Incident Response & Analysis: Ransomware Attack and Security Tool Investigations

Documented and analyzed multiple cybersecurity incidents using an Incident Handler's Journal. This included investigating a ransomware attack at a healthcare organization, analyzing suspicious network traffic with Wireshark and tcpdump, and investigating malicious file hashes with VirusTotal. Applied the NIST Incident Response Lifecycle across all cases, focusing on Detection & Analysis, and Containment, Eradication, and Recovery phases.

Tools: Wireshark, tcpdump, VirusTotal
Skills: Incident documentation, ransomware analysis, phishing investigation, file hash verification, packet capture and analysis, NIST IR Lifecycle application, technical reporting

Case 1: Ransomware Attack on Healthcare Clinic

Who	Organized cybercriminal group targeting healthcare and transportation sectors
What	Ransomware deployed after phishing emails with malicious attachments were opened, encrypting critical files
When	Tuesday, 9:00 a.m.
Where	Small U.S. healthcare clinic
Why	Financial gain via ransom demand for decryption key

Case 2: Packet Capture Analysis (Wireshark)

Analyzed PCAP file to detect abnormal network activity. Learned to filter and inspect packets for suspicious traffic patterns. Gained familiarity with GUI-based network protocol analysis.

Case 3: Live Traffic Capture (tcpdump)

Captured and filtered network traffic in real time using CLI-based tcpdump. Overcame command syntax challenges through iterative testing and review.

Case 4: Malicious File Hash Investigation (VirusTotal)

Investigated SHA-256 file hash flagged by security systems. Confirmed malicious classification through VirusTotal's multi-engine scan results. Determined initial infection vector (malicious email attachment) and recommended preventive measures.

Reflection

This project reinforced the importance of clear, structured documentation in incident handling. Working with real-world tools like Wireshark, tcpdump, and VirusTotal strengthened my confidence in threat detection and analysis. It also highlighted the value of user training and awareness to prevent common attack vectors like phishing.