School of
Nation Builders

NATIONAL COLLEGE OF
SCIENCE & TECHNOLOGY
COMPUTER STUDIES DEPARTMENT

ICT 024

TCP and UDP Vulnerabilities

TOPIC 3

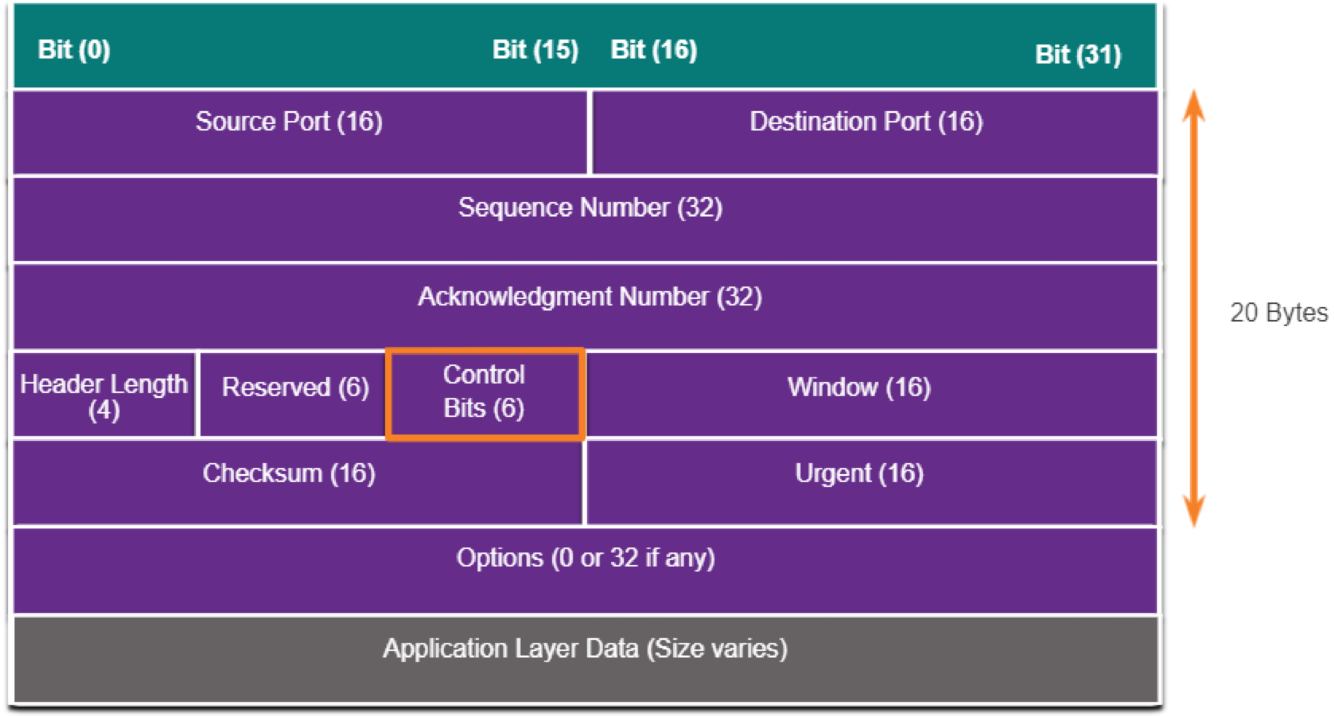
Prepared by: Calix Olaguer

TCP Segment Header

TCP segment information appears immediately after the IP header. The fields of the TCP segment and the flags for the Control Bits field are displayed in the figure.

The following are the six control bits of the TCP segment:

- **URG** – Urgent pointer field significant
- **SYN** – Synchronize sequence numbers
- **ACK** – Acknowledgement field significant
- **PSH** – Push function
- **FIN** – No more data from sender
- **RST** – reset the connection



Bit (0) Bit (15) Bit (16) Bit (31)

Source Port (16) | Destination Port (16)

Sequence Number (32)

Acknowledgment Number (32)

Header Length (4) | Reserved (6) | Control Bits (6) | Window (16)

Checksum (16) | Urgent (16)

Options (0 or 32 if any)

Application Layer Data (Size varies)

20 Bytes

TCP Services

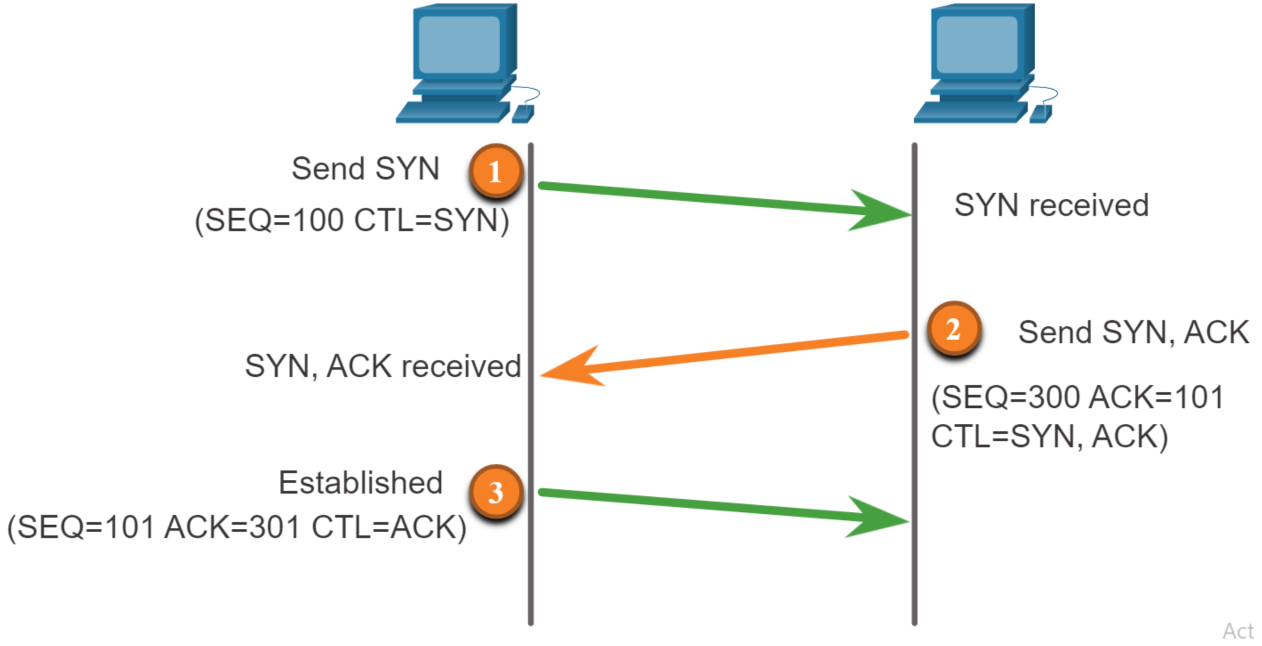
TCP provides these services:

- **Reliable delivery** – TCP incorporates acknowledgments to guarantee delivery, instead of relying on upper layer protocols to detect and resolve errors. If a timely acknowledgement is not received, the sender retransmits the data. Requiring acknowledgments of received data can cause substantial delays. Examples of application layer protocols that make use of TCP reliability include HTTP, SSL/TLS, FTP, DNS zone transfers, and others.
- **Flow control** – TCP implements flow control to address this issue. Rather than acknowledge with a single acknowledgment segment.
- **Stateful communication** – TCP stateful communication between two parties occurs during the TCP three-way handshake. Before data can be transferred using TCP, a three-way handshake opens the TCP connection, as shown in the figure.

TCP three-Way Handshake

A TCP connection is established in three steps:

1. The initiating client requests a client-to-server communication session with server.
2. The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
3. The initiating client acknowledges the server-to-client communication session.



TCP Attacks

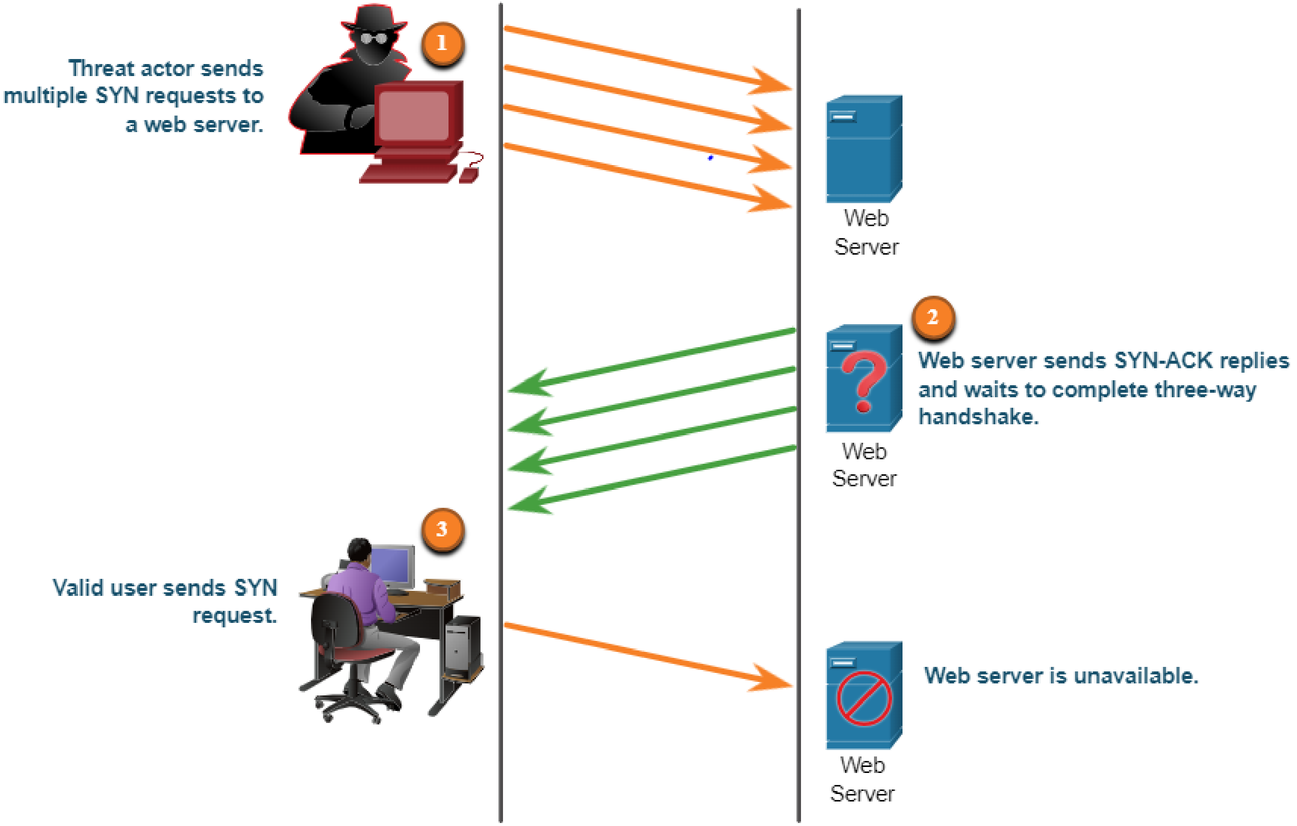
Network applications use TCP or UDP ports. Threat actors conduct port scans of target devices to discover which services they offer.

TCP SYN Flood Attack

The TCP SYN Flood attack exploits the TCP three-way handshake. The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target. The target devices replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelm with half-open TCP connections, and TCP services are denied to legitimate users.

TCP SYN Flood Attack

1. The threat actor sends multiple SYN requests to a web server.
2. The web server replies with SYN-ACKs for each SYN request and waits to complete the three-way handshake. The threat actor does not respond to the SYN-ACKs.
3. A valid user cannot access the web server because the web server has too many half-opened TCP connections.


Threat actor sends multiple SYN requests to a web server.
1
Web Server
2
Web server sends SYN-ACK replies and waits to complete three-way handshake.
Web Server
3
Valid user sends SYN request.
Web server is unavailable.
Web Server

TCP Reset Attack

A TCP reset attack can be used to terminate TCP communications between two hosts. TCP can terminate a connection in a civilized manner and uncivilized manner.

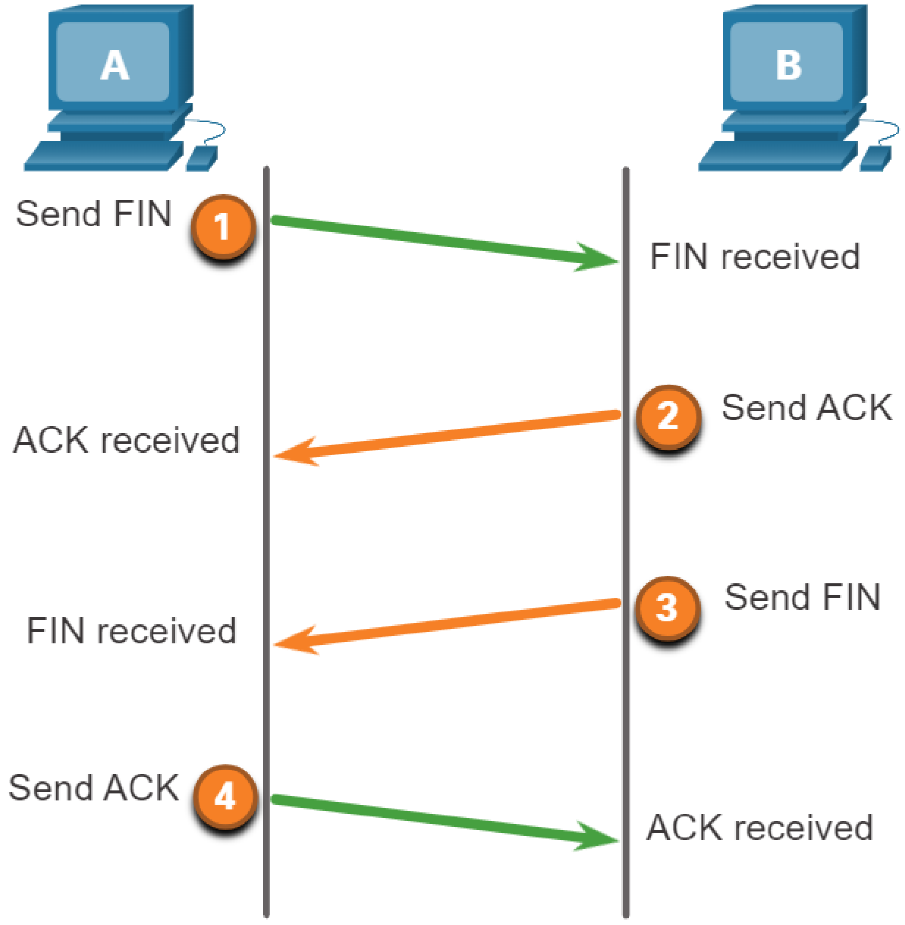
The figure displays the civilized manner when TCP uses a four-way exchange consisting of a pair of FIN and ACK segments from each TCP endpoint to close the TCP connection.

The uncivilized manner is when a host receives an TCP segment with the RST bit set. This is an abrupt way to tear down the TCP connection and inform the receiving host to immediately stop using the TCP connection.

Terminating a TCP connection

Terminating a TCP session uses following four-way exchange process:

1. When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
2. The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
3. The server sends a FIN to the client to terminate the server-to-client session
4. The client responds with an ACK to acknowledge the FIN from the server.



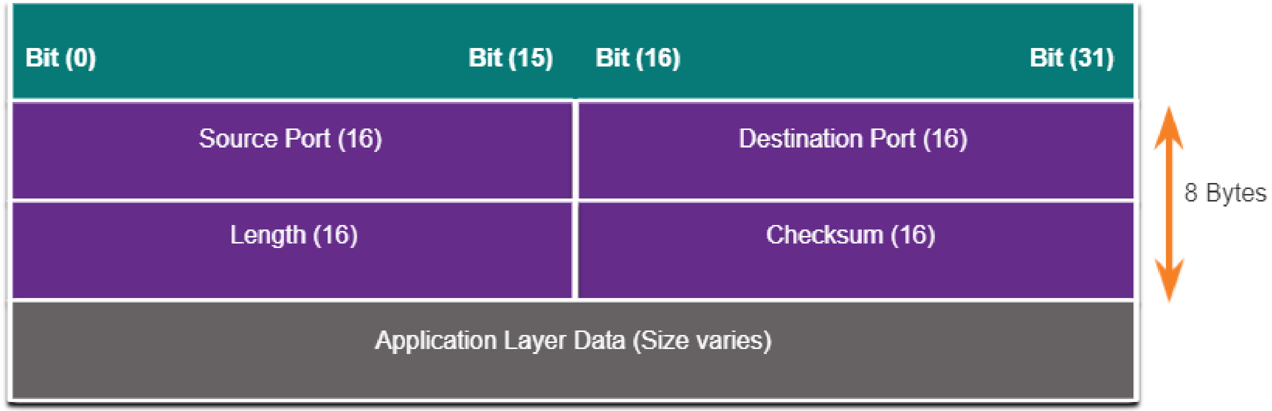
A sends ACK response to B

TCP Session Hijacking

TCP session hijacking is another TCP vulnerability. Although difficult to conduct, a threat actor takes over an already-authenticated host as it communicates with the target. The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not received, data from target device.

UDP Segment Header and Operation

UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol. It has much lower overhead than TCP because it is not connection-oriented and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability. The UDP segment structure, shown in the figure, is much smaller than TCP's segment structure.



Bit (0) Bit (15) Bit (16) Bit (31)

Source Port (16) Destination Port (16)

Length (16) Checksum (16)

Application Layer Data (Size varies)

8 Bytes

UDP attacks

UDP is not protected by any encryption. You can add encryption to UDP, but it is not available by default. The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination. Changing the data in the traffic will alter the 16-bit checksum, but the checksum is optional and is not always used. When the checksum is used, the threat actor can create a new checksum based on the new data payload, and then record it in the header as a new checksum. The destination device will find that the checksum matches the data without knowing that the data has been altered. This type of attack is not widely used.

UDP Flood Attacks

You are more likely to see a UDP flood attack. In a UDP flood attack, all the resources on a network are consumed. The threat actor must use a tool like a UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood UDP packets, often from a spoofed host, to a server on the subnet. The program will sweep through all the known ports trying to find closed port. This will cause the server to reply with an ICMP port unreachable message. Because there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

THANK YOU!

ICT 024

IP Vulnerabilities and Threats

Topic 2

Prepared by: Calix Olaguer

IPv4 and IPv6

IP does not validate whether the source IP address contained in a packet actually came from that source. For this reason, threat actors can send packets using a spoofed source IP address. Threat actors can also tamper with the other fields in the IP header to carry out their attacks. Security analysts must understand the different fields in both the IPv4 and IPv6 headers.

Some of the more common IP related attacks are shown in the table.

IP Attack Techniques	Description
ICMP attacks	Threat actors use Internet Control Message Protocol (ICMP) echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
Amplification and reflection attacks	Threat actors attempt to prevent legitimate users from accessing information or services using DoS and DDoS attacks.
Address spoofing attacks	Threat actors spoof the source IP address in an IP packet to perform blind spoofing or non-blind spoofing.
Man-in-the-middle attack (MITM)	Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They could eavesdrop by inspecting captured packets, or alter packets and forward them to their original destination.
Session hijacking	Threat actors gain access to the physical network, and then use an MITM attack to hijack a session.

ICMP Attacks

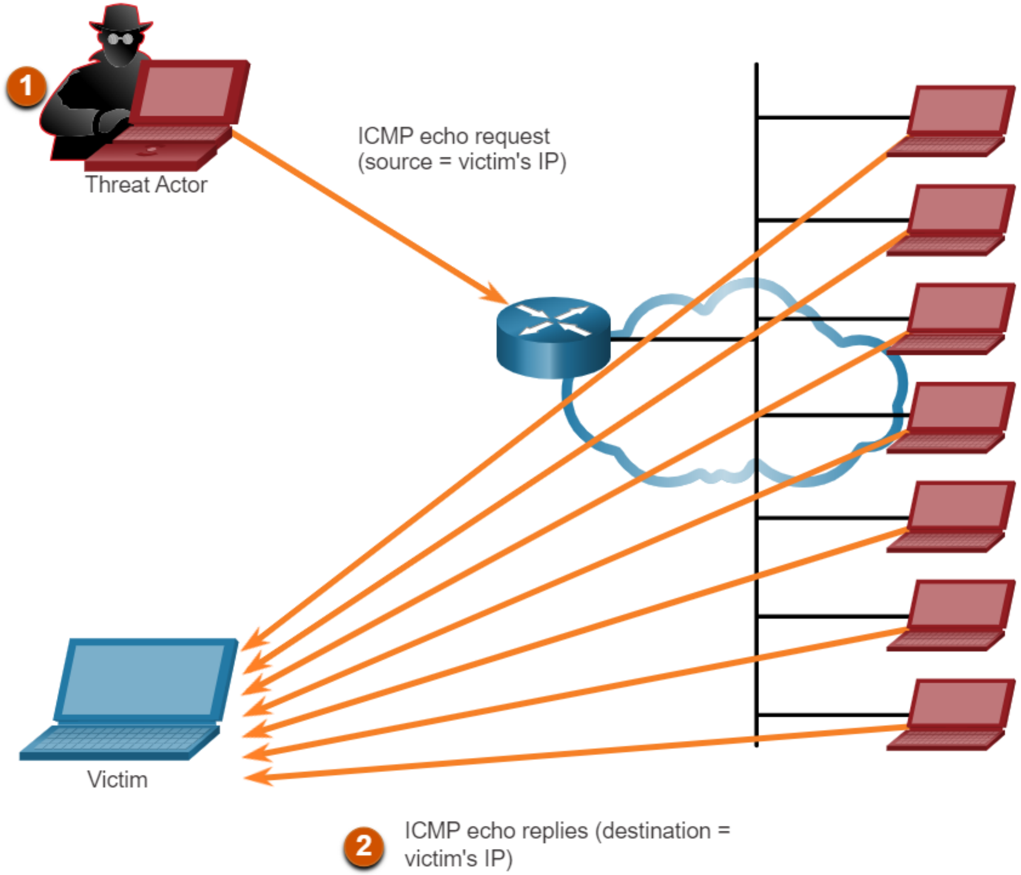
Threat actors use ICMP for reconnaissance and scanning attacks. They can launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors also use ICMP for DoS attacks.

Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet. Security analysts should be able to detect ICMP-related attacks by looking at captured traffic and log files. In the case of large networks, security devices such as firewalls and intrusion detection systems (IDS) detect such attacks and generate alters to the security

ICMP Messages used by Hackers	Description
ICMP echo request and echo reply	This is used to perform host verification and DoS attacks.
ICMP unreachable	This is used to perform network reconnaissance and scanning attacks.
ICMP mask reply	This is used to map an internal IP network.
ICMP redirects	This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.
ICMP router discovery	This is used to inject bogus route entries into the routing table of a target host

Amplification and Reflection Attacks

Threat actors often use amplification and reflection techniques to create DoS attacks. The example in the figure illustrates how an amplification and reflection techniques called a Smurf attack is used to overwhelm a target host.



1. **Amplification** – The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.
2. **Reflection** – these hosts all reply to the spoofed IP address of the victim to overwhelm it.

Threat actors also use resources exhaustion attacks. These attacks consume the resources of a target host to either to crash it or to consume the resources of a network.

Address Spoofing Attacks

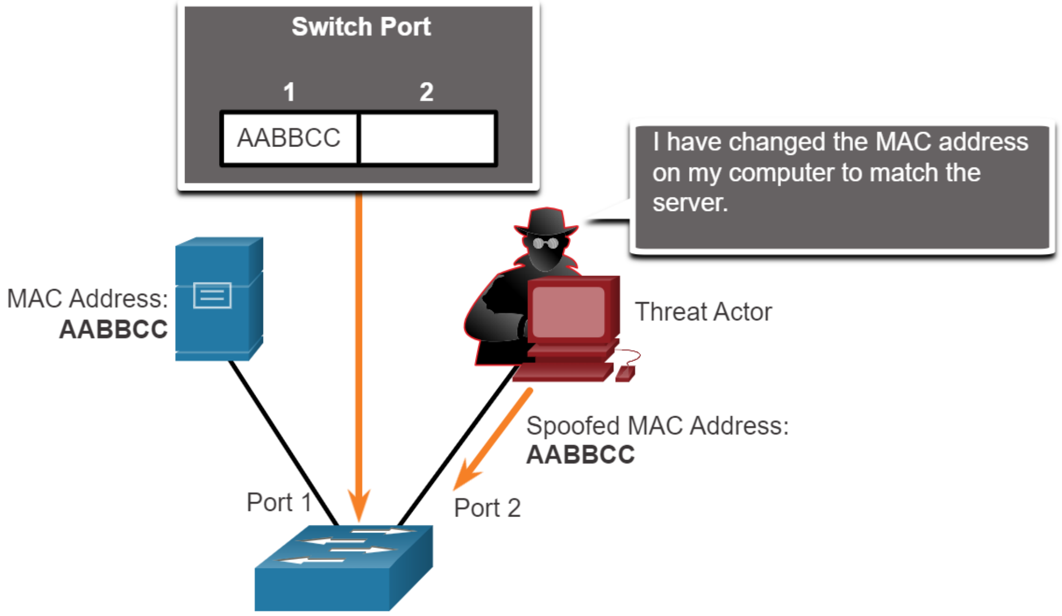
IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations. Spoofing is usually incorporated into another attack such as a Smurf attack.

Spoofing attacks can be non-blind or blind:

- **Non-blind spoofing** – The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction . It can also hijack an authorized session.
- **Blind spoofing** – The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

MAC address spoofing attacks are used when threat actors have access to the internal network. Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure. The attacking host then sends a frame throughout the network with the newly-configured MAC address. When the switch receives the frame, it examines the source MAC address.

Threat Actor Spoofs a Server’s MAC address.



Switch Port

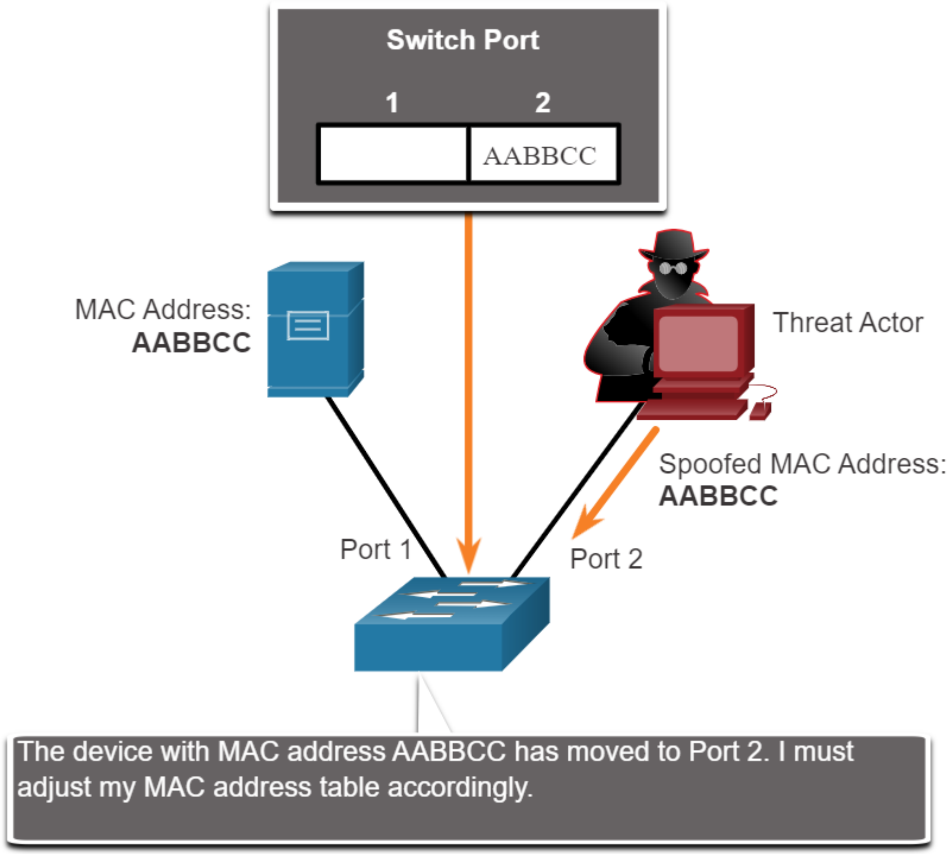
1	2
AABBCC	

I have changed the MAC address on my computer to match the server.

Activat

The switch overwrites the current CAM table entry and assigns the MAC address to the new port, as shown in the figure. It then forwards frames destined for the target host to the attacking host.

Switch Updates CAM Table with spoofed Address



Switch Port

1	2
	AABBCC

The device with MAC address AABBCC has moved to Port 2. I must adjust my MAC address table accordingly.

Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MITM condition

THANK YOU!

School of
Nation Builders

NATIONAL COLLEGE OF
SCIENCE & TECHNOLOGY

COMPUTER STUDIES DEPARTMENT

ICT 024

SOCIAL ENGINEERING ATTACKS

TOPIC 1

Prepared by: Calix Olaguer

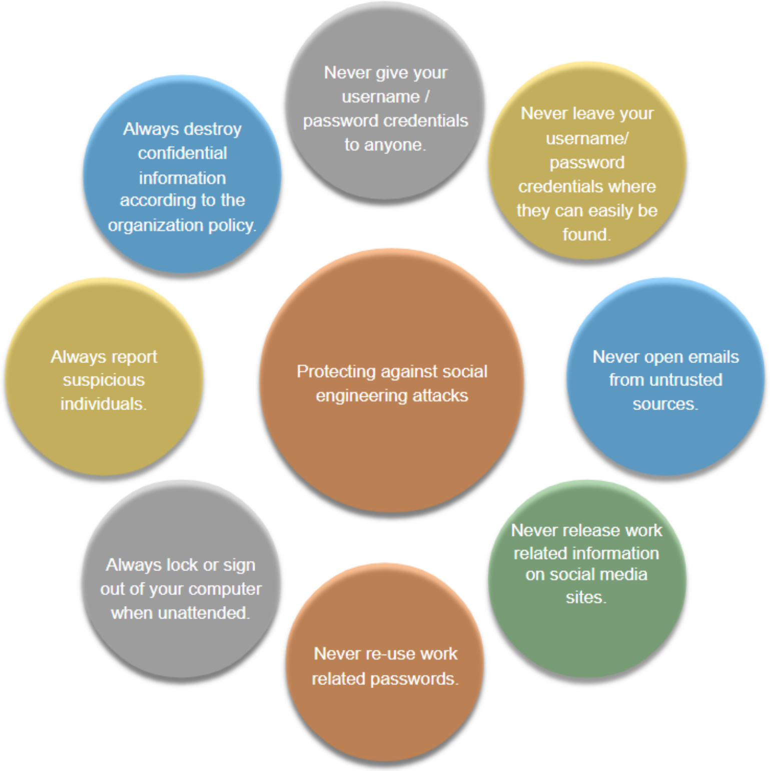
Social Engineering Attacks

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Some social engineering techniques are performed in-person while others may use the

Social Engineering Attack	Description
Pretexting	A threat pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
Spear phishing	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Also known as junk mail, this is unsolicited email which often containts harmful links, malware, or deceptive.

Social Engineering Attack	Description
Something for Something	Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.
Impersonation	This type of attack is where a threat actor pretends to be someone they are not to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents.

The **Social Engineering Toolkit (SET)** was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks.


Protecting against social engineering attacks

Never give your username / password credentials to anyone.

Never leave your username/ password credentials where they can easily be found.

Never open emails from untrusted sources.

Never release work related information on social media sites.

Never re-use work related passwords.

Always lock or sign out of your computer when unattended.

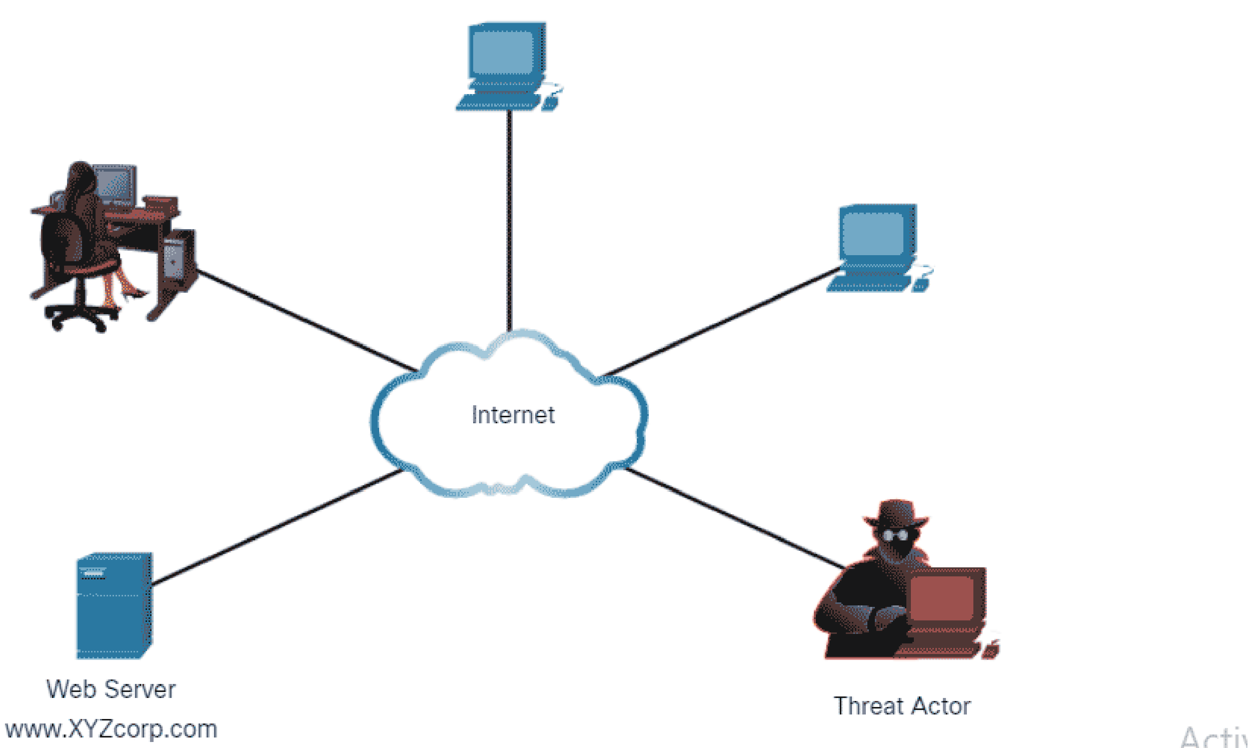
Always report suspicious individuals.

Always destroy confidential information according to the organization policy.

A **Denial of Service (DoS)** attack crates some sort of interruption of network services to users, devices, or applications. There are two major types of DoS attacks:

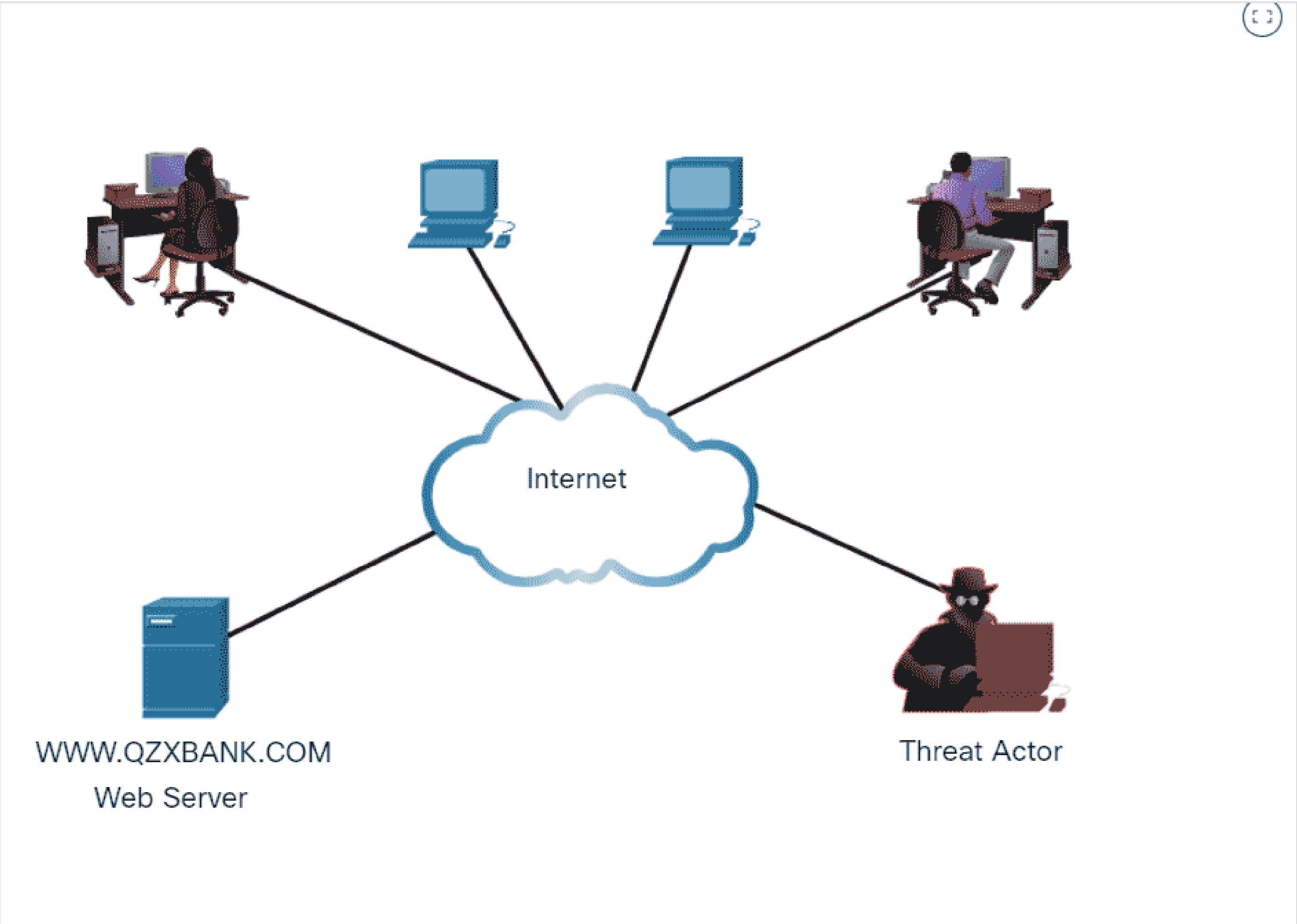
- **Overwhelming Quantity of Traffic** – The threat actor sends an enormous quantity of data at a rate that the network, hos**t**, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
- **Maliciously Formatted Packets** – The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.

DoS attacks are a major risk because they interrupt communication and cause significant a loss of time and money.



Acti

A **Distributed Denial of Service (DDoS)** is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, A threat actor builds a network of infected hosts, known as zombies The threat actor uses a command and control (CnC) system to send control messages to the zombies. The zombies constantly scan and infect more hosts with bot malware. The bot malware is designed to infect host, making it a zombie that can communicate with the CnC system. The collection of zombies is called a botnet. When ready, the threat actor instructs the CnC system to make the bot net of zombies carry out DDoS attack.


Internet
WWW.QZXBANK.COM
Web Server
Threat Actor

THANK YOU!