06 Network Security Principle

Notebook:	FGA Cyber		
Created:	7/10/2019 9:18 AM	**Updated:**	7/10/2019 11:27 AM
Author:	clink200032@gmail.com		
URL:	https://static-course-assets.s3.amazonaws.com/CyberOps11/en/course/module6/6.1.1.1...		

Threat, Vulnerability, Risk.

We are under attack and attackers want access to our assets. Assets are anything of value to an organization such as data and other intellectual property, servers, computers, smart phones, tablets, and more.

To better understand any discussion of network security, it is important to know the following terms:

- **Threat** – A potential danger to an asset such as data or the network itself.
- **Vulnerability and Attack Surface** – A weakness in a system or its design that could be exploited by a threat. An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. For example, your operating system and web browser could both need security patches. They are each vulnerable to attacks. Together, they create an attack surface the threat actor can exploit.
- **Exploit** - The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. The attacker does not need an account in the end system to exploit the vulnerability. In a local exploit, the threat actor has some type of user or administrative access to the end system. A local exploit does not necessarily mean that the attacker has physical access to the end system.
- **Risk** – The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.

Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset. There are four common ways to manage risk:

- **Risk acceptance** – This is when the cost of risk management options outweighs the cost of the risk itself. The risk is accepted without action.
- **Risk avoidance** – This is an action that avoids any exposure to the risk. This is usually the most expensive risk mitigation option.
- **Risk limitation** – This limits a company's risk exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance. It is the most commonly used risk mitigation strategy.
- **Risk transfer** –The risk is transferred to a willing third party such as an insurance company.

Other commonly used network security terms include:

- **Countermeasure** – The **protection** solution that mitigates a threat or risk.
- **Impact** - The resulting damage to the organization that is caused by the threat.

Note: A local exploit requires inside network access such as a user with an account on the network. A remote exploit does not require an account on the network to exploit that network's vulnerability.

Hacker vs Threat Actor

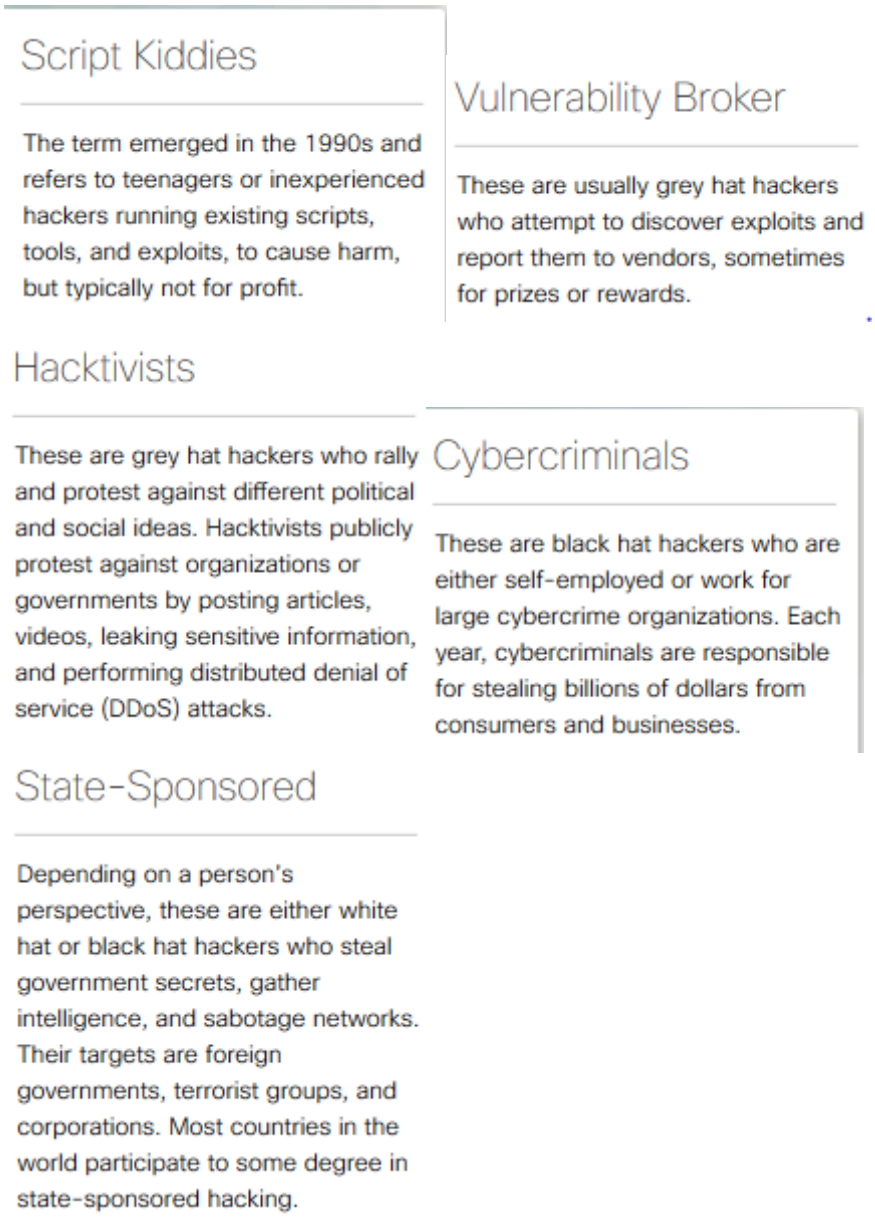
As we know, "hacker" is a common term used to describe a threat actor. However, the term "hacker" has a variety of meanings:

- A clever programmer capable of developing new programs and coding changes to existing programs to make them more efficient.
- A network professional that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- A person who tries to gain unauthorized access to devices on the Internet.
- Individuals who run programs to prevent or slow network access to a large number of users, or corrupt or wipe out data on servers.

As shown in the figure, the terms white hat hacker, black hat hacker, and grey hat hacker are often used to describe hackers.

Good or bad, hacking is an important aspect of network security. In this course, the term threat actor is used when referring to those individuals or groups that could be classified as gray or black hat hackers.

Type of Threat Actor



Cybercriminal

Cybercriminals are threat actors who are motivated to make money using any means necessary. While sometimes cybercriminals work independently, they are more often financed and sponsored by criminal organizations. It is estimated that globally, cybercriminals steal billions of dollars from consumers and businesses every year.

Cybercriminals operate in an underground economy where they buy, sell, and trade exploits and tools. They also buy and sell the private information and intellectual property they steal from victims. Cybercriminals target small businesses and consumers, as well as large enterprises and industries.

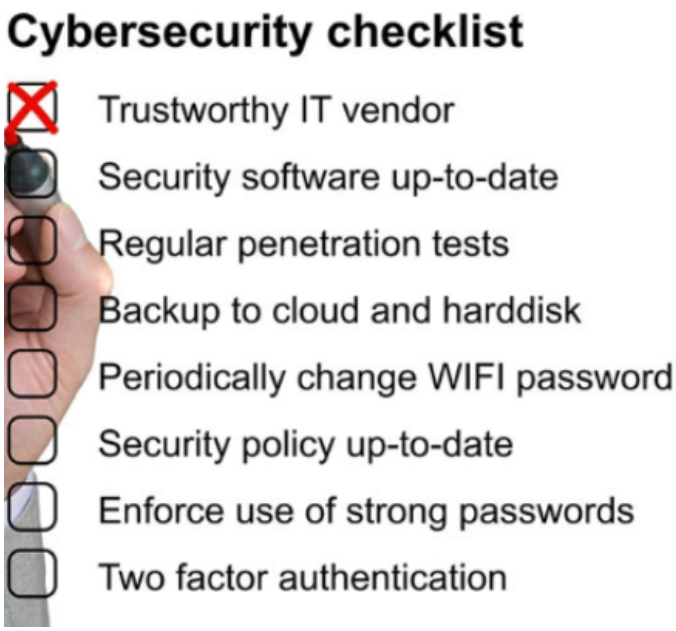
Cybersecurity Task

Threat actors do not discriminate. They target the vulnerable end devices of home users and small-to-medium sized businesses, as well as large public and private organizations.

To make the Internet and networks safer and more secure, we must all develop good cybersecurity awareness. Cybersecurity is a shared responsibility which all users must practice.

For example, we must report cybercrime to the appropriate authorities, be aware of potential threats in email and the web, and guard important information from theft.

Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those listed in the figure.



Cyber Threat Indicator

Many network attacks can be prevented by sharing information about attack indicators. Each attack has unique identifiable attributes. These are known as **cyber threat indicators** or simply **attack indicators**.

For instance, a user receives an email claiming they have won a big prize (Figure 1). Clicking on the link in the email results in an attack. The attack indicators could include the fact the user did not enter that contest, the IP address of the sender, the email subject line, the included link to click, or an attachment to download, among others.

Governments are now actively promoting cybersecurity. For instance, the U.S. Department of Homeland Security (DHS) and United States Computer Emergency Readiness Team (**US-CERT)** are leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost. DHS and US-CERT use a system called Automated Indicator Sharing (AIS). AIS enables the sharing of attack indicators between the US government and the private sector as soon as the threat is verified.

Click here for more information on AIS.

The DHS also promotes cybersecurity to all users. For instance, they have an annual campaign in October called "Cybersecurity Awareness Month". This campaign was developed to promote and raise awareness about cybersecurity. As shown in Figure 2, the DHS also promotes the "**Stop. Think. Connect.**" campaign to encourage all citizens to be safer and more secure online. The campaign provides material on a wide variety of security topics including:

- Best Practices for Creating a Password
- Best Practices for Using Public Wi-Fi
- Five Every Day Steps Towards Online Safety
- How to Recognize and Prevent Cybercrime

- Five Steps to Protecting Your Digital Home

Click here for a complete list of topics made available by the DHS "**Stop. Think. Connect.**" Campaign.

Hacker Characteristic	White Hat	Gray Hat	Black Hat
After hacking into ATM machines remotely using a laptop, I worked with ATM manufacturers to resolve the found security vulnerabilities. I was not originally hired by the ATM manufacturer to test their security.		✓	
From my laptop, I transferred $10 million to my bank account using victim account numbers and PINs after viewing recordings of victims entering the numbers.			✓
My job is to identify weaknesses in the computer system in my company.	✓		
I used malware to compromise several corporate systems to steal credit card information and sold that information to the highest bidder.			✓
During my research for security exploits, I stumbled across a security vulnerability on a corporate network that I am authorized to access.	✓		
While I was searching for security vulnerabilities, I gained unauthorized access to a company's network and left the message "Your security is flawed".		✓	
I am working with technology companies to fix a flaw with DNS.	✓		

Attack Tool

To exploit a vulnerability, an attacker must have a technique or tool that can be used. **Over the years**, attack tools have become more sophisticated, and highly automated, requiring less technical knowledge to use them than in the past.

Evolution of Security Tool

Ethical hacking involves many different types of tools to test and keep the network and its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. However, many of these tools can also be used by threat actors for exploitation.

Threat actors have also created various hacking tools. These tools are explicitly written for nefarious reasons. Cybersecurity personnel must also know how to use these tools when performing network penetration tests.

Figures 1 and 2 highlight categories of common network 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 continually being developed.

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

Forensic Tools

These tools are used by white hat hackers to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.

Hacking Operating Systems

These are specially designed operating systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, Knoppix, BackBox Linux.

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.

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.

Encryption Tools

These tools safeguard the contents of an organization's data at rest and data in motion. 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 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.

Password Crackers

Password theft is the most vulnerable security threat. Password cracking tools are often referred to as password recovery tools and can be used to crack or recover the 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 and access the system. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

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 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.

Fuzzers to Search Vulnerabilities

Fuzzers are tools used by hackers when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.

Wireless Hacking Tools

Wireless networks are more susceptible to network security threats. 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.

Packet Crafting Tools

These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.

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.

Category of Attack

Eavesdropping Attack

This is when a hacker captures and "listens" to network traffic. This attack is also referred to as sniffing or snooping.

Data Modification Attack

If hackers 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 hacker constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

Password-Based Attacks

If hackers discover a valid user account, the attackers have the same rights as the real user. Hackers could use that valid account to obtain lists of other users and network information. They could also change server and network configurations, modify, reroute, or delete data.

Denial-of-Service Attack

A DoS attack prevents normal use of a computer or network by valid users. After gaining access to your network, a DoS attack can crash applications or network services. A DoS attack can also 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

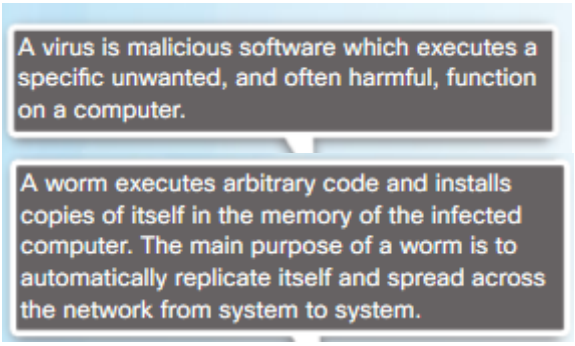
This attack occurs when hackers have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.

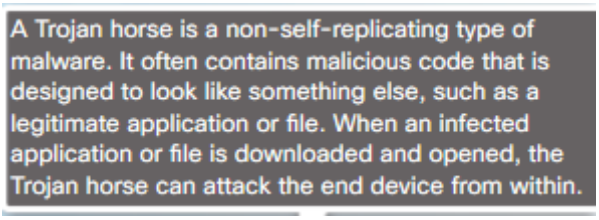
Compromised-Key Attack

If a hacker 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.

Term	Description
Password-based	Attackers have the same rights as the authorized users after the attackers gain access to the accounts.
Data Modification	The threat actors can alter the data in the packet without the knowledge of the sender or receiver.
Man-in-the-Middle	The threat actors have positioned themselves between a source and destination to monitor, capture, and control the communication transparently.
Compromised Key	A threat actor has gained a secret key that allows him access to a secured communication without the knowledge of the sender or receiver.
Eavesdropping	A threat actor captures and listens to the network traffic.
Sniffer	An application or device that can read, monitor, and capture unencrypted network data exchanges and read network packets.
IP Address Spoofing	A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
Denial-of-Service	This attack prevents the normal use of a computer or network by valid users.

6.2.1 Malware





Virus

A virus is a type of malware that propagates by inserting a copy of itself into another program. Viruses then spread from one computer to another, infecting the computers. Most viruses require human help to spread. For example, when someone connects an infected USB drive to their PC, the virus will enter the PC. The virus may then infect a new USB drive, and spread to new PCs. Viruses can lay dormant for an extended period and then activate at a specific time and date.

A simple virus may install itself at the first line of code in an executable file. When activated, the virus might check the disk for other executables so that it can infect all the files it has not yet infected. Viruses can be harmless, such as those that display a picture on the screen, or they can be destructive, such as those that modify or delete files on the hard drive. Viruses can also be programmed to mutate to avoid detection.

Most viruses are now spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are now the most common type of virus.

Trojan Horse

The term Trojan horse originated from Greek mythology. Greek warriors offered the people of Troy (the Trojans) a giant hollow horse as a gift, as shown in the figure. The Trojans brought the giant horse into their walled city, unaware that it contained many Greek warriors. At night, after most Trojans were asleep, the warriors burst out of the horse, opened the city gates, and allowed a sizeable force to enter and take over the city.

Trojan horse malware is software that **appears to be legitimate**, but **it contains malicious code which exploits the privileges of the user that runs it**. Often, Trojans are found attached to online games.

Users are commonly tricked into loading and executing the Trojan horse on their systems. While playing the game, the user will not notice a problem. In the background, the Trojan horse has been installed on the user's system. The malicious code from the Trojan horse continues operating even after the game has been closed.

The Trojan horse concept is flexible. It can cause immediate damage, provide remote access to the system, or access through a back door. It can also perform actions as instructed remotely, such as "send me the password file once per week." This tendency of malware to send data back to the cybercriminal highlights the need to monitor outbound traffic for attack indicators.

Custom-written Trojan horses, such as those with a specific target, are difficult to detect.

Trojan Horse Clasification

Trojan horses are usually classified according to the damage that they cause, or the manner in which they breach a system, as shown in the figure:

- **Remote-access Trojan horse** - This enables unauthorized remote access.
- **Data-sending Trojan horse** - This provides the threat actor with sensitive data, such as passwords.

- **Destructive Trojan horse** - This corrupts or deletes files.
- **Proxy Trojan horse** - This will use the victim's computer as the source device to launch attacks and perform other illegal activities.
- **FTP Trojan horse** -This enables unauthorized file transfer services on end devices.
- **Security software disabler Trojan horse** - This stops antivirus programs or firewalls from functioning.
- **DoS Trojan horse** - This slows or halts network activity.

Worm

Computer worms are similar to viruses because they replicate and can cause the same type of damage. Specifically, worms replicate themselves by independently exploiting vulnerabilities in networks. Worms can slow down networks as they spread from system to system.

Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network.

Worms are responsible for some of the most devastating attacks on the Internet. As shown in Figure 1, in 2001 the Code Red worm had infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers as shown in Figure 2.

The initial infection of the SQL Slammer worm, known as the worm that ate the Internet, is shown in Figure 3. SQL Slammer was a denial of service (DoS) attack that exploited a buffer overflow bug in Microsoft's SQL Server. At its peak, the number of infected servers doubled in size every 8.5 seconds. This is why it was able to infect 250,000+ hosts within 30 minutes, as shown in Figure 4. When it was released on the weekend of January 25, 2003, it disrupted the Internet, financial institutions, ATM cash machines, and more. Ironically, a patch for this vulnerability had been released 6 months earlier. The infected servers did not have the updated patch applied. This was a wake-up call for many organizations to implement a security policy requiring that updates and patches be applied in a timely fashion.

Worms share similar characteristics. They all exploit an enabling vulnerability, have a way to propagate themselves, and they all contain a payload.

Worm Component

Despite the mitigation techniques that have emerged over the years, worms have continued to evolve and pose a persistent threat. Worms have become more sophisticated over time, but they still tend to be based on exploiting weaknesses in software applications.

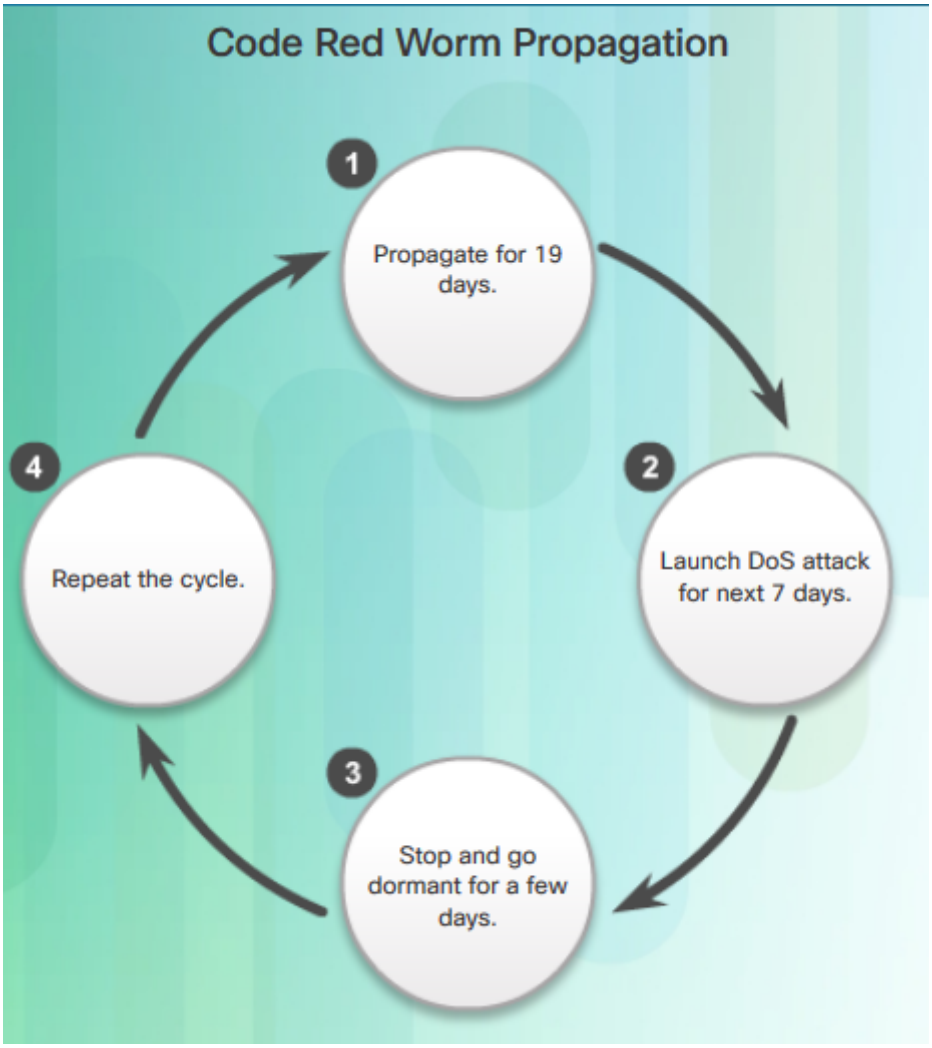
Most worm attacks consist of three components, as shown in Figure 1:

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

Worms are self-contained programs that attack a system to exploit a known vulnerability. Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again. Their propagation mechanisms are commonly deployed in a way that is difficult to detect.

Figure 2 displays the propagation technique used by the Code Red worm.

Note: Worms never really stop spreading on the Internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.



Ransomware

Threat actors have used viruses, worms, and Trojan horses to carry their payloads and for other malicious reasons. However, malware continues to evolve.

Currently, **the most dominating malware is ransomware**. Ransomware is malware that denies access to the infected computer system or its data. The cybercriminals **then demand payment to release the computer system.**

Ransomware has evolved to become the most profitable malware type in history. In the first half of 2016, ransomware campaigns targeting both individual and enterprise users became more widespread and potent.

There are dozens of ransomware variants. **Ransomware frequently uses an encryption algorithm to encrypt system files and data.** The majority of known ransomware encryption algorithms cannot be easily decrypted, leaving victims with little option but to pay the asking price. Payments are typically paid in Bitcoin because users of bitcoin can remain anonymous. Bitcoin is an open-source, digital currency that nobody owns or controls. Click here to learn more about bitcoins.

Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns. Social engineering is also used, as when cybercriminals who identify themselves as security technicians call homes and persuade users to connect to a website that downloads the ransomware to the user's computer.

Other Malware

These are some examples of the varieties of modern malware:

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

This list will continue to grow as the Internet evolves. New malware will always be developed. A major goal of cybersecurity operations is to learn about new malware and how to promptly mitigate it.

Malware Type	Description
Virus	Malicious software that executes a specific, unwanted, and often harmful function on a computer.
Worm	Malware that executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of this malware is to automatically replicate from system to system across the network.
Trojan Horse	Non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file. It attacks the device from within.
Spyware	Malware used to gather information about a user, and, without the user's consent, sends the information to another entity.
Adware	Malware that typically displays annoying pop-ups to generate revenue for its author.
Phishing	Malware that attempts to convince people to divulge sensitive information.
Scareware	Malware that includes scam software that uses social engineering to shock, cause anxiety, or cause the perception of a threat. It is generally directed at an unsuspecting user.
Rootkit	Malware that is installed on a compromised system and provides privileged access to the hacker.
Ransomware	Malware that denies access to the infected computer system and demands a person be paid in order for the restriction to be removed.

6.2.2 Common Network Attack

Although, there is no standardized way of categorizing network attacks, the method used in this course classifies attacks in three major categories.

- Reconnaissance Attacks
- Access Attacks
- DoS Attacks

Reconnaissance Attacks

Reconnaissance is known as **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. **When directed at an endpoint on the network, such as PCs and servers, a recon attack is also called host profiling**. This is because the attacker can get a profile of the system including operating system type and version. If a system is not fully patched, the attacker will then look for known vulnerabilities to exploit.

Recon attacks precede intrusive access attacks or DoS attacks, and often employ the use of widely available tools.

These are some of the techniques used by malicious threat actors conducting reconnaissance attacks:

- **Perform an information query of a target** - The threat actor is looking for initial information about a target. Readily available tools are used including a Google search of the organization's website. Public information about the target network is available from DNS registries using dig, nslookup, and whois utilities.
- **Initiate a ping sweep of the target networks** – The threat actor initiates a ping sweep of the target networks revealed by the previous DNS queries to identify target network addresses. The ping sweep identifies which IP addresses are active. This allows creation of a logical topology of the target network.
- **Initiate a port scan of active IP addresses** - The threat actor then initiates port scans on the live hosts identified by the ping sweep to determine which ports or services are available. Port scanning tools such as Nmap, SuperScan, Angry IP Scanner, and NetScanTools initiate connections to the target hosts by scanning for ports that are open on the target computers.
- **Run Vulnerability Scanners** – The threat actor uses a vulnerability scanning tool such as **Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, or Open VAS** to query the identified ports. The goal is to identify potential vulnerabilities on the target hosts.
- **Run Exploitation tools** - The threat actor now attempts to exploit the identified vulnerabilities in the system. The threat actor uses vulnerability exploitation tools such as **Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker**.

Click Play in Figure 1 to view an animation of a threat actor using the whois command to find information about a target.

Click Play in Figure 2 to view an animation of a threat actor doing a ping sweep of the target's network address space to discover live and active IP addresses.

Click Play in Figure 3 to view an animation of a threat actor performing a port scan on the discovered active IP addresses using Nmap.

Access Attack

Access attack**s exploit known vulnerabilities** in **authentication services, FTP services, and web services** to gain entry to web accounts, confidential databases, and other sensitive information. The goal of the threat actor may be to steal information or to remotely control the inside host.

There are at least three reasons that threat actors would use access attacks on networks or systems:

- To retrieve data

- To gain access to systems
- To escalate access privileges

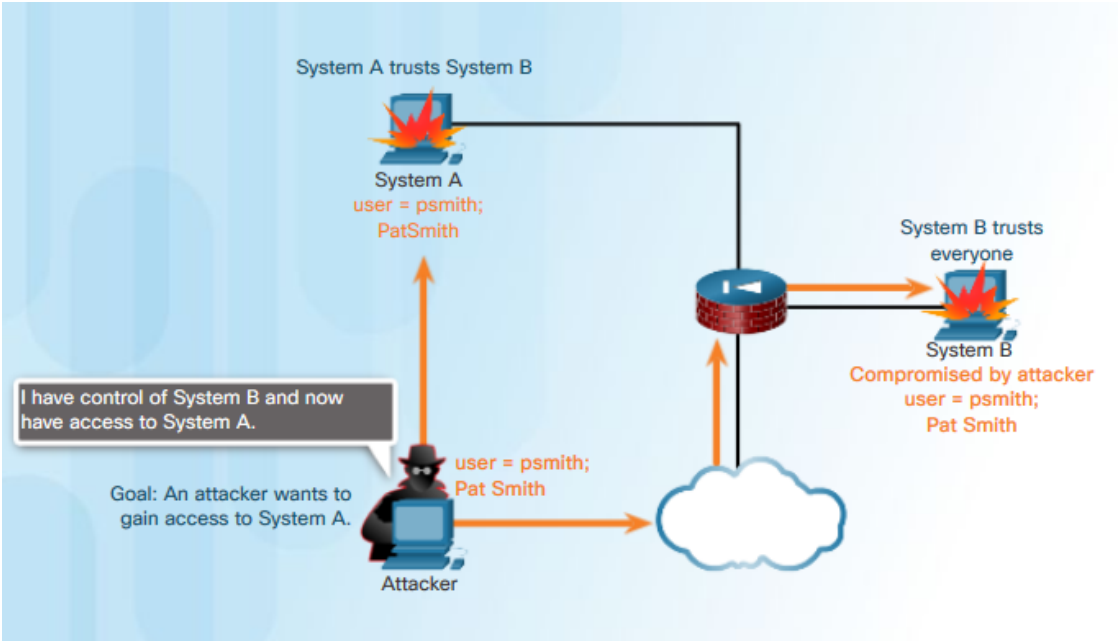
Click Play in the figure to view an animation of a threat actor using an access attack to gain root privileges to an FTP server.

Type of Access Attack

There are several common types of access attacks:

- **Password attack** - Threat actors attempt to discover critical system passwords using various methods such as phishing attacks, dictionary attacks, brute-force attacks, network sniffing, or using social engineering techniques. Brute-force password attacks involve repeated attempts using tools such as Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
- **Pass-the-hash** - The threat actor already has access to the user's machine and uses malware to gain access to the stored password hashes. The threat actor then uses the hashes to authenticate to other remote servers or devices without using brute-force. Hashing is discussed in more detail later in the course.
- **Trust exploitation** - Threat actors use a trusted host to gain access to network resources. For example, an external host that accesses an internal network over VPN is trusted. If that host is attacked, the attacker may use the trusted host to gain access to the internal network.
- **Port redirection** - This is when a threat actor uses a compromised system as a base for attacks against other targets.
- **Man-in-the-middle attack** - The threat actor is positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.
- **IP, MAC, DHCP Spoofing** - Spoofing attacks are attacks in which one device attempts to pose as another by falsifying address data. There are multiple types of spoofing attacks. For example, MAC address spoofing occurs when one computer accepts data packets based on the MAC address of another computer that is the actual destination for the data.

Click Play in the animation in Figure 1 to view an example of trust exploitation.



The port redirection example in Figure 2 displays a threat actor using SSH to connect to compromised Host A. Host A is trusted by Host B; therefore, the threat actor is allowed to use Telnet to access it.

Figure 3 displays an example of a man-in-the-middle attack. Click each numbered plus sign (+) sign to learn more about that step in the man-in-the-middle attack.

Social engineering is a type of access attack that attempts to manipulate individuals into performing actions or divulging confidential information such as passwords and usernames. It typically involves the use of social skills to manipulate inside network users to divulge information needed to access the network.

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.

Examples of social engineering attacks include:

- **Pretexting** - This is when a threat actor calls an individual and lies to them in an attempt to gain access to privileged data. An example involves a threat actor who pretends to need personal or financial data in order to confirm the identity of the recipient.
- **Spam** - Threat actors may use spam email to trick a user into clicking an infected link, or downloading an infected file.
- **Phishing** - There are many variations of this social engineering technique. A common version is the threat actor sends enticing custom-targeted spam email to individuals with the hope the target user clicks on a link or downloads malicious code.
- **Something for Something (Quid pro quo)** - This is when a threat actor requests personal information from a party in exchange for something like a **free gift.**
- **Tailgating** - This is when a threat actor quickly follows an authorized person with a corporate badge into a badge-secure location. The threat actor then has access to a secure area.
- **Baiting** - This is when a threat actor leaves a malware-infected physical device, such as a USB flash drive in a public location such as a corporate washroom. The finder finds the device and inserts it into their computer. On a Windows host, the **autoplay** feature may automatically install the malware.
- **Visual hacking** – This is where a threat actor **physically** observes the victim entering credentials such as a **workstation login, an ATM PIN,** or the combination on a physical lock. This practice is also referred to as "shoulder surfing".

Phising Social Engineering

Phishing is a common social engineering technique that **threat actors use to send emails that appear to be from a legitimate organization** (such as a bank). The goal is to get the victim to **submit personal or sensitive information such as usernames, passwords, account information, financial information, and more.** The email could also attempt to trick **the recipient into installing malware on their device.**

Variations of phishing attacks include:

- **Spear phishing** - This is a targeted phishing attack tailored for a specific individual or organization and is more likely to successfully deceive the target.
- **Whaling** – This is similar to spear phishing but is focused on big targets such as top executives of an organization.
- **Pharming** – This attack compromises domain name services by injecting entries into local host files. Pharming also includes poisoning the DNS by compromising the DHCP servers that specify DNS servers to their clients.
- **Watering hole** – This attack first determines websites that a target group visits regularly. Next, the threat actor attempts to compromise those websites by infecting them with malware that can identify and target only members of the target group.

- **Vishing** – This is a phishing attack using **voice and the phone system instead of email.**
- **Smishing** – This is a phishing attack using **SMS** texting instead of email.

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

Click here to learn more about SET.

Strengthen the Weakest Link

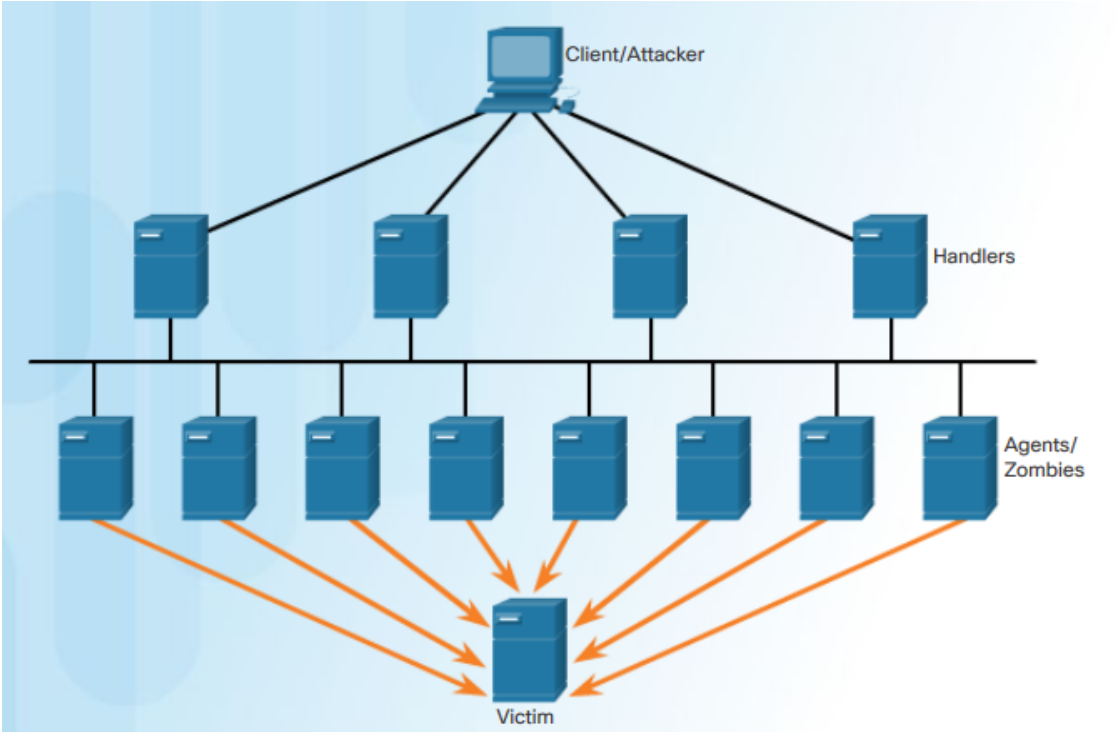
Cybersecurity is only as strong as its weakest link. Since computers and other Internet-connected devices have become an essential part of our lives, they no longer seem new or different. People have become very casual in their use of these devices and rarely think about network security. The weakest link in cybersecurity can be the personnel within an organization, with social engineering as a major security threat. Because of this, one of the most effective security measures that an organization can take is to **train its personnel and create a "security-aware culture."**

DOS Attack

If threat actors can compromise many hosts, they can perform a Distributed DoS Attack (DDoS). DDoS attacks are similar in intent to DoS attacks, except that a DDoS attack increases in magnitude because it originates from multiple, coordinated sources, as shown in the figure. A DDoS attack can use hundreds or thousands of sources, as in IoT-based DDoS attacks.

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

- **Zombies** – Refers to a group of compromised hosts (i.e., agents). These hosts run malicious code referred to as robots (i.e., bots). The zombie malware continually attempts to self-propagate like a worm.
- **Bots** - Bots are malware that are designed to infect a host and communicate with a handler system. Bots can also log keystrokes, gather passwords, capture and analyze packets, and more.
- **Botnet** – Refers to a group of zombies that have been infected using self-propagating malware (i.e., bots) and are controlled by handlers.
- **Handlers** – Refers to a master **command-and-control (CnC** or **C2)** server controlling groups of zombies. The originator of a botnet can use Internet Relay Chat (IRC) or a web server on the C2 server to remotely control the zombies.
- **Botmaster** – This is the threat actor in control of the botnet and handlers.



Note: There is an underground economy where botnets can be bought (and sold) for a nominal fee. This can provide threat actors with botnets of infected hosts ready to launch a DDoS attack.

As an example, a DDoS attack could proceed as follows:

1. The threat actor builds or **purchases a botnet of zombie hosts.**

2. Zombie computers continue to scan and infect more targets to create more zombies.

3. When ready, the botmaster uses the handler systems to make the botnet of zombies carry out the DDoS attack on the chosen target.

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

Buffer Overflow Attack

The goal of a threat actor when using a buffer overflow DoS attack is to find a system memory-related flaw on a server and exploit it. Exploiting the buffer memory by overwhelming it with unexpected values usually renders the system inoperable, creating a DoS attack.

For example, a threat actor enters input that is larger than expected by the application running on a server. The application accepts the large amount of input and stores it in memory. The result is that it may consume the associated memory buffer and potentially overwrite adjacent memory, eventually corrupting the system and causing it to crash.

An early example of using malformed packets was the **Ping of Death**. In this legacy attack, the threat actor sent a ping of death, which was an echo request in an IP packet larger than the maximum packet size of 65,535 bytes. The receiving host would not be able to handle a packet of that size and it would crash.

Buffer overflow attacks are continually evolving. For instance, a remote denial of service attack vulnerability was recently discovered in Microsoft Windows 10. Specifically, **a threat actor created malicious code to access out-of-scope memory.** When this code is accessed by the Windows AHCACHE.SYS process, it attempts to trigger a system crash, denying service to the user. Click here to read the Talos blog on this attack.

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

Evasion Method

Threat actors learned long ago that "to hide is to thrive". This means their malware and attack methods are most effective when they are undetected. For this reason, many attacks use stealthy evasion techniques to disguise an attack payload. Their goal is to prevent detection by network and host defenses.

Some of the evasion methods used by threat actors include:

- **Encryption and tunneling –** This evasion technique uses tunneling to hide the content, or encryption to scramble its contents, making it difficult for many security detection techniques to detect and identify the malware.
- **Resource exhaustion –** This evasion technique keeps the host too busy to properly use security detection techniques.
- **Traffic fragmentation** – This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network.
- **Protocol-level misinterpretation** – This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check.
- **Traffic substitution** - In this evasion technique, the threat actor attempts to trick the IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data.
- **Traffic insertion** - Similar to traffic substitution, but the threat actor inserts extra bytes of data in a malicious sequence of data. The IPS rules miss the malicious data, accepting the full sequence of data.
- **Pivoting** – This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to login to another host using the same credentials.
- **Rootkits** - A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system.

New attack methods are constantly being developed. Network security personnel must be aware of the latest attack methods in order to detect them.

Network Attack Type	Reconnaissance	Access	DoS	Social Engineering
Buffer Overflow			✓	
Tailgating				✓
Password		✓		
Port Scanning	✓			
Smurf			✓	
Man-in-the-Middle		✓		
Baiting				✓
IP, MAC, DHCP Spoofing		✓		
TCP SYN Flood			✓	
Ping Sweep	✓			
Port Redirection		✓		

Component	Description
Bots	They are designed to infect a host and communicate with a handler system.
Botnet	A network of compromised hosts that have been infected using self-propagating malware.
Handlers	The master command and control servers can control groups of compromised hosts.
Bots	They can log keystrokes, gather passwords, capture and analyze packets, and more.
Zombies	A group of compromised hosts that run malicious codes and can self-propagate like a worm.
Botmaster	The hacker in control of the compromised network and the servers controlling the groups of compromised hosts.

In this chapter, you learned how networks are attacked. You learned the types of threats and attacks used by threat actors. Threat actors are gray or black hat hackers that attempt to gain unauthorized access to our networks. They may also run programs that prevent or slow network access for others. Cybercriminals are threat actors that are motivated solely by financial gain.

Threat actors use a variety of tools including:

- Password crackers
- Wireless hacking tools
- Network scanning and hacking tools
- Packet crafting tools
- Packet sniffers
- Rootkit detectors
- Forensic tools
- Debuggers
- Hacking operating systems

- Encryption tools
- Vulnerability exploitation tools
- Vulnerability scanners

These tools can be used to launch a variety of attacks including:

- Eavesdropping
- Data modification
- IP address spoofing
- Password cracking
- Denial of service
- Man-in-the-middle
- Compromised key
- Network sniffing

Malware, or malicious code, is software that is specifically designed to damage, disrupt, steal, or generally inflict some other "bad" or illegitimate action on data, hosts, or networks. The three most common types of malware are viruses, worms, and Trojan horses:

- A virus is a type of malware that propagates by inserting a copy of itself into another program.
- Worms are similar to viruses because they replicate and can cause the same type of damage. Whereas a virus requires a host program to run, worms can run by themselves.
- A Trojan horse is software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.

Malware continues to evolve. The most dominate attack currently is ransomware. Ransomware is malware that denies access to the infected computer system or its data until the owner pays the cybercriminal.

All the various types of tools threat actors use to launch network attacks can be classified as one or more of the following:

- **Reconnaissance** - This is unauthorized discovery and mapping of systems, services, or vulnerabilities.
- **Access attacks** – These exploit known vulnerabilities to gain entry to web accounts, confidential databases, and other sensitive information.
- **Social engineering** – This is an attempt to manipulate individuals into performing actions or divulging confidential information such as passwords and usernames.
- **Denial of Service** – This occurs by overwhelming the network with a large quantity of traffic, or maliciously formatting packets that the receiver is unable to handle causing the device to run very slowly or even crash.
- **Buffer overflow** – This uses a system memory-related flaw on a server to overwhelm it with unexpected values. The goal is to render it inoperable.

To stay hidden and continue their attack, threat actors use a variety of evasion methods including:

- Encryption and tunneling
- Resource exhaustion
- Traffic fragmentation
- Protocol-level misinterpretation
- Traffic substitution
- Traffic insertion
- Pivoting
- Rootkits