

¡Atrapando a Hackers con T-POT! Explorando un Honeypot en Ciberseguridad



Por:
Muriel Jaramillo
Gilberto Ramos



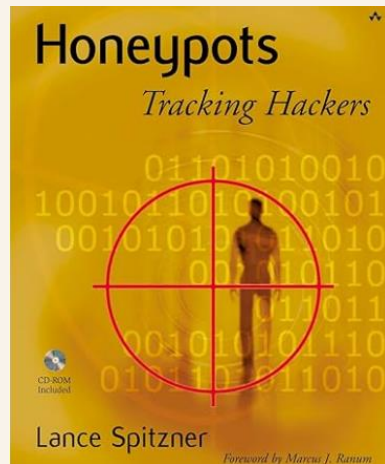
Lic. En Ciberseguridad



ANTECEDENTES

Los honeypots tienen una historia única. A pesar de que los conceptos han existido durante más de una década, solo recientemente se han desarrollado productos comerciales o se han publicado artículos sobre el concepto.

- 1990/1991— Primeras obras públicas que documentan conceptos de honeypot: The Cuckoo's Egg de Clifford Stoll.
- En 1999 un grupo de personas lideradas por Lance Spitzner fundaron “Honeynet Project”, grupo sin fines de lucro dedicado a investigar la comunidad blackhat y compartir los resultados de sus investigaciones con otros.



¿QUÉ ES UN HONEYPOT Y T-POT?

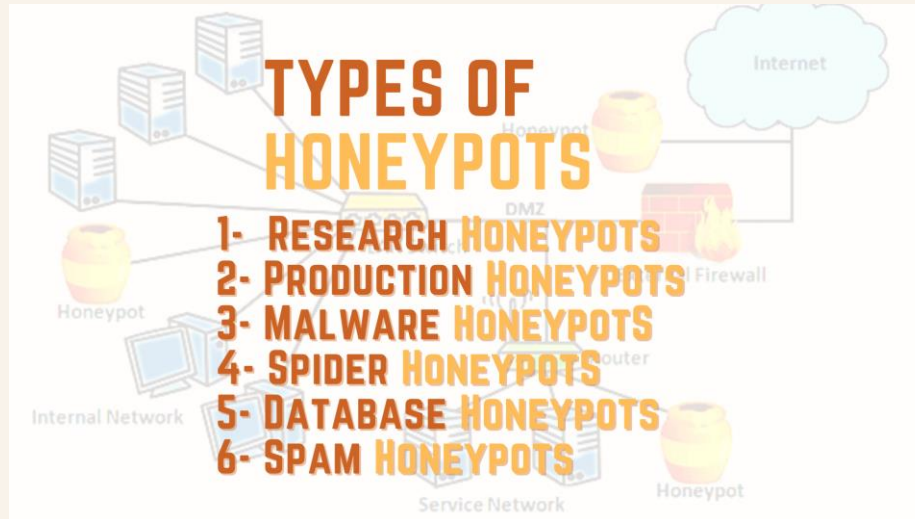


- ❖ En ciberseguridad, el significado de honeypot se refiere a una red diseñada intencionalmente para ser comprometida con la esperanza de atraer Ciberdelincuentes para que revelen sus métodos. Este enfoque ayuda a identificar amenazas potenciales y a obtener información sobre las tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes.
- ❖ T-pot es una plataforma de honeypot de código abierto que combina más de 20 honeypots diferentes en un solo paquete. Es una herramienta poderosa que le permite implementar y administrar varios honeypots a la vez. Con T-Pot, puede probar diferentes configuraciones de honeypot y luego ajustarlas según las necesidades de su entorno.



¿PARA QUÉ SIRVE UN HONEYPOT?

Los honeypots son utilizados principalmente por los investigadores para comprender mejor las vulnerabilidades de seguridad en las redes y como señuelos para las empresas que buscan proteger sus activos.

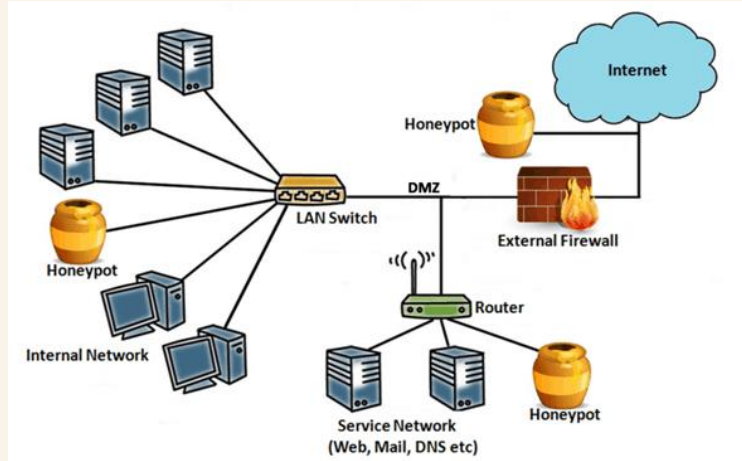


PROS Y CONTRAS DE USAR UN HONEYPOT

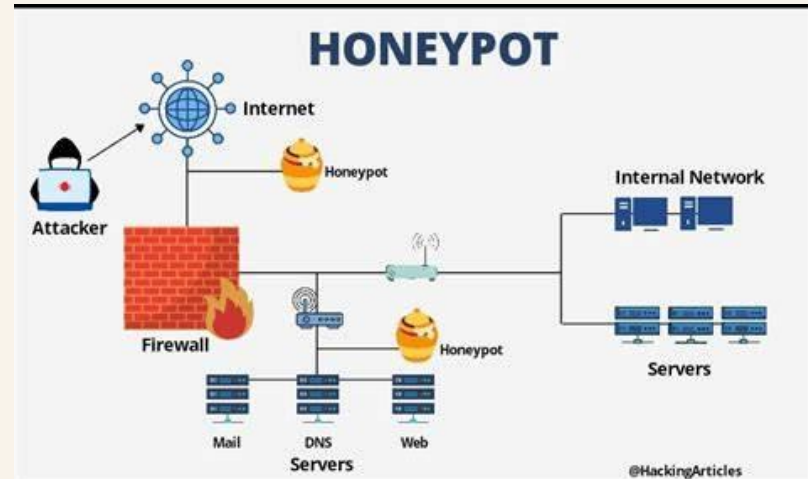
1	Recopilación de datos reales
2	Evitar ataques futuros
3	Tienen una baja tasa de falsos positivos
4	Evolución continua
5	Identificación de amenazas internas y externas

1	El atacante al identificar las huellas digitales de un honeypot, puede crear ataques falsos
2	Puede ser utilizado para atacar otros sistemas
3	Requiere recursos y tiempo

UBICACIÓN DE UN HONEYPOT

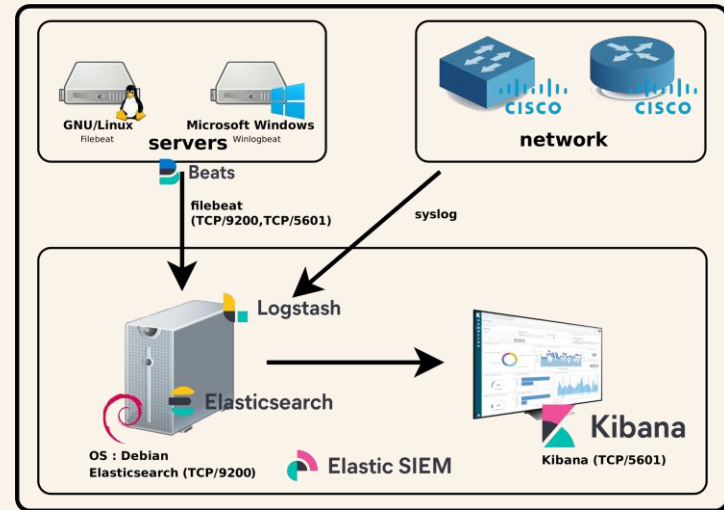


- Antes del Firewall
- Detrás del Firewall
- En la DMZ



Rol del SIEM, Honeypot y Elastic para Optimizar un SOC

- ❖ SIEM: Procesa eventos en tiempo real, genera alertas y detecta anomalías en la red Honeypot: Simula sistemas vulnerables para captar ataques y recopilar inteligencia.
- ❖ Elastic Stack(ELK): Elasticsearch, Logstash y Kibana proporcionan un análisis visual y en profundidad de los datos.
- ❖ Los datos del honeypot en el SIEM, enriquecidos y visualizados en Elastic, ayudan al SOC a responder a amenazas emergentes y adaptar defensas.



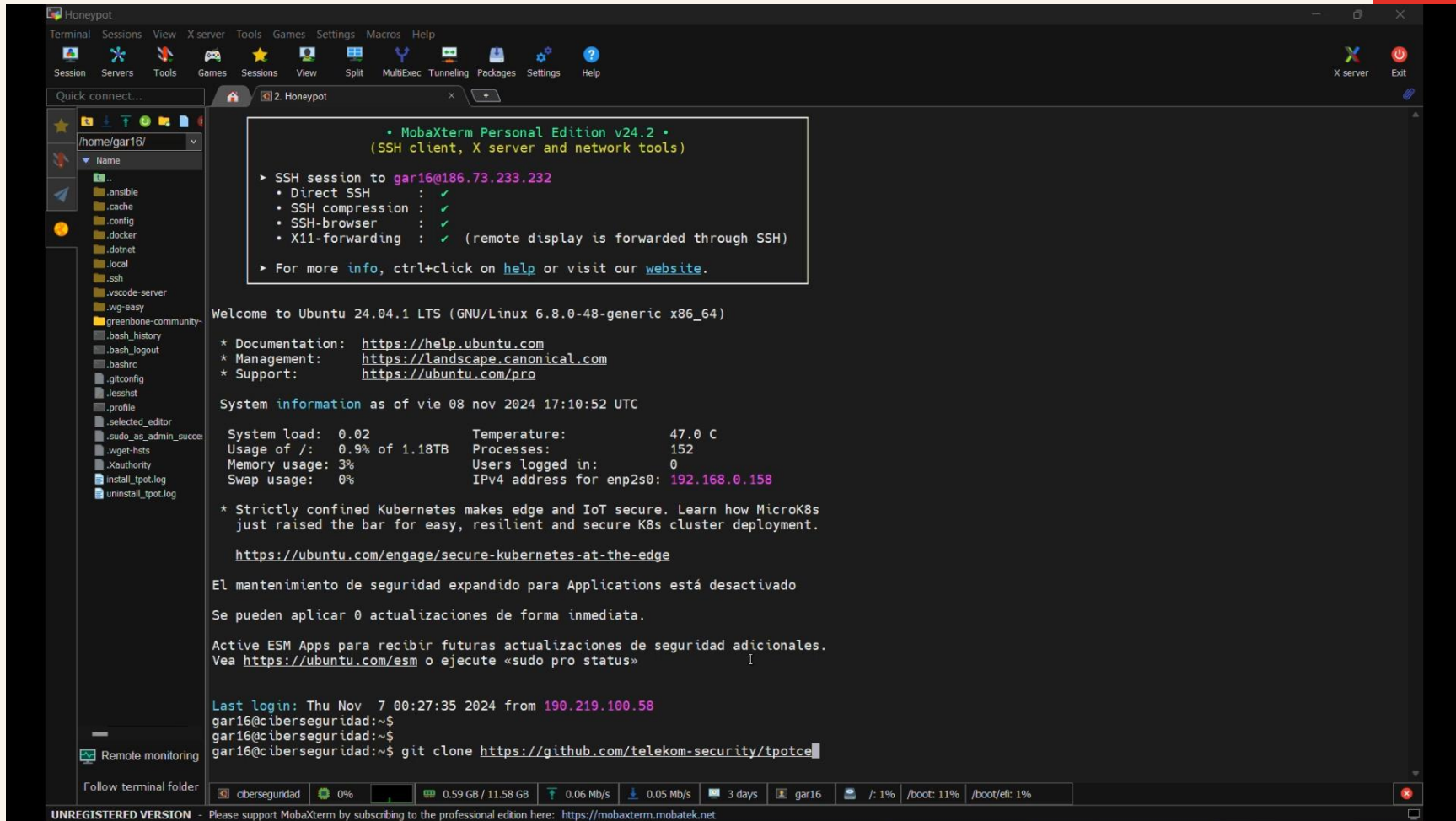
REQUISITOS DEL SISTEMA

Características técnicas

- 4 núcleos de CPU
- 8 a 16 GB de RAM
- Disco de 160 GB
- Sistema operativo Linux (debian, ubuntu, fedora, etc)
- Hardware físico, máquina virtual o en la nube



VIDEO DE INSTALACIÓN DE T-POT



The screenshot shows the MobaXterm Personal Edition v24.2 interface. The terminal window displays the following content:

```
• MobaXterm Personal Edition v24.2 •
(SSH client, X server and network tools)

> SSH session to gar16@186.73.233.232
  • Direct SSH : ✓
  • SSH compression : ✓
  • SSH-browser : ✓
  • X11-forwarding : ✓ (remote display is forwarded through SSH)

> For more info, ctrl+click on help or visit our website.
```

Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-48-generic x86_64)

* Documentation: <https://help.ubuntu.com>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/pro>

System information as of vie 08 nov 2024 17:10:52 UTC

System load: 0.02	Temperature: 47.0 C
Usage of /: 0.9% of 1.18TB	Processes: 152
Memory usage: 3%	Users logged in: 0
Swap usage: 0%	IPv4 address for enp2s0: 192.168.0.158

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

<https://ubuntu.com/engage/secure-kubernetes-at-the-edge>

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea <https://ubuntu.com/esm> o ejecute «sudo pro status»

Last login: Thu Nov 7 00:27:35 2024 from 190.219.100.58
gar16@ciberseguridad:~\$
gar16@ciberseguridad:~\$
gar16@ciberseguridad:~\$ git clone https://github.com/telekom-security/tpotce

The bottom status bar shows system metrics: 0.59 GB / 11.58 GB, 0.06 Mb/s, 0.05 Mb/s, 3 days, gar16, /: 1%, /boot: 11%, /boot/efi: 1%.

MANEJO DEL HONEYPOT

¡Muestra, no cuentes... Hagámoslo!



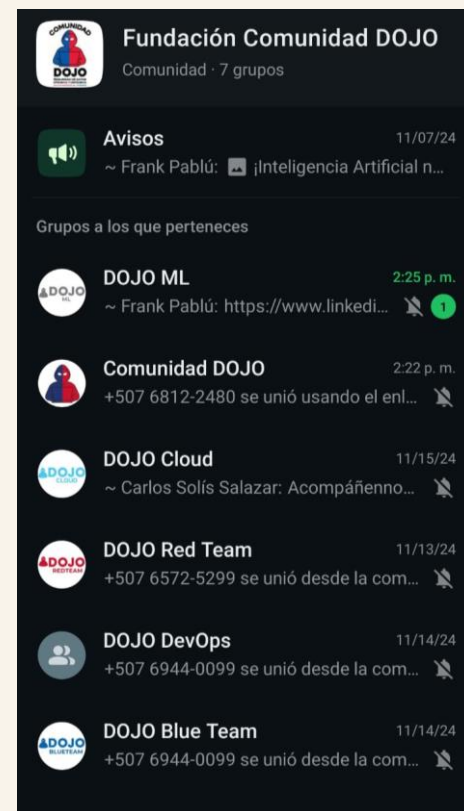
Honeypot For Dummies



@cybertechseries



COMUNIDADES





WEBGRAFÍA

<https://www.youtube.com/watch?v=SgH9rWB9ivQ&t=57s>

<https://www.youtube.com/watch?v=Xj3SaJjEjyk&t=624s>

<https://www.youtube.com/watch?v=QxUCU4IIOKI>

<https://www.redeszone.net/tutoriales/seguridad/que-es-honeypot/>

<https://es.wikipedia.org/wiki/Honeypot>

<https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>

<https://us.norton.com/blog/iot/what-is-a-honeypot>

<https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/>

<https://www.geeksforgeeks.org/what-is-honeypot/>

<https://medium.com/@abbasiharoon/setting-up-t-pot-a-practical-guide-to-deploying-honeypots-and-trapping-attackers-32b9cba7a16f>

<https://infosecwriteups.com/honeypots-104-t-pot-your-all-in-one-honeypot-platform-guide-0ba2643bc597>

[las 11 mejores herramientas SIEM para proteger a su organización de los ciberataques](#)

[La historia de los honeypots - Honeypots: Rastreando a los hackers \[Libro\]](#)

[Definición e historia de los Honeypots - ANÁLISIS CONCEPTUAL](#)

[LevelBlue - Open Threat Exchange](#)

<https://es.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/>

¡MUCHAS GRACIAS!

Preguntas || Dudas

