## **DoS and DDoS**

## 

## **In this module we will focus Denial-of-Service(DoS) and Distributed Denial-of Service(DDoS) attacks. This module cover understanding of different DoS**

## **and DDoS attacks, attacking techniques, concept, attacking tools and its countermeasures. How to defend against these attacks.**

## 

## **What is a Denial-of-Service Attack?**

## **Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.**

## **In a DoS attack, attackers flood a victim system with nonlegitimate service requests or traffic to overload its resources**

## **DoS attack leads to unavailability of a particular website and slow network performance.**

## 

## **What are Distributed Denial of Service Attacks?**

## **A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service**

## **for users of the targeted system.**

## **To launch a DDoS attack, an attacker uses botnets and attacks a single system.**

## 

## **DoS and DDoS Impact**

## **Loss of Goodwill**

## **Disabled Network**

## **Financial Loss**

## **Disabled Organization**

## **Like Flipkart got down in past.**

## 

## **DoS/DDoS Attack Techniques**

## **Bandwidth Attacks and Service Request Floods**

## **SYN Attack**

## **SYN Flooding Attack**

## **ICMP Flood Attack**

## **Botnet Attack**

## **And many more**

## 

## **Bandwidth Attacks**

## **When a DDoS attack is launched, flooding a network, it can cause network equipment such as switches and routers to be overwhelmed due to the significant**

## **statistical change in the network traffic.**

## **Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets.**

## **Basically, all bandwidths is used and no bandwidth remains for legitimate use.**

## 

## **Service Request Floods**

## **An attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections.**

## **Service request flood attacks flood servers with a high rate of connections from a valid source**

## **It initiates a request on every connection**

## 

## **SYN Attack**

## **The attacker sends a large number of SYN request to target server (victim) with fake source IP addresses.**

## **The target machine sends back a SYN/ACK in response to the request and waits for the ACK to complete the session setup**

## **The target machine does not get the response because the source address is fake.**

## 

## **SYN Flooding Attack**

## **SYN Flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake.**

## **When Host B receives the SYN request from A, it must keep track of the partially opened connection in a "listen queue" for at least 75 seconds**

## **A malicious host can exploit the small size of the listen queue by sending multiple SYN requests the a host, but never replying to the SYN/ACK.**

## **The victim's listen queue is quickly filled up**

## **The ability of holding up each incomplete connection for 75 seconds can be cumulatively used as a Denial of Service attack.**

## 

## **ICMP Flood Attack**

## **ICMP flood attack is a type DoS attack in which attacker send a large number of ICMP packets.**

## 

## **Practical Part :**

## **1. Syn Flooding Attack Using Metasploit :**

## **Commands -**

## **#nmap -p 21 192.168.1.132**

## **#msfconsole**

## **#use auxiliary/dos/tcp/synflood**

## **#show options**

## **#set RHOST <victim ip address>**

## **#set RPORT 21**

## **#set SHOST <spoofable ip address>**

## **#set TIMEOUT 30000**

## **#exploit**

## 

## **Now open Victim Machine and wireshark in our system to check the performance and packet flow.**

## 

## **2. Syn Flooding Attack Using Hping3 :**

## **Hping3 - It is a network tool, which is used for crafting the packets, testing the firewall, digital footprinting and much more.**

## **Use command #hping3 <victim ip address> --flood**

## **Now open Victim Machine and wireshark in our system to check the performance and packet flow.**

## 

## **Botnets :**

## **A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks.**

## 

## **Ping of Death attack :**

## **The attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.**

## **IPV4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,535 bytes. Some TCP/IP systems were never designed to handle**

## **packets larger than the maximum, making them vulnerable to packets above that size.**

## 

## **Ping of Death Attack Using Hping3 :**

## **#hping3 192.168.195.183 -c 10000000000 -d 999999999 --rand-source --flood -p 21 - We Can Modify this command according to our need and we can use multiple**

## **systems and multiple terminal for this attack.**

## **Now open Victim Machine and wireshark in our system to check the performance and packet flow, or**

## **Check the site status after DDOS:- https://isitdown.us/ https://www.isitdownrightnow.com/**

## 

## **How to Prevent or defend against a DoS or DDoS Attack :**

## **1. Traffic Analysis and Filtering**

## **2. Blackhole or Sinkholing**

## **3. Ip-based Prevention**

## **4. Shutting Down the services**

## 

## **1. Traffic Analysis and Filtering - In this we monitor the data and traffic flowing into our network. We try to filter this.**

## 

## **2. Blackhole or Sinkholing - In this prevention we try to redirect the waste traffic to some other place. Basically we put limit on our system for the coming packet, and**

## **the extra packet will be redirected to other place.**

## **For better understanding we have some videos : https://www.youtube.com/watch?v=mf6OMPNfLN8 https://www.youtube.com/watch?v=yPNKQZar-Fw&ab\_channel=HackerSploit**

## 

## **3. Ip-based Prevention - In this our IDS And IPS helps us in collecting the packet information and prevent the attack. Our IDS will detect the abnormal packets activity**

## **and it will send logs to admin after that admin will block the Malicious Ip. Until in some cases our IPS can protect the attack.**

## **horizontal line**