



Introduction To HoneyPots

A guided room covering the deployment of honeypots and analysis of botnet activities

<https://tryhackme.com/room/introductiontohoneypots>

~

Task 3 Cowrie Demo

Create a file and then log back in is the file still there? (Yay/Nay)

Nay

Task 5 Attacks Against SSH

How many passwords include the word "password" or some other variation of it e.g "p@ssw0rd"

```
grep 'p.*ss' Top200Creds.txt | wc -l
```

```
demo@acmeweb:~$ ls
BotCommands Top200Creds.txt Tunneling
demo@acmeweb:~$ grep 'p.*ss' Top200Creds.txt
/admin/password/
/root/password1/
/root/password/
/user1/password/
/MikroTik/password/
/default/password/
/admin1/password/
/profile1/password/
/user/password/
/admin/password/
/admin1/password/
/user1/password/
/profile1/password/
/MikroTik/password/
/default/password/
demo@acmeweb:~$ grep 'p.*ss' Top200Creds.txt | wc -l
15
demo@acmeweb:~$
```

What is arguably the most common tool for brute-forcing SSH?

hydra

What intrusion prevention software framework is commonly used to mitigate SSH brute-force attacks?

fail2ban

Task 6 Typical Bot Activity

What CPU does the honeypot "use"?

cat /proc/cpuinfo will result Intel(R) Core(TM) i9-11900KB CPU @ 3.30GHz

Does the honeypot return the correct values when uname -a is run? (Yay/Nay)

Nay

What flag must be set to pipe wget output into bash?

-o

How would you disable bash history using unset?

unset HISTFILE

Task 7 Identification Techniques

What brand of device is the bot in the first sample searching for?
(BotCommands/Sample1.txt)

MikroTik

dev/ttyGSM* /dev/ttyUSB-mod* /var/spool/sms/*

×



All

Videos

Images

News

Maps

More

Tools

About 18,800 results (0.88 seconds)

https://www.malwaremily.com > 011-microtik

A Botnet's Search for MikroTik Routers | malwaremily

/ip cloud print ifconfig uname -a cat /proc/cpuinfo ps | grep '[Mm]iner' ps -ef | grep '[Mm]iner' ls -la /dev/ttyGSM* /dev/ttyUSB-mod* /var/spool/sms/* ...

What are the commands in the second sample changing? (BotCommands/Sample2.txt)

root password

What is the name of the group that runs the botnet in the third sample? (BotCommands/Sample3.txt)

outlaw

```
free -m | grep Mem | awk '{print $2, $3, $4, $5, $6, $7}' botnet
```

```
default ... free -m | grep Mem | awk '{print $2, $3, $4, $5, $6, $7}'.
```

<https://malware.news> > outlaw-updates-kit-to-kill-older-... ⋮

[Outlaw Updates Kit to Kill Older Miner Versions, Targets More ...](#)

Feb 10, 2020 — ... free -m | grep Mem | awk '{print \$2, \$3, \$4, \$5, \$6, \$7}' ls -lh \$(which ls)
which ls crontab -l w uname -m cat /proc/cpuinfo | grep ...

<https://www.trendmicro.com> > fr_fr > research > outlaw... ⋮

[Outlaw Updates: Kill Old Miner Versions, Target More - Trend ...](#)

Feb 10, 2020 — ... free -m | grep Mem | awk '{print \$2, \$3, \$4, \$5, \$6, \$7}' ls -lh \$(which ls)
which ls crontab -l w uname -m cat /proc/cpuinfo | grep ...

Task 8 SSH Tunnelling

What application is being targetted in the first sample? (Tunnelling/Sample1.txt)

```
demo@acmeweb:~/Tunnelling$ cat Sample1.txt
2021-03-17T10:09:51.052837Z [SSHChannel cowrie-discarded-direct-
on' on HoneyPotSSHTransport,118939,0.0.0.0] discarded direct-t
th data b'POST /xmlrpc.php HTTP/1.1\r\nAccept: text/html,appli
age/webp,image/apng,*/*;q=0.8\r\nAccept-Encoding: gzip, deflat
onnection: keep-alive\r\nContent-Length: 201\r\nContent-Type:
: <A DOMAIN>\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mo
pleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.109 Safa
ding="UTF-8"?><methodCall><methodName>wp.getUsersBlogs</methoc
```

Wordpress

Is the URL in the second sample malicious? (Tunnelling/Sample2.txt) (Yay/Nay)

Nay