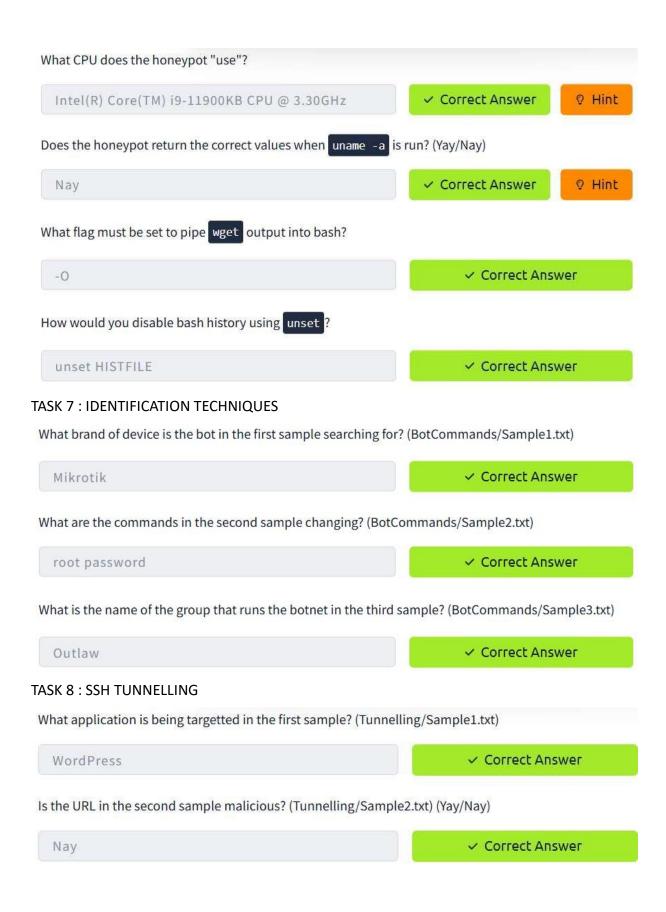
EX NO: 9 **DEPLOYMENT OF HONEYPOTS AND ANALYSIS** NAME: JASON FREDDY DATE: 16.04.2025 OF BOTNET ACTIVITIES ROLL NO: 231901014 AIM: A guided room covering the deployment of honeypots and analysis of botnet activities TASK 2 : TYPES OF HONEYPOTS Read and understand the above No answer needed ✓ Correct Answer TASK 3: COWRIE DEMO Try running some commands in the honeypot ✓ Correct Answer No answer needed Create a file and then log back in is the file still there? (Yay/Nay) ✓ Correct Answer 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. ✓ Correct Answer 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" ✓ Correct Answer ∀ Hint 15 What is arguably the most common tool for brute-forcing SSH? ✓ Correct Answer hydra What intrusion prevention software framework is commonly used to mitigate SSH brute-force attacks? ✓ Correct Answer Fail2Ban

TASK 6: TYPICAL BOT ACTIVITY



## **CONCLUSION:**

Honeypot and analysis of botnet activities is successfully deployed.