HONEYPOT

ciberseguridad Cohorte 1

BeTek

03

PROBLEMA IDENTIFICADO

La falta de visibilidad y alerta temprana sobre los posibles ataques a la red.

- EL 20% de las redes comprometidas permanecen sin detectar por mas de un mes (Fuente: FireEye M-Trends Report).

Dificultad para identificar técnicas y orígenes de ataques.

- Los ataques cibernéticos se originan principalmente en países como Estados Unidos (10%), Turquía (4.7%) y Rusia (4.3%), lo que complica la atribución geográfica.

problema

04

PROBLEMA IDENTIFICADO

Incremento de ciberataques

- En el primer trimestre de 2024, las organizaciones experimentaron un promedio de 1,308 ataques cibernéticos por semana, lo que representa un incremento del 28% respecto al último trimestre de 2023 y un 5% más que el año anterior.

Complejidad de las técnicas de ataque

- Los atacantes emplean técnicas avanzadas como ransomware, phishing e ingeniería social, dificultando la detección.

problema

SOLUCIÓN PROPUESTA

Implementar honeypots dentro de la red organizacional con el objetivo de:

Detectar actividades sospechosas y ataques.

Identificar técnicas y procedencia de los atacantes.

Generar alertas tempranas que permitan actuar antes de que la amenaza impacte sistemas críticos

Capturar y registrar comportamientos maliciosos para análisis posterior.

solucion

COMO SE RESUELVE EL PROBLEMA

Lanzamiento del honeypot

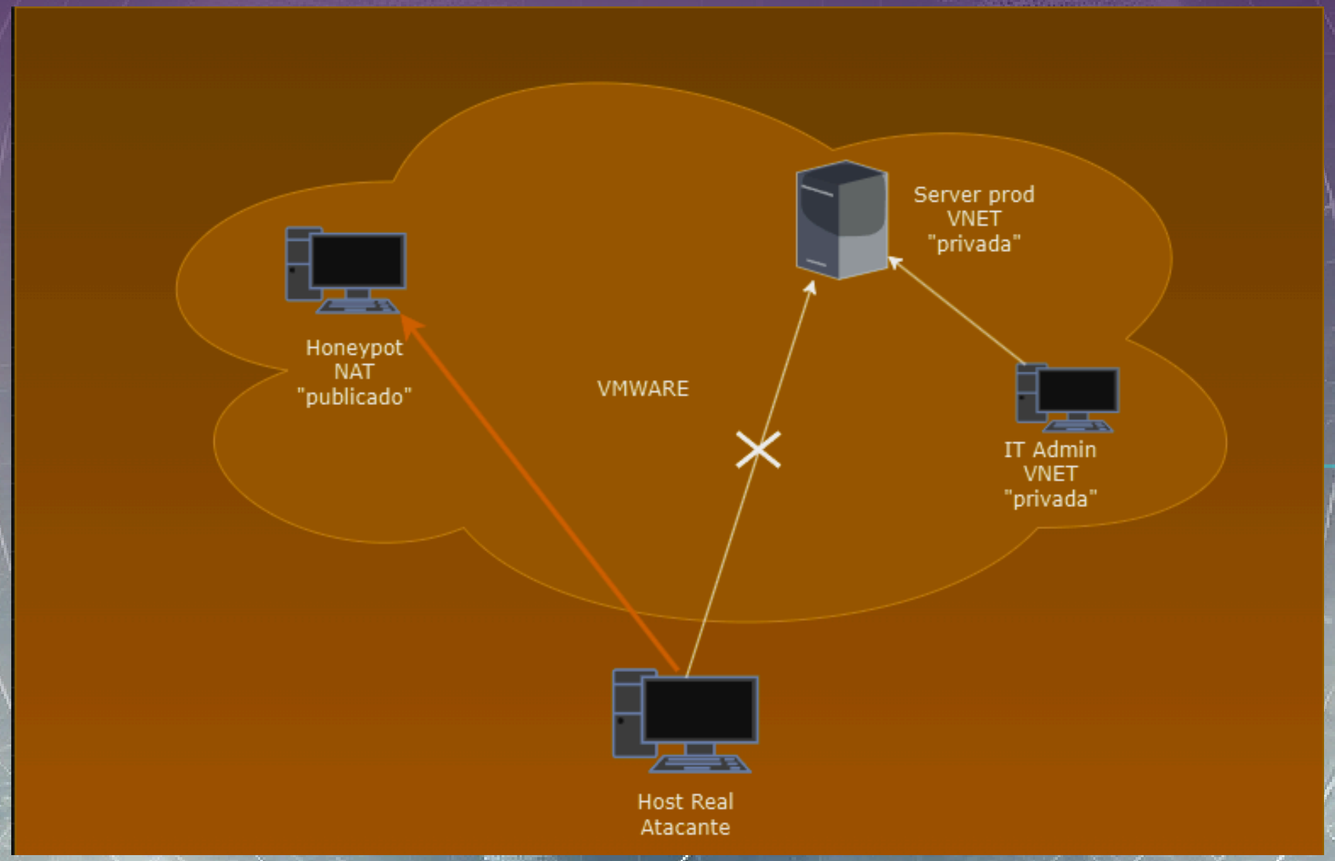
Analisis de registros

Análisis de comportamiento del atacante

Ajustes del sistema

implementación

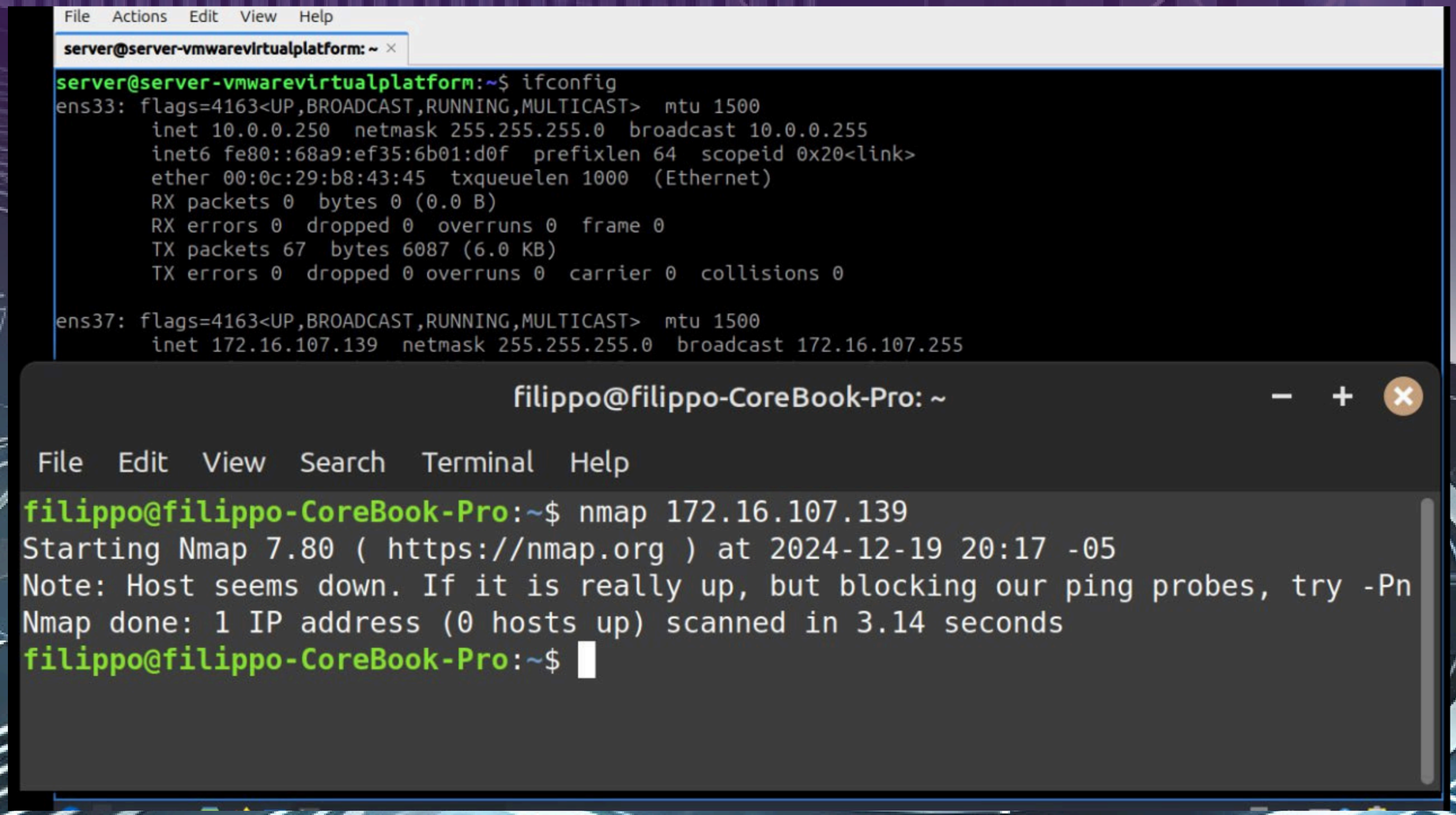
TOPOLOGÍA



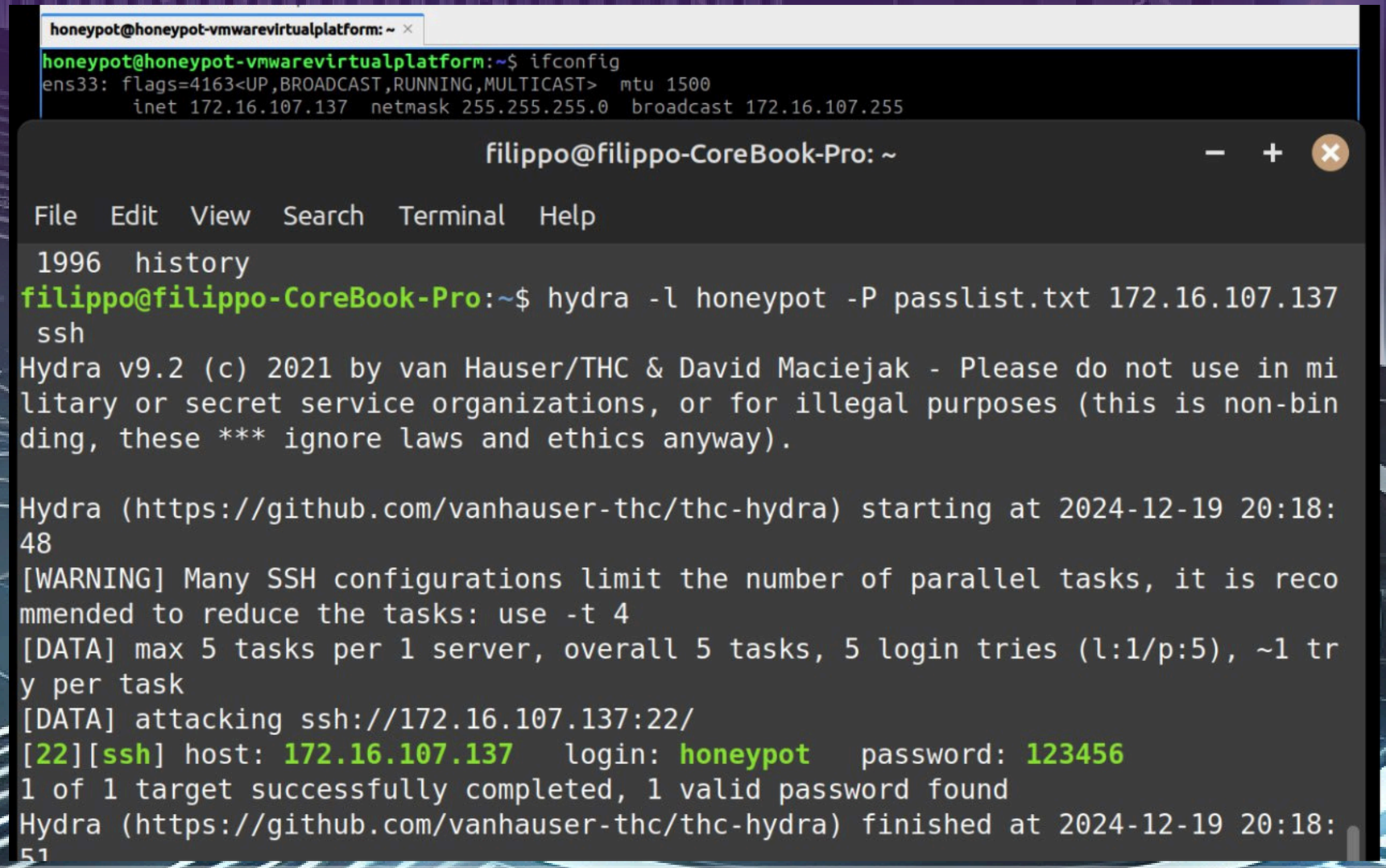
topología

RESULTADOS

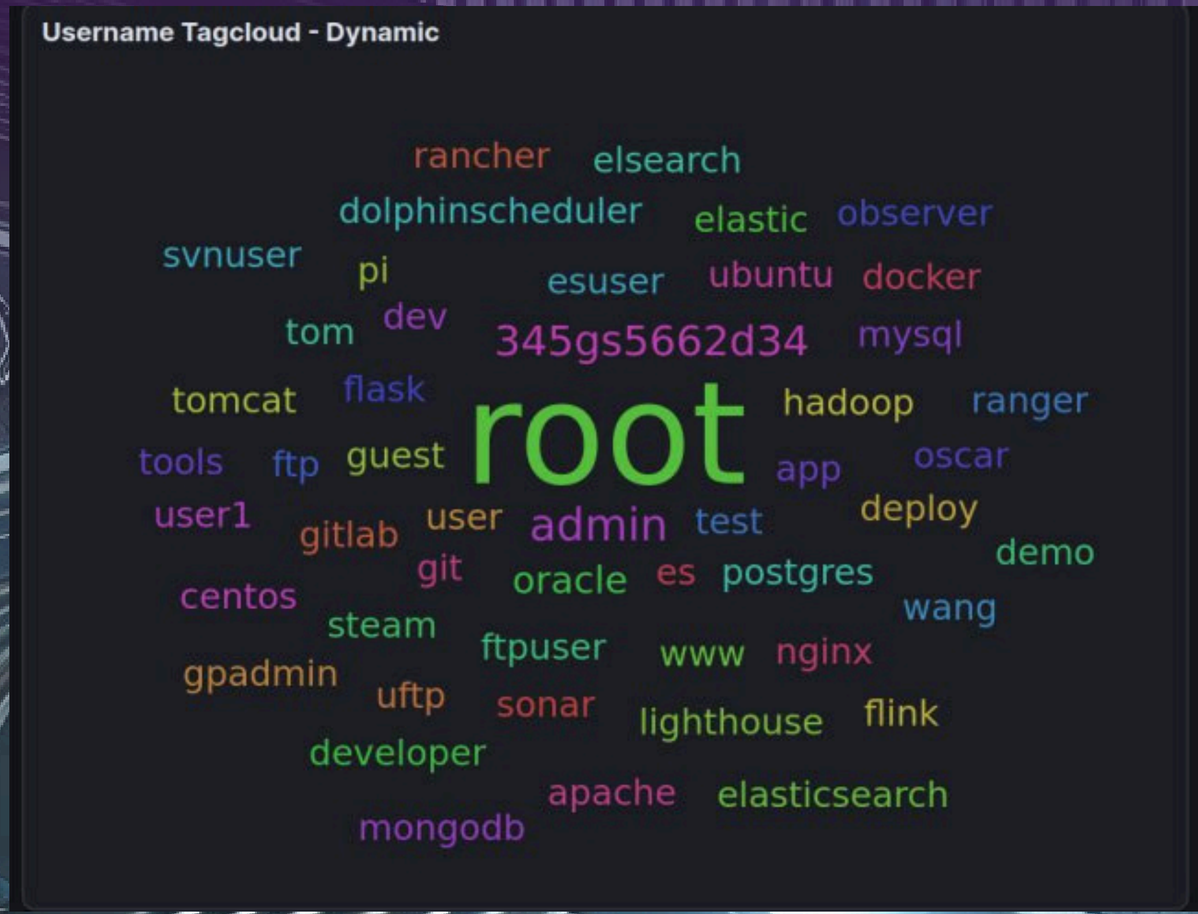
07

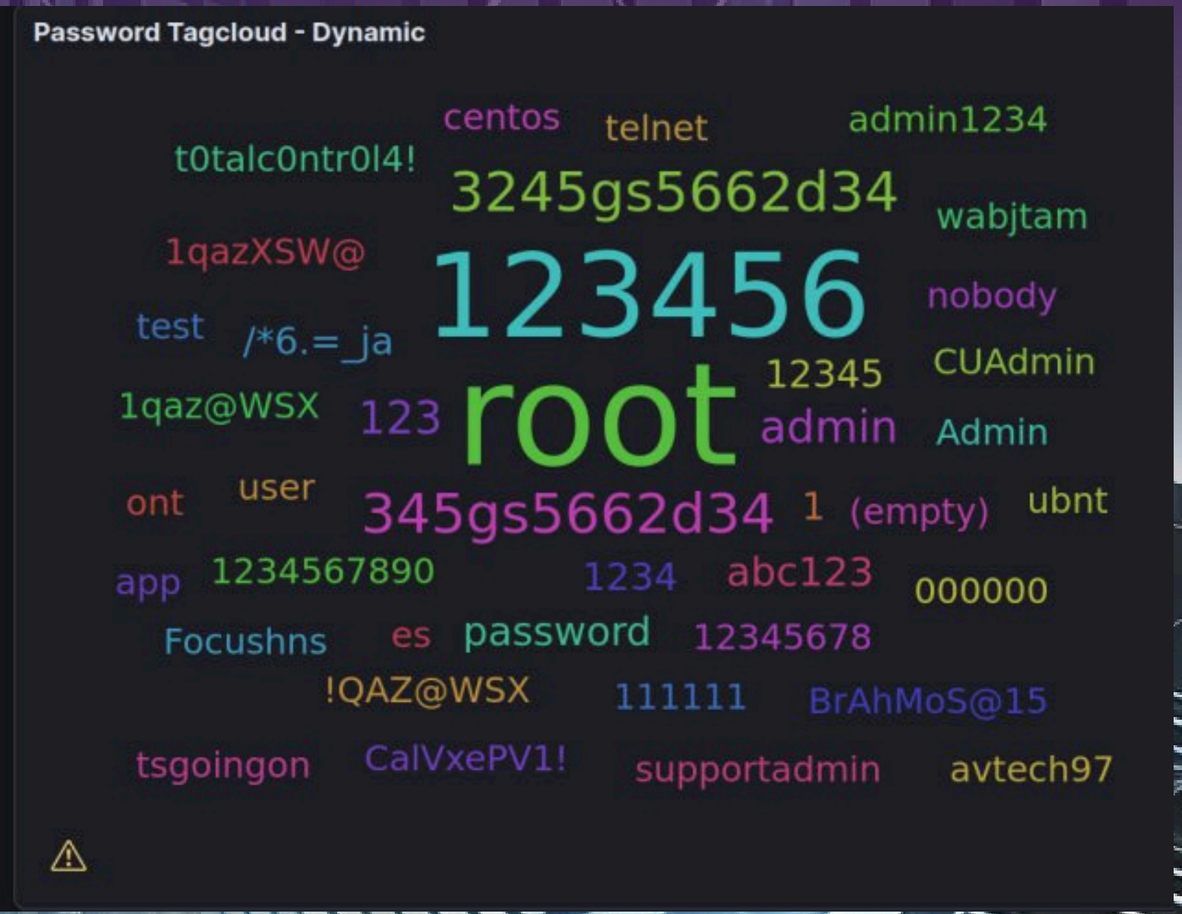


RESULTADOS


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 military or secret service organizations, or for illegal purposes (this is non-binding, 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 recommended 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 try 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

RESULTADOS


Username Tagcloud - Dynamic
rancher
elsearch
dolphinscheduler
elastic
observer
svnuser
pi
esuser
ubuntu
docker
tom
dev
345gs5662d34
mysql
tomcat
flask
root
hadoop
ranger
tools
ftp
guest
app
oscar
user1
gitlab
user
admin
test
deploy
demo
git
oracle
es
postgres
centos
wang
steam
ftpuser
www
nginx
gpadmin
uftp
sonar
lighthouse
flink
developer
apache
elasticsearch
mongodb


Password Tagcloud - Dynamic
centos
telnet
admin1234
t0talc0ntr0l4!
3245gs5662d34
wabjtam
1qazXSW@
123456
nobody
test
/*6.=_ja
12345
CUAdmin
1qaz@WSX
123
root
admin
Admin
ont
user
345gs5662d34
1
(empty)
ubnt
app
1234567890
1234
abc123
000000
Focushns
es
password
12345678
!QAZ@WSX
111111
BrAhMoS@15
tsgoingon
CalVxePV1!
supportadmin
avtech97

RESULTADOS

Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
3462	Data Communic	38,632
14061	DIGITALOCEAN	3,746
4134	Chinanet	3,358
210644	Aeza Internatio	2,658
138968	rainbow networ	2,489
8075	MICROSOFT-C(	2,487
131127	GLOBAL TECHN	1,854
4808	China Unicom B	1,836
136052	PT Cloud Hostir	1,714
16276	OVH SAS	1,593

Src IP - Top 10 - Dynamic

Source IP	Count
183.91.160.89	1,854
117.50.213.252	1,723
116.193.222.195	1,281
103.100.159.215	1,252
47.239.233.10	1,249
123.205.121.86	1,248
103.119.3.35	1,246
134.209.31.107	1,246
20.127.141.235	1,246
45.150.32.168	1,246

Cowrie Input - Top 10

Command Line Input	Count
shell	3,534
system	3,534
enable	1,767
sh	1,767
ping ;sh	1,754
/bin/busybox wget --he	1,666
cat /proc/mounts | grep	1,666
cat /proc/mounts | grep	1,666
echo -e \x67\x61\x79\x	1,666
for i in	1,666

CONCLUSION

- Un honeypot no solo mejora la detección de amenazas y la recolección de información crítica, sino que también facilita la toma de decisiones para fortalecer la seguridad de la red, reduciendo riesgos y tiempos de respuesta ante incidentes.
-

conclusión

¡ GRACIAS !

"Si quieres protegerte, primero debes entender cómo piensa el lobo."

BeTek