SYN FLOOD ATTACK USING HPING3

* ZINEEDDINE BOUMRAR

1. Introduction :

A SYN flood attack is a type of Denial-of-Service (DoS) attack that exploits the TCP three-way handshake by sending a large number of SYN requests to a target system. This overwhelms the target and prevents legitimate traffic from being processed. Here's a step-by-step guide to performing a SYN flood attack on a Windows 7 machine using hping3.

1. Steps Followed :
2. Prerequisites

* Linux Machine:
  + Install hping3 on a Linux machine .
* Target Machine:
  + Windows 7 machine set up as the target.

1. Verify Connectivity

* Ensure the Windows 7 machine is on the same network as your Linux machine.
  + Confirm the IP address of the Windows 7 machine.
* Ping the Windows 7 machine from your Linux machine to ensure connectivity.

1. Perform the SYN Flood Attack

* sudo hping3 -S -p 80 --flood 192.168.1.100

1. Monitor the Target Machine

* On the Windows 7 machine, monitor the network traffic and system performance.
  + Open Command Prompt and use **netstat** to check for a large number of SYN\_RECV states:
    1. netstat -an | find "SYN\_RECV"
  + Use Task Manager to observe CPU and memory usage.

1. What i did :

In a SYN flood attack, I exploit a vulnerability in the TCP three-way handshake by sending a large number of SYN requests to the target server without completing the handshake. This causes the server to allocate resources for each half-open connection, eventually overwhelming it and preventing legitimate users from connecting. By continuously bombarding the server with these requests, I can exhaust its resources and cause a denial of service, demonstrating the critical need for robust security measures to mitigate such attacks.

1. Defenses Against SYN Flood Attacks

* SYN Cookies:
  + A technique to handle SYN floods by not allocating resources until the connection is fully established.
* Rate Limiting:
  + Limiting the rate of incoming SYN packets.
* Firewalls and Intrusion Detection Systems (IDS):
  + Configured to detect and mitigate SYN flood attacks.