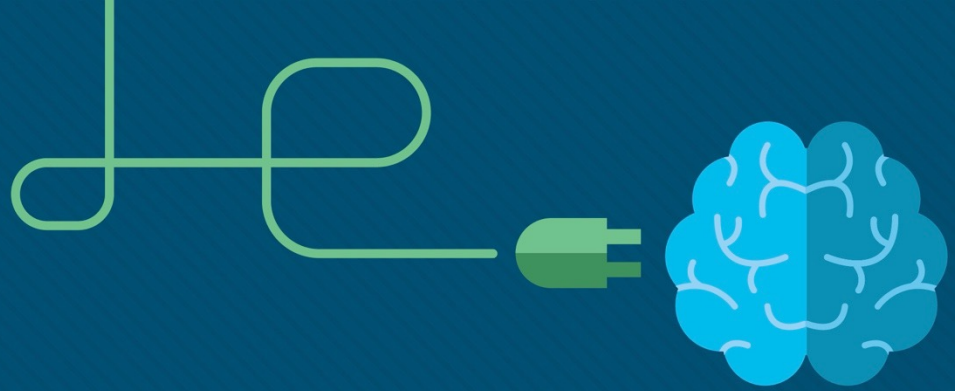


Chapter 5: Principles of Network Security

Information Security

Dr. Ayman Aljarbouh

5.1 Attackers and Their Tools

Module Objectives

Module Title: Attackers and Their Tools

Module Objective: Explain how networks are attacked.

Topic Title	Topic Objective
Who is Attacking our Network?	Explain how network threats have evolved.
Threat Actor Tools	Describe the various types of attack tools used by Threat Actors.
Malware	Describe types of malware.

Threat, Vulnerability, and Risk

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

Threat, Vulnerability, and Risk (Contd.)

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

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

Hacker vs. Threat Actor

‘Hacker’ is a common term used to describe a threat actor.

Hacker has a variety of meanings that are as follows:

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

Types of hackers:

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

Hacker vs. Threat Actor (Contd.)

White Hat Hackers:

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

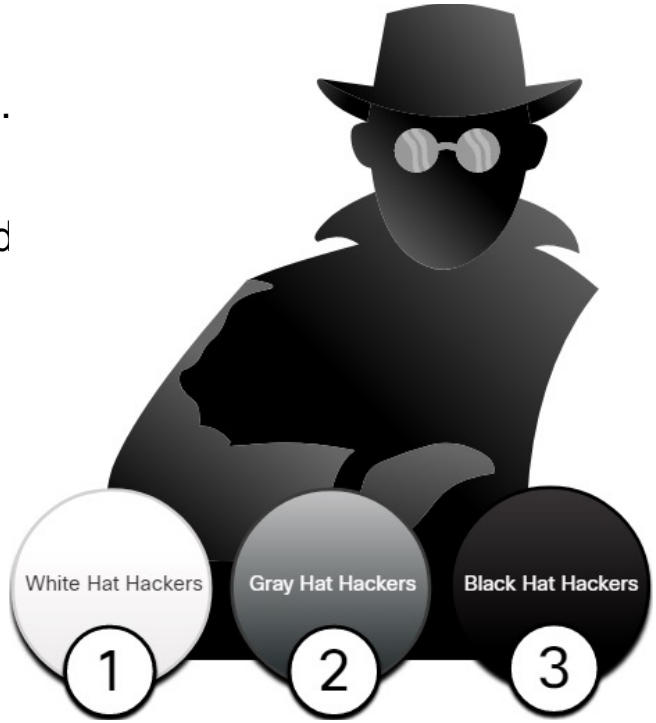
Gray Hat Hackers:

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

Black Hat Hackers:

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

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



Evolution of Threat Actors

Types of Threat Actors:

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

Who is Attacking Our Network?

Cybercriminals

- Money-motivated threat actors.
- Buy, sell, and trade exploits, and private information and intellectual property.
- Steal from consumers, small businesses, as well as large enterprises and industries.

Cybersecurity Tasks

- Develop good cybersecurity awareness.
- Report cybercrime to authorities.
- Be aware of potential threats in email and web
- Guard important information from theft.
- Organizations must take action and protect their assets, users, and customers.
- Develop cybersecurity tasks and implement those tasks on a reoccurring basis.

Evolution of Security Tools

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

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

Evolution of Security Tools (Contd.)

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

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

Evolution of Security Tools (Contd.)

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

Categories of Attacks

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

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

Categories of Attacks (Contd.)

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

Types of Malware

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

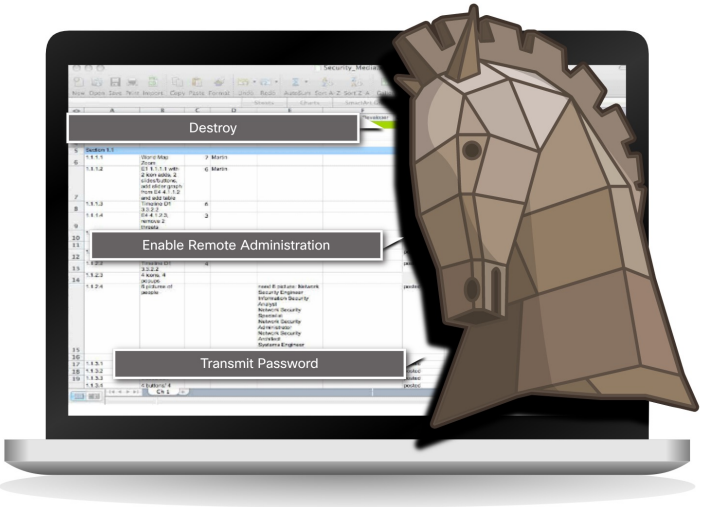
Viruses

- Type of malware that propagates by inserting a copy of itself into another program.
- Spread from one computer to another, infecting computers.
- Spread by USB memory drives, CDs, DVDs, network shares and email.
- Can lay dormant and activate at a specific time and date.
- Requires human action to insert malicious code into another program.
- Executes a specific unwanted, and often harmful, function on a computer.

Trojan Horses

- Malicious code that is designed to look legitimate.
- Often found attached to online games.
- Non-replicating type of malware.
- Exploits the privileges of the user that runs the malware.
- Can cause immediate damage, provide remote access to the system, or access through a back door.

Trojan Horses Classification

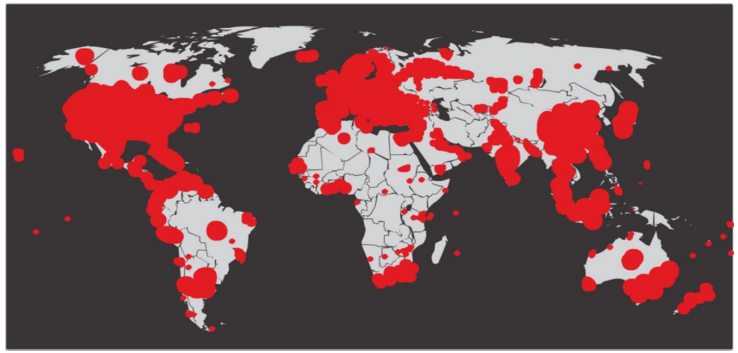


- **Remote-access Trojan horse** - Enables unauthorized remote access.
- **Data-sending Trojan horse** - Provides the threat actor with sensitive data, such as passwords.
- **Destructive Trojan horse** - Corrupts or deletes files.
- **Proxy Trojan horse** - Will use the victim's computer as the source 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.
- **DoS Trojan horse** - Slows or halts network activity.

Worms

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

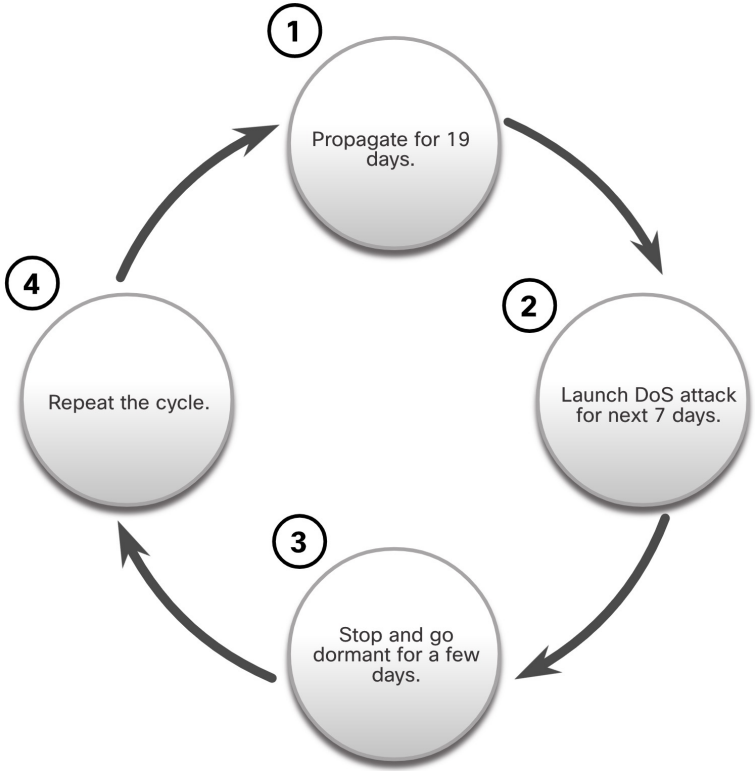
Initial Code Red Worm Infection



Code Red Infection 19 hours later

Worm Components

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



Code Red Worm Propagation

Ransomware

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

Other Malware

- Modern Malware
  - **Spyware** - Used to gather information about a user and send the information to another entity without the user's consent. Can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers.
  - **Adware** - Typically displays annoying pop-ups to generate revenue for its author. May analyze user interests by tracking the websites visited and 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. 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 without your knowledge to your contact list
  - Files have been modified or deleted
  - Increased CPU and/or memory usage
  - Problems connecting to networks
  - Slow computer or web browser speeds
  - Unknown processes or services running
  - Unknown TCP or UDP ports open
  - Connections are made to hosts on the Internet without user action
  - Strange computer behavior
- **Note:** Malware behavior is not limited to the above list.

New Terms and Commands

• Trojan horse • Rootkit Detectors • Exploit • Threat • Vulnerability	• State-Sponsored Hacking • Black Hat Hackers • Gray Hat Hackers • White Hat Hackers • Cybercriminals • Hacktivists

Lab 19 - Anatomy of Malware

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