Module 2: Network Threats

Networking Security v1.0
(NETSEC)

Module Objectives

Module Title: Network Threats

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

Topic Title	Topic Objective
Who is Attacking Our Network?	Explain how network threats have evoloved.
Threat Actor Tools	Describe the various types of attack tools used by Threat Actors.
Malware	Describe types of malware.
Common Network Attacks - Reconnaissance, Access, and Social Engineering	Explain reconnaissance, access, and social engineering network attacks.
Network Attacks - Denial of Service, Buffer Overflows, and Evasion Configurations	Explain Denial of Service, buffer overflow, and evasion attacks.

2.1 Who is Attacking Our Network?

Hacker vs. Threat Actor

As we know, “hacker” is a common term used to describe a threat actor. The term “hacker” has a variety of meanings, as follows:

- 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.
- An individual who runs programs to prevent or slow network access to many users, or to corrupt or destroy data on servers.

You may see references to white hat, gray hat, and black hat hackers.

Evolution of Threat Actors

Since hacking started in the 1960s with phone freaking, or phreaking, it has evolved to include many types of threat actors.

Threat Actor	Explanation
Script Kiddies	Script kiddies emerged in the 1990s. They are teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
Vulnerability Brokers	Vulnerability brokers are grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
Hacktivists	Hacktivists are grey hat hackers who rally and protest against different political and social ideas.
Cybercriminals	Cybercriminal is a term for black hat hackers who are either self-employed or working for large cybercrime organizations.
State- Sponsored	State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations.

Cybercriminals

Cybercriminals are threat actors who are motivated to make money using any means necessary.

- While some 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.

Cybersecurity Tasks

Organizations must act to protect their assets, users, and customers. They must develop and practice cybersecurity tasks, including the following:

- Use a trustworthy IT vendor
- Keep security software up-to-date
- Perform regular penetration tests
- Back up to cloud and hard disk
- Periodically change WIFI password
- Keep security policy up-to-date
- Enforce use of strong passwords
- Use two factor authentication

Cyber Threat Indicators

Many network attacks can be prevented by sharing information about **indicators of compromise** (IOC). Each attack has unique, identifiable attributes. Indicators of compromise are the evidence that an attack has occurred.

IOCs can be features that identify the following:

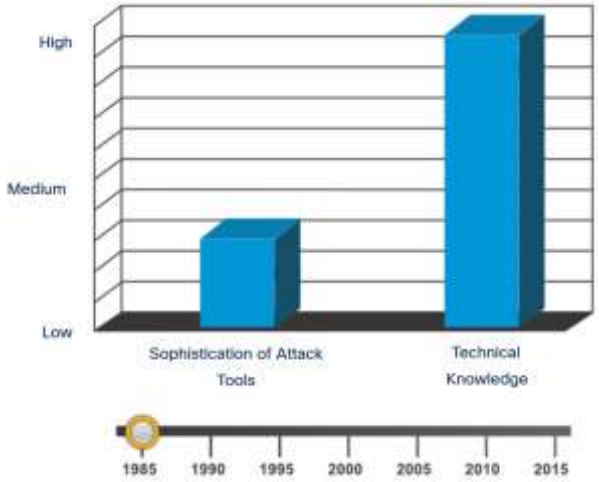
- malware files
- IP addresses of servers that are used in attacks
- filenames
- characteristic changes made to end system software

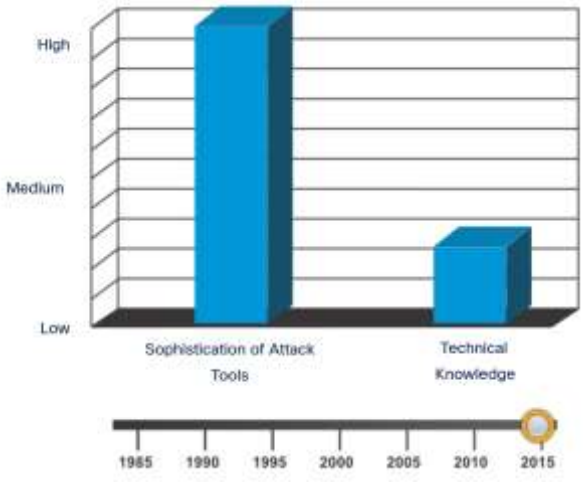
Indicators of attack (IOA) focus more on the motivation behind an attack and the potential means by which threat actors have, or will, compromise vulnerabilities to gain access to assets. IOAs are concerned with the strategies that are used by attackers.

2.2 Threat Actor Tools

Introduction of 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.





Evolution of Security Tools

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

Categories of Tools	Description
password crackers	Passwords are 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. 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.
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.
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	Packet crafting 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.
packet sniffers	Packet sniffer 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	A rootkit detector is a directory and file integrity checker used by white hat hackers to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.

Evolution of Security Tools (Cont.)

Categories of Tools	Description
fuzzers	Fuzzers are tools used by threat actors when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
forensic tools	White hat hackers use forensic tools to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.
debuggers	Debugger tools are used by black hat hackers to reverse engineer binary files when writing exploits. They are also used by white hat hackers when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.
hacking operating systems	Hacking operating systems are specially designed operating systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, SELinux, Knoppix, Parrot OS, and BackBox Linux.
encryption tools	These tools safeguard the contents of an organization's data when it is stored or transmitted. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Examples of these tools include VeraCrypt, CipherShed, Open SSH, OpenSSL, 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 Tool Kit, 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 these tools include Nipper, Securia PSI, Core Impact, Nessus, SAINT, and Open VAS.

Categories of Attacks

Category of Attack	Description
eavesdropping attack	An eavesdropping attack is when a threat actor captures and listens to network traffic. This attack is also referred to as sniffing or snooping.
data modification attack	Data modification attacks occur when a threat actor has captured enterprise traffic and has altered the data in the packets without the knowledge of the sender or receiver.
IP address spoofing attack	An IP address spoofing attack is when a threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
password-based attacks	Password-based attacks occur when a threat actor obtains the credentials for a valid user account. Threat actors then use that account to obtain lists of other users and network information. They could also change server and network configurations, and modify, reroute, or delete data.
denial-of-service (DoS) attack	A DoS attack prevents normal use of a computer or network by valid users. After gaining access to a 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.

Categories of Attacks (Cont.)

Category of Attack	Description
man-in-the-middle attack (MiTM)	A MiTM 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	A compromised key attack occurs when a threat actor obtains a secret key. This 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. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted, and the threat actor does not have access to the key.

2.3 Malware

Types of Malware

Malware is short for malicious software or malicious code. It is code or software that is specifically designed to damage, disrupt, steal, or generally inflict some other “bad” or illegitimate action on data, hosts, or networks.

End devices are especially prone to malware attacks.

Three most common types of malware are:

- virus
- worm
- Trojan horse

Viruses

A virus is a type of malware that spreads by inserting a copy of itself into another program. After the program is run, viruses then spread from one computer to another, infecting the computers. Most viruses require human help to spread.

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 also be programmed to mutate to avoid detection.

Most viruses are now spread by USB memory drives, CDs, DVDs, network shares, and email.

Trojan Horses

Trojan horse malware is software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user who 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."

Trojan Horse Classification

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 table.

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

Worms

Computer worms are like 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.

SQL Slammer, known as the worm that ate the internet, 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. It infected 250,000+ hosts within 30 minutes, as shown in the figure.

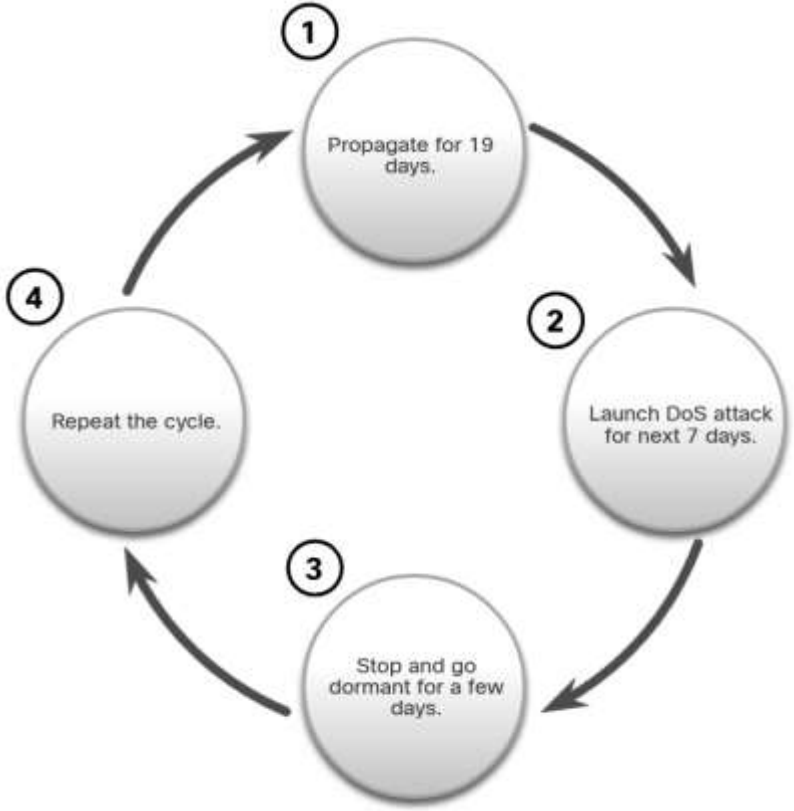
Worm Components

Most worm attacks consist of three components:

- **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.

Worm Components (Cont.)

The propagation technique used by the Code Red worm is shown in the figure.



Ransomware

Currently, the most dominant 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.
- There are dozens of ransomware variants.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Payments are typically paid in Bitcoin because users of bitcoin can remain anonymous.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used.

Other Malware

These are some examples of the varieties of modern malware:

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

Common Malware Behaviors

Computers infected with malware often exhibit one or more of the following symptoms:

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

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

Types of Network Attacks

To mitigate attacks, it is useful to first categorize the various types of attacks. By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.

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

Video - Reconnaissance Attacks

This video will explain the following techniques used in a reconnaissance attack:

- Perform an information query on a target
- Initiate a ping sweep of the target network
- Initiate a port scan of active ip addresses
- Run vulnerability scanners
- Run exploitation tools

Access Attacks

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

Technique	Description
Password Attacks	In a password attack, the threat actor attempts to discover critical system passwords using various methods.
Spoofing Attacks	In spoofing attacks, the threat actor's device attempts to pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.
Trust Exploitation	In a trust exploitation attack, a threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
Port redirection	In a port redirection attack, a threat actor uses a compromised system as a base for attacks against other targets.
Man-in-the-Middle	In a man-in-the-middle attack, the threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.
Buffer Overflow Attack	In a buffer overflow attack, the threat actor exploits the buffer memory and overwhelms it with unexpected values. This usually renders the system inoperable, resulting in a DoS attack.

Video - Access and Social Engineering Attacks

This video will cover the following:

- Techniques used in access attacks (password attacks, spoofing attacks, trust exploitations, port redirections, man-in-the-middle attacks, buffer overflow attacks)
- Techniques used in social engineering attacks (pretexting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, dumpster diving)

Social Engineering Attacks

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. 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.
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	In this type of attack, a threat actor pretends to be someone else to gain the trust of a victim.

Social Engineering Attacks (Cont.)

Social Engineering Attack	Description
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.

Strengthening the Weakest Link

Cybersecurity is only as strong as its weakest link. Because computers and other internet-connected devices have become an essential part of our lives, they no longer seem new or different.

The weakest link in cybersecurity can be the personnel within an organization, and social engineering is 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.”

2.5 Network Attacks - Denial of Service, Buffer Overflows, and Evasion

Video - Denial of Service Attacks

This video will cover the following:

- Techniques used in Denial-of-Service attacks (overwhelming quantity of traffic, maliciously formatted packets)
- Techniques used in Distributed Denial-of-Service attacks (zombies)

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
- Maliciously Formatted Packets

A Distributed DoS Attack (DDoS) is like a DoS attack, but it originates from multiple, coordinated sources.

Components of DDoS Attacks

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

Component	Description
zombies	This 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 is 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	This refers to a group of zombies that have been infected using self-propagating malware (i.e., bots) and are controlled by handlers.
handlers	This 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 who is in control of the botnet and handlers.

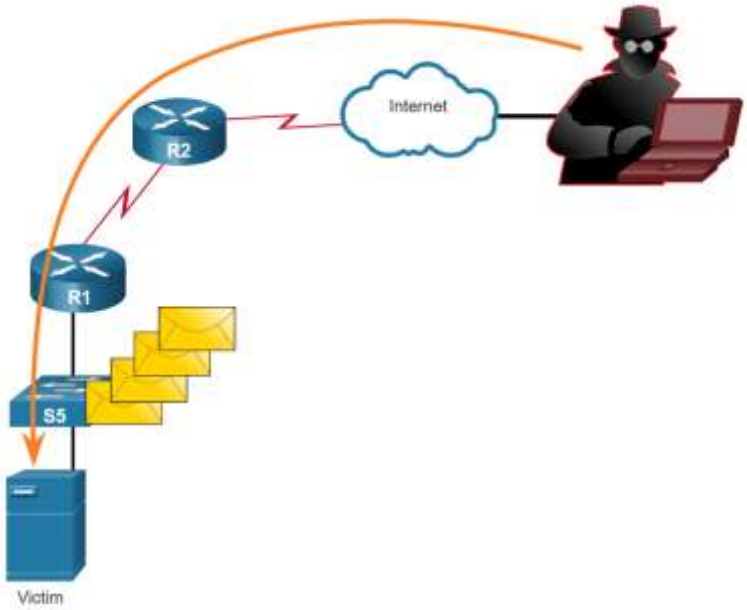
Video - Mirai Botnet

This video will demonstrate a DDoS attack using Mirai Botnet.

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.

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



Evasion Methods

Some of the evasion methods used by threat actors include:

Evasion Method	Description
Encryption and tunneling	This evasion technique uses tunneling to hide, or encryption to scramble, malware files. This makes it difficult for many security detection techniques to detect and identify the malware. Tunneling can mean hiding stolen data inside of legitimate packets.
Resource exhaustion	This evasion technique makes the target host too busy to properly use security detection techniques.
Traffic fragmentation	This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network.
Protocol-level misinterpretation	This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check.
Traffic substitution	In this evasion technique, the threat actor attempts to trick an IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data.

Evasion Methods (Cont.)

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

2.6 Network Threats Summary

What Did I Learn in this Module?

- Understanding network security requires you to understand the following terms: threat, vulnerability, attack surface, exploit, and risk.
- Four common ways to manage risk are risk acceptance, risk avoidance, risk reduction, and risk transfer.
- Threat actors include script kiddies, vulnerability brokers, hacktivists, cybercriminals, and state-sponsored hackers.
- Threat actors use a variety of attack tools including password crackers, wireless hacking tools, network security scanning and hacking tools, packet crafting tools, and many more.
- Categories of attacks include eavesdropping attacks, data modification attacks, IP address spoofing attacks, password-based attacks, denial-of-service attacks, man-in the-middle attacks, and others.
- Three common types of malware include are virus, worm, and Trojan horse.
- A virus spreads by inserting a copy of itself into another program.
- Trojan horse malware is software that appears to be legitimate, but it contains malicious code that exploits the privileges of the user that runs it.
- Worms are similar to viruses because they replicate and can cause the same type of damage. Viruses require a host program to run. Worms can run themselves.

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

- Ransomware denies access to the infected system or its data and then demands payment to release the computer system.
- Reconnaissance is information gathering where threat actors perform unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Access attacks exploit known vulnerabilities and include password attacks, spoofing attacks, trust exploitation attacks, and others.
- Social engineering is an access attack that attempts to manipulate individuals into performing unsafe actions or divulging confidential information and include pretexting, phishing, spam, impersonation, tailgating, shoulder surfing, dumpster diving, etc.
- There are two major types of DoS attacks: overwhelming quantity of traffic and maliciously formatted packets.
- DDoS attacks are similar in intent to DoS attacks, except that the DDoS attack increases in magnitude because it originates from multiple, coordinated sources.
- The following terms are used to describe DDoS attacks: zombies, bots, botnet, handlers, and botmaster.
- Evasion methods include encrypting and tunneling, resource exhaustion, traffic fragmentation, and more.


CISCO