Student Guide: Network Threat Analysis Simulation

This guide is designed to transform you from a "log reader" into a **Security Analyst**. In this simulation, you are performing **Incident Response (IR)** to identify how a malware outbreak started and which systems are still at risk.

Phase 1: The Briefing

A suspicious file named svch0st.exe has been detected across the network.
Analyst Tip: In the IT world, svchost.exe (with an 'o') is a legitimate Windows process. The file svch0st.exe (with a zero) is an example of **Typosquatting** or **Masquerading**. This is a common technique used by attackers to hide in plain sight.

Phase 2: Host Analysis (The "What")

Your first step is to check the local Antivirus (AV) logs on each machine to see if the security software stopped the threat.

1. Identify "Successful Remediations"

Look for systems where the AV worked as intended:

- **10.20.2.15:** The log shows the file was found and **successfully quarantined**.
- **192.168.30.25:** Similarly, this system detected the match and the file was **quarantined**.

Conclusion: These devices are **Clean**. Even though they were targeted, the technical control (AV) prevented the infection from taking hold.

2. Identify "Active Infections"

Look for "Error" messages or "Disabled" features:

- **192.168.30.15:** This is a major red flag. The logs show the malware **disabled scheduled scans and updates**. This is a classic **Persistence** technique—the malware is protecting itself from being deleted.
- **192.168.30.35:** The AV detected the file but reported an **"Unable to quarantine"** error. This means the malware is likely running and "locked," preventing the AV from moving it.

Conclusion: These devices are **Infected**.

Phase 3: Network Analysis (The "Who")

Now we look at the **Firewall Log** to find **Patient Zero** (the Origin). We are looking for the system that is actively "attacking" or "pivoting" to other internal machines.

Finding the Origin: 10.20.2.25

We label 10.20.2.25 as the **Origin** for three specific reasons found in the logs:

1. **Failed Control:** Like the other infected hosts, its AV was **unable to quarantine** the file.
2. **Internal Pivoting:** The firewall shows this IP initiating connections to 192.168.30.15 and 192.168.30.35 using **RPC (Port 135)** and **SMB (Port 445)**. These protocols are frequently used for **Lateral Movement**—spreading malware from one computer to another.
3. **External Beacons:** It is seen communicating with external IPs (like 57.203.54.183) over Port 443. In exam terms, this is called **Command and Control (C2)** traffic.

Phase 4: Final Diagnostic Table

Use this table to verify your answers before submitting the simulation.

Host IP	Evidence Found	Status
10.20.2.25	Failed quarantine; initiates lateral movement to other hosts.	**Origin**
192.168.30.15	Malware disabled security services; receiving traffic from origin.	**Infected**
192.168.30.35	Heuristic match found but quarantine failed; outbound traffic seen.	**Infected**
10.20.2.15	File successfully quarantined; no further suspicious activity.	**Clean**
192.168.30.25	File successfully quarantined; system remains stable.	**Clean**

Exam Readiness Summary

- **Lateral Movement:** When an attacker moves from one compromised host to others within the same network (often via SMB/RPC).
- **Heuristics:** A detection method that looks for *patterns* or *behaviors* of malware rather than a specific "fingerprint" (seen in host 10.20.2.25 and 192.168.30.35).
- **Quarantine:** Moving a malicious file to a safe, isolated folder where it cannot execute. If this fails, the system is considered compromised.