MODULE 11 Session Hijacking LAB REPORT

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/185bc85e-504b-4608-a989-070262584323

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01: Perform Session Hijacking

Task 1: Hijack a Session using Zed Attack Proxy (ZAP)

1. Configure the victim's machine (Windows 11) to use the attacker's machine (Windows Server 2019) as a proxy.
2. Launch ZAP on the attacker's machine.
3. Set up ZAP as a proxy and intercept traffic from the victim's machine.
4. Modify the intercepted requests to redirect the victim to a different website (www.goodshopping.com in this case).
5. Demonstrate successful session hijacking by showing that the victim's browser displays the manipulated website even though the address bar still shows the original website.

Task 2: Intercept HTTP Traffic using bettercap

1. Use bettercap on the Parrot Security machine to intercept HTTP traffic.
2. Set up bettercap to perform ARP spoofing and HTTP proxying.
3. Sniff HTTP traffic from the victim's machine (Windows 11) using bettercap.
4. Capture website browsing and login credentials entered by the victim on a non-HTTPS website (www.moviescope.com).

Task 3: Intercept HTTP Traffic using Hetty

Use Hetty on the Windows 11 machine to intercept HTTP traffic.

Configure the victim's machine (Windows Server 2022) to use the attacker's machine (Windows 11) as a proxy.

Launch Hetty and create a project.

Capture HTTP traffic from the victim's machine (Windows Server 2022) using Hetty.

Extract login credentials entered by the victim on the website (www.moviescope.com).

These tasks provide a comprehensive overview of how session hijacking can be carried out using different tools and techniques.

It's crucial for ethical hackers and penetration testers to understand these concepts to identify and mitigate such vulnerabilities in real-world scenarios.

Lab 02: Detect Session Hijacking:

Task 1: Detect Session Hijacking using Wireshark

Launch Wireshark: Open Wireshark on the target machine (Windows 11).

Start Capturing Traffic: Double-click the primary network interface (Ethernet) in Wireshark to start capturing network traffic.

Prepare for Session Hijacking Attack: On the attacker machine (Parrot Security), use bettercap to initiate a session hijacking attack. This involves setting up the network interface, performing ARP probing and reconnaissance, and starting network sniffing.

Observe ARP Packets: Switch back to the Wireshark window on the target machine (Windows 11) and observe the captured ARP packets. A high number of ARP requests indicates that the attacker's system (10.10.1.13) is acting as a client for all IP addresses in the subnet, potentially intercepting traffic intended for the victim machine (10.10.1.11).

By observing the ARP packets captured by Wireshark, the network administrator can detect signs of ARP spoofing, which is a common technique used in session hijacking attacks.

Document any suspicious activity observed during the Wireshark capture for further analysis and remediation.