Denial of Service

IT 444 – Network Security

Overview

- Attempt to flood a network in order to prevent legitimate traffic
- Attempt to disrupt connections in order to disrupt access to a service
- Attempt to prevent a particular user from accessing a service
- Attempt to disrupt service to a specific system

DOS Impact

- Consumption of scarce and nonrenewable resources
- Consumption of bandwidth, disk space, CPU time, or data structures
- Actual physical destruction or alteration of network components
- Destruction of programming and files in a computer system

DOS Impact

- Network connectivity: the goal is to stop hosts or networks from communicating on the network or to disrupt network traffic
- A fraggle attack results in the con- sumption of the available network bandwidth between the two machines, possibly affecting network connectivity for all machines
- An intruder may attempt to consume disk space in other ways, including generating excessive e-mail messages, or by placing files in anonymous FTP areas or network shares
- Alteration of the configuration of a computer, or the components in the network, may disrupt the normal functioning of the system. For instance, changing information stored in a router can disable a network

Type of attacks - Smurf

- A network-level attack against a host
- The attacker sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses with a spoofed source IP of a victim
- If the routing device delivering traffic to those broadcast addresses accepts the IP broadcast, hosts on that IP network will take the ICMP echo request and will each reply to it with an echo reply, multiplying the traffic by the number of hosts that are responding

Smurf Attack

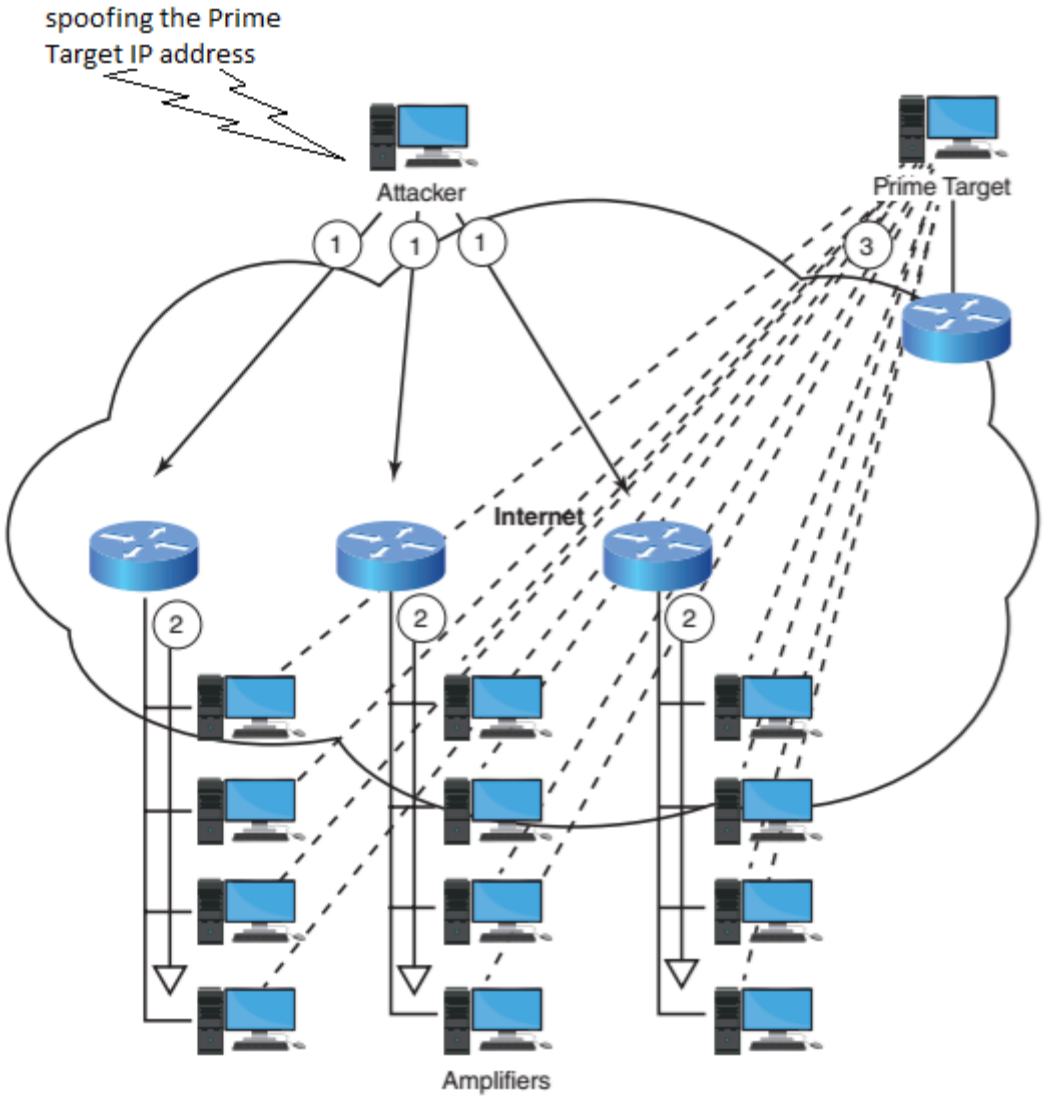


Figure 6-1 In this attack, the systems on the network respond to the spoofed IP address.

Other DOS Types

- Buffer Overflow: the most common attack. Sends excessive data to an application that either brings down the application or forces the data being sent to the host system app => crash a vulnerable system with excessive traffic to an application
- Ping of Death: sends an ICMP echo packet of > 65,536 bytes allowed by the IP protocol. Packets sent over TCP/IP can be broken down into smaller segments and reassembled at the destination. Many operating systems do not know what to do when they receive an oversized packet, so they freeze, crash, or reboot

Teardrop DOS

- Teardrop: IP requires that a packet that is too large for the next outgoing router interface to handle be broken up into fragments. Attackers can exploit this vulnerability by manipulating the offset value of the second or latter fragment(s) to overlap with a previous fragment. The receiving system is not able to reassemble the packet and may crash, hang, or reboot

SYN Attack

- The attacker sends a series of SYN requests to a target machine.
- The attack creates incomplete TCP connections that use up network resources.
- Using 3-way handshake - SYN, SYN/ACK and ACK.
- In a SYN attack, the hacker sends a fake SYN request to the server
- When the server sends an ACK to the client, a response ACK is never sent.
- This leaves the server waiting to complete the connection.

Bot

- Bots are software applications that run automated tasks over the Internet.
- Bots can also be used to coordinate denial-of-services attacks.
- The main purpose of a bot is to collect data
- It is possible for a person whose computer has been com-promised to be charged with click fraud, despite being unaware of the fraud being perpetrated via his or her system

Botnet

- Botnets can be used for both positive and negative ends
- A relatively small botnet of only 1,000 bots has a combined band- width that is larger than the Internet connection of most corporate systems
- Botnets, also called agents that an intruder can send to a server system to perform some illegal activity
- Attackers can use botnets to perform
  - Distributed denial-of-service attacks
  - Spamming: E-mail addresses can be
  - harvested from Web pages or some other sources.
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Manipulating online polls and games
  - Mass identity theft

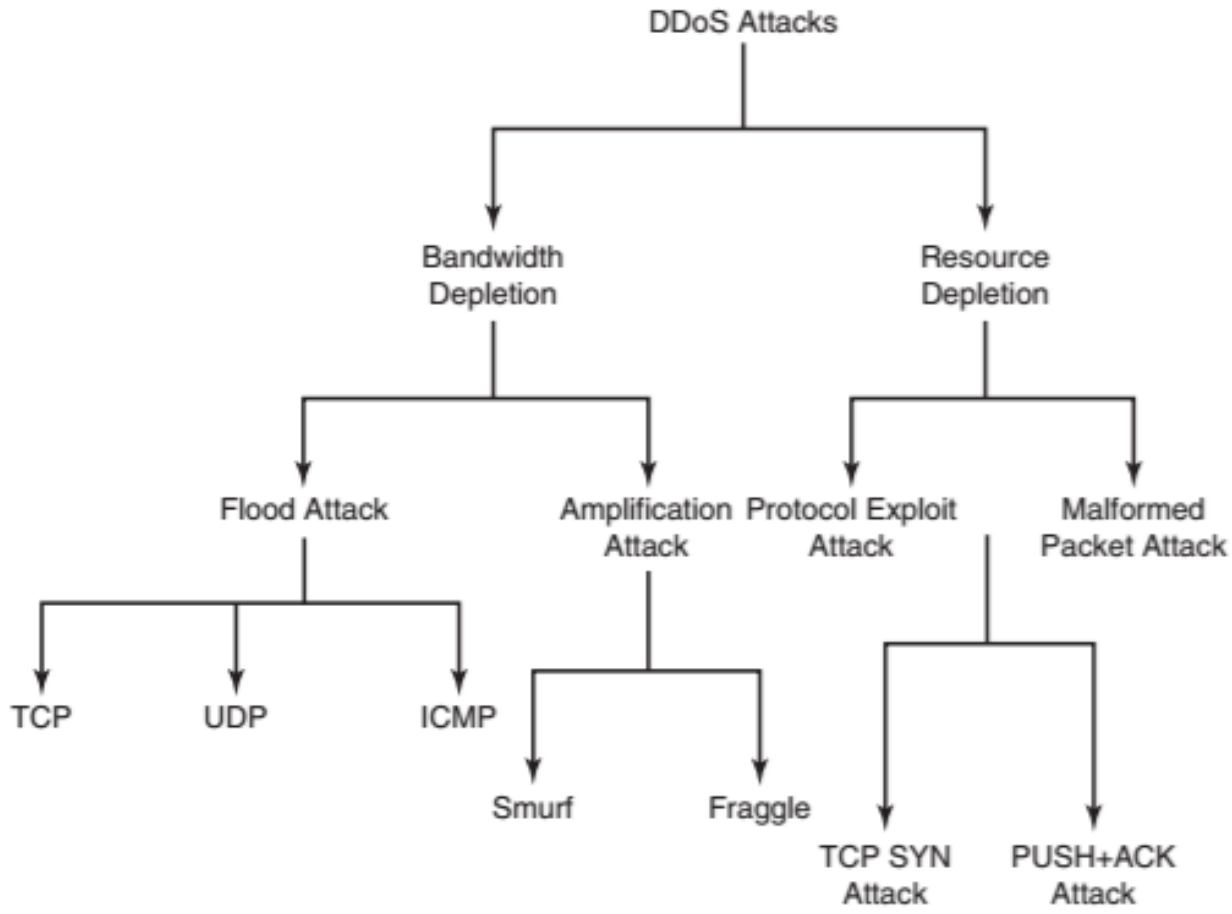
How Bots infect

- First runs by copying itself to the system direc- tory. Then it adds to the following registry entries so it automatically starts when Windows boots:
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run;
  - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- Massive spreading: scan for network machines to infect by probing ports 139, Microsoft for RPC locator service and 445, SMB
- Connect Back to IRC: establish a direct channel and attackers can remotely control the victim's computer
- Attacker Takes Control of the Victim's Computer

Conduct a DDoS Attack

- Write a virus that will send ping packets to a target network/Web site.
- Infect a minimum of 30,000 computers with this virus and turn them into “zombies.”
- Trigger the zombies to launch the attack by sending wake-up signals to the zombies or by activating them with certain data.
- The zombies will start attacking the target server until it is disinfected.

DDOS Taxonomy



The reflected DOS Attacks

- The TCP three-way handshake vulnerability is exploited.
- Zombies send out a large number of SYN packets with the target system as the IP source address
- Any widely accessible Internet server can be used as a reflection server.
- A simple script can be used to collect a large number of Internet routers' IP addresses
- The list of reflection servers can be constantly maintained with- out difficulty by bouncing a valid, nonspoofed SYN packet off the machine.
- The answering SYN/ACK will confirm the machine's presence and its availability to participate in future reflection attacks unknowingly.
- Each SYN spoofing attack host will be used to distribute fake SYN packet to all reflector

Reflective DNS Attacks

- Uses a botnet to send a large number of queries to open DNS servers
- These queries are spoofed to look like they have come from the target, and the DNS server replies to that network address
- If DNS servers are used to do malicious work, it offers key bene- fits to attackers
  - It hides the systems and makes it harder for the victim to find the original source of the attack.
- Stop the more-common bot-delivered attack by blocking traffic from the attacking machines. But blocking queries from DNS servers is problematic

DOS Prevention

- Prevent installation of distributed attack tools on the systems.
- Prevent origination of IP packets with spoofed source addresses.
- Monitor the network for signatures of distributed attack tools.
- Employ stateful inspection firewalling.

Discussion of Labs

- Reading: Chapter 6