VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Course Code: BCSE354E

Lab Slot: L33+L34

Faculty: Dr. Priya V

Project Title:

Executing Denial of Service attack in Kali Linux and mitigating them.

Team Members:

1. **Roshan (21BIT0619)**
2. **Ambatipudi Vidya (21BIT0710)**
3. **Poli Vardhini Reddy (21BIT0382)**
4. **R Vinay Kumar (21BIT0484)**
5. **P Lokesh Sai (21BIT0405)**

Project Description:

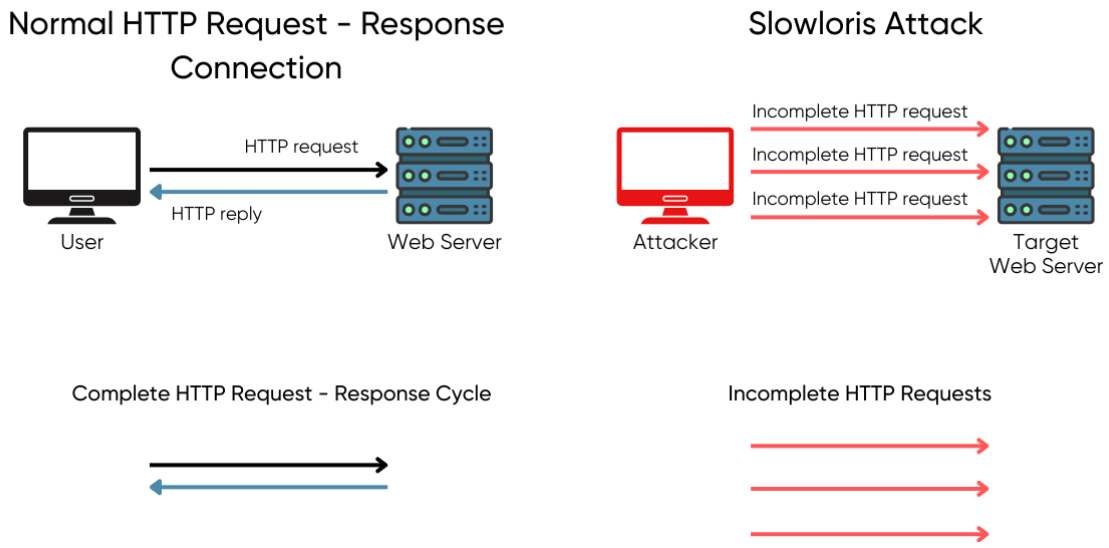
This project will investigate the functionality of Denial-of-Service (DoS) attack tools commonly found in Kali Linux, focusing on dSniff, LOIC, hping3, Slowloris and their potential exploitation methods. DoS attacks aim to overwhelm a system or network with traffic, making it unavailable to legitimate users. The project will adopt an ethical hacking approach, analyzing these tools to understand how attackers might use them and how to defend against such attacks. We will not be launching actual attacks. Instead, we will set up a secure lab environment in Kali Linux to become familiar with dSniff, LOIC, hping3 and Slowloris.

Tools:

1. Kali Linux
2. LOIC
3. hping3
4. dSniff
5. Slowloris

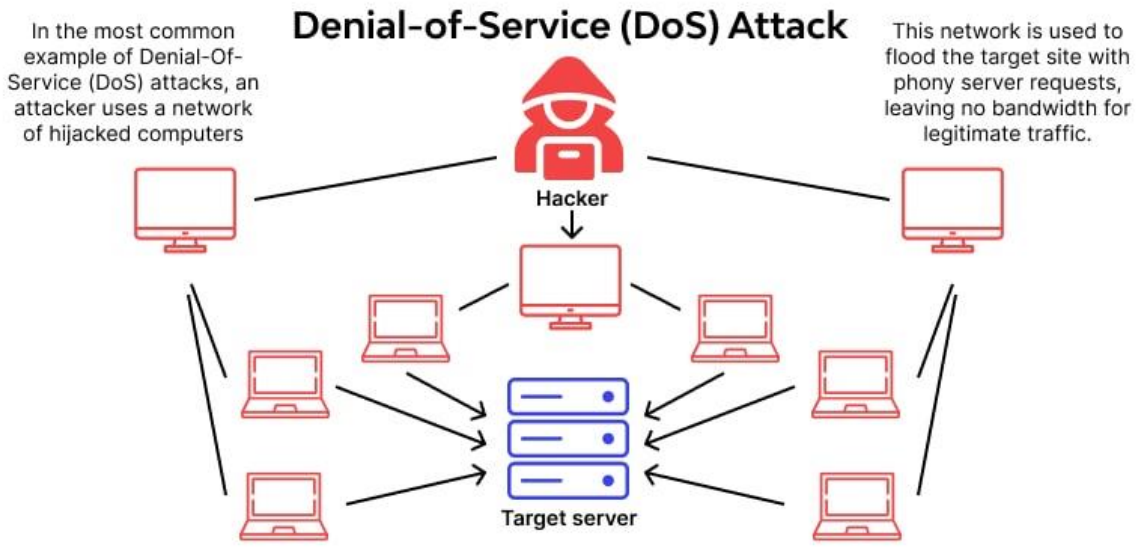
Application of Tools in the project with a neat sketch:

Using LOIC, hping3, dSniff and Slow loris, we can simulate the DoS attack by giving the IP address of the system that has to be attacked. All of these methods could be done in Kali Linux. These tools send continuous traffic to the IP address given, and leaves no room for legitimate traffic by consuming all the resources. Following is an example of an attack done using Slowloris.



Steps:

1. **Installing Kali Linux:** Install and set up Kali Linux on a VM. Kali Linux is specifically designed for penetration testing and network security assessments, which makes it a useful tool for identifying and exploiting vulnerabilities in computer systems.
2. **Inspecting tools for DoS:** Introduce yourselves to the tools available for DoS attacks in Kali Linux, such as LOIC, hping3, dSniff, and Slowloris. Understand how they would be helpful in conducting a DoS attack.
3. **Launch a DoS attack:** Using the tools you've discovered in the earlier step, implement the DoS attack in Kali Linux.
4. **Observing the attack:** Monitor how the traffic is being received, and how the resources are being consumed.



Mitigating DoS attacks:

- Limit the number of concurrent connections.
- Deploy a specialized WAF (Web Application Firewall).
- Monitor web logs and other data sources.
- Keep software up to date.
- By restricting the IP address or subnet of the system (using iptables) that is attacking.

Expected Outcome:

The conclusion of this project is to successfully learn how to launch a Denial-of-Service attack using the tools in Kali Linux, understand how the attackers implement DoS in various ways, and how to tackle those kinds of attacks, and make sure the system is intact.