Denial Of Service

- The goal of a denial of service attack is to deny legitimate users access to a particular resource.
- An incident is considered an attack if a malicious user intentionally disrupts service to a computer or network resource.
- Resource exhaustion (consume all bandwidth, disk space)

Types of attacks

- There are three general categories of attacks.
  - Against users
  - Against hosts
  - Against networks

Local DOS against hosts

- fork() bomb
- intentionally generate errors to fill logs, consuming disk space, crashing
- The power switch!!

Local DOS:Countermeasures

- partition disks
- disk quotas
- set process limits
- monitor system activity/CPU/Disk Usage
- Physical Security

Network Based Denial of Service Attacks

- UDP bombing
- tcp SYN flooding
- ping of death
- smurf attack

- Most involve either resource exhaustion or corruption of the operating system runtime environment.

UDP bombing

- Two UDP services: echo (which echos back any character received) and chargen (which generates character) were used in the past for network testing and are enabled by default on most systems.
- These services can be used to launch a DOS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic.

UDP service denial: Countermeasures

- Disable echo, chargen and all other unused services whenever possible, such /etc/inetd.conf on Unix, and “no udp small-services” on Cisco IOS.

- Filter UDP traffic at the firewall level. Only allow legitimate traffic such as UDP port 53 (DNS) – Of course, remember the firewalls lecture

Windows UDP attacks

- NewTear, Newtear2, Bonk, and Boink are tools that exploit the same weakness in the Microsoft Windows 9.x/NT TCP/IP stack.
- The attacker sends the victim a pair of malformed IP fragments which get re-assembled into an invalid UDP datagram. Upon receiving the invalid datagram, the victim host “blue-screens” and freezes or reboots (The pathologic offset attack)
- Countermeasure: Apply vendor patches

TCP SYN Flooding

- Also referred to as the TCP “half-open” attack
- To establish a legitimate TCP connection:
  - the client sends a SYN packet to the server
  - the server sends a SYN-ACK back to the client
  - the client sends an ACK back to the server to complete the three-way handshake and establish the connection

TCP SYN Flooding (cont’d)

- The attack occurs by the attacker initiating a TCP connection to the server with a SYN. (using a legitimate or spoofed source address)
- The server replies with a SYN-ACK
- The client then doesn’t send back a ACK, causing the server to allocate memory for the pending connection and wait.

(If the client spoofed the initial source address, it will never receive the SYN-ACK)

TCP SYN Flooding: Results

- The half-open connections buffer on the victim server will eventually fill
- The system will be unable to accept any new incoming connections until the buffer is emptied out.
- There is a timeout associated with a pending connection, so the half-open connections will eventually expire.
- The attacking system can continue sending connection requesting new connections faster than the victim system can expire the pending connections.

TCP SYN Flooding: Countermeasures

- Apply vendor’s patches.
  - Most OS vendors have minimized the risks in newer OS releases and have patches for older releases.
- Install Ingress/Egress router filters to prevent some IP spoofing locally.

Ping of Death

- The TCP/IP specification allows for a maximum packet size of 65,536 octets.
- The ping of death attack sends oversized ICMP datagrams (encapsulated in IP packets) to the victim.
- Some systems, upon receiving the oversized packet, will crash, freeze, or reboot, resulting in denial of service.
- Countermeasures: Most systems are now immune, but apply vendor patches if needed.

When Smurfs go bad!!

- A smurf attack consists of a host sending an ICMP echo request (ping) to a network broadcast address.(usually network addresses with the host portion of the address having all **1**s)

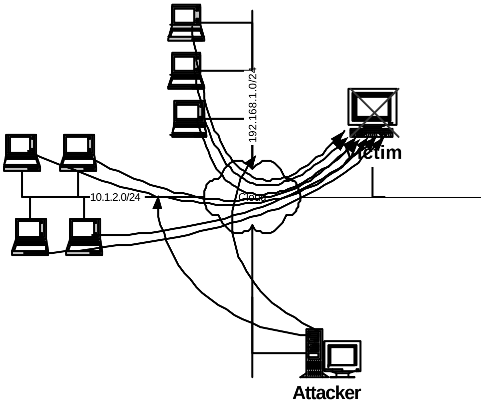
- Every host on the network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic.

Is it much farther Papa Smurf?

- There are 3 players in the smurf attack
  - the attacker,the intermediary (which can also be a victim) and the victim
- In most scenarios the attacker spoofs the IP source address as the IP of the intended victim to the intermediary network broadcast address.
- Every host on the intermediary network replies, flooding the victim and the intermediary network with network traffic.
- Result: Performance may be degraded such that the victim, the victim and intermediary networks become congested and unusable

Smurf Attack Example

Smurf Example



1. Attacker sends ICMP packet with spoofed source IP

Victim→10.1.2.255

2. Attacker sends ICMP packet with spoofed source IP

Victim→192.168.1.255

3. Victim is flooded with ICMP echo responses

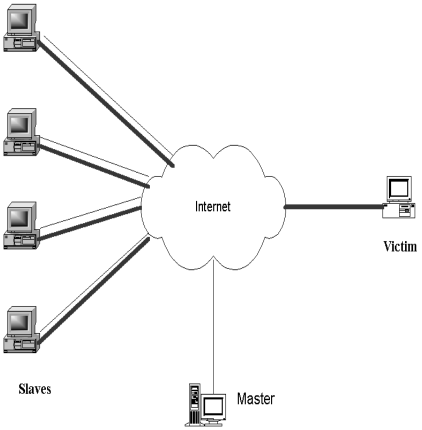
4. Victim hangs?

Smurf: Countermeasures

- Configure routers to deny IP broadcast traffic onto your network from other networks. In almost all cases, IP-directed broadcast functionality is not needed.
- Configure hosts (via kernel variable) to NOT reply to a packet sent to a broadcast address
- Configure Ingress/Egress filters on routers to counteract IP address spoofing.

Distributed Denial of Service Attacks (DDOS)

- Attacker logs into Master and signals slaves to launch an attack on a specific target address (victim).
- Slaves then respond by initiating TCP, UDP, ICMP or Smurf attack on victim.



Distributed Denial of Service Attacks (DDoS)

- trin00 (WinTrinoo)
- Tribe Flood Netowrk (TFN) (TFN2k)
- Shaft
- stacheldraht
- Mstream

Trin00

- Affects Windows and many Unix OS's
- Attacker scans for exploits, gains root, and downloads Trin00 programs.
- Attacker->Master->Daemon hierarchy
  (One -> More -> Many)
- Attacker can telnet into a Master to initiate commands, which are distributed amongst its Daemons.

Trin00 (con't)

- Communication between Master->Daemon through a password-protected cleartext UDP-based protocol.
- Daemons attack the target with a UDP or TCP packet bombardment.
- Used in the February 2000 attacks on eBay, Amazon, CNN, etc.

Real World DDoS

```
4081   0.224610 119.226.89.96 -> poor.student.1.83 TCP 33081 > 60785 [SYN]
    Seq=3693150756 Ack=0 Win=32768 Len=0
4082   0.224610 poor.student.1.83 -> 223.144.66.65 TCP 52284 > 19586 [RST, ACK]
    Seq=0 Ack=423694111 Win=0 Len=0
4083   0.224610  3.41.60.116 -> poor.student.2.231 TCP 5594 > 40940 [SYN]
    Seq=2132997225 Ack=0 Win=32768 Len=0
4084   0.224610 poor.student.1.83 -> 50.180.94.71 TCP 33289 > 11952 [RST, ACK]
    Seq=0 Ack=1790973261 Win=0 Len=0
4085   0.224610 244.214.39.108 -> poor.student.2.231 TCP 38802 > 23759 [SYN]
    Seq=747020069 Ack=0 Win=32768 Len=0
4086   0.224610 poor.student.1.83 -> 198.183.172.81 TCP 57223 > 43146 [RST, ACK]
    Seq=0 Ack=3749566807 Win=0 Len=0
4087   0.224610 64.81.138.119 -> poor.student.1.83 UDP Source port: 1026
    Destination port: 24661
4088   0.224610 poor.student.2.231 -> 96.247.9.94  TCP 48931 > 50749 [RST, ACK]
    Seq=0 Ack=1188357973 Win=0 Len=0
4089   0.224610 103.227.64.42 -> poor.student.1.83 TCP 45715 > 63366 []
    Seq=3389528594 Ack=0 Win=16384 Len=0
4090   0.224610 poor.student.1.83 -> 211.107.218.23 TCP 12666 > 48183 [RST, ACK]
    Seq=0 Ack=2803931407 Win=0 Len=0
4091   0.224610  87.29.46.64 -> poor.student.1.83 TCP 17092 > 47365 [SYN]
    Seq=3446572548 Ack=0 Win=32768 Len=0
4092   0.224610 poor.student.1.83 -> 58.24.148.57 TCP 26667 > 9797 [RST, ACK]
    Seq=0 Ack=3710546447 Win=0 Len=0
4093   0.224610  8.116.40.43 -> poor.student.1.83 TCP 38367 > 32889 [SYN]
    Seq=1914703987 Ack=0 Win=32768 Len=0
4094   0.225448 poor.student.1.83 -> 68.132.173.125 TCP 64470 > 35524 [RST, ACK]
    Seq=0 Ack=1819819023 Win=0 Len=0
4095   0.225448 75.115.186.26 -> poor.student.1.83 TCP 4082 > 29772 [SYN]
    Seq=4245878839 Ack=0 Win=32768 Len=0
```

TFN (2k)

- Smurf attack
- ICMP flood
- SYN flood
- UDP flood
- All three at once

Stackeldraht

- ICMP flood
- SYN flood
- UDP flood
- Smurf attack

Shaft

- ICMP flood
- SYN flood
- UDP flood
- All three at once

DDOS: Countermeasures

- RID:
  - Sends out packets and listens for reply
  - Detects Trinoo, TFN, Stacheldraht
- NIPC - find_ddos tool
  - Runs on local system
  - Detects Trinoo, TFN, TFN2k
- Bindview's Zombie Zapper
  - Tells DDOS slave to stop flooding traffic