

Descripción del problema

Contexto General

En el panorama actual de la ciberseguridad, las organizaciones enfrentan un número creciente de ataques informáticos dirigidos a sus infraestructuras, sistemas y datos. Estos ataques, motivados por diversas razones, como el robo de información, la interrupción de servicios o el sabotaje, ponen en riesgo los principios fundamentales de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad (triada CID). Garantizar que los datos sean accesibles únicamente para usuarios autorizados, que permanezcan sin alteraciones no autorizadas y que estén disponibles cuando se necesiten, es crucial para la continuidad operativa de cualquier organización.

Aunque herramientas tradicionales como los firewalls y los sistemas de detección de intrusos (IDS) juegan un rol importante, su alcance puede ser limitado. Estas soluciones tienden a enfocarse en bloquear amenazas conocidas o reaccionar ante ataques en curso, sin proporcionar una visión profunda de las tácticas, técnicas y procedimientos (TTPs) de los atacantes.

Es en este contexto donde los honeypots y las plataformas SIEM (Security Information and Event Management) desempeñan un papel clave. Los honeypots no solo sirven como señuelos para atraer a los atacantes, sino que también permiten estudiar su comportamiento en un entorno controlado, proporcionando información valiosa que ayuda a anticiparse a futuros ataques. Por su parte, los sistemas SIEM recopilan, analizan y correlacionan datos de eventos en tiempo real desde múltiples fuentes de la red, ofreciendo una visión integral de las amenazas y asegurando un monitoreo continuo de la infraestructura.

Al combinar estas tecnologías, las organizaciones pueden fortalecer sus defensas, mejorando tanto la detección como la respuesta a incidentes, mientras protegen los pilares fundamentales de la triada CID frente a un panorama de amenazas en constante evolución.

1. Ciberseguridad y Amenazas Informáticas

La tecnología ha cambiado la forma de vivir en la mayoría de sociedades, mejorando desmesuradamente la calidad de vida. Sin embargo, el uso de la tecnología digital algunas veces puede volverse en contra del usuario, sea persona, empresa e incluso gobierno. A medida que el internet incrementa la interacción humana y mejora las relaciones sociales se convierte en una espada de doble filo dado que el ciberespacio no tiene límites y en

este se pueden llevar a cabo actividades ilegales. (Raufo, Tsado & Ben-Edet, 2021)

La ciberseguridad comprende un conjunto de prácticas, tecnologías y controles diseñados para proteger los sistemas y datos frente a accesos no autorizados, ataques y daños.

Los tipos de amenazas incluyen:

- **Ataques de fuerza bruta:** Intentos automatizados de descubrir credenciales de acceso.
- **Exploits:** Uso de vulnerabilidades conocidas para comprometer un sistemas.
- **Malware:** Software malicioso diseñado para dañar o comprometer dispositivos.

La detección y el análisis de estas amenazas son componentes esenciales para mitigar riesgos y minimizar el impacto de incidentes de seguridad.

2. Honeypots: Concepto y Clasificación

Un **honeypot** es un sistema de ciberseguridad diseñado para simular vulnerabilidades reales y atraer a los atacantes. Los honeypots tienen tres principales funcionalidades (1) Detección, (2) Prevención e (3) Investigación. (Javadpour et al, 2024)

Se clasifica en:

- **De baja interacción:** Simula servicios básicos y es más seguro, pero con datos limitados.
- **De alta interacción:** Simula sistemas completos, proporcionando datos más ricos, pero con mayores riesgos si se comprometen.

Los **honeypots** permiten:

- Identificar vectores de ataque emergentes.
- Analizar tácticas y herramientas de los atacantes.
- Desviar amenazas lejos de sistemas reales.

3. Análisis de Logs y Recolección de Datos

Los logs son registros generados por el honeypot que documentan cada interacción. Su análisis permite:

- Identificar patrones en intentos de ataque.
- Reconocer direcciones IP sospechosas
- Clasificar técnicas de ataque, como inyecciones de comandos o escaneo de puertos.

4. Herramientas Seleccionadas

En este proyecto se utilizó la herramienta Vmware workstation pro para la configuración de la red, la herramienta syslog-ng para guardar los registros de los tentativos de acceso por parte del atacante, los servicios http (con su respectiva página web y un login), ssh y ftp.

El atacante utilizará Hydra para descubrir la contraseña (voluntariamente débil), ssh y ftp para vulnerar la máquina.

Objetivos del Proyecto

Propósito General del Proyecto

Este proyecto se realiza con el propósito de proporcionar un entorno controlado y

seguro para estudiar los intentos de ataque dirigidos a servicios simulados.

Busca identificar patrones, métodos y herramientas utilizadas por los atacantes, permitiendo una mejor comprensión de las amenazas actuales y ayudando a las organizaciones y profesionales a reforzar sus defensas cibernéticas.

- **¿Por qué se realiza este proyecto?**

Para identificar y analizar tácticas de ataque, mejorar estrategias de seguridad y generar conocimiento sobre amenazas emergentes.

¿Qué problema intenta resolver?

La falta de herramientas proactivas que permitan recopilar datos detallados sobre intentos de ataque en tiempo real y entender los comportamientos de los atacantes.

Objetivo General

Diseñar, implementar y desplegar un honeypot que permita detectar, registrar y analizar intentos de ataque.

Objetivos Específicos

1. Configurar un entorno de honeypot seguro y funcional:
2. Registrar y recopilar datos de los intentos de ataque
3. Analizar los datos obtenidos.

Metodología del Proyecto

La metodología de este proyecto se centró en el diseño, implementación y análisis de un honeypot como herramienta de detección y estudio de ataques cibernéticos. Este proceso requirió la integración de diferentes herramientas y técnicas para simular un entorno de red realista y atractivo para los atacantes. La estrategia metodológica asegura que los objetivos planteados sean alcanzados de manera estructurada, precisa y replicable.

1. Enfoque metodológico

El enfoque seguido en este proyecto es experimental y analítico, ya que se diseñó y configuró un entorno controlado para capturar información sobre posibles intentos de ataque. El proceso involucra tres fases principales:

- ❖ **Planeación:** Se diseña la arquitectura del honeypot considerando los elementos esenciales para simular un entorno realista (red interna, servicios falsos, y red atacante).
- ❖ **Implementación:** Se configuran los elementos tecnológicos, incluyendo el honeypot, los servicios simulados (HTTP, FTP, SSH) y el sistema IDS/EDR para la recolección y análisis de datos.
- ❖ **Recolección y análisis de datos:** Los datos recolectados se procesan para identificar patrones de ataque, evaluar vulnerabilidades y obtener conclusiones útiles para fortalecer la seguridad de redes reales.

- ❖ **Evaluación y presentación:** Análisis de resultados y generación de conclusiones.

2. Procedimientos y Técnicas

1. Planeación del Entorno

- Identificación de los componentes necesarios: Honeypot (servicios SSH, FTP Y HTTP), red interna y red atacante.
- Definición de las direcciones IP y subredes para la simulación (172.16.0.0/24 para la red interna, incluyendo el honeypot, y 192.168.1.0/24 para la red atacante).

2. Configuración del Honeypot:

- Uso de herramientas como SSH, FTP y un servidor HTTP simulado.
- Configuración de logs detallados para registrar internos de conexión, credenciales falsas y comandos ejecutados.

3. Simulación de la red atacante:

- Implementación de la máquina host que represente a los atacantes, equipada con herramientas como Nmap y Hydra para realizar pruebas de ataque controladas.

4. Implementación del Sistema de registro de logs:

- Integración con un servidor de análisis de logs (syslog-ng).

5. Captura y análisis de datos:

- Recolección de logs de cada componente del honeypot.
- Uso de herramientas de análisis para identificar patrones en los intentos de ataque.

3. Diseño Detallado de la Arquitectura

La imagen describe una arquitectura de red segmentada utilizando máquinas virtuales en VMware y un Honeypot como señuelo (ver diagrama):

1. Honeypot (NAT “publicado”):

- Se configura en una red pública con reglas que permiten el acceso desde el exterior (a través de NAT), pero el tráfico a

los servidores privados está restringido. El honeypot se configura para atraer a los atacantes.

2. Servidor de producción (vnet “privada”):

- Los servidores reales y de administración están en una red privada, aislados del tráfico directo externo. Los comandos del firewall *iptables* protegen esta red bloqueando conexiones no deseadas.

3. Servidor de administración (IT ADMIN vnet "privada"):

- Simula el origen de los ataques cibernéticos.
- La máquina atacante (192.168.1.210) ejecuta herramientas como Nmap para interactuar con el honeypot.

4. Sistema de logs:

- Monitorea todo el tráfico entre las redes y registra eventos sospechosos para su análisis.

Este diseño permite simular un entorno realista donde los atacantes interactúan con los servicios falsos, generando datos valiosos para el análisis.

4. Justificación

La metodología aplicada garantiza que los objetivos específicos del proyecto sean alcanzados de manera estructurada y efectiva.

- La separación en redes (interna, honeypot y atacante) replica un entorno empresarial típico, facilitando la identificación de vulnerabilidades y el análisis de patrones de ataque.
- La simulación de un atacante proporciona un contexto realista para evaluar la efectividad del honeypot.
- El análisis de los datos recolectados ayudará a identificar métodos comunes de ataque y recomendaciones de seguridad aplicables a redes reales.

5. Cronograma

Fase	Actividad	Duración estimada	Descripción
Preparación	Configuración del entorno	1 día	<ul style="list-style-type: none">● Instalación de SO (Linux).● Configuración de red básica.● Actualización del sistema y dependencias necesarias.
Honeypot	Implementación	1 día	<ul style="list-style-type: none">● Configurar servicio SSH.● Implementar servicio FTP.● Crear servidor web falso para HTTP honeypot.
Red Interna	Configuración de servicios internos	1 día	<ul style="list-style-type: none">● Implementar un servidor web interno básico● Ajustar firewall para proteger la red interna.
Sistema IDS	Instalación y configuración	1 día	<ul style="list-style-type: none">● Configurar sistema de logs para monitorear tráfico en ambas subredes.● Crear reglas personalizadas.● Verificar registros y alertas.
Red atacante	Instalación de herramientas de prueba	1 día	<ul style="list-style-type: none">● Configurar máquinas con Nmap, Hydra, y las herramientas necesarias.● Preparar scripts de ataque para probar vulnerabilidades.
Pruebas	Validación de todos los componentes	1 día	<ul style="list-style-type: none">● Simular ataques desde la red atacante.● Revisar logs de honeypots para validar detecciones.
Documentación	Generar informes finales	1 día	<ul style="list-style-type: none">● Resumir configuraciones.● Presentar resultados de pruebas de seguridad.

Los servicios que fueron ofrecidos en el honeypot fueron:

- **HTTP (Protocolo de Transferencia de Hipertexto):** Es el protocolo que permite a los navegadores web comunicarse con los servidores para mostrar páginas web. En resumen, es la base de la web.
- **FTP (Protocolo de Transferencia de Archivos):** Sirve para transferir archivos entre un ordenador (cliente) y un servidor. Es decir, se usa para subir y bajar ficheros.
- **SSH (Shell Seguro):** Es un protocolo que permite acceder y controlar de forma remota otro ordenador de manera segura. Es como una línea de comandos remota pero con cifrado para proteger la comunicación.

Configuración

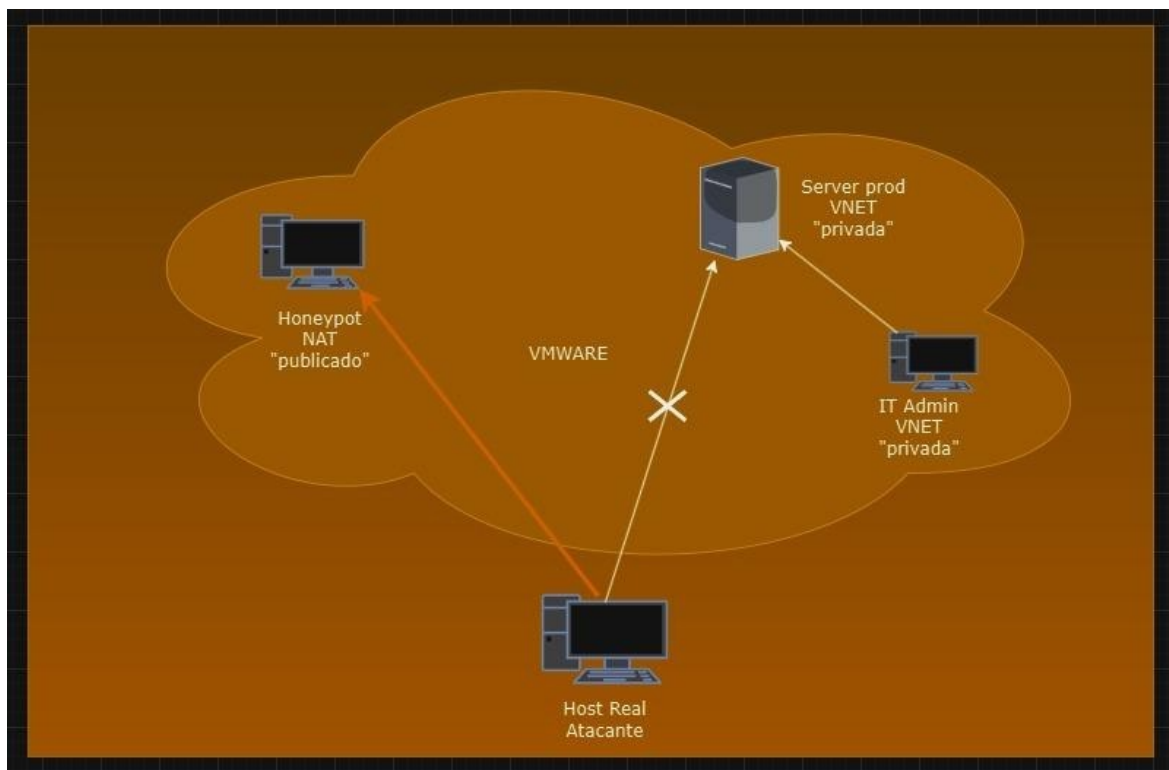
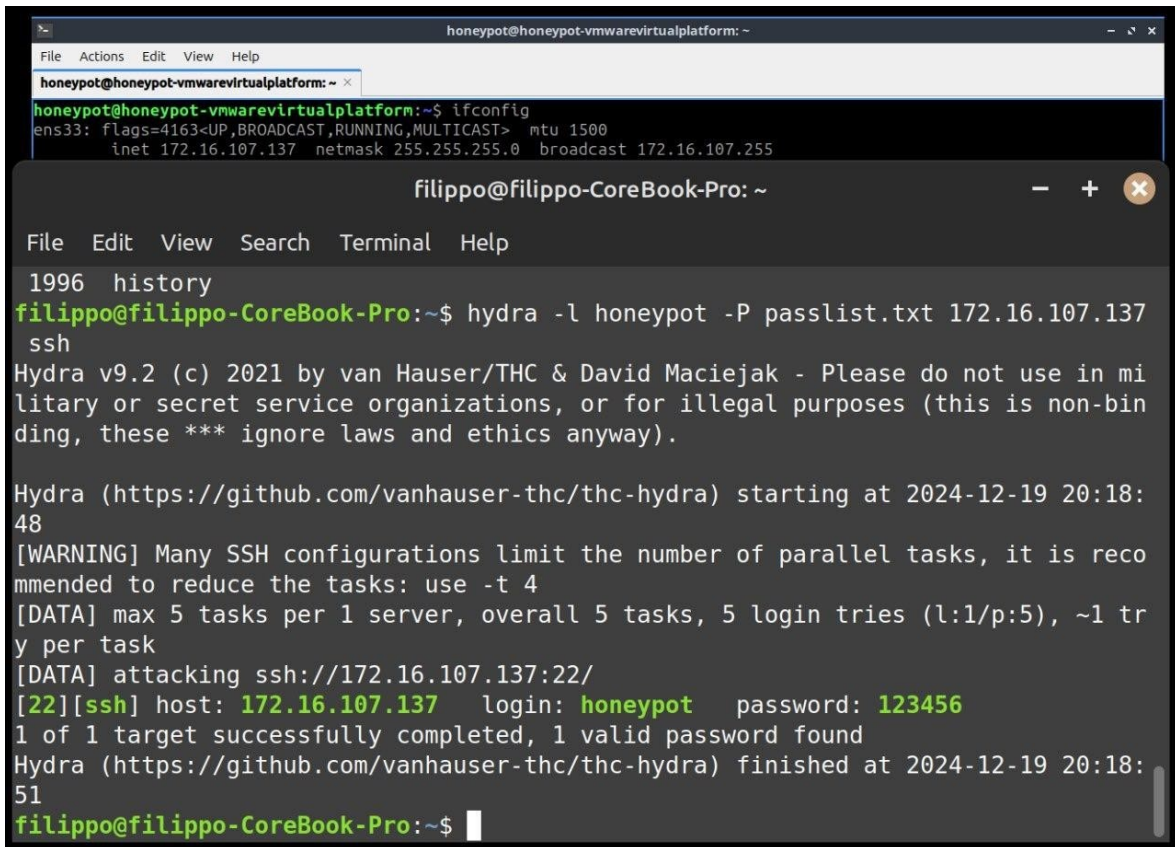


Imagen propia: Topología del ZFA Honeypot

Se puede apreciar que existen dos segmentos de red privados, el honeypot es público, es decir, con los servicios expuestos para que el atacante tenga acceso a ellos, pero, el atacante de ninguna manera puede acceder al server que a su vez si permite la conexión con IT Admin.

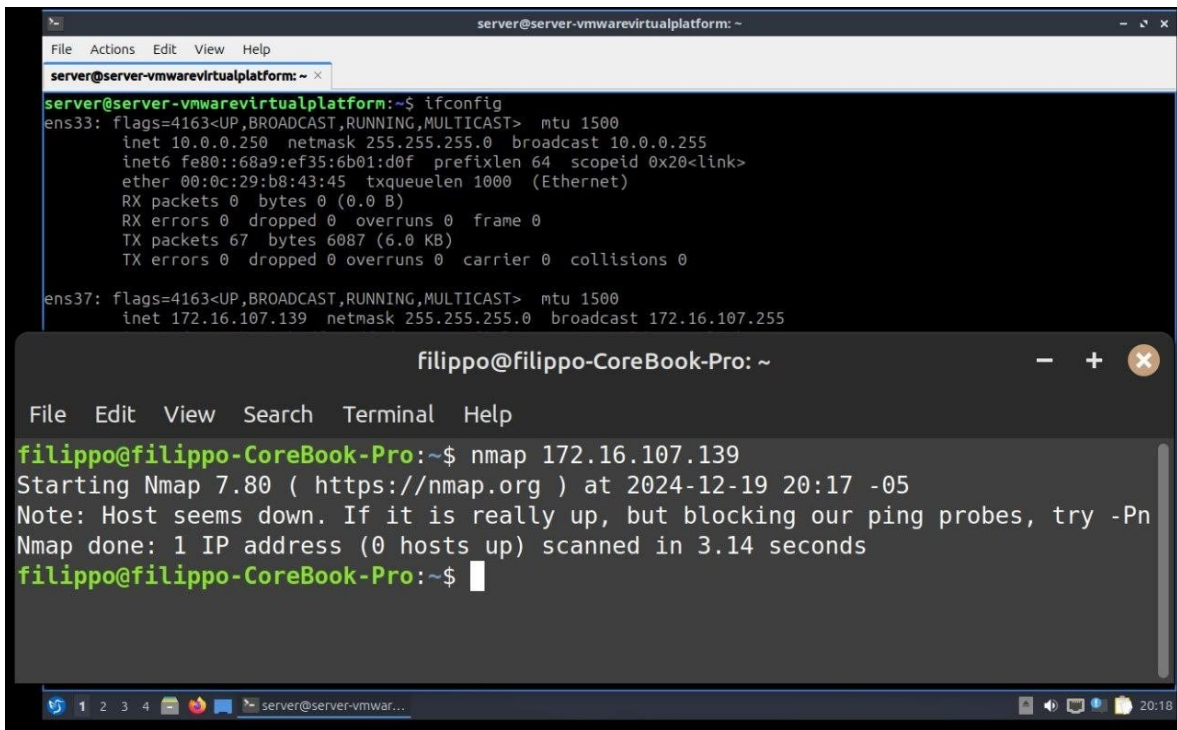
Resultados



The image shows two overlapping terminal windows. The top window, titled 'honeypot@honeypot-vmwarevirtualplatform: ~', displays the output of the 'ifconfig' command for the 'ens33' interface, showing an IP address of 172.16.107.137. The bottom window, titled 'filippo@filippo-CoreBook-Pro: ~', shows a terminal session where the user runs 'history' and then a Hydra brute-force attack on an SSH service at 172.16.107.137 using a password list. The attack is successful, finding the password '123456'.

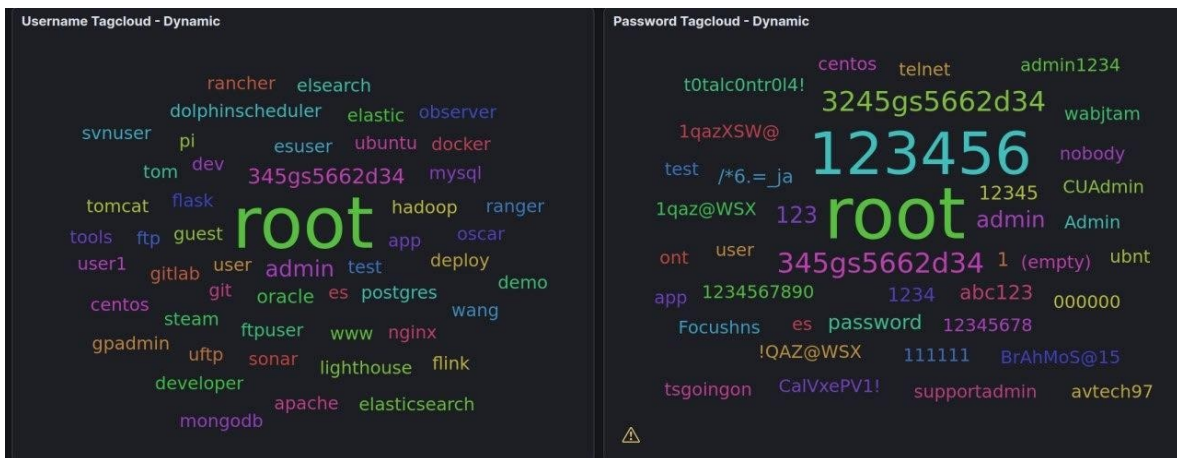
```
honeypot@honeypot-vmwarevirtualplatform: ~  
File Actions Edit View Help  
honeypot@honeypot-vmwarevirtualplatform: ~  
honeypot@honeypot-vmwarevirtualplatform:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 172.16.107.137 netmask 255.255.255.0 broadcast 172.16.107.255  
  
filippo@filippo-CoreBook-Pro: ~  
File Edit View Search Terminal Help  
1996 history  
filippo@filippo-CoreBook-Pro:~$ hydra -l honeypot -P passlist.txt 172.16.107.137  
ssh  
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi  
litary or secret service organizations, or for illegal purposes (this is non-bin  
ding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-19 20:18:  
48  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco  
mmended to reduce the tasks: use -t 4  
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 tr  
y per task  
[DATA] attacking ssh://172.16.107.137:22/  
[22][ssh] host: 172.16.107.137 login: honeypot password: 123456  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-19 20:18:  
51  
filippo@filippo-CoreBook-Pro:~$
```

Fuente propia: Ataque de fuerza bruta para descubrir contraseña del SSH.



```
server@server-vmwarevirtualplatform: ~  
File Actions Edit View Help  
server@server-vmwarevirtualplatform: ~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.0.250 netmask 255.255.255.0 broadcast 10.0.0.255  
    inet6 fe80::68a9:ef35:6b01:d0f prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:b8:43:45 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 67 bytes 6087 (6.0 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.16.107.139 netmask 255.255.255.0 broadcast 172.16.107.255  
  
filippo@filippo-CoreBook-Pro: ~  
File Edit View Search Terminal Help  
filippo@filippo-CoreBook-Pro:~$ nmap 172.16.107.139  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-19 20:17 -05  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.14 seconds  
filippo@filippo-CoreBook-Pro:~$
```

Fuente propia: Máquina atacante no llega al servidor real de la empresa (host seems down)



Fuente propia: Visualización con los usuarios y las contraseñas más usadas para vulnerar el servicio SSH.

Attacker AS/N - Top 10 - Dynamic			Src IP - Top 10 - Dynamic		Cowrie Input - Top 10	
AS	ASN	Count	Source IP	Count	Command Line Input	Count
3462	Data Communic	38,632	183.91.160.89	1,854	shell	3,534
14061	DIGITALOCEAN	3,746	117.50.213.252	1,723	system	3,534
4134	Chinanet	3,358	116.193.222.195	1,281	enable	1,767
210644	Aeza Internatio	2,658	103.100.159.215	1,252	sh	1,767
138968	rainbow networ	2,489	47.239.233.10	1,249	ping ;sh	1,754
8075	MICROSOFT-CO	2,487	123.205.121.86	1,248	/bin/busybox wget --he	1,666
131127	GLOBAL TECHN	1,854	103.119.3.35	1,246	cat /proc/mounts grep	1,666
4808	China Unicom B	1,836	134.209.31.107	1,246	cat /proc/mounts grep	1,666
136052	PT Cloud Hostir	1,714	20.127.141.235	1,246	echo -e \x67\x61\x79\x	1,666
16276	OVH SAS	1,593	45.150.32.168	1,246	for i in	1,666

Fuente propia: Direcciones IP y proveedores de internet de los ciberdelincuentes, y comandos más utilizados una vez vulnerada la máquina.

Conclusiones

Es innegable que la ciberseguridad es uno de los campos que más desarrollo sigue teniendo y va a la par en que se siguen desarrollando las demás tecnologías. Día tras día los ataques informáticos se incrementan de manera dramática y es menester implementar y actualizar los sistemas de prevención, detección y respuesta.

Los honeypots marcan una tendencia y una herramienta eficiente para mejorar la ciberseguridad en muchas organizaciones. Dado que con estos, se estudia principalmente el comportamiento de los ciberdelincuentes y por ende, se toman las medidas adecuadas y ajustadas a los comportamientos que se observan. Blindando los sistemas o servicios reales que posee una organización para que no existan detenciones, errores y fugas abruptas ocasionadas por ciberdelincuencia que ponga en vilo la continuidad del negocio.

Referencias

Abiodun Raufu, Lucy Tsado, Emmanuel Ben-Edet. International Journal of Law, Crime and Justice, Volume 64, 2021, 100454, ISSN 1756-0616, <https://doi.org/10.1016/j.ijlcrj.2020.100454>.
(<https://www.sciencedirect.com/science/article/pii/S1756061620304894>)

Amir Javadpour, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, Chafika Benzaïd. A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security, Volume 140, 2024, 103792, ISSN

0167-4048.<https://doi.org/10.1016/j.cose.2024.103792>.
(<https://www.sciencedirect.com/science/article/pii/S0167404824000932>)

Niclas Ilg, Paul Duplys, Dominik Sisejkovic, Michael Menth. A survey of contemporary open-source honeypots, frameworks, and tools. Journal of Network and Computer Applications, Volume 220, 2023, 103737, ISSN 1084-8045. <https://doi.org/10.1016/j.jnca.2023.103737>.
(<https://www.sciencedirect.com/science/article/pii/S108480452300156X>)