MODULE 10 Denial-of-Service LAB REPORT

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/83d0c8b5-5c79-4249-8e5b-872df062a32a

Username on EC-Council System

1. 2110886@uj.edu.sa

Lab 01: Perform DoS and DDoS Attacks using Various Techniques

Task 1: Perform a DoS Attack (SYN Flooding) using Metasploit:

- Utilize Metasploit's auxiliary module to perform a SYN flooding attack on a target host (Windows 11).
- Spoof the IP address of the attacking machine (Parrot Security) to impersonate another machine (Windows Server 2019).
- Monitor the attack using Wireshark and observe the impact on the target machine.

Task 2: Perform a DoS Attack using hping3:

Utilize hping3 tool to conduct SYN flooding and Ping of Death (PoD) attacks on a target host (Windows 11).

Spoof the IP address to disguise the origin of the attack.

Capture and analyze network traffic using Wireshark to observe the attack impact.

Task 3: Perform a DoS Attack using Raven-storm:

Utilize Raven-storm tool to launch Layer 3 and Layer 4 DoS attacks on a target host (Windows Server 2019).

Configure the attack parameters and monitor network traffic using Wireshark.

Task 4: Perform a DDoS Attack using HOIC:

Employ HOIC tool to execute HTTP flood DDoS attack on a target host (Parrot Security) from multiple attacking machines (Windows 11, Windows Server 2019, Windows Server 2022).

Configure the target URL, power, and threads for the attack.

Monitor network traffic using Wireshark to assess the impact on the target machine.

Task 5: Perform a DDoS Attack using LOIC:

- Utilize LOIC tool to conduct UDP flood DDoS attack on a target host (Parrot Security) from multiple attacking machines (Windows 11, Windows Server 2019, Windows Server 2022).
- Configure the target IP address, method, threads, and power for the attack.
- Monitor network traffic using Wireshark to evaluate the impact on the target machine.

Key Learnings:

- Understanding various DoS and DDoS attack techniques and their impact on network resources.
- Hands-on experience in configuring and launching DoS/DDoS attacks using different tools such as Metasploit, hping3, Raven-storm, HOIC, and LOIC.
- Familiarity with spoofing IP addresses, configuring attack parameters, monitoring network traffic using Wireshark, and assessing the impact of attacks on target systems.
- Insight into the significance of network security measures and the importance of safeguarding against DoS and DDoS threats to mitigate potential risks and vulnerabilities.

Lab 02: Detect and Protect Against DoS and DDoS Attacks

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

1. **Install Anti DDoS Guardian:**
    - Launch the Anti DDoS Guardian setup wizard on the target system (Windows 11).
    - Follow the installation steps provided, including accepting User Account Control prompts and security warnings.
    - Uncheck unnecessary options such as "Stop RDP Brute Force" during installation.
    - Complete the installation process and ensure the desktop shortcut option is selected.

Learning: Understand the installation process of Anti DDoS Guardian and the importance of deselecting unnecessary options during setup.

2. **Configure Anti DDoS Guardian Settings:**
    - Open Anti DDoS Guardian and familiarize yourself with the dashboard, displaying information about incoming and outgoing traffic.
    - Navigate to the settings and ensure default configurations are maintained unless specified otherwise.
    - Learn about Anti DDoS Guardian's features such as monitoring network flow, limiting bandwidth, and managing TCP/UDP connections.

Learning: Gain familiarity with the Anti DDoS Guardian interface and its capabilities in monitoring and protecting against DDoS attacks.

3. **Launch and Configure Low Orbit Ion Cannon (LOIC) on Attacker Machines:**
    - Access the attacker machines (Windows Server 2019 and Windows Server 2022).
    - Navigate to the directory containing LOIC (provided in the lab instructions).
    - Launch LOIC.exe and configure the tool to target the Windows 11 machine (the victim).
    - Set attack options such as attack method (UDP), threads, and power level.

Learning: Understand how to configure LOIC for launching DDoS attacks and the significance of selecting appropriate attack parameters.

4. **Initiate DDoS Attack:**
    - Once LOIC is configured on all attacker machines, click the "IMMA CHARGIN MAH LAZER" button to initiate the DDoS attack.
    - Observe the flood of packets being sent from the attacker machines to the target (Windows 11) in Anti DDoS Guardian's dashboard.

Learning: Recognize the impact of a DDoS attack on network traffic and the importance of monitoring tools like Anti DDoS Guardian in detecting such attacks.

5. **Monitor and Block Suspicious Traffic:**
    - In Anti DDoS Guardian, observe the packets captured from the attacker machines (Windows Server 2019 and Windows Server 2022).
    - Identify the IP addresses associated with the attack traffic.

- Use Anti DDoS Guardian's "Block IP" feature to block the malicious IP addresses.

Learning: Learn to identify suspicious traffic patterns and take proactive measures to block attackers using Anti DDoS Guardian.

6. **Stop DDoS Attack and Clean Up:**
    - Once the attack has been mitigated by blocking malicious IP addresses, stop the DDoS attack on all attacker machines.
    - Close all open windows associated with LOIC and Anti DDoS Guardian on both attacker and target machines.
    - Uninstall Anti DDoS Guardian from the target system (Windows 11) via Control Panel -> Programs and Features.

Learning: Understand the importance of promptly stopping DDoS attacks and removing any installed protection tools after the exercise.

Conclusion:

This lab provided hands-on experience in detecting and protecting against DDoS attacks using Anti DDoS Guardian. Key takeaways include understanding the installation and configuration of DDoS protection tools, monitoring network traffic for anomalies, and taking proactive measures to block attackers.