Module 13-17

CyberOps Associate

Brno – Week of March 23

Barthelemy.camia-temperton@esigelec.fr

Summary

Introduction

#whoami

Barthélemy CAMIA-TEMPERTON
French lecturer, specialized in Cybersecurity

Diploma

- ❑ Master's-level engineering degree in cybersecurity

Current role

- ❑ Lecturer in Information and Communication Technologies
- ❑ Head of the Cybersecurity program

ESIGELEC
ÉCOLE D'INGÉNIEURS-ES GÉNÉRALISTES

Previous work experiences

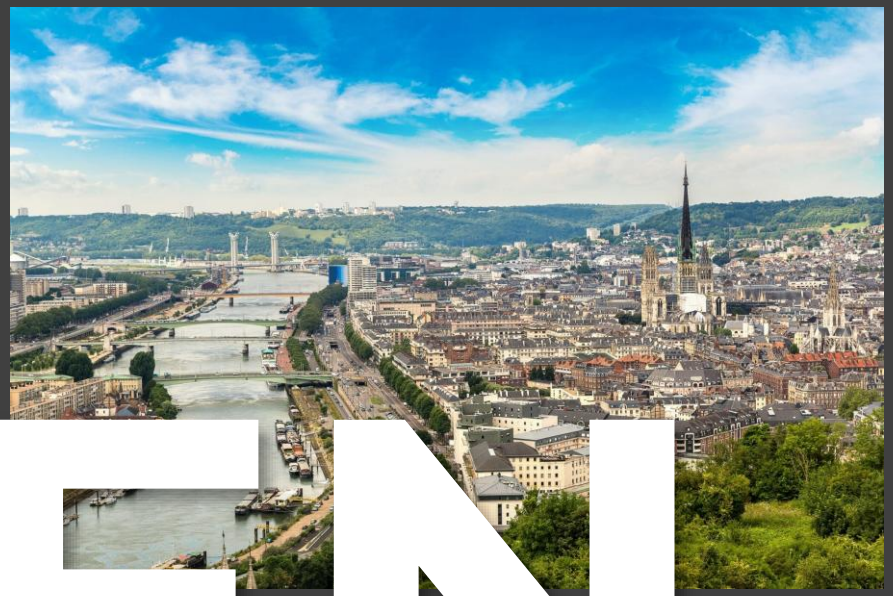
- ❑ Cybersecurity apprentice at Thales (Leading defense company)
- ❑ Cybersecurity consultant at Deloitte Luxembourg (Big Four)

THALES
Deloitte.

Certifications

- ❑ Certified Hacking Forensic Investigator (CHFI by EC-Council)
- ❑ Certified Ethical Hacker (CEH by EC-Council)
- ❑ Cloud Digital Leader (by Google)

EC-Council
EC-Council
Google



ROUEN

Rouen & Esigelec

ROUEN

- **650 000** inhabitants
- **50 000** students
- **1h15** from Paris
- **1h00** from the sea
- **200+** historic monuments
- **5M+** tourists per year

ESIGELEC

- **1 400** engineering students
- **94** partner universities
- **36** student associations
- **2** English-taugh programs (Master of Technology)
  - ❑ Software Engineering and Digital Transformation
  - ❑ Electronic Embedded Systems





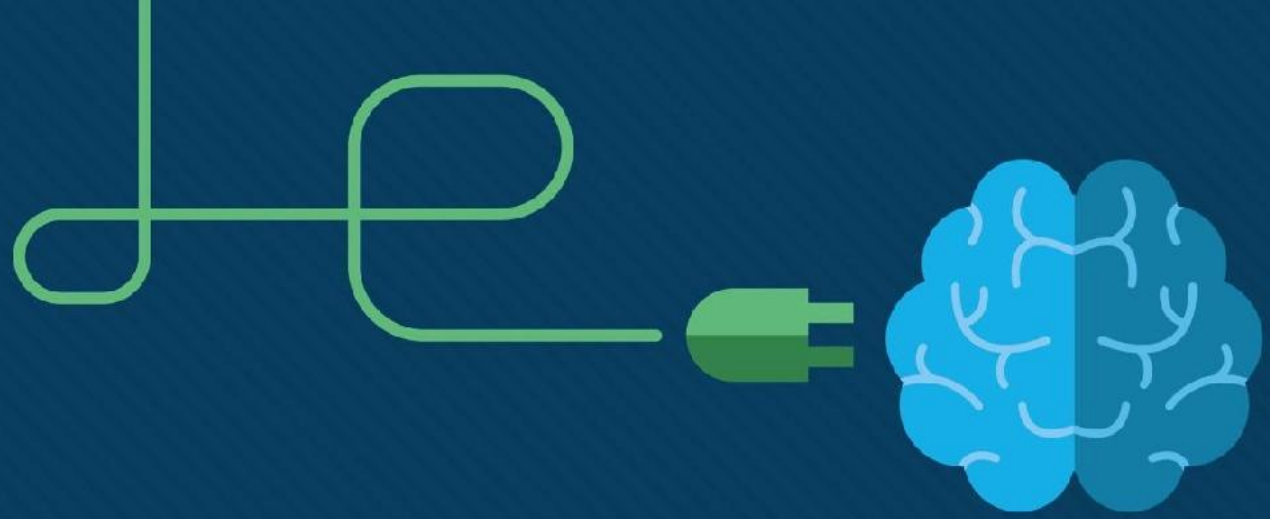
ESIGELEC

Module 13 Attackers and their tools

Module 13: Attackers and Their Tools

Instructor Materials

CyberOps Associate v1.0



Module 13:Attackers and Their Tools

CyberOps Associate v1.0

Module Objectives

- **Module Title:** Attackers and Their Tools
- **Module Objective:** Explain how networks are attacked.

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.

13.1 Who is Attacking Our Network?

Threat, Vulnerability, and Risk

- Attackers wants 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.

Threat, Vulnerability, and Risk (Contd.)

- **Common network security terms:**
  - Countermeasure – Actions taken to protect assets by mitigating a threat or reducing risk.
  - Impact - The potential damage to the organization that is caused by the threat
- **Note:** A local exploit requires inside network access such as a user with an account on the network. It does not require an account on the network to exploit that network's vulnerability.

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

- Hacking started in the 1960s with phone freaking, which refers to using various audio frequencies to manipulate phone systems.
- In the early 1960's, threat actors realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.
- In the mid-1980's, threat actors wrote 'war dialing' programs which dialed each telephone number in a given area in search of computers, bulletin board systems, and fax machines.
- When a phone number was found, password-cracking programs were used to gain access.

Evolution of Threat Actors (Contd.)

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.

Cybercriminals

- Cybercriminals are threat actors who are motivated to make money using any necessary means.
- At times, cybercriminals work independently or they are financed and sponsored by criminal organizations.
- They steal billions of dollars from consumers and businesses every year.
- They operate in underground economy and buy and sell personal information and intellectual property that they steal from victims.
- They target small businesses and consumers, as well as large enterprises and industries.

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.

Cyber Threat Indicators

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

Cyber Threat Indicators (Contd.)

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.

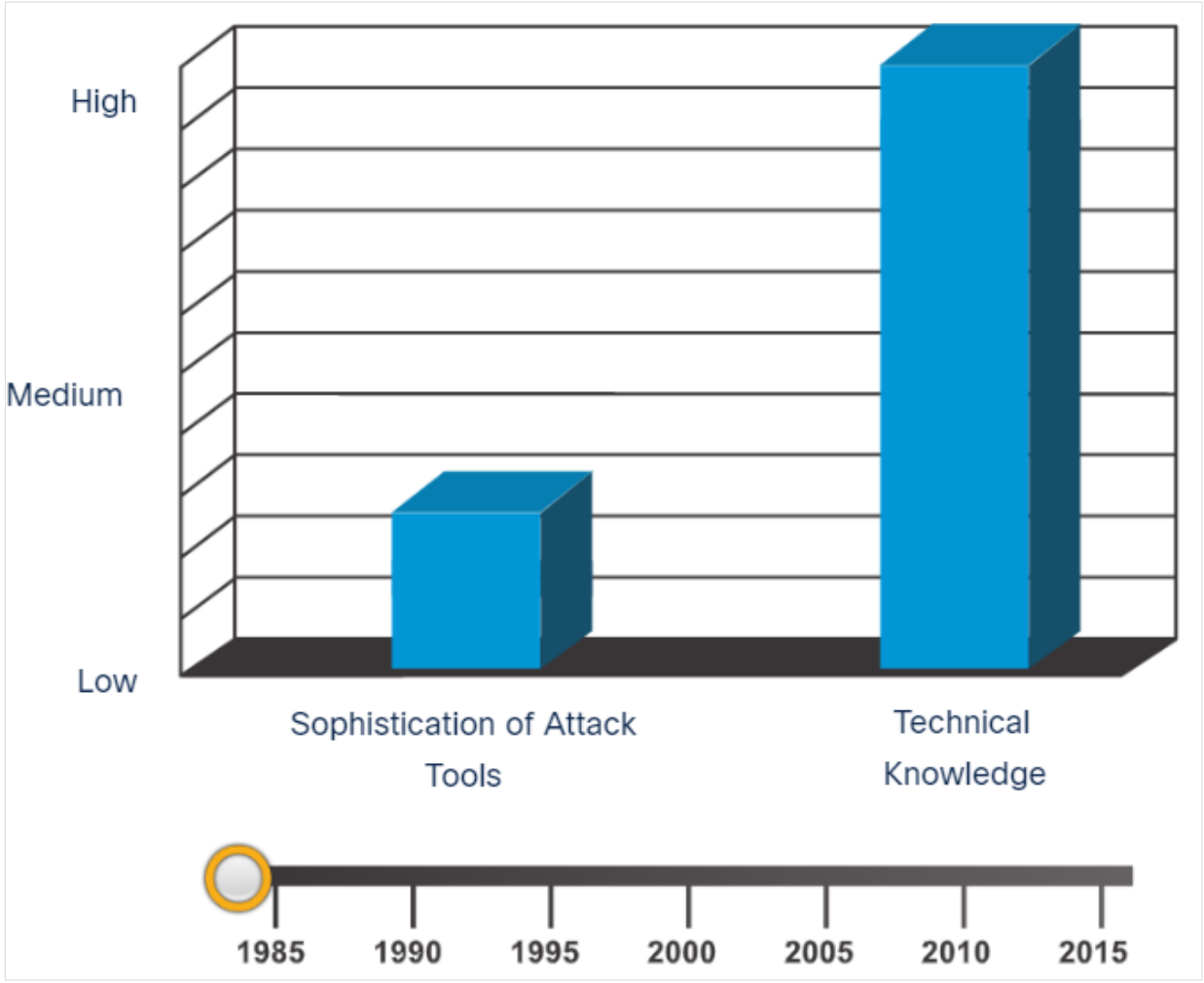
Threat Sharing and Building Cybersecurity Awareness (Contd.)

- The theme for the NCASM for 2019 was **Own IT. Secure IT. Protect IT.**
- Security topics provided through campaign:
  - Social media safety
  - Updating privacy settings
  - Awareness of device app security
  - Keeping software up-to-date
  - Safe online shopping
  - Wi-Fi safety
  - Protecting customer data

13.2 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.

Category 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.)

Category 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.

13.3 Attackers and Their Tools Summary

What Did I Learn in this Module?

- To understand network security, it is important to understand the terms such as threat, vulnerability, attack surface, exploit, and risk.
- Risk management is the process of providing protective measures by protecting the asset.
- Four common ways to manage risk are risk acceptance, risk avoidance, risk reduction, and risk transfer.
- Hacker is a term used to describe a threat actor. White hat hackers are ethical hackers that use their skills for good, ethical, and legal purposes.
- Grey hat hackers are individuals who commit crimes and do unethical things, but not for personal gain.
- Black hat hackers are criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

What Did I Learn in this Module? (Contd.)

- Many network attacks can be prevented by sharing information about Indicators of Compromise (IOC). CISA and NCSA are examples of cybersecurity promoting organizations.
- Attack tools have become more sophisticated, and highly automated.
- Many of the tools are Linux or UNIX based and knowledge of these are useful to a cybersecurity professional.
- Tools include password crackers, wireless hacking tools, network security scanning and hacking tools, packet crafting tools, packet crafting tools, packet sniffers, rootkit detectors, fuzzers to search vulnerabilities, forensic tools, debuggers, hacking operating systems, encryption tools, vulnerability exploitation tools, and vulnerability scanners.
- Categories of attacks include eavesdropping attacks, data modification attacks, IP address spoofing attacks, password-based attacks, denial-of-service attacks, man-in the-middle attacks, compromised key attacks, and sniffer attacks.


CISCO

Module 14 Common threats and attacks

Module 14: Common Threats and Attacks

Instructor Materials

CyberOps Associate v1.0

Module 14: Common Threats and Attacks

CyberOps Associate v1.0

Module Objectives

Module Title: Common Threats and Attacks

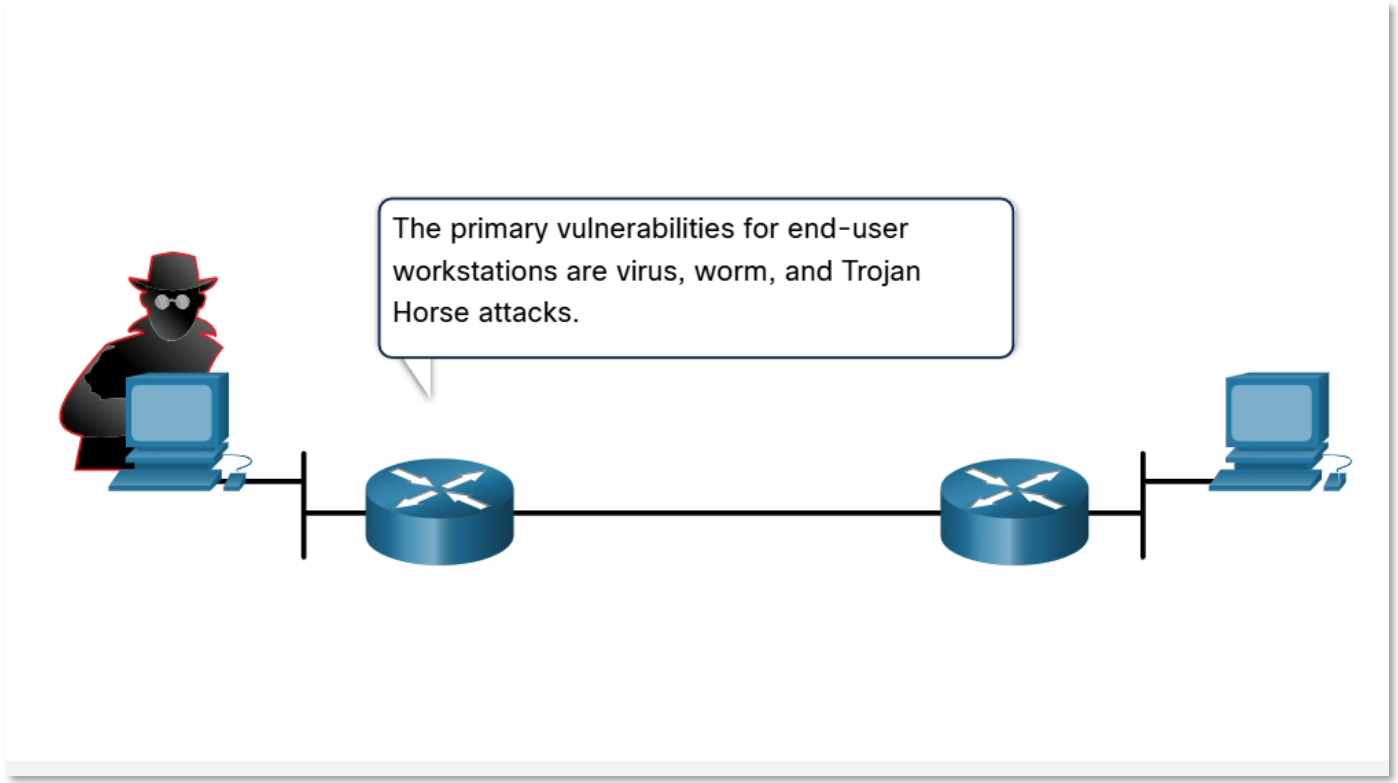
Module Objective: Explain the various types of threats and attacks.

Topic Title	Topic Objective
Malware	Describe types of malware.
Common Network Attacks - Reconnaissance, Access, and Social Engineering	Explain reconnaissance, access, and social engineering network attacks.
Network Attacks - Denial of Service, Buffer Overflows, and Evasion	Explain Denial of Service, buffer overflow, and evasion attacks.

14.1 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.



Viruses

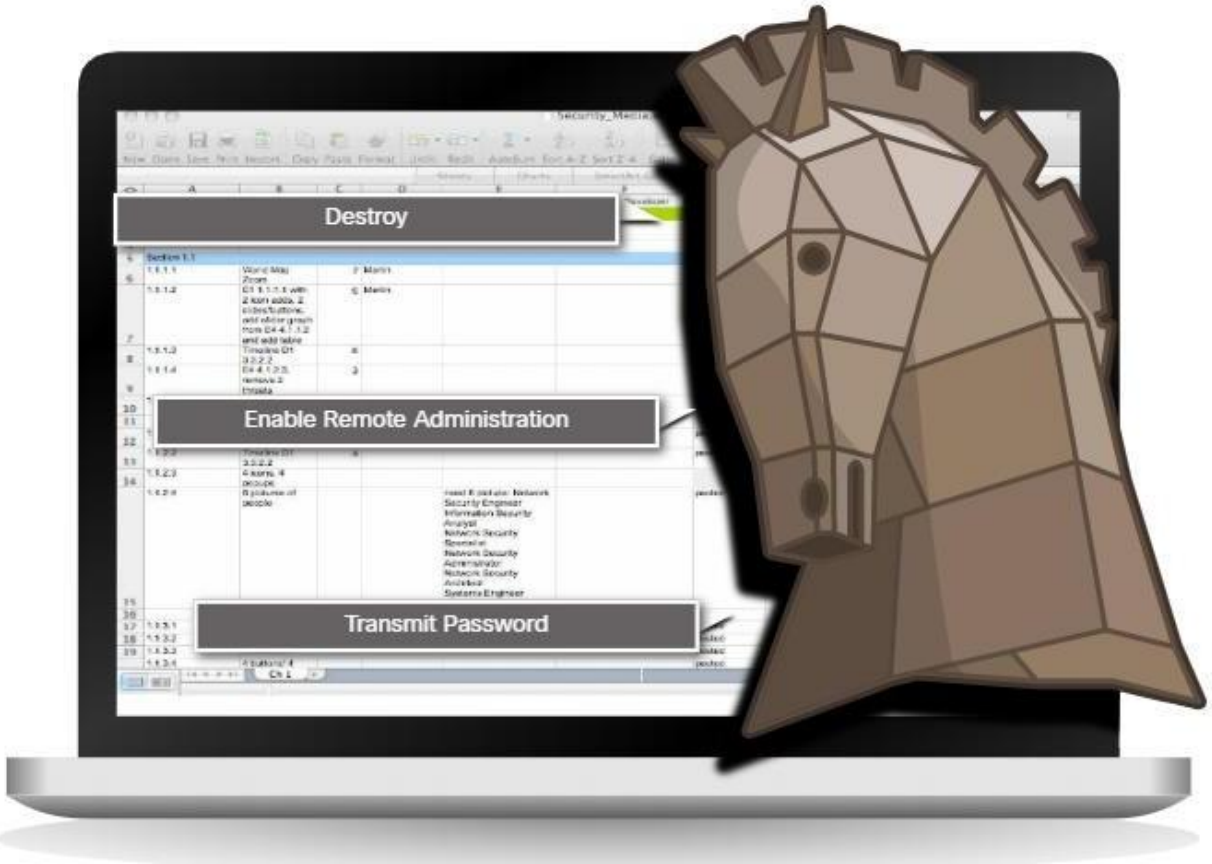
- A virus is a type of malware that spreads by inserting a copy of itself into another program.
- After the program is run, viruses spread from one computer to another, thus infecting the computers.
- A simple virus may install itself at the first line of code in an executable file.
- Viruses can be 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 manner in which 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.

Worms

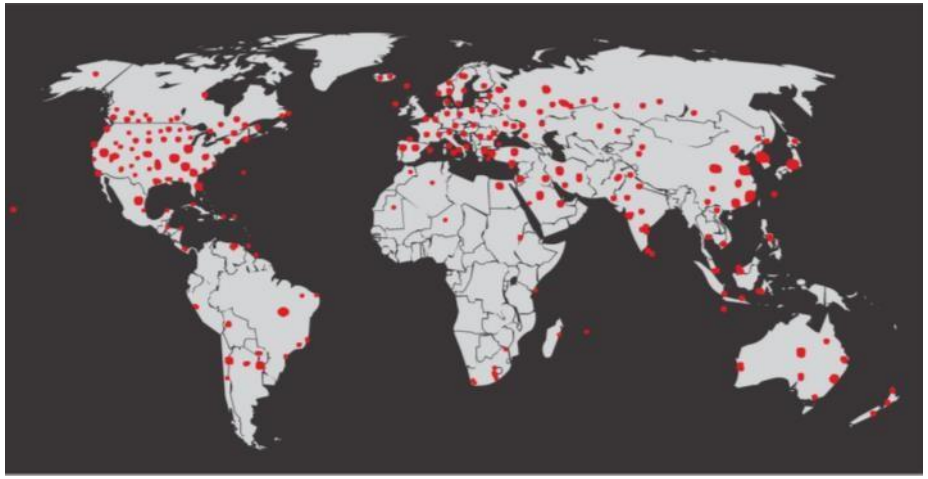
- Computer worms are similar to viruses because they replicate themselves by independently exploiting vulnerabilities in networks.
- Worms can slow down networks as they spread from system to system.
- Worms can run without a host program.
- However, once the host is infected, the worm spreads rapidly 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

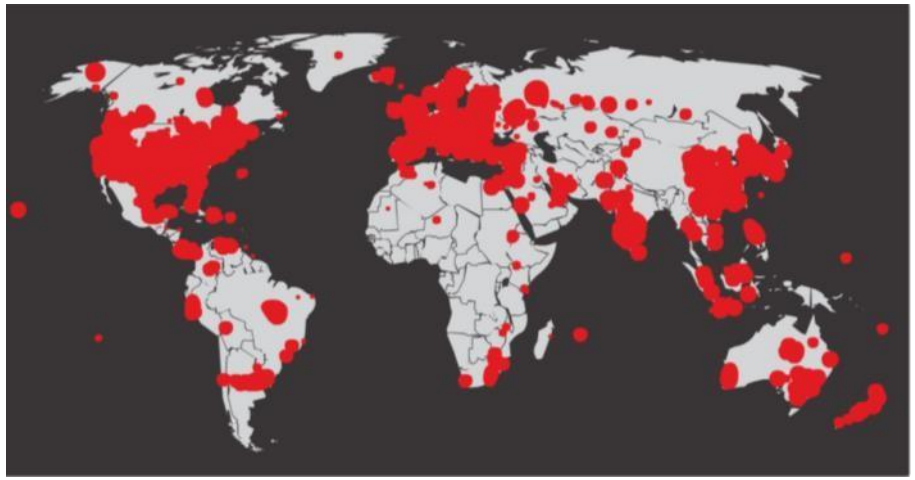
Code Red Infection 19 hours later

Worms (Contd.)

- 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.



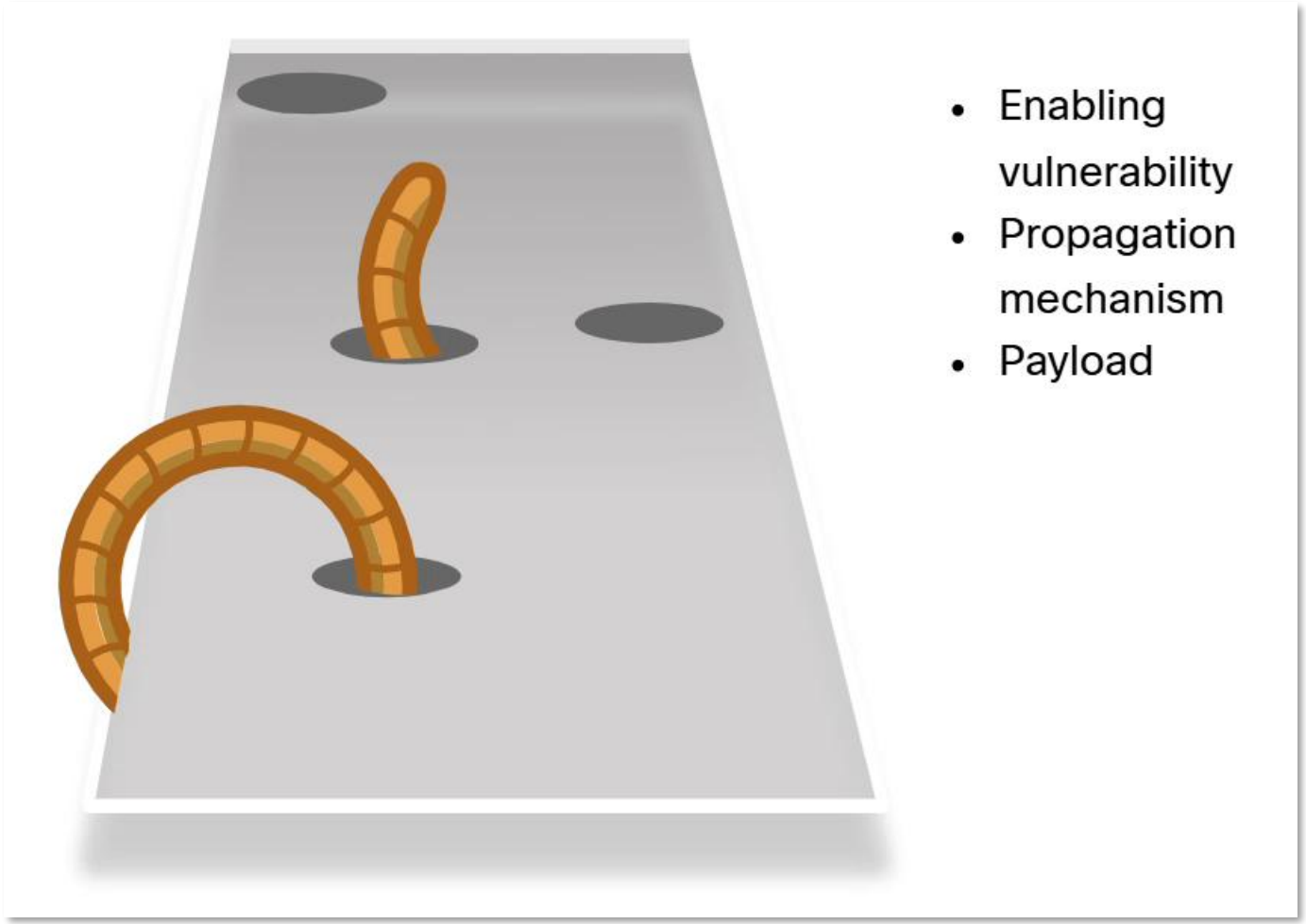
Initial SQL Slammer Infection



SQL Slammer Infection 30 minutes later

Worm Components

Click Play in the figure to view the three components of worm attacks.



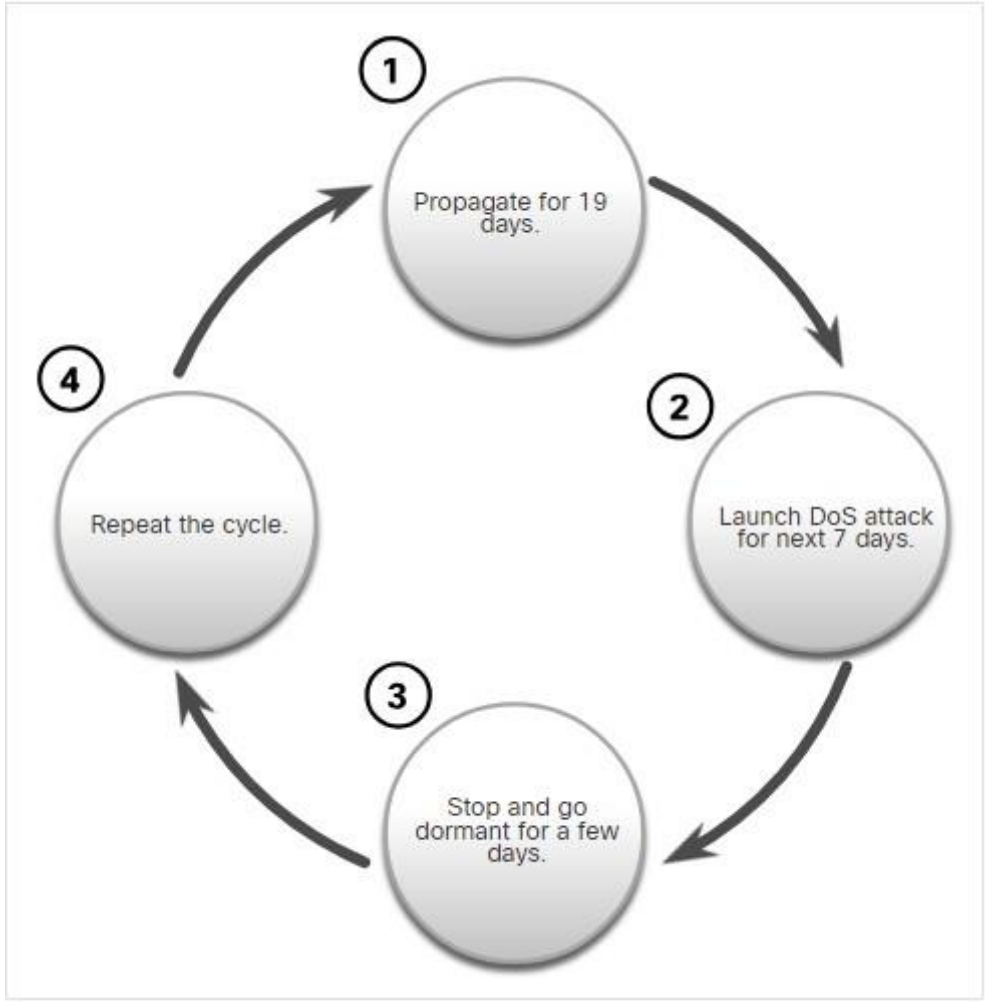
Worm Components (Contd.)

The three worm components are as follows:

- **Enabling vulnerability -** A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
- **Propagation mechanism -** After gaining access to a device, the worm replicates itself and locates new targets.
- **Payload -** Any malicious code that results in some action is a payload. Most often this is used to create a backdoor that allows a threat actor to access the infected host or to create a DoS attack.

Worm Components (Contd.)

- Worms are self-contained programs that attack a system to exploit a known vulnerability.
- Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again.
- This propagation mechanism is commonly deployed in a way that is difficult to detect.
- **Note**: Worms never stop spreading on the internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.



Code Red Worm Propagation

Ransomware

- 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.

Other Malware

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.

Lab – Anatomy of Malware

In this lab, you will research and analyze some recent malware.

14.2 Common Network Attacks - Reconnaissance, Access, and Social Engineering

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.

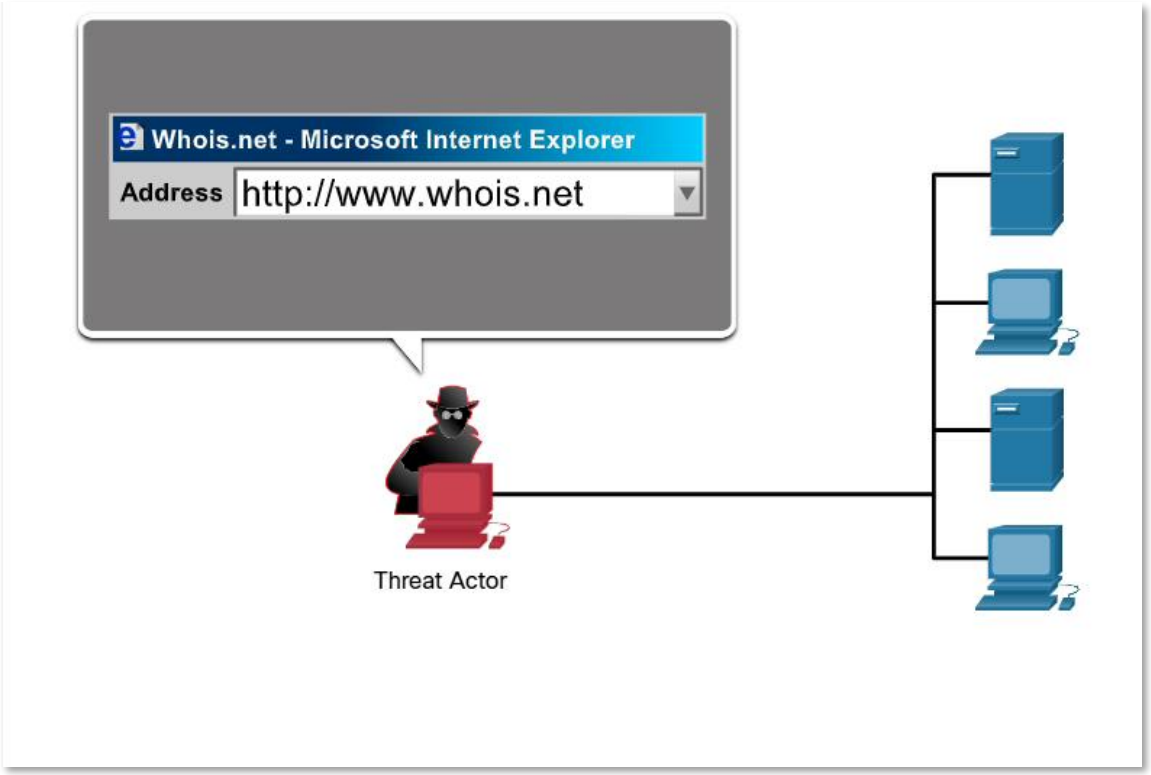
Reconnaissance Attacks (Contd.)

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

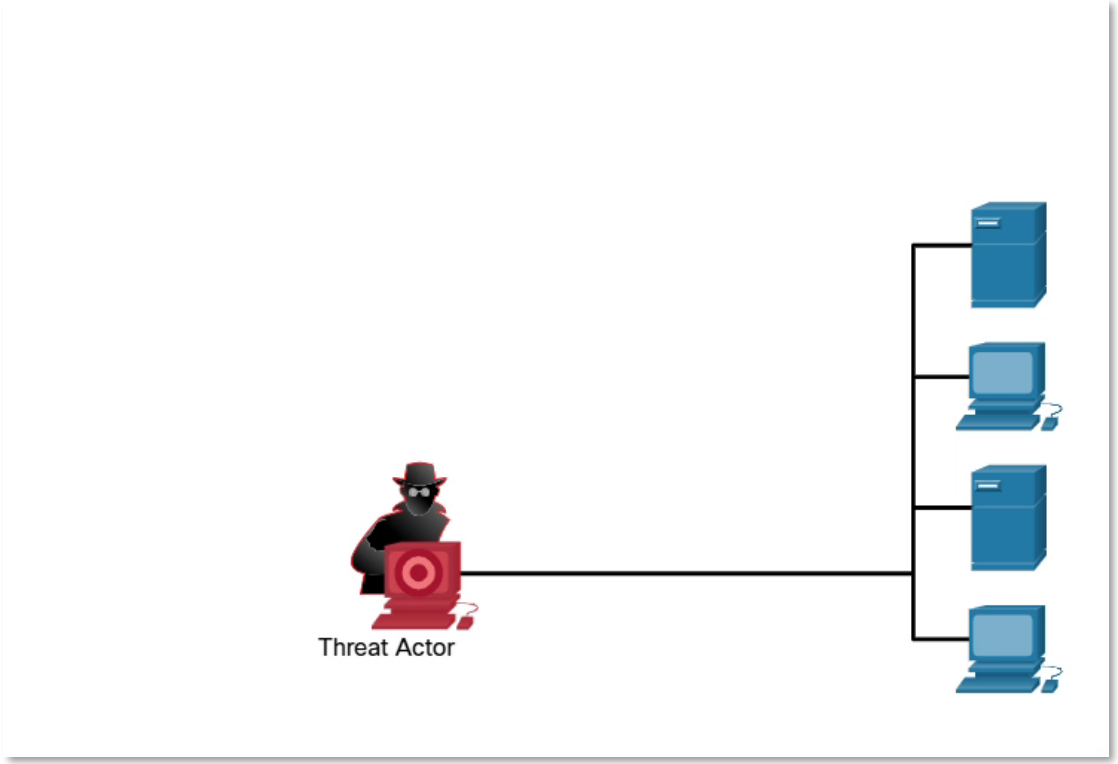
Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.
Initiate a ping sweep of the target network	The information query usually 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 NetScanTools.
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.

Reconnaissance Attacks (Contd.)

Internet Information Queries: Click Play in the figure to view an animation of a threat actor using the who is command to find information about a target.

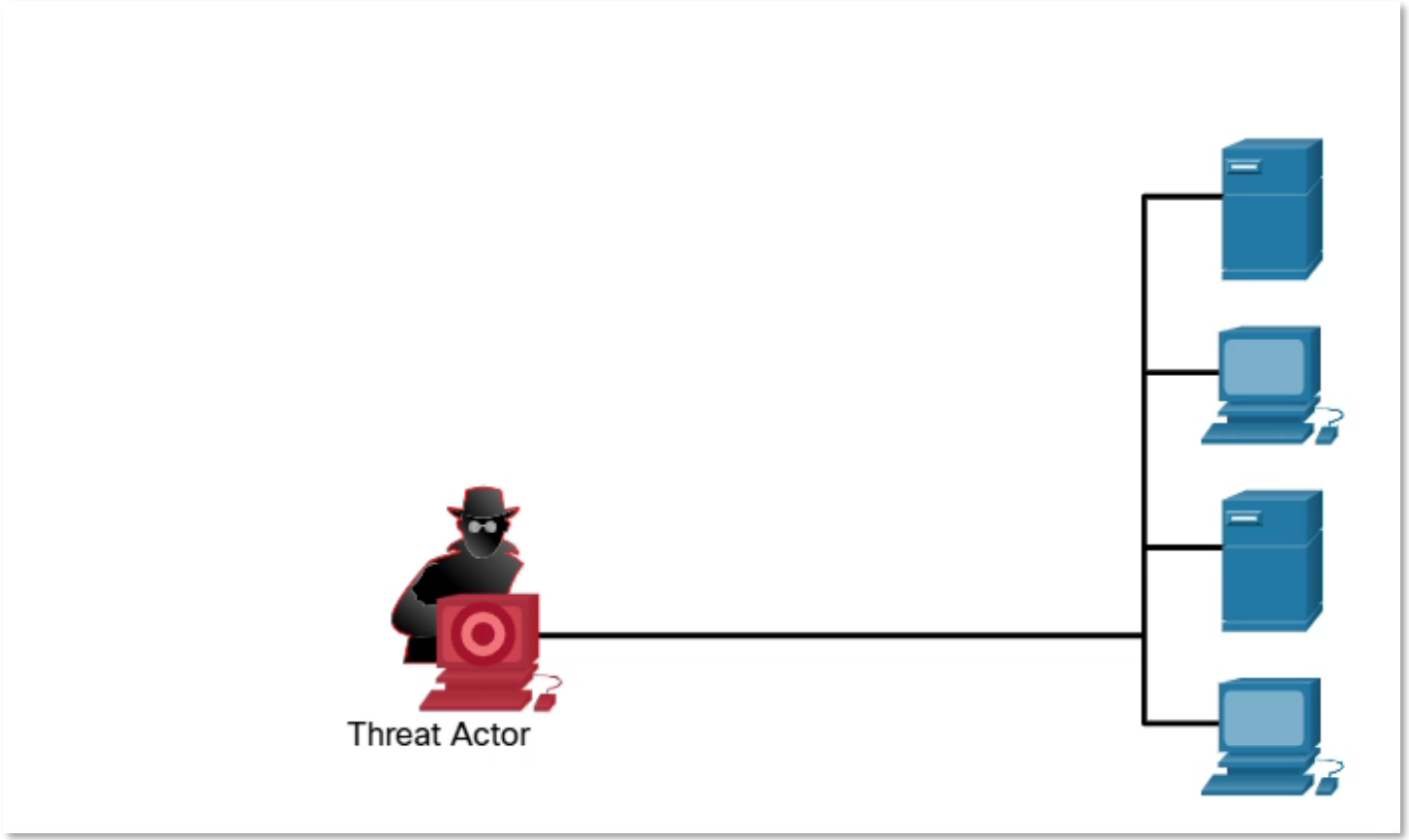


Performing Ping Sweep: Click Play in the figure to view an animation of a threat actor doing a ping sweep of the target's network address to discover live and active IP addresses.



Reconnaissance Attacks (Contd.)

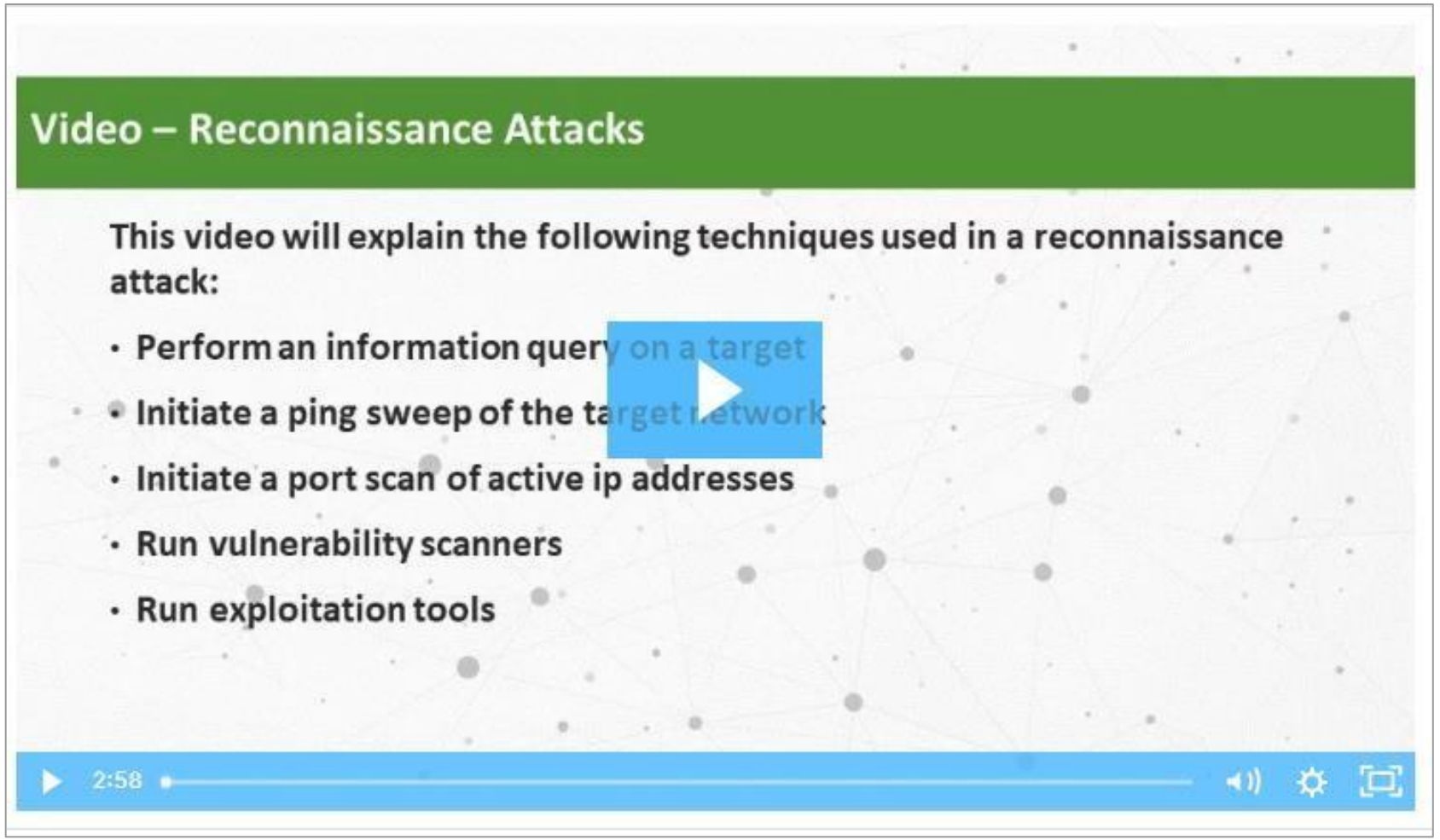
Performing Port Scan: Click Play in the figure to view an animation of a threat actor performing a port scan on the discovered active IP addresses using Nmap.



Video - Reconnaissance Attacks

Watch the video to learn about the different techniques in a reconnaissance attack.

Link to video



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

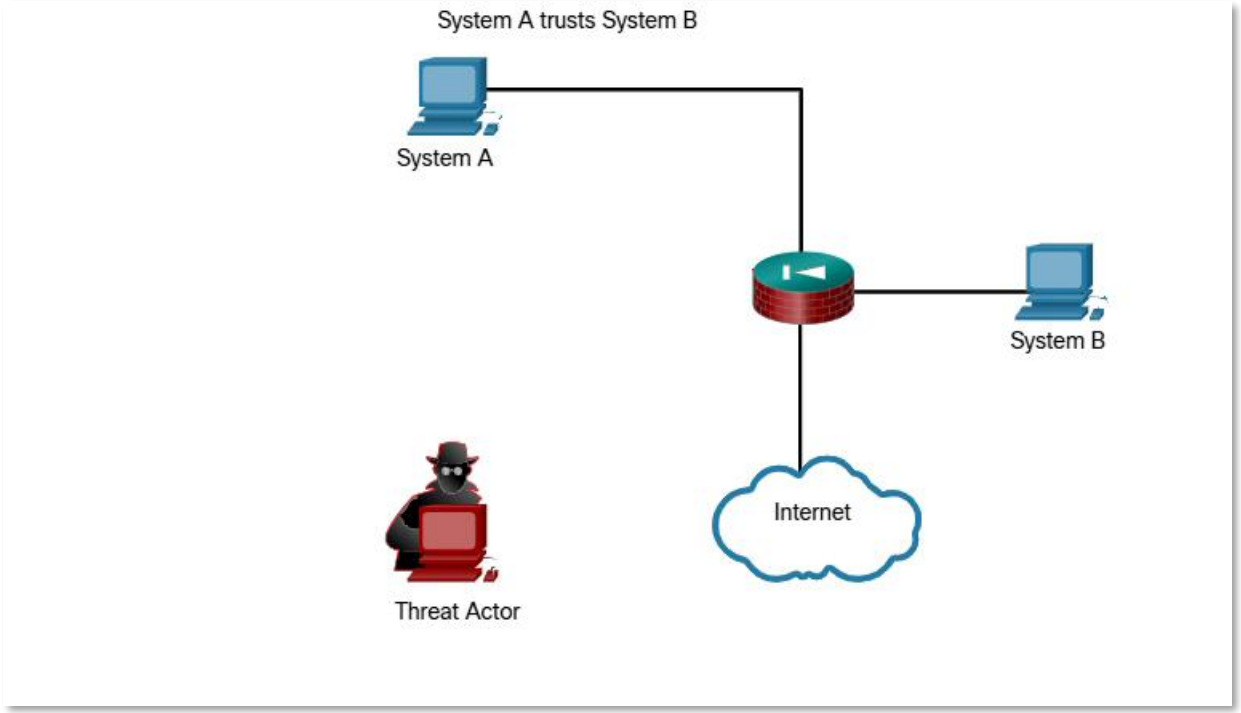
- The threat actor attempts to discover critical system passwords using a variety of password cracking tools.

Spoofing Attacks

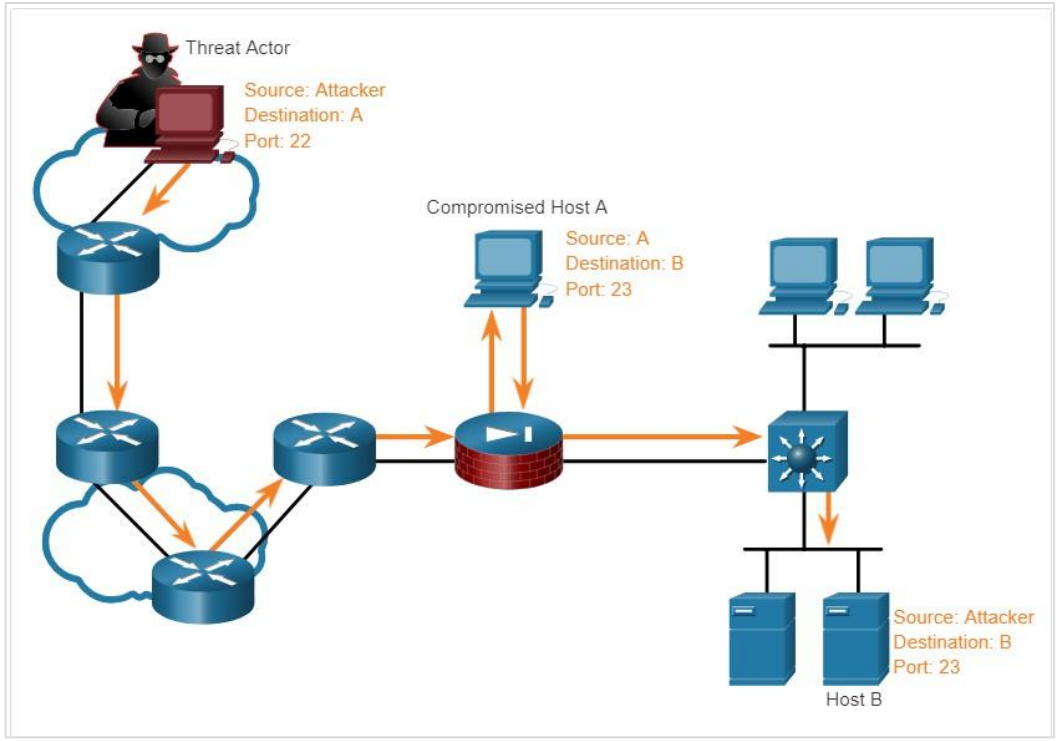
- The threat actor device attempts to pose as another device by falsifying data.
- Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.
    - Trust exploitations
    - Port redirections
    - Man-in-the-middle attacks
    - Buffer overflow attacks

Access Attacks (Contd.)

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

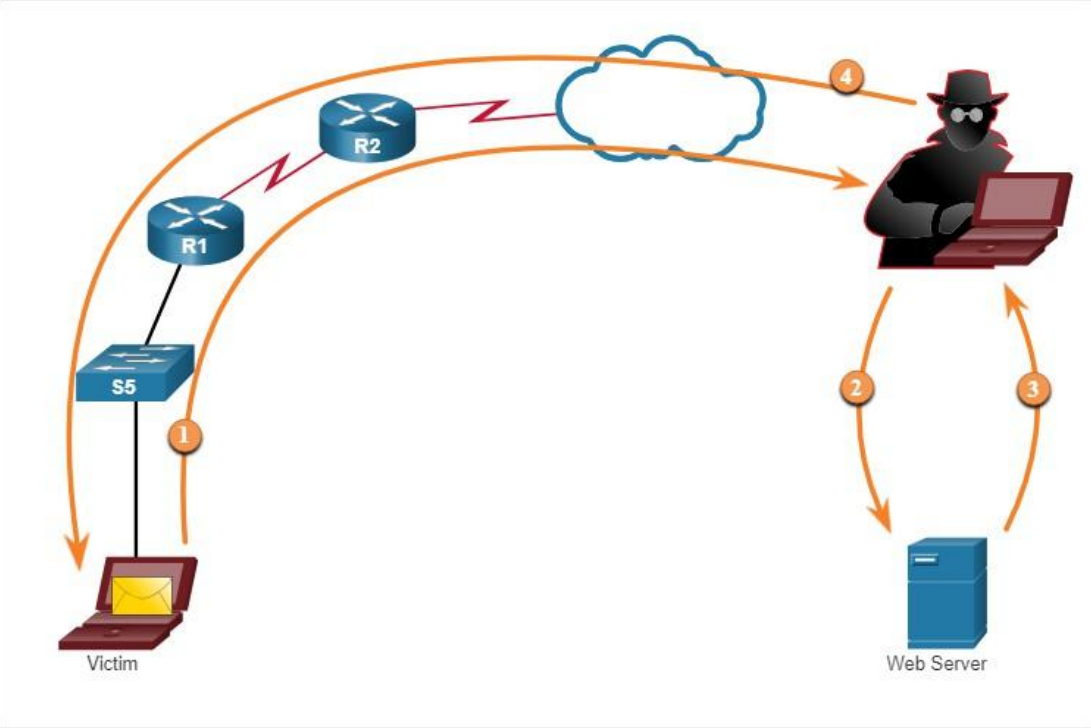


Port Redirection Example: The example shows a threat actor using SSH (port 22) to connect to a compromised Host A trusted by Host B. Hence, the threat actor can use Telnet (port 23) to access it.

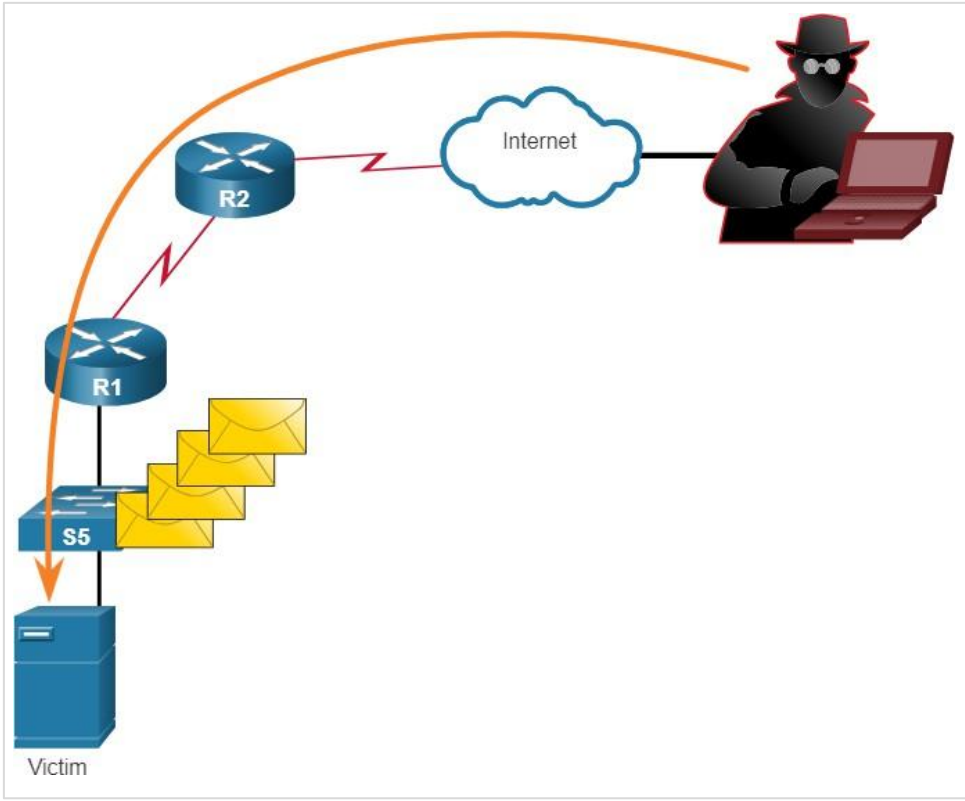


Access Attacks (Contd.)

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.



Video - Access and Social Engineering Attacks

Watch the video to see the demonstration of the types of access and social engineering attacks.

Link to video

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’.

Lab – Social Engineering

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

14.3 Network Attacks – Denial of Service, Buffer Overflows, and Evasion

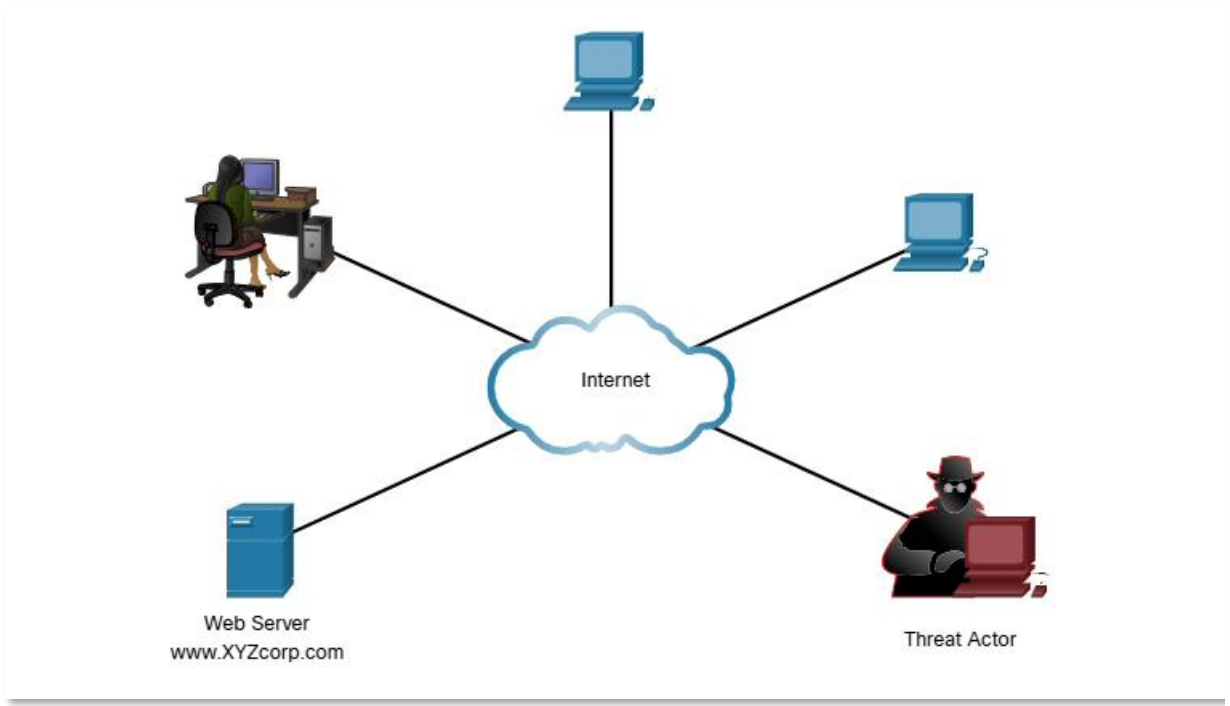
Video – Denial of Service Attacks

Watch the video to learn about Denial of Service attacks.

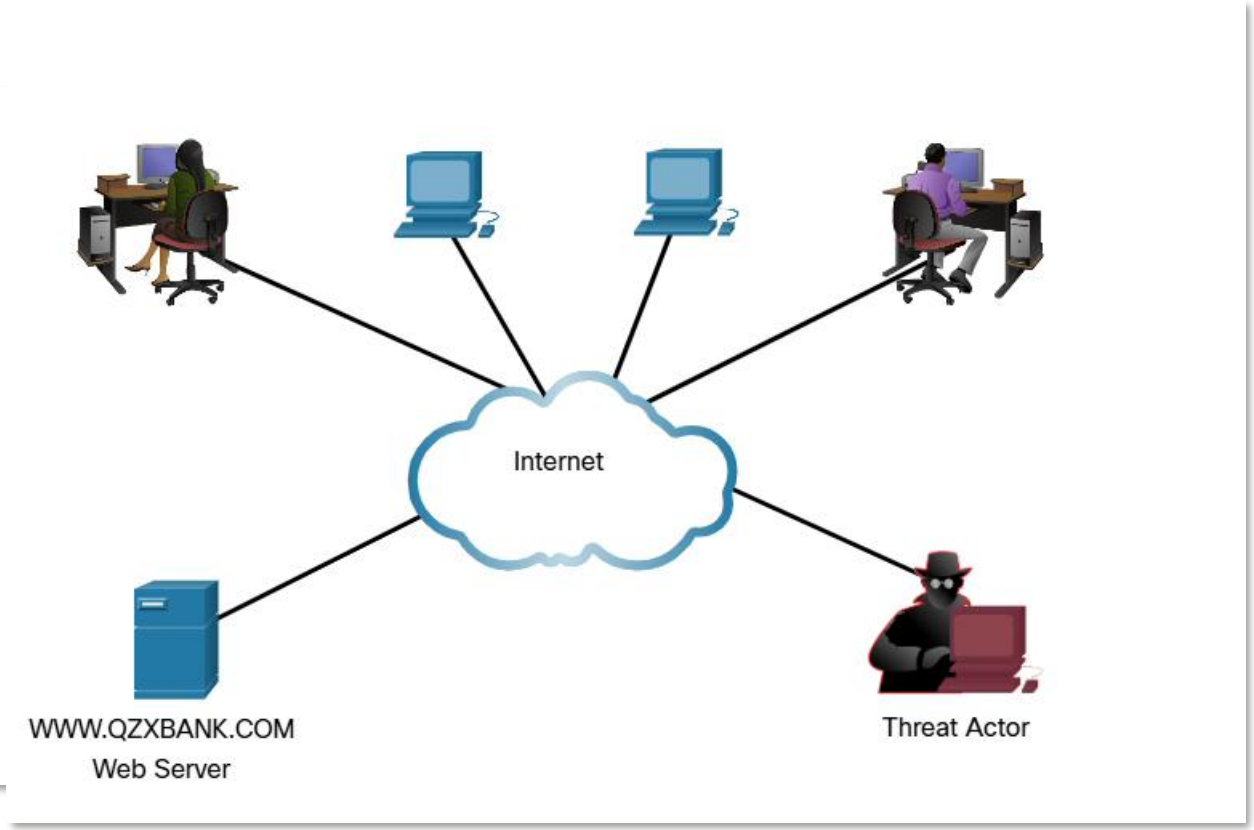
Link to video

DoS and DDoS Attacks (Contd.)

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.



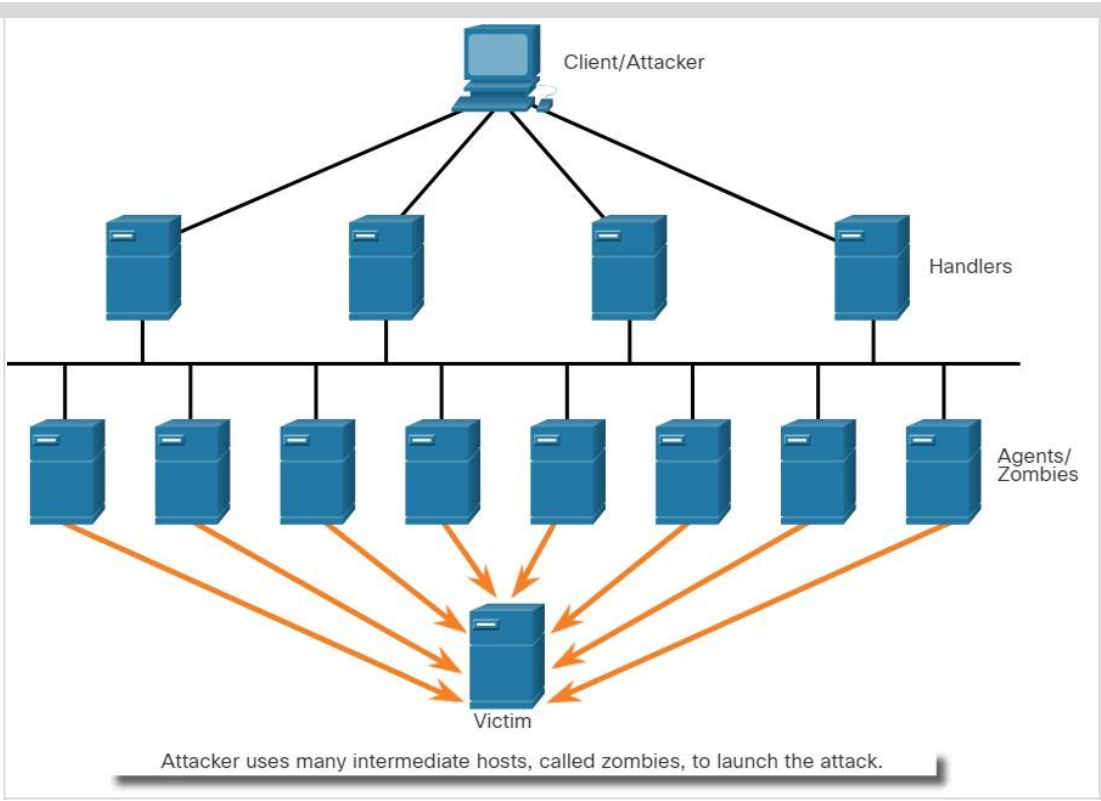
DoS and DDoS Attacks

- 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.



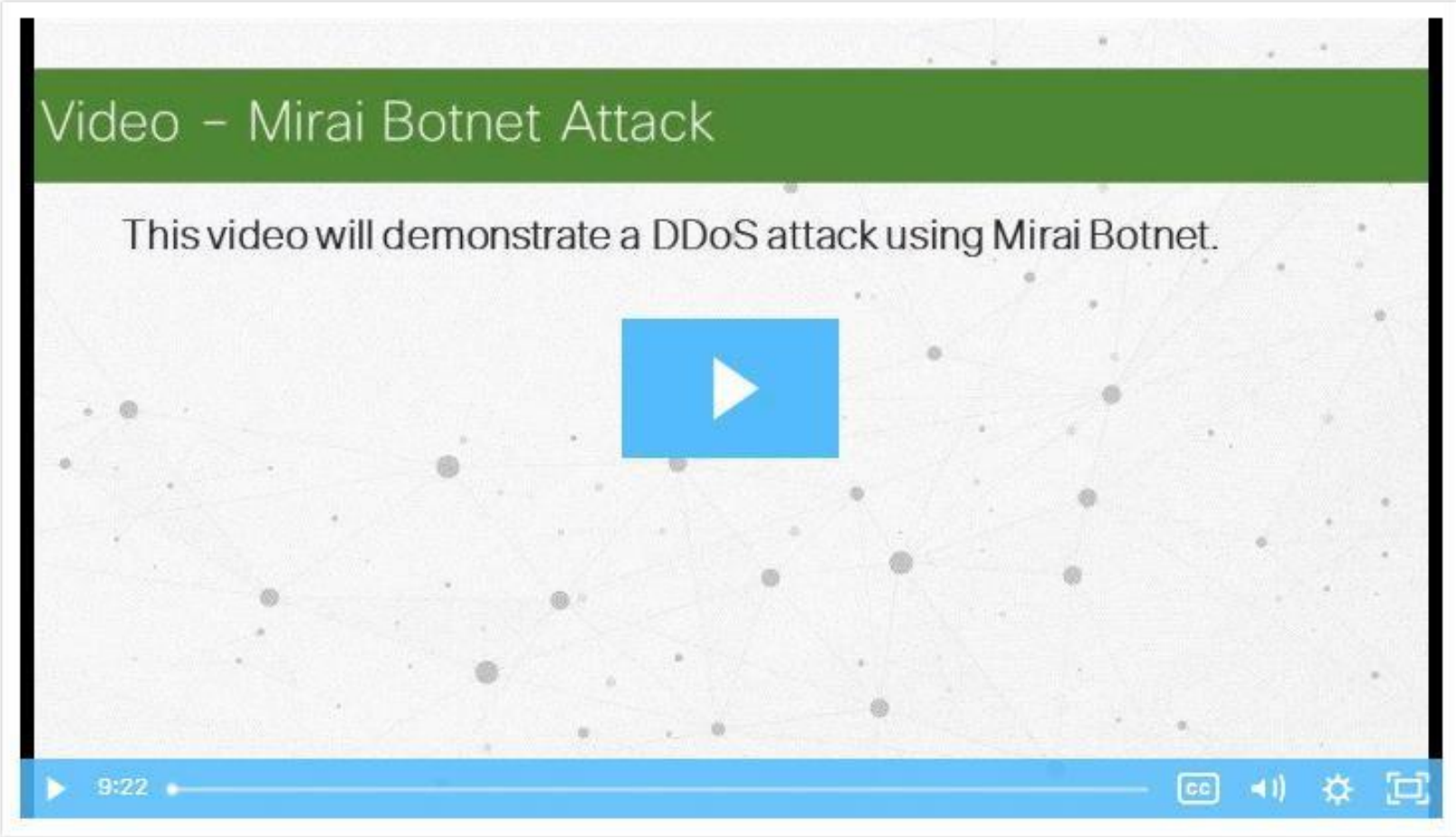
Video Demonstration – Mirai Botnet

- Mirai is a malware that targeted IoT devices configured with default login information.
- The botnet was used as part of a Distributed Denial of Service (DDoS) attack.

Video Demonstration – Mirai Botnet (Contd.)

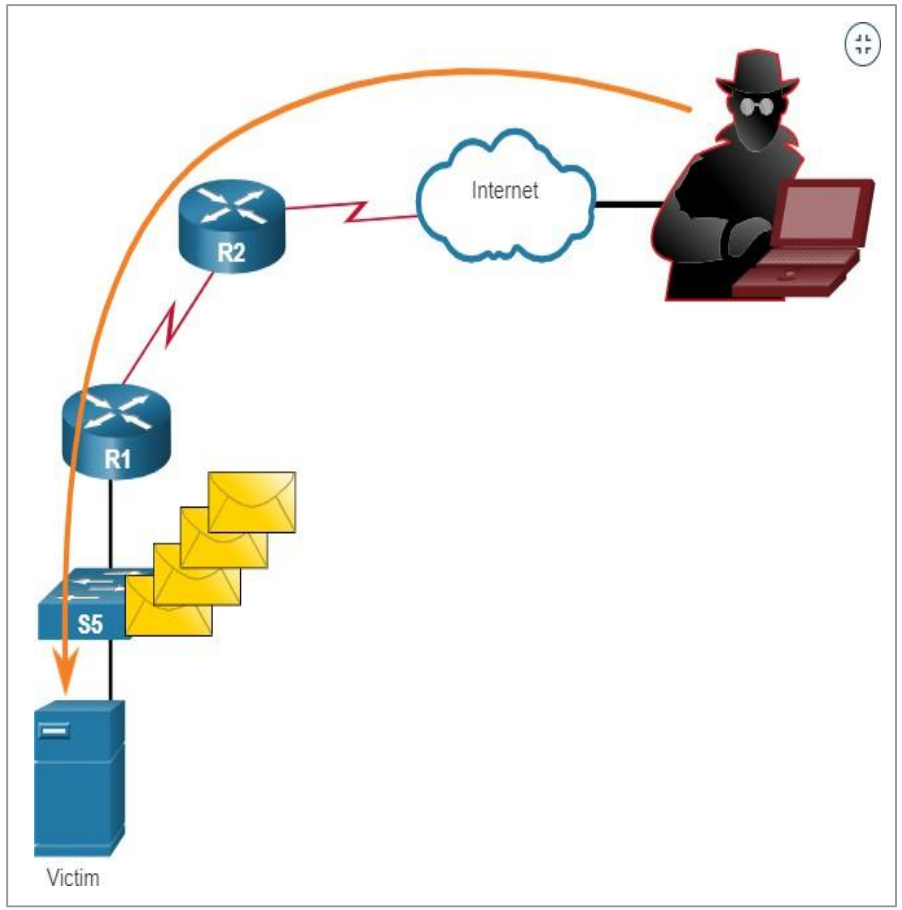
Play the video to view a demonstration of how a botnet-based DDoS attack makes services unavailable.

Link to video



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.
- **Note:** It is estimated that one third of malicious attacks are the result of buffer overflows.



Evasion Methods

The evasion methods used by threat actors include:

Evasion Method	Description
Encryption and tunneling	This evasion technique uses tunneling to hide, or encryption to scramble, malware files. This makes it difficult for many security detection techniques to detect and identify the malware. Tunneling can mean hiding stolen data inside of legitimate packets.
Resource exhaustion	This evasion technique makes the target host too busy to properly use security detection techniques.
Traffic fragmentation	This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network.

Evasion Methods (Contd.)

Evasion Method	Description
Protocol-level misinterpretation	This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check.
Traffic substitution	In this evasion technique, the threat actor attempts to trick an IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data.
Traffic insertion	Similar to traffic substitution, but the threat actor inserts extra bytes of data in a malicious sequence of data. The IPS rules miss the malicious data, accepting the full sequence of data.

Evasion Methods (Contd.)

Evasion Method	Description
Pivoting	This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to login to another host using the same credentials.
Rootkits	A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system.
Proxies	Network traffic can be redirected through intermediate systems in order to hide the ultimate destination for stolen data. In this way, known command-and-control not be blocked by an enterprise because the proxy destination appears benign. Additionally, if data is being stolen, the destination for the stolen data can be distributed among many proxies, thus not drawing attention to the fact that a single unknown destination is serving as the destination for large amounts of network traffic.

14.4 Common Threats and Attacks Summary

What Did I Learn in this Module?

- Malware is short for malicious software or malicious code.
- Most viruses are spread through USB memory drives, CDs, DVDs, network shares, and email.
- Trojans are found in online games.
- Three common types of malware are virus, worm, and Trojan horse.
- Threat actors can also attack the network from outside.
- The three major categories are reconnaissance, access, and DoS attacks.
- Recon attacks precede access or DoS attacks.
- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services.
- DoS attacks create some sort of interruption of network services to users, devices, or applications.

What Did I Learn in this Module? (Contd.)

- DDoS attacks are similar in intent to DoS attacks, except that the DDoS attack increases in magnitude because it originates from multiple, coordinated sources.
- Mirai is a malware that targets IoT devices configured with default login information.
- The goal of a threat actor when using a buffer overflow DoS attack is to find a system memory-related flaw on a server and exploit it.


CISCO

Module 15 Network monitoring and tools

Module 15: Network Monitoring and Tools

Instructor Materials

CyberOps Associate v1.0

Module 15: Network Monitoring and Tools

CyberOps Associate v1.0

Module Objectives

Module Title: Network Monitoring and Tools

Module Objective: Explain network traffic monitoring.

Topic Title	Topic Objective
Introduction to Network Monitoring	Explain the importance of network monitoring.
Introduction to Network Monitoring Tools	Explain how network monitoring is conducted.

15.1 Introduction to Network Monitoring

Network Security Topology

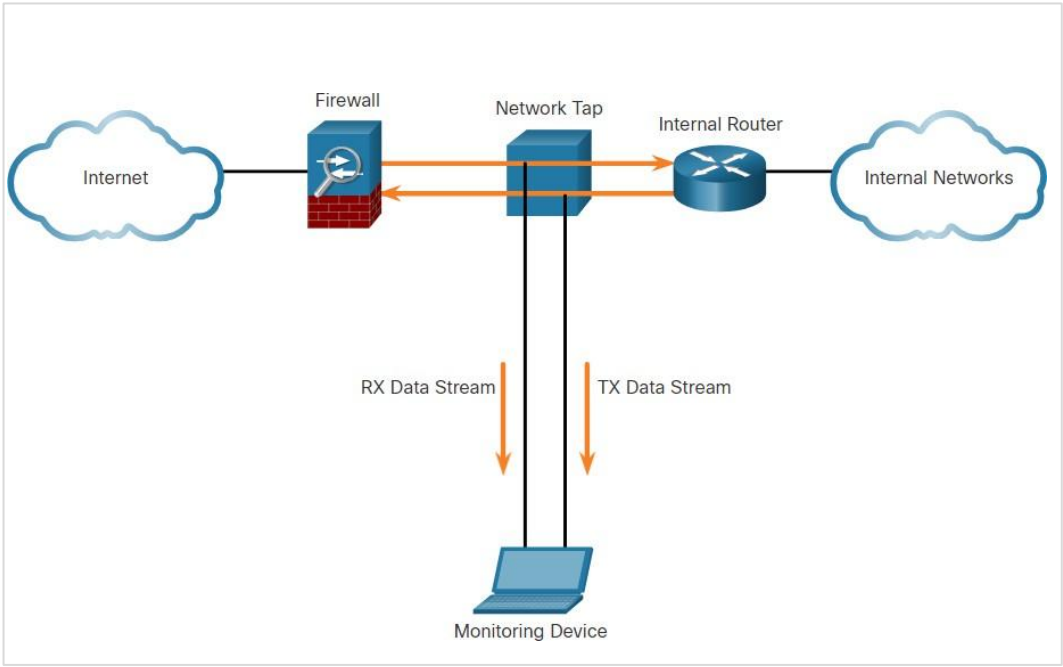
- To mitigate threats, all networks must be secured and protected.
- Network requires a security infrastructure consisting of firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and endpoint security software to protect.
- These methods and technologies are used to introduce automated monitoring, creating security alerts, or automatically blocking offensive devices.
- For large networks, an extra layer of protection is added.
- Devices such as firewalls and IPS operate based on pre-configured rules and monitor traffic and compare it against the configured rules. If there is a match, the traffic is handled according to the rule.
- An important part of the cybersecurity analyst is to review all alerts generated by network devices and determine the validity of the alerts.

Network Monitoring Methods

- The day-to-day operations of a network consists of traffic flow, bandwidth usage, and resource access. These patterns identify normal network behavior.
- To determine normal network behavior, network monitoring must be implemented.
- The tools such as IDS, packet analyzers, SNMP, NetFlow, and others are used for network monitoring .
- There are two common methods used to capture traffic and send it to network monitoring devices:
  - Network taps, sometimes known as Test Access Points (TAPs)
  - Traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

Network Taps

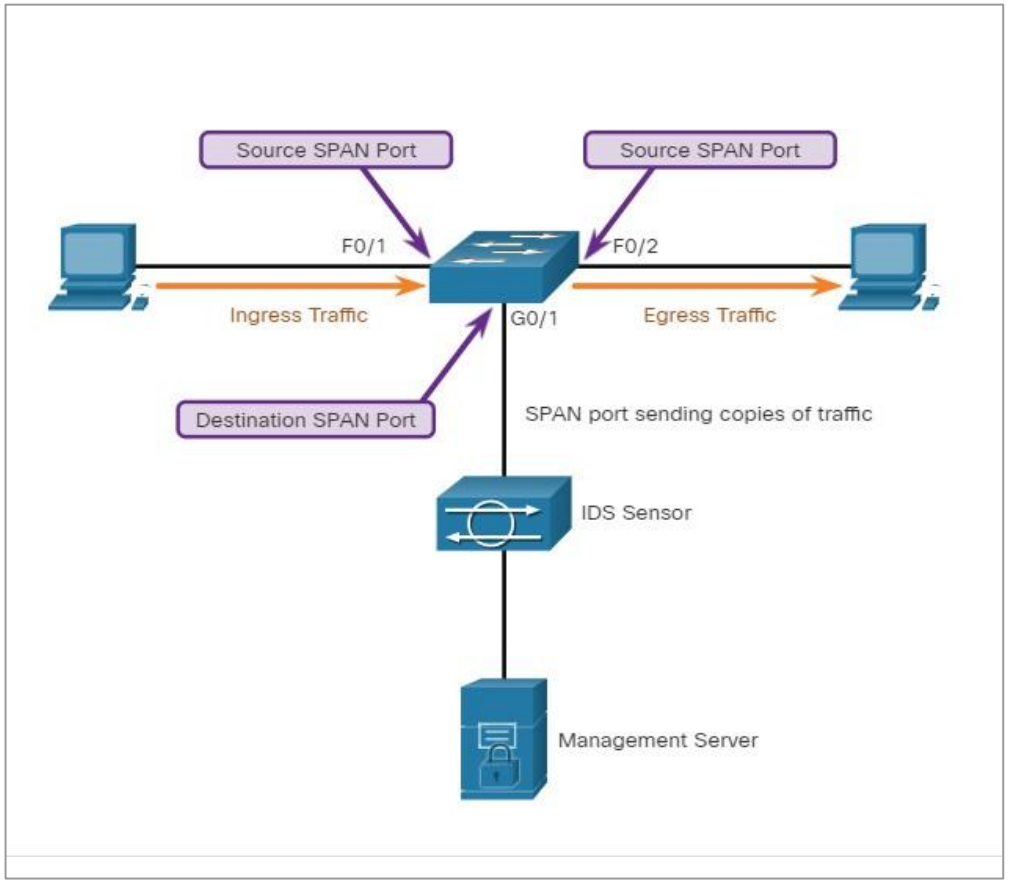
- A network tap is a passive splitting device implemented inline between a device of interest and the network.
- Hardware device placed between two network devices
- Copies all traffic passing through the link
- Very reliable (no packet loss)
- No configuration required
- Often used for security monitoring



Implementing a TAP in a Sample Network

Traffic Mirroring and SPAN

- Feature on a switch (software-based)
- Mirrors traffic from a port or VLAN to another port
- Requires configuration on the switch
- May drop packets if the switch is overloaded
- Often used for troubleshooting and temporary monitoring

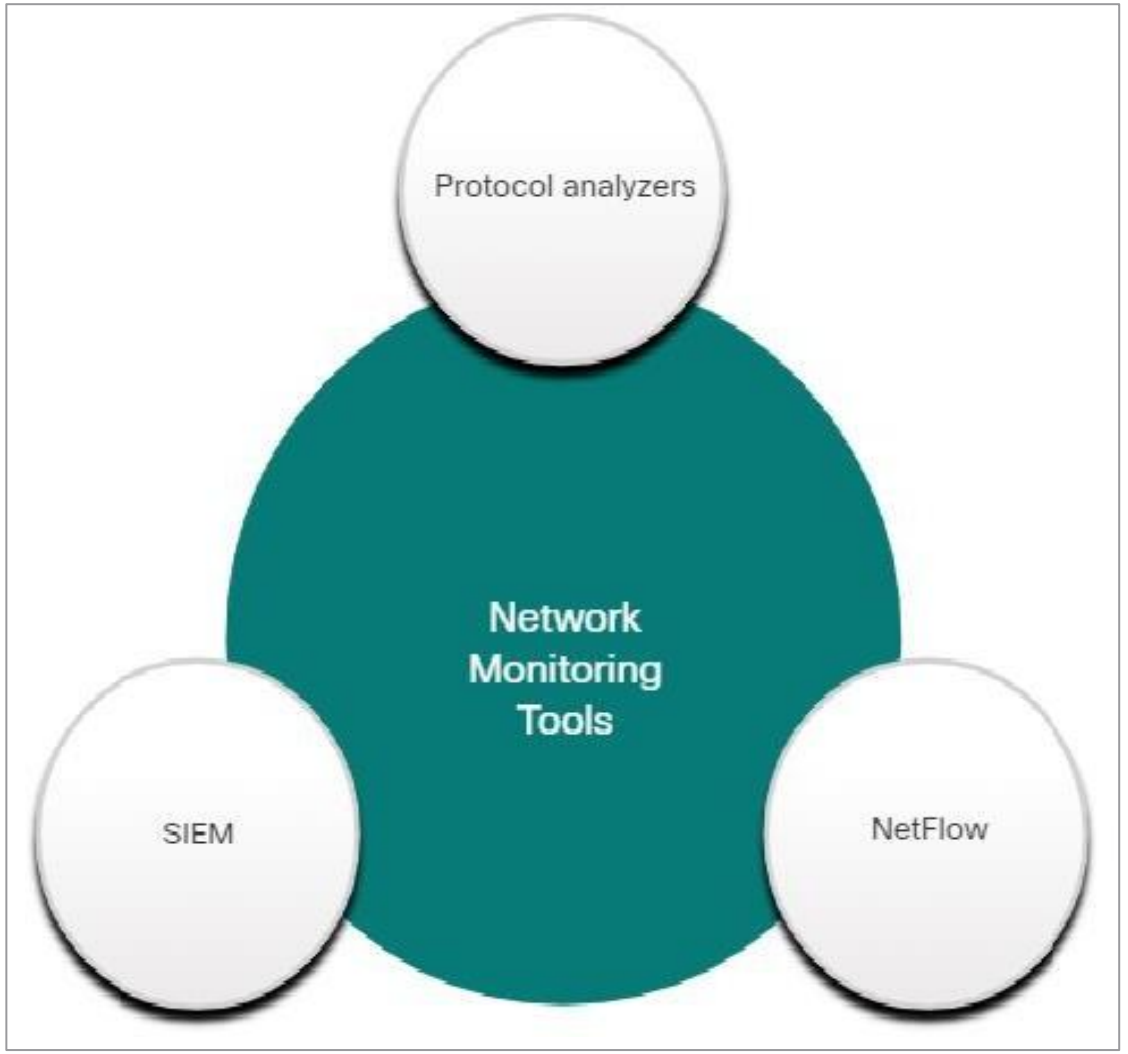


Switch interconnecting two hosts and mirroring traffic to an IDS and Network Management Server

15.2 Introduction to Network Monitoring Tools

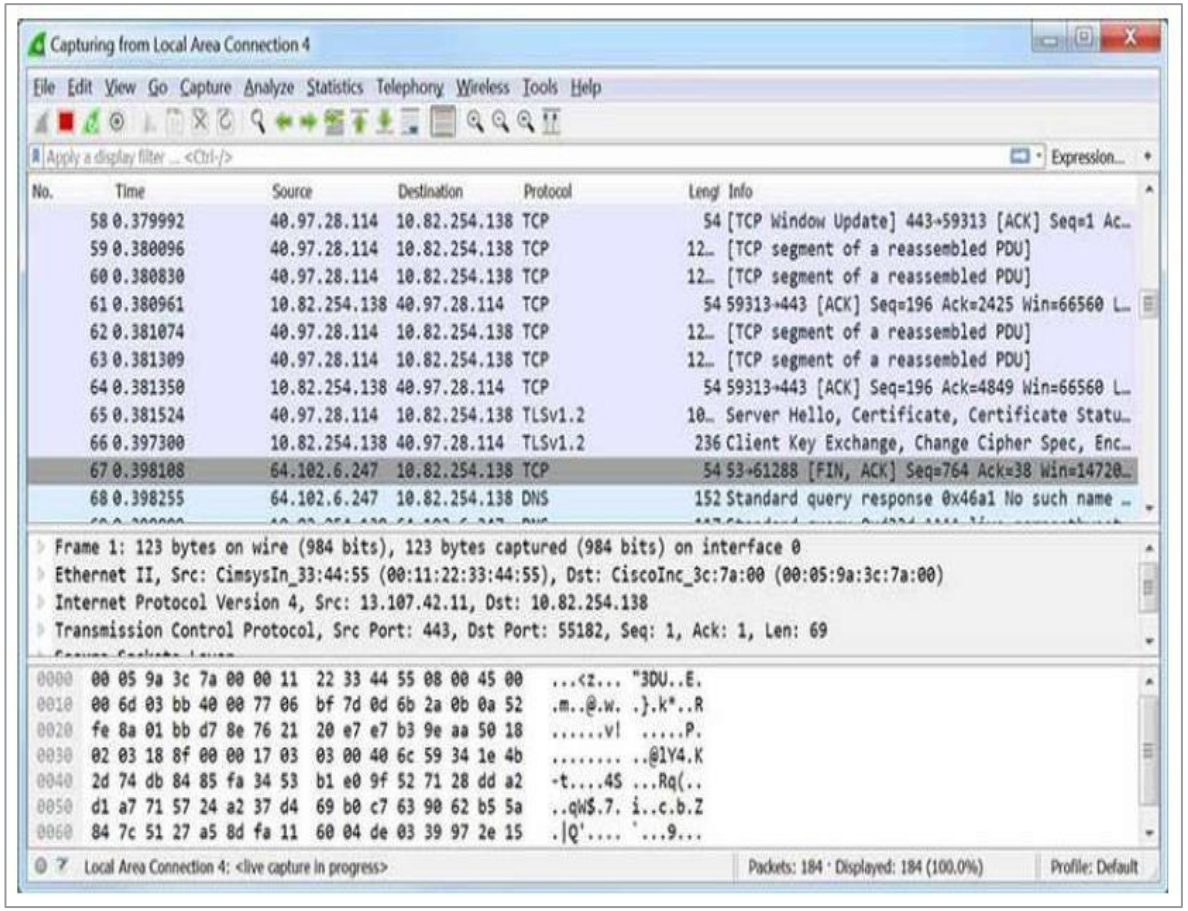
Network Security Monitoring Tools

- Common tools that are used for network security monitoring include:
  - Network protocol analyzers such as Wireshark and Tcpdump
  - NetFlow
  - Security Information and Event Management Systems (SIEM)
- It is common for security analysts to rely on log files and Simple Network Management Protocol (SNMP) for network behavior discovery.



Network Protocol Analyzers

- Network protocol analyzers (or 'packet sniffer' applications) are programs used to capture traffic.
- Protocol analyzers display what is happening on the network through a graphical user interface.
- Network protocol analyzers are not only used for security analysis but also used for network troubleshooting, software and protocol development, and education.
- As shown in the figure, Wireshark is used in Windows, Linux, and Mac OS environments. It is a very useful tool for learning network protocol communications.



Network Protocol Analyzers (Contd.)

- Frames captured by Wireshark are saved in a PCAP file that contains information regarding the frame, interface, packet length, time stamps, and all binary files sent across the network.
- Wireshark can open files containing captured traffic from other software such as the **tcpdump** utility.
- The example in the command output displays a sample **tcpdump** capture of **ping** packets.

```
[root@secOps analyst]# tcpdump -i hl-eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on hl-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64
10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64
10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64
10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64
10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64
10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

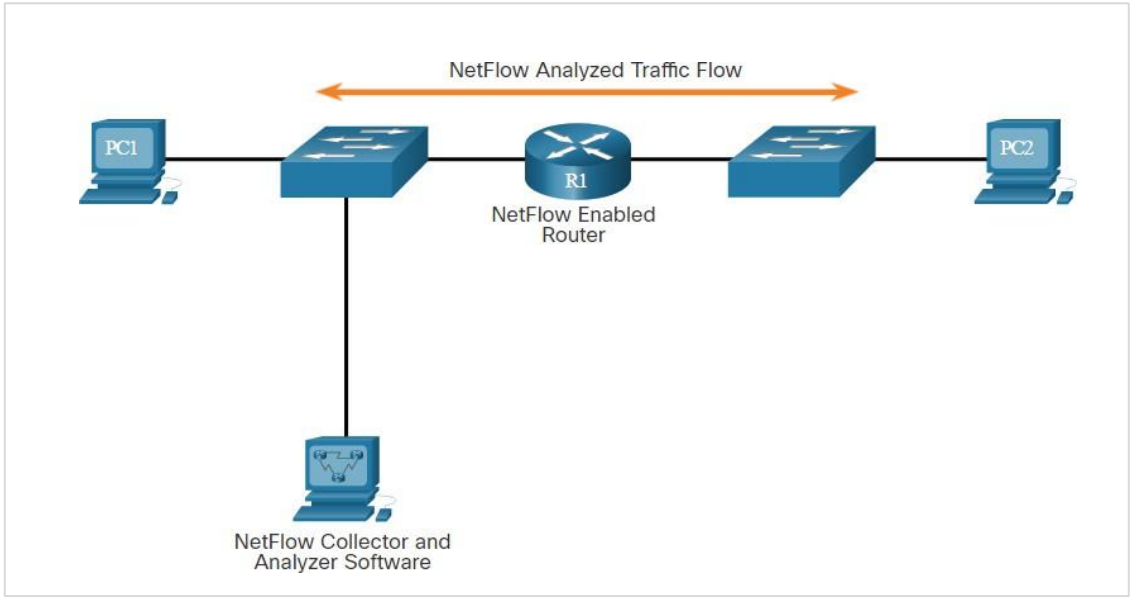
- **Note**: **windump** is a Microsoft Windows variant of **tcpdump**. **tshark** is a Wireshark command line tool that is similar to **tcpdump**.

NetFlow

- NetFlow is a Cisco IOS technology that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch.
- NetFlow is the standard for collecting IP operational data in IP networks.
- NetFlow can be used for network and security monitoring, network planning, and traffic analysis. It provides a complete audit trail of basic information about every IP flow forwarded on a device.
- Although NetFlow stores flow information in a local cache on the device, it should always be configured to forward data to a NetFlow collector which stores the NetFlow data.

NetFlow (Contd.)

- NetFlow can monitor application connection by tracking byte and packet counts for that individual application flow.
- It pushes the statistics over to an external server called a NetFlow collector.
- Cisco Stealthwatch collects NetFlow statistics to perform advanced functions including:
  - **Flow stitching -** It groups individual entries into flows.
  - **Flow deduplication -** It filters duplicate incoming entries from multiple NetFlow clients.
  - **NAT stitching** - It simplifies flows with NAT entries.



PC1 connected to PC2 using HTTPS

SIEM and SOAR

SIEM

- Security Information Event Management (SIEM) is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events.
- SIEM systems include the following essential functions:
  - **Forensic analysis** – The ability to search logs and event records from sources and provide complete information for forensic analysis.
  - **Correlation** – Examines logs and events from different systems or applications, speeding detection of and reaction to security threats.
  - **Aggregation** - Reduces the volume of event data by consolidating duplicate event records.
  - **Reporting** - Presents the correlated and aggregated event data in real-time monitoring and long-term summaries.

SIEM and SOAR (Contd.)

- SIEM provides details on the source of suspicious activity:
  - User information such as username, authentication status, location.
  - Device information such as manufacturer, model, OS version, MAC address, network connection method, and location.
  - Posture information such as compliance of the device with the security policy and updated antivirus files and OS patches.

SOAR

- Security Orchestration, Automation, and Response (SOAR) enhances SIEM.
- SOAR helps security teams investigate security incidents and add enhanced data gathering and a number of functionalities that aid in security incident response.

SIEM and SOAR (Contd.)

- SOAR solutions:
  - Provides case management tools that allow cybersecurity personnel to research and investigate incidents, frequently by integrating threat intelligence into the network security platform.
  - Use artificial intelligence to detect incidents that aid in incident analysis and response.
  - Automate complex incident response procedures and investigations, which are potentially labor intensive tasks performed by Security Operations Center (SOC) staff by executing run books.
  - Offers dashboards and reports to document incident response to improve SOC key performance indicators and can enhance network security for organizations.
- SOAR helps analysts respond to the threat.

SIEM Systems

- An open source product called Security Onion includes the ELK suite for SIEM functionality.
- ELK is an acronym for three products from Elastic:
  - **Elasticsearch -** Document oriented full text search engine.
  - **Logstash -** Pipeline processing system that connects ‘inputs’ to ‘outputs’ with optional ‘filters’ in between.
  - **Kibana -** Browser based analytics and search dashboard for Elasticsearch.
- **Note**: SolarWinds Security Event Manager and Splunk Enterprise Security are two popular proprietary SIEM systems used by SOCs.

Lab - Packet Tracer - Logging Network Activity

In this Packet tracer, you will do the following:

- Intercept credentials using a sniffer device, while observing an FTP session. An exchange of Syslog messages will also be intercepted by a sniffer device.

15.3 Network Monitoring and Tools Summary

What Did I Learn in this Module?

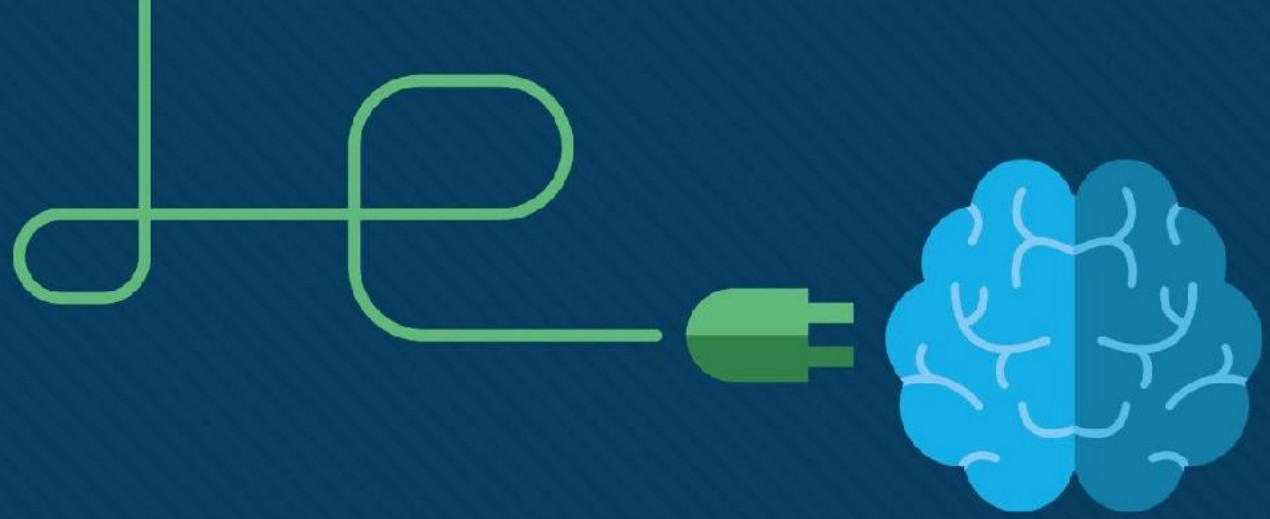
- To mitigate threats, all networks should be secured and protected using a defense-in-depth approach.
- This requires a security infrastructure that consists of firewalls, IDS, IPS, and endpoint security software.
- A cybersecurity analyst needs to review all alerts that are generated by network devices and validate them.
- Tools such as IDS, packet analyzers, SNMP, NetFlow, and others are used to determine normal network behavior.
- Two common methods that are used to capture traffic and send it to network monitoring devices are network taps and traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

What Did I Learn in this Module? (Contd.)

- Common tools that are used for network security monitoring include network protocol analyzers (Wireshark and Tcpdump), NetFlow, and SIEM.
- Network protocol analyzers are programs that are used to capture traffic.
- Netflow is a Cisco IOS feature that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch. It can be used for network and security monitoring, network planning, and traffic analysis.
- SIEM is a technology that is used to provide real time reporting and long-term analysis of security events.


CISCO

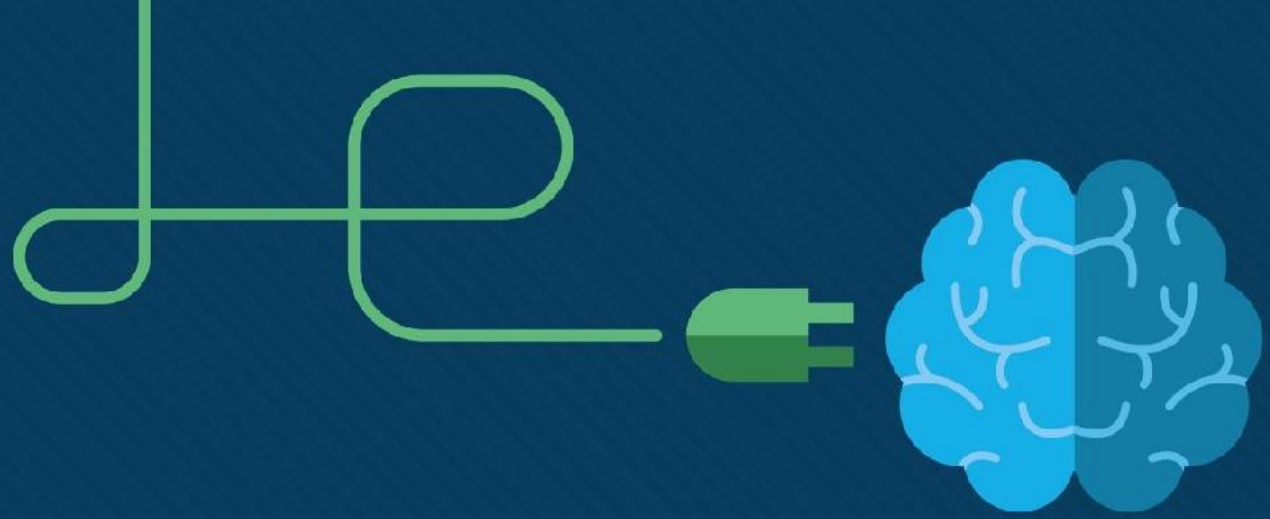
Module 16 Attacking the foundation



Module 16: Attacking the Foundation

Instructor Materials

CyberOps Associate v1.0



Module 16: Attacking the Foundation

CyberOps Associate v1.0

Module Objectives

Module Title: Attacking the Foundation

Module Objective: Explain how TCP/IP vulnerabilities enable network attacks.

Topic Title	Topic Objective
IP PDU Details	Explain the IPv4 and IPv6 header structure.
IP Vulnerabilities	Explain how IP vulnerabilities enable network attacks.
TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities enable network attacks.

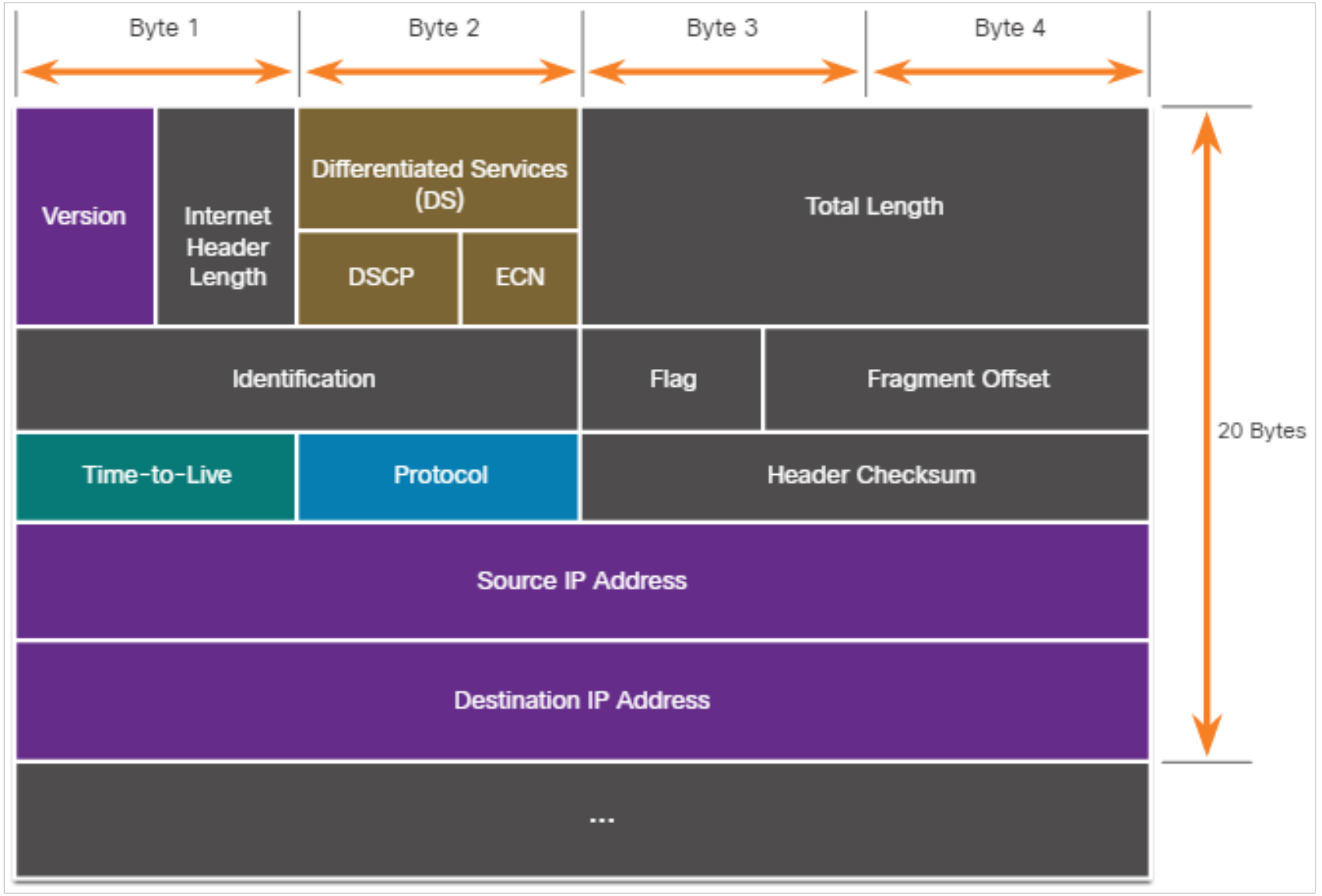
16.1 IP PDU Details

IPv4 and IPv6

- IP was designed as a Layer 3 connectionless protocol. It provides the necessary functions to deliver a packet from a source host to a destination host over an interconnected system of networks.
- IP makes no effort to 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.
- Also, threat actors can tamper with the other fields in the IP header to carry out their attacks. So, it is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.

The IPv4 Packet Header

The fields in the IPv4 packet header are shown in the figure. There are 10 fields in the IPv4 packet header.



The IPv4 Packet Header (Contd.)

The following table describes the IPv4 header fields:

IPv4 Header Field	Description
Version	• Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
Internet Header length	• A 4-bit field containing the length of the IP header. • The minimum length of an IP header is 20 bytes.
Differentiated Services or DiffServ (DS)	• Formerly called the Type of Service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. • The six most significant bits of the DiffServ field are the Differentiated Services Code Point (DSCP). • The last two bits are the Explicit Congestion Notification (ECN) bits.
Total length	• Specifies the length of the IP packet including the IP header and the user data. • The total length field is 2 bytes, so the maximum size of an IP packet is 65,535 bytes.

The IPv4 Packet Header (Contd.)

IPv4 Header Field	Description
Identification, Flag, and Fragment offset	• As an IP packet moves, it might need to cross a route that cannot handle the size of the packet. The packet will be divided, or fragmented, into smaller packets and reassembled later. • These fields are used to fragment and reassemble packets.
Time-to-Live (TTL)	• Contains an 8-bit binary value that is used to limit the lifetime of a packet. • The packet sender sets the initial TTL value, and it is decreased by one each time the packet is processed by a router. • If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address.
Protocol	• Field is used to identify the next level protocol. • This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. • Common values include ICMP (1), TCP (6), and UDP (17).

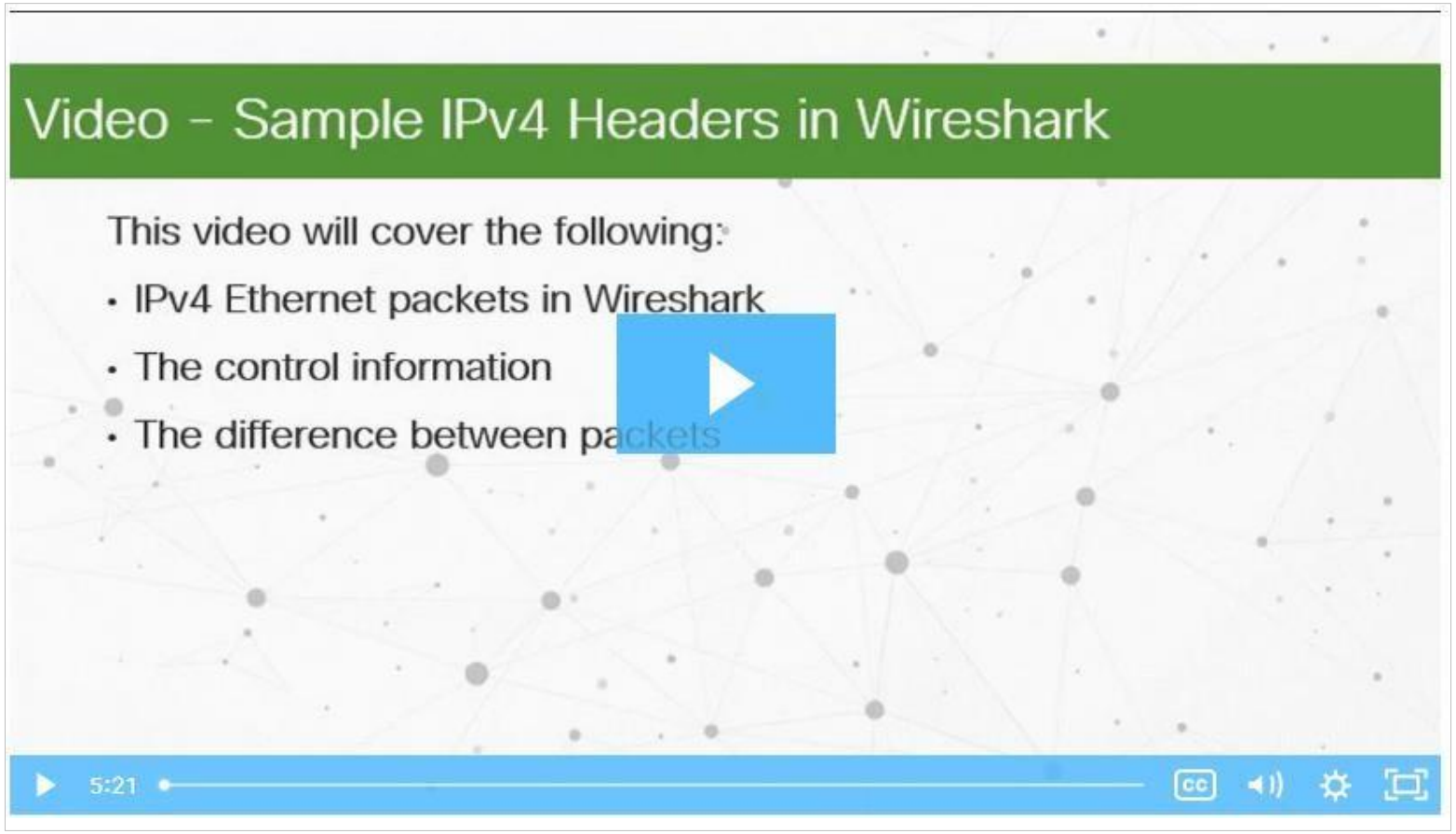
The IPv4 Packet Header (Contd.)

IPv4 Header Field	Description
Header checksum	• A value that is calculated based on the contents of the IP header. • Used to determine if any errors have been introduced during transmission.
Source IPv4 Address	• Contains a 32-bit binary value that represents the source IPv4 address of the packet. • The source IPv4 address is always a unicast address.
Destination IPv4 Address	• Contains a 32-bit binary value that represents the destination IPv4 address of the packet.
Options and Padding	• This is a field that varies in length from 0 to a multiple of 32 bits. • If the option values are not a multiple of 32 bits, 0s are added or padded to ensure that this field contains a multiple of 32 bits.

Video - Sample IPv4 Headers in Wireshark

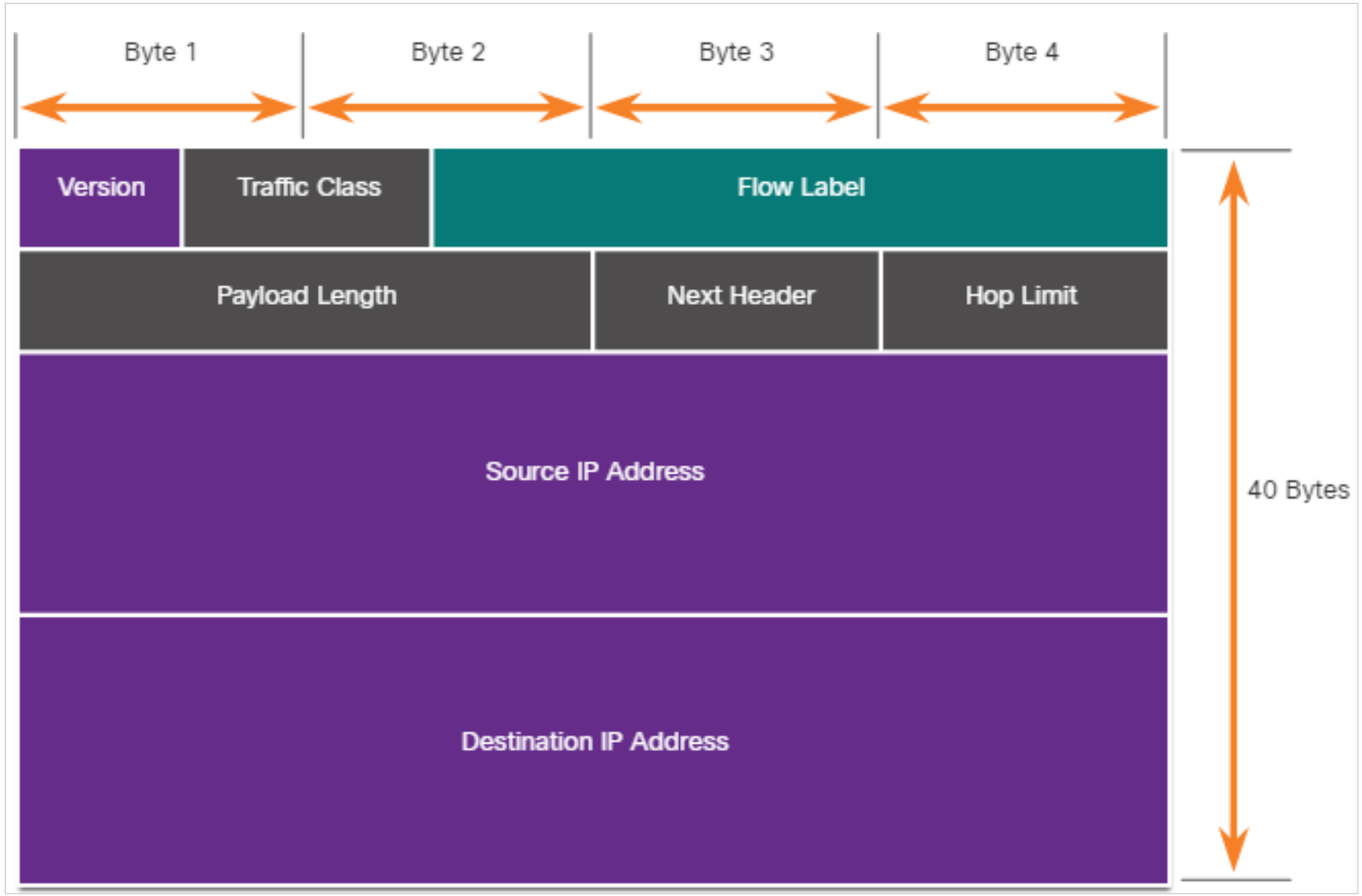
Click Play in the figure to view a demonstration of examining IPv4 headers in a Wireshark capture.

Link to video



The IPv6 Packet Header

There are eight fields in the IPv6 packet header, as shown in the figure.



The IPv6 Packet Header (Contd.)

The following table describes the IPv6 header fields:

IPv6 Header Field	Description
Version	• This field contains a 4-bit binary value set to 0110 that identifies this as an IPv6 packet.
Traffic Class	• This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
Flow Label	• This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
Payload Length	• This 16-bit field indicates the length of the data portion or payload of the IPv6 packet.
Next Header	• This 8-bit field is equivalent to the IPv4 Protocol field. • It indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol.

The IPv6 Packet Header (Contd.)

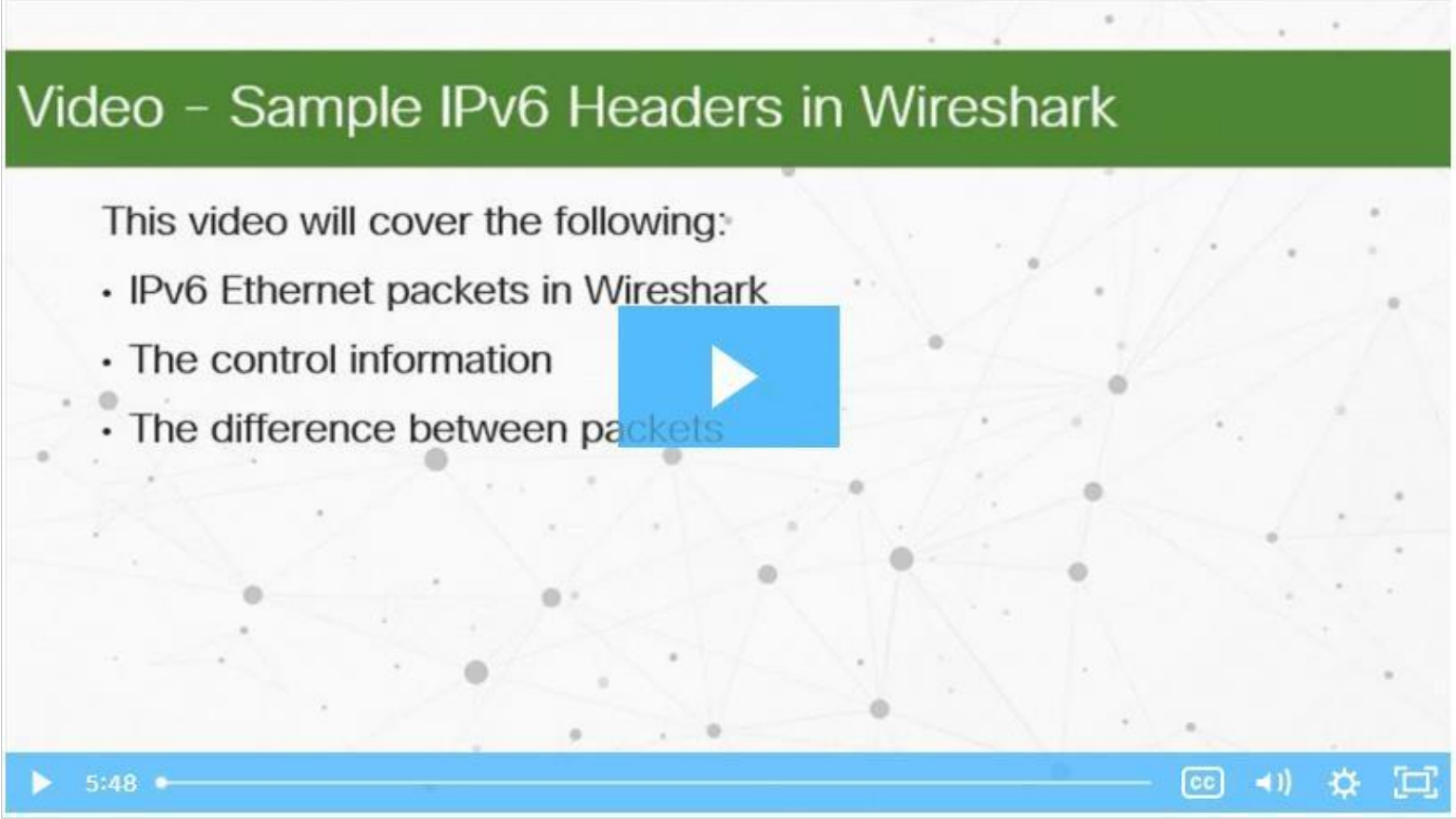
IPv6 Header Field	Description
Hop Limit	•This 8-bit field replaces the IPv4 TTL field. •This value is decremented by a value of 1 by each router that forwards the packet. •When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host, indicating that the packet did not reach its destination because the hop limit was exceeded.
Source IPv6 Address	•This 128-bit field identifies the IPv6 address of the sending host.
Destination IPv6 Address	•This 128-bit field identifies the IPv6 address of the receiving host.

- An IPv6 packet also contain extension headers (EH) that provide optional network layer information.
- Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility, and more.

Video - Sample IPv6 Headers in Wireshark

Click Play in the figure to view a demonstration of examining IPv6 headers in a Wireshark capture.

Link to video



16.2 IP Vulnerabilities

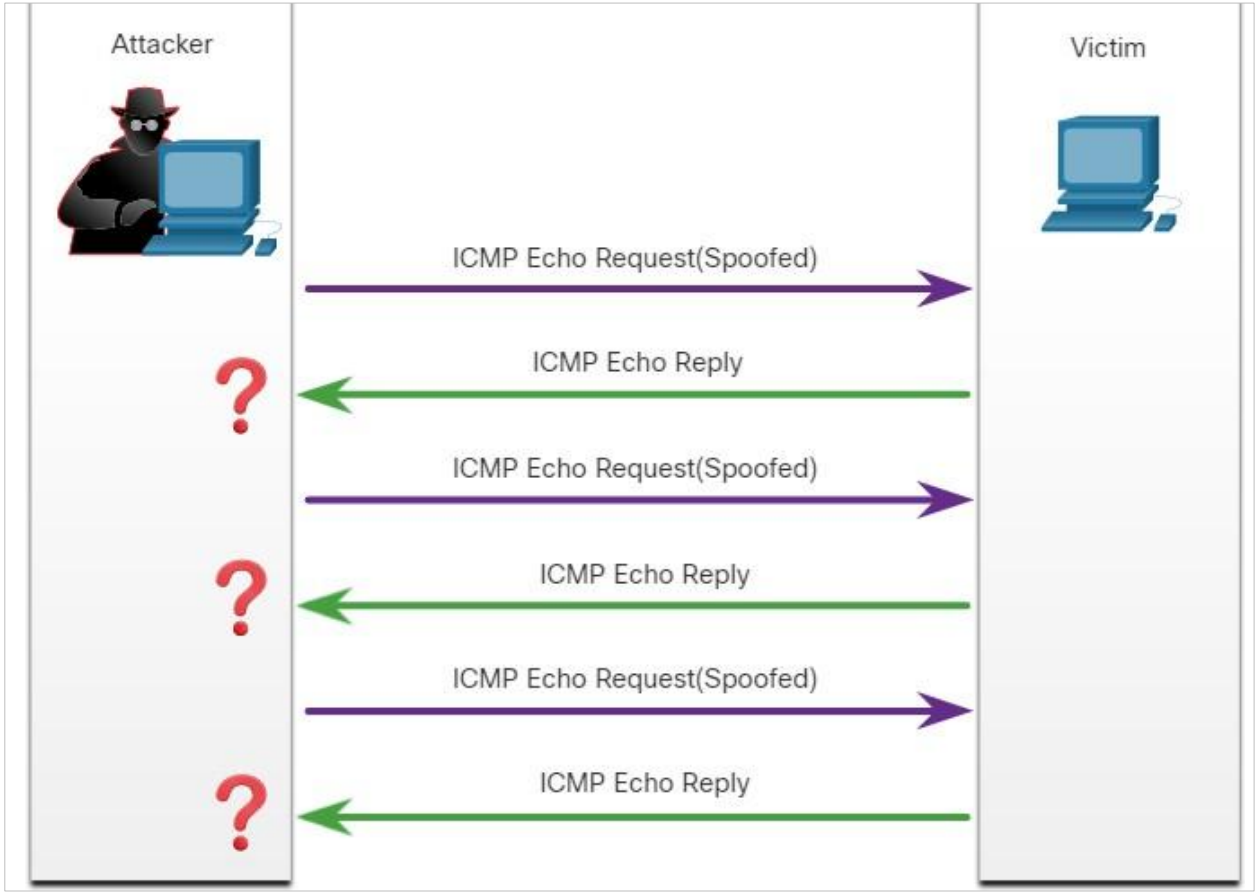
IP Vulnerabilities

The following table lists some of the common IP-related attacks:

IP Attacks	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.
DoS attacks	Threat actors attempt to prevent legitimate users from accessing information or services.
DDoS attacks	Similar to a DoS attack, but features a simultaneous, coordinated attack from multiple source machines.
Address spoofing attacks	Threat actors spoof the source IP address in an attempt 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 simply 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

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. ICMP messages are generated by devices when a network error or outage occurs.
- The ping command is a user-generated ICMP message, called an echo request, that is used to verify connectivity to a destination.
- Threat actors use ICMP for reconnaissance and scanning attacks.
- Threat actors also use ICMP for DoS and DDoS attacks, as shown in the ICMP flood attack in the figure.



***Note**: ICMP for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) are susceptible to similar types of attacks.*

ICMP Attacks (Contd.)

- Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet.
- The following table lists the common ICMP messages of interest to threat actors.

ICMP Message	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.

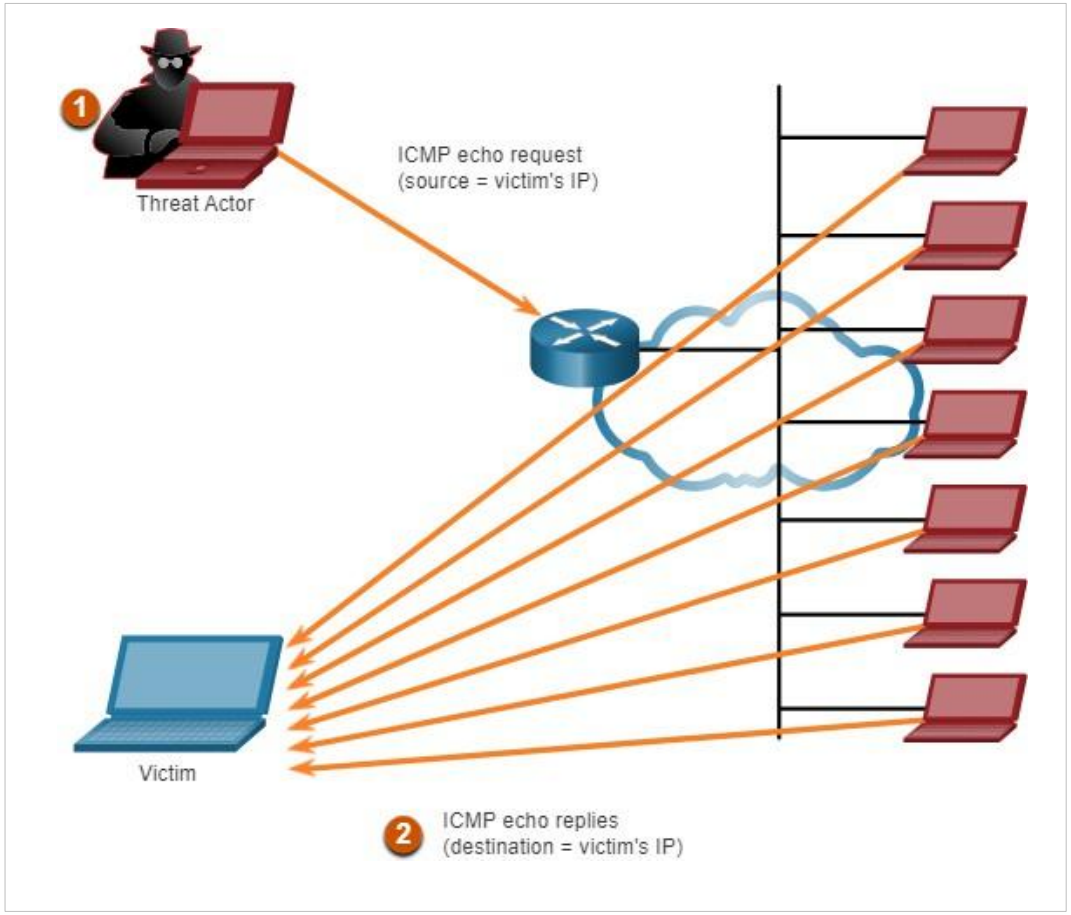
Video - Amplification, Reflection, and Spoofing Attacks

Click Play in the figure to view a video of amplification, reflection, and spoofing attacks.

Link to video

Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques to create DoS attacks.
- The figure shows how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.
  - **Amplification** - The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.
  - **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.
- Threat actors also use resource exhaustion attacks.



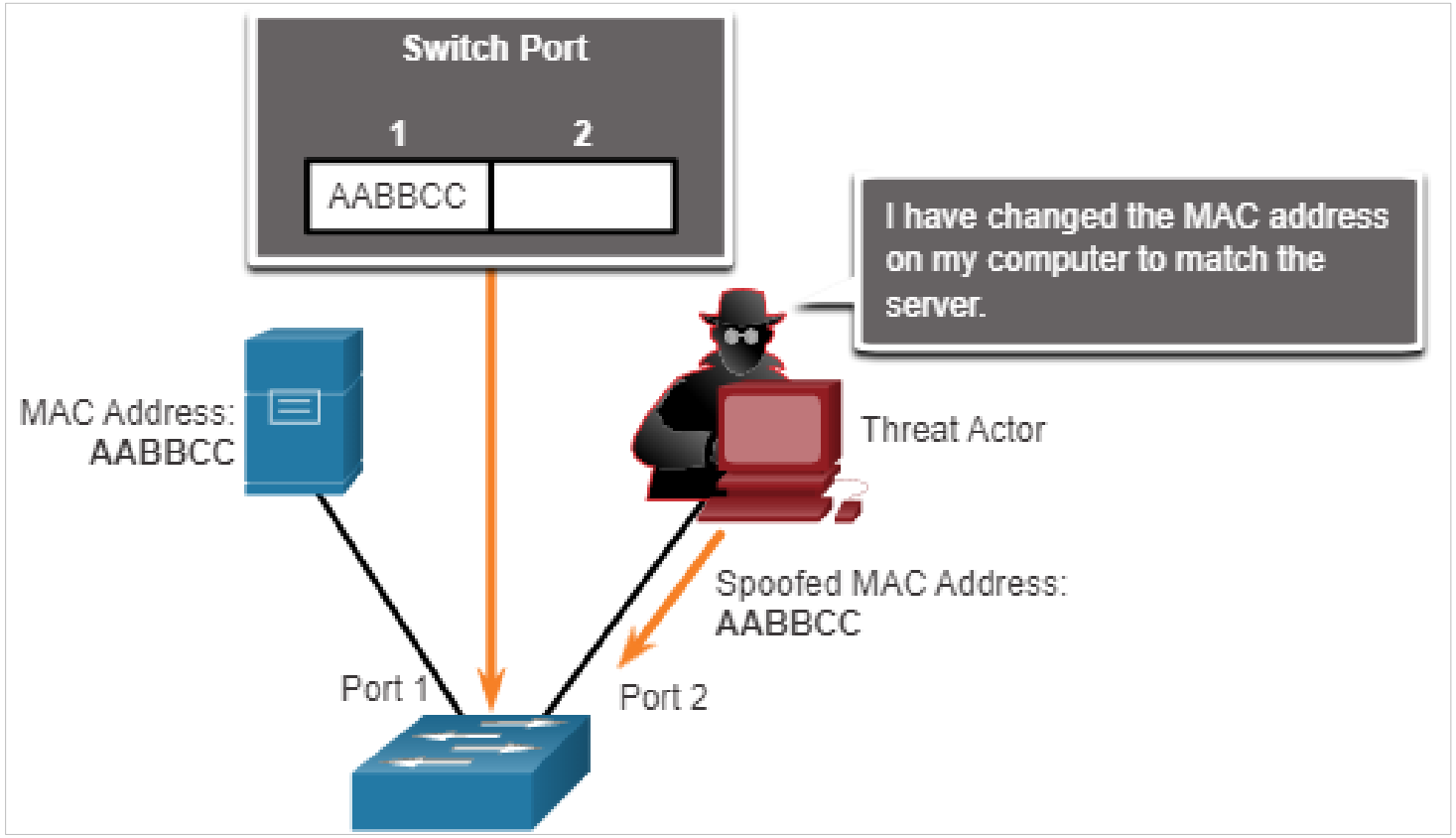
***Note**: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.*

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.

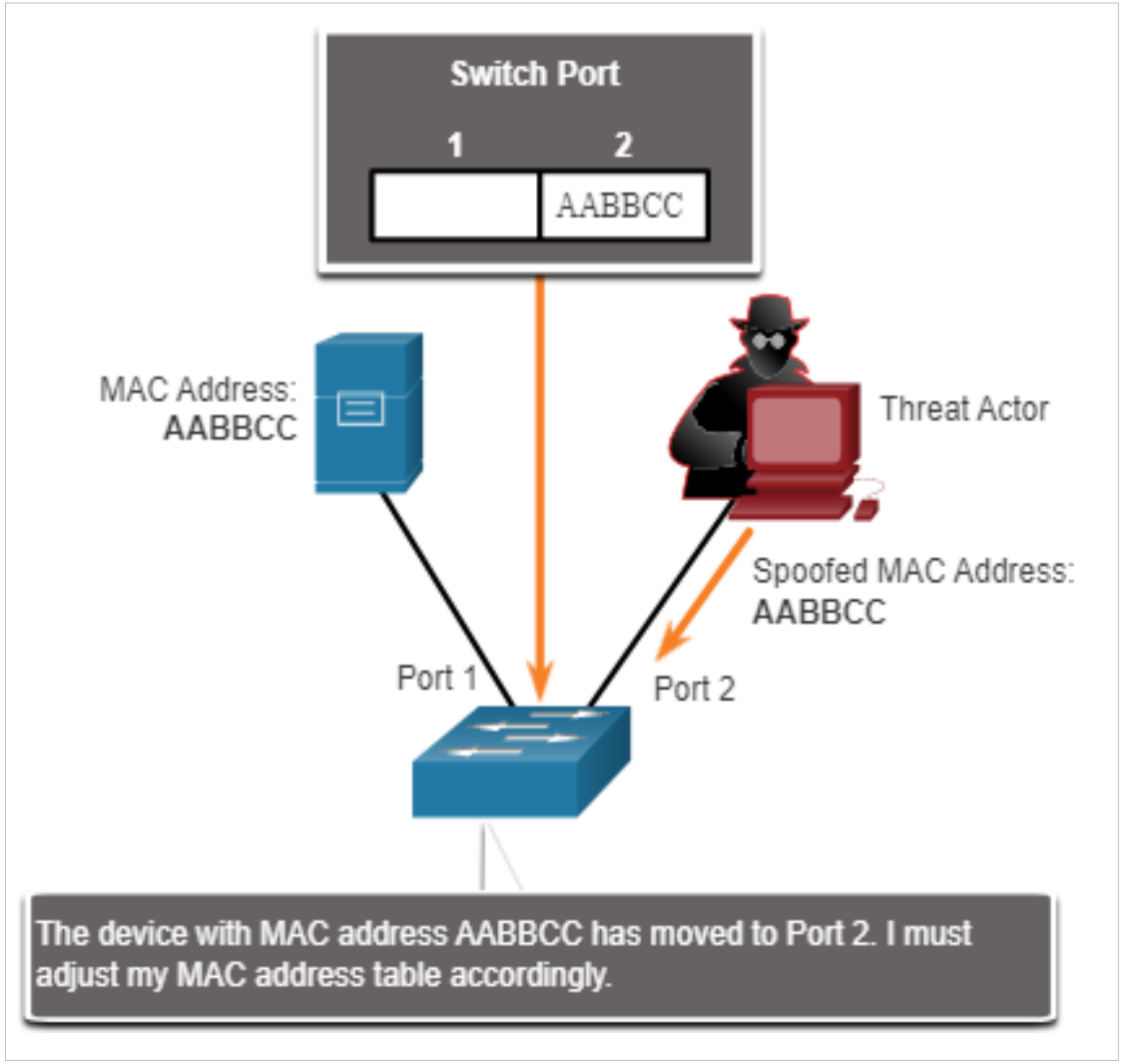
Address Spoofing Attacks (Contd.)

- 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.



Address Spoofing Attacks (Contd.)

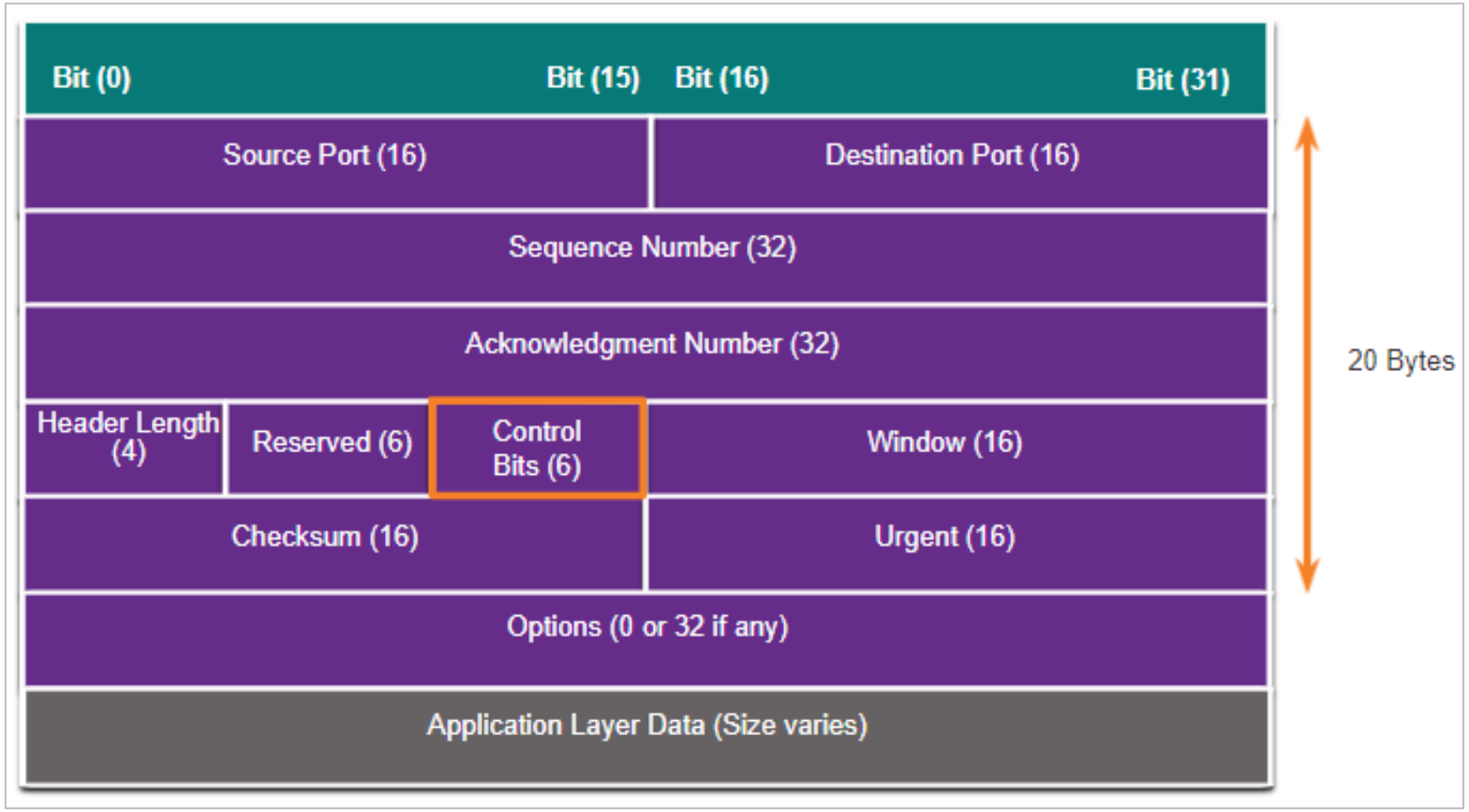
- The switch overwrites the current CAM table entry and assigns the MAC address to the new port, as shown in the figure.
- It then forwards frames destined for the target host to the attacking host.
- Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MiTM condition.



16.3 TCP and UDP Vulnerabilities

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
  - **ACK** - Acknowledgment field significant
  - **PSH** - Push function
  - **RST**- Reset the connection
  - **SYN** - Synchronize sequence numbers
  - **FIN** - No more data from sender



TCP Services

TCP provides these services:

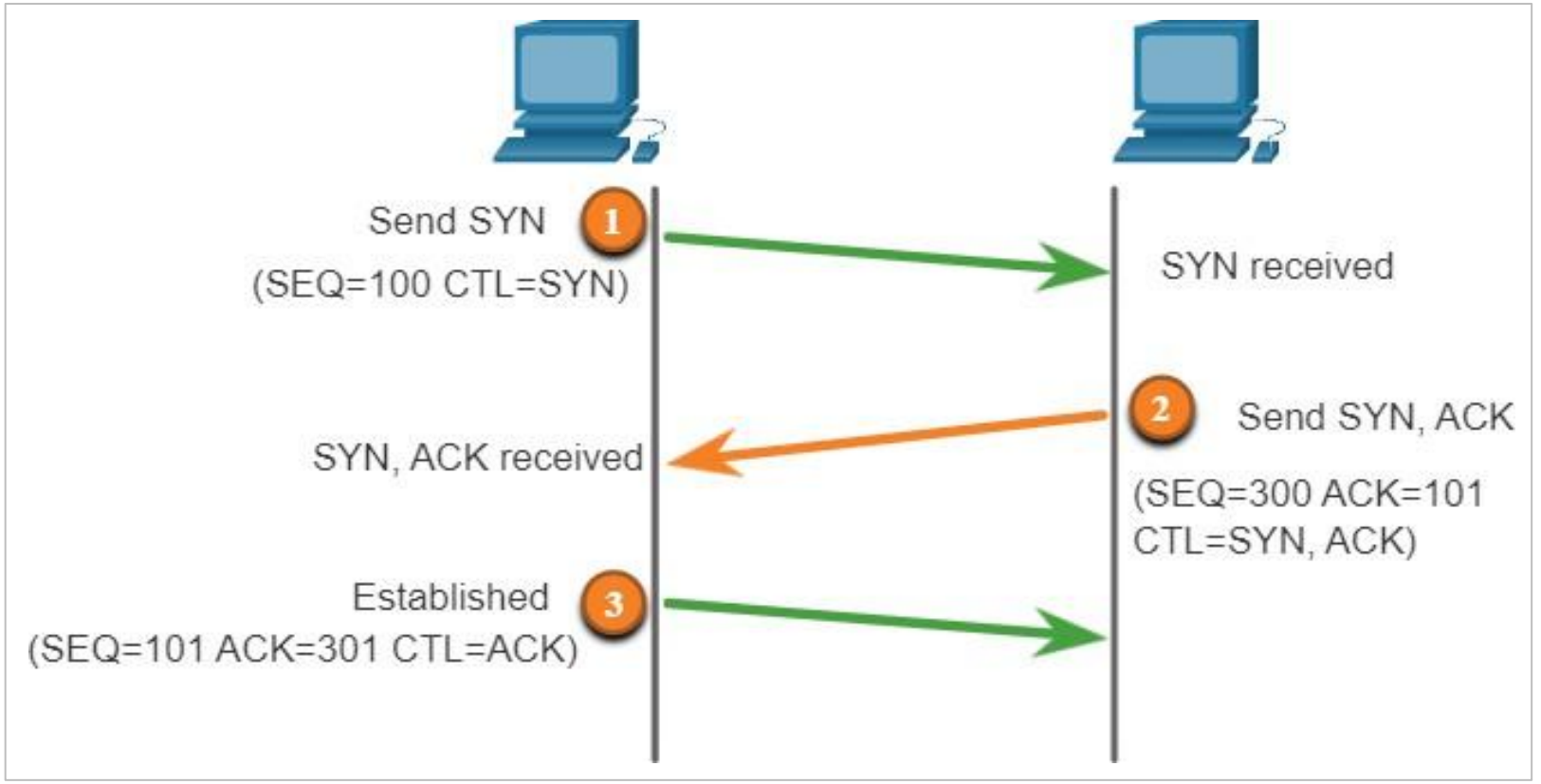
- **Reliable delivery** - TCP incorporates acknowledgments to guarantee delivery, instead of relying on upper-layer protocols to detect and resolve errors. If a timely acknowledgment is not received, the sender retransmits the data. Requiring acknowledgments of received data can cause substantial delays. 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 one segment at a time, multiple segments can be acknowledged 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. If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.

TCP Services (Contd.)

TCP Three-Way Handshake

A TCP connection is established in three steps:

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

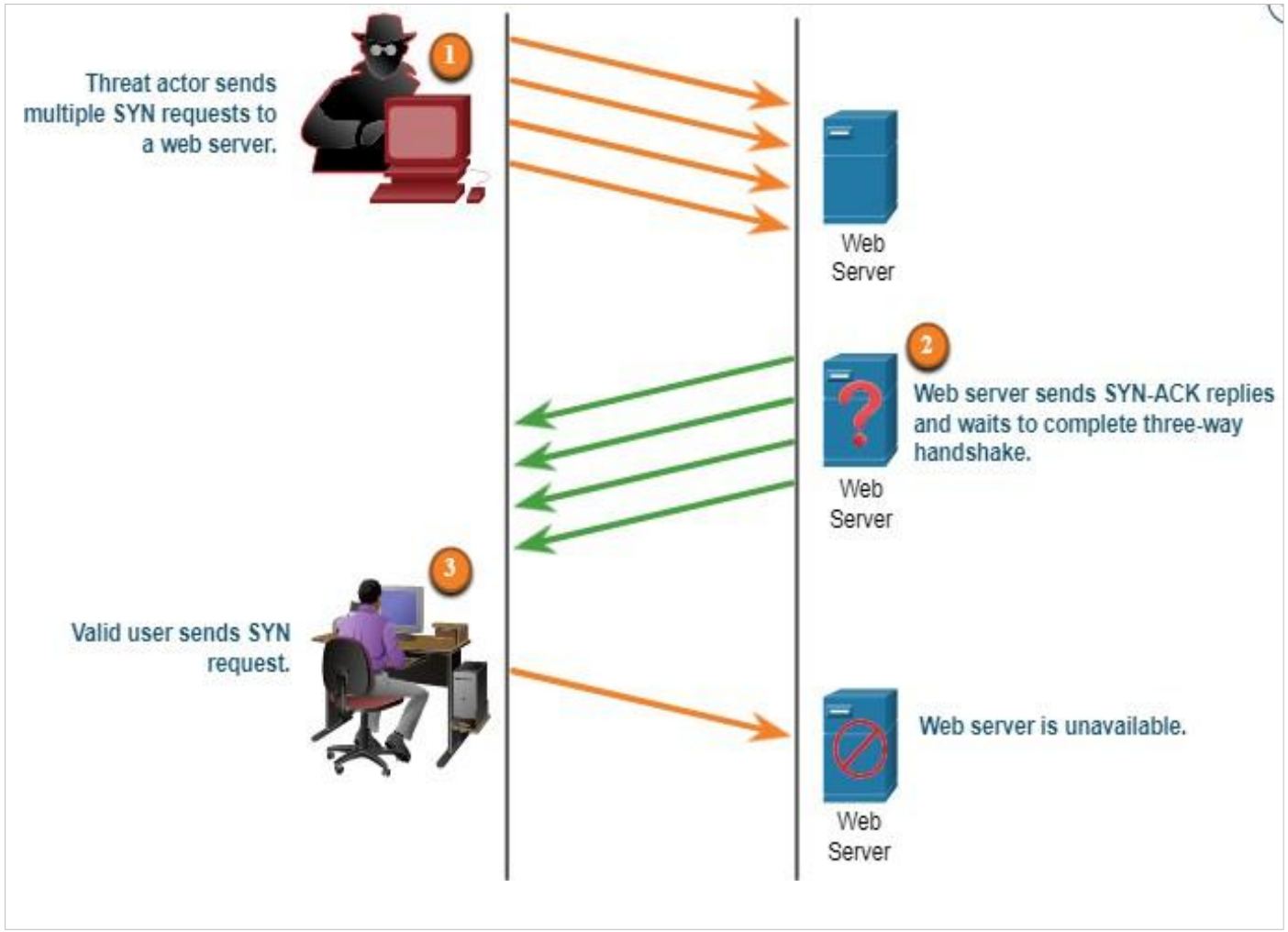


TCP Attacks

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

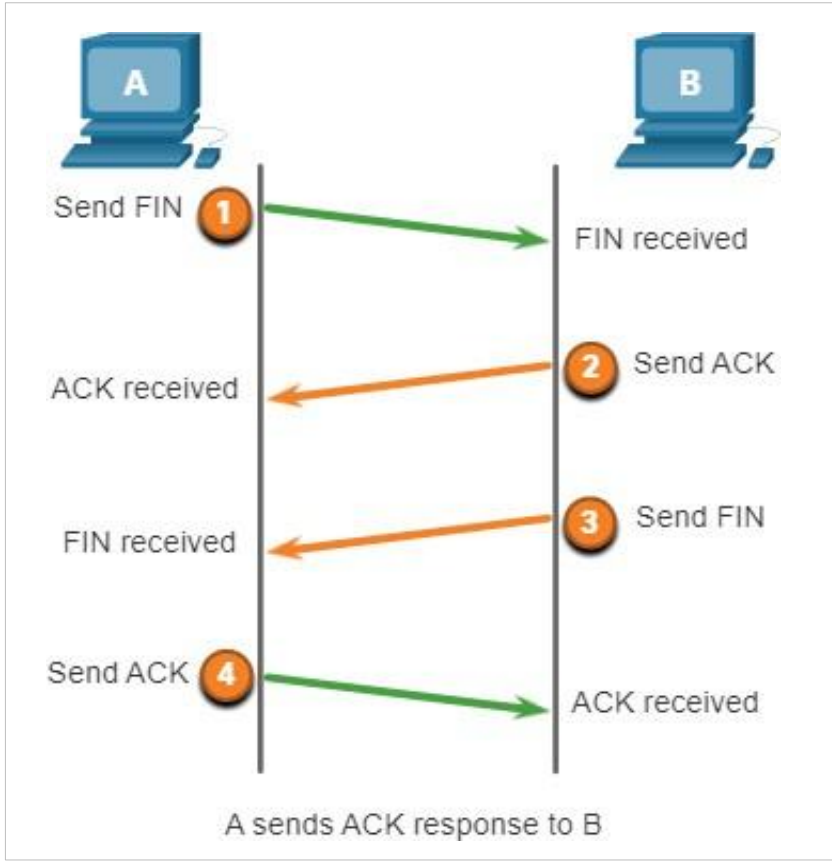
- The TCP SYN Flood attack exploits the TCP three-way handshake.
- The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target.
- The target replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK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



TCP Attacks (Contd.)

TCP Reset Attack

- A TCP reset attack can be used to terminate TCP communications between two hosts.
- A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.
- Terminating a TCP session uses the following four-way exchange process:
- When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
- The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
- The server sends a FIN to the client to terminate the server-to-client session.
- The client responds with an ACK to acknowledge the FIN from the server.



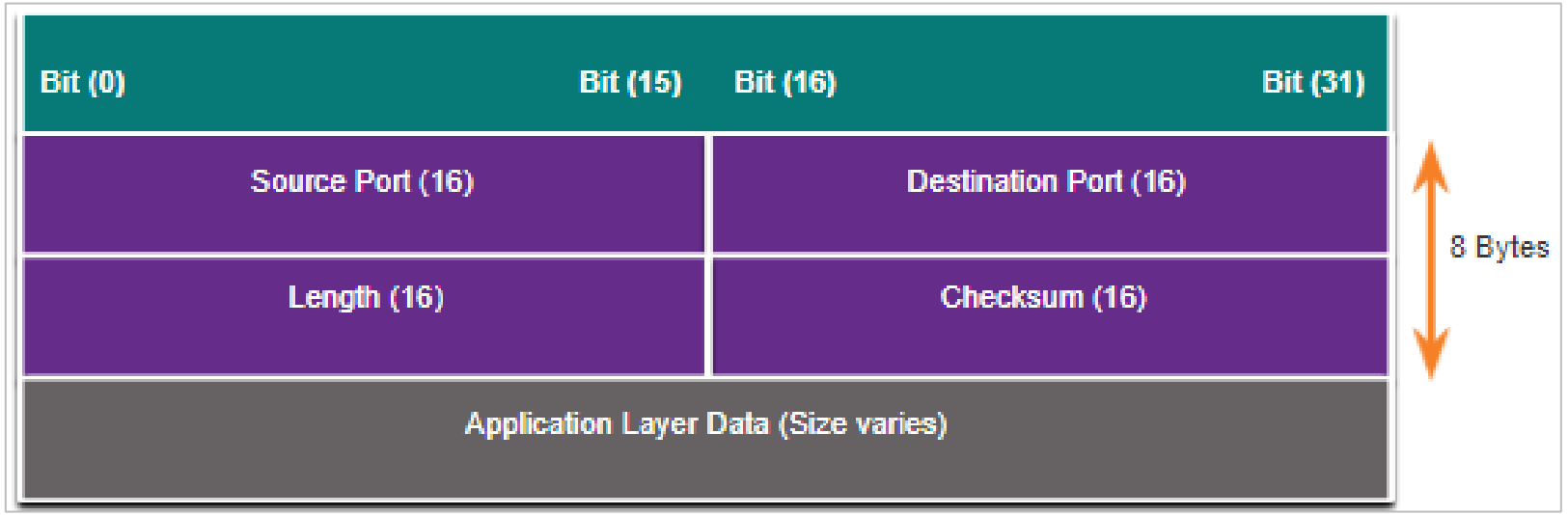
TCP Attacks (Contd.)

TCP Session Hijacking

- TCP session hijacking is another TCP vulnerability.
- 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 receive, data from the target device.

UDP Segment Header and Operation

- UDP is commonly used by DNS, DHCP, 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.
- The UDP segment structure, shown in the figure, is much smaller than TCP.
- Although UDP is normally called unreliable, this does not mean that applications that use UDP are always unreliable. It means that these functions are not provided by the transport layer protocol and must be implemented elsewhere if required.



- The low overhead of UDP makes it very desirable for protocols that make simple request and reply transactions.

UDP Attacks

- UDP is not protected by any encryption. Encryption can be added 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.

UDP Flood Attacks

- In a UDP flood attack, all the resources on a network are consumed.
- The threat actor must use a tool like UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood of 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 ports. This will cause the server to reply with an ICMP port unreachable message.
- As 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.

16.4 Attacking the Foundation Summary

What Did I Learn in this Module?

- IP was designed as a Layer 3 connectionless protocol.
- The IPv4 header consists of several fields while the IPv6 header contains fewer fields. It is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.
- There are different types of attacks that target IP. Common IP-related attacks include:
  - ICMP attacks
  - Denial-of-Service (DoS) attacks
  - Distributed Denial-of-Service (DoS) attacks
  - Address spoofing attacks
  - Man-in-the-middle attack (MiTM)
  - Session hijacking

What Did I Learn in this Module? (Contd.)

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable.
- TCP segment and UDP datagram information appear immediately after the IP header. It is important to understand Layer 4 headers and their functions in data communication.
- Threat actors can conduct a variety of TCP related attacks:
  - TCP port scans
  - TCP SYN Flood attack
  - TCP Reset Attack
  - TCP Session Hijacking attack
- The UDP segment (i.e., datagram) is much smaller than the TCP segment, which makes it very desirable for use by protocols that make simple request and reply transactions such as DNS, DHCP, SNMP, and others.

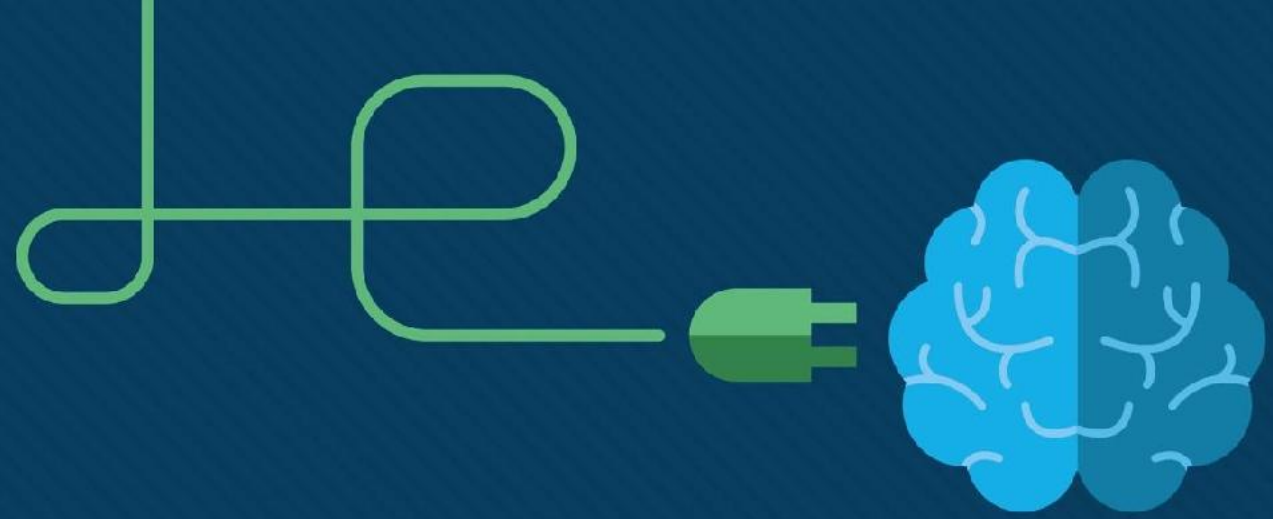

CISCO

Module 17 Attacking what we do

Module 17:Attacking What We Do

Instructor Materials

CyberOps Associate v1.0



Module 17:Attacking What We Do

CyberOps Associates v1.0

Module Objectives

Module Title: Attacking What We Do

Module Objective: Explain how common network applications and services are vulnerable to attack.

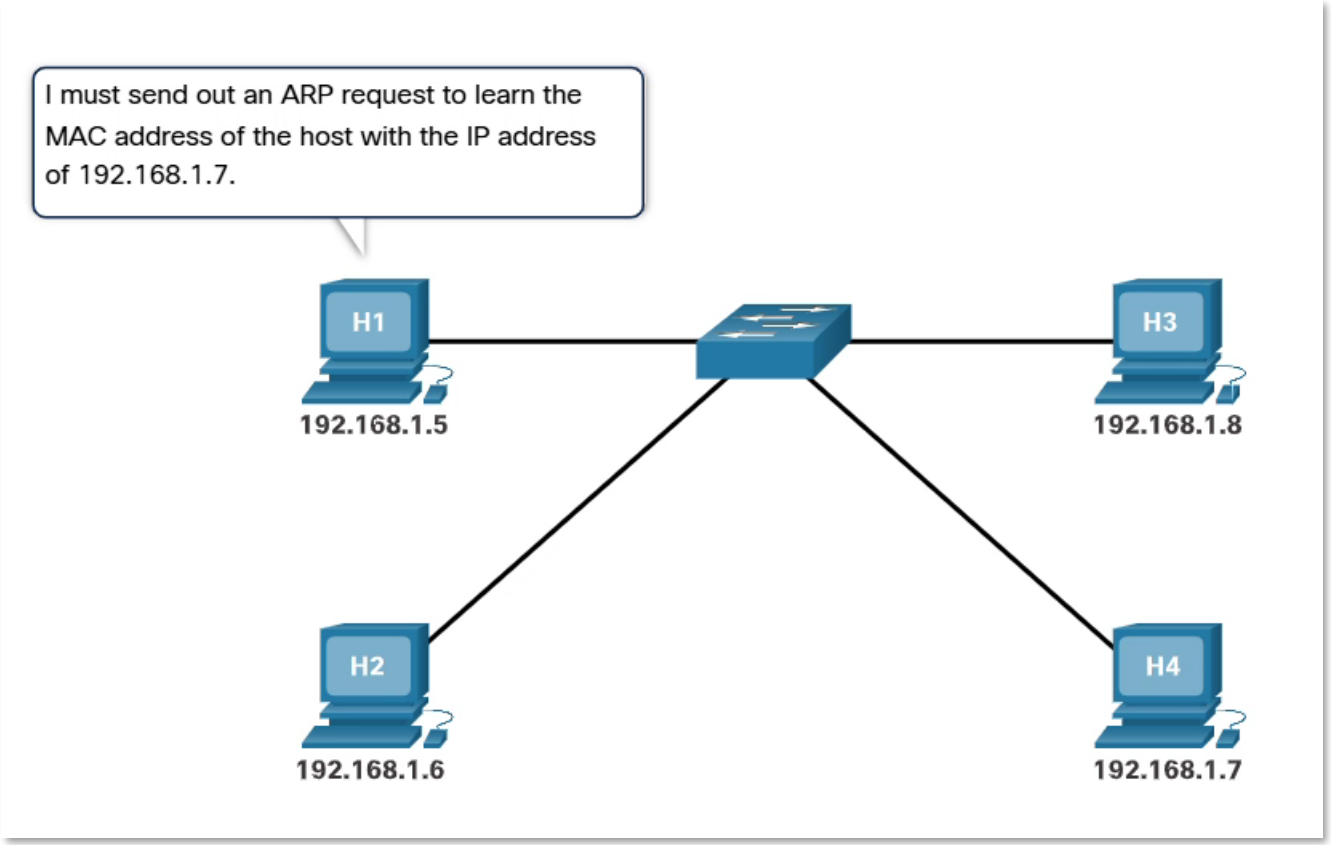
Topic Title	Topic Objective
IP Services	Explain IP service vulnerabilities
Enterprise Services	Explain how network application vulnerabilities enable network attacks

17.1 IP Services

ARP Vulnerabilities

- Hosts broadcast an ARP Request to other hosts on the network segment to determine the MAC address of a host with a particular IP address.
- The host with the matching IP address in the ARP Request sends an ARP Reply called “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network
- The goal is to associate the threat actor’s MAC address with the IP address of the default gateway in the ARP caches of hosts on the LAN segment.

Play the animation to see the ARP process at work.

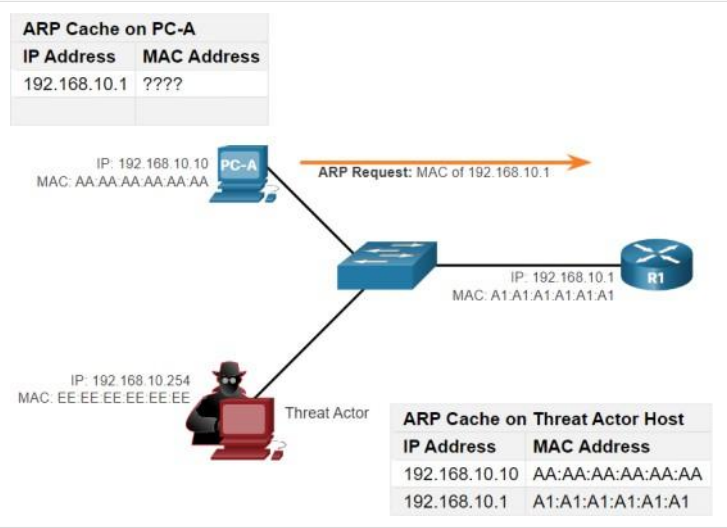


ARP Cache Poisoning

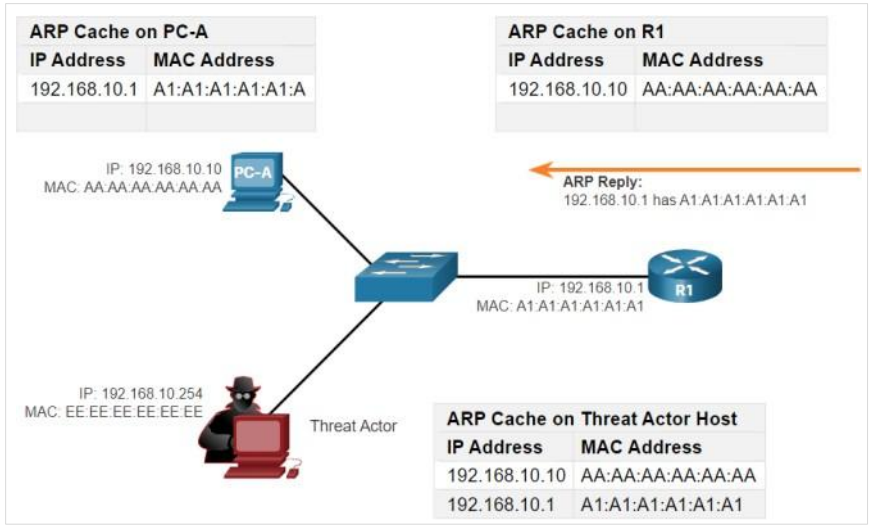
- ARP cache poisoning can be used to launch various man-in-the-middle attacks.

ARP cache poisoning process

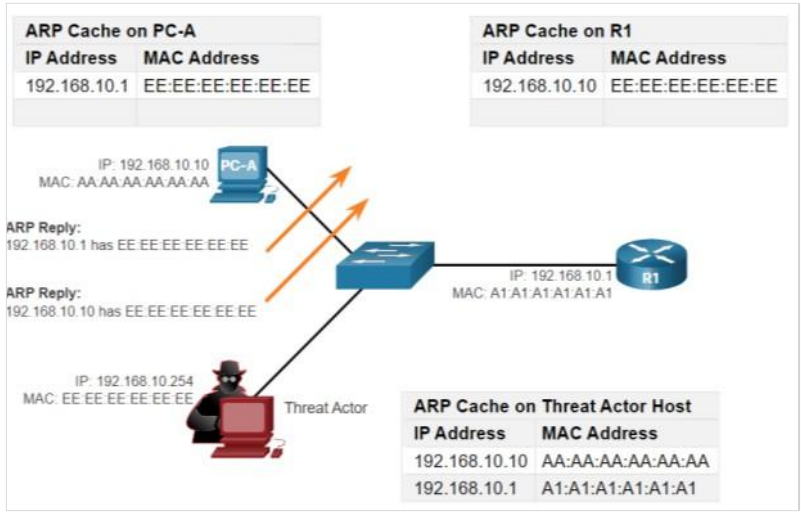
ARP Request



ARP Reply



Spoofed Gratuitous ARP replies



***Note**: There are many tools available on the internet to create ARP MITM attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others.*

DNS Attacks

DNS attacks include the following:

DNS open resolver attacks:

- A DNS open resolver is a publicly open DNS server such as Google DNS (8.8.8.8) that answers client's queries outside its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

DNS Resolver Vulnerabilities	Description
DNS cache poisoning attacks	Threat actors send spoofed, falsified Record Resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites.
DNS amplification and reflection attacks	Threat actors send DNS messages to the open resolvers using the IP address of a target host.
DNS resource utilization attacks	This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver.

DNS Attacks (Contd.)

DNS Stealth Attacks

- To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

DNS Stealth Techniques	Description
Fast Flux	Threat actors use this technique to hide their phishing and malware delivery sites. The DNS IP addresses are continuously changed within minutes.
Double IP Flux	Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack.
Domain Generation Algorithms	Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers.

DNS Attacks (Contd.)

DNS Domain Shadowing Attacks

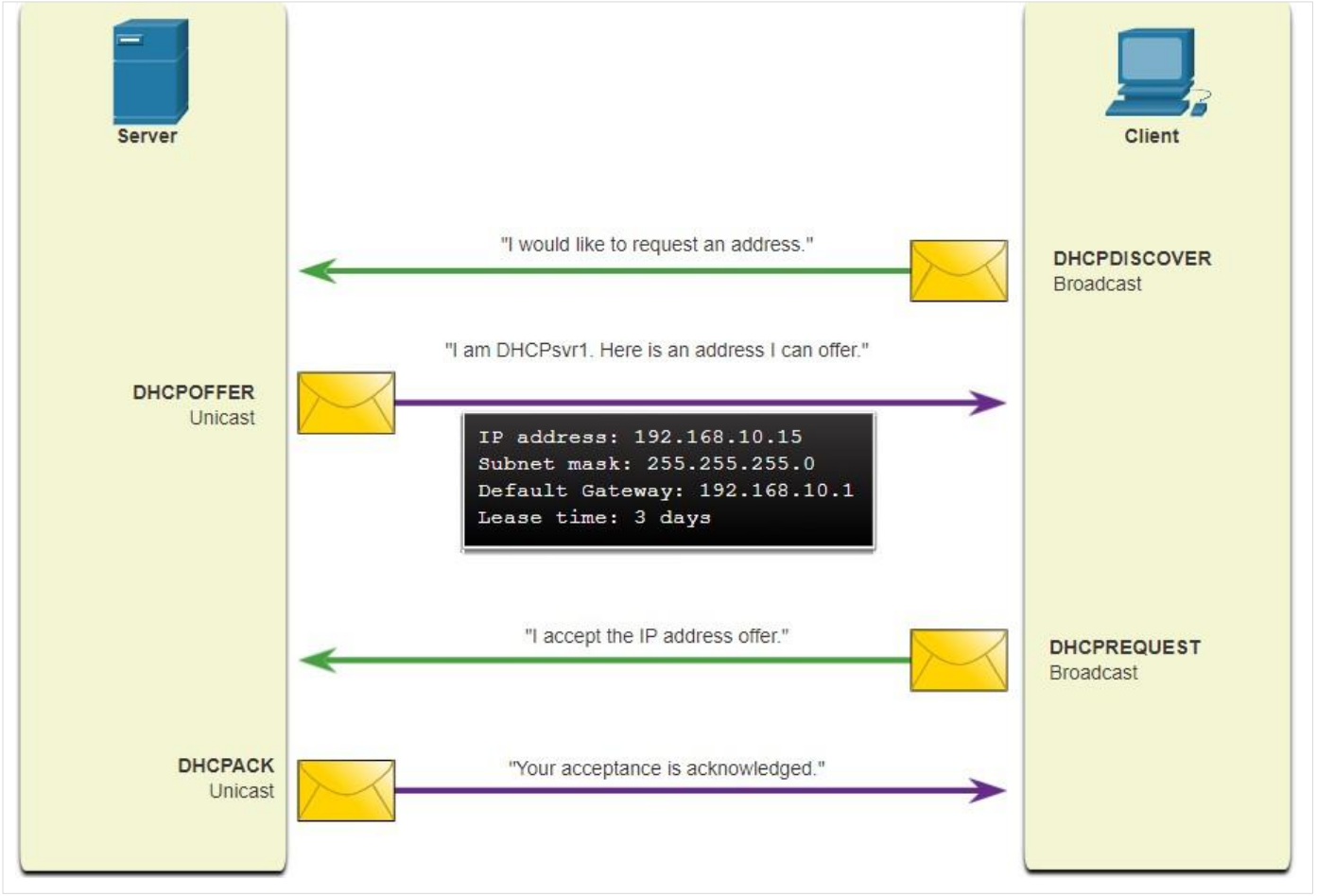
- In Domain Shadowing, threat actor gather domain account credentials in order to create multiple sub-domains which will be used during the attacks.
- These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

DNS Tunneling

- It is necessary for the cybersecurity analyst to be able to detect when an attacker is using DNS tunneling to steal data, and prevent and contain the attack.
- To accomplish this, the security analyst must implement a solution that can block the outbound communications from the infected hosts.
- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions.
- For the threat actor to use DNS tunneling, the different types of DNS records such as TXT, MX, SRV, NULL, A, or CNAME are altered. For example, a TXT record can store the commands that are sent to the infected host bots as DNS replies.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.

DHCP

- DHCP servers dynamically provide IP configuration information to clients.
- In the figure, a client broadcasts a DHCP discover message.
- The DHCP server responds with a unicast offer that includes addressing information the client can use.
- The client broadcasts a DHCP request to tell the server that the client accepts the offer.
- The server responds with a unicast acknowledgment accepting the request.



Normal DHCP Operation

DHCP Attacks

DHCP Spoofing Attack

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

A rogue server can provide a variety of misleading information such as:

- **Wrong default gateway -** Threat actor provides an invalid gateway, or the IP address of its host to create a MITM (Man In The Middle) attack.
- **Wrong DNS server -** Threat actor provides an incorrect DNS server address pointing the user to a malicious website.
- **Wrong IP address -** Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.

Exploring DNS Traffic

In this lab, you will complete the following objectives:

- Capture DNS Traffic
- Explore DNS Query Traffic
- Explore DNS Response Traffic

17.2 Enterprise Services

HTTP and HTTPS

- To investigate web-based attacks, security analysts must have a good understanding of how a standard web-based attack works.

Common stages of a typical web attack:

- The victim unknowingly visits a web page that has been compromised by malware.
- The compromised web page redirects the user to a site containing malicious code.
- The user visits this site with malicious code and their computer becomes infected.
- After identifying a vulnerable software package running on the victim's computer, the exploit kit contacts the exploit kit server to download the malicious code.
- After the victim's computer has been compromised, it connects to the malware server and downloads a payload.
- The final malware package is run on the victim's computer.

HTTP and HTTPS (Contd.)

- Server connection logs can often reveal information about the type of scan or attack.
- The different types of connection status codes are:
  - **Informational 1xx**
  - **Successful 2xx**
  - **Redirection 3xx**
  - **Client Error 4xx**
- To defend against web-based attacks:
  - Always update the OS and browsers with current patches and updates.
  - Use a web proxy to block malicious sites.
  - Use the best security practices from the Open Web Application Security Project (OWASP) when developing web applications.
  - Educate end users by showing them how to avoid web-based attacks.

Common HTTP Exploits

Malicious iFrames

- An iFrame is an HTML element that allows the browser to load another web page from another source.
- In iFrame attacks, the threat actors insert advertisements from other sources into the page.
- Threat actors compromise a webserver and modify web pages by adding HTML for the malicious iFrame.
- As the iFrame is running in the page, it can be used to deliver a malicious exploit. such as spam advertising, exploit kits, and other malware.

Steps to prevent or reduce malicious iFrames:

- Use a web proxy like to block malicious sites.
- Ensure web developers do not use iFrames.
- Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.
- Ensure the end user understands what an Iframe is.

Common HTTP Exploits (Contd.)

HTTP 302 Cushioning

- Threat actors use the 302 Found HTTP response status code to direct the user's web browser to a new location.
- The browser believes that the new location is the URL provided in the header. The browser is invited to request this new URL. This redirect function can be used multiple times until the browser finally lands on the page that contains the exploit.

Steps to prevent or reduce HTTP 302 cushioning attacks:

- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.
- Ensure the end user understands how the browser is redirected through a series of HTTP 302 redirections.

Common HTTP Exploits (Contd.)

Domain Shadowing

- When a threat actor create a domain shadowing attack, first they compromise a domain. Then they must create multiple subdomains of that domain to be used for the attacks using Hijacked domain registration logins.
- After these subdomains have been created, attackers can use them even if they are found out to be malicious domains. They can simply make more from the parent domain.

Steps to prevent or reduce Domain shadowing attacks:

- Secure all domain owner accounts.
- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to web sites that are known to be malicious.
- Make sure that domain owners validate their registration accounts and look for any subdomains that they have not authorized.

Email

- As the level of use of email rises, security becomes a greater priority.
- The way users access email today also increases the opportunity for the threat of malware to be introduced.

Examples of email threats:

- **Attachment-based attacks -** Threat actors embed malicious content in business files such as an email from the IT department.
- **Email spoofing -** Threat actors create email messages with a forged sender address that is meant to fool the recipient into providing money or sensitive information.
- **Spam email -** Threat actors send unsolicited email containing advertisements or malicious files.
- **Open mail relay server -** This is an SMTP server that allows anybody on the internet to send mail.

Web-Exposed Databases

- Web applications commonly connect to a relational database to access data.
- As relational databases often contain sensitive data, databases are a frequent target for attacks.

Code Injection

- The attacker's commands are executed through the web application and has the same permissions as the web application.
- This type of attack is used because often there is insufficient validation of input.

SQL Injection

- Threat actors use SQL injections to breach the relational database, create malicious SQL queries, and obtain sensitive data from the relational database.
- A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and sometimes, issue commands to the operating system.

Client-side Scripting

Cross-Site Scripting

- Cross-Site Scripting (XSS) is where web pages that are executed on the client-side, within their own web browser, are injected with malicious scripts.
- These scripts can be used by Visual Basic, JavaScript, and others to access a computer, collect sensitive information, or deploy more attacks and spread malware.
- The two main types of XSS are **Stored (persistent)** and **Reflected (non-persistent).**
- **Ways to prevent or reduce XSS attacks**:
  - Ensure that web application developers are aware of XSS vulnerabilities and how to avoid them.
  - Use an IPS implementation to detect and prevent malicious scripts.
  - Use a web proxy to block malicious sites.
  - Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.

Attacking a MySQL Database

In this lab, you will complete the following objective :

- View a PCAP file from a previous attack against a SQL database.

Reading Server Logs

In this lab, you will complete the following objectives:

- Reading Log Files with **cat**, **more**, and **less**
- Log Files and Syslog
- Log Files and **journalctl**

17.3 Attacking What We Do Summary

What Did I Learn in this Module?

- Any client can send an unsolicited ARP Reply called a “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network, creating an MiTM attack to redirect traffic.
- The Domain Name Service (DNS) protocol uses Resource Records (RR) to identify the type of DNS response.
- DNS open resolvers are vulnerable to multiple malicious activities, including DNS cache poisoning, in which falsified records are provided to the open resolver.
- In DNS amplification and reflection attacks, the benign nature of the DNS protocol is exploited to cause DoS/ DDoS attacks.
- In DNS resource utilization attacks, a DoS attack is launched against the DNS server itself.
- Threat actors use Fast Flux, in which malicious servers will rapidly change their IP address.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.

What Did I Learn in this Module?

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.
- The compromised web page redirects the user to a site that hosts malicious code which is known as a drive-by download.
- Cross-Site Scripting (XSS) attacks occur when browsers execute malicious scripts on the client and provide threat actors with access to sensitive information on the local host.
- The OWASP Top 10 Web Application Security Risks is designed to help organizations create secure web applications.


CISCO

Labs

Labs to do

- 14.1.11 Lab - Anatomy of Malware
- 14.2.9 Lab - Social Engineering
- 15.0.3 Class Activity - What's going on?
- 15.2.7 Packet Tracer - Loggin Network Activity (with attached file)
- 17.1.7 Lab - Exploring DNS Traffic
- 17.2.6 Lab - Attacking a MySQL Database
- 17.2.7 Lab - Reading Server Logs

Please prepare a lab report as a single PDF file that includes all the labs mentioned. Send the document to barthelemy.camia-temperton@esigelec.fr, with the subject line: "BRNO - NAME Surname - Lab Report".

The file should be named: "NAME_Surname_Labs_Report.pdf".

Ensure that your report follows the basic principles of a clear and well-structured document.

Appendices

Master of Technology

🌐 Website

https://en.esigelec.fr/master-program/

📧 Email

international@esigelec.fr

Our Master's programs are taught entirely in English. The curriculum design and the mandatory 4–6-month internship at the end of the program, enable students to gain work experience while studying. We pride ourselves on moulding graduates who have a head start on being industry-ready!

We offer two intakes:

- 24 months / 4 semesters (intake in September only)
- 18 months / 3 semesters (intake in February only)

Software Engineering and Digital Transformation

SEMESTER 1: 30 CREDITS / 354 HOURS

Course unit	Module	Duration (hours)	Weight	ECTS Credits
Computer Science 1	Introduction to Object Oriented Programming with Java	40	3	8
	Fundamentals of Data Communication and Networking	24	2	
	Fundamentals of Web-Centric Development	30	3	
Digital Electronics	Binary Logic & Digital Functions	30	3	9
	LabView	30	3	
	C Programming	30	3	
Communication & Language	Cross Cultural Awareness and Working in a Team	36	3	6
	French as a Foreign Language / English as a Foreign Language	60	3	
Specialized Courses for SEDT	Java Project	50	4	7
	Database Management Systems	24	3	
Total Credits				30

SEMESTER 2: 30 CREDITS / 340 HOURS

Course unit	Module	Duration (hours)	Weight	ECTS Credits
Computer Science 2	Enterprise Network	20	2	13
	Object Oriented Programming with Java EE	40	4	
	Development of Mobile Application	40	4	
	Intro to .NET Framework (C#)	24	3	
Business Intelligence	Analysis & Design with UML	32	2	12
	Big Data: Challenges & Opportunities	40	4	
	PL/SQL Programming for Databases	20	2	
	Artificial Intelligence: Principles & Techniques	30	2	
	Python for Data Analysis	20	2	
Communication & Language 2	Oral Communications & Presentation Skills	14	1	5
	French as a Foreign Language / English as a Foreign Language	60	4	
Total Credits				30

SEMESTER 3: 30 CREDITS / 336 HOURS

Course unit	Module	Duration (hours)	Weight	ECTS Credits
Information Systems	Cloud Computing	30	2	10
	Information Systems & Organizations	20	3	
	Information System Security	30	3	
	Web-centric Development & ASP.NET	20	2	
Business Management	Management Control & Business	32	3	7
	Marketing in a Technical Environment	22	3	
	Intellectual Property & Internet Protection Laws	12	1	
Project Development & Management	Project management	30	2	9
	R & D Project	80	7	
Foreign Language	French as a Foreign Language / English as a Foreign Language	60	4	4
Total Credits				30

Electronic Embedded Systems

SEMESTER 1: 30 CREDITS / 354 HOURS

Course unit	Module	Duration (hours)	Weight	ECTS Credits
Computer Science 1	Introduction to Object Oriented Programming with Java	40	3	8
	Fundamentals of Data Communication and Networking	24	2	
	Fundamentals of Web-Centric Development	30	3	
Digital Electronics	Binary Logic & Digital Functions	30	3	9
	LabView	30	3	
	C Programming	30	3	
Communication & Language	Cross Cultural Awareness and Working in a Team	36	3	6
	French as a Foreign Language / English as a Foreign Language	60	3	
Specialized Courses for EES	Bibliographical Study	12	1	7
	Digital Electronics Project	32	3	
	Fundamentals of Electronics	30	3	
Total Credits				30

SEMESTER 2: 30 CREDITS / 392 HOURS

Course unit	Module	Duration (hours)	Weight	ECTS Credits
Digital Systems	Microprocessors	60	4	8
	VHDL & Logic Synthesis	30	2	
	Communication Busses	30	2	
Embedded Operating Systems	Real Time Operating Systems	30	3	6
	Embedded Linux	30	3	
Embedded Software	Embedded C programming	30	2	6
	Analysis & Design with UML	32	2	
	Embedded Java	30	2	
Instrumentation	Smart Sensors	30	3	6
	Specific Instrumentation	30	3	
Communication & Language 2	French as a Foreign Language / English as a Foreign Language	60	4	4
Total Credits				30

SEMESTER 3: 30 CREDITS / 330 HOURS

Course unit	Module	Duration (hours)	Weight	ECTS Credits
Embedded Communication	IoT Architectures and Protocols	30	4	10
	Python Programming & Image Treatments	30	3	
	Android Programming	30	3	
Embedded Electronics	System on Chip	20	2	6
	DSP Processors	20	2	
	Safety Systems	20	2	
Communication & Language 3	Oral Communication & Presentation Skills	14	1	5
	French as a Foreign Language / English as a Foreign Language	60	4	
Project Development & Management	Project Management	30	2	9
	R&D Project	80	7	
Total Credits				30

Map