EX NO : 9 DEPLOYMENT OF HONEYPOTS AND ANALYSIS OF BOTNET ACTIVITIES ROLL

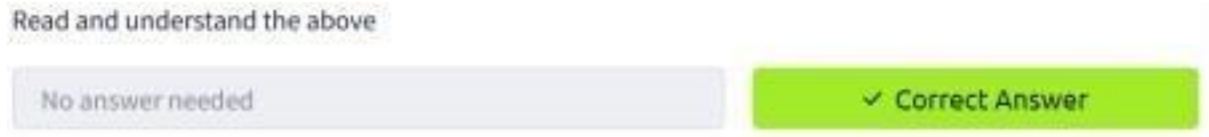
Date:13-4-25 **231901016**

Jose Mugilan D

AIM:

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

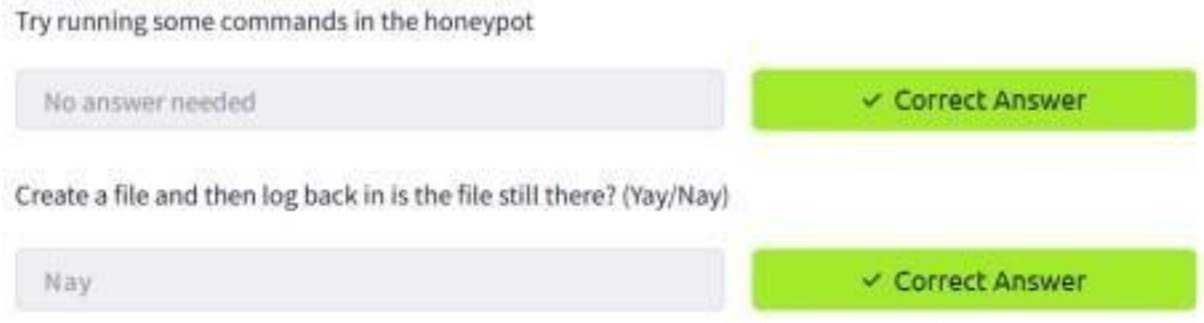
TASK 2 : TYPES OF HONEYPOTS



Read and understand the above

No answer needed

TASK 3 : COWRIE DEMO



Try running some commands in the honeypot

No answer needed

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

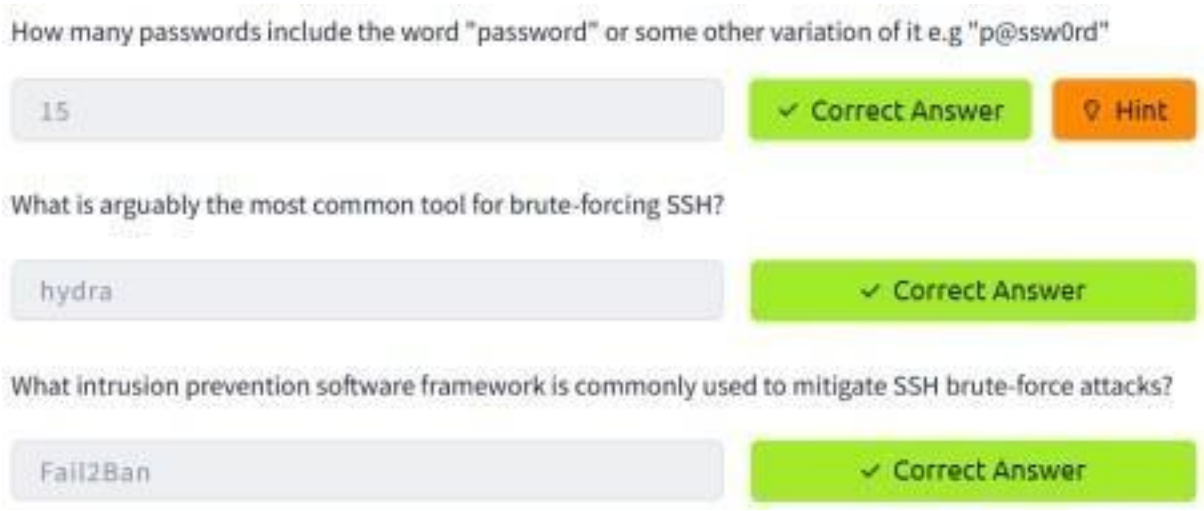
Nay

TASK 4 : COWRIE LOGS

Have a look through the logs and see how the activity from the last task has been recorded by the system.

No answer needed

TASK 5 : ATTACKS AGAINST SSH



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

15

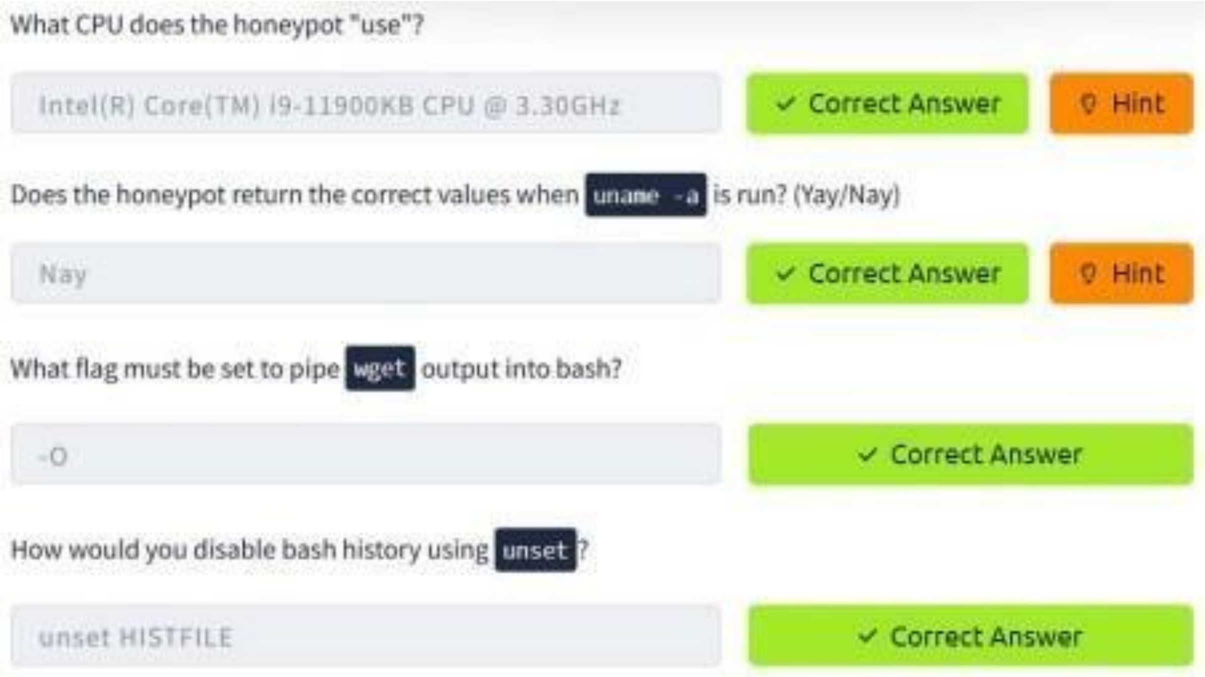
What is arguably the most common tool for brute-forcing SSH?

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"?

Intel(R) Core(TM) i9-11900KB CPU @ 3.30GHz

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

Nay

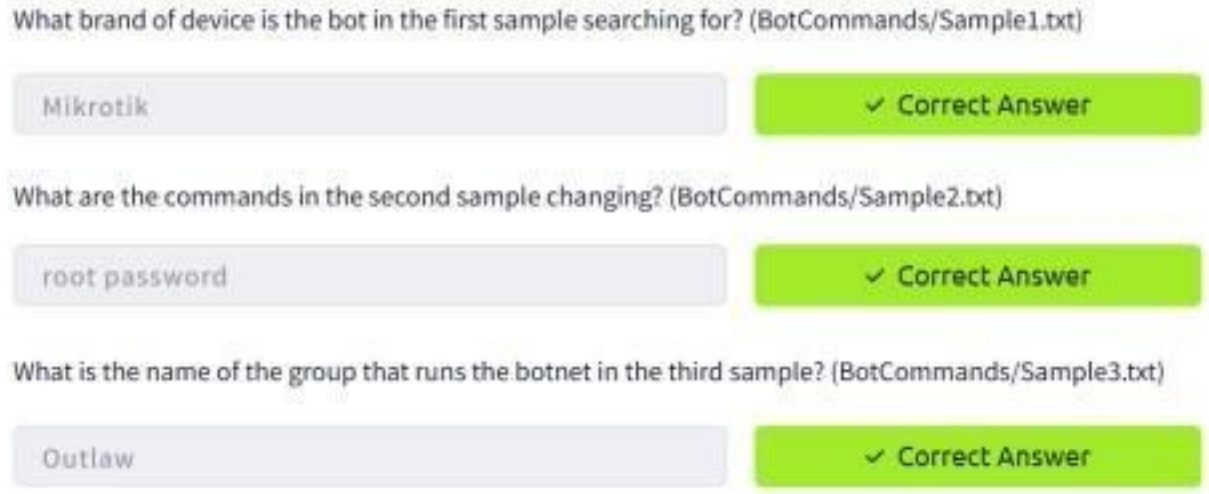
What flag must be set to pipe `wget` output into bash?

-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

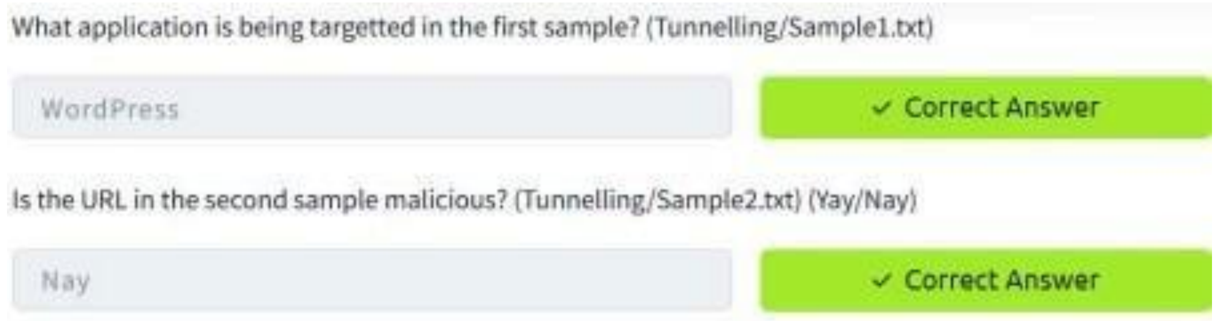
What are the commands in the second sample changing? (BotCommands/Sample2.txt)

root password

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

Outlaw

TASK 8 : SSH TUNNELLING



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

WordPress

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

Nay

CONCLUSION :

Honeypot and analysis of botnet activities is successfully deployed.