Denial of Service

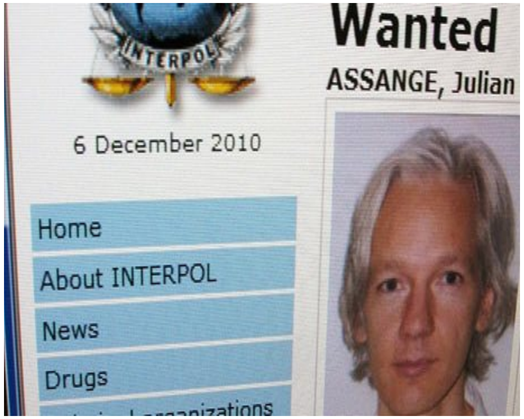
Chapter 11

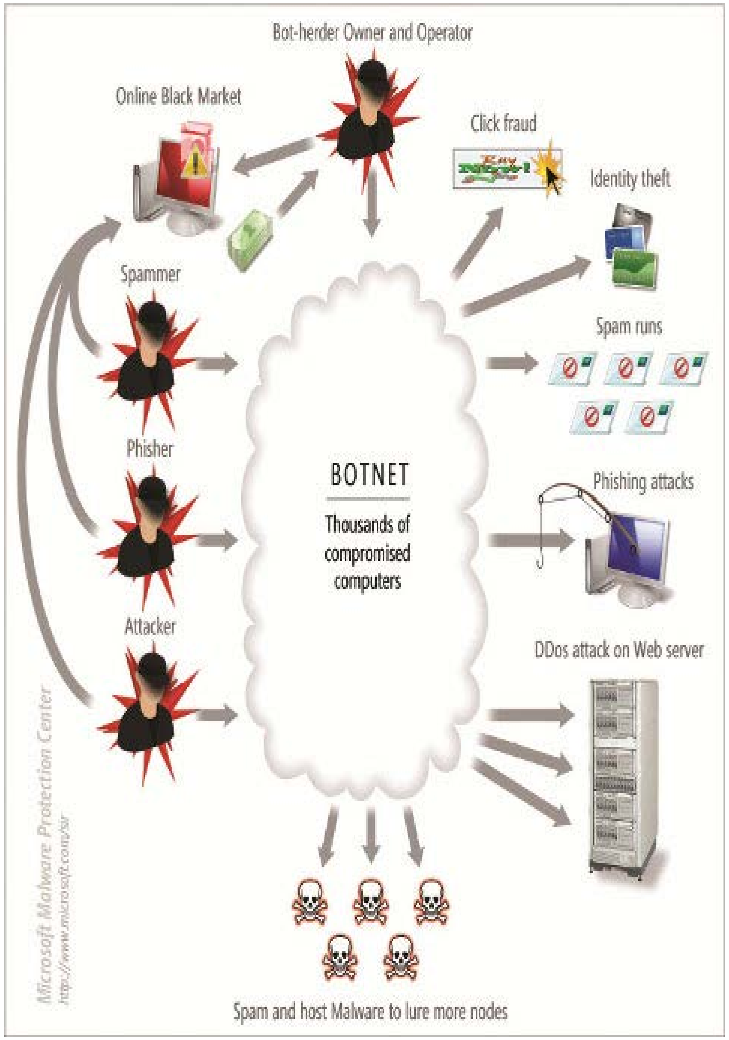
Goals of Denial-of-Service Attacks

- Goal is to deny or disrupt use of resources
- Unavailability of a resource
- Loss of access to a website
- Slow performance
- Increase in spam emails

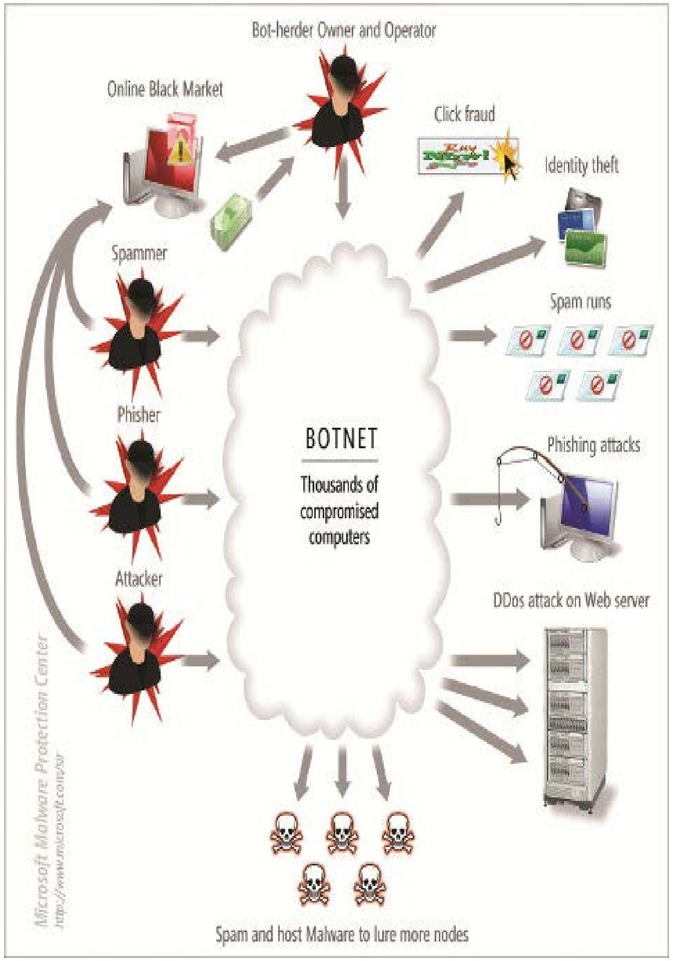
Case Study: WikiLeaks

- After Julian Assange's WikiLeaks release of government information, many financial institutions stopped serving WikiLeaks.
- Hackers targeted these institutions' websites with DoES attacks, making them unavailable to customers.
- The companies ultimately hardened their sites, but hackers had shown they could disrupt major targets.




Bot-herder Owner and Operator
Online Black Market
Click fraud
Identity theft
Spammer
Spam runs
Phisher
BOTNET
Thousands of compromised computers
Phishing attacks
Attacker
DDos attack on Web server
Spam and host Malware to lure more nodes
Microsoft Malware Protection Center
http://www.microsoft.com/sir

Denial-of-Service Goals and Motivations


Bot-herder Owner and Operator
Online Black Market
Click fraud
Identity theft
Spammer
Spam runs
Phisher
BOTNET
Thousands of compromised computers
Phishing attacks
Attacker
DDos attack on Web server
Spam and host Malware to lure more nodes
Microsoft Malware Protection Center
http://www.microsoft.com/sir

- Web server compromise
- Back-end resources
- Network or computer specific
- Extortion via a threat of a DoS attack
- Turf wars and fights between online gangs
- Anticompetition business practices
- Punishment for undesired actions
- Expression of anger and criticism
- Training for other attacks
- Self-induced
- No reason at all

Types of Attacks

A successful DoS attack is a highly noticeable event that makes it a popular weapon of choice for hacktivists, cyber vandals, extortionists, and those looking to make a point.

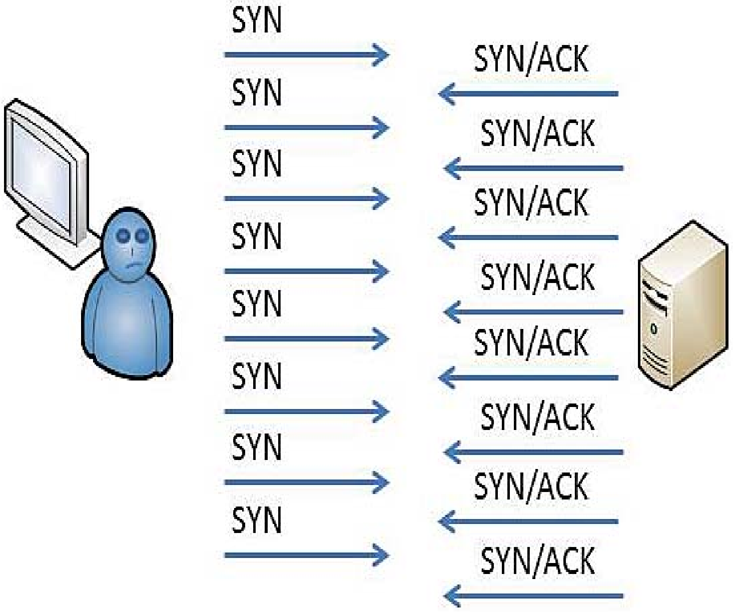
- **Type #1: Volumetric attacks**
  - 65% of attacks
  - Eats resources
  - Hard to mitigate
- **Type #2: Application-layer attacks**
  - 17% of DDoS attacks.
  - HTTP flood is a form

Forms of Denial of Service

- Service request floods
- SYN attack/flood
- ICMP flood attack
- Ping of death
- Teardrop
- Smurf and/or fraggle
- Land

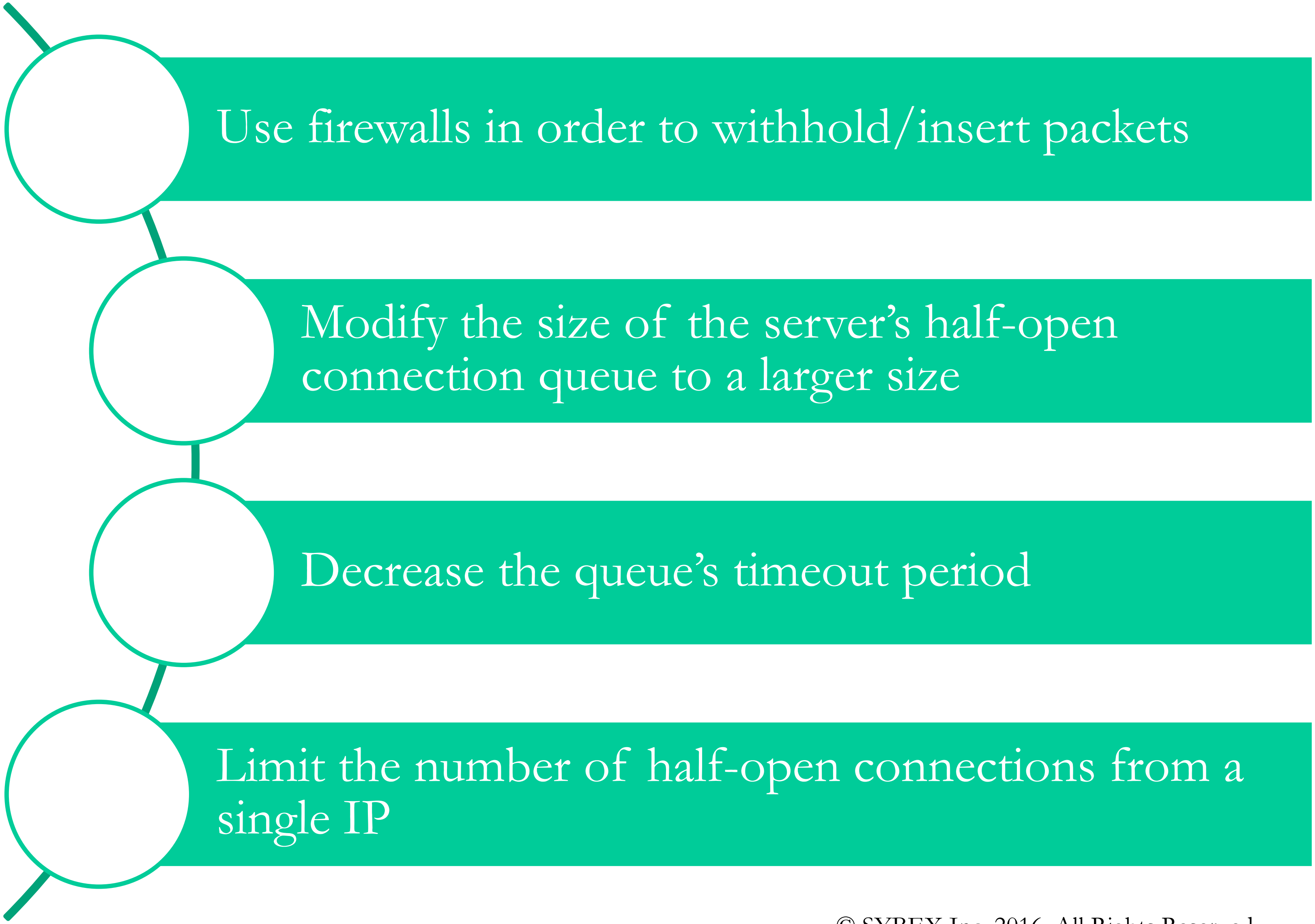
SYN Floods at Work

The basic idea behind SYN flooding utilizes the three-way handshake that begins with a user sending a “synchronize” (SYN) message to the server.



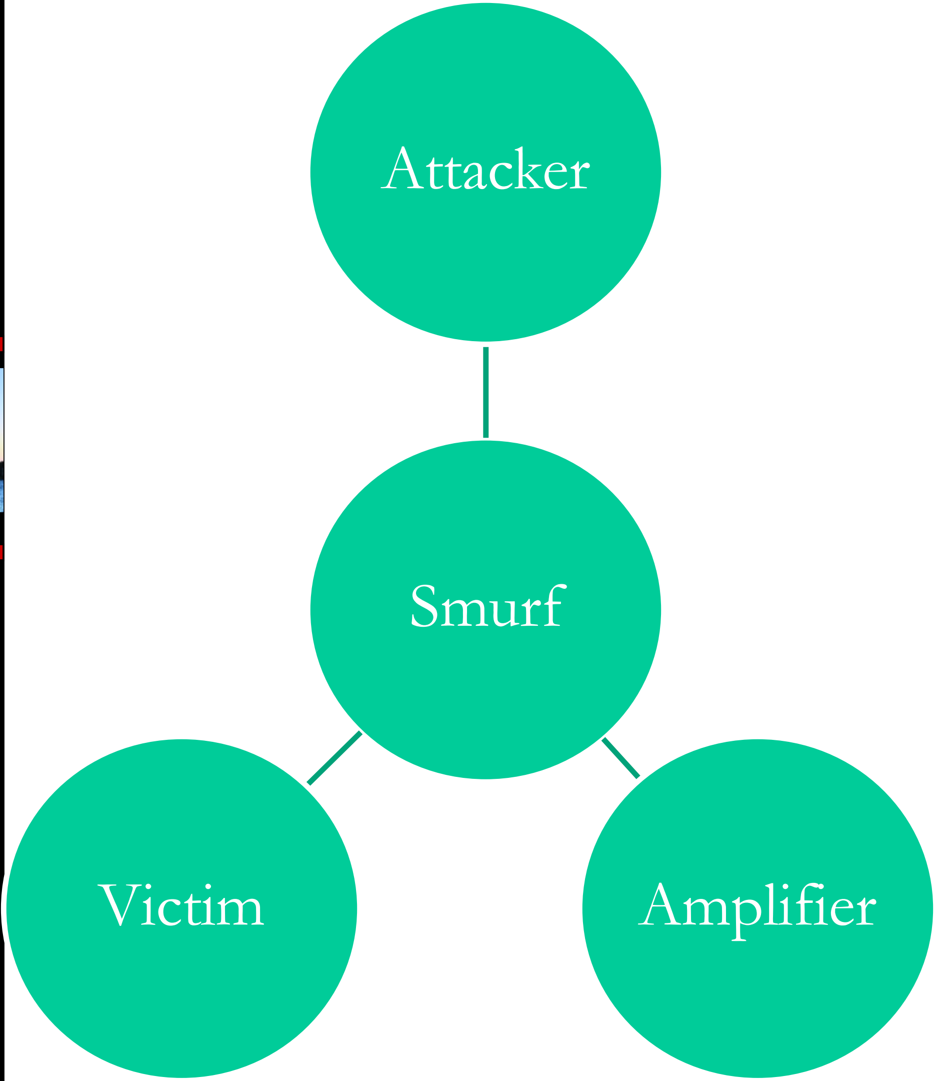
- Attacker floods server with SYN packets with spoofed source address
- Server responds with SYN/ACK reply to fake source address
- No ACK reply server must wait until half-open connection times out
- Prevents legitimate users from accessing the server

SYN Flood Countermeasures



- Use firewalls in order to withhold/insert packets
- Modify the size of the server's half-open connection queue to a larger size
- Decrease the queue's timeout period
- Limit the number of half-open connections from a single IP

Smurf Attack

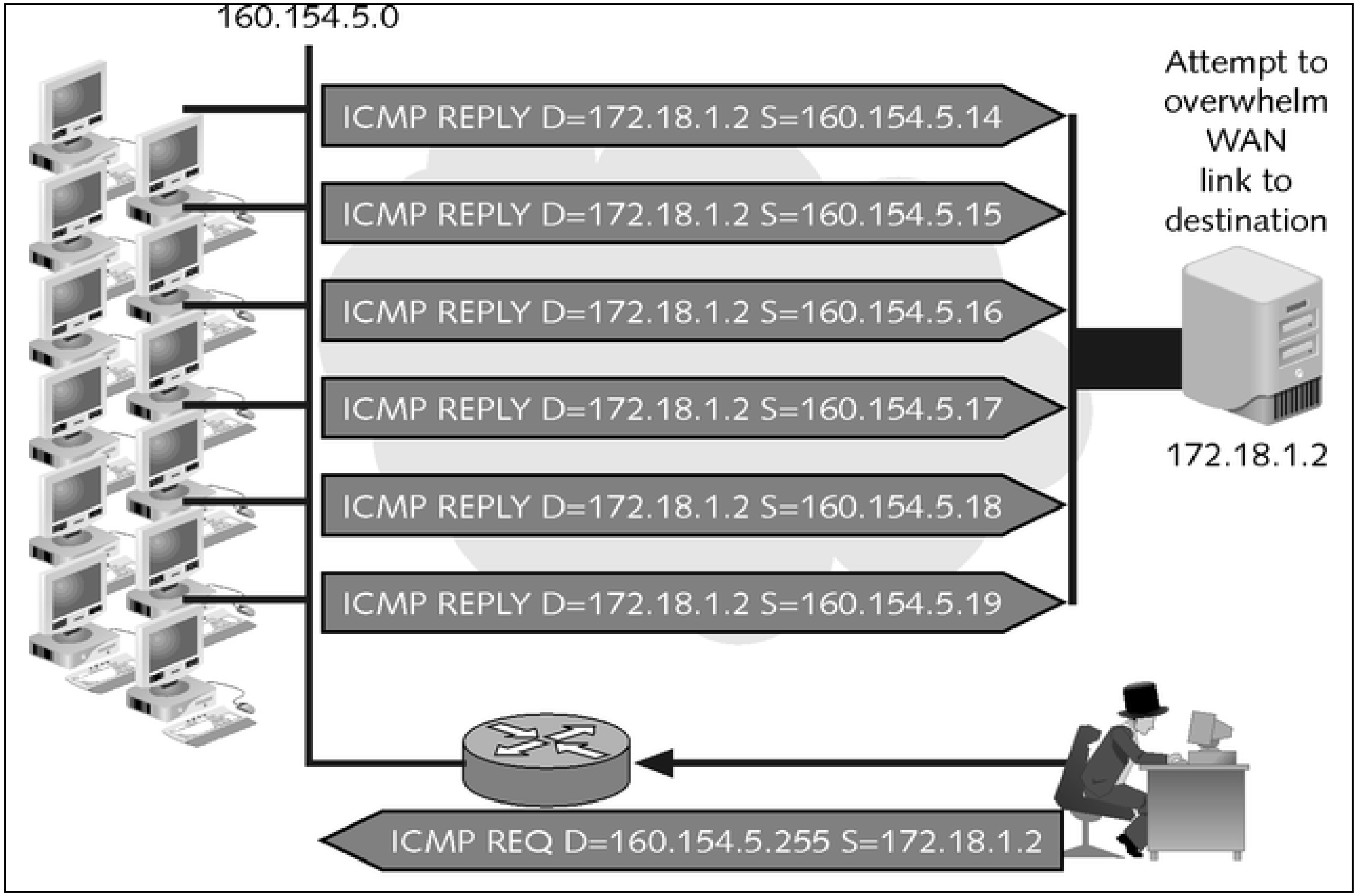


A misconfigured router forwarding the broadcast request to the subnet

Machines that will respond to this ICMP broadcast request

Note that there is not much a victim can do about this attack since the link is simply overloaded with packets.

Anatomy of a Smurf Attack


160.154.5.0
ICMP REPLY D=172.18.1.2 S=160.154.5.14
ICMP REPLY D=172.18.1.2 S=160.154.5.15
ICMP REPLY D=172.18.1.2 S=160.154.5.16
ICMP REPLY D=172.18.1.2 S=160.154.5.17
ICMP REPLY D=172.18.1.2 S=160.154.5.18
ICMP REPLY D=172.18.1.2 S=160.154.5.19
Attempt to overwhelm WAN link to destination
172.18.1.2
ICMP REQ D=160.154.5.255 S=172.18.1.2

Steps Leading to a Smurf Attack

- Huge numbers of ICMP requests are sent to the victim’s IP address.
- The source destination IP address is spoofed.
- The hosts on the victim’s network respond to the ICMP requests.
- This creates a significant amount of traffic on the victim’s network, resulting in consumption of bandwidth and ultimately causing the victim’s server to crash.

Countermeasures for Smurf Attacks

The router should be configured so that it does not forward directed broadcasts onto networks.

Servers should be configured to not respond to a directed broadcast request.

The victim’s ISP must take some actions to block ICMP Echo Reply floods.

Fraggle Attack

- **Floods a target with UDP packets**
- **Targets packets toward a victim**
- **Uses intermediate network to amplify attack**
- **Much like smurf attack but based on UDP**

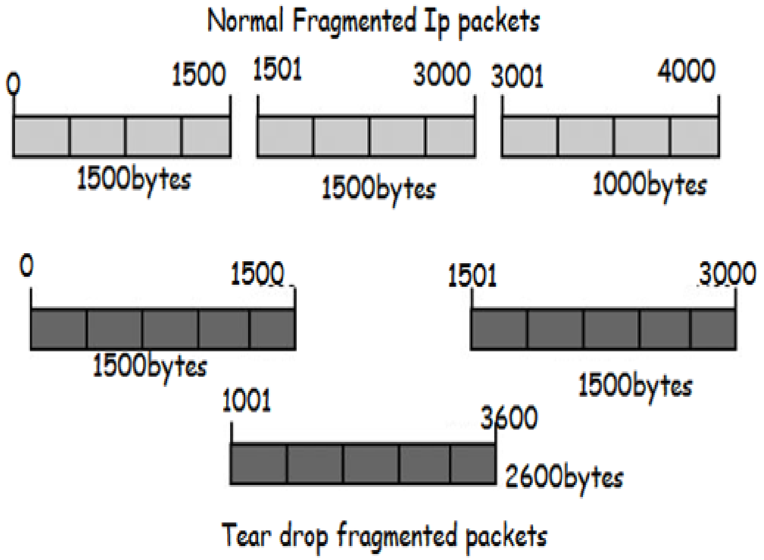
Note that a fraggle attack is a variation of a smurf attack where an attacker sends a large amount of UDP traffic to an IP broadcast address, with the intended victim's spoofed source IP address.

Ping of Death

- Uses IP packet fragmentation techniques to crash remote systems
- Transmits large ICMP packets (> 65,535 bytes) to victim host
- IP packet fragmented into Ethernet frames
- When fragments are reassembled, large size causes crash or lock-up
- Modern systems typically not vulnerable

Teardrop Attacks

In the teardrop attack, the attacker's IP address puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.



Exploits fragmentation process

Specifies illogical offsets

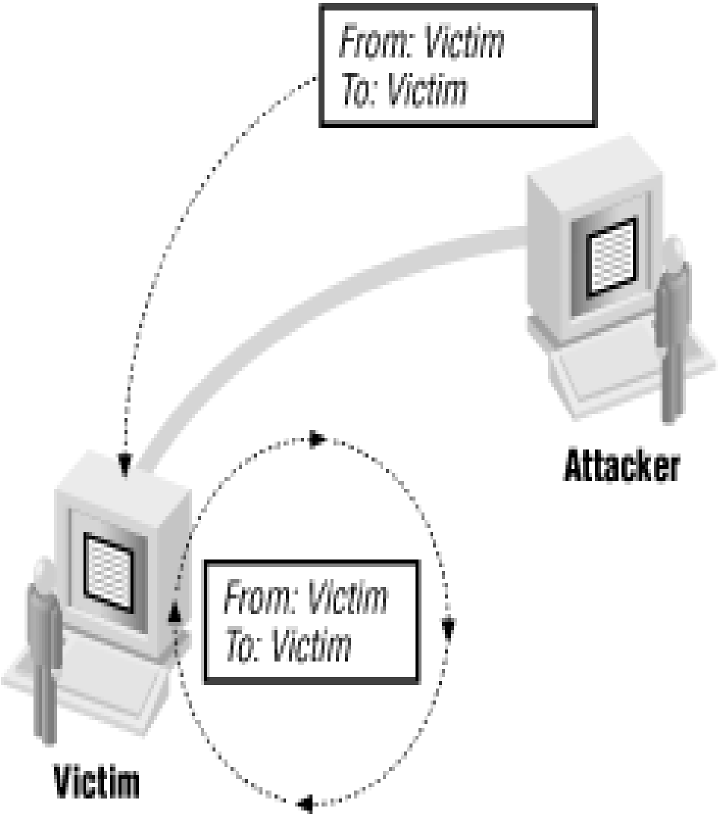
Receiving system will reassemble packet

Illogical offsets can cause system crash

Older systems tend to be targets

Newer systems usually do not have this problem

Land Attack



- Looks similar to Syn-Flood
- Sometimes referred to as “infinite loop” attack
- Crashes a system by sending it a forged packet
- Packet has source and destination set to the victim’s IP address
- Makes system think it is sending itself a message
- Can crash or slow a system
- Newer systems not vulnerable

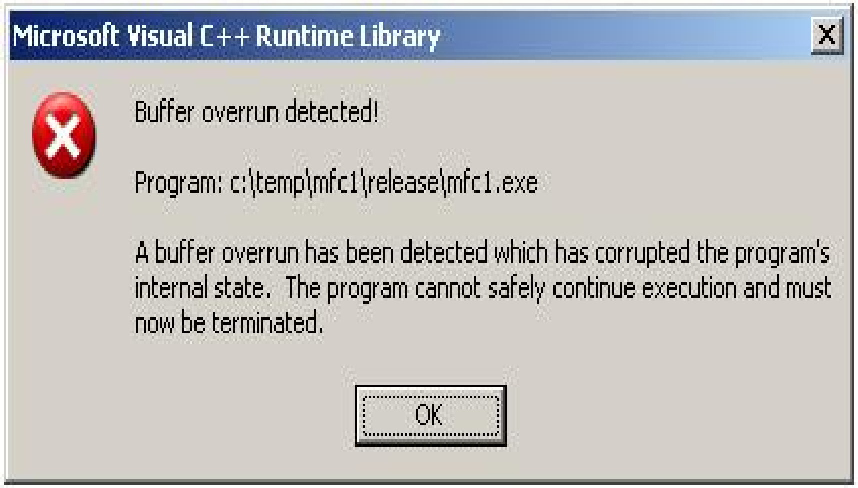
Permanent Denial of Service

By exploiting security flaws or misconfigurations, permanent denial of service (PDoS) can destroy the firmware and/or basic functions of system.

- Also known a Permanent Denial of Service (PDoS)
- Phlashing is a form
- Running a highly virtualized environment
- Organizations highly dependent on IoT
- Organizations with centralized security gateways
- Organizations that are considered critical infrastructure

A Word About Buffer Overflows

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.



Buffer overrun detected!

Program: c:\temp\mfc1\release\mfc1.exe

A buffer overrun has been detected which has corrupted the program's internal state. The program cannot safely continue execution and must now be terminated.

Occurs when a program attempts to store data in memory

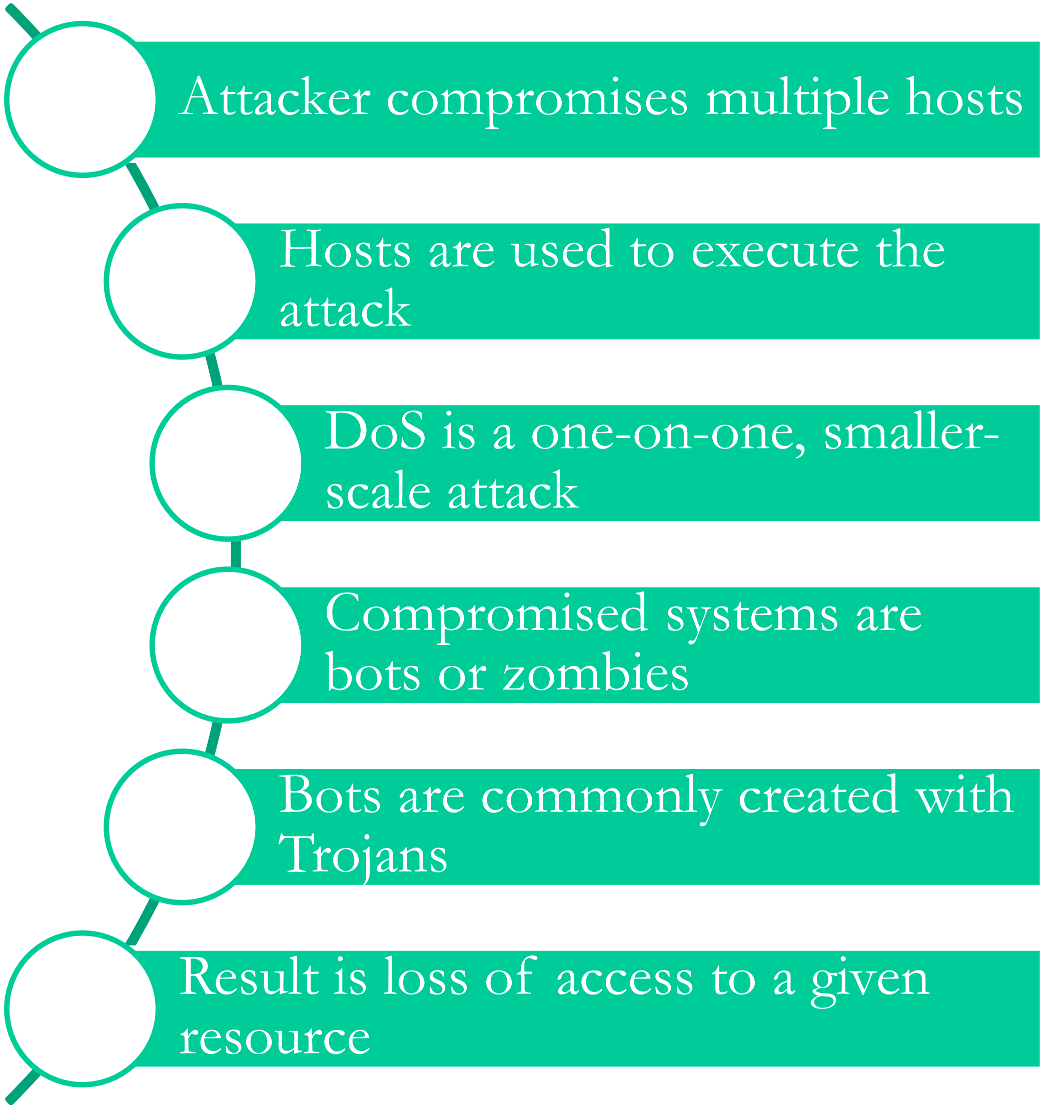
Can occur because of programming errors

Can be uncovered in any software

Usually are patched when discovered

DDoS Attacks

A standard DoS attack can be launched from a single malicious client, whereas a DDoS attack uses a distributed group of computers to attack a single target.



- Attacker compromises multiple hosts
- Hosts are used to execute the attack
- DoS is a one-on-one, smaller-scale attack
- Compromised systems are bots or zombies
- Bots are commonly created with Trojans
- Result is loss of access to a given resource

Defending Against DoS

- Disabling unnecessary services
- Using anti-malware
- Enabling router throttling
- Using a reverse proxy
- Enabling ingress and egress filtering
- Degrading services
- Absorbing the attack

DDoS and DoS Tools

- LOIC, HOIC
- XOIC
- HULK
- UDP Flooder
- RUDY
- ToR's Hammer
- Pyloris
- OWASP Switchblade
- DAVOSET
- GoldenEye HTTP DoS Tool
- THC-SSL-DOS
- DDOSIM: Layer 7 DDoS Simulator

Summary

- Denial-of-service attacks
- How denial-of-service attacks work