

Information Security Operations Center

Prepared by
Dr. Ibrahim Gomaa

جامعة الجميع الذكية

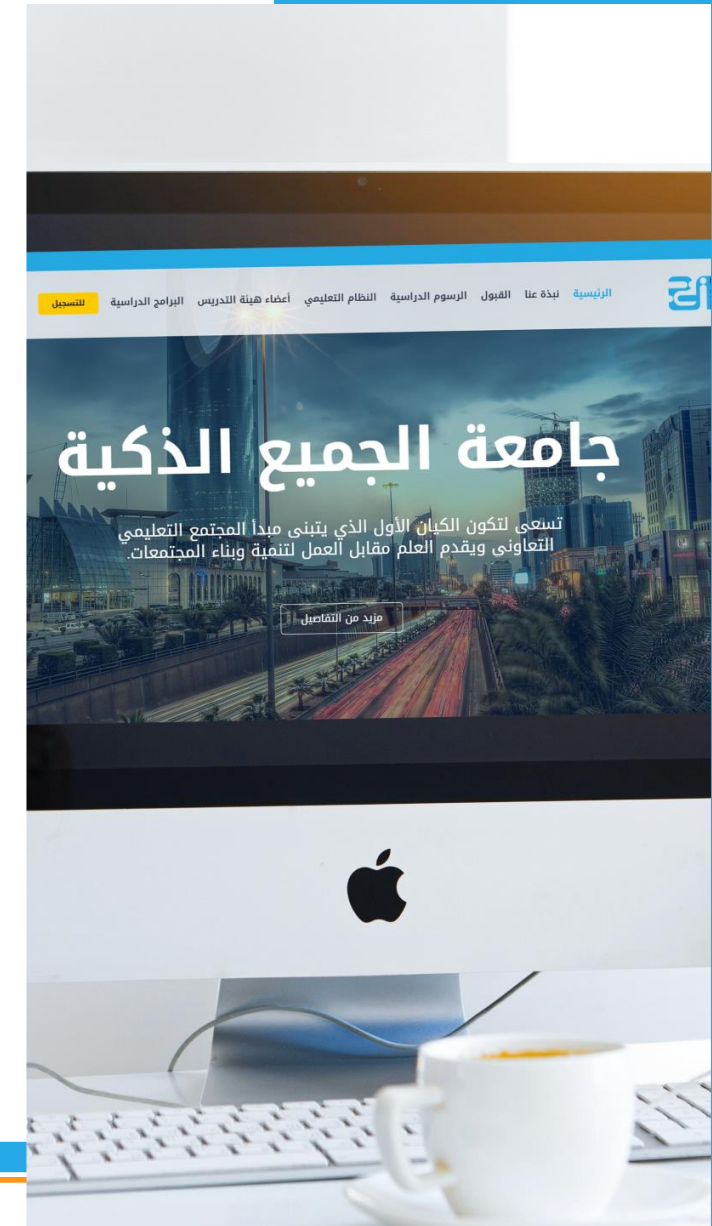
تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 4: Network Attacks Types

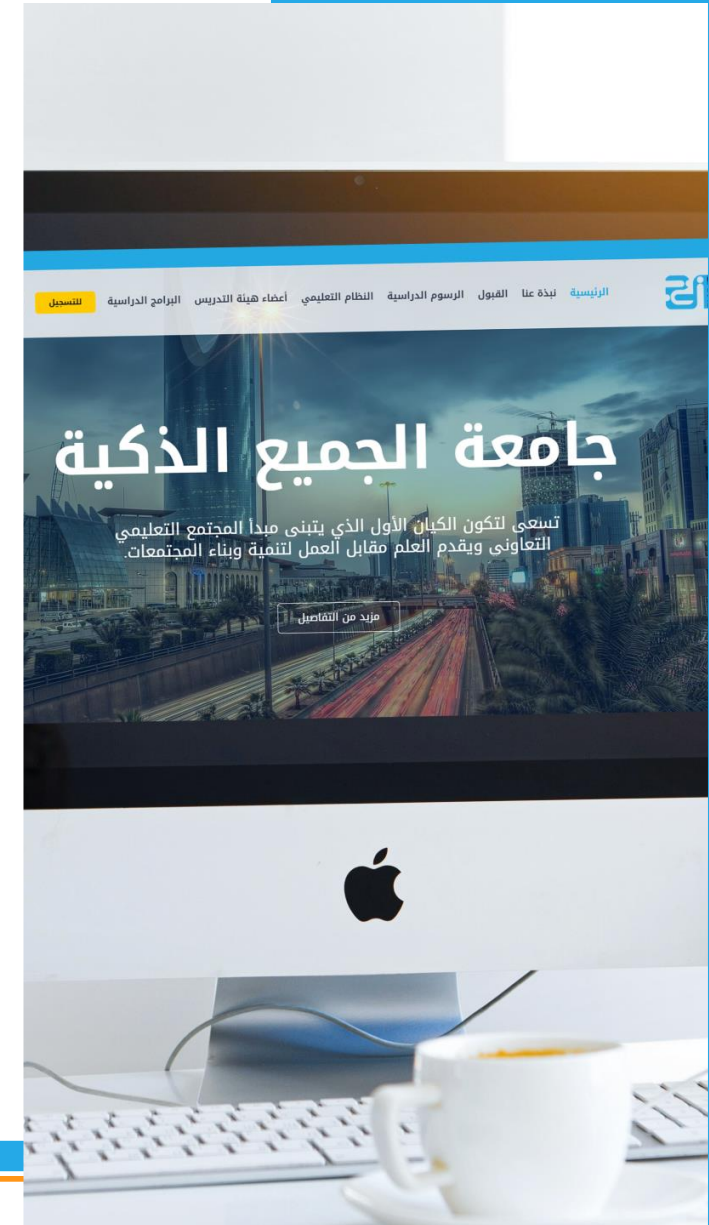


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Topic Title	Topic Objective
Who is Attacking our Network	Explain how network threats have evolved.
Threat Actor Tools	Describe the various types of attack tools used by Threat Actors.
Malware	Describe types of malware.
Common Network Attacks - Reconnaissance, Access, and Social Engineering, DoS, DDos	Explain reconnaissance, access, social engineering network attacks, DoS and DDos



Who is Attacking our Network



Threat, Vulnerability, and Risk

Attackers want to access our assets such as data and other intellectual property, servers, computers, smart phones, tablets, and so on



Threat, Vulnerability, and Risk (Contd.)

To understand network security, it is important to know the following terms:

TERM	EXPLANATION
Threat	A potential danger to an asset such as data or the network itself.
Vulnerability	A weakness in a system or its design that could be exploited by a threat.
Attack Surface	An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system.
Exploit	The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. In a local exploit, the threat actor has some type of user or administrative access to the end system. It does not necessarily mean that the attacker has physical access to the end system.
Risk	The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.

Threat, Vulnerability, and Risk (Contd.)

Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset.

Four ways to manage risk:

Risk Management Strategy	Explanation
Risk acceptance	When the cost of risk management options outweighs the cost of risk, the risk is accepted, and no action is taken.
Risk avoidance	This means avoiding any exposure to risk by eliminating the activity, thus resulting in losing any benefits from the activity.
Risk reduction	This reduces the exposure to risk. It is the most commonly used risk mitigation strategy. This strategy requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity that is at risk.
Risk transfer	Some or all of the risk is transferred to a willing third party such as insurance company.

Hacker vs. Threat Actor

‘Hacker’ is a common term used to describe a threat actor. Hacker has a variety of meanings that are as follows:

- A clever programmer capable of developing new programs and making coding changes to existing programs to make them more efficient.
- A network professional that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- An individual who run programs to prevent or corrupt data on servers.

Types of hackers:

- White Hat hackers
- Gray Hat hackers
- Black Hat hackers

Hacker vs. Threat Actor (Contd.)

White Hat Hackers:

- White hat hackers are ethical hackers who use their programming skills for good, ethical, and legal purposes.

Gray Hat Hackers:

- Grey hat hackers are individuals who commit crimes and unethical things, but not for personal gain or to cause damage.

Black Hat Hackers:

- Black hat hackers are unethical criminals who violate computer and network security for personal gain.

Note: The term ‘threat actor’ is used when referring to individuals or groups that could be classified as gray or black hat hackers.



Evolution of Threat Actors

Types of Threat Actors:

- **Script kiddies** - It refers to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
- **Vulnerability brokers** - It refers to grey hat hackers who attempt to discover exploits and report them to vendors, for prizes or rewards.
- **Hacktivists** - It refers to grey hat hackers who rally and protest against different political and social ideas.
- **Cybercriminals** - It refers to black hat hackers who are either self-employed or working for large cybercrime organizations.
- **State-sponsored** - State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations.



Evolution of Threat Actors

Types of Threat Actors:

- **Script kiddies** - It refers to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
- **Vulnerability brokers** - It refers to grey hat hackers who attempt to discover exploits and report them to vendors, for prizes or rewards.
- **Hactivists** - It refers to grey hat hackers who rally and protest against different political and social ideas.
- **Cybercriminals** - It refers to black hat hackers who are either self-employed or working for large cybercrime organizations.
- **State-sponsored** - State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations.



Cybersecurity Tasks

- Threat actors target the home users, small-to-medium sized businesses, as well as large public and private organizations.
- Hence, Cybersecurity is a shared responsibility which all users must practice to make the internet and networks safer and more secure.
- Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those mentioned in the figure.



Indicators Of Compromise (IOC)

- IOCs are the evidence that an attack has occurred, and each attack has unique identifiable attributes.
- IOCs can be features that identify malware files, IP addresses of servers that are used in attacks, filenames, and characteristic changes made to end system software, among others.
- IOCs help cybersecurity personnel identify what has happened in an attack and develop defenses against the attack.

```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0
sha1   eb019ad1c73ee69195c3fc84ebf44e95c147bef8
md5    3a104b73bb96dfed288097e9dc0a11a8

DNS requests
domain log.studiox.link
domain my.studiox.link
domain _sips._tcp.studiox.link
domain sip.studiox.link

Connections
ip     198.51.100.248
ip     203.0.113.82
```

Summary of the IOC for a piece of malware

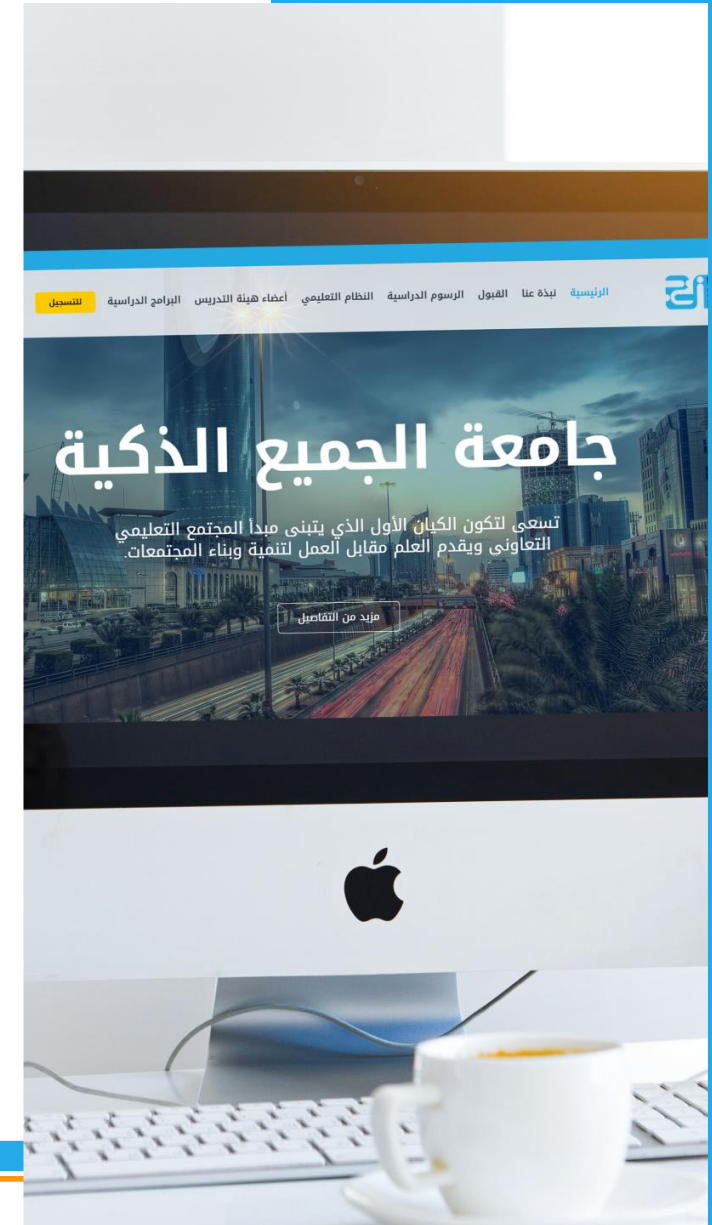
Indicators of Attack (IOA)

- IOA focus more on the motivation and strategies behind an attack and the attackers to gain access to assets.
- IOAs helps to generate a proactive security approach that can be reused in multiple contexts and multiple attacks. Defending against a strategy can therefore prevent future attacks.

Threat Sharing and Building Cybersecurity Awareness

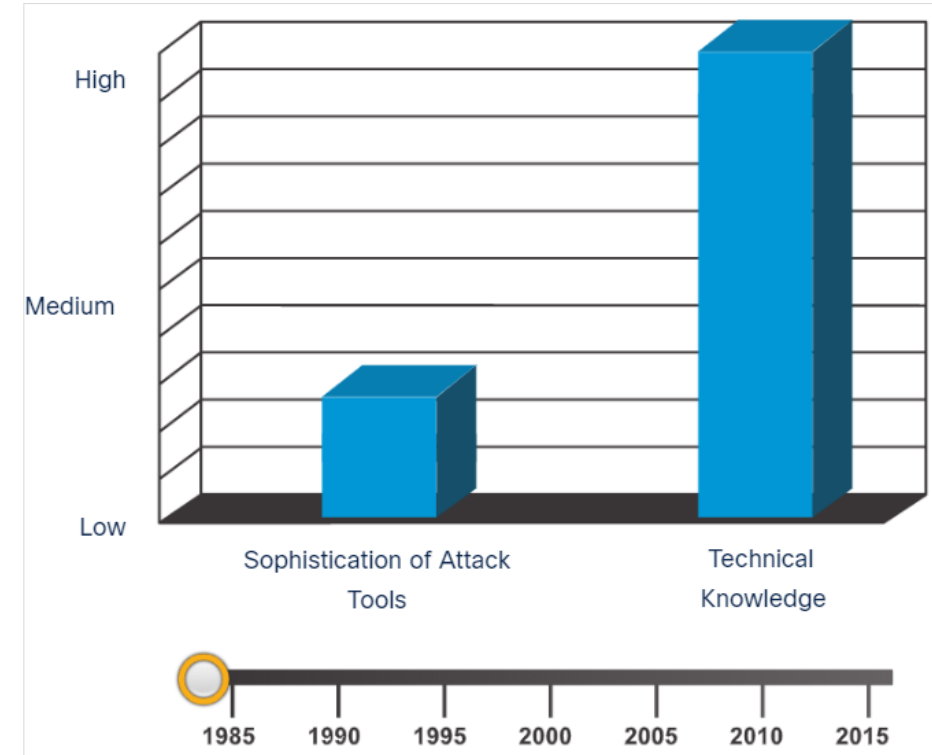
- Governments are now actively promoting cybersecurity.
- The US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost.
- CISA use a system called Automated Indicator Sharing (AIS) which enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified.
- The European Union Agency for Cybersecurity (ENISA) delivers advice and solutions for the cybersecurity challenges of the EU member states.
- The CISA and the National Cyber Security Alliance (NCSA) have an annual campaign in every October called National Cybersecurity Awareness Month (NCASM) to raise awareness about cybersecurity.

Threat Actor Tools



Introduction of Attack Tools

- To exploit vulnerability, a threat actor must have a technique or tool.
- Over the years, attack tools have become more sophisticated, and highly automated.
- These new tools require less technical knowledge to implement.
- In the figure, drag the white circle across the timeline to view the relationship between the sophistication of attack tools versus the technical knowledge required to use them.



Evolution of Security Tools

- Ethical hacking involves using many different types of tools to test the network and end devices.
- To validate the security of a network and its systems, many network penetration testing tools have been developed and many of these tools can also be used by threat actors for exploitation.
- Threat actors have also created various hacking tools. Cybersecurity personnel must also know how to use these tools when performing network penetration tests.

Note: *Most of these tools are UNIX or Linux based; therefore, a security professional should have a strong UNIX and Linux background.*

Evolution of Security Tools (Contd.)

The following table lists some of the categories of common network penetration testing tools

Categories of Tools	Description
Password crackers	Used to crack or recover the password. Eg: John the Ripper, Ophcrack
Wireless hacking tools	Used to intentionally hack into a wireless network to detect security vulnerabilities. Eg: Aircrack-ng, Kismet
Network scanning and hacking tools	Used to probe network devices, servers, and hosts for open TCP or UDP ports. Eg: Nmap, SuperScan
Packet crafting tools	Used to probe and test a firewall's robustness. Eg: Hping, Scapy
Packet sniffers	Used to capture and analyze packets within traditional Ethernet LANs or WLANs. Eg: Wireshark, Tcpdump
Rootkit detectors	It is a directory and file integrity checker used by white hats to detect installed root kits. Eg: AIDE, Netfilter
Fuzzers to search vulnerabilities	Used by threat actors when attempting to discover a computer system's security vulnerabilities. Eg: Skipfish, Wapiti

Evolution of Security Tools (Contd.)

Categories of Tools	Description
Forensic tools	White hat hackers use these tools to sniff out any trace of evidence existing in a particular computer system. Eg: Sleuth Kit, Helix
Debuggers	Used by black hats to reverse engineer binary files when writing exploits and used by white hats when analyzing malware. Eg:GDB, WinDbg
Hacking operating systems	These are preloaded with tools and technologies optimized for hacking. Eg: Kali Linux, SELinux
Encryption tools	These tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Eg: VeraCrypt, CipherShed
Vulnerability exploitation tools	These tools identify whether a remote host is vulnerable to a security attack. Eg: Metasploit, Core Impact
Vulnerability scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Eg:Nipper, Securia PSI

Categories of Attacks

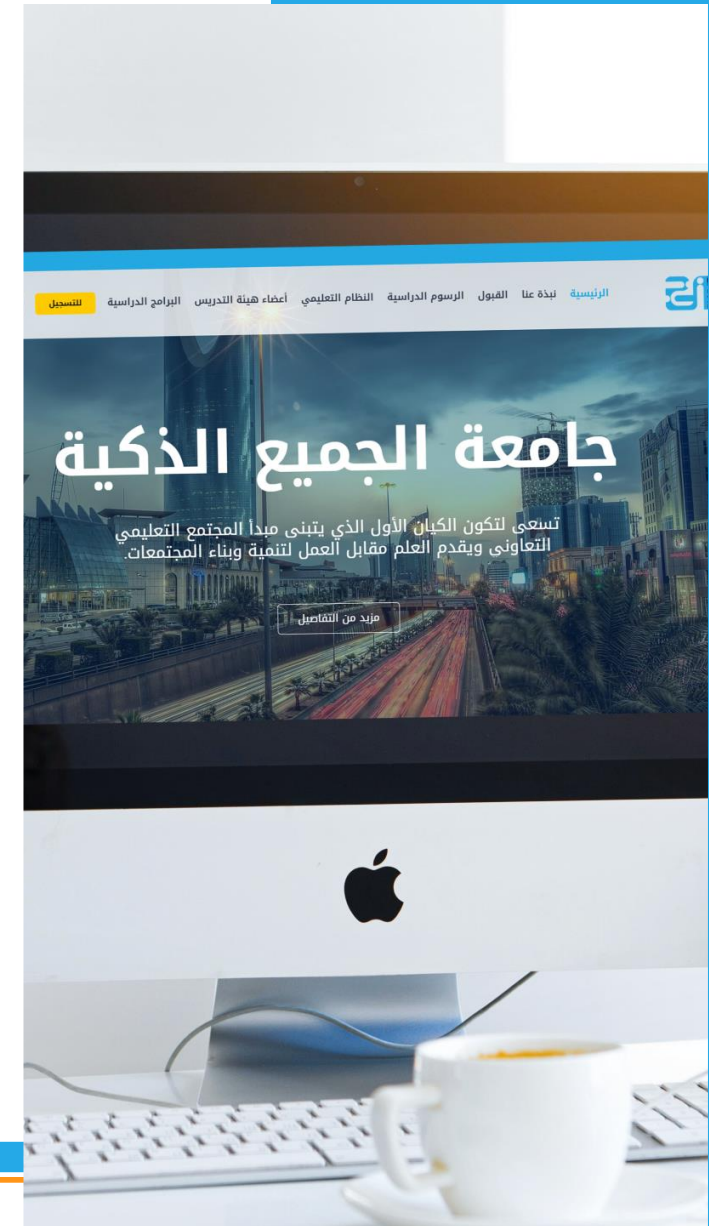
- Threat actors use the previously mentioned tools or a combination of tools to create various attacks.
- It is important to understand that threat actors use a variety of security tools to carry out these attacks.
- The following table displays common types of attacks.

Categories of Attack	Description
Eavesdropping attack	An eavesdropping attack is when a threat actor captures and listens to network traffic. This is also called as sniffing or snooping.
Data modification attack	Data modification attacks occur when a threat actor has captured enterprise traffic and has altered the data in the packets without the knowledge of the sender or receiver.
IP address spoofing attack	An IP address spoofing attack is when a threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

Categories of Attacks (Contd.)

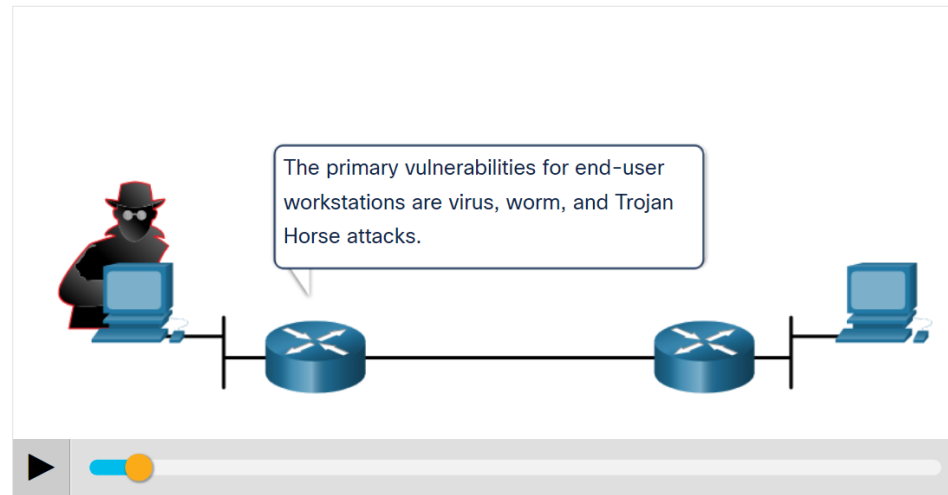
Categories of Attack	Description
Password-based attacks	Password-based attacks occur when a threat actor obtains the credentials for a valid user account.
Denial-of-service (DoS) attack	A DoS attack prevents normal use of a computer or network by valid users. This attack can block traffic, which results in a loss of access to network resources.
Man-in-the-middle attack (MiTM)	A MiTM attack occurs when threat actors have positioned themselves between a source and destination.
Compromised key attack	A compromised-key attack occurs when a threat actor obtains a secret key. A compromised key can be used to gain access to a secured communication without the sender or receiver.
Sniffer attack	A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

Malware



Types of Malware

- Malware is a code or software designed to damage, disrupt, steal, or inflict some other ‘bad’ or illegitimate action on data, hosts, or networks.
- The three most common types of malware are Virus, Worm, and Trojan horse.
- Play the animation to view examples of the different malware types.



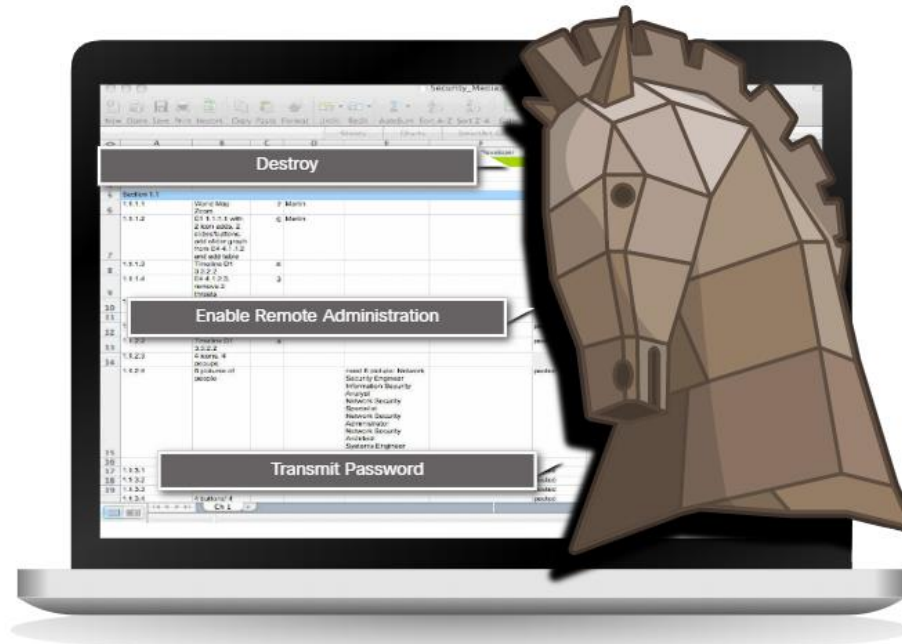
- A virus is a type of malware that spreads by inserting a copy of itself into another program.
- After the program is run, viruses spread from one computer to another, thus infecting the computers.
- A simple virus may install itself at the first line of code in an executable file.
- Viruses can be harmless, for those that display a picture on the screen, or they can be destructive. They can also modify or delete files on the hard drive.
- Most viruses spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are a common type of virus.

Trojan Horses

- Trojan horse malware is a software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.
- Trojans are found attached to online games.
- Users are commonly tricked into loading and executing the Trojan horse on their systems
- The Trojan horse concept is flexible.
- It can cause immediate damage, provide remote access to the system, or access through a back door.
- Custom-written Trojan horses with a specific target are difficult to detect.

Trojan Horses Classification

- Trojan horses are usually classified according to the damage that they cause, or the way they breach a system.



Trojan Horses Classification (Contd.)

The types of Trojan horses are as follows:

Type of Trojan Horse	Description
Remote-access	Enables unauthorized remote access.
Data-sending	Provides the threat actor with sensitive data, such as passwords.
Destructive	Corrupts or deletes files.
Proxy	Uses the victim's computer as the source device to launch attacks and perform other illegal activities.
FTP	Enables unauthorized file transfer services on end devices.
Security software disabler	Stops antivirus programs or firewalls from functioning.
Denial of Service (DoS)	Slows or halts network activity.
Keylogger	Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form.

- Computer worms are like viruses because they replicate themselves by independently exploiting vulnerabilities in networks.
- Worms can slow down networks as they spread from system to system.
- Worms can run without a host program.
- However, once the host is infected, the worm spreads rapidly over the network.
- In 2001, the Code Red worm had initially infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers.



Initial Code Red Worm Infection

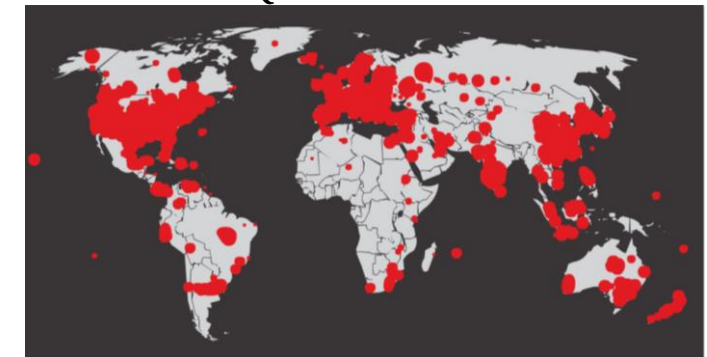


Code Red Infection 19 hours later

- The initial infection of the SQL Slammer worm is known as the worm that ate the internet.
- SQL Slammer was a Denial of Service (DoS) attack that exploited a buffer overflow bug in Microsoft's SQL Server.
- The number of infected servers doubled in size every 8.5 seconds.
- The infected servers did not have the updated patch that was released 6 months earlier.
- Hence it is essential for organizations to implement a security policy requiring updates and patches to be applied in a timely fashion.



Initial SQL Slammer Infection



SQL Slammer Infection 30 minutes later

- Ransomware is a malware that denies access to the infected computer system or its data.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used, when cybercriminals pretending to be security technicians make random calls at homes and persuade users to connect to a website that downloads ransomware to the user's computer.

- The examples of modern malware are as follows:

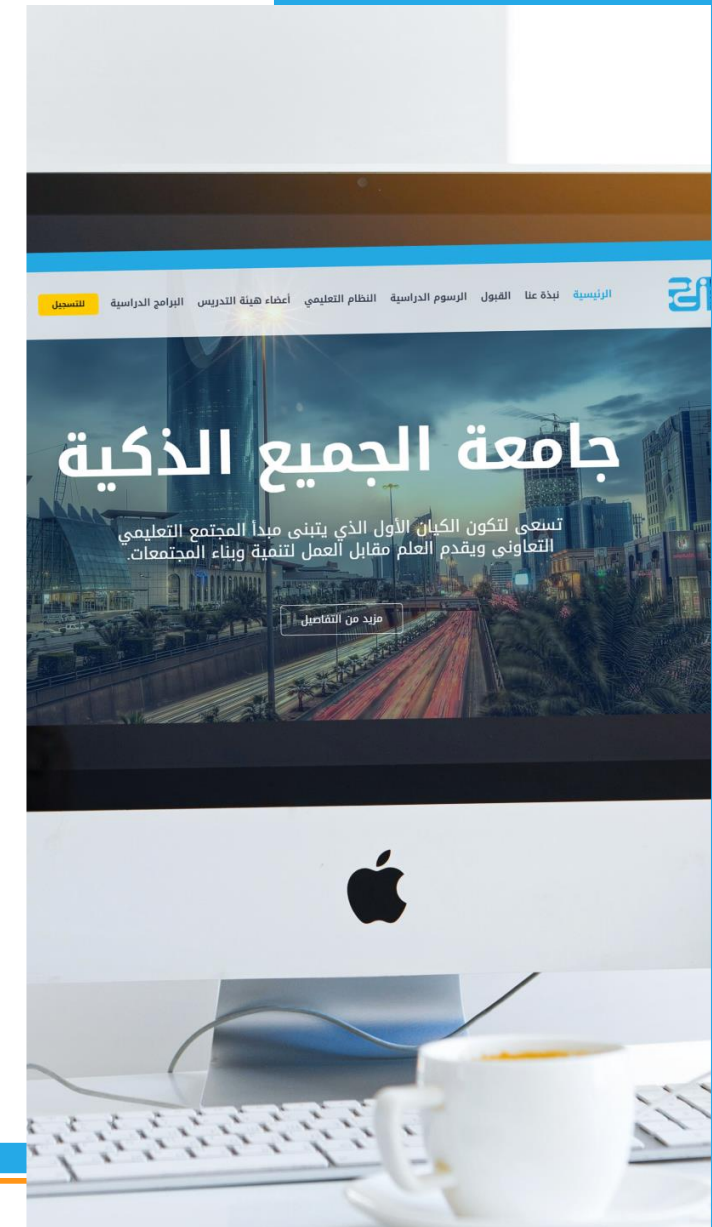
Type of Malware	Description
Scareware	Includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. It is generally directed at an unsuspecting user and attempts to persuade the user to infect a computer by taking action to address the bogus threat.
Phishing	Attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers.
Rootkits	Installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.
Spyware	Used to gather information about a user and send the information to another entity without the user's consent. Spyware can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers.
Adware	Displays annoying pop-ups to generate revenue for its author. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Common Malware Behaviors

- Computers infected with malware often exhibit one or more of the following symptoms:
 - Appearance of strange files, programs, or desktop icons
 - Antivirus and firewall programs are turning off or reconfiguring settings
 - Computer screen is freezing, or system is crashing
 - Emails are spontaneously being sent without your knowledge to your contact list
 - Files have been modified or deleted
 - Increased CPU and/or memory usage
 - Problems connecting to networks
 - Slow computer or web browser speeds
 - Unknown processes or services running
 - Unknown TCP or UDP ports open
 - Connections are made to hosts on the Internet without user action
 - Strange computer behavior

Note: Malware behavior is not limited to the above list.

Common Network Attacks - Reconnaissance, Access, Social Engineering, DoS and DDoS



Types of Network Attacks

- Malware is a means to get a payload delivered .
- When a payload is delivered and installed, it can be used to cause a variety of network-related attacks from the inside as well as from the outside.
- Network attacks are classified into three categories:
 - Reconnaissance Attacks
 - Access Attacks
 - DoS Attacks

Reconnaissance Attacks

- Reconnaissance is information gathering.
- Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Recon attacks precede access attacks or DoS attacks.

Reconnaissance Attacks (Contd.)

- The techniques used by malicious threat actors to conduct reconnaissance attacks are as follows:

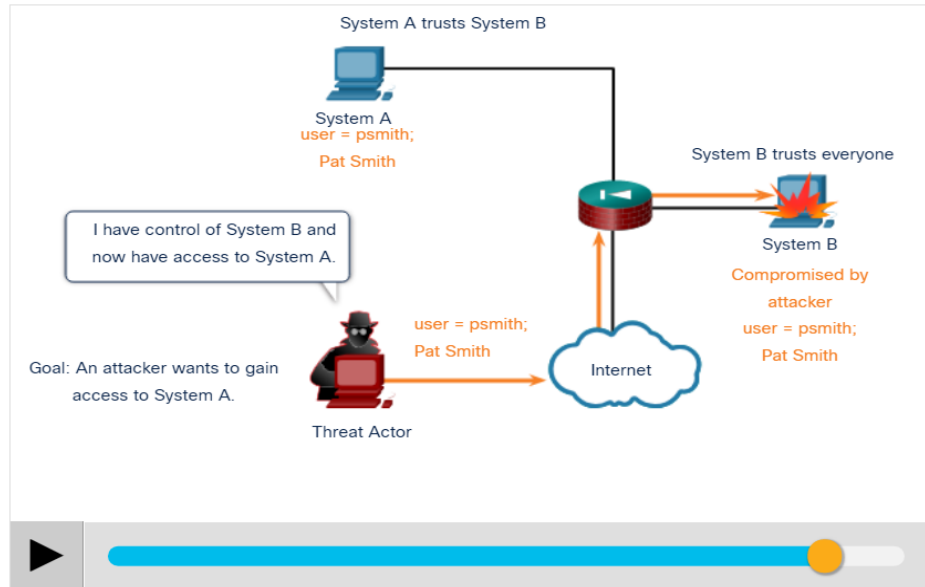
Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.
Initiate a ping sweep of the target network	The information query usually reveals the target's network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active.
Initiate a port scan of active IP addresses	This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScan Tools.
Run vulnerability scanners	This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, and Open VAS.
Run exploitation tools	The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Access Attacks

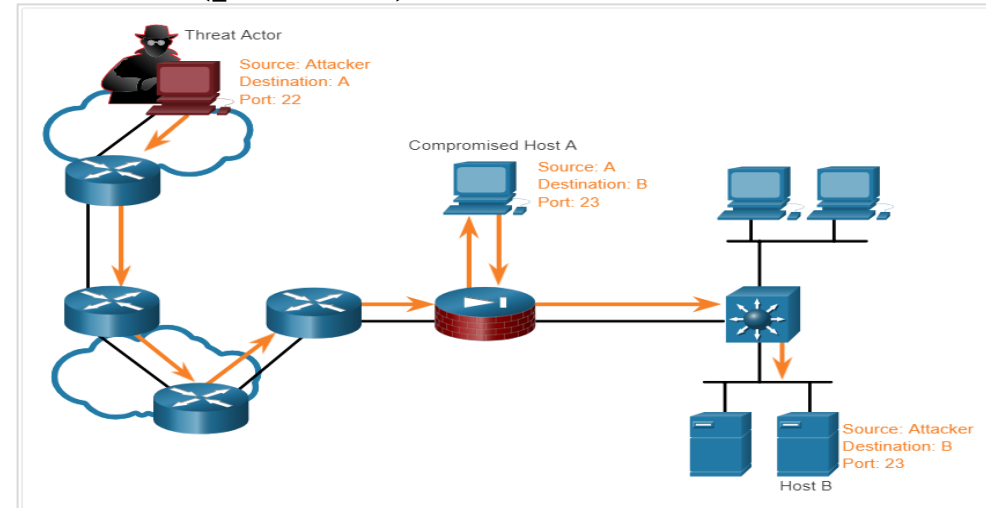
- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry into web accounts, confidential databases, and other sensitive information.
- Password Attacks
 - The threat actor attempts to discover critical system passwords using a variety of password cracking tools.
- Spoofing Attacks
 - The threat actor device attempts to pose as another device by falsifying data.
 - Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.
 - Trust exploitations
 - Port redirections
 - Man-in-the-middle attacks
 - Buffer overflow attacks

Access Attacks (Contd.)

- **Trust Exploitation Example:** Click Play in the figure to view an example of trust exploitation.

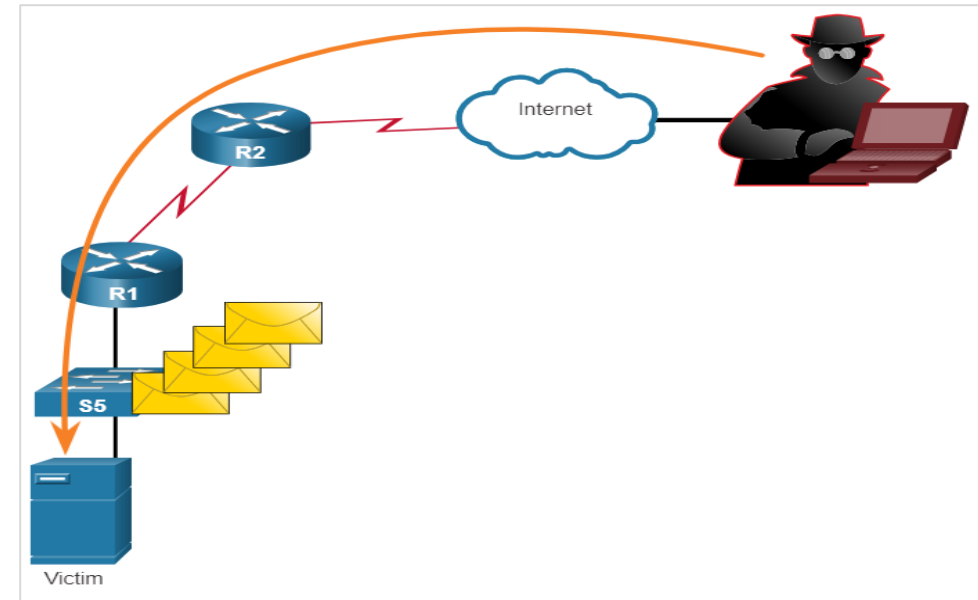
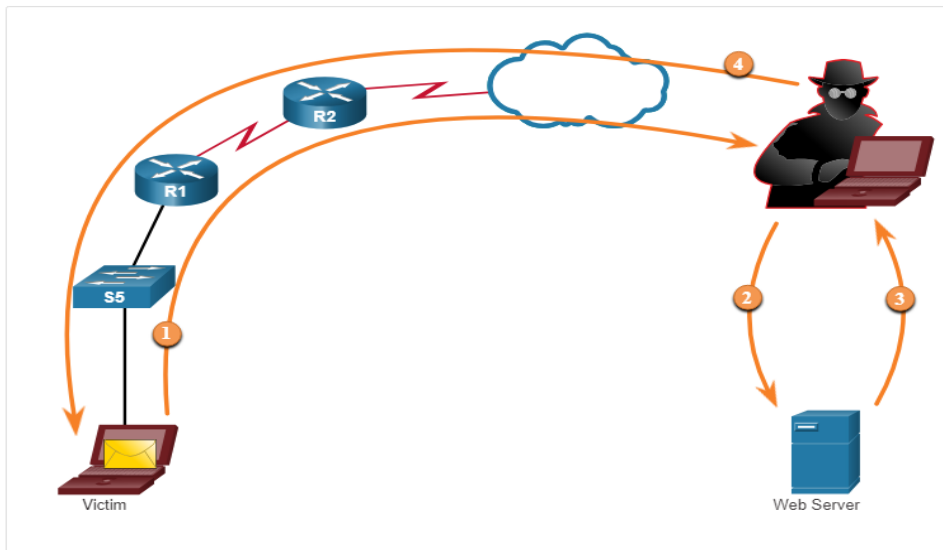


- **Port Redirection Example:** The example shows a threat actor using SSH (port 22) to connect to a compromised Host A trusted by Host B. Hence, the threat actor can use Telnet (port 23) to access it.



Access Attacks (Contd.)

- **Man-in-the-Middle Attack Example:** The figure displays an example of a man-in-the-middle attack.
- **Buffer Overflow Attack:** The figure shows that the threat actor is sending many packets to the victim in an attempt to overflow the victim's buffer.



Social Engineering Attacks

- Social Engineering is an access attack that attempts to manipulate individuals into performing actions or divulging into confidential information.
- Some social engineering techniques are performed in-person or via the telephone or internet.
- Social engineering techniques are explained in the below table.

Social Engineering Attack	Description
Pretexting	A threat actor 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 contains harmful links, malware, or deceptive content.

Social Engineering Attacks (Contd.)

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	In this type of attack, a threat actor pretends to be someone else 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.

Social Engineering Attacks (Contd.)

- The Social Engineer Toolkit (SET) was designed to help white hat hackers and other network security professionals to create social engineering attacks to test their own networks.
- Enterprises must educate their users about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.



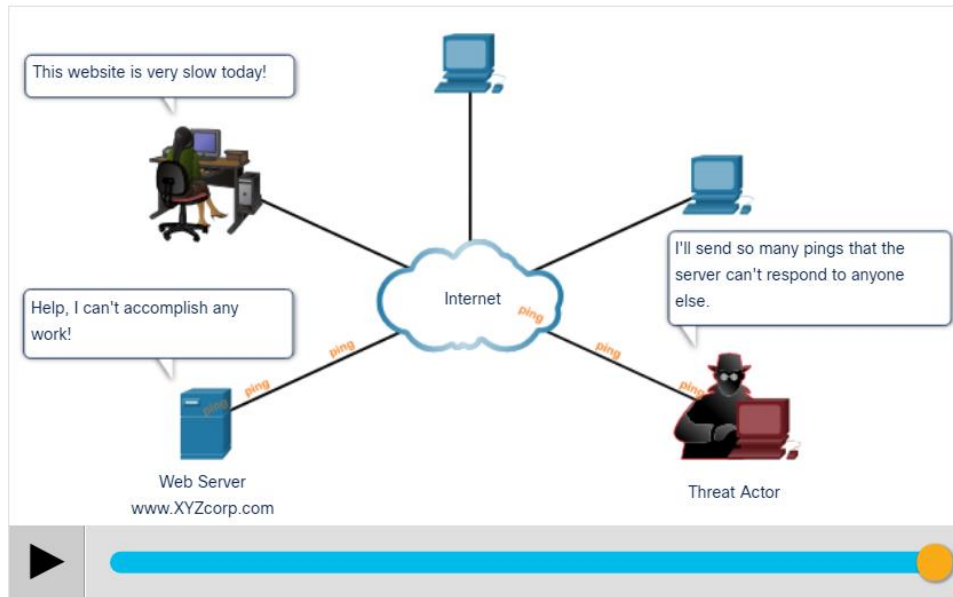
Social Engineering Protection Practices

Strengthening the Weakest Link

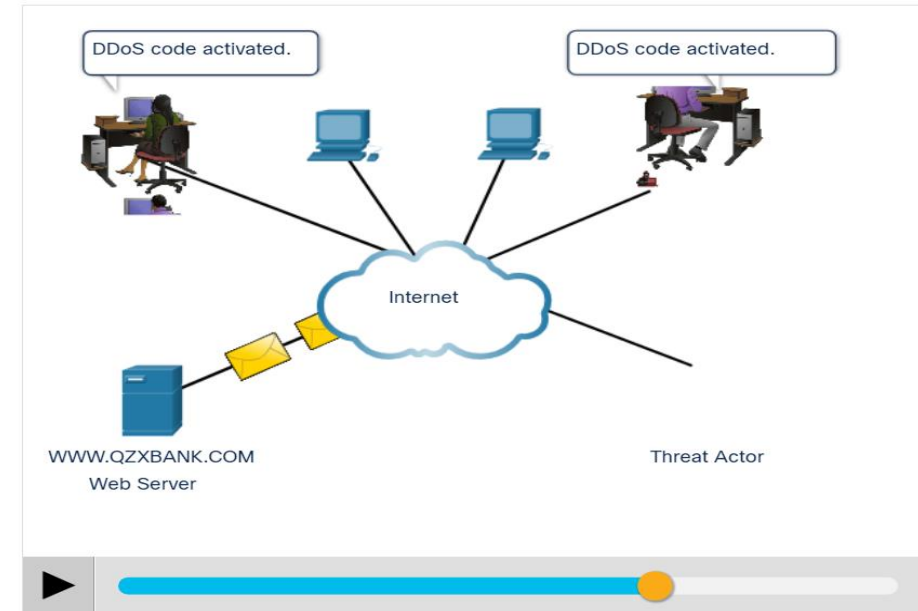
- Cybersecurity is as strong as its **weakest link**.
- The weakest link in cybersecurity can be the personnel within an organization, and social engineering is a major security threat.
- One of the most effective security measures that an organization can take is to train its personnel and create a ‘security-aware culture’.

DoS and DDoS Attacks

- **DoS Attack:** Click Play in the figure to view the animation of a DoS attack.



- **DDoS Attack:** Click Play in the figure to view the animations of a DDoS attack.



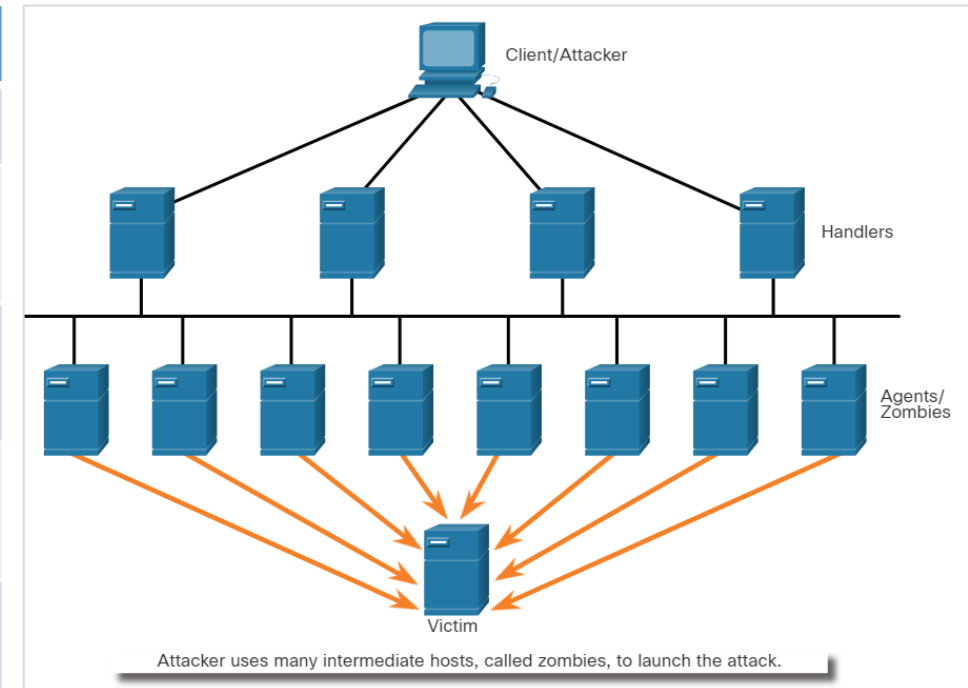
DoS and DDoS Attacks

- **A Denial of Service (DoS)** attack creates some sort of interruption in network services to users, devices, or applications. The two types of DoS attacks are as follows:
 - **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle.
 - **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it.

Components of DDoS Attacks

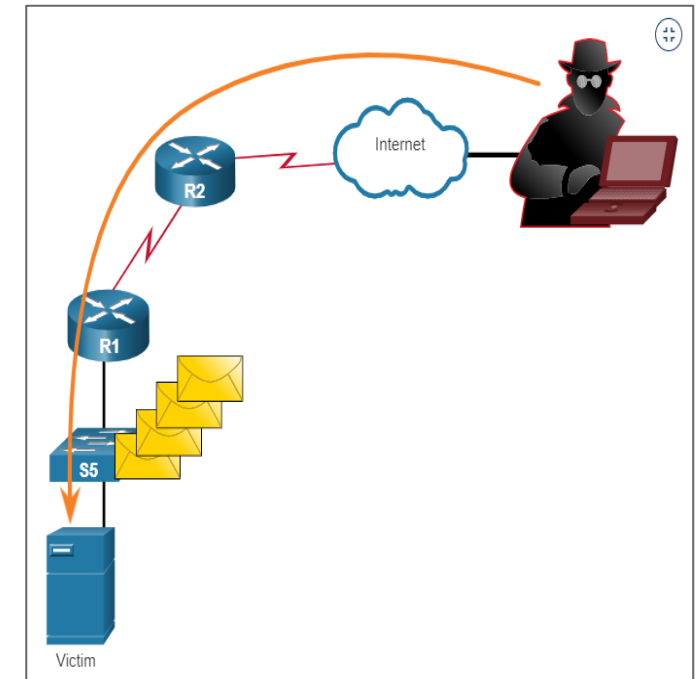
- The following terms are used to describe the components of a DDoS:

Component	Description
zombies	A group of compromised hosts. These hosts run malicious code.
bots	Bots are malware that is designed to infect a host and communicate with a handler system.
botnet	A group of zombies that have been infected using self-propagating malware and are controlled by handlers.
handlers	A master command-and-control (CnC or C2) server controlling groups of zombies.
botmaster	Enables unauthorized file transfer services on end devices.



Buffer Overflow Attack

- The threat actor uses the buffer overflow DoS attack to find a system memory-related flaw on a server and exploit it.
- For instance, a remote denial of service attack vulnerability was discovered in Microsoft Windows 10, where the threat actor created malicious code to access out-of-scope memory.
- Another example is ping of death, where a threat actor sends a ping of death, which is an echo request in an IP packet that is larger than the maximum packet size.
- The receiving host cannot handle a packet size and it would crash.



Thanks

