Identifying Cyberattacks Using Network Monitoring Tools

Objective: Analyze captured network traffic logs using monitoring tools (like `tcpdump`, `Wireshark`) to detect signs of cyberattacks (e.g., port scanning, brute-force login attempts, protocol misuse, etc.).

Tool(s) Used: `tcpdump`, `Wireshark`

Log File Analyzed: HTTP-log.xlsx

Summary of Network Activity

The captured traffic shows a full TCP three-way handshake between source IP `198.51.100.23` and destination IP `192.0.2.1`, followed by the HTTP GET request for `/sales.html` and a 200 OK response.

Protocol Analysis

- **Protocol Involved**: TCP and HTTP
- **Transport Lay Activity**:
  The initial TCP handshake (`SYN`, `SYN-ACK`, `ACK`) was successfully completed.
- **Application Layer Activity**:
  The HTTP request was well-formed and returned a valid HTML response, indicating the server was reachable and responding as expected.

Detection and Analysis

Although this log shows no direct signs of malicious activity such as failed login attempts or port scans, it is important to establish a baseline of normal activity to later contrast with anomalous behavior.

However, a few things should still be noted:

- No encryption was used (plain HTTP), which means sensitive data could be intercepted via sniffing.
- If this were combined with suspicious DNS logs or ICMP failures, it could suggest a redirection or spoofing campaign.

How Network Monitoring Tools Were Used

- tcpdump helped capture low-level packet data
- Wireshark would typically be used to decode protocols and view application-layer payloads (like GET requests and responses)

These tools enable visibility into traffic behavior and assist in detecting:

- Unusual port usage
- Unexpected destinations
- Malformed requests
- Large Volumes of repeated traffic (DoS)

NIST CSF Mapped

- **Identify**: Established normal network activity (GET request over HTTP)
- **Detect**: No immediate threats, but use of HTTP should be flagged for policy review
- **Protect (follow-up)**: Recommend enforcing HTTPS and monitoring for unencrypted traffic