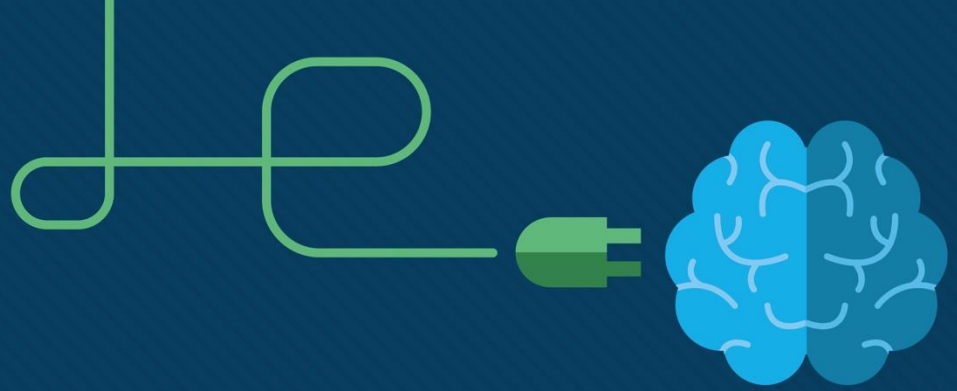


Module 13:Attackers and Their Tools

CyberOps Associate v1.0

Module Objectives

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

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

13.1 Who is Attacking Our Network?

Threat, Vulnerability, and Risk

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

Threat, Vulnerability, and Risk (Contd.)

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

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

Threat, Vulnerability, and Risk (Contd.)

- Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset.

Four ways to manage risk:

Risk Management Strategy	Explanation
Risk acceptance	When the cost of risk management options outweighs the cost of risk, the risk is accepted, and no action is taken.
Risk avoidance	This means avoiding any exposure to risk by eliminating the activity, thus resulting in losing any benefits from the activity.
Risk reduction	This reduces the exposure to risk. It is the most commonly used risk mitigation strategy. This strategy requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity that is at risk.
Risk transfer	Some or all of the risk is transferred to a willing third party such as insurance company.

Threat, Vulnerability, and Risk (Contd.)

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

Hacker vs. Threat Actor

'Hacker' is a common term used to describe a threat actor. Hacker has a variety of meanings that are as follows:

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

Types of hackers:

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

Hacker vs. Threat Actor (Contd.)

White Hat Hackers:

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

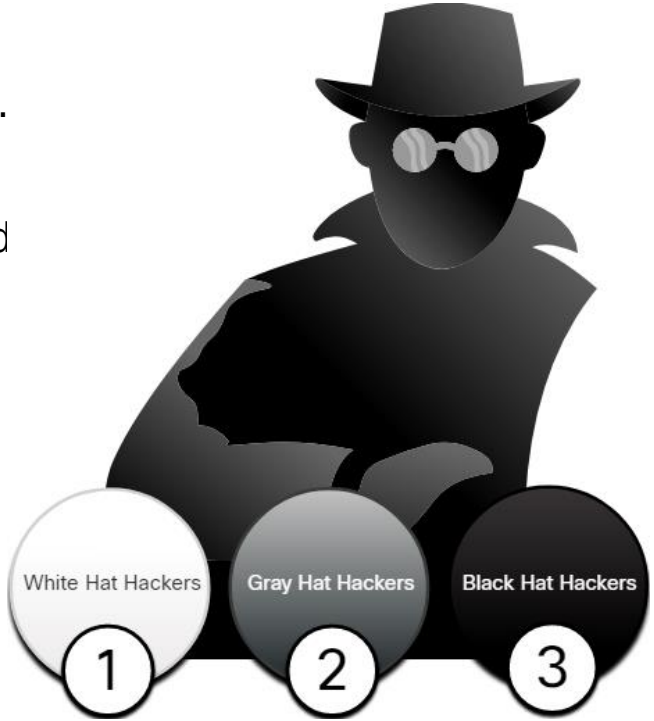
Gray Hat Hackers:

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

Black Hat Hackers:

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

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



Evolution of Threat Actors

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

Evolution of Threat Actors (Contd.)

Types of Threat Actors:

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

Cybercriminals

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

Cybersecurity Tasks

- Threat actors target the home users, small-to-medium sized businesses, as well as large public and private organizations.
- Hence, Cybersecurity is a shared responsibility which all users must practice to make the internet and networks safer and more secure.
- Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those mentioned in the figure.

Cyber Threat Indicators

Indicators Of Compromise (IOC)

- IOCs are the evidence that an attack has occurred and each attack has unique identifiable attributes.
- IOCs can be features that identify malware files, IP addresses of servers that are used in attacks, filenames, and characteristic changes made to end system software, among others.
- IOCs help cybersecurity personnel identify what has happened in an attack and develop defenses against the attack.

```
Malware File - "studiox-link-standalone-v20.03.8-stable.exe"
        sha256  6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0
        sha1    eb019ad1c73ee69195c3fc84ebf44e95c147bef8
        md5     3a104b73bb96dfed288097e9dc0a11a8
DNS requests
        domain  log.studiox.link
        domain  my.studiox.link
        domain  _sips._tcp.studiox.link
        domain  sip.studiox.link
Connections
        ip      198.51.100.248
        ip      203.0.113.82
```

Summary of the IOC for a piece of malware

Cyber Threat Indicators (Contd.)

Indicators of Attack (IOA)

- IOA focus more on the motivation and strategies behind an attack and the attackers to gain access to assets.
- IOAs helps to generate a proactive security approach that can be reused in multiple contexts and multiple attacks. Defending against a strategy can therefore prevent future attacks.

Threat Sharing and Building Cybersecurity Awareness

- Governments are now actively promoting cybersecurity.
- The US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost.
- CISA use a system called Automated Indicator Sharing (AIS) which enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified.
- The European Union Agency for Cybersecurity (ENISA) delivers advice and solutions for the cybersecurity challenges of the EU member states.
- The CISA and the National Cyber Security Alliance (NCSA) have an annual campaign in every October called National Cybersecurity Awareness Month (NCASM) to raise awareness about cybersecurity.

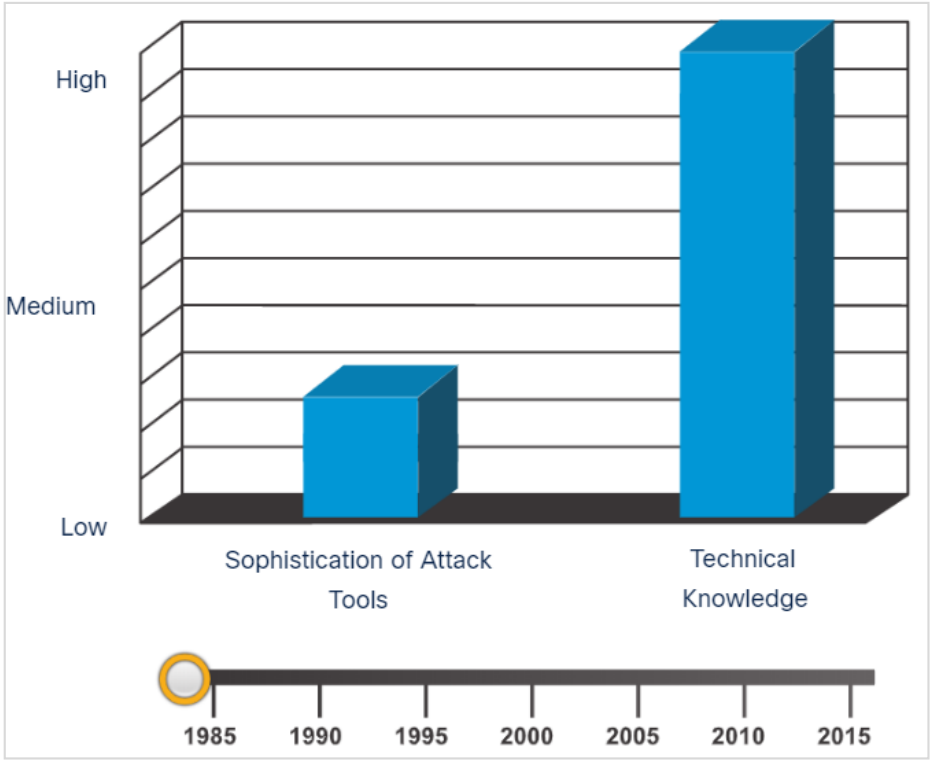
Threat Sharing and Building Cybersecurity Awareness (Contd.)

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

13.2 Threat Actor Tools

Introduction of Attack Tools

- To exploit vulnerability, a threat actor must have a technique or tool.
- Over the years, attack tools have become more sophisticated, and highly automated.
- These new tools require less technical knowledge to implement.
- In the figure, drag the white circle across the timeline to view the relationship between the sophistication of attack tools versus the technical knowledge required to use them.



Evolution of Security Tools

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

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

Evolution of Security Tools (Contd.)

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

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

Evolution of Security Tools (Contd.)

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

Categories of Attacks

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

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

Categories of Attacks (Contd.)

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

13.3 Attackers and Their Tools Summary

What Did I Learn in this Module?

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

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

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


CISCO