Network Security

/ Network Threats / Who is Attacking Our Network?

Who is Attacking Our Network?

2.1.1

Threat, Vulnerability, and 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.

Network Security

To better understand any discussion of 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. For example, your operating system and web browser could both need security patches. They are each vulnerable to attacks and are exposed on the network or the internet. Together, they create an attack surface that 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, as shown in the table:

Risk Management Strategy	Explanation

Risk Management Strategy	Explanation
Risk acceptance	This is when the cost of risk management options outweighs the cost of the risk itself. The risk is accepted, and no action is taken.
Risk avoidance	This means avoiding any exposure to the risk by eliminating the activity or device that presents the risk. By eliminating an activity to avoid risk, any benefits that are possible from the activity are also lost.
Risk reduction	This reduces exposure to risk or reducing the impact of risk by taking action to decrease the 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 an insurance company.

Other commonly used network security terms include:

- **Countermeasure** - The actions that are 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. A remote exploit does not require an account on the network to exploit that network's vulnerability.

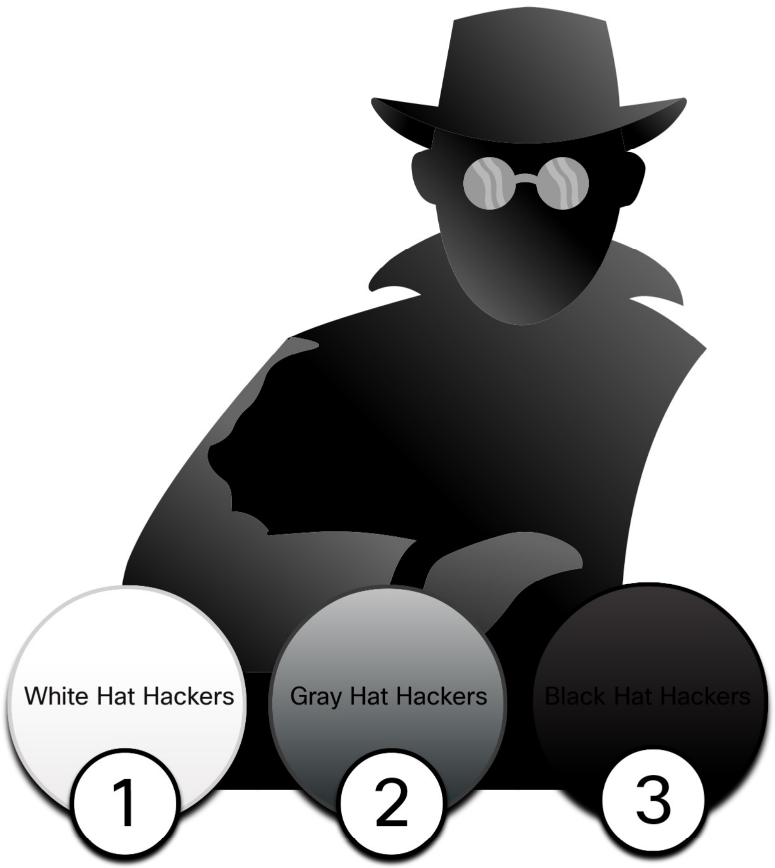
2.1.2

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, 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 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.

1. White hat hackers are ethical hackers who use their programming skills for good, ethical, and legal purposes. They may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers and security personnel who attempt to fix the vulnerability before it can be exploited. Some organizations award prizes or bounties to white hat hackers when they provide information that helps to identify vulnerabilities.
2. Grey hat hackers are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. An example would be someone who compromises a network without permission and then discloses the vulnerability publicly. Grey hat hackers may disclose a vulnerability to the affected organization after having compromised

their network. This allows the organization to fix the problem.

3. Black hat hackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks. Black hat hackers exploit vulnerabilities to compromise computer and network systems.

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.

2.1.3

Evolution of Threat Actors

Hacking started in the 1960s with phone freaking, or phreaking, which refers to using various audio frequencies to manipulate phone systems. At that time, telephone switches used various tones, or tone dialing, to indicate different functions. Early 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-1980s, computer dial-up modems were used to connect computers to networks. 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. Since then, general threat actor profiles and motives have changed quite a bit.

There are many different types of threat actors.

ⓘ Click the buttons to see definitions for the different types of threat actors.

Script kiddies Vulnerability brokers Hacktivists Cybercriminals State-sponsored

Script kiddies emerged in the 1990s and refers to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.

● ● ● ● ●

Network Security

2.1.4

Cybercriminals

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 personal information and intellectual property that they steal from victims. Cybercriminals target small businesses and consumers, as well as large enterprises and industries.

Network Security

2.1.5

Cybersecurity Tasks

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.

Cybersecurity checklist

☒ Trustworthy IT vendor

□ Security software up-to-date

□ Regular penetration tests

□ Backup to cloud and hard disk

□ Periodically change WIFI password

□ Security policy up-to-date

□ Enforce use of strong passwords

□ Two factor authentication

2.1.6

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

Network Security

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. A summary of the IOC for a piece of malware is shown in the figure.

```
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
```

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

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. For this reason, rather than informing response to a single threat, IOAs can help generate a proactive security approach. This is because strategies can be reused in multiple contexts and multiple attacks. Defending against a strategy can therefore prevent future attacks that utilize the same, or similar strategy.

2.1.7

Threat Sharing and Building Cybersecurity Awareness

Governments are now actively promoting cybersecurity. For instance, 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 uses 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 threats are verified. CISA offers many resources that help to limit the size of the

United States attack surface.

The CISA and the National Cyber Security Alliance (NCSA) promote cybersecurity to all users. For example, they have an annual campaign in every October called “National Cybersecurity Awareness Month” (NCASM). This campaign was developed to promote and raise awareness about cybersecurity.

The theme for the NCASM for 2019 was “**Own IT. Secure IT. Protect IT.**” This campaign encouraged all citizens to be safer and more personally accountable for using security best practices online. The campaign provides material on a wide variety of security topics including:

- 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

The European Union Agency for Cybersecurity (ENISA) delivers advice and solutions for the cybersecurity challenges of the EU member states. ENISA fills a role in Europe that is similar to the role of CISA in the US.

Network Security

2.1.8

Check Your Understanding - What Color is my Hat?

Click the appropriate response for each characteristic to indicate the type of hacker it describes.

I hacked into ATM machines without the manufacturer's authorization and discovered several vulnerabilities. I then contacted the ATM manufacturer to share my findings with them.

White Hat | **Gray Hat** | **Black Hat**

I secretly installed a debit card skimmer device on an ATM machine. A few days later, I retrieved it and it had captured the account numbers and pins numbers of over 1000 people. I then proceeded to transfer money from their accounts to an offshore bank account.

White Hat | **Gray Hat** | **Black Hat**

My job is to identify weaknesses in the computer system in my company.

White Hat | **Gray Hat** | **Black Hat**

Network Security

I used malware to compromise several corporate systems to steal credit card information and sold that information to the highest bidder.

White Hat | **Gray Hat** | **Black Hat**

During my research for security exploits, I stumbled across a security vulnerability on a corporate network that I am authorized to access.

White Hat | **Gray Hat** | **Black Hat**

While I was searching for security vulnerabilities, I gained unauthorized access to a company’s network and left the message “Your security is flawed”.

White Hat | **Gray Hat** | **Black Hat**

I am working with technology companies to fix a flaw with DNS.

White Hat | **Gray Hat** | **Black Hat**

Check | Show Me | Reset

2.0
Introduction

2.2
Threat Actor Tools

Network Security