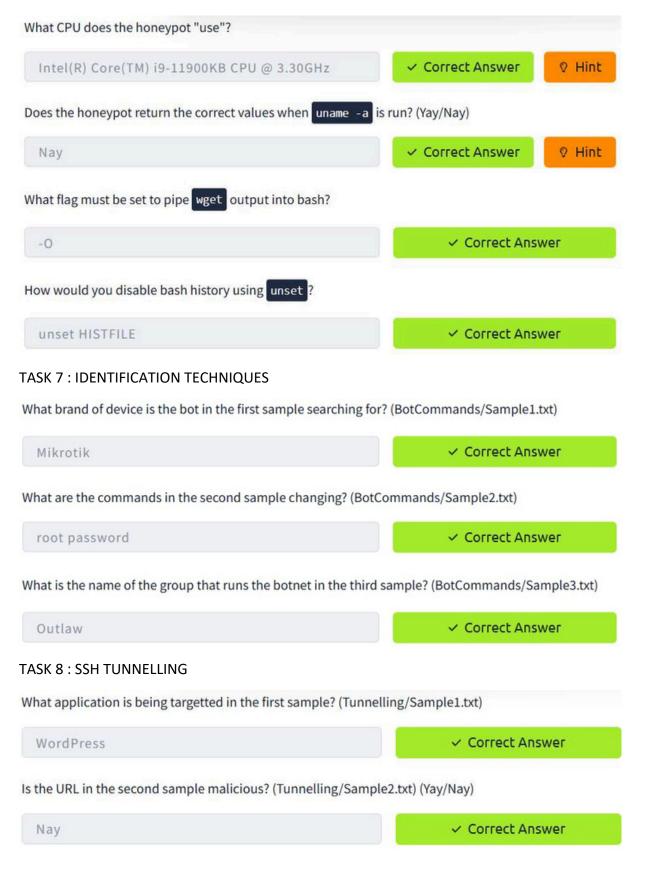
EX NO: 9 **DEPLOYMENT OF HONEYPOTS AND ANALYSIS** DATE: 16.04.2025 OF BOTNET ACTIVITIES AIM: A guided room covering the deployment of honeypots and analysis of botnet activities TASK 2: TYPES OF HONEYPOTS Read and understand the above No answer needed ✓ Correct Answer **TASK 3: COWRIE DEMO** Try running 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" ♥ Hint 15 ✓ Correct Answer What is arguably the most common tool for brute-forcing SSH? hydra ✓ Correct Answer What intrusion prevention software framework is commonly used to mitigate SSH brute-force attacks?

Fail2Ban

✓ Correct Answer

TASK 6: TYPICAL BOT ACTIVITY



CONCLUSION:

Honeypot and analysis of botnet activities is successfully deployed.