Updated Documentation: Network Security Tools Usage

Tool 1: Wireshark Analysis

Objective: Analyze network packet data to identify security threats, anomalies, and traffic patterns.

Procedure:

1. **Packet Capture:**
   - Loaded the PCAP file into Wireshark for analysis.
   - Applied filters such as mdns, icmp, udp, and tls to focus on specific traffic.
2. **Key Findings:**
   - **MDNS Traffic:** Detected service discovery protocols indicating device presence and services on the local network. Notable devices include “iPhone X” and “Java.”
   - **ICMP Traffic:** “Destination unreachable” packets highlight potential misconfigured devices or network issues.
   - **TLS Connections:** Observed encrypted communications with external IPs, including connections to plugins.nessus.org.
   - **SSDP Traffic:** Devices searching for UPnP services suggest active service discovery on the network.
3. **Security Concerns:**
   - Validate devices issuing MDNS and SSDP queries to ensure no rogue devices are present.
   - Check the legitimacy of external TLS connections.

Evidence:

- Wireshark screenshot: Filtered view showing MDNS traffic and device discovery.

Tool 2: Network Vulnerability Scanner

Objective: Identify vulnerabilities in the network infrastructure using an automated scanning tool.

Procedure:

1. **Scanning Target:**
   - Scanned the website of DAE using a vulnerability scanner.
   - Focused on identifying low-risk vulnerabilities.
2. **Findings:**
   - The scan detected low-severity vulnerabilities related to network misconfigurations and service exposures.
   - Key findings include:
     - **Traceroute Information:** Enabled on the target, allowing path analysis to the host.

    - **Web Server Misconfigurations:** Some servers do not return 404 error codes, which could expose information.
    - **Unknown Service Detection:** Services with unidentified banners were found on certain ports.
    - **SYN Scanning:** TCP ports were detected as open using SYN scans.

3. **Implications:**
    - Exposure of traceroute and open ports increases the risk of reconnaissance by attackers.
    - Unknown services or improper configurations can lead to information disclosure.
4. **Recommendations:**
    - Protect traceroute endpoints with firewalls or IP filters.
    - Ensure web servers are configured to return appropriate error codes.
    - Investigate and secure services running on detected open ports.

Evidence:

- Summary of low-risk vulnerabilities from the scan:
    - Host: 34.149.87.45
    - Ports: 0 (Traceroute), 80 (Web Server), 443 (Unknown Service)

Tool 3: Network Penetration Testing

Objective: Simulate an attack to test network defenses using penetration testing tools.

Procedure (Pending Nmap Data):

1. Perform active reconnaissance using Nmap to scan for vulnerabilities.
2. Attempt basic exploits or configuration analysis to test defensive measures.

Findings and Recommendations:

(Will be updated later)

Final Recommendations

1. **Mitigation:**
    - Implement IP filtering to restrict traceroute access.
    - Harden web server configurations to prevent reconnaissance.
    - Secure open ports and investigate unknown services.
2. **Monitoring:**
    - Continuously monitor for MDNS and SSDP traffic to detect unauthorized devices or services.
    - Regularly scan and patch vulnerabilities using tools like Nessus or OpenVAS.

3. **Hardening:**

- Disable unnecessary services on hosts and network devices.
- Use TLS configurations that adhere to modern security standards.