INTRODUCTION ON

D-DOS

Groups.Hcon.in

Presentation by
RAJKUMAR PATOLIYA

What is d-dos ? ? ?

- The full form of the D-DOS is Distributed Denial of Service.
- The attacks are carried out by flooding site traffic at appoint in a site where it cannot handle traffic.
- The attempt of D-Dos is to make resource(network + machine) unavailable to its intended users.
- Perpetrators of dos attacks mostly on sites or services hosted on high-profile web servers such as banks, credit card gateways and root name servers.

Effect of D-Dos on System

- The targeted machine with external communication request gets saturated so that it cannot respond to the traffic created on servers.
- In general terms, Dos attacks are implemented by either forcing the targeted computers to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the users and the victim so that they can no longer communicate with each other.

Groups.Hcon.in

Symptoms

- Slow network performance is observed.
- Sudden increase in no. of junk files.
- Unavailability of particular website
- Increase in no. of spam mails received
- Disconnection of internet connection (wired or wireless)

Groups.Hcon.in

HOW DO D-DOS ATTACK WORK ?

- Hacker or Clint locates large number of vulnerable system on the network.
- Clint installs the D-DOS remote control program on the system, creating a slave system.
- Hackers have the control on the entire system by through master device. It directs the slave to attack on target.
- During attack a no. of large data packets are sent by slaves to target system.
- Due to this the system gets shutdown or users are denied access And system finally gets because of large stream of packets.

Groups.Hcon.in

TYPES OF D-DOS

1) BUFFER OVERFLOW ATTACKS
2) SYN FLOOD ATTACKS
3) TEARDROP ATTACKS
4) SMURF ATTACKS
5) VIRUSES/WORMS

BUFFER OVERFLOW ATTACKS

- Poorly written code is the one of the best way for the occurrence of BOA.
- Here program do not see the size of the data to be inserted into buffer.
- The attackers attacks by changing the program variable to no. larger than expected and executing the arbitrary code

Groups.Hcon.in

SYN FLOOD ATTACKS

- Normally the SYN (Synchronize Sequence number) packets are sent from system A to System B.
- In return the system B send the SYN/ACK (synchronization acknowledged) packets to system A.
- Here hostile Clint makes all SYN request appear valid but because of the fake IP address the server cannot shutdown without sending RST (Reset) packets back to hostile Clint.
- Before the time runs out the another SYN request arrives, these type of connection is known as half open connection.

Groups.Hcon.in

TEARDROP ATTACKS

- The larger data packet are broken into the small data fragments so to send to the network.
- Many older kernels checked for fragments that were too large, but did not check for and reject fragments that were too small. Hackers took advantage of this vulnerability and would construct packets that were smaller than acceptable, causing systems to reboot or halt.

SMURF ATTACKS

- An amplifying or intermediary networks broadcast address receives forged ICMP (Internet Control Message Protocol)packets from the attacker.
- The packets appear as though the victim has initiated the request, causing all systems on the amplifying network to send a response to the victim.
- Hence it is named as Smurf attack.

VIRUSES-WORMS

- Viruses are programs or “malware” code snippets that infect systems and can be harmless or destructive. Self-replicating viruses are worms that consume resources.

TYPES OF D-DOS PROGRAMS

1) TFN (Tribal flood network).
2) Trin00
3) TFN2K
4) Stacheldrahat etc.

D-DOS PREVENTION METHOD

- There is no specific defensive method for the prevention against DDoS attacks.
- Scanning system on regular basis, keep patches up-to-date, close unneeded services and implementing firewall filtering is the good starting point to secure the system.
- The one of the biggest problem in DDoS attacks is spoofed IP address hence, egress filtering must be put on a routers to solve this issue.

Groups.Hcon.in

FEEDBACK

- I M INTRESTED IN LISTENING FROM YOUR SIDE…..PLEASE !!!