EX NO: 9 DEPLOYMENT OF HONEYPOTS AND ANALYSIS NAME: NAVEEN CH

DATE: 16.04.2025 OF BOTNET ACTIVITIES ROLL NO: 231901033

### AIM:

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

### TASK 2: TYPES OF HONEYPOTS

Read and understand the above



### Try running some commands in the honeypot

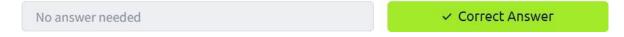


✓ Correct Answer

## TASK 4 : COWRIE LOGS

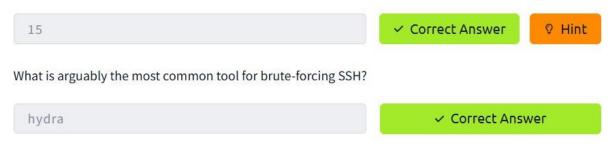
Nay

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

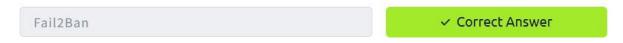


### **TASK 5: ATTACKS AGAINST SSH**

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



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



TASK 6: TYPICAL BOT ACTIVITY

What CPU does the honeypot "use"?	
Intel(R) Core(TM) i9-11900KB CPU @ 3.30GHz	✓ Correct Answer
Does the honeypot return the correct values when uname -a is run? (Yay/Nay)	
Nay	✓ Correct Answer
What flag must be set to pipe wget output into bash?	
-O	✓ Correct Answer
How would you disable bash history using unset?	
unset HISTFILE	✓ Correct Answer
TASK 7 : IDENTIFICATION TECHNIQUES	
What brand of device is the bot in the first sample searching for? (BotCommands/Sample1.txt)	
Mikrotik	✓ Correct Answer
What are the commands in the second sample changing? (BotCommands/Sample2.txt)	
root password	✓ Correct Answer
What is the name of the group that runs the botnet in the third sample? (BotCommands/Sample3.txt)	
Outlaw	✓ Correct Answer
TASK 8 : SSH TUNNELLING	
What application is being targetted in the first sample? (Tunnelling/Sample1.txt)	
WordPress	✓ Correct Answer
Is the URL in the second sample malicious? (Tunnelling/Sample2.txt) (Yay/Nay)	
Nay	✓ Correct Answer

# CONCLUSION:

Honeypot and analysis of botnet activities is successfully deployed.