir ataques.

Bibliografía

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Zhou, Y. (2017). *Understanding the Mirai Botnet.* https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf.

Arroyo, D., Gayoso, V., & Hernández, L. (2020). *Ciberseguridad.* Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas.

AVG Technologies. (2020). *What Is an Exploit in Computer Security?* https://www.avg.com/es/signal/computer-security-exploits.

Buchanan, W., Prasad, A., Chandramouli, R., & Benslimane, A. (2021). *Implementing Enterprise Cybersecurity With Open-Source Software and Standard Architecture.* Gistrup: River Publishers.

Chicano, E. (2015). *Auditoría de Seguridad Informática.* Málaga: IC Editorial.

Díaz, G., Alzórriz, I., Sancristóbal, E., & Castro, M. (2014). *Procesos y herramientas para la seguridad de redes.* Madrid: Universidad Nacional de Educación a Distancia.

EC-Council. (2021). *Ethical Hacking Essentials.* New Mexico: EC-Council New Mexico.

Escrivá, G., Romero, R., Ramada, D., & Onrubia, R. (2013). *Seguridad Informática.* Madrid: Macmillan Iberia, S.A.

Gallego, E., & López, J. (2004). *Honeynets: Aprendiendo del Atacante.* Universidad Politécnica de Madrid.

Gordon Lyon. (2022). *Nmap.* https://nmap.org/.

Howell, P. (2018). *Mirai IoT botnet variant likely used in January DDoS attack against Dutch banks.* https://www.cyberscoop.com/iot-botnet-dutch-banks-recorded-future/.

ISO/IEC. (2013). *International Standard ISO/IEC 27000.* Switzerland.

ISO/IEC. (2013). *International Standard ISO/IEC 27002.* Geneva: ISO.

Kaspersky. (2022). *43% of businesses don't protect their full IoT suite.* https://www.kaspersky.com/about/press-releases/2022_43-of-businesses-dont-protect-their-full-iot-suite.

Kaspersky Lab. (2019). *IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019.* https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019.

López, E. (2017). *Raspberry Pi: fundamentos y aplicaciones.* Madrid: RA-MA Editorial.

National Security Agency. (2002). *Information Assurance Technical Framework (IATF) Release 3.1.* Fort Meade, Maryland: National Security Agency.

Netscout Systems, Inc. (2019). *Dawn of the Terrobit Era.* USA: Netscout Systems, Inc.

Nokia. (2020). *Threat Intelligence Report 2020.* https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html.

OffSec Services Limited. (2022). *Hping3.* https://www.kali.org/tools/hping3/.

OWASP Foundation, Inc. (2018). *OWASP Internet of Things.* https://owasp.org/www-project-internet-of-things/.

Palo Alto Networks. (2020). *2020 Unit 42 IoT Threat Report.* Santa Clara: Palo Alto Networks.

Rapid7 Inc. (2022). *Metasploit.* https://docs.rapid7.com/metasploit/.

Raspberry Pi Foundation. (2022). *Raspberry Pi.* https://www.raspberrypi.com/products/raspberry-pi-4-model-b/.

Red Hat. (2020). *What is CVE.* https://www.redhat.com/es/topics/security/what-is-cve.

Statista. (2021). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030.* https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Team, A. (2018). *Fast & Furious IoT Botnets: Regifting Exploits.* https://www.netscout.com/blog/asert/fast-furious-iot-botnets-regifting-exploits.

UIT-T. (2018). Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela. *Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad*, 7-21.

Verdejo, G. (2003). *Seguridad en Redes IP.* Bellaterra: Universidad Autónoma de Barcelona.

Wang, J., & Kissel, Z. (2015). *Introduction to Network Security : Theory and Practice.* John Wiley & Sons, Incorporated.

Wren, C., Reilly, D., & Berry, T. (2010). *Footprinting: A Methodology for Auditing eSystem Vulnerabilities*. IEEE, 1-5.

Apéndices