Student Guide:

Host-Based Incident Response Simulation

This guide is designed to help you navigate the **Host-Based Incident Response (IR)** simulation. In this exercise, you aren't just looking at network traffic; you are logging directly into a compromised workstation to find and remove threats using the **Linux Command Line Interface (CLI)**.

Phase 1: Mission Briefing

In this simulation, you are a Security Analyst performing **Host Forensics**. You have two scenarios to investigate:

- **Scenario 1 (The Beacon):** Active malware communicating with a hacker's server.
- **Scenario 2 (The Cron):** A hidden script scheduled to run automatically at regular intervals.

Analyst Goal: Identify the **Indicator of Compromise (IoC)**, stop the active threat (Containment), and delete the malicious files (Eradication).

Phase 2: The Forensic Toolkit

Use these commands to "peel back the layers" of the system:

Command	Analyst Rationale (Why you use it)
netstat	**Behavior:** View active network connections and associated PIDs. Look for unusual "Remote Ports".
ps aux	**Context:** List running processes to correlate a connection (PID) to a specific program or script in memory.
ls -l / stat	**Trust:** List files or view metadata (timestamps/owner) to spot risky executables and world-writable (**777**) modes.
history	**Timeline:** Reconstruct recent command history to see how a file was introduced and executed.
kill <PID>	**Containment:** Immediately terminate a running process to stop active malicious behavior.
rm <file>	**Eradication:** Remove a file from the disk to delete persistence and prevent re-execution.

Phase 3: Investigation Walkthrough (Scenario 1)

Step 1: Detect the IoC (The Analyst Mindset)

Run netstat. You will see two active outbound connections. You must decide which one is the threat:

- **Connection A (PID 3341):** Connecting to **Remote Port 443**.
- **Connection B (PID 4472):** Connecting to **Remote Port 4444**.

How to think like an Analyst:

1. **Ignore the Local Port:** Both PIDs use high local ports (e.g., 51234). These are **ephemeral ports** assigned by the OS and are usually meaningless.
2. **Evaluate the Remote Port:** This tells you what *service* the computer is talking to. Port **443** is standard HTTPS, used by legitimate services like APIs or updates.
3. **Identify the Outlier:** Port **4444** is a "non-standard" port. It is rarely used for legitimate business and is a well-known default for hacking tools like Metasploit.
4. **The Conclusion:** PID 3341 is likely a **False Positive**. PID 4472 is your **Indicator of Compromise (IoC)** because the destination port is unusual and warrants deeper validation.

Step 2: Correlate the Process

Run ps aux. Look for **PID 4472**. You will see it is a script called nightbeacon.sh running out of the /tmp/ directory.

Analyst Tip: Legitimate system scripts rarely run from /tmp. Attackers use this folder because it often has open "write" permissions for all users.

Step 3: Validate the File

Run stat nightbeacon.sh. The permissions are **0777** (world-writable). This violates the **Principle of Least Privilege**, as an executable script should never be editable by every user on a system.

Step 4: Remediate (The Golden Rule)

You must follow the correct **Sequence of Events**:

1. **Stop Memory (kill 4472):** Stop the process first to halt active external communication.
2. **Remove Disk (rm nightbeacon.sh):** Once the process is dead, delete the file to prevent it from being triggered again.

Phase 4: Investigation Walkthrough (Scenario 2)

Step 1: Identify the "Heartbeat"

Run cat /etc/cron.d/sysupdate to view the scheduled tasks.

Step 2: Analyze the Schedule

Look for the timing code: * * * * *.

- Five stars mean the script runs **every minute**. Legitimate "System Updates" usually run daily or weekly. This high frequency is a strong sign of **persistence**.

Step 3: Containment

Run rm /etc/cron.d/sysupdate. This "breaks the cycle" and stops the system from automatically relaunching the malicious script.

Exam Readiness Summary

- **False Positive:** An alert that looks suspicious but is legitimate (e.g., PID 3341 using Port 443).
- **Persistence:** How malware survives a reboot, often via **Scheduled Tasks** (Cron jobs).
- **Containment vs. Eradication:** Containment stops the active behavior (kill); Eradication removes the source (rm).
- **Sequencing:** Always stop the running code before deleting the file to ensure no malicious activity remains in memory.