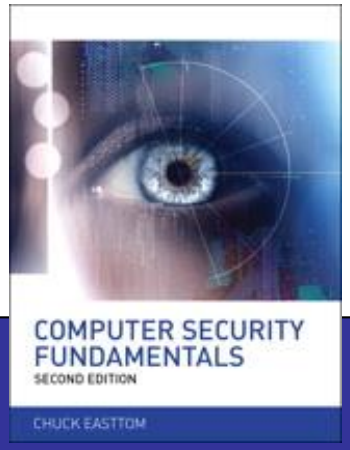
Computer Security Fundamentals

by Chuck Easttom

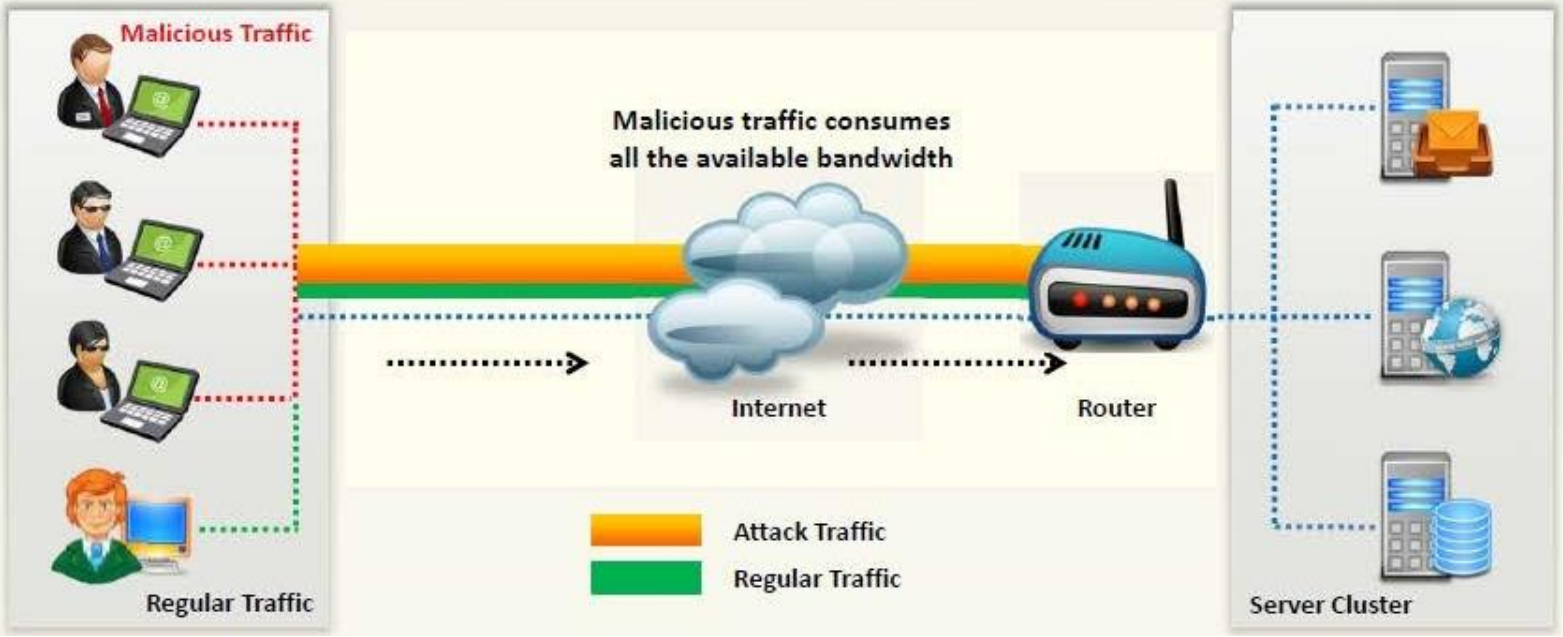


Chapter 4 Objectives

- Understand how DoS attacks are accomplished
- Know how certain DoS attacks work
- Protect against DoS attacks
- Defend against specific DoS 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 **non-legitimate service requests or traffic** to overload its resources
- DoS attack leads to **unavailability of a particular website** and **slow network performance**



WHAT IS DENIAL OF SERVICE ATTACK?

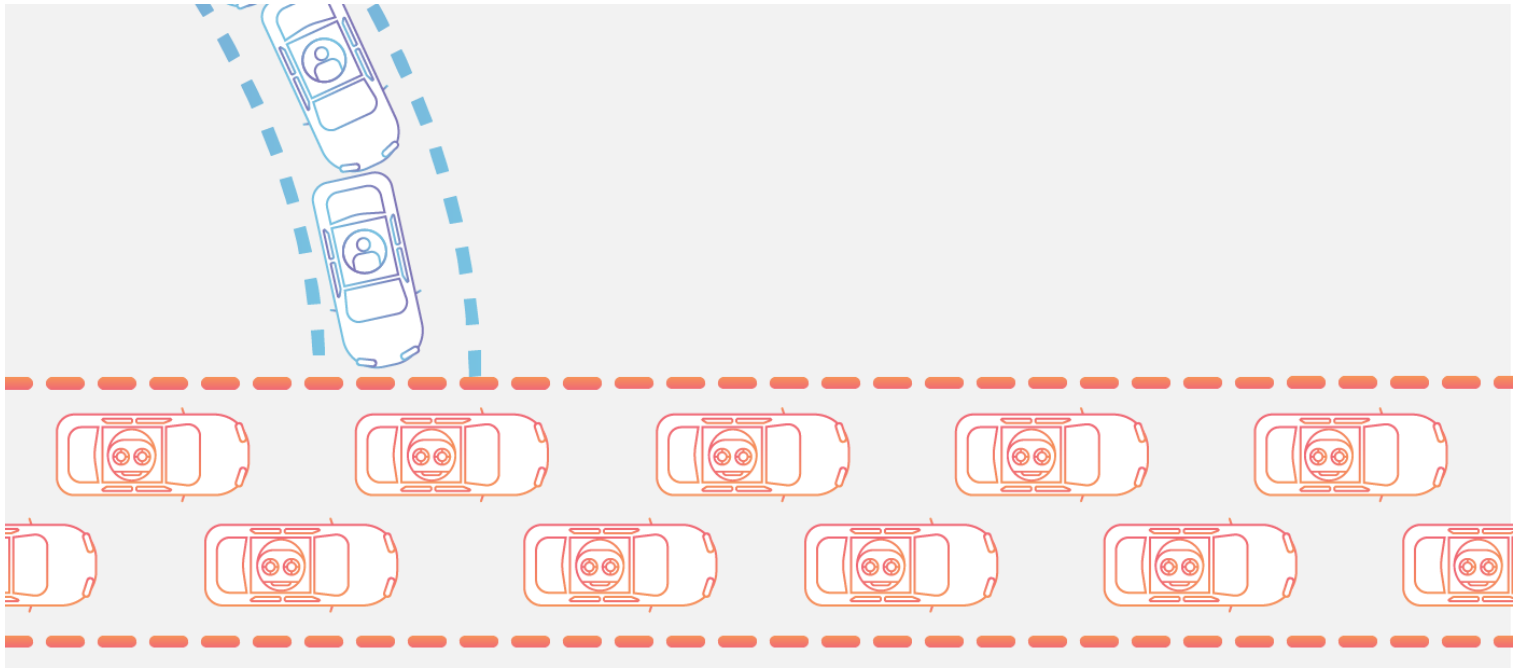
- ***D****enial-****o****f-****s****ervice attack,* is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

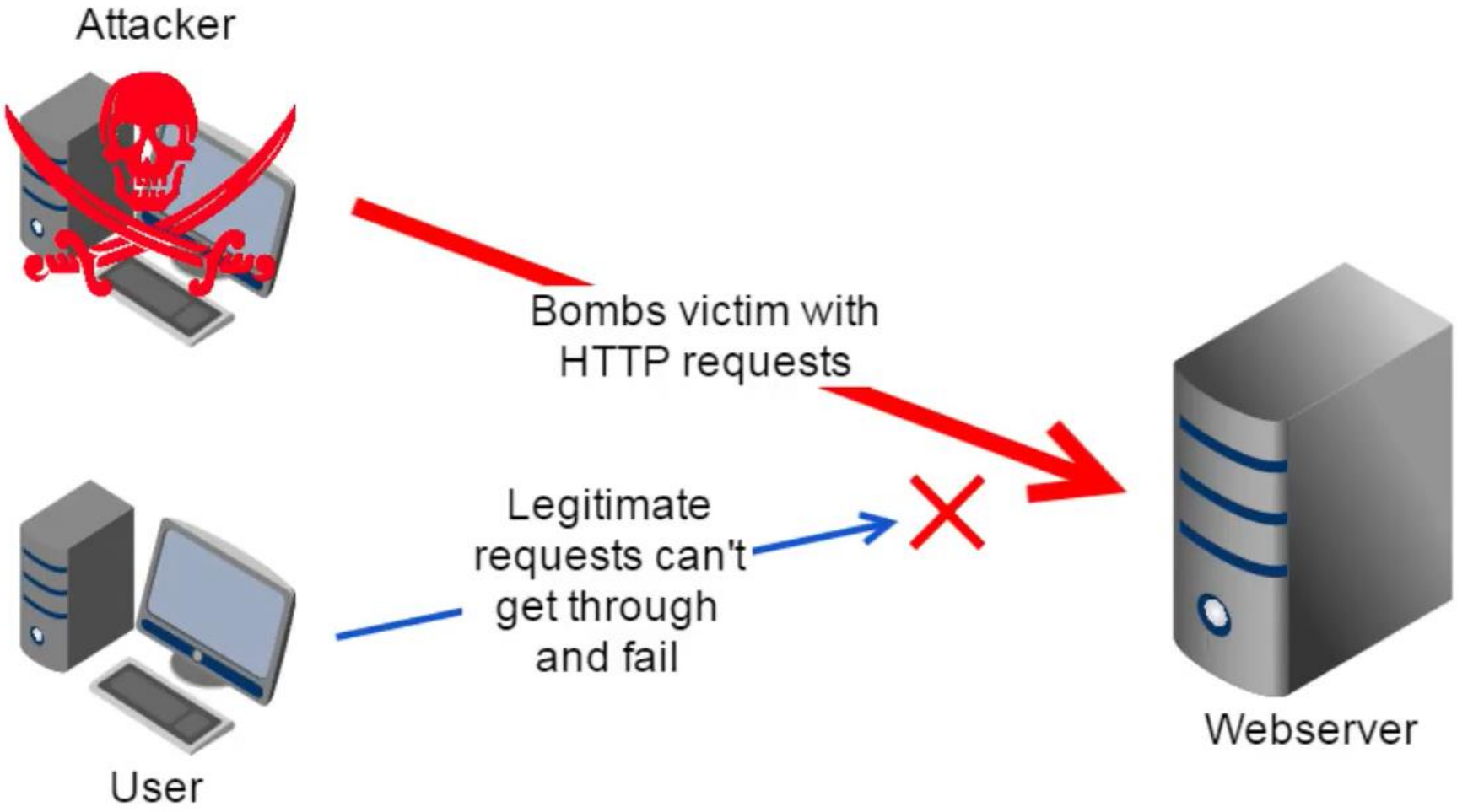
- DoS attack, **d**enial-**o**f-**s**ervice attack, is an explicit attempt to make a computer resource unavailable by either injecting a computer virus or flooding the network with useless traffic.

WHAT IS DENIAL OF SERVICE ATTACK? cont'

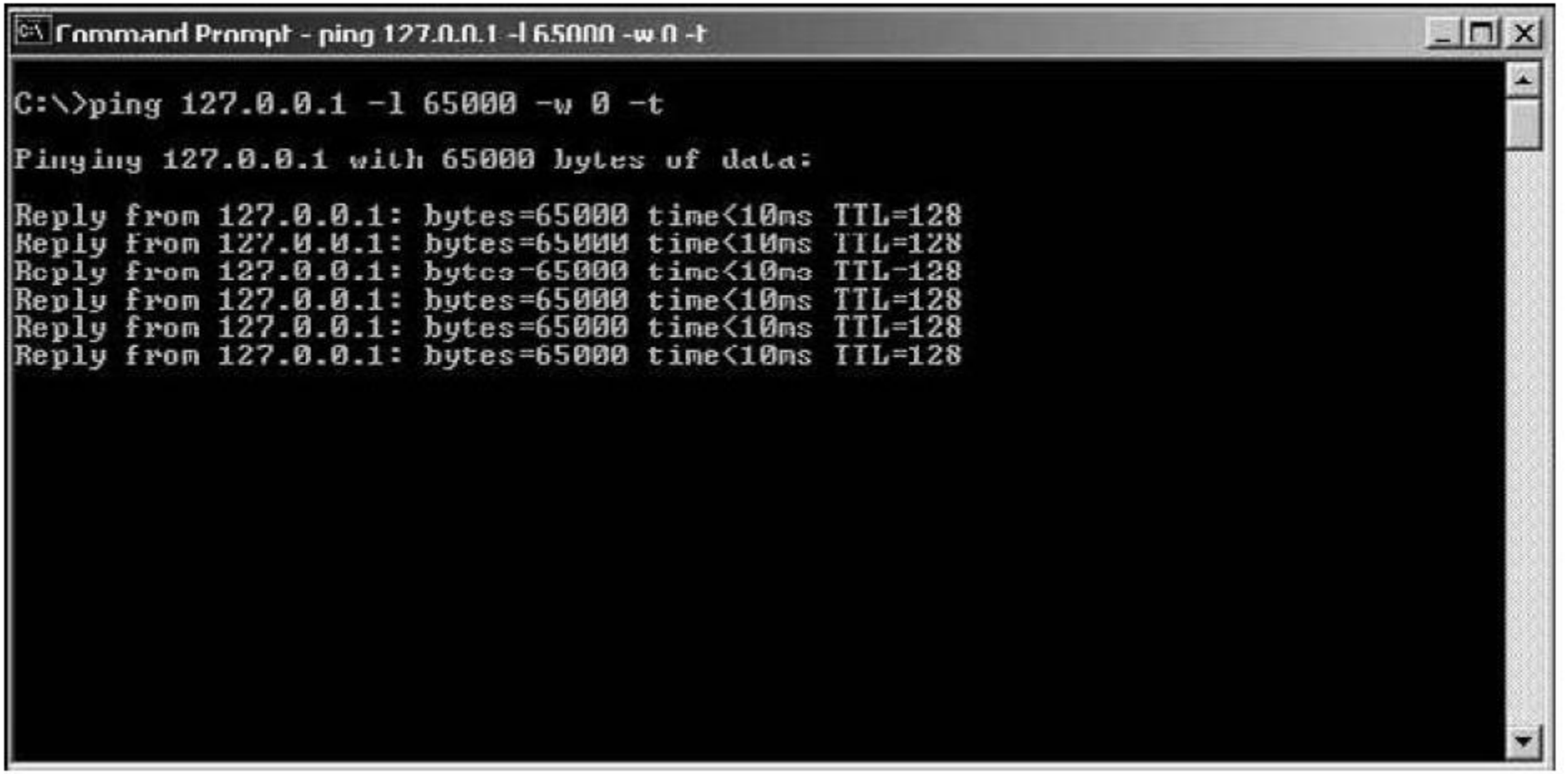
Its aim is to prevent legitimate users by:

- Attempting to flood a network
- To disrupt connections between computers
- Disrupt service to a specific system or person




Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
Webserver
User

Ping attack illustration

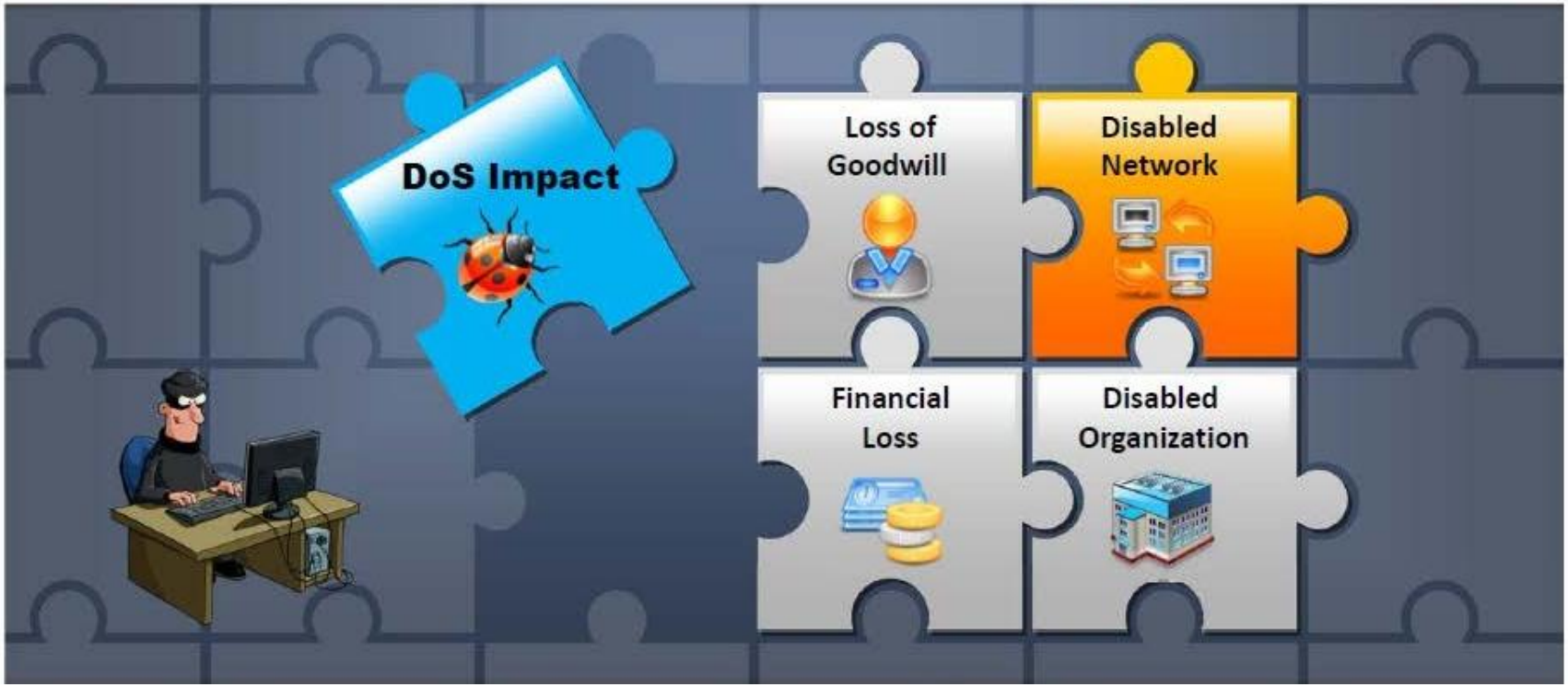


Introduction (cont.)

- Computers have physical limitations
  - Number of users
  - Size of files
  - Speed of transmission
  - Amount of data stored
- Exceed any of these limits and the computer will cease to respond
- Same as cars on highway

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**



Overview

- Common Tools Used for DoS
  - TFN and TFN2K
  - Stacheldracht

Overview (cont.)

Stacheldracht on the Symantec site

Bandwidth Attacks

01

A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses **several computers to flood a victim**

02

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**

03

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

04

Basically, all bandwidth 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**

Overview (cont.)

- DoS Weaknesses
  - The flood must be sustained.
    - When machines are disinfected, the attack stops.
    - Hacker's own machine are at risk of discovery.

Common forms of Attack

- SYN Floods
- Ping of death
- Smurf Attack
- Teardrop Attack
- Ping of flood
- Land Attack

SYN Attack

01

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

02

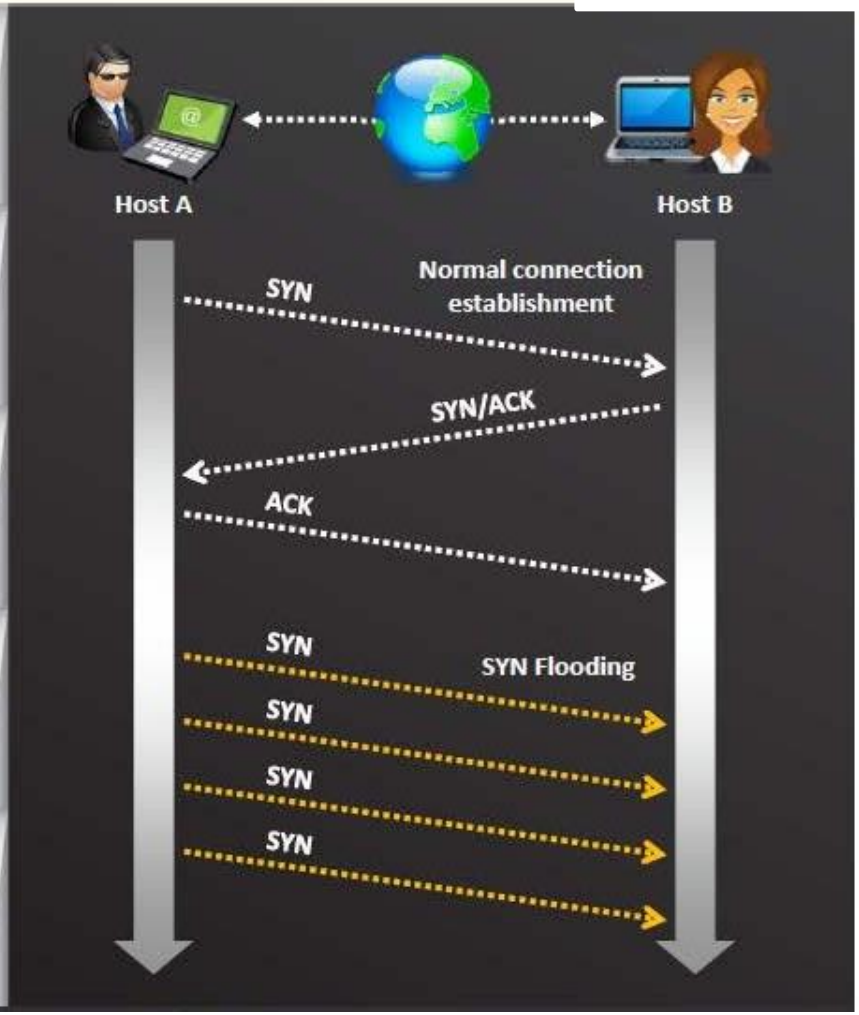
03

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

Note: This attack exploits the **three-way handshake** method

SYN Flooding

1. SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**
2. 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
3. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but **never replying** to the SYN/ACK
4. The victim's listen queue is **quickly filled up**
5. This ability of **holding up each incomplete connection for 75 seconds** can be cumulatively used as a Denial-of-Service attack



DoS Attacks

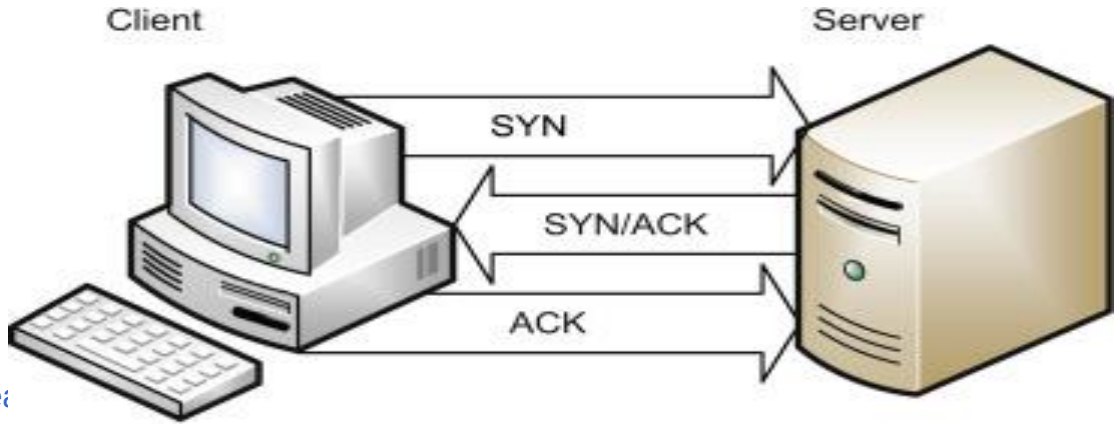
- TCP SYN Flood Attack
  - Hacker sends out a SYN packet.
  - Receiver must hold space in buffer.
  - Bogus SYNs overflow buffer.

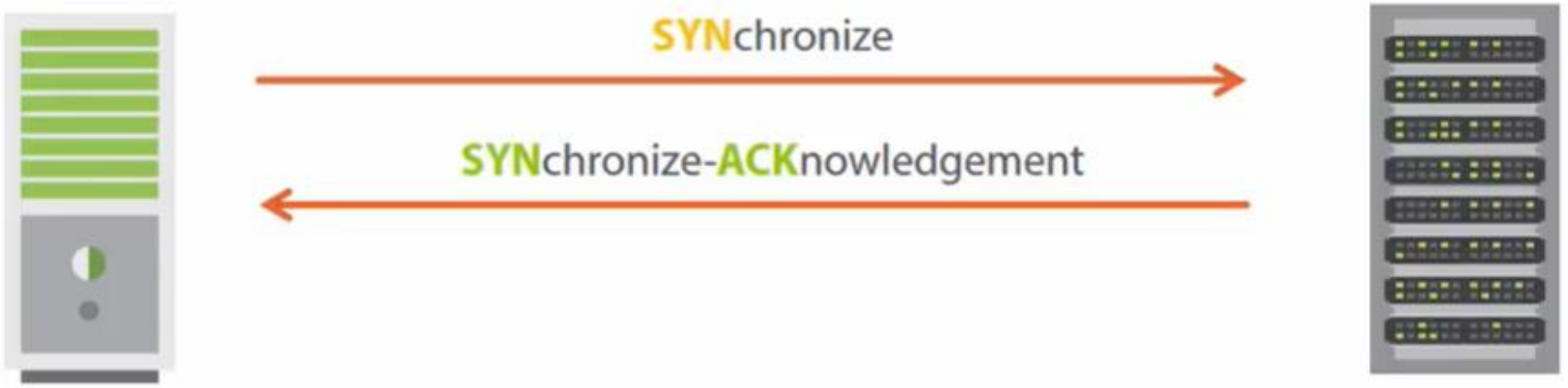
SYN Floods

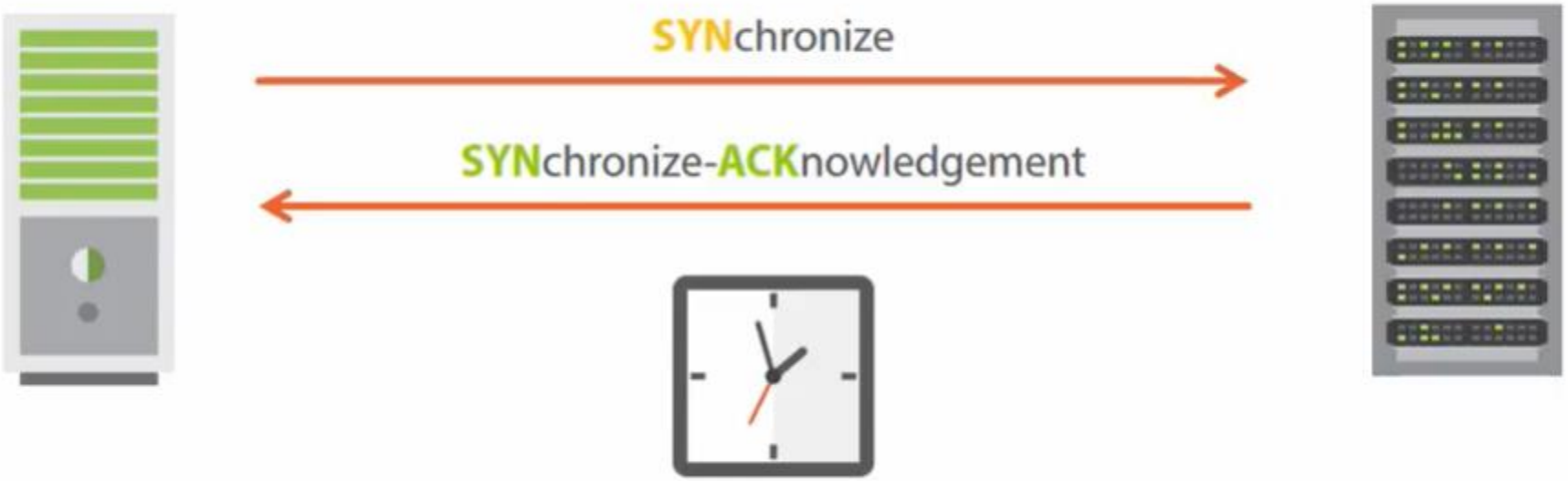
- It takes advantage of the flaw of TCP three-way handshaking behavior.
- Sends many requests to the connection.
- Do not response to replies.
- The SYN flood attack sends TCP connections requests faster than a machine can process them

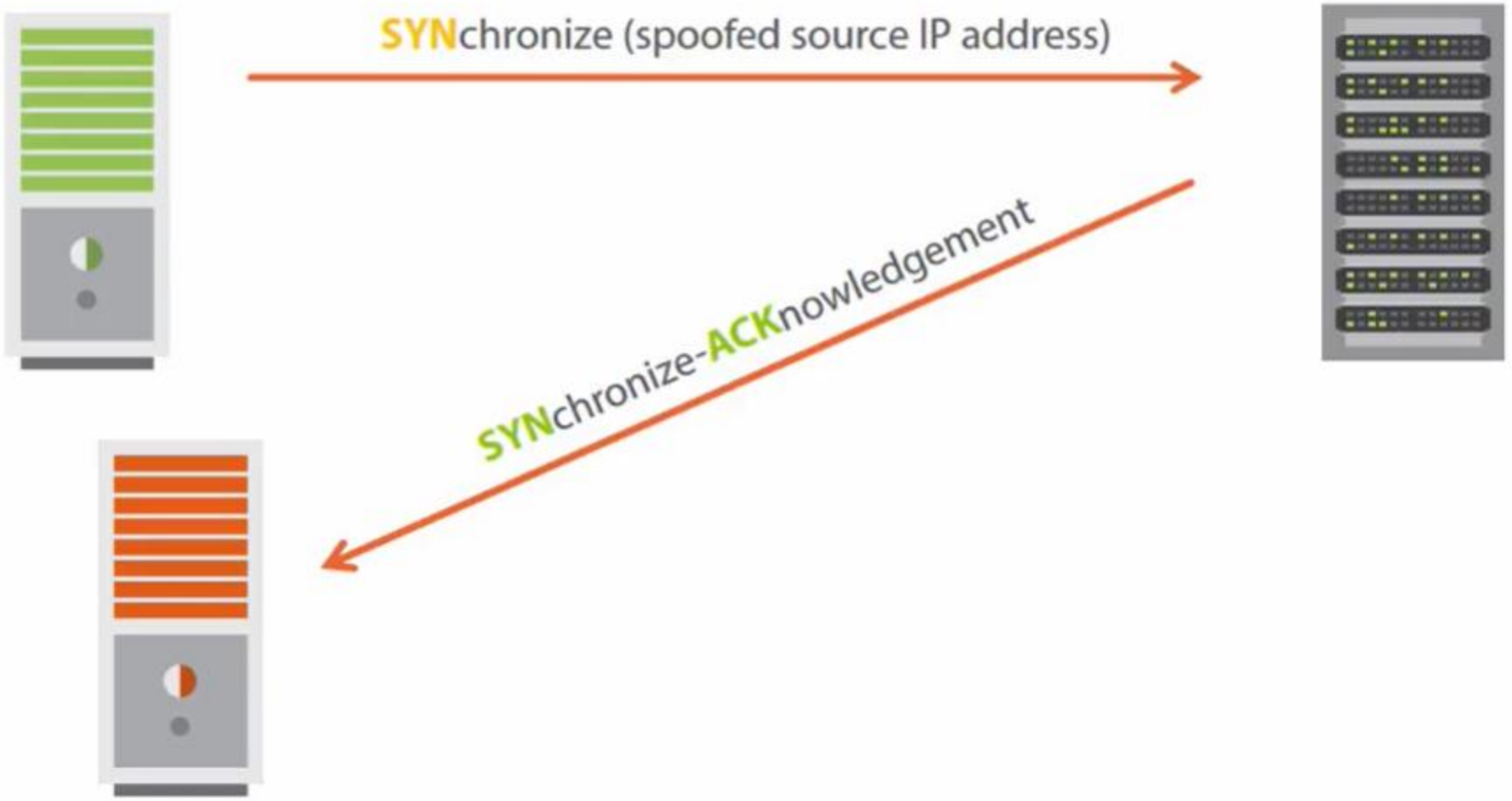
The three-way handshake

- Client sends a packet with the SYN flag set.
- Server allocates resources for the client and then responds with the SYN and ACK flags set.
- Client responds with the ACK flag set.

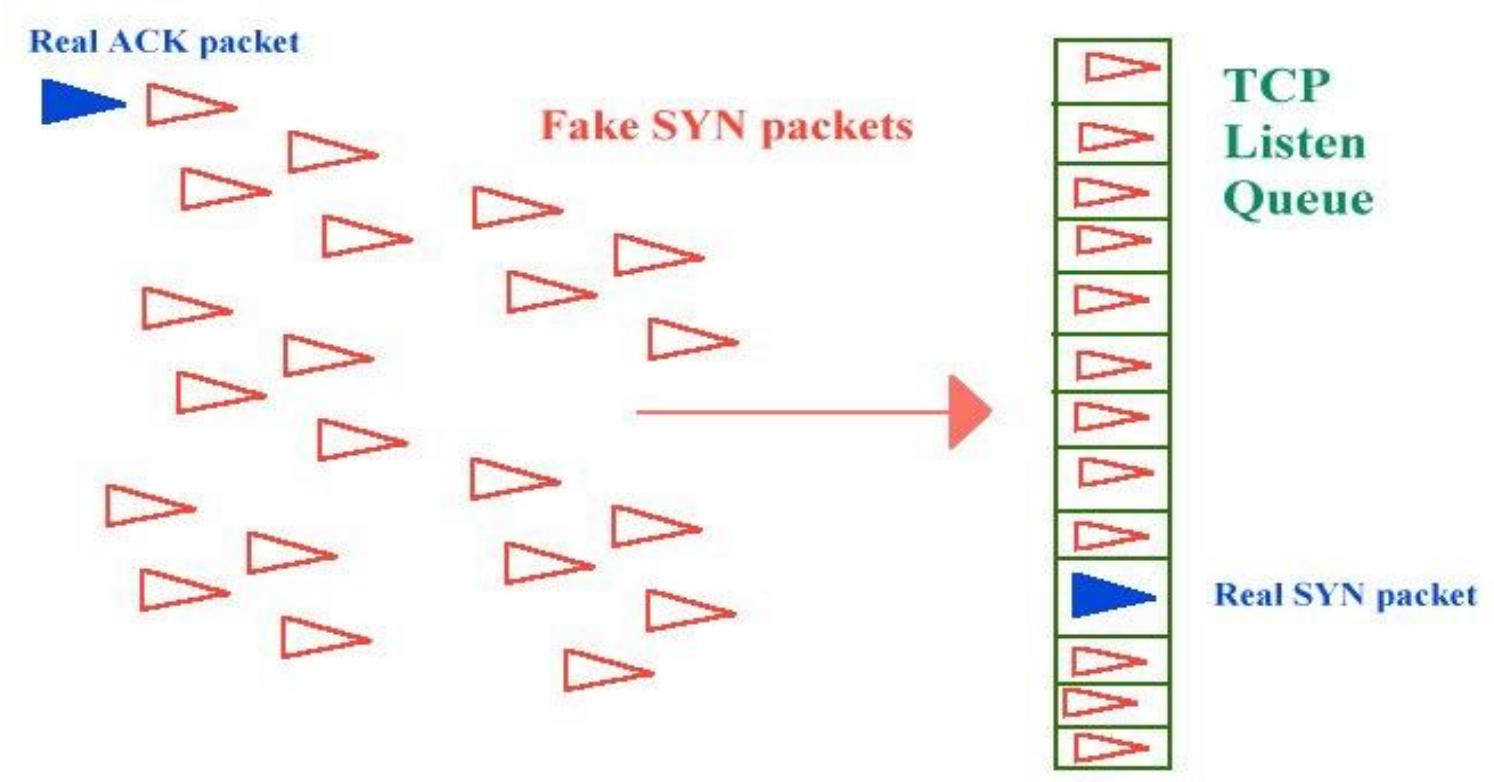



SYNchronize
SYNchronize-ACKnowledgement


SYNchronize
SYNchronize-ACKnowledgement


SYNchronize (spoofed source IP address)
SYNchronize-ACKnowledgement

DoS Attacks (cont.)



DoS Attacks (cont.)

- Methods of Prevention
  - SYN Cookies
    - Initially no buffer is created.
    - Client response is verified using a cookie.
    - The SYN+ACK contains a carefully constructed cookie, generated as a hash that contains the IP address, port number, and other information from the client machine requesting the connection
    - Only then is the buffer created.
    - Resource-intensive.

Micro Blocks

- Simply allocating a micro-record instead of allocating a complete connection object (an entire buffer segment) to the SYN object.

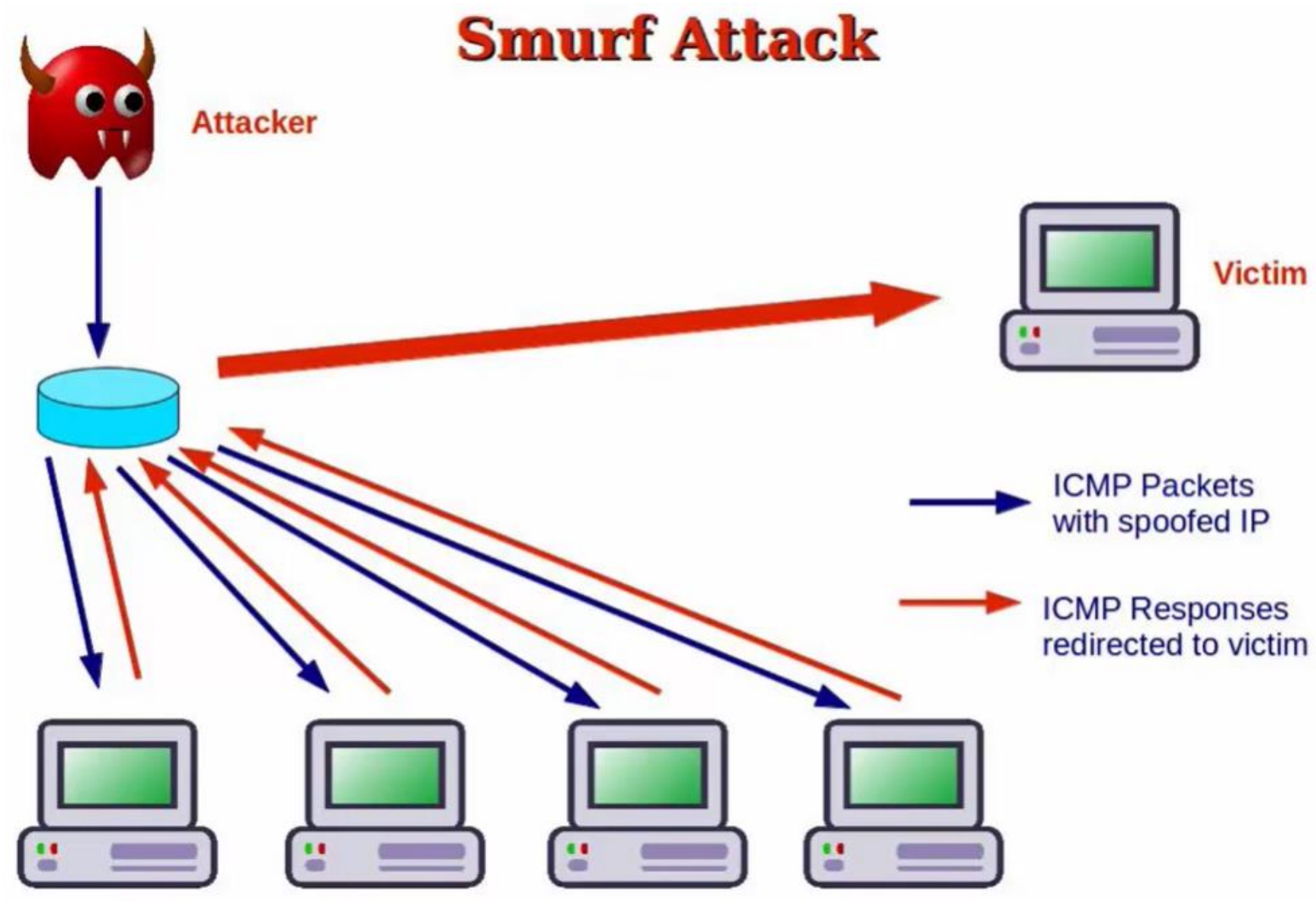
- In this way, an incoming SYN object can allocate as little as 16 bytes of space, making it significantly more difficult to flood a system.

RST Cookies

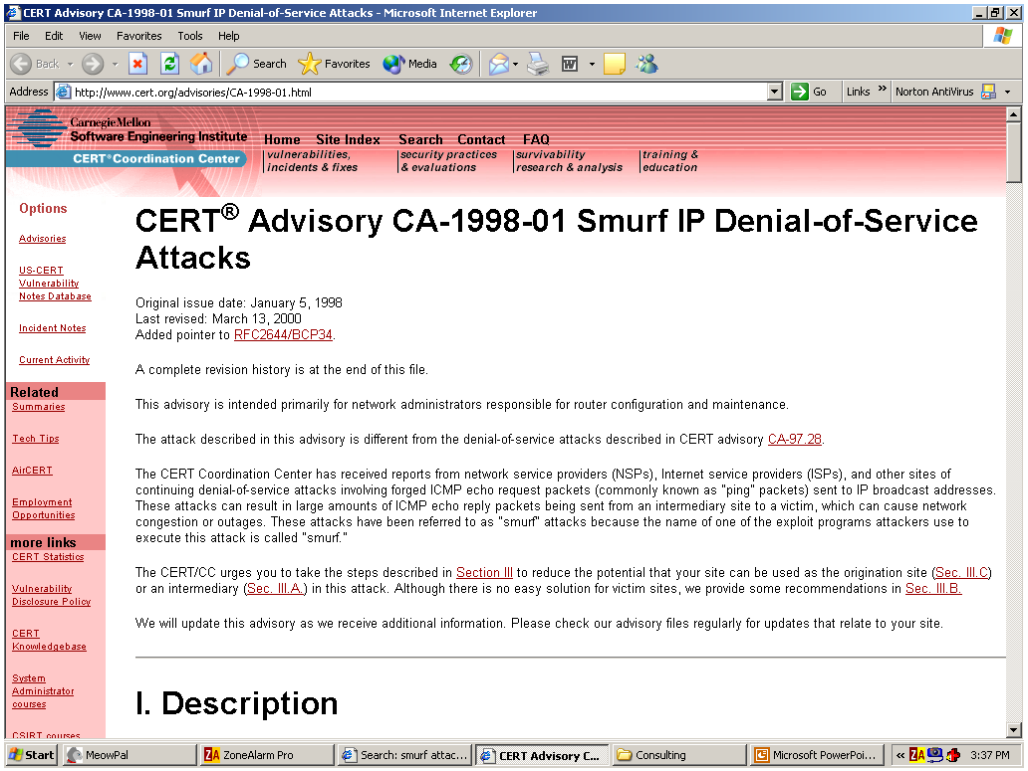
- Sends a false SYNACK back
- Should receive an RST in reply
- Verifies that the host is legitimate
- Not compatible with Windows 95

DoS Attacks (cont.)

- Smurf IP Attack
  - Hacker sends out ICMP broadcast with spoofed source IP.
    - Intermediaries respond with replies.
    - ICMP echo replies flood victim.
    - The network performs a DDoS on itself.


Smurf Attack
Attacker
Victim
ICMP Packets
with spoofed IP
ICMP Responses
redirected to victim

DoS Attacks (cont.)



CERT listing on Smurf attacks

DoS Attacks (cont.)

- Protection against Smurf attacks
  - Guard against Trojans.
  - Have adequate AV software.
  - Ensure routers don’t forward ICMP broadcasts.

DoS Attacks (cont.)

- UDP Flood Attack
  - Hacker sends UDP packets to a random port
  - When the target system receives a UDP packet, it automatically determines what application is waiting on the destination port
  - In this case, since there is no application waiting on the port, the target system will generate an ICMP packet of “destination unreachable” and attempt to send it back to the forged source address.

Ping of flood (ICMP Flood Attack)

- Attacker simply sends a huge number of "ICMP Echo Requests(ping)" to the victim.
- It sends ICMP packets as fast as possible without waiting for replies.
- The continuing combination of requests and replies can slow the network or, in extreme cases, to disconnect.

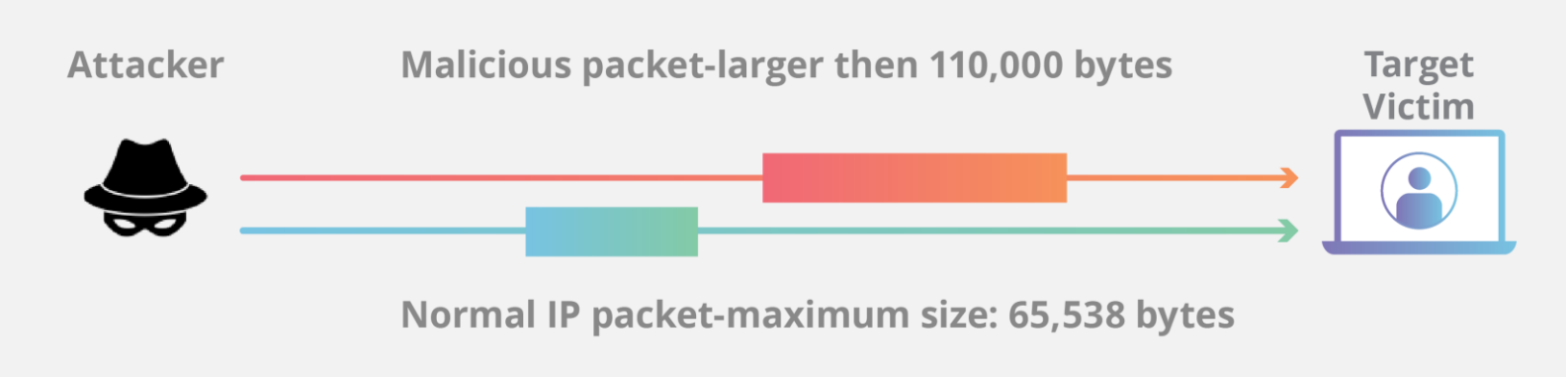
Ping of death

- Is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the bytes allowed by the IP protocol. Since the received ICMP(Internet Control Message Protocol) echo request packet is bigger than the normal IP packet size, the victim cannot reassemble the packets. The OS may be crashed or rebooted as a result.

- Sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.
- “ping”, is a network utility used to test a network connection, and it works much like sonar – a “pulse” is sent out and the “echo” from that pulse tells the operator information about the environment.
- If the connection is working, the source machine receives a reply from the targeted machine.

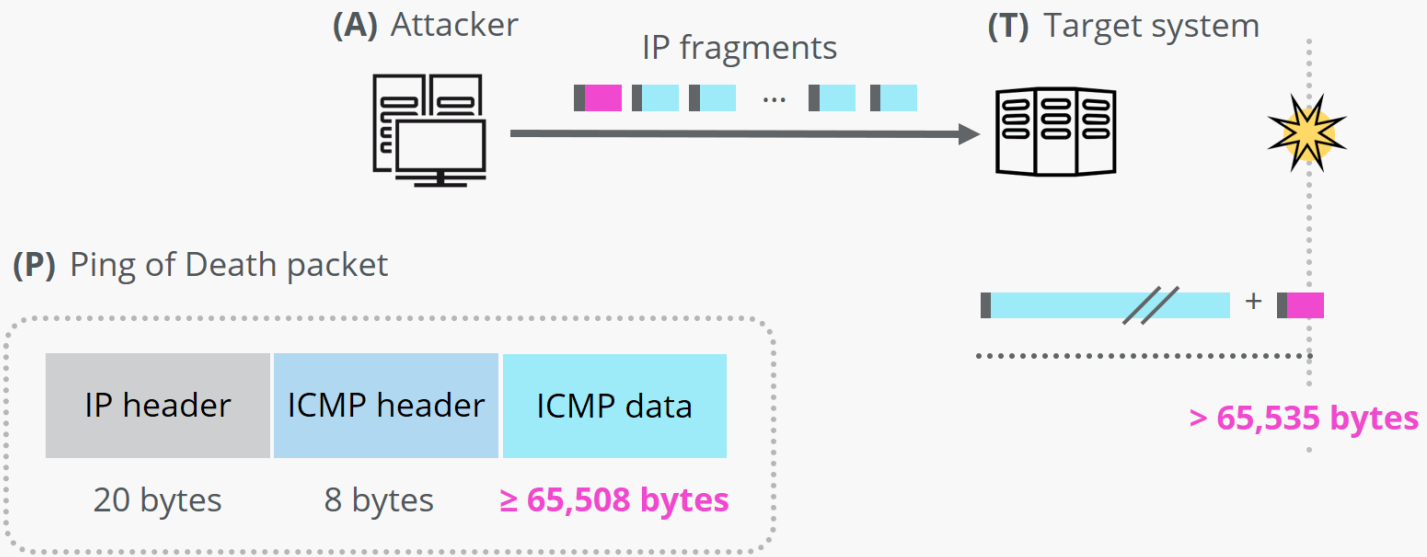
- IP4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,538 bytes.
- Some TCP/IP systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.
- When a maliciously large packet is transmitted from the attacker to the target, the packet becomes fragmented into segments, each of which is below the maximum size limit

- When the target machine attempts to put the pieces back together, the total exceeds the size limit and a buffer overflow can occur, causing the target machine to freeze, crash or reboot



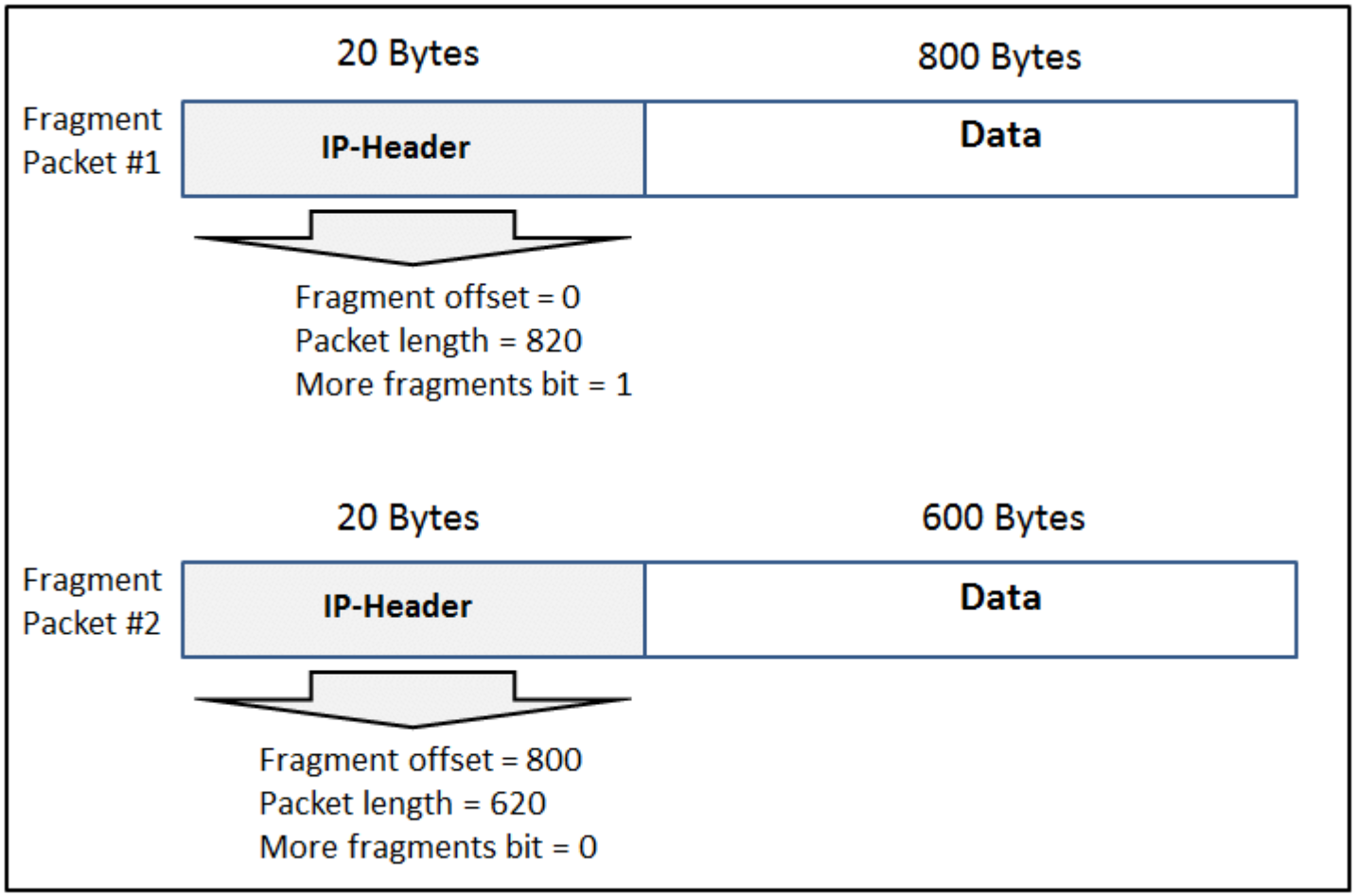
Ping of Death

How it works



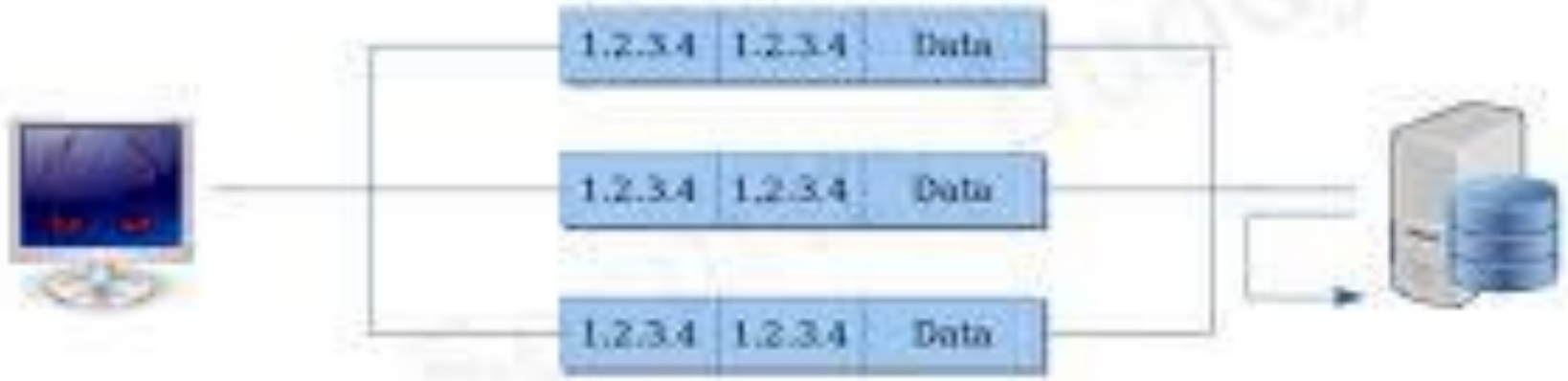
Teardrop Attack

- Divides large files into fragments.
- An attacker sends two fragments that cannot be reassembled properly by manipulating the header of packet and cause reboot or halt of victim system.


20 Bytes
800 Bytes
Fragment
Packet #1
IP-Header
Data
Fragment offset = 0
Packet length = 820
More fragments bit = 1
20 Bytes
600 Bytes
Fragment
Packet #2
IP-Header
Data
Fragment offset = 800
Packet length = 620
More fragments bit = 0

DoS Attacks (cont.)

- Land Attack
  - Simplest of all attacks
  - Hacker sends packet with the same source and destination IP
  - System “hangs” attempting to send and receive message


1.2.3.4
1.2.3.4
Data
1.2.3.4
1.2.3.4
Data
1.2.3.4
1.2.3.4
Data

Distributed Denial of Service (DD0S)

- DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

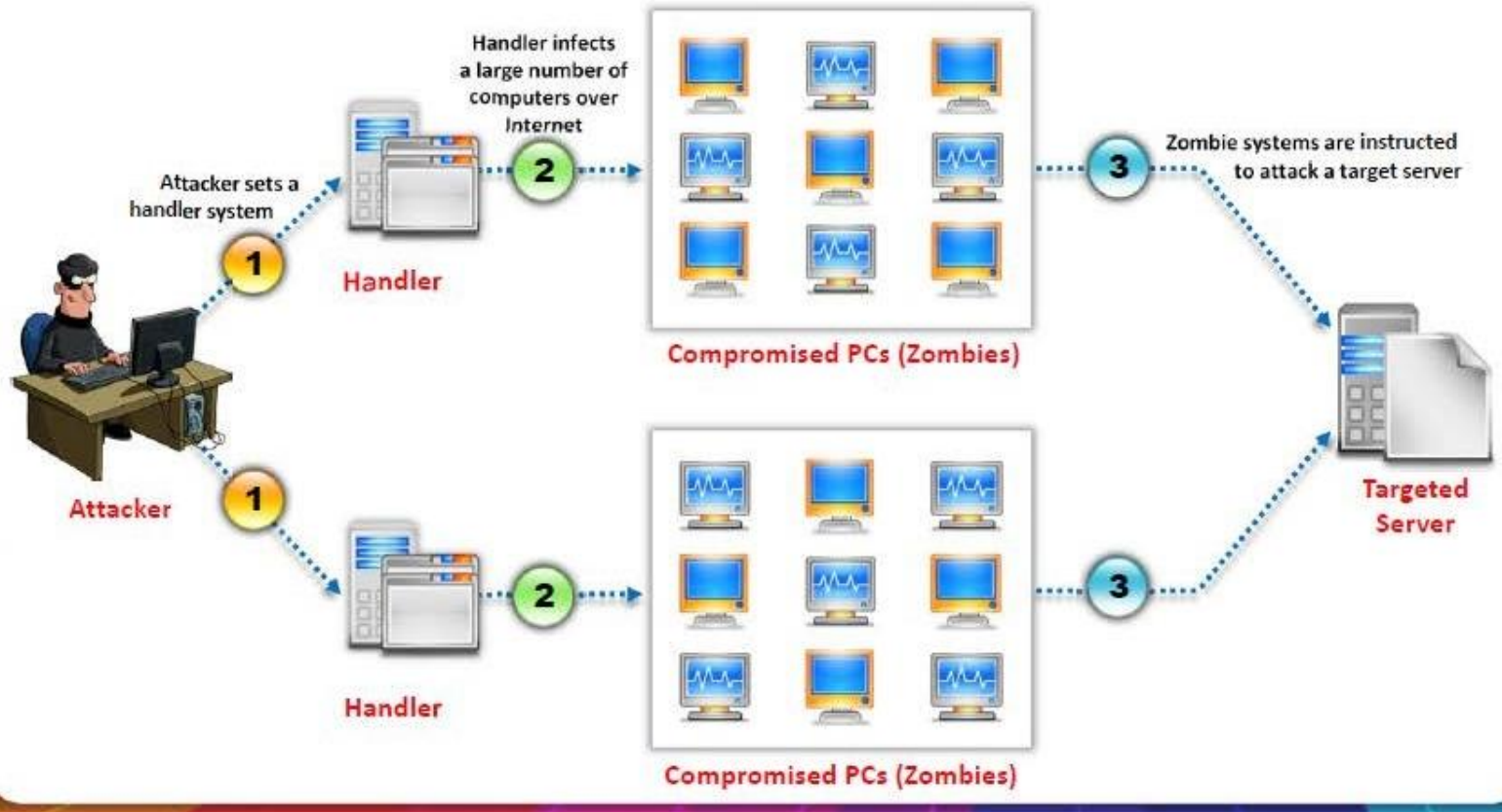
Distributed Denial of Service (DD0S)

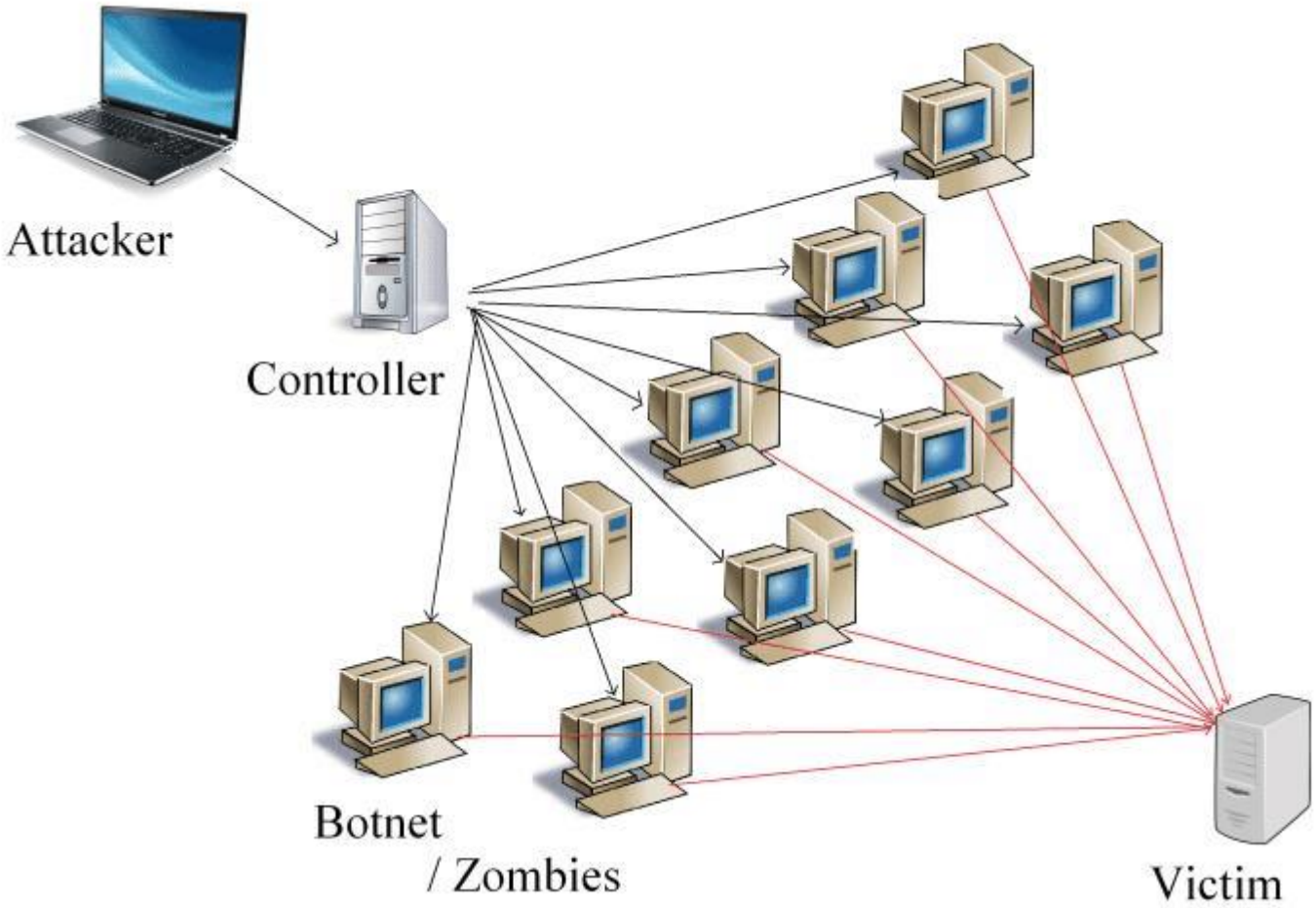
- These networks consist of computers and other devices (such as IoT devices)which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.
- Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

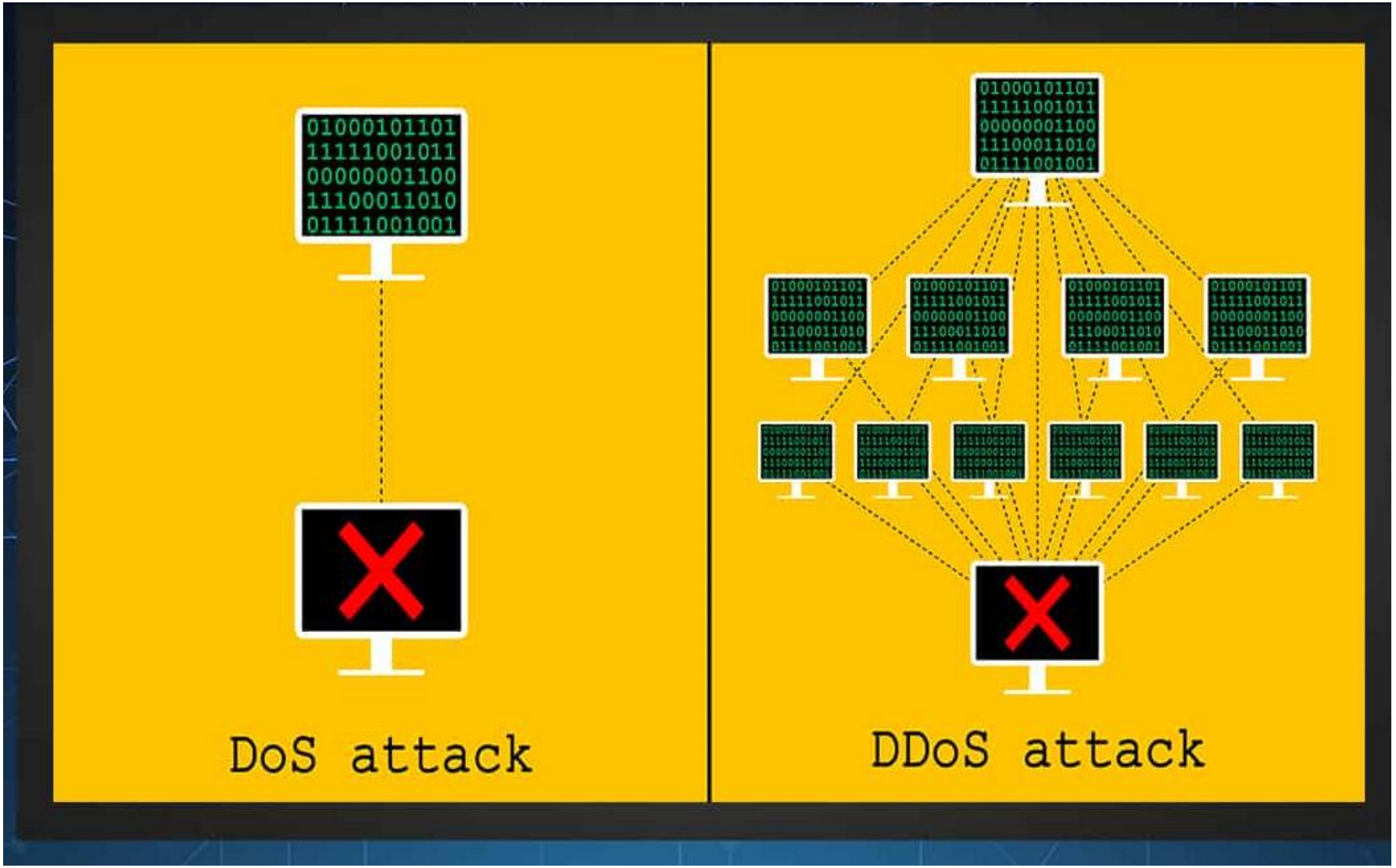
D DoS

- When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

How Distributed Denial of Service Attacks Work




Attacker
Controller
Botnet
/ Zombies
Victim


DoS attack
DDoS attack

Real-World Examples

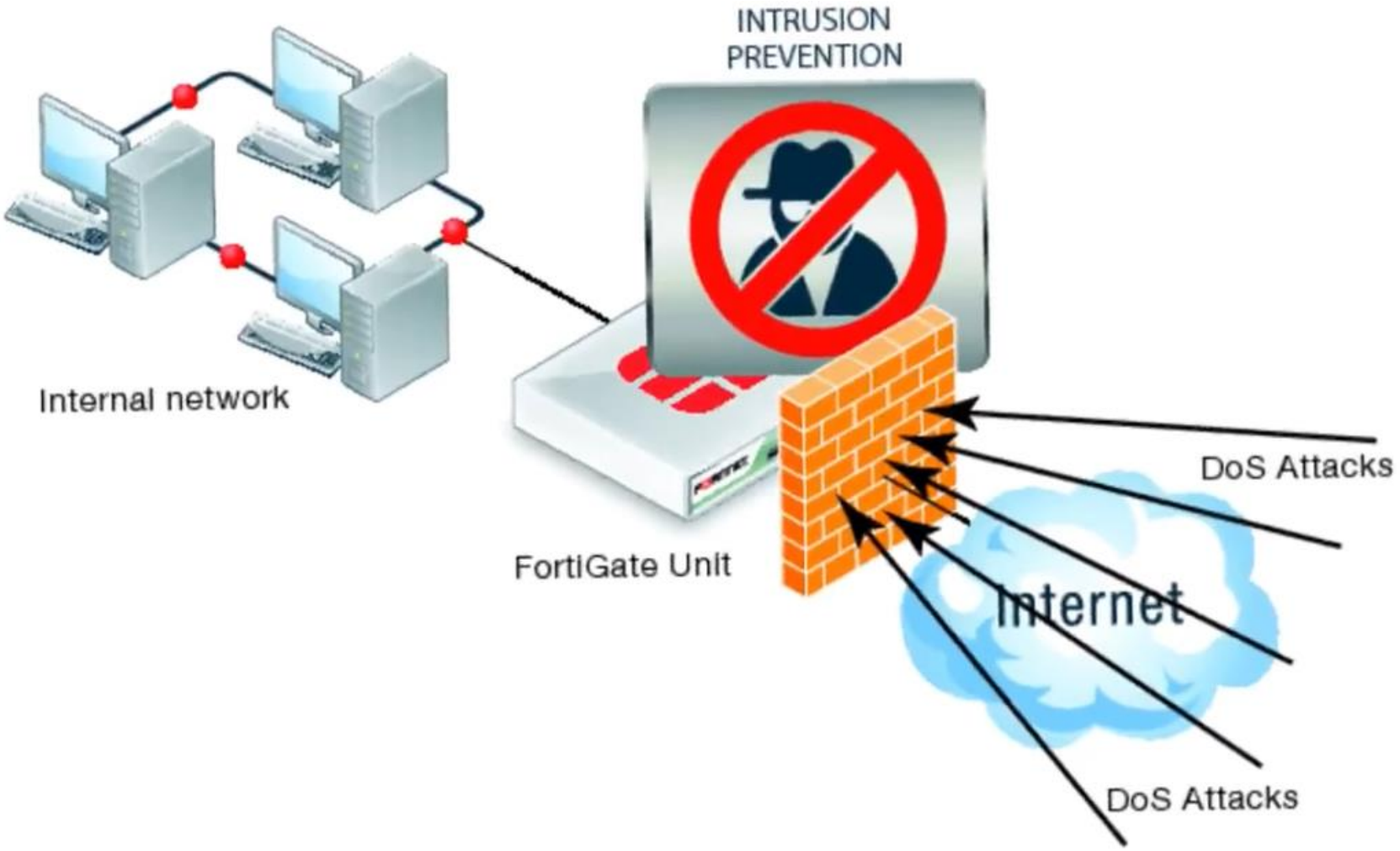
- MyDoom
  - Worked through e-mail

How to Defend Against DoS Attacks

- In addition to previously mentioned methods
  - Configure your firewall to
    - Filter out incoming ICMP packets.
    - Disallow any incoming traffic.
  - Use tools such as NetStat and others.

How to Defend Against DoS Attacks (cont.)

- Disallow traffic not originating within the network.
- Disable all IP broadcasts.
- Filter for external and internal IP addresses.
- Keep AV signatures updated.
- Keep OS and software update.
- Have an Acceptable Use Policy.


INTRUSION
PREVENTION
Internal network
FortiGate Unit
DoS Attacks
Internet
DoS Attacks

Dos Attack Tools

- 1. LOIC (Low Orbit Icon)
- 2. HOIC(High Orbit Icon)
- 3. HULK(HTTP Unbearable Load King)
- 4. PyLoris
- 5. Tors Hammer
- 6. SlowLoris
- 7.Golden Eye
- Hping3

DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit

The Pandora DDoS Bot Toolkit is an updated variant of the Dirt Jumper DDoS toolkit

It offers five distributed denial of service (DDoS) attack modes

It generates five attack types:

- HTTP min
- HTTP download
- HTTP Combo
- Socket Connect
- Max Flood

DoS and DDoS Attack Tools: Dereil and HOIC

http://sourceforge.net

Dereil

Dereil is professional (DDoS) Tools with modern patterns for attack via **TCP**, **UDP**, and **HTTP protocols**

HOIC

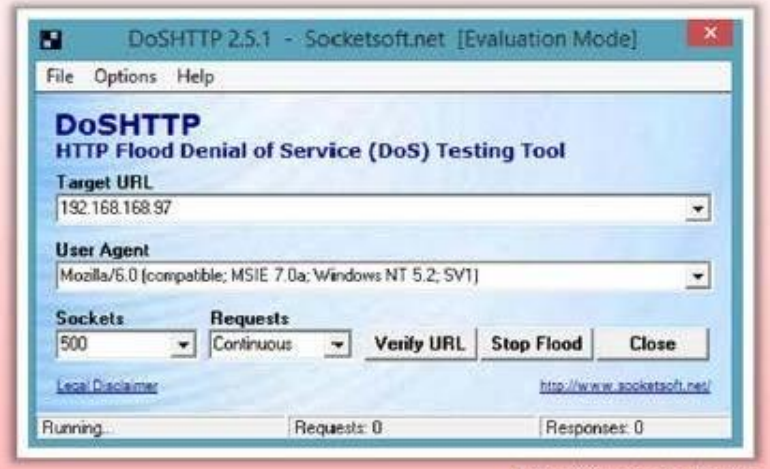
HOIC makes a DDoS attacks to **any IP address**, with a user selected port and a user selected protocol

http://sourceforge.net

DoS and DDoS Attack Tools: DoS HTTP and BanglaDos

DoS HTTP

- DoSHTTP is **HTTP Flood** Denial of Service (DoS) Testing Tool for Windows
- It includes **URL verification**, **HTTP redirection**, port designation, performance monitoring and enhanced reporting
- It uses **multiple asynchronous sockets** to perform an effective HTTP Flood



http://socketsoft.net

BanglaDos

http://sourceforge.net

DoS and DDoS Attack Tools

Tor's Hammer
http://packetstormsecurity.com

Moihack Port-Flooder
http://sourceforge.net

Anonymous-DoS
http://sourceforge.net

DDOSIM
http://sourceforge.net

DAVOSET
http://packetstormsecurity.com

HULK
http://www.sectorix.com

PyLoris
http://sourceforge.net

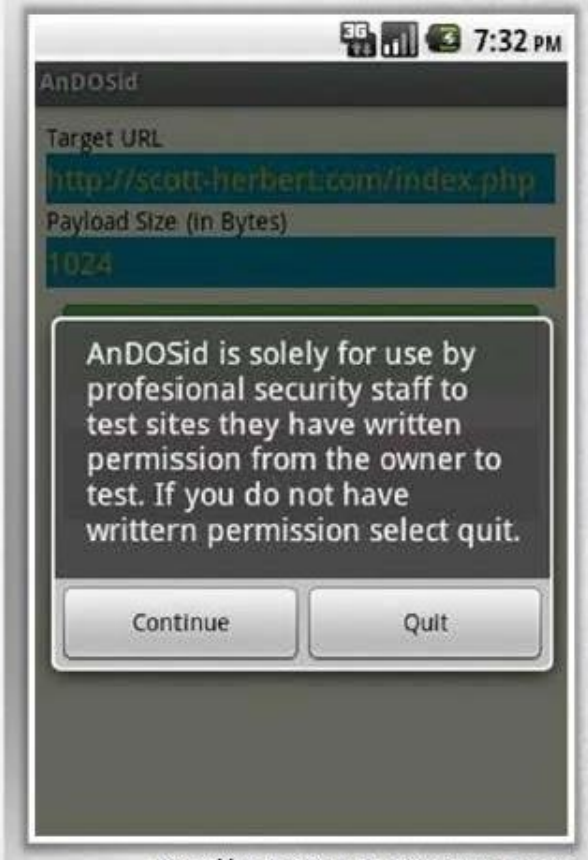
R-U-Dead-Yet
https://code.google.com

LOIC
http://sourceforge.net

GoldenEye HTTP Denial Of Service Tool
http://packetstormsecurity.com

DoS and DDoS Attack Tool for Mobile: AnDOSid

- AnDOSid allows attacker to simulate a **DOS attack** (A http post flood attack to be exact) and **DDoS attack on a web server** from mobile phones



http://andosid.android.informer.com

DoS and DDoS Attack Tool for Mobile: Low Orbit Ion Cannon (LOIC)

- Android version of Low Orbit Ion Cannon (LOIC) software is used for **flooding packets** which allows attacker to **perform DDoS attack** on target organization

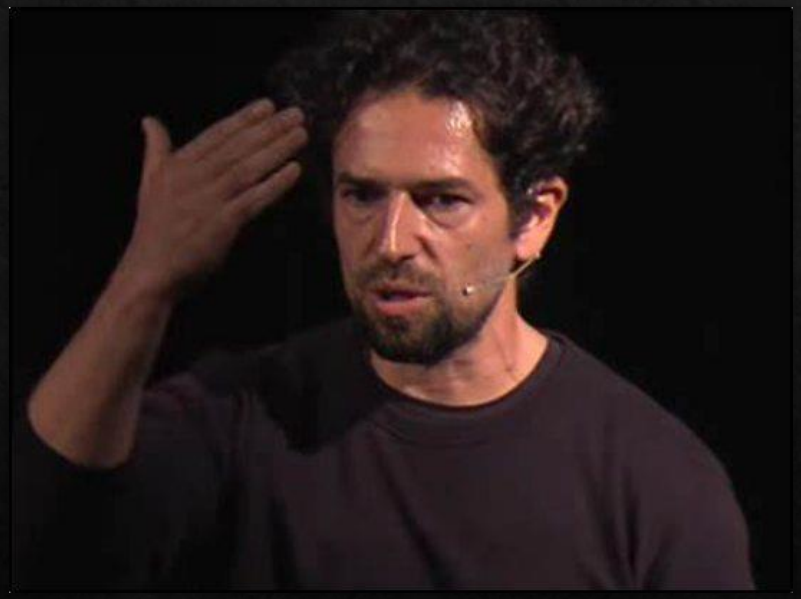
https://github.com

Hping3

- Hping-3 is a tool that is pre-installed in a kali machine and In simple words, the tool can send packets throughout the network and could see the flow of the network in an organisation.
- It is even effective in executing a three way server network response attack.
- It is especially known for showing the response of the targets to an attack situation. Therefore, it would be brilliant for simulations too.

- hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.
- It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols.
- By sending the packets throughout the network the red team members will identify any problem in the network and even check for the firewall.
- This tool is good in the good hands but if it is in EVIL hands then the tool is a devil 😼🧍

Who Developed The Hping3 Tool



The tool was developed by Salvatore Sanfilippo.

if you want to install the tool in Linux distributaries just enter

sudo apt-get install hping3

What all the hping3 tool can do□□

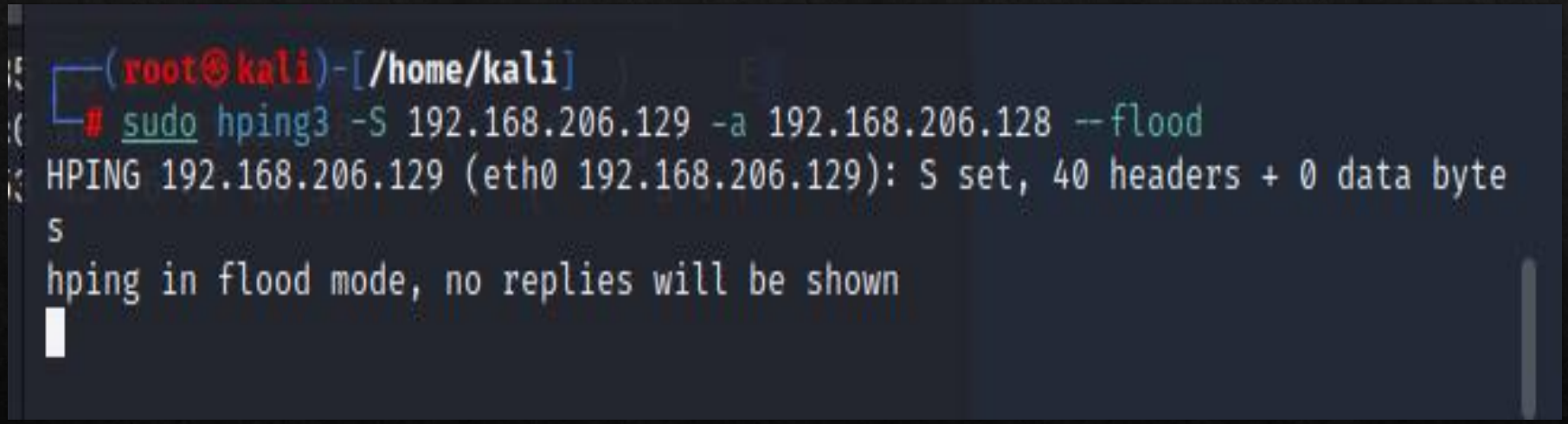
1. Firewall testing
2. Advanced port scanning
3. Network testing.
4. MTU discovery (Manual path discovery)
5. Advanced traceroute,(All protocols are supported)
6. Remote OS fingerprinting
7. Remote uptime guessing
8. TCP/IP stacks auditing
9. hping can also be useful to students that are learning TCP/IP.

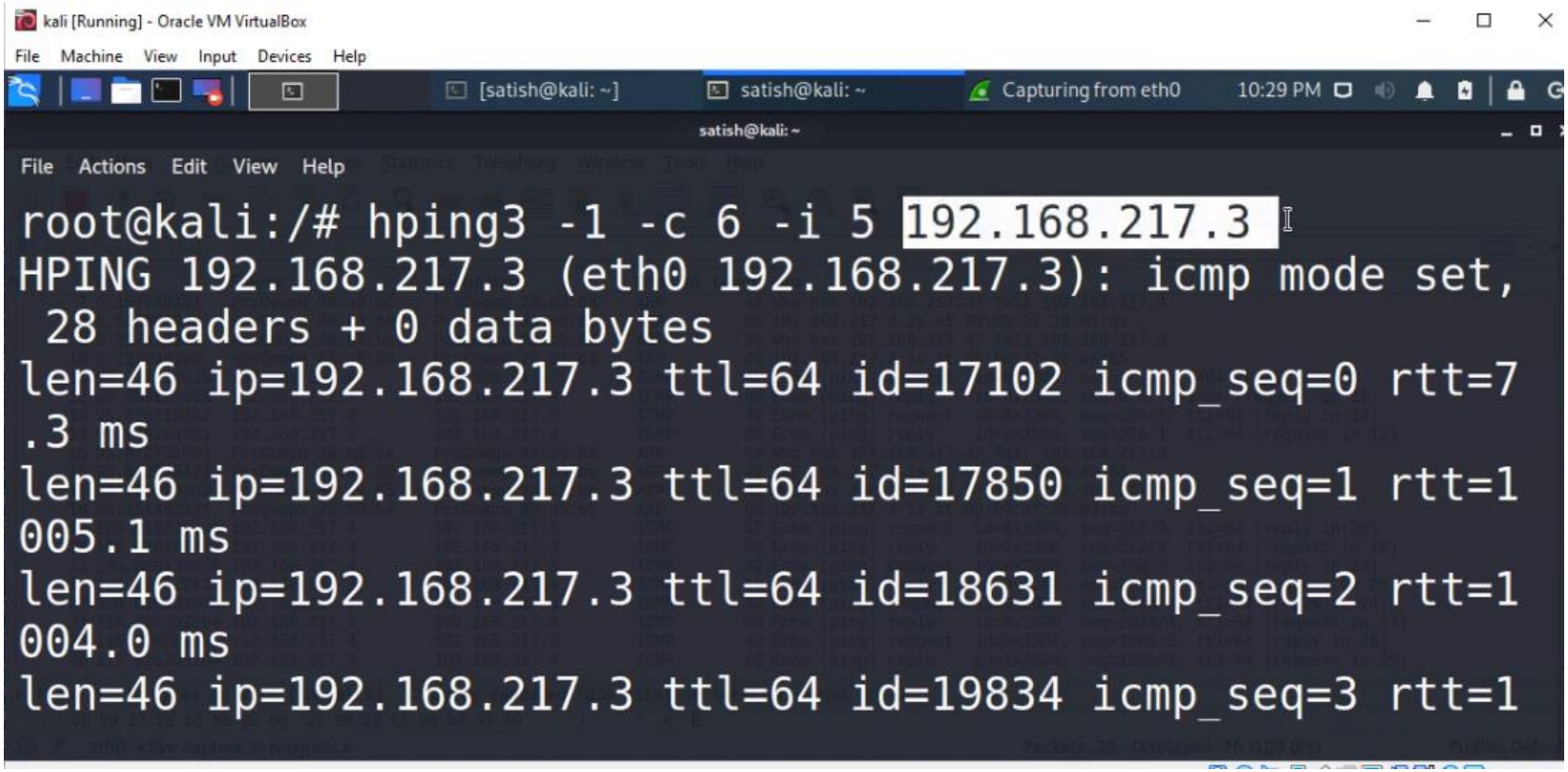
Useful commands in hping3 tool 👇

- -c –count: packet count
- –faster: alias for -i u1000 (100 packets for second)
- –flood: sent packets as fast as possible. Don’t show replies.
- -V –verbose: verbose mode
- -0 –rawip: RAW IP mode
- -1 –icmp: ICMP mode
- -2 –udp: UDP mode
- -8 –scan: SCAN mode.
- -9 –listen: listen mode

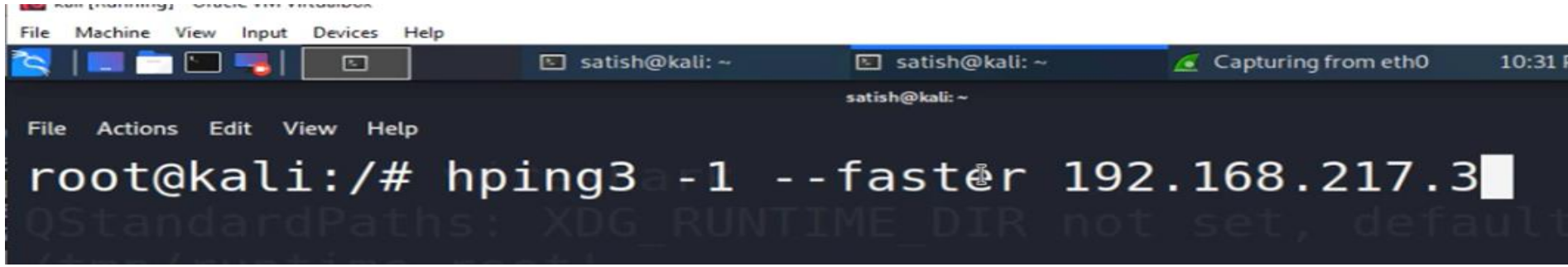
- -a –spoof: spoof source address
- -C –icmptype: icmp type
- -K –icmpcode: icmp code
- -L –setack: set TCP ack
- -F –fin: set FIN flag
- -S –syn: set SYN flag
- -R –rst: set RST flag
- -A –ack: set ACK flag
- -X –xmas: set X unused flag (0x40)
- -Y –ymas: set Y unused flag (0x80)

SYN flooding on a victim




kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[satish@kali: ~]
satish@kali: ~
Capturing from eth0
10:29 PM
satish@kali: ~
File Actions Edit View Help
root@kali:/# hping3 -1 -c 6 -i 5 192.168.217.3
HPING 192.168.217.3 (eth0 192.168.217.3): icmp mode set,
28 headers + 0 data bytes
len=46 ip=192.168.217.3 ttl=64 id=17102 icmp_seq=0 rtt=7
.3 ms
len=46 ip=192.168.217.3 ttl=64 id=17850 icmp_seq=1 rtt=1
005.1 ms
len=46 ip=192.168.217.3 ttl=64 id=18631 icmp_seq=2 rtt=1
004.0 ms
len=46 ip=192.168.217.3 ttl=64 id=19834 icmp_seq=3 rtt=1

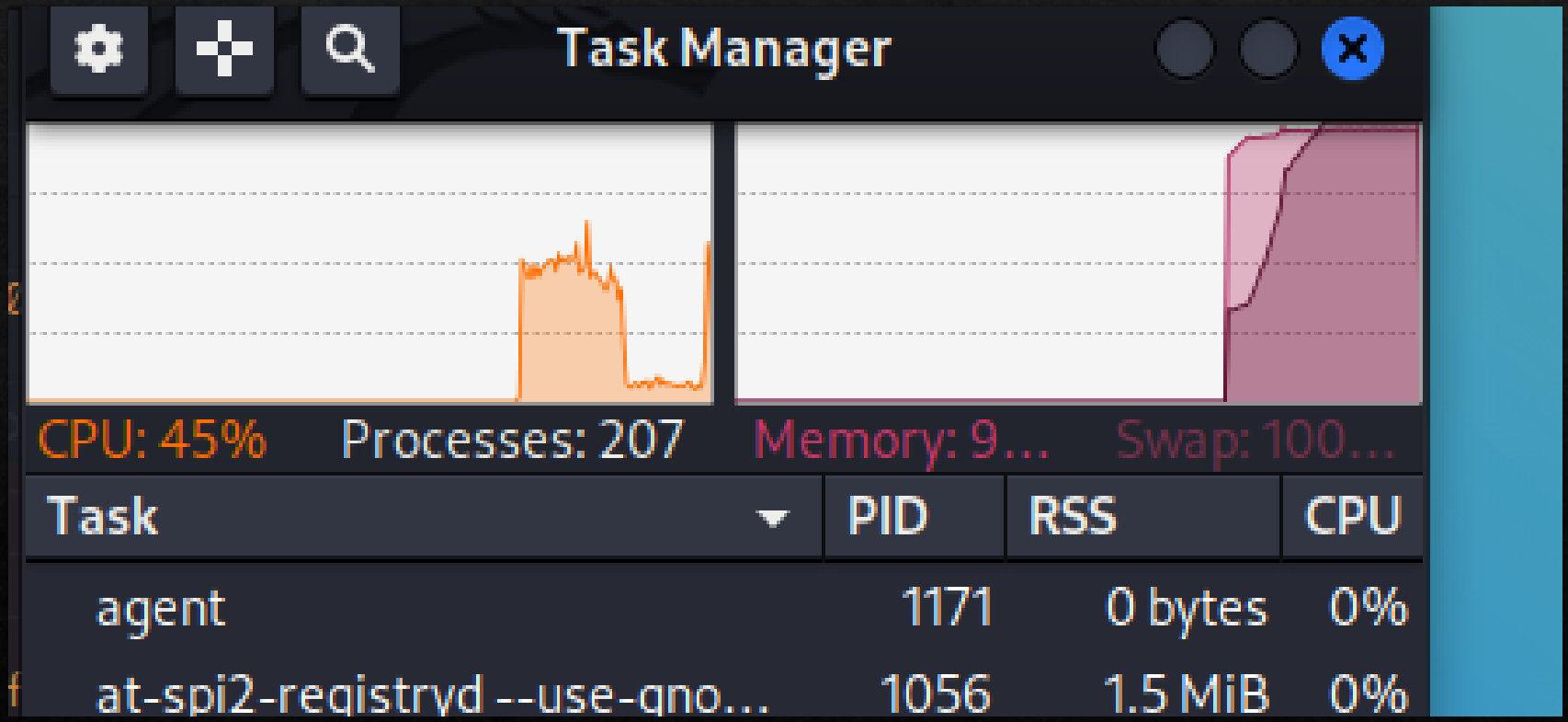

[satish@kali: ~]
satish@kali: ~
Capturing from eth0
10:29 PM
satish@kali: ~
File Actions Edit View Help
root@kali:/# hping3 -1 --fast 192.168.217.3


File Machine View Input Devices Help
satish@kali: ~
satish@kali: ~
Capturing from eth0
10:31
satish@kali: ~
File Actions Edit View Help
root@kali:/# hping3 -1 --faster 192.168.217.3

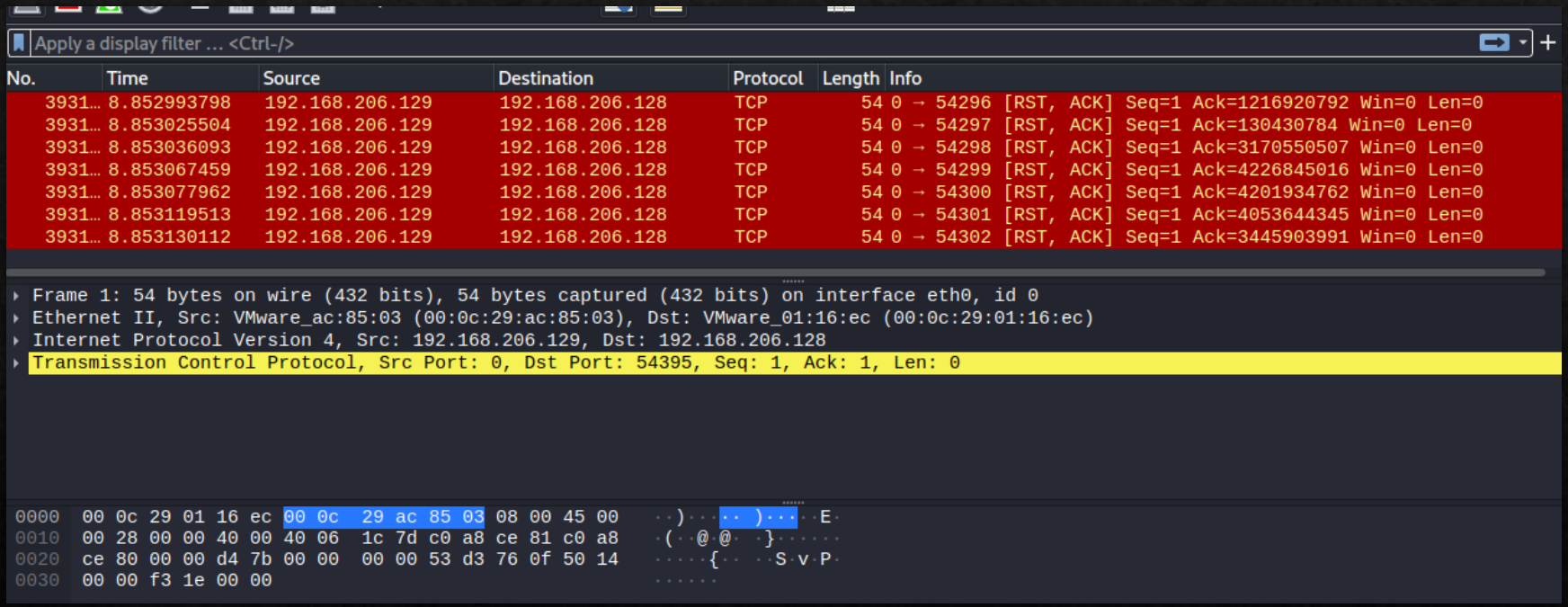

File Machine View Input Devices Help
satish@kali: ~
satish@kali: ~
Capturing from eth0
10:36 PM
satish@kali: ~
File Actions Edit View Help
root@kali:/# hping3 -1 -a 192.168.217.2 -c 1 192.168.217
.3


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
satish@kali: ~
satish@kali: ~
Capturing from eth0
10:39 PM
satish@kali: ~
File Actions Edit View Help
root@kali:/# hping3 -1 --rand-source -c 1 192.168.217.3

Task Manager



Wireshark


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
3931… 8.852993798 192.168.206.129 192.168.206.128 TCP 54 0 → 54296 [RST, ACK] Seq=1 Ack=1216920792 Win=0 Len=0
3931… 8.853025504 192.168.206.129 192.168.206.128 TCP 54 0 → 54297 [RST, ACK] Seq=1 Ack=130430784 Win=0 Len=0
3931… 8.853036093 192.168.206.129 192.168.206.128 TCP 54 0 → 54298 [RST, ACK] Seq=1 Ack=3170550507 Win=0 Len=0
3931… 8.853067459 192.168.206.129 192.168.206.128 TCP 54 0 → 54299 [RST, ACK] Seq=1 Ack=4226845016 Win=0 Len=0
3931… 8.853077962 192.168.206.129 192.168.206.128 TCP 54 0 → 54300 [RST, ACK] Seq=1 Ack=4201934762 Win=0 Len=0
3931… 8.853119513 192.168.206.129 192.168.206.128 TCP 54 0 → 54301 [RST, ACK] Seq=1 Ack=4053644345 Win=0 Len=0
3931… 8.853130112 192.168.206.129 192.168.206.128 TCP 54 0 → 54302 [RST, ACK] Seq=1 Ack=3445903991 Win=0 Len=0
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: VMware_ac:85:03 (00:0c:29:ac:85:03), Dst: VMware_01:16:ec (00:0c:29:01:16:ec)
Internet Protocol Version 4, Src: 192.168.206.129, Dst: 192.168.206.128
Transmission Control Protocol, Src Port: 0, Dst Port: 54395, Seq: 1, Ack: 1, Len: 0
0000 00 0c 29 01 16 ec 00 0c 29 ac 85 03 08 00 45 00
0010 00 28 00 00 40 00 40 06 1c 7d c0 a8 ce 81 c0 a8
0020 ce 80 00 00 d4 7b 00 00 00 00 53 d3 76 0f 50 14
0030 00 00 f3 1e 00 00

DoS/DDoS Countermeasure Strategies

01 Absorbing the Attack

- Use additional capacity to absorb attack; it **requires preplanning**
- It requires **additional resources**

02 Degrading Services

- **Identify critical services** and stop non critical services

03 Shutting Down the Services

- Shut down all the services until the **attack has subsided**

DoS/DDoS Countermeasures: Protect Secondary Victims

Install **anti-virus** and **anti-Trojan** software and keep these up-to-date

Increase **awareness of security issues** and prevention techniques in all Internet users

Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources

Properly configure and regularly update the **built-in defensive mechanisms** in the core hardware and software of the systems

DoS/DDoS Countermeasures: Detect Potential Attacks

Egress Filtering

- Scanning the **packet headers of IP packets** leaving a network
- Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network

Ingress Filtering

- Protects from **flooding attacks** which originate from the valid prefixes (IP addresses)
- It enables the originator to be traced to its **true source**

TCP Intercept

- Configuring TCP Intercept **prevents DoS attacks** by intercepting and validating the TCP connection requests

Post-Attack Forensics

1. DDoS attack traffic patterns can help the network administrators to develop **new filtering techniques** for preventing the attack traffic from entering or leaving the networks

2. Analyze router, firewall, and **IDS logs** to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and **law enforcement** agencies

3. **Traffic pattern analysis**: Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic

4. Using these characteristics, the result of traffic pattern analysis can be used for updating **load-balancing** and **throttling** countermeasures

Denial-of-Service (DoS) Attack
Penetration Testing

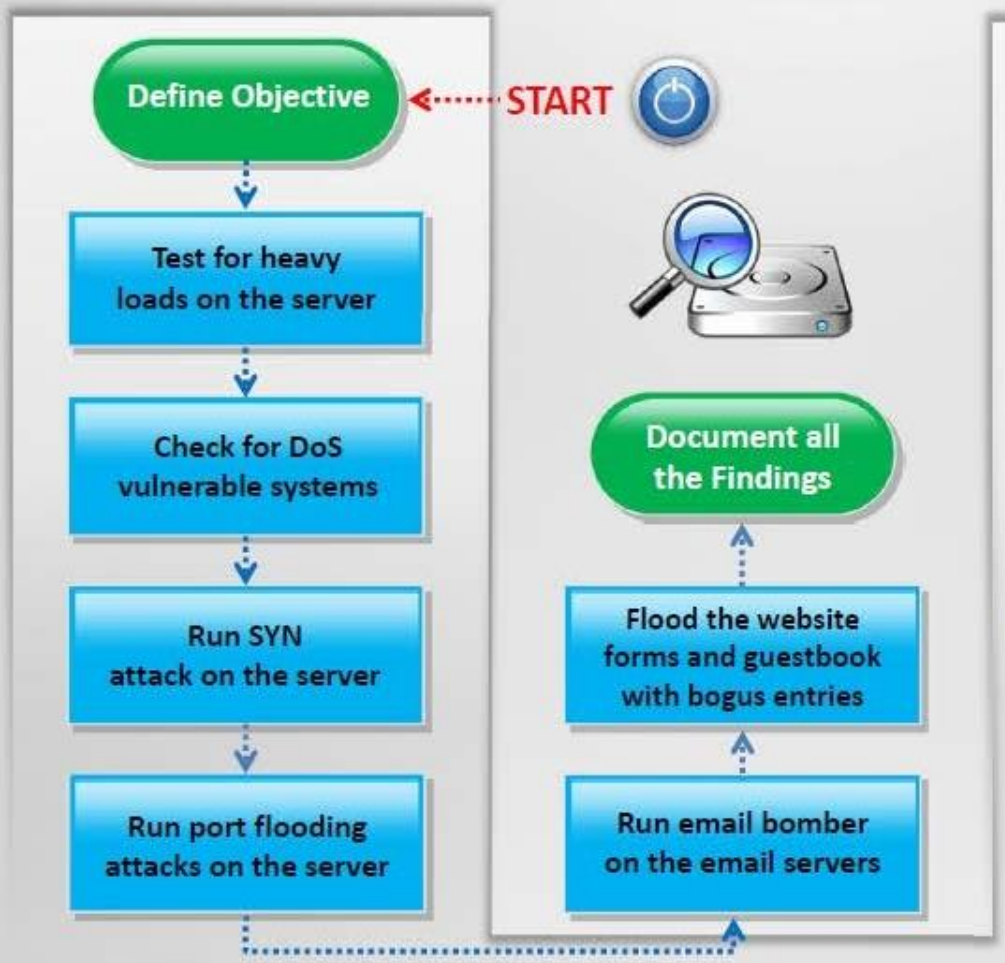
1. DoS attack should be incorporated into Pen testing plans to find out if the **network server** is susceptible to DoS attacks

2. DoS Pen Testing **determines minimum thresholds for DoS attacks on a system**, but the tester cannot ensure that the system is resistant to DoS attacks

3. The pen tester **floods the target network with traffic**, similar to hundreds of people repeatedly requesting the service in order to check the system stability

4. Pen testing results will help the administrators to **determine and adopt suitable network perimeter security controls** such as load balancer, IDS, IPS, Firewalls, etc.

Denial-of-Service (DoS) Attack
Penetration Testing (Cont'd)



- Test the web server using automated tools such as **Webserver Stress Tool** and **JMeter** for load capacity, server-side performance, locks, and other scalability issues
- Scan the network using automated tools such as **Nmap**, **GFI LanGuard**, and **Nessus** to discover any systems that are vulnerable to DoS attacks
- Flood the target with connection request packets using tools such as **Dirt Jumper DDoS Toolkit**, **Dereil**, **HOIC**, and **DoS HTTP**
- Use a port flooding attack to flood the port and increase the CPU usage by maintaining all the connection requests on the ports under blockade. Use tools **LOIC** and **Moihack Port Flooder** to automate a port flooding attack
- Use tools **Mail Bomber** to send a large number of emails to a target mail server
- Fill the forms with **arbitrary** and **lengthy** entries

Module Summary

- 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
- 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
- Attacker uses various techniques to carry out DoS/DDoS attacks on the target but these attacks are basically categorized into; volumetric attacks, fragmentation attacks, TCP state-exhaustion attacks, and application layer attacks
- There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, like a major corporation that offers criminal services
- A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks
- Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
- The pen tester floods the target network with traffic, similar to hundreds of people repeatedly requesting the service in order to check the system stability

Summary

- DoS attacks are common.
- DoS attacks are unsophisticated.
- DoS attacks are devastating.
- Your job is constant vigilance.