CCNA 3 v7.0 Curriculum: Module 3 – Network Security Concepts

itexamanswers.net/ccna-3-v7-0-curriculum-module-3-network-security-concepts.html

April 7, 2020

Contents

3.0. Introduction

3.0.1. Why should I take this module?

Welcome to Network Security Concepts!

Perhaps you've heard one of the hundreds of news stories about a data security breach within a large corporation or even a government. Was your credit card number exposed by a breach? Your private health information? Would you like to know how to prevent these data breaches? The field of network security is growing every day. This module provides a detailed landscape of the types of cybercrime and the many ways we have to fight back against cybercriminals. Let's get started!

3.0.2. What will I learn in this module?

Module Title: Network Security Concepts

Module Objective: Explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.

Topic	Topic Title
Current State of Cybersecurity	Describe the current state of cybersecurity and vectors of data loss.
Threat Actors	Describe tools used by threat actors to exploit networks.
Malware	Describe malware types.
Common Network Attacks	Describe common network attacks.
IP Vulnerabilities and Threats	Explain how IP vulnerabilities are exploited by threat actors.
TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities are exploited by threat actors.

Topic	Topic Title
IP Services	Explain how IP services are exploited by threat actors.
Network Security Best Practices	Describe best practices for protecting a network.
Cryptography	Describe common cryptographic processes used to protect data in transit.

3.0.3. Ethical Hacking Statement

In this module, learners may be exposed to tools and techniques in a “sandboxed”, virtual machine environment to demonstrate various types of cyber attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and local institution. If the learner is considering using attack tools for educational purposes, they should contact their instructor prior to any experimentation.

Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator’s motivations. It is the learner’s responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

3.1. Current State of Cybersecurity

3.1.1. Current State of Affairs

Cyber criminals now have the expertise and tools necessary to take down critical infrastructure and systems. Their tools and techniques continue to evolve.

Cyber criminals are taking malware to unprecedented levels of sophistication and impact. They are becoming more adept at using stealth and evasion techniques to hide their activity. Lastly, cyber criminals are exploiting undefended gaps in security.

Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety.

Maintaining a secure network ensures the safety of network users and protects commercial interests. Organizations need individuals who can recognize the speed and scale at which adversaries are amassing and refining their cyber weaponry. All users should be aware of security terms in the table.

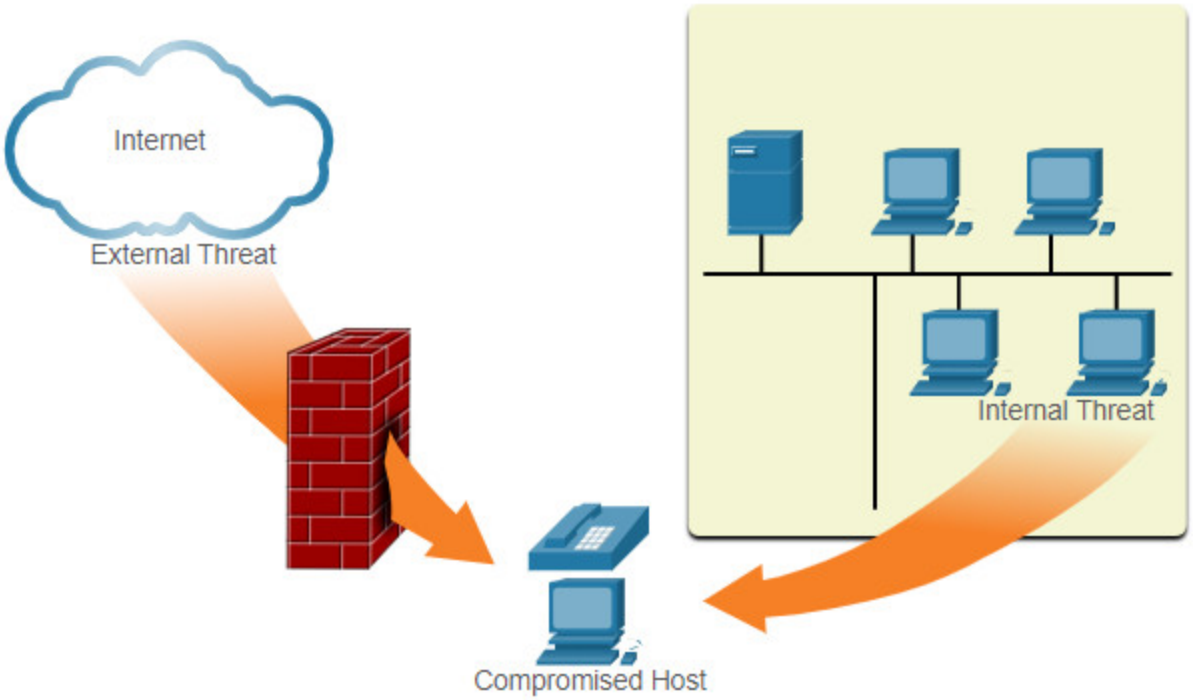
Security Terms	Description
Assets	An asset is anything of value to the organization. It includes people, equipment, resources, and data.
Vulnerability	A vulnerability is a weakness in a system, or its design, that could be exploited by a threat.
Threat	A threat is a potential danger to a company's assets, data, or network functionality.
Exploit	An exploit is a mechanism that takes advantage of a vulnerability.
Mitigation	Mitigation is the counter-measure that reduces the likelihood or severity of a potential threat or risk. Network security involves multiple mitigation techniques.
Risk	Risk is the likelihood of a threat to exploit the vulnerability of an asset, with the aim of negatively affecting an organization. Risk is measured using the probability of the occurrence of an event and its consequences.

Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack.

3.1.2. Vectors of Network Attacks

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.

External and Internal Threats



Note: A DoS attack occurs when a network device or application is incapacitated and no longer capable of supporting requests from legitimate users.

An internal user, such as an employee, can accidentally or intentionally:

- Steal and copy confidential data to removable media, email, messaging software, and other media.
- Compromise internal servers or network infrastructure devices.
- Disconnect a critical network connection and cause a network outage.
- Connect an infected USB drive into a corporate computer system.

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

Network security professionals must implement tools and apply techniques for mitigating both external and internal threats.

3.1.3. Data Loss

Data is likely to be an organization's most valuable asset. Organizational data can include research and development data, sales data, financial data, human resource and legal data, employee data, contractor data, and customer data.

Data loss or data exfiltration is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. The data loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action resulting in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Common data loss vectors are displayed in the table.

Data Loss Vectors	Description
Email/Social Networking	Intercepted email or IM messages could be captured and reveal confidential information.
Unencrypted Devices	If the data is not stored using an encryption algorithm, then the thief can retrieve valuable confidential data.
Cloud Storage Devices	Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
Removable Media	One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost.
Hard Copy	Confidential data should be shredded when no longer required.
Improper Access Control	Passwords or weak passwords which have been compromised can provide a threat actor with easy access to corporate data.

Network security professionals must protect the organization's data. Various Data Loss Prevention (DLP) controls must be implemented which combine strategic, operational and tactical measures.

3.2. Threat Actors

3.2.1. The Hacker

In the previous topic, you gained a high-level look at the current landscape of cybersecurity, including the types of threats and vulnerabilities that plague all network administrators and architects. In this topic, you will learn more details about particular types of threat actors.

Hacker is a common term used to describe a threat actor. As shown in the table, the terms white hat hacker, black hat hacker, and gray hat hacker are often used to describe a type of hacker.

Hacker Type	Description
White Hat Hackers	These are ethical hackers who use their programming skills for good, ethical, and legal purposes. White hat hackers may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be exploited.
Gray Hat Hackers	These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. Gray hat hackers may disclose a vulnerability to the affected organization after having compromised their network.
Black Hat Hackers	These are unethical criminals who compromise computer and network security for personal gain, or for malicious reasons, such as attacking networks.

Note: In this course, we will not use the term hacker outside of this module. We will use the term threat actor. The term threat actor includes hackers. But threat actor also includes any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack.

3.2.2. Evolution of Hackers

Hacking started in the 1960s with phone freaking, or phreaking, which refers to using audio frequencies to manipulate phone systems. At that time, telephone switches used various tones to indicate different functions. Early hackers realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.

In the mid-1980s, computer dial-up modems were used to connect computers to networks. Hackers wrote “war dialing” programs which dialed each telephone number in a given area in search of computers. When a computer was found, password-cracking programs were used to gain access.

The table displays modern hacking terms and a brief description of each.

Hacking Term	Description
Script Kiddies	These are teenagers or inexperienced hackers running existing scripts, tools, and exploits, to cause harm, but typically not for profit.

Hacking Term	Description
Vulnerability Broker	These are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
Hacktivists	These are gray hat hackers who publicly protest organizations or governments by posting articles, videos, leaking sensitive information, and performing network attacks.
Cyber criminals	These are black hat hackers who are either self-employed or working for large cybercrime organizations.
State-Sponsored	These are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

3.2.3. Cyber Criminals

It is estimated that cyber criminals steal billions of dollars from consumers and businesses. Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more. They also buy and sell the private information and intellectual property they steal. Cyber criminals target small businesses and consumers, as well as large enterprises and entire industries.

3.2.4. Hacktivists

Two examples of hacktivist groups are Anonymous and the Syrian Electronic Army. Although most hacktivist groups are not well organized, they can cause significant problems for governments and businesses. Hacktivists tend to rely on fairly basic, freely available tools.

3.2.5. State-Sponsored Hackers

State-sponsored hackers create advanced, customized attack code, often using previously undiscovered software vulnerabilities called zero-day vulnerabilities. An example of a state-sponsored attack involves the Stuxnet malware that was created to damage Iran's nuclear enrichment capabilities.

3.3. Threat Actor Tools

3.3.1 Video – Threat Actor Tools

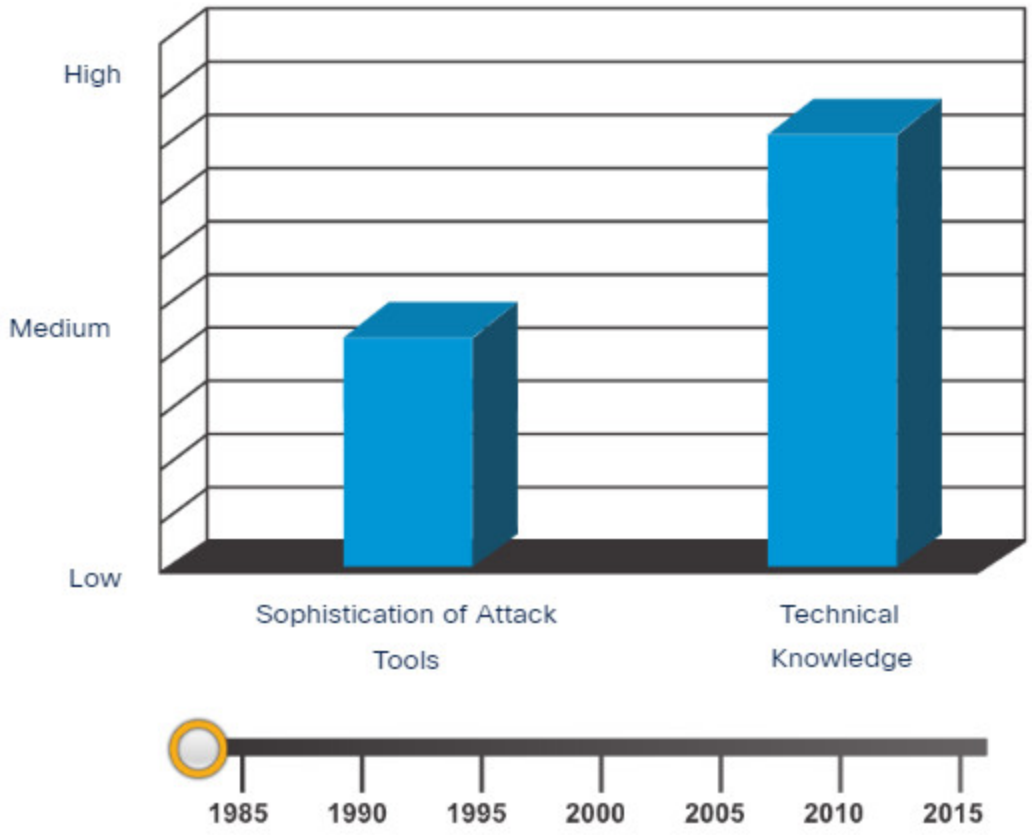
3.3.2. Introduction to Attack Tools

To exploit a 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.

shows a bar with sophistication of attack on the left and a bar with technical knowledge on the right. In 1985, attacks were not very sophisticated and required a lot of technical knowledge. As time passed, the sophistication of attack grew and the required technical knowledge diminished.

Sophistication of Attack Tools vs. Technical Knowledge



3.3.3. Evolution of Security Tools

Ethical hacking involves many different types of tools used to test the network and keep its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. It is unfortunate that many of these tools can be used by black hat hackers for exploitation.

Black hat hackers have also created many hacking tools. These tools are created explicitly for nefarious reasons. White hat hackers must also know how to use these tools when performing network penetration tests.

The table highlights categories of common penetration testing tools. Notice how some tools are used by white hats and black hats. Keep in mind that the list is not exhaustive as new tools are always being developed.

Penetration Testing Tool	Description
Password Crackers	Password cracking tools are often referred to as password recovery tools and can be used to crack or recover a password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
Wireless Hacking Tools	Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.
Network Scanning and Hacking Tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Packet Crafting Tools	These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
Packet Sniffers	These tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.
Rootkit Detectors	This is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.
Fuzzers to Search Vulnerabilities	Fuzzers are tools used by threat actors to discover a computer's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
Forensic Tools	These tools are used by white hat hackers to sniff out any trace of evidence existing in a computer. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.

Penetration Testing Tool	Description
Debuggers	These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.
Hacking Operating Systems	These are specially designed operating systems preloaded with tools optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, Knoppix, BackBox Linux.
Encryption Tools	Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, and Stunnel.
Vulnerability Exploitation Tools	These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.
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. Examples of tools include Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.

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

3.3.4. Attack Types

Threat actors can use the previously mentioned attack tools, or a combination of tools, to create attacks. The table displays common types of attacks. However, the list of attacks is not exhaustive as new attack vulnerabilities are constantly being discovered.

Attack Type	Description
Eavesdropping Attack	This is when a threat actor captures and “listens” to network traffic. This attack is also referred to as sniffing or snooping.
Data Modification Attack	If threat actors have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.
IP Address Spoofing Attack	A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

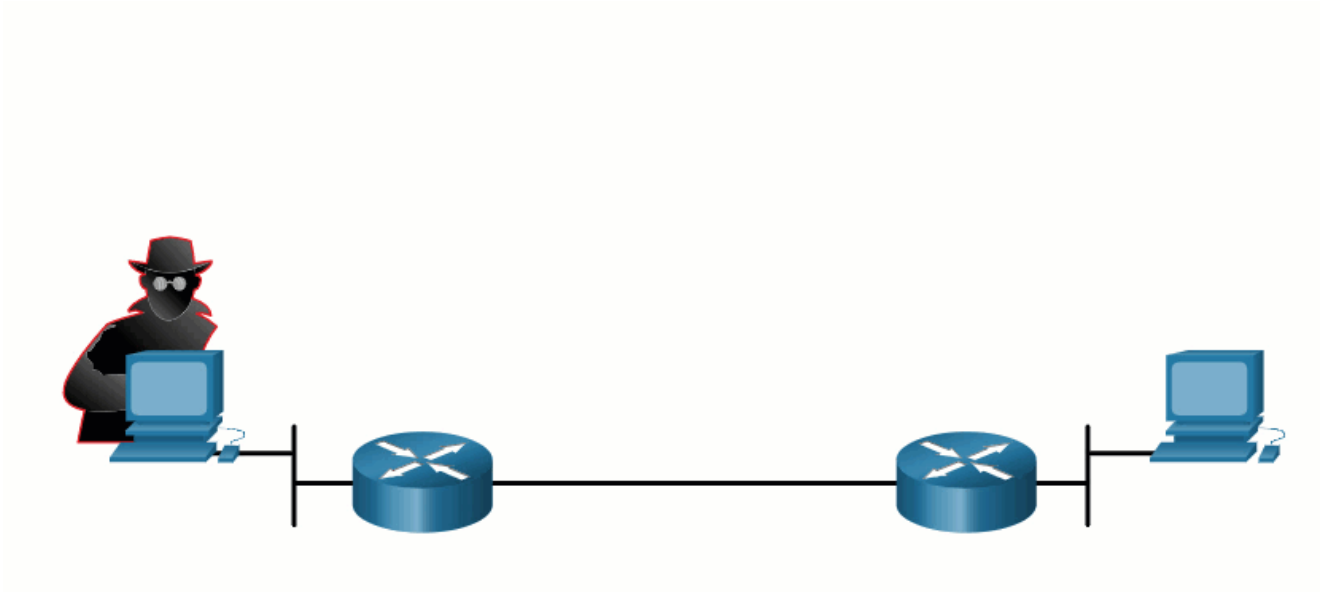
Attack Type	Description
Password-Based Attacks	If threat actors discover a valid user account, the threat actors have the same rights as the real user. Threat actors could use that valid account to obtain lists of other users, network information, change server and network configurations, and modify, reroute, or delete data.
Denial of Service Attack	A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.
Man-in-the-Middle Attack	This attack occurs when threat actors have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.
Compromised-Key Attack	If a threat actor obtains a secret key, that key is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of the attack.
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.

3.4. Malware

3.4.1. Overview of Malware

Now that you know about the tools that hacker use, this topic introduces you to different types of malware that hackers use to gain access to end devices.

End devices are particularly prone to malware attacks. It is important to know about malware because threat actors rely on users to install malware to help exploit the security gaps.



3.4.2. Viruses and Trojan Horses

The first and most common type of computer malware is a virus. Viruses require human action to propagate and infect other computers. For example, a virus can infect a computer when a victim opens an email attachment, opens a file on a USB drive, or downloads a file.

The virus hides by attaching itself to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer.

Viruses can:

- Alter, corrupt, delete files, or erase entire drives.
- Cause computer booting issues, and corrupt applications.
- Capture and send sensitive information to threat actors.
- Access and use email accounts to spread.
- Lay dormant until summoned by the threat actor.

Modern viruses are developed for specific intent such as those listed in the table.

Types of Viruses	Description
Boot sector virus	Virus attacks the boot sector, file partition table, or file system.
Firmware virus	Virus attacks the device firmware.
Macro virus	Virus uses the MS Office or other applications macro feature maliciously.
Program virus	Virus inserts itself in another executable program.

Types of Viruses	Description
Script virus	Virus attacks the OS interpreter which is used to execute scripts.

Threat actors use Trojan horses to compromise hosts. A Trojan horse is a program that looks useful but also carries malicious code. Trojan horses are often provided with free online programs such as computer games. Unsuspecting users download and install the game, along with the Trojan horse.

There are several types of Trojan horses as described in the table.

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

Viruses and Trojan horses are only two types of malware that threat actors use. There are many other types of malware that have been designed for specific purposes.

3.4.3. Other Types of Malware

The table shows details about many different types of malware.

Malware	Description

Malware	Description
Adware	• Adware is usually distributed by downloading online software. • Adware can display unsolicited advertising using pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website. • Pop-up windows may be difficult to control as new windows can pop-up faster than the user can close them.
Ransomware	• Ransomware typically denies a user access to their files by encrypting the files and then displaying a message demanding a ransom for the decryption key. • Users without up-to-date backups must pay the ransom to decrypt their files. • Payment is usually made using wire transfer or crypto currencies such as Bitcoin.
Rootkit	• Rootkits are used by threat actors to gain administrator account-level access to a computer. • They are very difficult to detect because they can alter firewall, antivirus protection, system files, and even OS commands to conceal their presence. • They can provide a backdoor to threat actors giving them access to the PC, and allowing them to upload files, and install new software to be used in a DDoS attack. • Special rootkit removal tools must be used to remove them, or a complete OS re-install may be required.
Spyware	• Similar to adware, but used to gather information about the user and send to threat actors without the user's consent. • Spyware can be a low threat, gathering browsing data, or it can be a high threat capturing personal and financial information.
Worm	• A worm is a self-replicating program that propagates automatically without user actions by exploiting vulnerabilities in legitimate software. • It uses the network to search for other victims with the same vulnerability. • The intent of a worm is usually to slow or disrupt network operations.

3.5. Common Network Attacks

3.5.1. Overview of Network Attacks

As you have learned, there are many types of malware that hackers can use. But these are not the only ways that they can attack a network, or even an organization.

When malware is delivered and installed, the payload can be used to cause a variety of network related attacks.

To mitigate attacks, it is useful to underst

and the types of attacks. By categorizing network attacks, it is possible to address types of attacks ratherthan individual attacks.

Networks are susceptible to the following types of attacks:

- Reconnaissance Attacks
- Access Attacks
- DoS Attacks

3.5.2 Video – Reconnaissance Attacks

Click Play in the figure to view a video about reconnaissance attacks.

3.5.3. Reconnaissance Attacks

Reconnaissance is information gathering. It is analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something. What the thief is actually doing is looking for vulnerable homes to break into, such as unoccupied residences, residences with easy-to-open doors or windows, and those residences without security systems or security cameras.

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.

Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table.

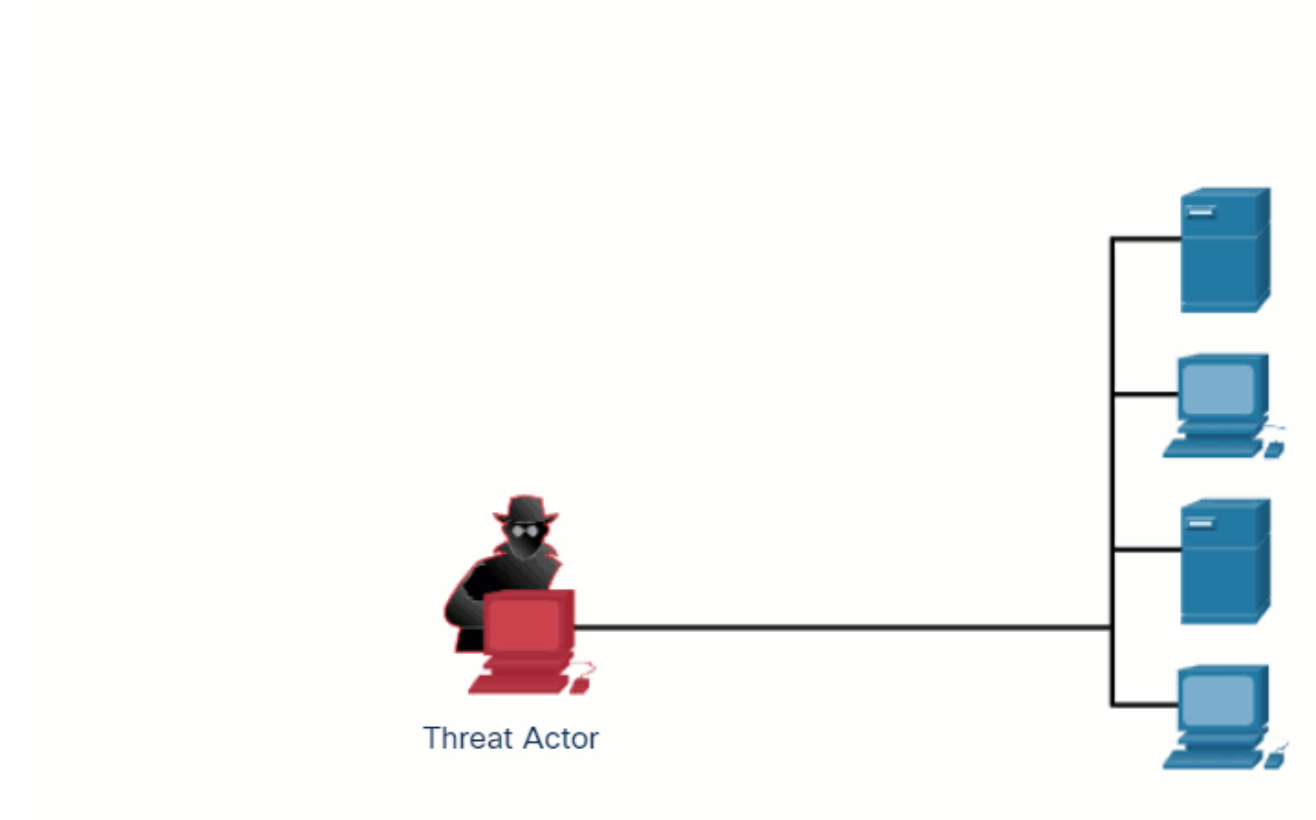
Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.

Technique	Description
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.

Click each button to view the progress of a reconnaissance attack from information query, to ping sweep, to port scan.

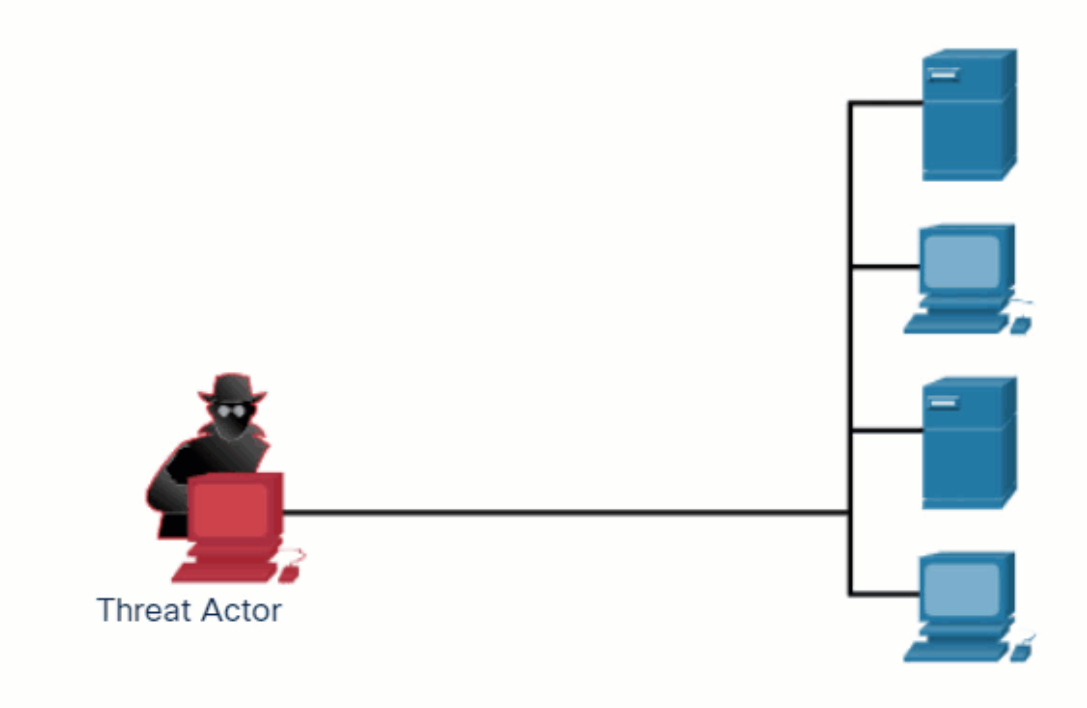
Internet Information Queries

Click Play in the figure to view an animation of a threat actor using the whois command to find information about a target.



Performing Ping Sweeps

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.



3.5.4 Video – Access and Social Engineering Attacks

Click Play in the figure to view a video about access and social engineering attacks.

3.5.5. Access Attacks

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. The purpose of these types of attacks is to gain entry to web accounts, confidential databases, and other sensitive information.

Threat actors use access attacks on network devices and computers to retrieve data, gain access, or to escalate access privileges to administrator status.

Password Attacks

In a password attack, the threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.

Spoofing Attacks

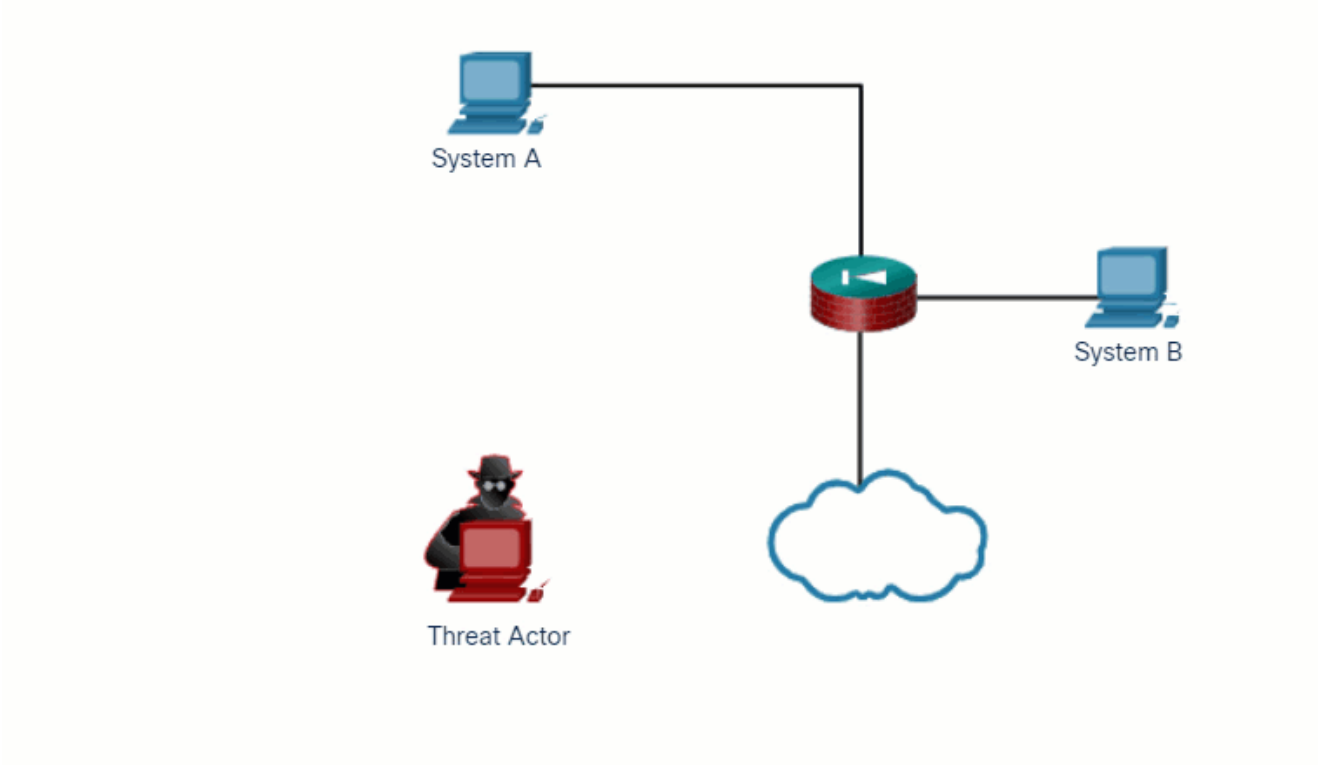
In spoofing attacks, the threat actor device attempts to pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing. These spoofing attacks will be discussed in more detail later in this module

Other Access attacks include:

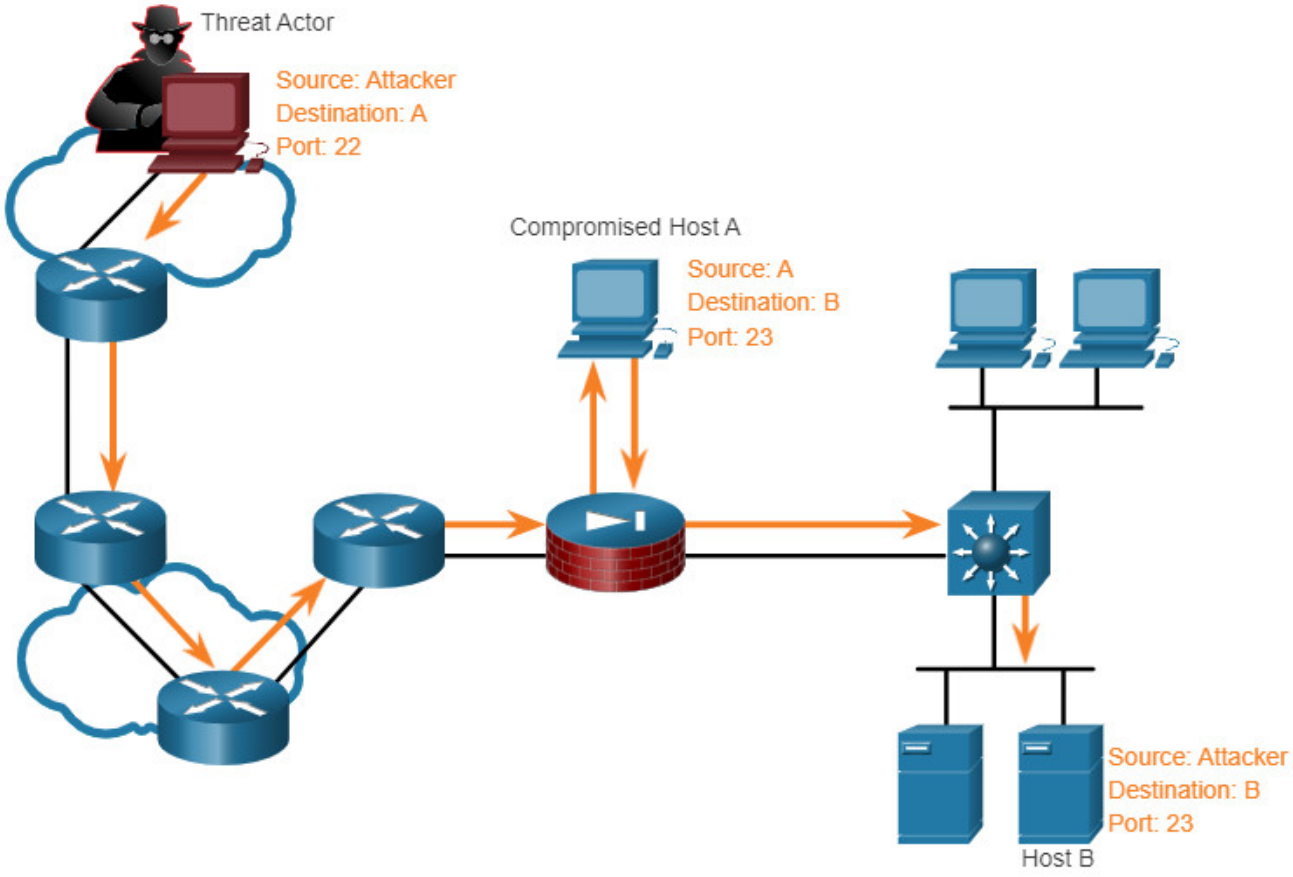
- Trust exploitations
- Port redirections
- Man-in-the-middle attacks
- Buffer overflow attacks

Click each button to view an illustration and explanation of these access attacks.

Trust Exploitation Example
In a trust exploitation attack, a threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target. Click Play in the figure to view an example of trust exploitation.



Port Redirection Example
In a port redirection attack, a threat actor uses a compromised system as a base for attacks against other targets. The example in the figure shows a threat actor using SSH (port 22) to connect to a compromised Host A. Host A is trusted by Host B and, therefore, the threat actor can use Telnet (port 23) to access it.



3.5.6. Social Engineering Attacks

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

Social engineers often rely on people's willingness to be helpful. They also prey on people's weaknesses. For example, a threat actor could call an authorized employee with an urgent problem that requires immediate network access. The threat actor could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

Information about social engineering techniques is shown in the 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.

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

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

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.

The figure shows recommended practices that should be followed by all users.

Recommended Social Engineering Protection Practices

3.5.7. Lab – Social Engineering

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

3.5.7 Lab – Social Engineering

3.5.8 Video – Denial of Service Attacks

Click Play in the figure to view a video about denial of service attacks.

3.5.9. DoS and DDoS Attacks

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

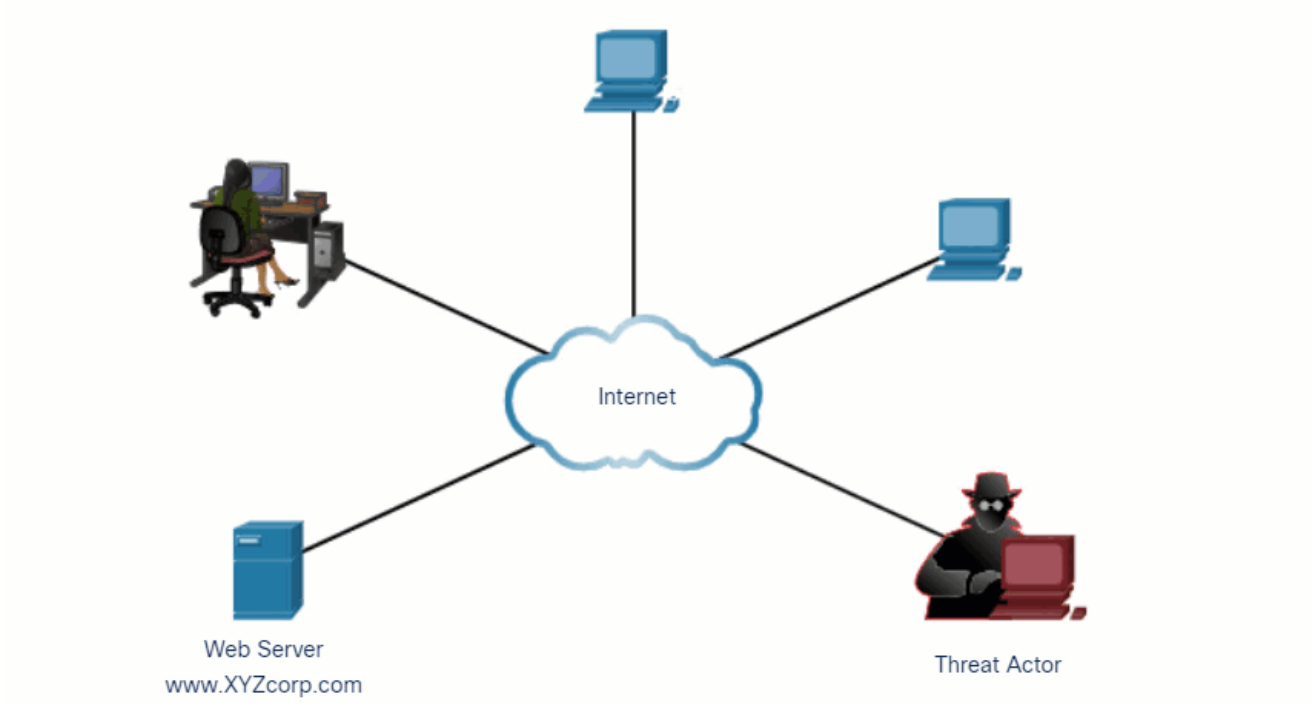
- **Overwhelming Quantity of Traffic** – The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
- **Maliciously Formatted Packets** – The threat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

Click each button for an illustration and explanation of DoS and DDoS attacks.

- DoS Attack
- DDoS Attack

DoS Attack
DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.

Click Play in the figure to view the animation of a DoS attack.



3.6. IP Vulnerabilities and Threats

3.6.1 Video – Common IP and ICMP Attacks

There are even more types of attacks than the ones discussed in the previous topics. Some specifically target IP vulnerabilities, as you will learn in this topic.

Click Play in the figure to view a video about common IP and ICMP attacks.

3.6.2. IPv4 and IPv6

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

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

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

3.6.3. ICMP Attacks

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

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

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

Common ICMP messages of interest to threat actors are listed in the table.

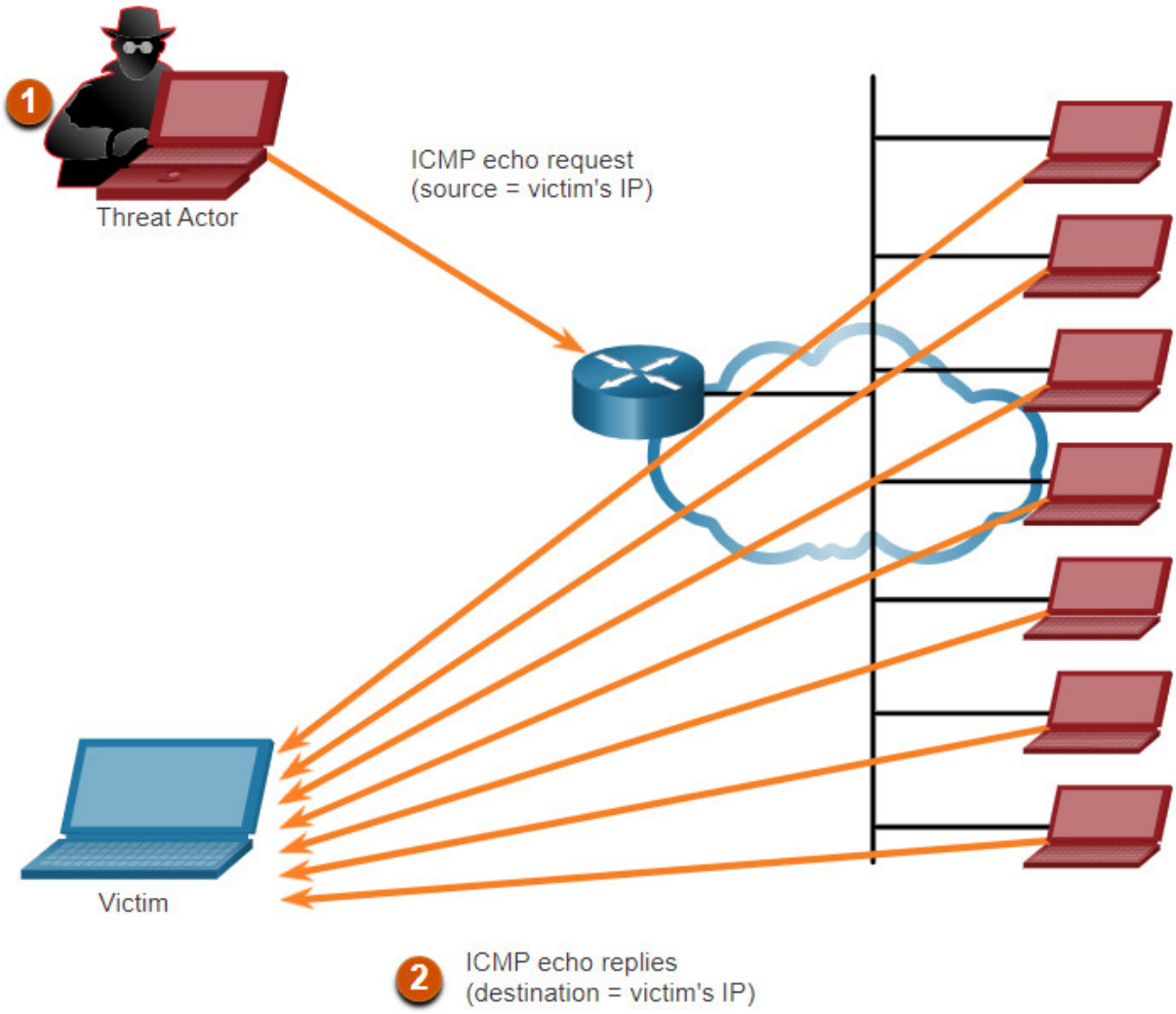
ICMP Messages used by Hackers	Description
ICMP echo request and echo reply	This is used to perform host verification and DoS attacks.
ICMP unreachable	This is used to perform network reconnaissance and scanning attacks.
ICMP mask reply	This is used to map an internal IP network.
ICMP redirects	This is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

3.6.4 Video – Amplification, Reflection, and Spoofing Attacks

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

3.6.5. Amplification and Reflection Attacks

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



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

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.

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

3.6.6. Address Spoofing Attacks

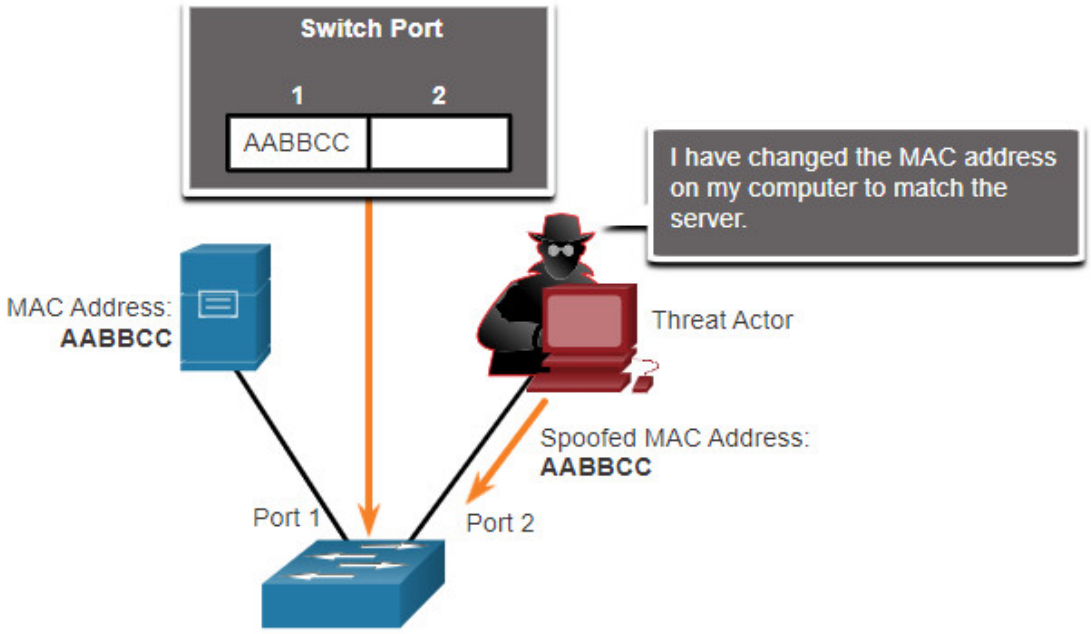
IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations.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

Spoofing attacks can be non-blind or blind:

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

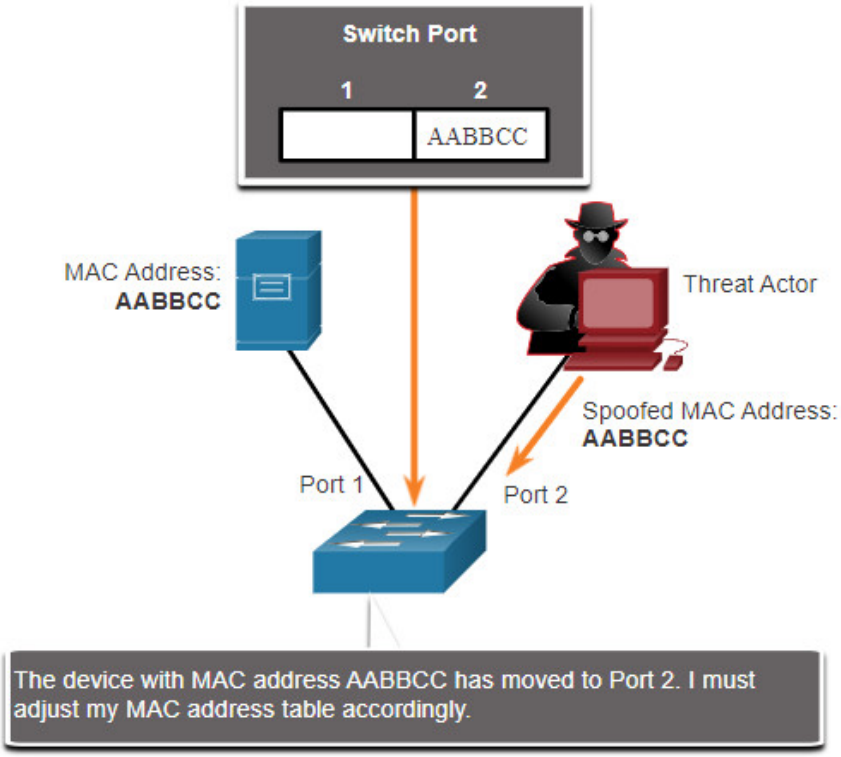
MAC address spoofing attacks are used when threat actors have access to the internal network. Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure. The attacking host then sends a frame throughout the network with the newly-configured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

Threat Actor Spoofs a Server's MAC Address



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

Switch Updates CAM Table with Spoofed Address



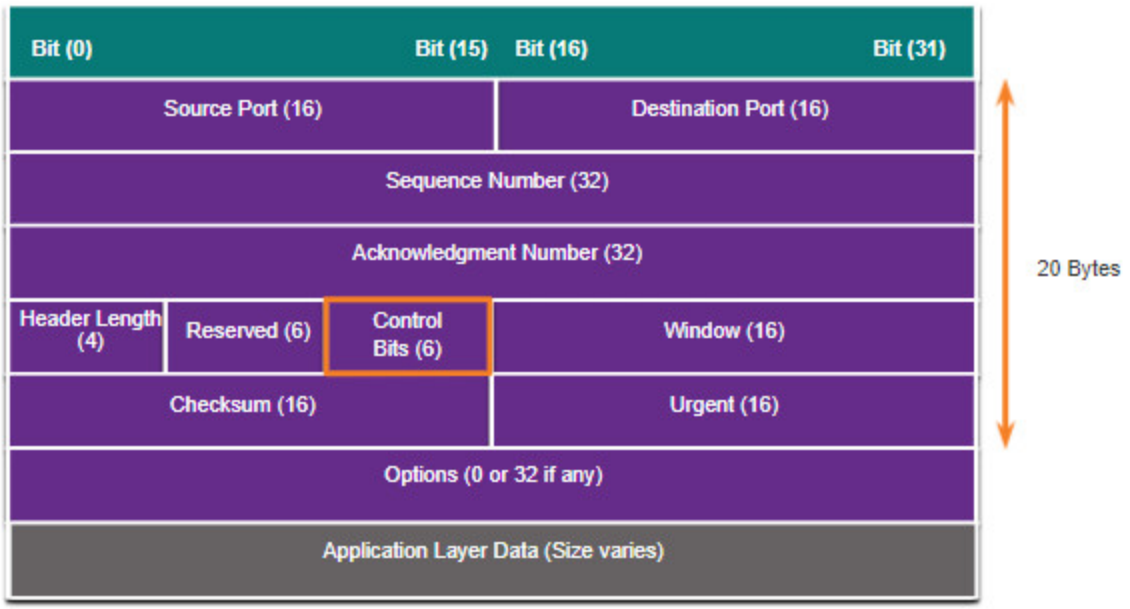
Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MITM condition.

3.7. TCP and UDP Vulnerabilities

3.7.1. TCP Segment Header

While some attacks target IP, this topic discusses attacks that target TCP and UDP.

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:

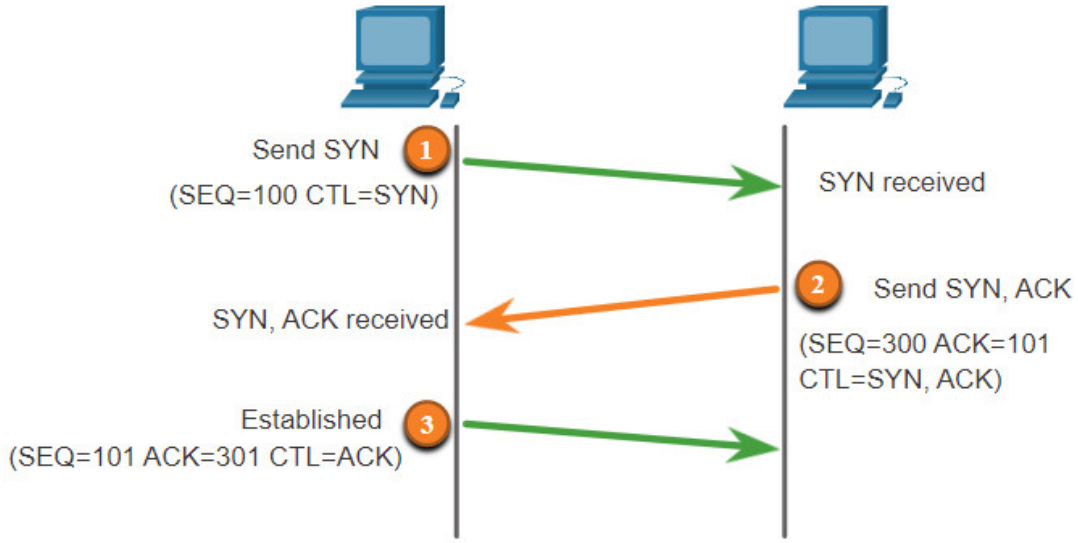
- **URG** – Urgent pointer field significant
- **ACK** – Acknowledgment field significant
- **PSH** – Push function
- **RST**– Reset the connection
- **SYN** – Synchronize sequence numbers
- **FIN** – No more data from sender

3.7.2. 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, as shown in the figure. If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.

TCP Three-Way Handshake



A TCP connection is established in three steps:

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

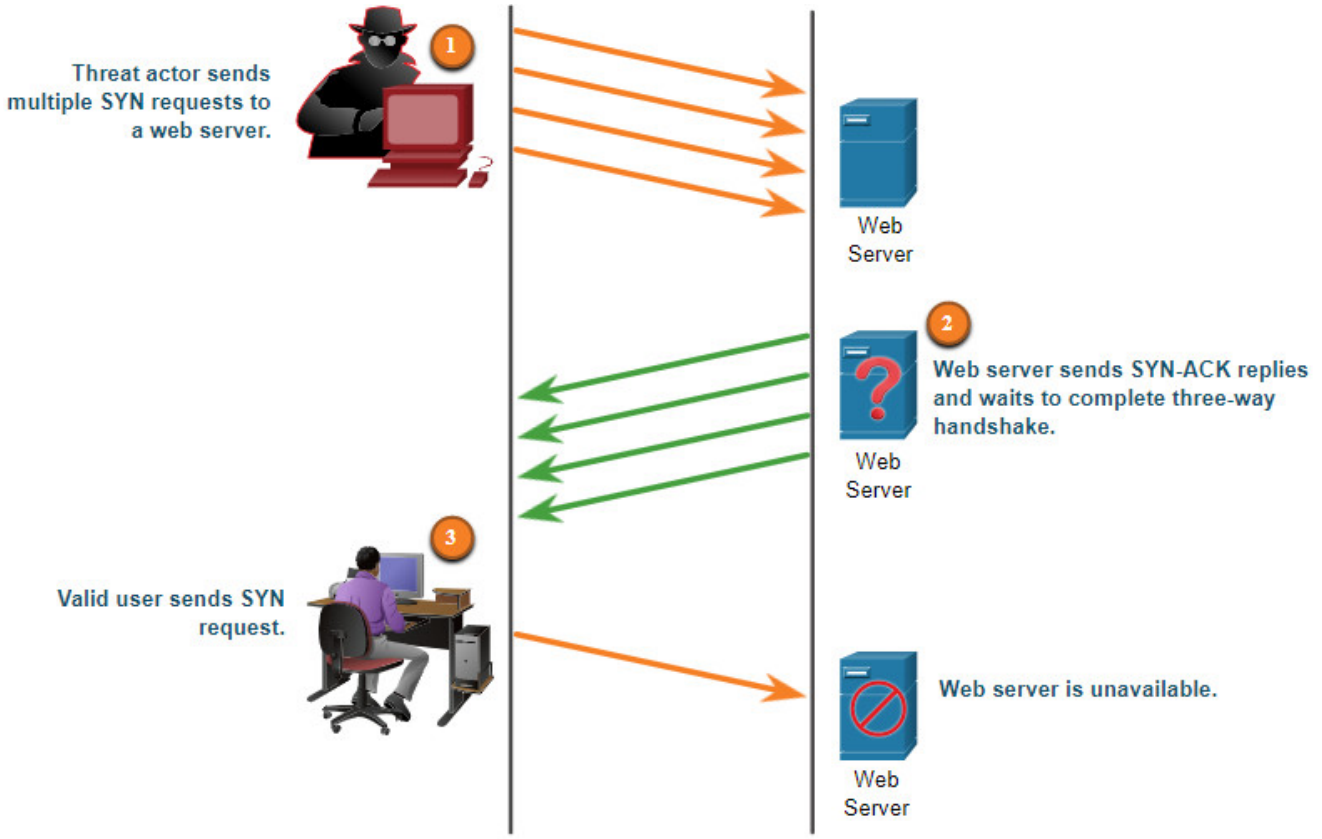
3.7.3. TCP Attacks

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 device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections, and TCP services are denied to legitimate users.

TCP SYN Flood Attack

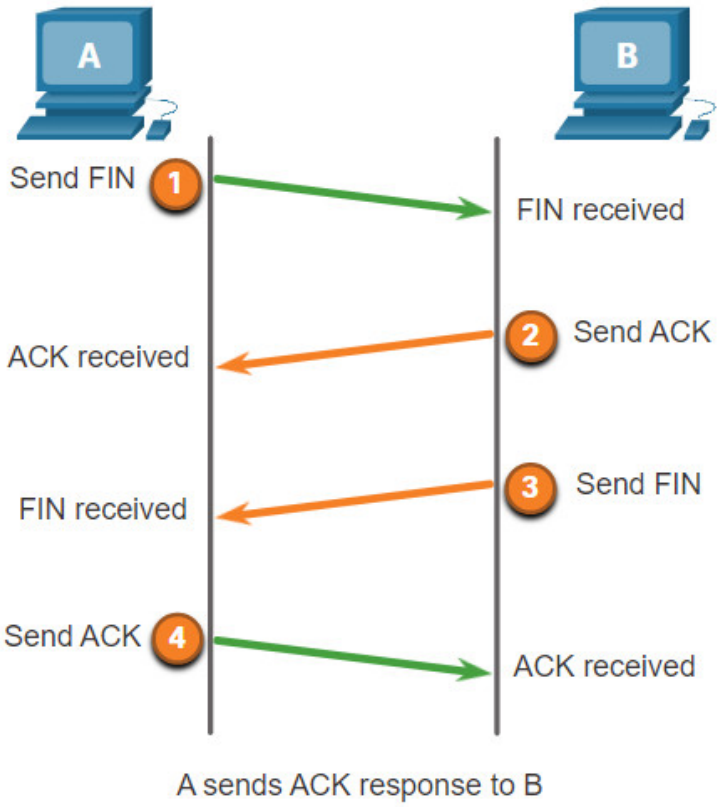


1. The threat actor sends multiple SYN requests to a webserver.
2. The web server replies with SYN-ACKs for each SYN request and waits to complete the three-way handshake. The threat actor does not respond to the SYN-ACKs.
3. A valid user cannot access the web server because the web server has too many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

TCP Reset Attack

A TCP reset attack can be used to terminate TCP communications between two hosts. The figure displays how TCP uses a four-way exchange to close the TCP connection using a pair of FIN and ACK segments from each TCP endpoint. A TCP connection terminates when it receives an RST bit. This is an abrupt way to tear down the TCP connection and inform the receiving host to immediately stop using the TCP connection. 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 Connection



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

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

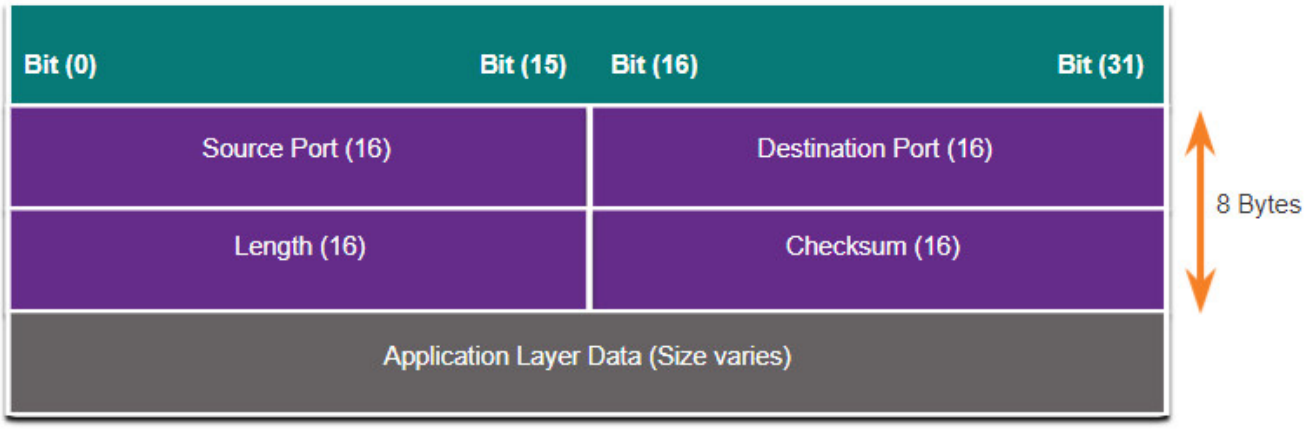
TCP Session Hijacking

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

3.7.4. UDP Segment Header and Operation

UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol. It has much lower overhead than TCP because it is not connection-oriented and

does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability. The UDP segment structure, shown in the figure, is much smaller than TCP's segment structure.



Although UPD is normally called unreliable, in contrast to TCP's reliability, this does not mean that applications that use UDP are always unreliable, nor does it mean that UDP is an inferior protocol. 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. For example, using TCP for DHCP would introduce unnecessary network traffic. If no response is received, the device resends the request.

3.7.5. UDP Attacks

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

UDP Flood Attacks

You are more likely to see a UDP flood attack. In a UDP flood attack, all the resources on a network are consumed. The threat actor must use a tool like 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. Because there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

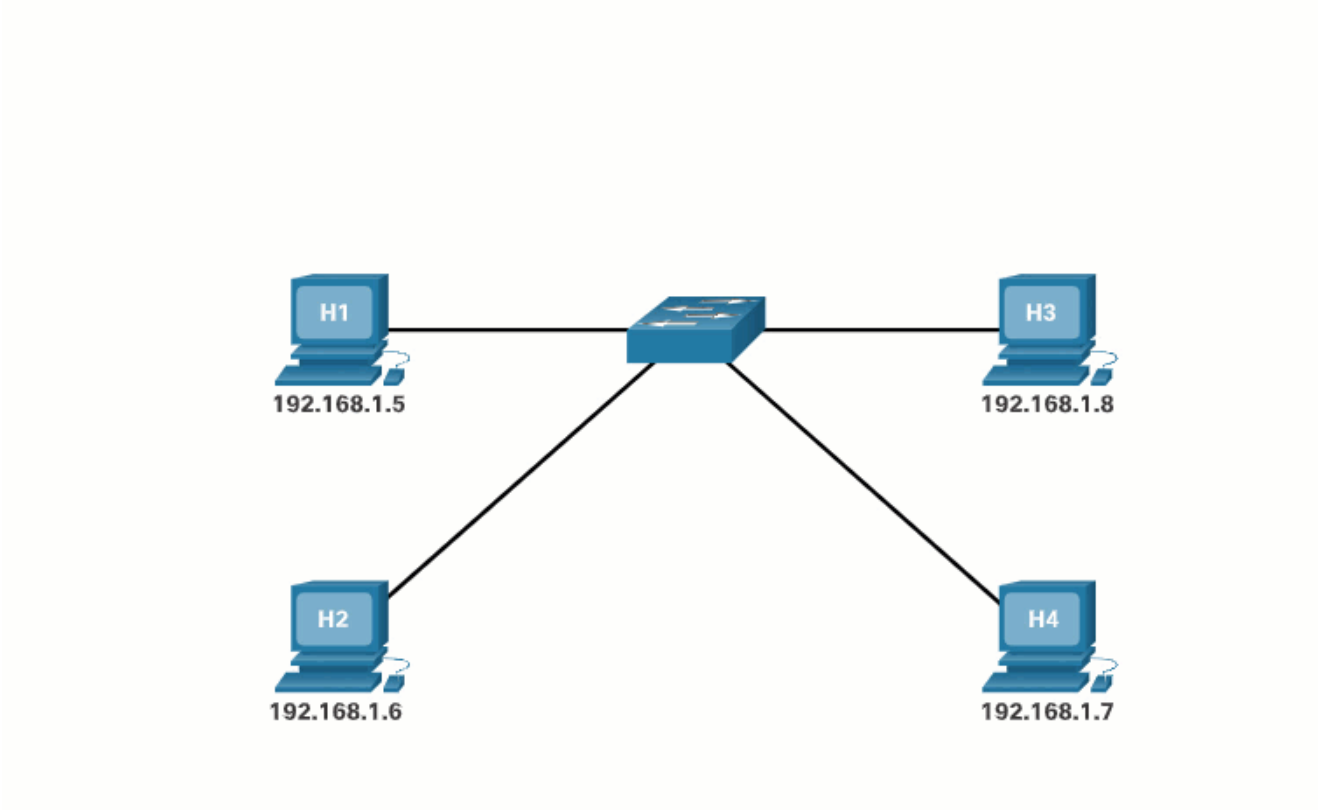
3.8. IP Services

3.8.1. ARP Vulnerabilities

Earlier in this module you learned about vulnerabilities with IP, TCP and UDP. The TCP/IP protocol suite was never built for security. Therefore, the services that IP uses for addressing functions such as ARP, DNS, and DHCP, are also not secure, as you will learn in this topic.

Hosts broadcast an ARP Request to other hosts on the segment to determine the MAC address of a host with a particular IP address. All hosts on the subnet receive and process the ARP Request. The host with the matching IP address in the ARP Request sends an ARP Reply.

The ARP Process



Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” This is often done when a device first boots up to inform all other devices on the local network of the new device’s MAC address. When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.

This feature of ARP also means that any host can claim to be the owner of any IP or MAC. A threat actor can poison the ARP cache of devices on the local network, creating an MITM attack to redirect traffic. The goal is to target a victim host, and have it change its default

gateway to the threat actor's device. This positions the threat actor in between the victim and all other systems outside of the local subnet.

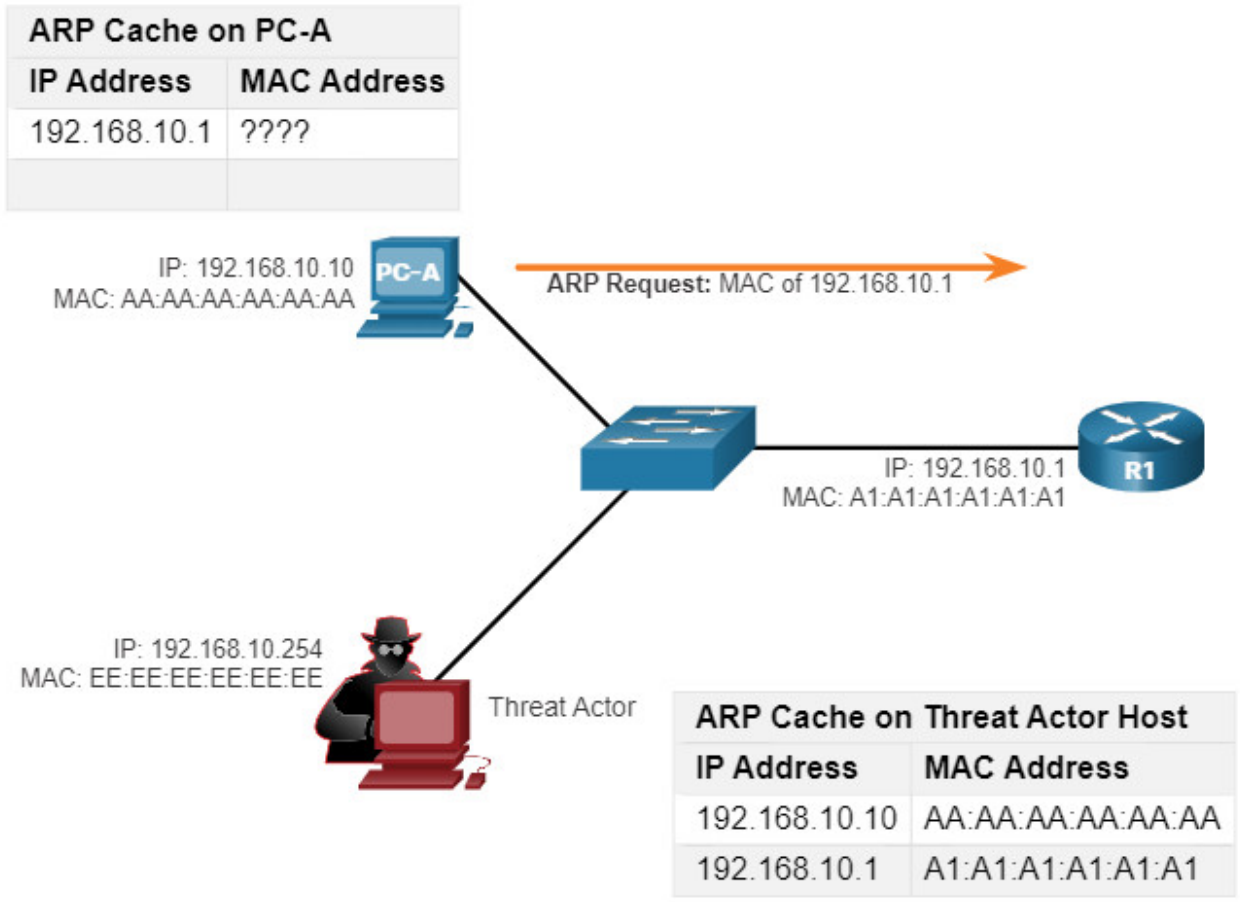
3.8.2. ARP Cache Poisoning

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

Click each button for an illustration and an explanation of the ARP cache poisoning process.

- ARP Request
- ARP Reply
- Spoofed Gratuitous ARP Replies

ARP Request
The figure shows how ARP cache poisoning works. PC-A requires the MAC address of its default gateway (R1); therefore, it sends an ARP Request for the MAC address of 192.168.10.1.



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

3.8.3 Video – ARP Spoofing

Click Play in the figure to view a video about ARP Spoofing.

3.8.4. DNS Attacks

The Domain Name Service (DNS) protocol defines an automated service that matches resource names, such as www.cisco.com, with the required numeric network address, such as the IPv4 or IPv6 address. It includes the format for queries, responses, and data and uses resource records (RR) to identify the type of DNS response.

Securing DNS is often overlooked. However, it is crucial to the operation of a network and should be secured accordingly.

DNS attacks include the following:

- DNS open resolver attacks
- DNS stealth attacks
- DNS domain shadowing attacks
- DNS tunneling attacks

DNS Open Resolver Attacks

Many organizations use the services of publicly open DNS servers such as GoogleDNS (8.8.8.8) to provide responses to queries. This type of DNS server is called an open resolver. A DNS open resolver answers queries from clients outside of 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 cache poisoning attacks can all be used to inform the DNS resolver to use a malicious name server that is providing RR information for malicious activities.
DNS amplification and reflection attacks	Threat actors use DoS or DDoS attacks on DNS open resolvers to increase the volume of attacks and to hide the true source of an attack. Threat actors send DNS messages to the open resolvers using the IP address of a target host. These attacks are possible because the open resolver will respond to queries from anyone asking a question.
DNS resource utilization attacks	A DoS attack that consumes the resources of the DNS open resolvers. This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver. The impact of this DoS attack may require the DNS open resolver to be rebooted or services to be stopped and restarted.

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 behind a quickly-changing network of compromised DNS hosts. The DNS IP addresses are continuously changed within minutes. Botnets often employ Fast Flux techniques to effectively hide malicious servers from being detected.
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 Domain Shadowing Attacks

Domain shadowing involves the threat actor gathering domain account credentials in order to silently create multiple sub-domains to be used during the attacks. These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

3.8.5. DNS Tunneling

Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions when a threat actor wishes to communicate with bots inside a protected network, or exfiltrate data from the organization, such as a password database. When the threat actor uses DNS tunneling, the different types of DNS records are altered. This is how DNS tunneling works for CnC commands sent to a botnet:

1. The command data is split into multiple encoded chunks.
2. Each chunk is placed into a lower level domain name label of the DNS query.
3. Because there is no response from the local or networked DNS for the query, the request is sent to the ISP's recursive DNS servers.
4. The recursive DNS service will forward the query to the threat actor's authoritative name server.
5. The process is repeated until all the queries containing the chunks of are sent.
6. When the threat actor's authoritative name server receives the DNS queries from the infected devices, it sends responses for each DNS query, which contain the encapsulated, encoded CnC commands.

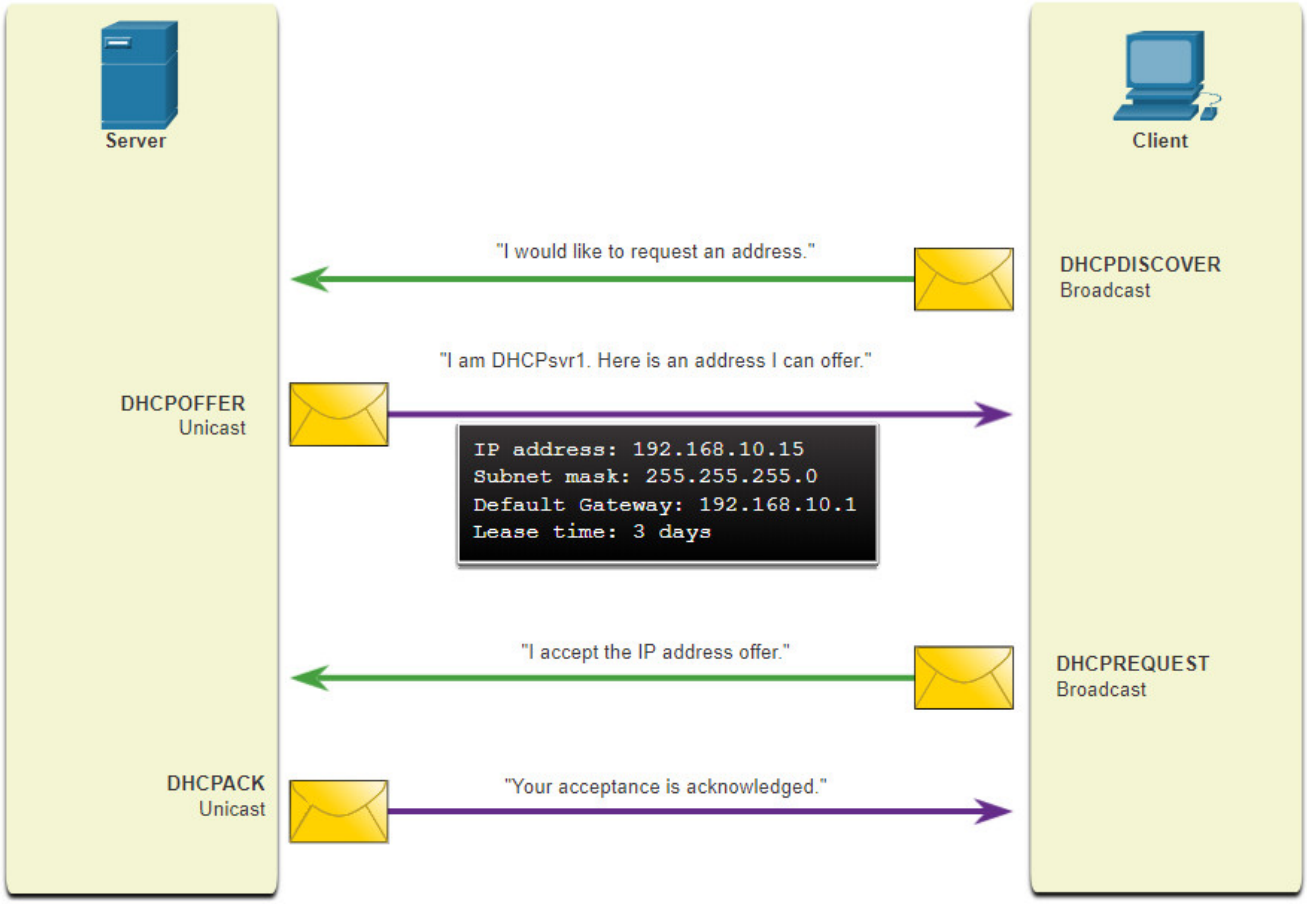
7. The malware on the compromised host recombines the chunks and executes the commands hidden within the DNS record.

To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic. Pay close attention to DNS queries that are longer than average, or those that have a suspicious domain name. DNS solutions, like Cisco OpenDNS, block much of the DNS tunneling traffic by identifying suspicious domains.

3.8.6. DHCP

DHCP servers dynamically provide IP configuration information to clients. The figure shows the typical sequence of a DHCP message exchange between client and server.

Normal DHCP Operation



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.

3.8.7. 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:

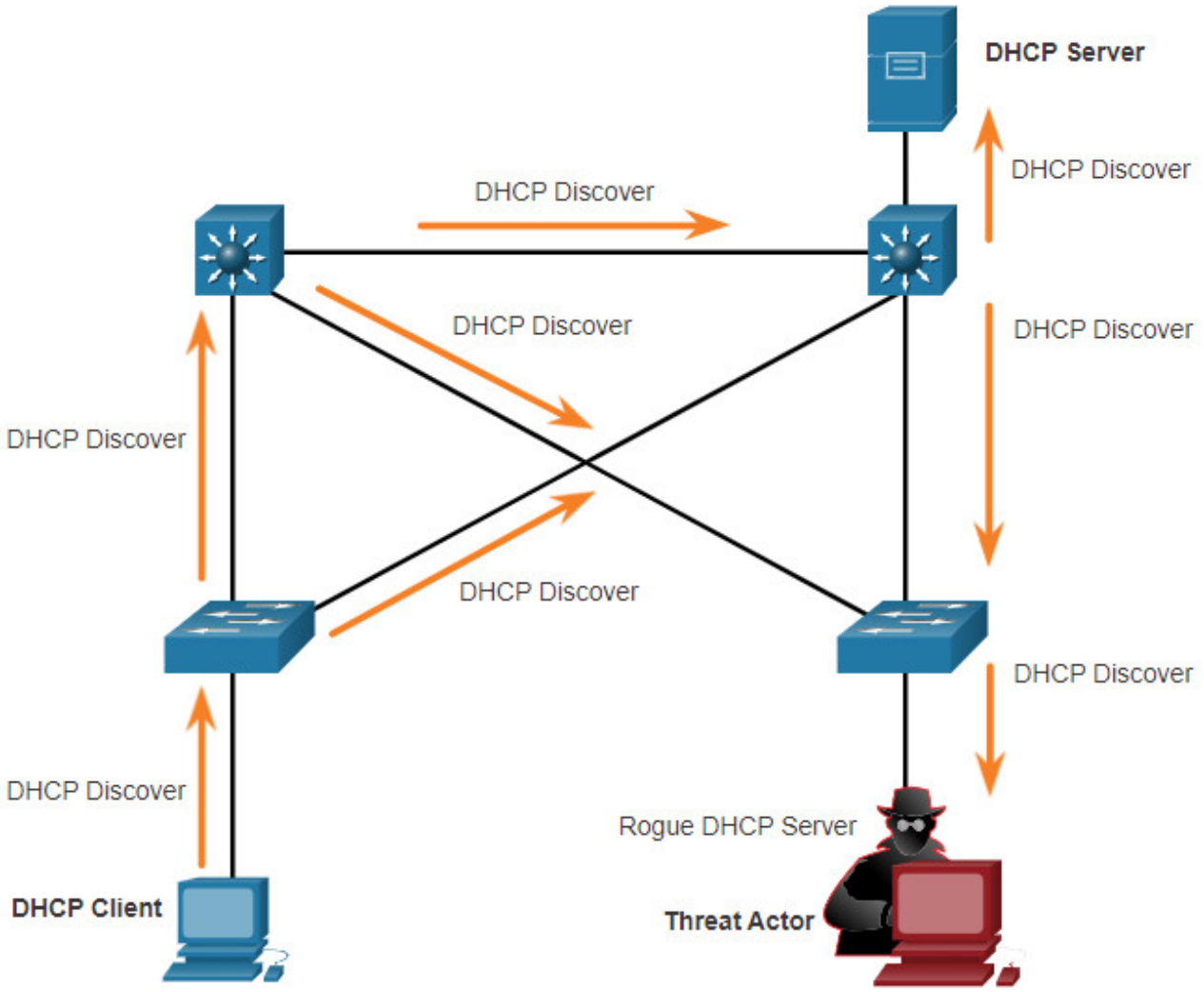
- **Wrong default gateway** – Threat actor provides an invalid gateway, or the IP address of its host to create a MITM attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
- **Wrong DNS server** – Threat actor provides an incorrect DNS server address pointing 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.

Assume a threat actor has successfully connected a rogue DHCP server to a switch port on the same subnet as the target clients. The goal of the rogue server is to provide clients with false IP configuration information.

Click each button for an illustration and explanation of the steps in a DHCP spoofing attack.

- 1. Client Broadcasts DHCP Discovery Messages
- 2. DHCP Servers Respond with Offers
- 3. Client Accepts Rogue DHCP Request
- 4. Rogue DHCP Acknowledges the Request

1. Client Broadcasts DHCP Discovery Messages
In the figure, a legitimate client connects to the network and requires IP configuration parameters. The client broadcasts a DHCP Discover request looking for a response from a DHCP server. Both servers receive the message.



3.8.8. Lab – Explore DNS Traffic

In this lab, you will complete the following objectives:

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

3.8.8 Lab – Explore DNS Traffic

3.9. Network Security Best Practices

3.9.1. Confidentiality, Integrity, and Availability

It is true that the list of network attack types is long. But there are many best practices that you can use to defend your network, as you will learn in this topic.

Network security consists of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Most organizations follow the CIA information security triad:

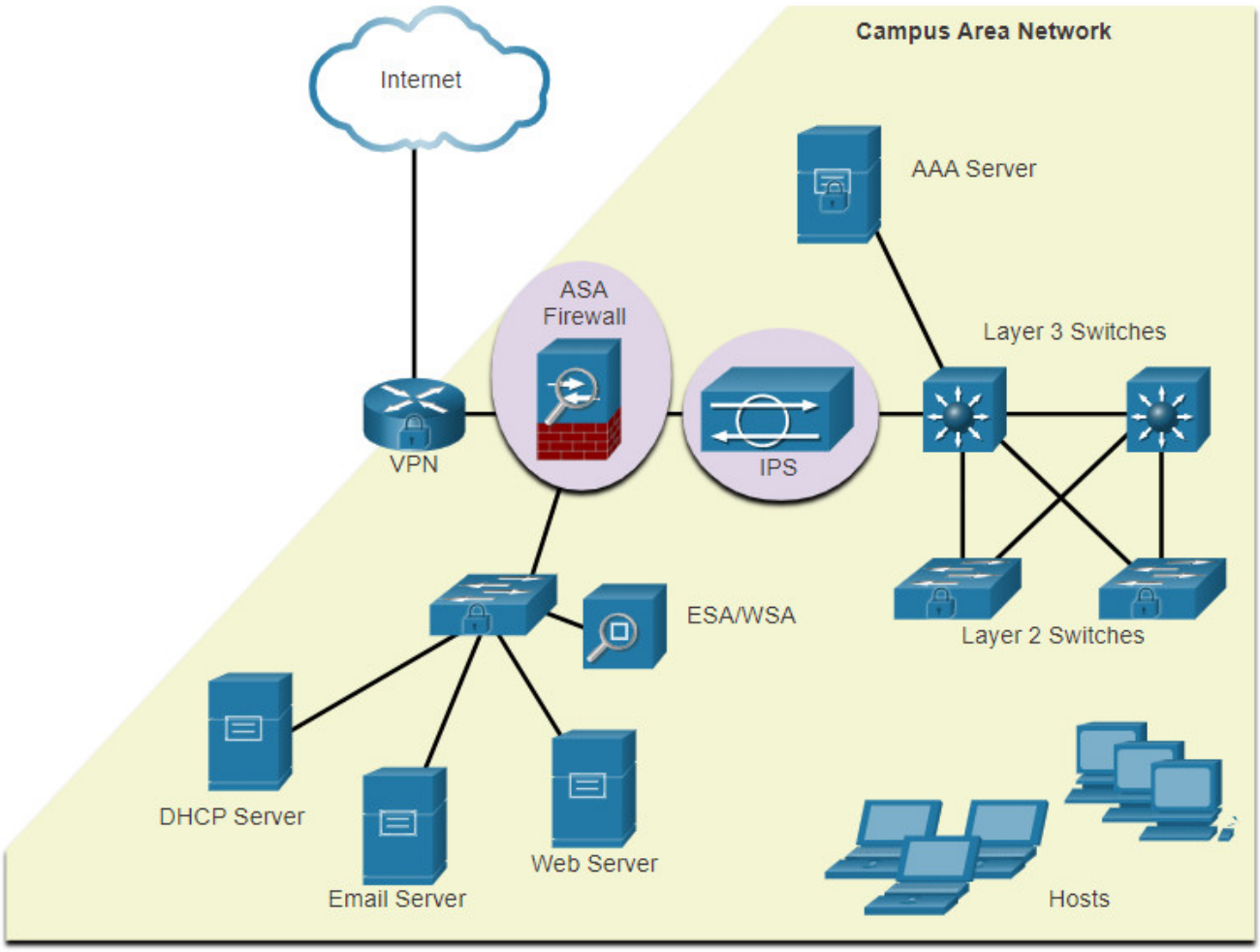
- **Confidentiality** – Only authorized individuals, entities, or processes can access sensitive information. It may require using cryptographic encryption algorithms such as AES to encrypt and decrypt data.
- **Integrity** – Refers to protecting data from unauthorized alteration. It requires the use of cryptographic hashing algorithms such as SHA.
- **Availability** – Authorized users must have uninterrupted access to important resources and data. It requires implementing redundant services, gateways, and links.

CIA Triad

3.9.2. The Defense-in-Depth Approach

To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. Most organizations employ a defense-in-depth approach to security. This is also known as a layered approach. It requires a combination of networking devices and services working together. Consider the network in the figure.

Protecting Against Network Attacks



Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats.

- **VPN** – A router is used to provide secure VPN services with corporate sites and remote access support for remote users using secure encrypted tunnels.
- **ASA Firewall** – This dedicated device provides stateful firewall services. It ensures that internal traffic can go out and come back, but external traffic cannot initiate connections to inside hosts.
- **IPS** – An Intrusion Prevention System (IPS) monitors incoming and outgoing traffic looking for malware, network attack signatures, and more. If it recognizes a threat, it can immediately stop it.
- **ESA/WSA** – The email security appliance (ESA) filters spam and suspicious emails. The web security appliance filters known and suspicious internet malware sites.
- **AAA Server** – This server contains a secure database of who is authorized to access and manage network devices. Network devices authenticate administrative users using this database.

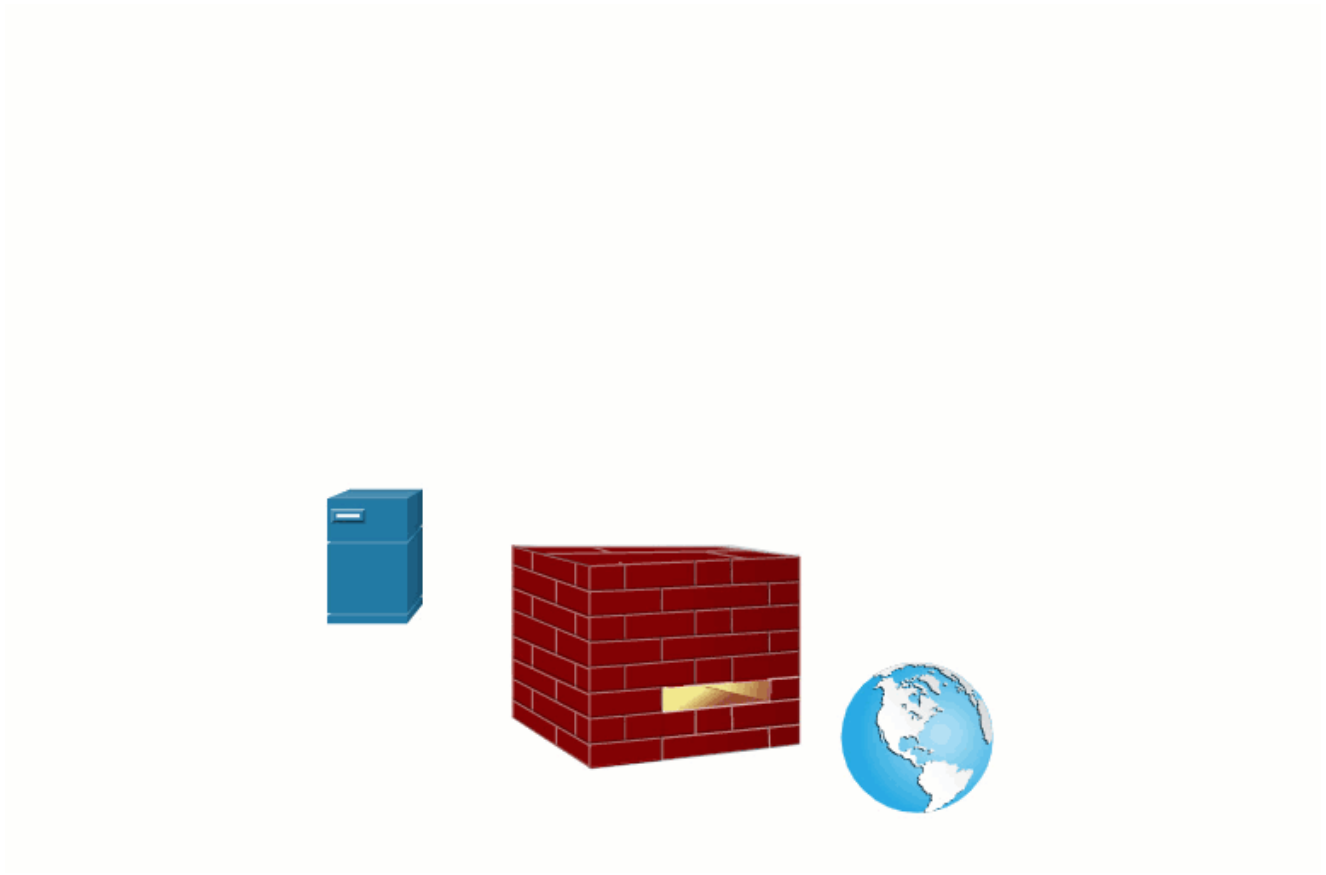
All network devices including the router and switches are hardened, which means that they have been secured to prevent threat actors from gaining access and tampering with the devices.

Next, you must secure the data as it travels across various links. This may include internal traffic, but it is more important to protect the data that travels outside of the organization to branch sites, telecommuter sites, and partner sites.

3.9.3. Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks. Click Play in the figure to view an animation of how a firewall operates.

Firewall Operation



All firewalls share some common properties:

- Firewalls are resistant to network attacks.
- Firewalls are the only transit points between internal corporate networks and external networks because all traffic flows through the firewall.
- Firewalls enforce the access control policy.

There are several benefits of using a firewall in a network:

- They prevent the exposure of sensitive hosts, resources, and applications to untrusted users.
- They sanitize protocol flow, which prevents the exploitation of protocol flaws.
- They block malicious data from servers and clients.
- They reduce security management complexity by off-loading most of the network access control to a few firewalls in the network.

Firewalls also present some limitations:

- A misconfigured firewall can have serious consequences for the network, such as becoming a single point of failure.
- The data from many applications cannot be passed through firewalls securely.
- Users might proactively search for ways around the firewall to receive blocked material, which exposes the network to potential attack.
- Network performance can slow down.
- Unauthorized traffic can be tunneled or hidden so that it appears as legitimate traffic through the firewall.

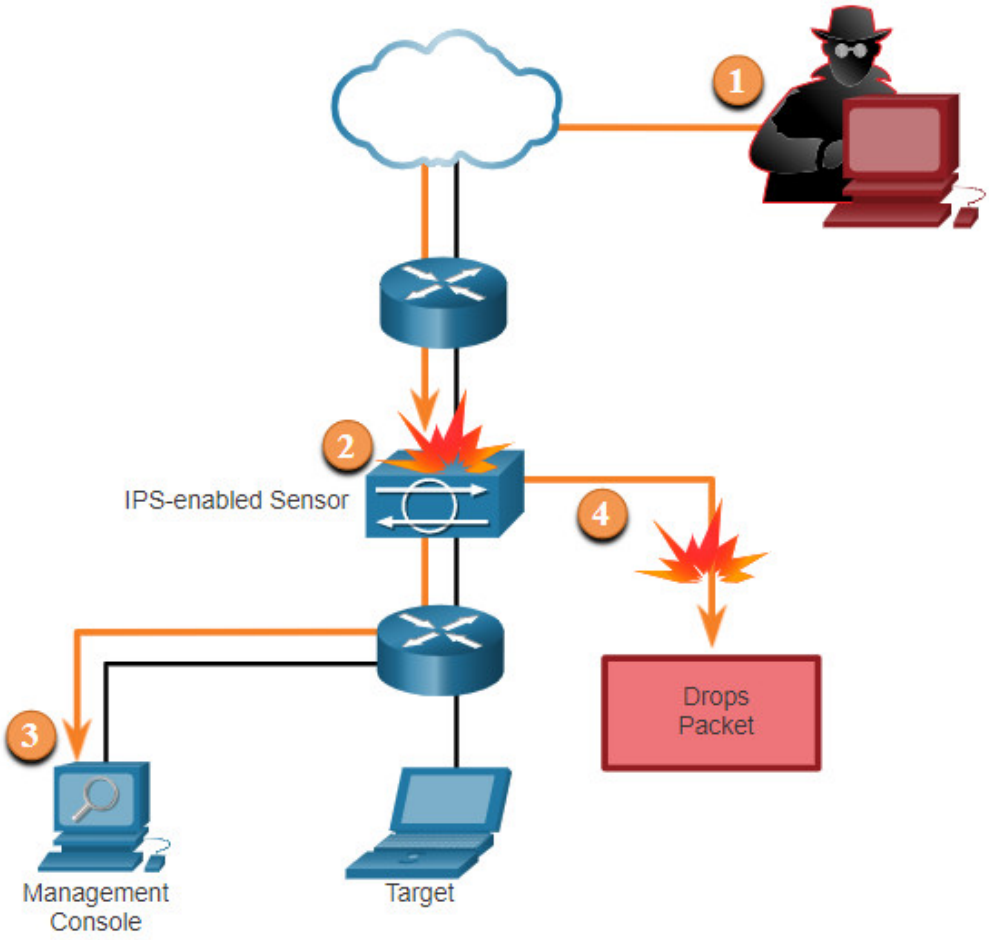
3.9.4. IPS

To defend against fast-moving and evolving attacks, you may need cost-effective detection and prevention systems, such as intrusion detection systems (IDS), or the more scalable intrusion prevention systems (IPS). The network architecture integrates these solutions into the entry and exit points of the network.

IDS and IPS technologies share several characteristics, as shown in the figure. IDS and IPS technologies are both deployed as sensors. An IDS or IPS sensor can be in the form of several different devices:

- A router configured with Cisco IOS IPS software
- A device specifically designed to provide dedicated IDS or IPS services
- A network module installed in an adaptive security appliance (ASA), switch, or router

IPS Operation



The figure shows how an IPS handles denied traffic.

1. The threat actor sends a packet destined for the target laptop.
2. The IPS intercepts the traffic and evaluates it against known threats and the configured policies.
3. The IPS sends a log message to the management console.
4. The IPS drops the packet.

IDS and IPS technologies detect patterns in network traffic using signatures. A signature is a set of rules that an IDS or IPS uses to detect malicious activity. Signatures can be used to detect severe breaches of security, to detect common network attacks, and to gather information. IDS and IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

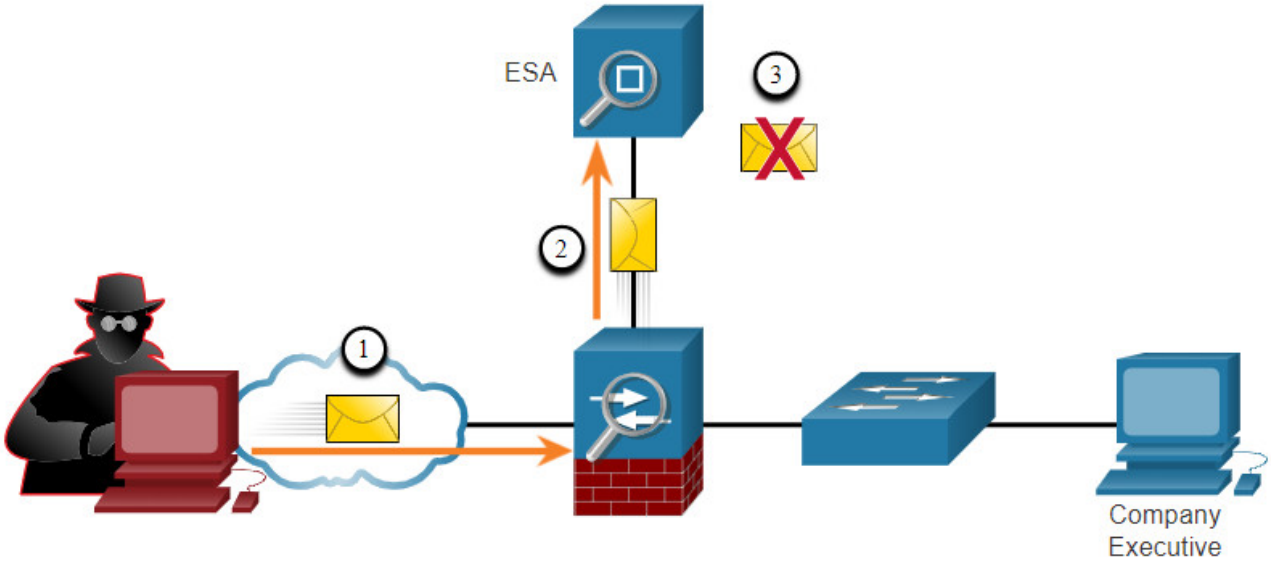
3.9.5. Content Security Appliances

Content security appliances include fine-grained control over email and web browsing for an organization's users.

Cisco Email Security Appliance (ESA)

The Cisco Email Security Appliance (ESA) is a special device designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.

In the figure, a threat actor sends a phishing email.



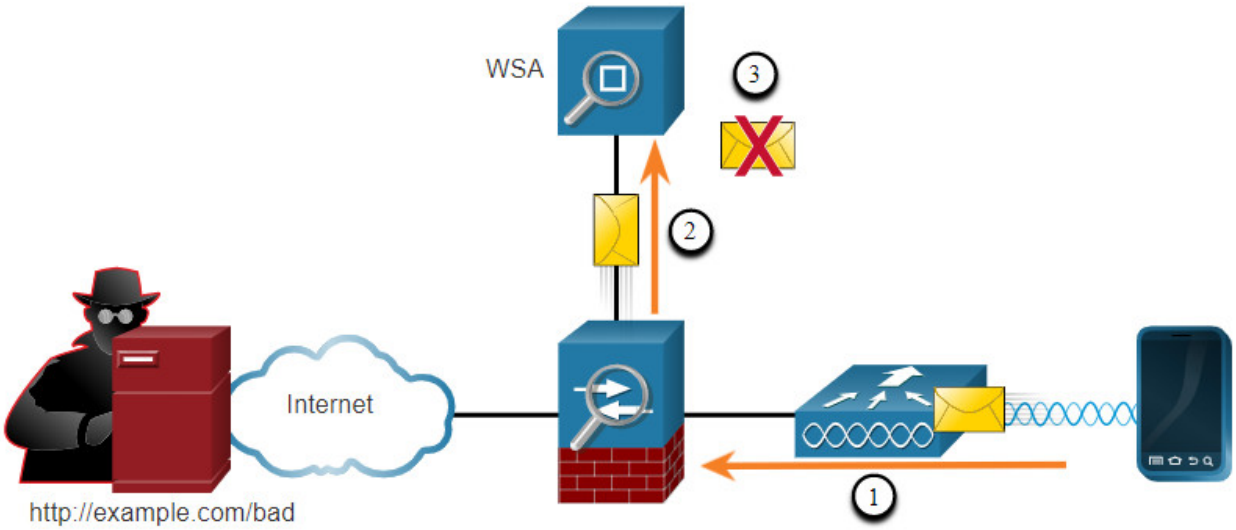
1. Threat actor sends a phishing attack to an important host on the network.
2. The firewall forwards all email to the ESA.
3. The ESA analyzes the email, logs it, and discards it.

Cisco Web Security Appliance (WSA)

The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.

Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization's requirements. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, web application filtering, and encryption and decryption of web traffic.

In the figure, a corporate user attempts to connect to a known blacklisted site.



1. A user attempts to connect to a website.
2. The firewall forwards the website request to the WSA.
3. The WSA evaluates the URL and determines that it is a known blacklisted site. The WSA discards the packet and sends an access denied message to the user.

3.10. Cryptography

3.10.1 Video – Cryptography

Early in the previous topic, cryptography is mentioned as part of the CIA information security triad. In this topic you will get a deeper dive into the many types of cryptography and how they are used to secure the network.

Click Play in the figure to view a video about cryptography.

3.10.2. Securing Communications

Organizations must provide support to secure the data as it travels across links. This may include internal traffic, but it is even more important to protect the data that travels outside of the organization to branch sites, telecommuter sites, and partner sites.

These are the four elements of secure communications:

- **Data Integrity** – Guarantees that the message was not altered. Any changes to data in transit will be detected. Integrity is ensured by implementing either Message Digest version 5 (MD5) or Secure Hash Algorithm (SHA) hash-generating algorithms.
- **Origin Authentication** – Guarantees that the message is not a forgery and does actually come from whom it states. Many modern networks ensure authentication with protocols, such as hash message authentication code (HMAC).

- **Data Confidentiality** – Guarantees that only authorized users can read the message. If the message is intercepted, it cannot be deciphered within a reasonable amount of time. Data confidentiality is implemented using symmetric and asymmetric encryption algorithms.
- **Data Non-Repudiation** – Guarantees that the sender cannot repudiate, or refute, the validity of a message sent. Nonrepudiation relies on the fact that only the sender has the unique characteristics or signature for how that message is treated.

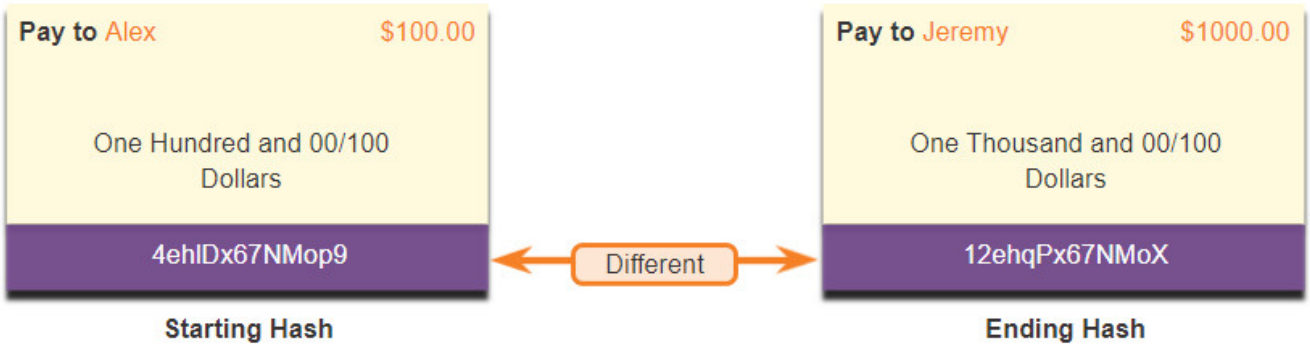
Cryptography can be used almost anywhere that there is data communication. In fact, the trend is toward all communication being encrypted.

3.10.3. Data Integrity

Hash functions are used to ensure the integrity of a message. They guarantee that message data has not changed accidentally or intentionally.

In the figure, the sender is sending a $100 money transfer to Alex.

Hash Algorithm



The sender wants to ensure that the message is not altered on its way to the receiver.

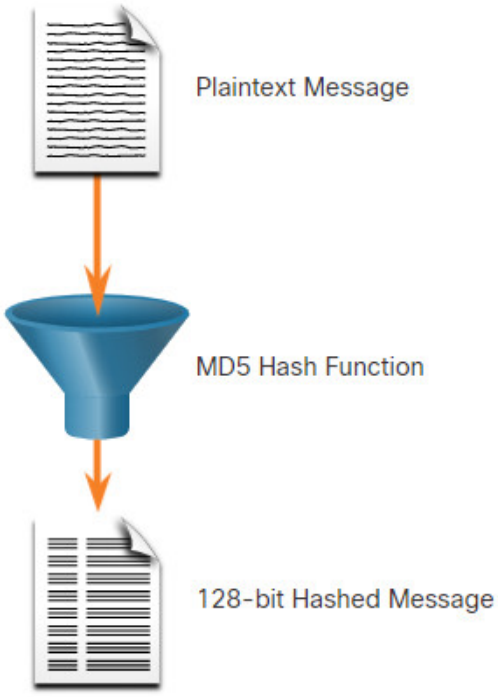
1. The sending device inputs the message into a hashing algorithm and computes its fixed-length hash of 4ehiDx67NMop9.
2. This hash is then attached to the message and sent to the receiver. Both the message and the hash are in plaintext.
3. The receiving device removes the hash from the message and inputs the message into the same hashing algorithm. If the computed hash is equal to the one that is attached to the message, the message has not been altered during transit. If the hashes are not equal, as shown in the figure, then the integrity of the message can no longer be trusted.

3.10.4. Hash Functions

There are three well-known hash functions.

MD5 with 128-bit Digest

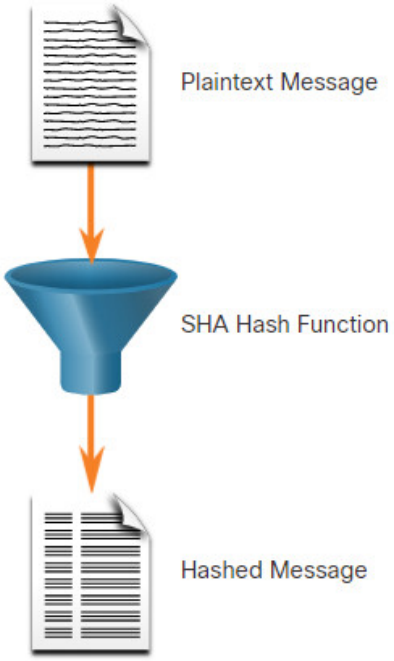
MD5 is a one-way function that produces a 128-bit hashed message, as shown in the figure. MD5 is a legacy algorithm that should only be used when no better alternatives are available. Use SHA-2 instead.



In the figure, a plaintext message is passed through an MD5 hash function. The result is a 128-bit hashed message.

SHA Hashing Algorithm

SHA-1 is very similar to the MD5 hash functions, as shown in the figure. Several versions exist. SHA-1 creates a 160-bit hashed message and is slightly slower than MD5. SHA-1 has known flaws and is a legacy algorithm. Use SHA-2 when possible.



In the figure, a plaintext message is passed through a SHA hash function. The result is a hashed message.

SHA-2

This includes SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), and SHA-512 (512 bit). SHA-256, SHA-384, and SHA-512 are next-generation algorithms and should be used whenever possible.

While hashing can be used to detect accidental changes, it cannot be used to guard against deliberate changes. There is no unique identifying information from the sender in the hashing procedure. This means that anyone can compute a hash for any data, if they have the correct hash function.

For example, when the message traverses the network, a potential threat actor could intercept the message, change it, recalculate the hash, and append it to the message. The receiving device will only validate against whatever hash is appended.

Therefore, hashing is vulnerable to man-in-the-middle attacks and does not provide security to transmitted data. To provide integrity and origin authentication, something more is required.

3.10.5. Origin Authentication

To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC). HMAC uses an additional secret key as input to the hash function.

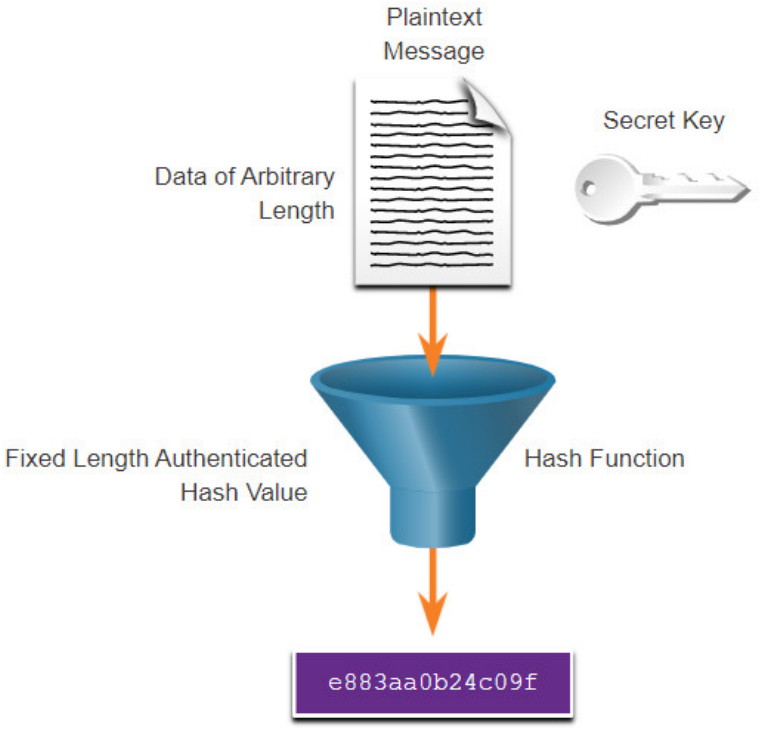
Click each button for an illustration and explanation about origin authentication using HMAC.

HMAC Hashing Algorithm

As shown in the figure, an HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key. Hash functions are the basis of the protection mechanism of HMACs.

Only the sender and the receiver know the secret key, and the output of the hash function now depends on the input data and the secret key. Only parties who have access to that secret key can compute the digest of an HMAC function. This defeats man-in-the-middle attacks and provides authentication of the data origin.

If two parties share a secret key and use HMAC functions for authentication, a properly constructed HMAC digest of a message that a party has received indicates that the other party was the originator of the message. This is because the other party possesses the secret key.

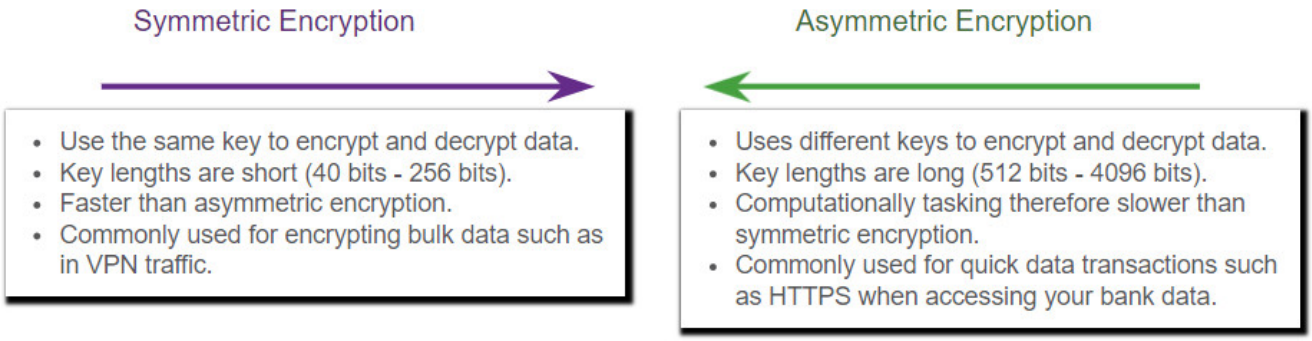


3.10.6. Data Confidentiality

There are two classes of encryption used to provide data confidentiality. These two classes differ in how they use keys.

Symmetric encryption algorithms such as (DES), 3DES, and Advanced Encryption Standard (AES) are based on the premise that each communicating party knows the pre-shared key. Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).

The figure highlights some differences between each encryption algorithm method.



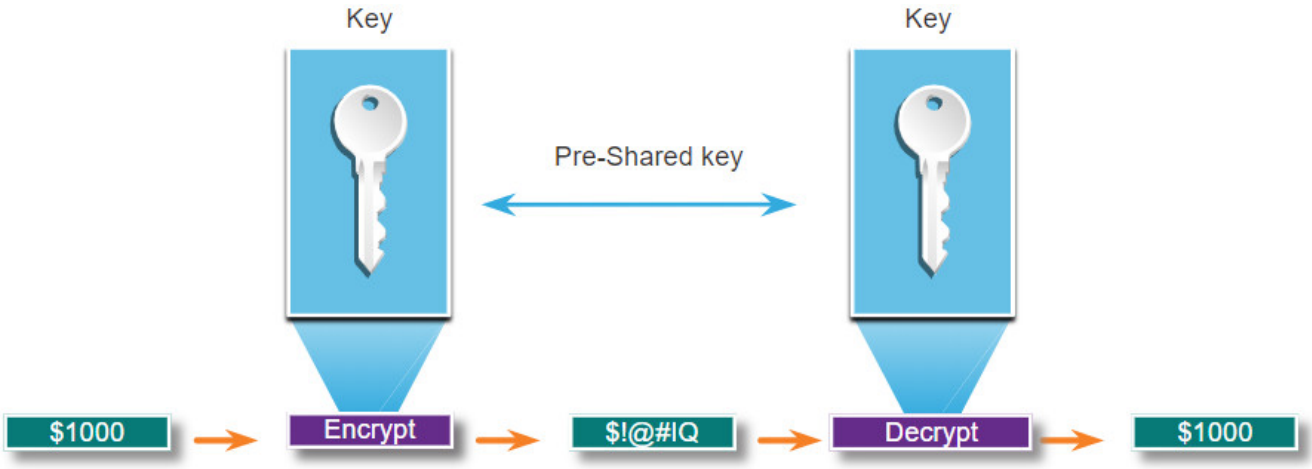
3.10.7. Symmetric Encryption

Symmetric algorithms use the same pre-shared key to encrypt and decrypt data. A pre-shared key, also called a secret key, is known by the sender and receiver before any encrypted communications can take place.

To help illustrate how symmetric encryption works, consider an example where Alice and Bob live in different locations and want to exchange secret messages with one another through the mail system. In this example, Alice wants to send a secret message to Bob.

In the figure, Alice and Bob have identical keys to a single padlock. These keys were exchanged prior to sending any secret messages. Alice writes a secret message and puts it in a small box that she locks using the padlock with her key. She mails the box to Bob. The message is safely locked inside the box as the box makes its way through the post office system. When Bob receives the box, he uses his key to unlock the padlock and retrieve the message. Bob can use the same box and padlock to send a secret reply to Alice.

Symmetric Encryption Example



Today, symmetric encryption algorithms are commonly used with VPN traffic. This is because symmetric algorithms use less CPU resources than asymmetric encryption algorithms. Encryption and decryption of data is fast when using a VPN. When using symmetric encryption algorithms, like any other type of encryption, the longer the key, the

longer it will take for someone to discover the key. Most encryption keys are between 112 and 256 bits. To ensure that the encryption is safe, use a minimum key length of 128 bits. Use a longer key for more secure communications.

Well-known symmetric encryption algorithms are described in the table.

Symmetric Encryption Algorithms	Description
Data Encryption Standard (DES)	This is a legacy symmetric encryption algorithm. It can be used in stream cipher mode but usually operates in block mode by encrypting data in 64-bit block size. A stream cipher encrypts one byte or one bit at a time.
3DES (Triple DES)	This is a newer version of DES, but it repeats the DES algorithm process three times. The basic algorithm has been well tested in the field for more than 35 years. It is considered very trustworthy when implemented using very short key lifetimes.
Advanced Encryption Standard (AES)	AES is a secure and more efficient algorithm than 3DES. It is a popular and recommended symmetric encryption algorithm. It offers nine combinations of key and block length by using a variable key length of 128-, 192-, or 256-bit key to encrypt data blocks that are 128, 192, or 256 bits long.
Software-Optimized Encryption Algorithm (SEAL)	SEAL is a faster alternative symmetric encryption algorithm to DES, 3DES, and AES. It uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms.
Rivest ciphers (RC) series algorithms	This algorithm was developed by Ron Rivest. Several variations have been developed, but RC4 is the most prevalent in use. RC4 is a stream cipher and is used to secure web traffic in SSL and TLS.

3.10.8. Asymmetric Encryption

Asymmetric algorithms, also called public-key algorithms, are designed so that the key that is used for encryption is different from the key that is used for decryption, as shown in the figure. The decryption key cannot, in any reasonable amount of time, be calculated from the encryption key and vice versa.

Asymmetric algorithms use a public key and a private key. Both keys are capable of the encryption process, but the complementary paired key is required for decryption. The process is also reversible. Data encrypted with the public key requires the private key to decrypt. Asymmetric algorithms achieve confidentiality, authentication, and integrity by using this process.

Asymmetric Encryption Example

Because neither party has a shared secret, very long key lengths must be used. Asymmetric encryption can use key lengths between 512 to 4,096 bits. Key lengths greater than or equal to 1,024 bits can be trusted while shorter key lengths are considered unreliable.

Examples of protocols that use asymmetric key algorithms include:

- **Internet Key Exchange (IKE) –** This is a fundamental component of IPsec VPNs.
- **Secure Socket Layer (SSL) –** This is now implemented as IETF standard Transport Layer Security (TLS).
- **Secure Shell (SSH) –** This protocol provides a secure remote access connection to network devices.
- **Pretty Good Privacy (PGP) –** This computer program provides cryptographic privacy and authentication. It is often used to increase the security of email communications.

Asymmetric algorithms are substantially slower than symmetric algorithms. Their design is based on computational problems, such as factoring extremely large numbers or computing discrete logarithms of extremely large numbers.

Because they are slow, asymmetric algorithms are typically used in low-volume cryptographic mechanisms, such as digital signatures and key exchange. However, the key management of asymmetric algorithms tends to be simpler than symmetric algorithms, because usually one of the two encryption or decryption keys can be made public.

Common examples of asymmetric encryption algorithms are described in the table.

Asymmetric Encryption Algorithm	Key Length	Description

Asymmetric Encryption Algorithm	Key Length	Description
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	The Diffie-Hellman algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security of this algorithm depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used given the number and the outcome.
Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA)	512 – 1024	DSS specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA, but is 10 to 40 times slower for verification.
Rivest, Shamir, and Adleman encryption algorithms (RSA)	512 to 2048	RSA is for public-key cryptography that is based on the current difficulty of factoring very large numbers. It is the first algorithm known to be suitable for signing as well as encryption. It is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.
ElGamal	512 – 1024	An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. A disadvantage of the ElGamal system is that the encrypted message becomes very big, about twice the size of the original message and for this reason it is only used for small messages such as secret keys.
Elliptical curve techniques	160	Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.

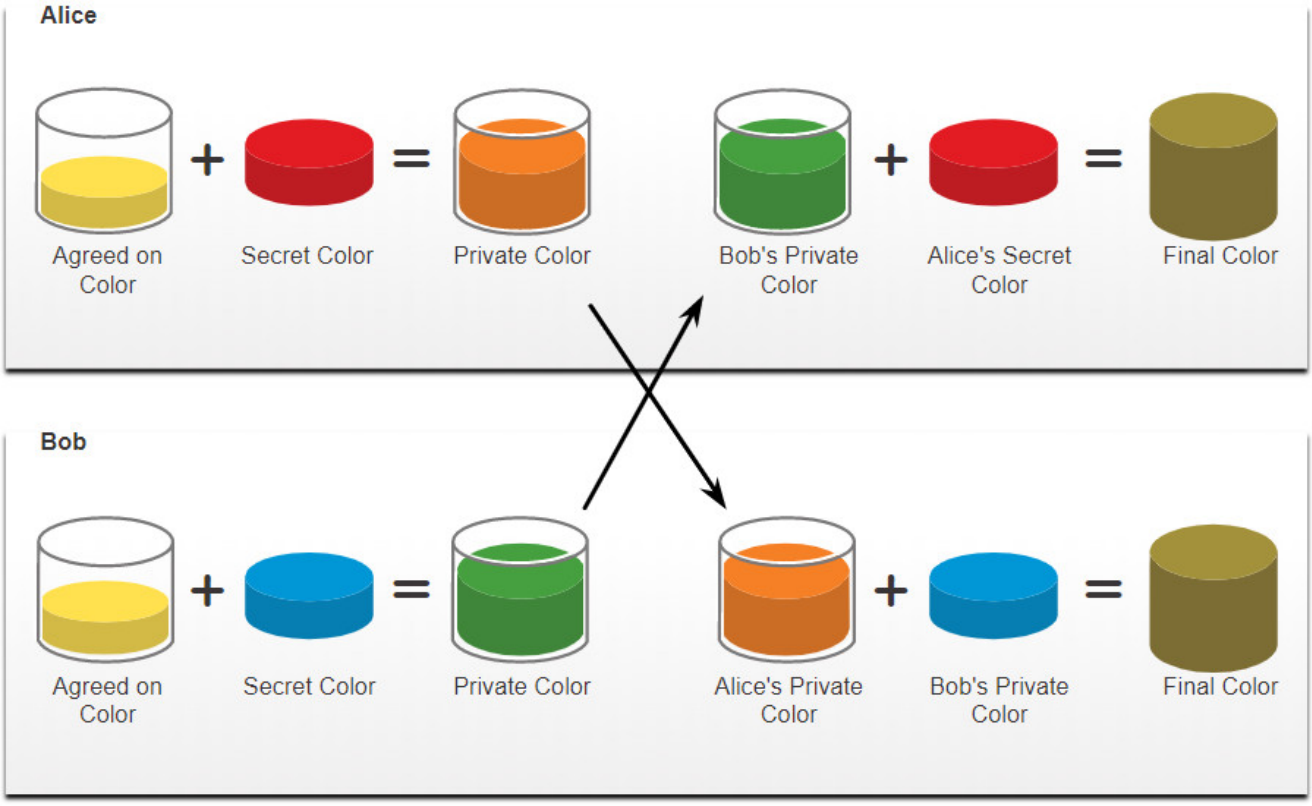
3.10.9. Diffie-Hellman

Diffie-Hellman (DH) is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before. The new shared key is never actually exchanged between the sender and receiver. However, because both parties know it, the key can be used by an encryption algorithm to encrypt traffic between the two systems.

Here are three examples of instances when DH is commonly used:

- Data is exchanged using an IPsec VPN.
- Data is encrypted on the internet using either SSL or TLS.
- SSH data is exchanged.

To help illustrate how DH operates, refer to the figure.



The colors in the figure will be used instead of complex long numbers to simplify the DH key agreement process. The DH key exchange begins with Alice and Bob agreeing on an arbitrary common color that does not need to be kept secret. The agreed on color in our example is yellow.

Next, Alice and Bob will each select a secret color. Alice chose red while Bob chose blue. These secret colors will never be shared with anyone. The secret color represents the chosen secret private key of each party.

Alice and Bob now mix the shared common color (yellow) with their respective secret color to produce a private color. Therefore, Alice will mix the yellow with her red color to produce a private color of orange. Bob will mix the yellow and the blue to produce a private color of green.

Alice sends her private color (orange) to Bob and Bob sends his private color (green) to Alice.

Alice and Bob each mix the color they received with their own, original secret color (Red for Alice and blue for Bob.). The result is a final brown color mixture that is identical to the other's final color mixture. The brown color represents the resulting shared secret key

between Bob and Alice.

DH security uses unbelievably large numbers in its calculations. For example, a DH 1024-bit number is roughly equal to a decimal number of 309 digits. Considering that a billion is 10 decimal digits (1,000,000,000), one can easily imagine the complexity of working with not one, but many 309-digit decimal numbers.

Unfortunately, asymmetric key systems are extremely slow for any sort of bulk encryption. Therefore, it is common to encrypt the bulk of the traffic using a symmetric algorithm, such as 3DES or AES and then use the DH algorithm to create keys that will be used by the encryption algorithm.

3.11. Module Practice and Quiz

3.11.1 Packet Tracer – Network Security Exploration

In this Packet Tracer Physical Mode (PTPM) activity, you will explore and implement several security procedures in different locations within the city of Greenville, North Carolina. Included are networks in a Data Center, an ISP, a Coffee Shop, and a Home.

The Data Center is provisioned for environmental and physical security. There is also software included to maintain access control. You will install an Internet of Things (IoT) smoke detector.

The Coffee Shop offers free wireless access to their patrons. You will implement a VPN to secure traffic.

The Home includes an office, a student's bedroom, and a living room. You will configure two home wireless LANs (WLANs) to require authentication for two different user types: family members and guests. These networks will also be configured with MAC address filtering to restrict access.

3.11.1 Packet Tracer – Network Security Exploration – Physical Mode

3.11.2. What did I learn in this module?

Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information. Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack. An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network.

The term ‘threat actor’ includes hackers and any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack. There are “White Hat”, “Gray Hat”, and “Black Hat” hackers. Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and more. Hacktivists tend to rely on fairly basic, freely available tools. State-sponsored hackers create advanced, customized attack code, often using previously undiscovered software vulnerabilities called zero-day vulnerabilities.

Attack tools have become more sophisticated and highly automated. These new tools require less technical knowledge to implement. Ethical hacking involves many different types of tools used to test the network and keep its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. Common types of attacks are: eavesdropping, data modification, IP address spoofing, password-based, denial-of-service, man-in-the-middle, compromised-key, and sniffer.

The three most common types of malware are worms, viruses, and Trojan horses. A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. A virus executes a specific unwanted, and often harmful, function on a computer. A Trojan horse is non-self-replicating. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within. Other types of malware are: adware, ransomware, rootkit, and spyware.

Networks are susceptible to the following types of attacks: reconnaissance, access, and DoS. Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. Types of access attacks are: password, spoofing, trust exploitations, port redirections, man-in-the-middle, and buffer overflow. Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. DoS and DDoS are attacks that create some sort of interruption of network services to users, devices, or applications.

Threat actors can send packets using a spoofed source IP address. Threat actors can also tamper with the other fields in the IP header to carry out their attacks. IP attack techniques include: ICMP, amplification and reflection, address spoofing, MITM, and session hijacking. Threat actors use ICMP for reconnaissance and scanning attacks. They launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors often use amplification and reflection techniques to create DoS attacks.

TCP segment information appears immediately after the IP header. TCP provides reliable delivery, flow control, and stateful communication. TCP attacks include: TCPSYN Flood attack, TCP reset attack, and TCP Session hijacking. UDP is commonly used by DNS, TFTP,

NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is not protected by encryption. UDP Flood attacks send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The result is very similar to a DoS attack.

Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” This mean that any host can claim to be the owner of any IP or MAC. A threat actor can poison the ARP cache of devices on the local network, creating an MITM attack to redirect traffic. ARP cache poisoning can be used to launch various man-in-the-middle attacks. DNS attacks include: open resolver attacks, stealth attacks, domain shadowing attacks, and tunneling attacks. To stop DNS tunneling, the network administrator must use a filter that inspects DNS traffic. A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

Most organizations follow the CIA information security triad: confidentiality, integrity, and availability. To ensure secure communications across both public and private networks, you must secure devices including routers, switches, servers, and hosts. This is known as defense-in-depth. A firewall is a system, or group of systems, that enforces an access control policy between networks. To defend against fast-moving and evolving attacks, you may need an intrusion detection systems (IDS), or the more scalable intrusion prevention systems (IPS).

The four elements of secure communications are data integrity, origin authentication, data confidentiality, and data non-repudiation. Hash functions guarantee that message data has not changed accidentally or intentionally. Three well-known hash functions are MD5 with 128-bit digest, SHA hashing algorithm, and SHA-2. To add authentication to integrity assurance, use a keyed-hash message authentication code (HMAC). HMAC is calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key. Symmetric encryption algorithms using DES, 3DES, AES, SEAL, and RC are based on the premise that each communicating party knows the pre-shared key. Data confidentiality can also be ensured using asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI). Diffie-Hellman (DH) is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before.

3.11.3 Module Quiz – Network Security Concepts

Download Slide Powerpoint (PPT)

CCNA 3 v7.0 Curriculum: Module 3 - Network Security Concepts.pptx

1 file(s) 1.93 MB

Download

Tags:ccna 3 v7 modules