Network Analysis Lab Report - ASAGBA JEREMIAH

Objective of the Lab

The primary goal of this lab was to conduct a comprehensive network analysis focusing on identifying and dissecting malicious activities within a given packet capture (PCAP) file. The lab aimed to enhance practical skills in traffic analysis, specifically in detecting web shell uploads, reconnaissance activities, and unauthorized remote command executions.

Skills Learned

- Proficient use of Wireshark for network traffic analysis.
- Identification and analysis of port scanning activities.
- Detection of web penetration testing tools like Gobuster and sqlmap in network traffic.
- Decoding and understanding malicious payloads in HTTP requests.
- Identification of web shell upload and execution.
- Recognizing and analyzing reverse shell connections.

Tools Used

- **Wireshark**: For opening and analyzing the PCAP file.
- **Gobuster 3.0.1:** Detected as a tool used for web penetration testing focused on brute-forcing URIs.
- **sqlmap 1.4.7:** Identified as a tool used for automating the process of detecting and exploiting SQL injection vulnerabilities.

Analysis and Findings

Initial Analysis

- **Capture File Properties:** Provided insights into the duration and the protocols used within the packet capture, hinting at potential points of entry.
- **Protocol Hierarchy and Conversations:** Helped identify the most active IP addresses and potential open ports, indicating the direction of further analysis.

Key Findings

1. **Port Scan Activity:**
    - Responsible IP: 10.251.96.5
    - Port Range Scanned: 1-1024
    - Type of Port Scan: TCP SYN

2. **Reconnaissance Tools Detected:**
    - Gobuster 3.0.1 and sqlmap 1.4.7 were used against open ports, indicating a thorough reconnaissance effort.

3. **Malicious File Upload:**
    - **PHP File Uploaded:** Editprofile.php
    - **Web Shell Uploaded:** Dbfunctions.php, serving as the gateway for remote command execution.

4. **Web Shell Execution:**
    - **Execution Parameter:** Cmd
    - **First Command Executed:** Id, indicating an attempt to identify the user privileges.
    - **Shell Connection Type:** Reverse Shell, utilizing port 4422 for the connection, enabling the attacker to have hands-on keyboard access to the server.

Steps Taken

1. Started with a preliminary analysis using Wireshark to understand the packet capture's context and to identify significant IPs and protocols.
2. Detected SYN packets and a SYN-ACK handshake, pinpointing successful connections on ports 80 and 22, which led to the identification of the port scanning activity.
3. Recognized the use of Gobuster and sqlmap tools in the traffic, suggesting unauthorized reconnaissance and exploitation attempts.
4. Decoded a malicious POST request indicating SQL injection and XSS attempts, alongside an attempt to execute system-level commands.
5. Traced the upload and execution of a malicious PHP file (Dbfunctions.php), which was used to establish a reverse shell connection.

Conclusion

The lab provided hands-on experience in network traffic analysis, emphasizing the importance of being able to detect and understand the indicators of compromise and the tactics, techniques, and procedures (TTPs) used by attackers. The successful identification and analysis of the reconnaissance tools, the malicious file upload, and the subsequent remote command execution highlight the critical need for robust network monitoring and security measures.