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
```

```
e<sup>3</sup>SH<sup>S</sup>This means adversaries will only be able to c
BotCommands Top200Creds.txt Tunnelling
demonacheweb:~$ grep tp. *ss o Top200Creds txthe service
/admin/sassword/ can be defeated by only allowing public-key au
/root/presword1/ly so many of them that you are pretty much gu
           word/
/user1/
             word/
MikroTik/mmword/dentials used against old Cowrie deploymen
default/www.word/f the passwords are extremely weak. Notable
 ′admin1/
              word/
                      /arious combinations of '1234' and rows of
/user/
           word/
/admin/
           ∰w0rd/
/admin1/
              w0rd/
/user1/pastsw0rd/d "password" or some other variation of it e.g
                w0rd/
/MikroTik/
                w0rd/
/default/
               w0rd/
demonacmeweb:~$ grep 'p.*ss' Top200Creds.txt | wc -l
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?

-0

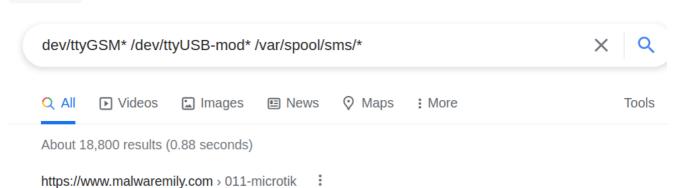
How would you disable bash history using unset?

unset HISTFILE

Task 7 Identification Techniques

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

MikroTik



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

C

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)

in a company c

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-1 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: Mc pleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.109 Safading="UTF-8"?><methodCall><methodName>wp.getUsersBlogs</method</pre>

Wordpress

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

Nay