**Module 10 : Denial - of -Service**

* **Denial-of-service:**
* to disrupt or shut down the normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate requests that trigger a crash. This causes the target to become slow, unresponsive, or utterly inaccessible to legitimate users. These malicious endeavors can cripple websites, disrupt services, and cause significant financial and reputational damage.
* malicious attempt to overwhelm an online service, rendering it unusable by flooding it with excessive requests.
* Pure form of Attack, Only used for attacking purpose.
* DoS attack : one to one attack by flooding unwanted request/traffic.
* DDoS attack: multiple compromised computer systems (often part of a botnet) are used to send a large volume of requests to the target, making it difficult for legitimate users to access the service.
* **Dos Attack:**

Attacker: kali os, Victim: Window 11

1. **syn flooding using metasploit**

Tool: msfconsole

**Steps:**

* Open both attacker and victim machine
* In kali os, goto terminal & scan port of window 11 “ sudo nmap 10.10.10.11”
* Open new tab in terminal > run tool metasploit “ sudo msfconsole”
* Search flood > select “auxillary/dos/tcp/synflood” > show options
* Set RHOST 10.10.10.11 > set RPORT (select any open / closed port)

(open port - in use, close port - not in used but can be used/turned on ,

Filtered port- managed by firewall policy)

* Cmd “ run” //starting DoS attack.
* Goto window 11 > task manager > performance // to monitor resource uses after Dos Attack
* In kali os, open wireshark > analyze the traffic request in both machines
* Check source ip & destination ip, destination port number and TCP traffic.
* **DoS Attack using hping3 tool (in kali os):**

Attacker: kali os

Victim: window 11

Tool: hping3

**Steps:**

* Goto terminal > open tool hping3 “ sudo hping3 -h”
* Cmd ( Sudo hping3 -S 10.10.10.11 - - flood )

( note: -S for sending syn traffic to target

– flood for flooding traffic to target )

* Open wireshark in window 11 and analyze incoming traffic status
* Open task manager > performance // analyze the performance of victim machine
* For spoffing source ip during Dos attack:

Cmd ( sudo hping3 -S 10.10.10.11 -a 10.10.10.22 - - flood)

// -a to spoof source address

* **DoS Attack using raven strom tool (in kali os):**

Attacker: kali os

Victim: window 11

Tool: hping3

**Steps:**

* In kali, Goto github > search Raven-Strom > copy url link > goto terminal > git clone the copied url link > ls > cd Raven-Strom > ls > pip3 install -r requirements.txt > python3 main.py
* Select module “ L4” > set target ip “ ip 10.10.10.11” > set destination port “ port 22” > run > yes
* Check the traffic in window 11 from wireshark tool

* **Dos Attack from Windows 11 using HOIC tool:**

Attacker: Window 11

Target: Kali Linux

Tool: High orbit Ion Cannon (HOIC)

**Steps:**

* In window goto backup drive E: > Module denial of service > Dos and DDos Attack tools > High orbit Ion Cannon (HOIC) > run "hoic2.1 exe "
* Add target " +" > assign target ip as url (http://10.10.10.13 )
* Assign attack power > Assign Booster "GenericBoost.hoic" > select target > check status > FIRE TEH LAZER!
* Open wireshark in both Kali and window 11 to analyse the Dos Attack.
* **Dos Attack from Windows 11 using LOIC tool:**

Attacker: Window 11

Target: Kali Linux

Tool: Low orbit Ion Cannon (LOIC)

**Steps:**

* In window goto backup drive E: > Module denial of service > Dos and DDos Attack tools > Low orbit Ion Cannon (HOIC) > run "LOIC exe "
* Assign target url / ip > lock on > assign port > assign method > assign speed then " IMMA CHARGIN MAH LAZER"
* **DoS & DDoS Protection using Anti\_DDoS\_Guardian tool (in window 11):**

Tool: Anti DDos Guardian

**Steps:**

* In window goto backup drive E: > Module denial of service > Dos and DDos protection tools > Anti\_DDoS Guardian > Anti\_DDoS Guardian setup exe
* Install tool > leave all by default > continue
* In kali os, Goto terminal > open tool hping3 “ sudo hping3 -h”
* Cmd ( Sudo hping3 -S 10.10.10.11 - - flood )

( note: -S for sending syn traffic to target

– flood for flooding traffic to target )

* Open anti\_ddos Guardian tool in window 11 and analyze incoming traffic status, check the blocked traffic (indicator: red)
* To enable the blocked traffic, select blocked traffic > rt.click > remove the IP address from the IP Block List.