Cybersecurity Fundamentals

Cybersecurity: On the Offense

Threat actor groups

25 Minutes

Module overview

This module focuses on the "offensive" side of cybersecurity, meaning the cyber attackers and their techniques. How do they hack? What could go wrong? You will learn about these topics:

- Types of cyber attacker groups
- Types of cyber attacks
- Steps in a typical cyber attack sequence, using the Lockheed Martin Cyber Kill Chain framework
- Attacker tactics and techniques, using the MITRE ATT&CK matrix
- How the cyber crime economy works
- Social engineering and common social engineering attacks
- Open source intelligence (OSINT) and common sources that cyber attackers use
- Technical scanning methods
- High profile case studies of cyber attacks to recognize what is possible and going on in the world

Threat actor groups

Cybersecurity professionals must be aware of the different types of threat actor groups, or cyber attacker groups. These are diverse groups and they vary substantially in motivation, resources, and techniques. Let's review and compare the five main types of cyber attacker groups.

Group 1: Script kiddie

The first group is the least advanced, the script kiddie. The term "script kiddie" refers to someone who uses programs, frequently basic hacking tools, without truly understanding what is going on behind the scenes. They may display a basic understanding of networking and programming, but lack technical skills as well as patience or strategic intent.

SUMMARY

- In practice, this demographic is mostly teenagers or young adults, who are self-taught via forums, videos, and experimentation.
- For many, the main motivations for their hacking efforts are reputation, status in the eyes of the hacking community, entertainment, or settling grudges.
- From a resourcing standpoint, script kiddies rely on off-the-shelf penetration testing tools and publicly available exploits.
- In most cases, they are very underfunded. They tend to display little trade-craft knowledge beyond that of basic proxies or disposable accounts.
- From a defensive standpoint, organizations must ensure that their patching schedule is effective. Should an easy exploit be developed, it is very likely that it will be deployed at some point. Defenses must be sufficient to ensure that another target appears easier which should be a sufficient deterrent.

Profile of a script kiddie

Who are they?	What is their objective?
Self-taught individuals, typically teenagers	Seek reputation enhancement or attack for fun
What resource do they have?	**How do you protect against them?**
Little funding, little or no technical expertise and assistance, may use free tools written by others	Ensure patching schedule is effective and basic perimeter defenses are up to date

Group 2: Hacktivist

The second group is the hacktivist. Hacktivist is a term which combines "hacker" and "activist". Hacktivists seek a political or economic change and will use hacking to achieve it.

SUMMARY

- The key, defining attribute of hacktivists is that they are driven by ideological reasons.
- The group of people who make up hacktivist groups ranges greatly. Like the script kiddie group, they are filled with impressionable amateurs, but when causes align on a highly topical issue, they are joined by more experienced members within the security community.
- The motivations of hacktivist groups are defined by their aims, which vary enormously. Generally, it involves supporting one cause the individuals believe in. This could be a side in the Middle East conflict, political activities, and so on.
- The most famous example of this group would be the hacking collective called **Anonymous (https://en.wikipedia.org/wiki/Anonymous_(group))**. Anonymous is a decentralized international hacktivist group that is known for cyber attacks against several governments, government institutions and government agencies, and corporations.
- Hacktivists use a range of basic tools which can be very effective when done at scale. Denial of Service (DoS) programs are a notable example in this area.
- While a single script kiddie poses little threat, several hundred launching parallel attacks can be significantly more challenging to deal with.
- As an organization, being astute is very important. Should an organization operate business in a sensitive area (e.g., animal testing, political causes), then it is possible it may come under a sustained attack from hacktivists at some point. Having good defenses will not be enough to deter all attacks, so organizations should plan methods to cope with a sustained attack.

Profile of a hacktivist

Who are they?	What is their objective?
Driven idealists forming loose coalitions	Want to bring about a change
What resource do they have?	**How do you protect against them?**
Operate at scale with varying tools and biggest attribute is size	Ensure defenses can cope with an extended disruptive attack

Group 3: Criminal gang

As long as there is easy money to be made, criminals will always be a problem for society. The internet's creation has created a new method for criminals to prey on victims with an unprecedented scale, range, and ease. Rather than run risks in person, aspiring criminals can send out millions of infected emails from halfway around the world and secure a ransom from a victim before transferring funds into cryptocurrencies to evade conventional policing methods. Capturing these criminals is extremely taxing and, due to international laws, securing a prosecution is near impossible. Sadly, most criminals are aware of these facts.

SUMMARY

- This is the fastest growing group and as a result, it is the broadest.
- Within the group, there are a range of activities. Gangs could be running ransomware attacks (where a victim is forced to pay to secure access back to their resources), committing extortion (where the threat of a large attack secures protection money), committing conventional theft of customer data or intellectual property, and so on.
- Being a cyber-based criminal is a full-time and potentially quite lucrative proposition. Gangs can range from a few individuals all the way to multinationals with hundreds of members. Within each gang, there are frequently specialists and they can trade information on the dark web. Consequently, criminal gangs are quite advanced and well-organized.
- From a resourcing standpoint, criminal gangs frequently develop and deploy their own malware. They even in some cases rent access to others who may be less technical. Like all software sales, they advertise, host reviews, and even have tech support. Criminal gangs have access to substantial amounts of infrastructure, such as servers and domains.
- To protect against a criminal gang, effective defenses should exist for critical assets. While discovering ransomware on an employee's laptop may be inconvenient for the company, discovering ransomware on a production sever could be devastating.
- From a financial perspective, the criminals will always adopt the quickest and easiest get-rich-quick scheme.

Profile of a criminal gang

Who are they?	What is their objective?
Groups of people in national and international teams	Driven by financial motivations
What resource do they have?	**How do you protect against them?**
Broad range of tools and equipment, bought and traded on the dark web	Need to have a fully trained workforce with protections around critical assets and back-ups

Group 4: Nation state hacker or advanced persistent threat (APT)

The next group, and one that receives the most media attention, perhaps unduly, is the nation state attackers. Many military organizations around the word now consider cyberspace a fifth sphere of conflict alongside sea, land, air, and space. Many nations have demonstrated the ability to project power across national borders to a great and expanding variety of consequences.

SUMMARY

- The role of nation state hackers is to provide a strategic advantage to their respective country. This may range from reconnaissance and information collection (e.g., traditional spying/signals intelligence) all the way to information subversion and manipulation.
- Members of these organizations are well-educated or trained and cover a range of backgrounds. They work full-time and typically work on the cutting edge within their respective fields.
- Their motivations are typically aligned closely with political or strategic objectives. A recent example of this were the Russian activities concerning the 2016 US presidential election. The aim was to interfere with the election as well as increase political and social discord.
-

From a resourcing standpoint, nation state hackers have access to advanced research, dedicated infrastructure teams, and tremendous political support.

- Protection against determined nation state hackers is tremendously challenging for organizations. Doing so effectively requires fully capable and coordinated security defenses.

Profile of a nation state hacker

Who are they?	What is their objective?
Highly trained and educated specialists	Follow strategic, multi-year plans on a wide range of issues
What resource do they have?	**How do you protect against them?**
Very large budgets, cutting-edge tooling, and leading-edge research	Incredibly difficult; need fully coordinated defenses around every aspect of the organization

Group 5: Malicious insider

The final group that is arguably the most concerning, is that of the malicious insider. The insider refers to a member within an organization that either intentionally or otherwise acts against it.

SUMMARY

- Malicious insiders can either start with a negative mindset within an organization or become resentful after a period of time.
- Motivations vary greatly and can cover just about everything, with financial interests and bitterness being two of the most common. In other cases, notoriety or fame can be motivators.
- A common example of an insider is an employee being blackmailed into allowing someone access to the employee's corporate accounts. Another common example is a disgruntled employee who steals corporate secrets before being fired. Perhaps the most famous insider attack of all time was Edward Snowden, who stole a large amount of National Security Agency (NSA) files from the US before giving them to WikiLeaks.
- Insiders do not usually rely on technical skills to execute their attacks. While some may shoulder surf or use social engineering to gain access from others, typically they use their own corporate access and permissions.
- Defense against insiders is best achieved by vetting employees, effective management, and then technical controls. Resorting to technical controls is frequently seen as a “get out of jail free card” for many companies and it frequently fails because you are, after all, trying to stop users who are extremely familiar with the system. In many cases, there are a lot of warning signs before somebody launches an inside attack. For instance this could be working alone, expressing resentment, failing in quality of work, or doing unexplained activities. Picking up on these signs is very important.

Profile of a malicious insider

Who are they?	What is their objective?
Staff members who work against an organization's own interests, either deliberately or accidentally	Seek revenge or have financial motives
What resource do they have?	**How do you protect against them?**
No budget or resources required; use granted access	Monitor staff carefully and ensure organization's culture is effective to prevent issues

> **Note**: Sometimes these descriptions of the types of cyber attackers are not always precise. In operations, hacktivists might recruit script kiddies and nation state hackers might recruit criminal gangs. Also, some cyber attackers will disguise their work to appear less advanced than they are. These facts can make it difficult to attribute threats to the correct party.

Offensive security researcher

You've learned about five common types of cyber attackers who have personal motivations or threatening, often illegal motivations. But, there are also individuals out there who are considered **offensive security researchers**. An offensive security researcher chooses to use, and monetize, their skill set for good, rather than criminal or exploitative activity. Often called "**ethical hackers**," they take on a real hacker mindset to use the same methods as real-life attackers, but with the goal of testing and fortifying systems to help clients and consumers be better protected from the real thing.

Working in cybersecurity today

Here are two leading cybersecurity experts who use their skill sets to offer valuable and often highly-paid advice and knowledge to organizations around the world.

Brian Krebs	**Georgia Wiedman**
Brian is a celebrated journalist who investigates cyber crime. He kicked off his career as a reporter for The Washington Post, where he wrote for the Security Fix blog from 1995 to 2009 and pushed the boundaries of cyber security reporting. Today, he owns the hugely popular blog **Krebs on Security (https://krebsonsecurity.com/)** and was named 2019's "**Cyber Security Person of the Year (https://krebsonsecurity.com/2019/12/ciso-magazine-honors-krebsonsecurity/)**" by CISO MAG. **Fun fact:** Brian's interest in cybersecurity was ignited after his entire home network was taken captive by a Chinese hacking group.	Georgia is a serial entrepreneur in the cybersecurity space and has worked as a penetration tester, security researcher, speaker, trainer, and author. She has gained a large following through her work in smartphone exploitation and mobile device security as the founder and CTO of **Shevirah (https://www.shevirah.com/)**. **Fun fact:** Georgia is an angel investor and has spoken and trained audiences around the world at venues like the NSA, West Point, and Black Hat.

This is the end of the lesson. Be sure to select the "**I've checked it out**" box to take a mini quiz to check your understanding of this lesson. You will be presented with three scenarios to then identify the correct type of cyber attacker group. This is required for lesson completion.

Types of cyber attacks

20 Minutes

There are many methods in which a cyber attacker can enter and exploit a system. Often, attacks are not technical at all, but rather an exploitation of how *humans* interact with the system in a flawed and vulnerable way. In this lesson, we have selected common types of cyber attacks. This is a representative sample to provide you with a few illustrative examples, rather than a comprehensive list. Let's examine these in greater depth.

Denial of service (DoS) attack

- A DoS attack is any type of attack that causes a complete or partial system outage.
- The means to perform a DoS attack can range from causing a system to crash to making it unreachable or incapable of continuing work due to abnormal levels of forwarded network traffic.

EXAMPLE

An attacker could send a maliciously formatted file to a server that causes it to overload. An example of this is a **billion laugh attack (https://en.wikipedia.org/wiki/Billion_laughs_attack)**, in which an XML file references itself, expanding to a considerably larger file.

Distributed denial of service (DDoS) attack

- A DDoS attack is a DoS attack that comes from more than one source at the same time.
- The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker.
- According to research, tens of millions of computers are likely to be infected with botnet programs worldwide.

EXAMPLE

An attacker could send a large number of page requests to a web server in a short space of time, overloading it. A similar impact is observed with ticket sales websites where a spike in user demand can overload systems.

Phishing attack

- A phishing attack is the practice of sending messages that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.
- It combines social engineering and technical trickery.
- Unsuspecting users open the email and may provide protected information or download malware.

EXAMPLE

An attacker could send an email with a file attachment or a link to a fake website that loads malware onto a target's computer.

Spear phishing attack

- Spear phishing attacks are a very targeted type of phishing activity.
- Attackers take the time to conduct research into targets and create messages that are personal and relevant, and thus likely more effective.

EXAMPLE

An attacker collects a target's details from social media and calls the target pretending to be a representative from the bank. The attacker advises the account is compromised and asks the target to transfer money to a "safe" bank account. The attack is convincing because of the attacker's apparently legitimate knowledge.

Malware

- Malware is a catch-all term for malicious software. It is any software designed to perform in a detrimental manner to a targeted user without the user's informed consent.
- It often triggers secretly when a user runs a program or downloads a file, which can often be unintentional.
- Once active, malware can block access to data and programs, steal information, and make systems inoperable.

EXAMPLE

Within the various types of malware, you will find examples related to their function, such as **keyloggers** (which captures a victim's keystrokes) or **ransomware** (which holds a victim's files captive in exchange for a ransom payment).

Man in the middle (MitM) attack

- A MitM attack occurs when hackers insert themselves in the communications between a client and a server.
- This allows hackers to see what's being sent and received by both sides.

EXAMPLE

An attacker could set up a "free" WiFi hot spot in a popular public location. Anyone who connects to that WiFi network could have their communications examined by the attacker, who may redirect victims to fake log-in screens or insert advertisements over webpages.

Domain name system (DNS) attack

- DNS is one of the core protocols used on the internet.
- Basically, the DNS protocol allows a computer to resolve a domain to an IP address, which allows a user to, for example, reach BMW's main website by typing "bmw.com" instead of writing an IP address that is hard to remember.
- DNS is used almost everywhere. As a core protocol of the internet, lots of attack vectors directly target DNS, including DNS spoofing, domain hijacking, and cache poisoning (just to name a few).

EXAMPLE

In 2016, the DNS service provided by a company called Dyn was attacked. This resulted in major outages across most of the US, leaving millions of Americans unable to access or use internet services.

Structured query language (SQL) injection

- SQL allows users to query databases.
- SQL injection is the placement of malicious code in SQL queries, usually via web page input. A successful attack allows common commands to be run. This can include deleting the database itself!
- SQL injection is one of the most common web hacking techniques.

EXAMPLE

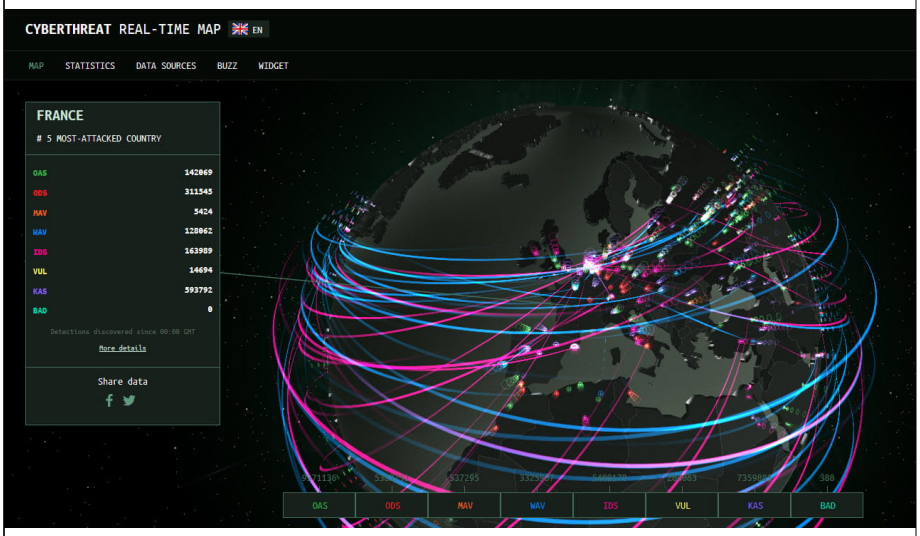
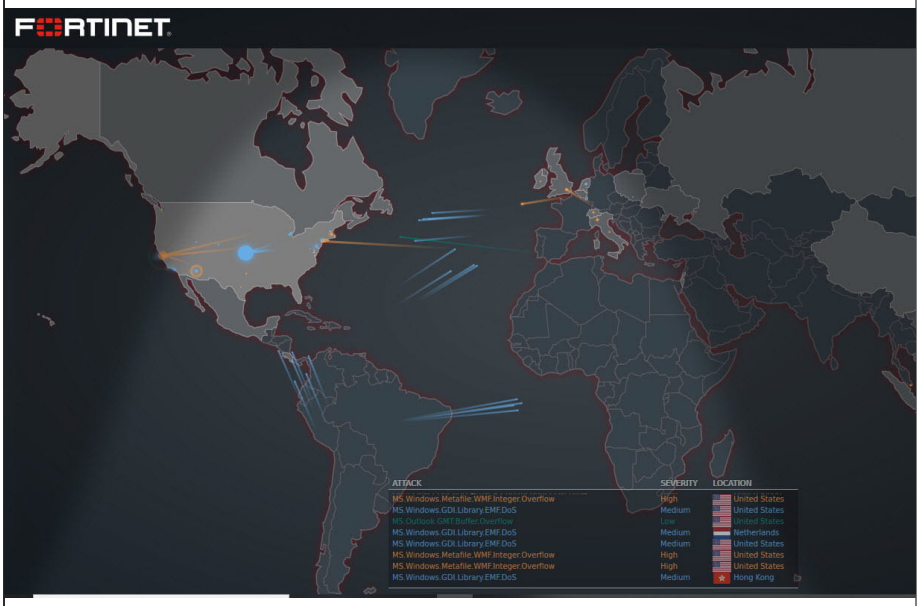
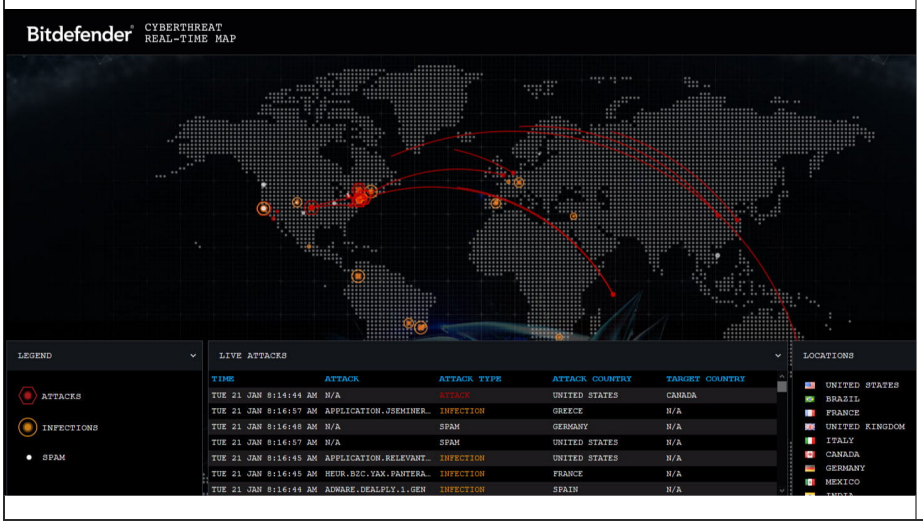
In the UK, two teenagers managed to target TalkTalk's website in 2015 to steal hundreds of thousands of customer records from a database that was remotely accessible.

This represents a handful of the many types of cyber attacks impacting organizations and individuals today. You will find DoS attacks on organizations are commonly reported in the news, phishing attacks are the most effective on a personal basis, and malware attacks are increasing in number and constantly evolving.

Activity

Fact: No person, organization, or country is immune to the dangers of cyber attacks.

In this activity, you can put on your explorer hat to access the following real-time maps and statistical visualizations of cyber attacks occurring around the world. Take a moment to access each site. It may take a moment to load. Check out the statistics. See just how many attacks are being documented across the globe! Right now!

1. Go to the Kapersky Cyberthreat Real-Time Map (https://cybermap.kaspersky.com/) 	• Navigate around the interactive world map to click and visit a specific country to view its latest data. • **Find the most attacked countries!** • You can change the language at the top of the web page. • Roll-over the color-coded types of threats and attacks.
2. Go to the Fortinet Threat Map (https://threatmap.fortiguard.com/) 	• Watch the attack details that scroll at the bottom of the screen. • **Figure out where most attacks are happening right now, before your eyes!** • This is a sub-set of data. Select **?** to view the legend of types of attacks displayed. Select **i** to learn more.
3. Go to the Bitdefender Cyberthreat Real-Time Map (https://threatmap.bitdefender.com/) 	• View the live attacks happening across the map for the selected country locations. • **Check out the various instances of spam, threats, and attacks!** • Notice that there is an "attack country" and "target country".

This is the end of the lesson. Be sure to select the "**I've checked it out**" box to take a mini quiz to check your understanding of this lesson. You will be presented with three descriptions to then identify the correct type of cyber attack that it represents. This is required for lesson completion.

Structure of a cyber attack

20 Minutes

As computer systems change so do the ways in which they can be compromised. For example, a cyber attack may rely on a computer running an outdated version of a web browser to be vulnerable to a specific piece of malware. Once the software is patched, that attack cannot be repeated in the exact same manner. However, while individual techniques may evolve with time, the overall **structure of a typical cyber attack** can be examined. In this lesson, we'll review a couple of ways this has been done over the years so you have a basic understanding.

> **Note**: This is meant to provide you with a quick overview and you can choose to explore more if you would like.

Introducing the Lockheed Martin Cyber Kill Chain® framework

Lockheed Martin Corporation (https://www.lockheedmartin.com/en-us/index.html) is an American global aerospace, defense, security, and advanced technologies company. Researchers at Lockheed Martin determined that there are parallels between the typical U.S. military concept of a "kill chain" and intrusions within digital networks. The word "chain" is used here to indicate a set of steps that must be completed in order, in which each step depends on the previous step's completion. Here is a walk-through of the seven steps in the **Cyber Kill Chain framework (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)** so you understand a typical cyber attack sequence.

Source: **Lockheed Martin, the Cyber Kill Chain® framework (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)**

1. **Reconnaissance**: During this stage, the attacker gathers information about the target. This can be achieved through probing digital servers, speaking with people close to the target, or just reading the news!
2. **Weaponization**: Once a specific vulnerability has been identified, a piece of malware is designed to exploit it. This process can range from downloading a sample of a database, purchasing a tool from a 3rd party, or developing something custom.
3. **Delivery:** The chosen malware must be sent to the target in some manner. Despite progress over the years, the most common method is still via email. Other methods can include website downloads and infected or modified USB devices.
4. **Exploitation**: Once malware is given to the target, it activates and performs a series of instructed steps. How this occurs is highly variable and depends on many details about the programs and operating system in use. This process is known as "exploiting a

vulnerability" and the software used to do it is known as **exploit code** or an **exploit.**

5. **Installation**: The malware attempts to get some element of persistence within the target system. This can be achieved through the creation of back doors, which can include creating new accounts, installing remote access programs, or introducing new vulnerabilities into the system. These factors mean that if the original vulnerability is patched, it is too late for the defender as the attacker's access remains.
6. **Command and Control (C2)**: A method for the attacker to communicate with the compromised systems must be established. This enables instructions and upgrades to be sent to the target and for data to be sent back to the attacker. This can be done using websites, direct connections, and even Twitter.
7. **Actions on Objectives**: Once all the previous steps have been completed, the attacker is free to complete the original intent. This could range from stealing data, modifying data, or destroying key system elements.

Introducing the MITRE ATT&CK matrix

MITRE (https://www.mitre.org/)is an American non-profit organization dedicated to solving problems for a safer world. It brings forward innovative ideas in a variety of areas including cyber threat sharing and cyber resilience. MITRE collected a set of tactics, techniques, and procedures (TTP) that cyber attackers have been using to develop **ATT&CK**. It stands for Adversarial Tactics, Techniques, and Common Knowledge. It is pronounced as "attack". This collected knowledge is presented in a matrix to help organizations examine cyber attacks in a simplified form. The **ATT&CK matrix (https://attack.mitre.org/)** is open and available to any person or organization for use at no charge.

The following graphic is a sample of the **ATT&CK matrix (https://attack.mitre.org/)**. You can see it is quite comprehensive.

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery

The column headers identify an **attacker tactic**. Each tactic can be considered as an **attacker's objective**. Then, the list under each column are the many **techniques** that the cyber attacker can use to achieve the tactic or objective. These link to more information.

> **EXAMPLE**
>
> A cyber attacker may want to gain **credentialed access** to a system. This is a tactic. In this scenario, if the attacker identifies poor logging and no account lockouts are in use, the attacker could choose to use the **Brute Force (https://attack.mitre.org/techniques/T1110/)** technique. In this technique, a program is run, which can try millions of username and password combinations until a successful one is identified. Should the chosen technique be unsuccessful, an attacker can simply switch to another approach and continue trying.

Importance of understanding cyber attacks

During a cyber attack, attackers can be quite persistent. It is rare that a single interruption to their attack will cause them to give up. Instead, it can be quite helpful to view cyber attacks as part of a longer campaign. Many attacks can last for months with attackers spreading their influence and defenders trying to identify and stop them. Good defenders will attempt to anticipate an attacker's next move and frameworks such as the MITRE ATT&CK matrix help them to achieve this.

Activity

Find an attacker tactic and techniques that intrigues you by visiting the **MITRE ATT&CK matrix (https://attack.mitre.org/)**.

Please type your answer to each question in the boxes. Your answers are just for you and are only saved in this course for you. Be sure to click **Save Text**.

1. First, select the column headings to read the details to better understand a few tactics. Then, pick **one tactic** you want to explore and study it. Which tactic did you pick and how would you explain it to someone who is not familiar with this topic?

Save Text Save Text

2. Once you have done this, examine **two techniques** that attackers utilize to achieve your selected tactic. What are the advantages of each technique and is one technique "easier" than the other?

Save Text Save Text

Funding and profitability of cyber crime

10 Minutes

While some cyber attackers are motivated by activism or national interest, the main driver of cyber crime is profitability. In this lesson, we'll examine a few methods of how cyber criminals make and use their money.

Underground ecosystem

The first element that is vital to the cyber crime economy is a thriving international marketplace made up of hundreds of forums, platforms, and systems. Within this market environment, criminals buy and sell data, identities, and tools to make profit. For example, a very common area of interest is money laundering. Should cyber criminals steal some money from a victim, they need to have a method to make the stolen money usable and ideally untraceable. They can do this by using a 3rd party specialist in an outsourcing-like manner.

Like a traditional economy, specialism drives efficiencies and allows criminals to focus on what they each do best.

Initial cash injection

So, with a marketplace set up, how do criminals get money? Below are three general methods by which they can achieve this.

Stolen from victim	• The most direct method is criminals attempting to steal money from their targeted victim. • While this can be done through compromising banking systems or compromising accounts, the most common manner is through fraud or deception. • These scams are often the "tech support scam" or other similar tricks intended to persuade a victim to give the criminal a financial benefit such as giving away bank details and personal information.
Criminal for hire	• Sometimes criminals offer their services to carry out illegal tasks to regular people and organizations. • This is commonly done using a denial of service (DoS) attack that attempts to overload key parts of a service. For instance, a criminal may offer the ability for an organization or individual to disable a competitor or rival. • In this model, the criminal does not take money from the victim. Instead, the criminal gets paid by the organization or individual. • Another example of this is computer misuse in a mercenary style. Imagine a person hiring a criminal to steal a competitor's key intellectual property or destroy a rival's databases.
Extorted from victim	• In this model, the criminal gains the ability to disrupt a victim by disabling key systems or threatening to divulge sensitive data. • In recent years this has become popular with the advent of ransomware. In a ransomware attack, a victim's key systems and files are encrypted in such a manner that renders them inoperable. To restore the systems and files, the victim is asked to pay the criminal a ransom to receive the decryption key. • Other extortion themed approaches can include threatening to divulge organization or customer data such as embarrassing executive emails or customer databases.

Cryptocurrency

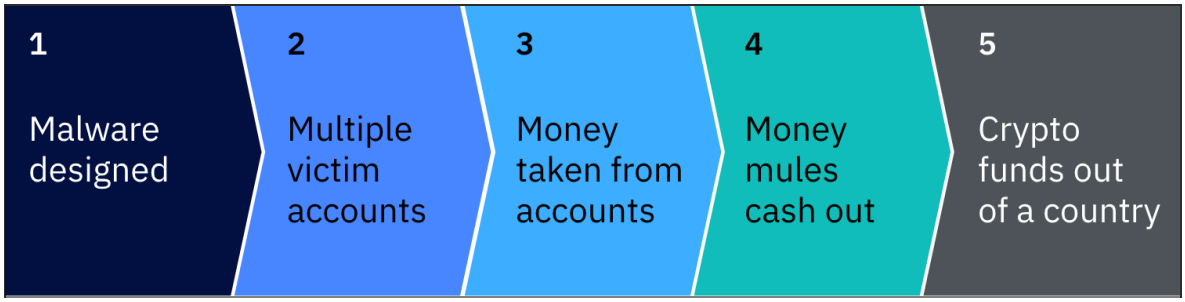
Over the last few years, there has been a rapid increase in cryptographically controlled currencies called **cryptocurrencies**. The original cryptocurrency, **Bitcoin (https://bitcoin.org/en/)**, proposed a new method for monetary exchange based on a shared ledger called a Blockchain. This concept has been built upon by subsequent new currencies that have been built in recent years.

When using an anonymous ledger outside of government control, payments are designed to be near impossible to regulate or block. This makes cryptocurrencies unbelievably useful for money laundering or for other criminal marketplace activities.

One notable consequence of cryptocurrencies was the rapid growth of ransomware. In this business model, the victim has to pay the attacker. When this was originally done with monetary substitutes such as gift cards, the process was slow and unreliable. Now, with the use of cryptocurrencies, it is easier for victims to make concealed payments.

The ecosystem in action

Let's look at a hypothetical case study drawing all of the monetary elements together. In this scenario, we'll follow an attack campaign across the life cycle. Follow the money trail!



1. The first stage of the journey involves a criminal gang producing a piece of malware which records keystrokes and screen shots.
2. The malware authors buy a list of known email addresses from another party and send out the malware as an email attachment. The objective is for the malware to work on the victims' machines so their banking details and other passwords can be stolen and sent to the malware authors. At this point, their work is done. They have a list of passwords and banking logins.
3. Now, the malware author may attempt to "cash out" themselves or sell the details to another gang to finish the process.
4. The criminal gang can attempt to login using the credentials and make transfers to money mules they have worked with previously. In this case, the mules are typically gullible or desperate individuals who have agreed to allow a stream of money through their accounts in exchange for payment.
5. To finish the process, the criminal gang could force the mules to buy and transfer cryptocurrencies to accounts controlled by the gang. As soon as this done, the campaign is complete. Should law enforcement investigate the crime, the trail often ends with only the money mule being traceable.

Social engineering

15 Minutes

In this course, you are learning about the importance of people when designing secure systems. People, whether they are employees or customers, are often mismanaged in security environments. They may be given confusing or contradictory advice, prevented from following good practices, or just become fatigued. All of this puts people in a vulnerable position to potentially be taken advantage of by a prospective cyber attacker. In this lesson, we'll highlight social engineering and techniques that attackers use. Rather than hacking a system, let's examine how they hack the individual instead!

What is social engineering?

Social engineering is the art of making someone do what you want them to do. It overlaps heavily with academic fields involving psychology, biology, and even mathematics!

In cybersecurity, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that could then be used for fraudulent purposes. Basically, how could someone trick another person into giving up something that is private? Social engineering attacks are the dark art of using social interactions to trick someone into making a security mistake.

Social engineering tactics can be employed in-person, over the phone, or online through websites, email, and social media.

Once an attacker can make an individual perform a certain action, then the attacker can gain access to sensitive systems, steal assets, or advance a more complex attack. This notion of focusing on persuading or tricking people may sound unreliable. But, there are many case studies that show social engineering is an incredibly powerful technique for attackers.

> EXAMPLES
>
> Effective social engineering tactics can result in defrauding vulnerable individuals of their savings through **scams and confidence tricks**. For organizations with physical buildings, social engineering also includes **tailgating**, or closely following, individuals in order to gain access to secure areas.

Why does social engineering work?

Social engineering works because humans are imperfect. There are two key elements to this: our decisions are irrational and our decision making is flawed. Let's look at each in greater detail.

Irrational behavior

We can all exhibit irrational behavior as shown by making decisions that do not further our long-term interests. If everyone was focused and logical, then we would not have vices. For instance, no one would play the lottery and we would eat healthy all the time. This is very far from the case.

In social engineering, drivers for short term gratification or greed can be utilized to manipulate a target. These targets are putting themselves at risk and often committing crimes unknowingly.

> EXAMPLES
>
> This is best shown when criminals persuade young adults to act as money launderers for gangs. There are also many other get-rich-quick schemes online. The victims in this case are **baited** into the scheme with false promises.

There are also cases where idleness is a great asset for social engineering. Taking shortcuts and the tendency to avoid rules are quite effective to use as a social engineering tactic on a target.

> EXAMPLES
>
> Within certain organizations, employees might skip a long business process like verifying caller identities or getting the right levels of approvals to grant access rights.

Flawed decision making

Human decision making varies greatly throughout the day and depends on changing circumstances. For instance, the colors on display in a room, the presence of other people, the amount of noise, and the temperature all have a measurable, biological impact on individuals and change their decision-making processes. Attackers benefit from affecting a target's decision making to achieve a result.

> EXAMPLES
>
> Attackers use time restrictions to create a sense of urgency. In addition, attackers may confuse a target by impersonating a trusted authority figure or even pretend to be a potential love interest. When an attacker builds up a false reason to engage with a target this tactic can be labelled as **pretexting**.

All these factors impact a target's ability to make a good decision or even identify they are being manipulated in the first place.

What makes a good social engineering attack?

A good social engineering attack typically has a few common elements.

1. It is **well researched.** If a social engineering attack is attempting to impersonate a member of a company, then attackers will make use of the company letterhead, jargon, or format to help build credibility. Not all methods are equally effective against everyone. Cyber attackers research to determine the best driver.
2. It is **delivered confidently**. In person, good social engineers are prepared, confident, and reassure targets. Knowing when to launch an attack and how to develop a rapport with the target is important. Usually a high value social engineering attack is built up over a series of exchanges lending credibility and reducing inhibitions with each exchange. Rushing these can backfire and be a way in which cyber attackers reveal themselves through desperation.
3. The attack **feels plausible and realistic**. The best social engineering attacks are often the ones where the victim does not even know they've been tricked.

How can you defend against social engineering?

It is important for individuals as well as employees to be aware and guard against these common social engineering attacks.

Aside from trusting nobody ever, there is a simple rule to defend against social engineering attacks designed to trick individuals like you. Essentially, the golden rule is that if something seems too good to be true, it probably is. So, if you are ever faced with a financial windfall out of the blue, a head hunting request, or a prize from a competition you did not enter, then be aware, inquisitive, and do

not be blinded by the benefit.

In addition, don't be afraid to challenge others who make unusual requests or appear out of place. If an unknown colleague makes a strange request or you see someone loitering in a restricted area, you can often ask for details or report your suspicions, as appropriate. Just because someone claims to have been sent by an executive from the head office and they are in a hurry to get by you into a building, you can pause to check. Often the cost of verification is far less than letting an imposter into your office!

Beware of phishing

Specifically addressing the very common **phishing email attacks**, here are some tips to help you detect phishing emails, whether personal or business-related.

1. Consider if you were expecting the email. Does it make sense that the sender chose to contact you? Is it too good to be true or pressuring you to act quickly?
2. Always check the sender email address. Is it from someone or a company that you recognize?
3. Look for the salutation. Is it addressing you with a generic greeting such as "Dear valued member" instead of your name?
4. Search for any language or grammar errors in the email. Does it have poor grammar or a lot of spelling errors?
5. Determine what the email is requesting. Is it asking you to visit a fake or "spoof" website? Call a fake customer service number? Open attachments that you did not request?
6. Look for the red flags of a fake request (e.g., asks for your bank information or password) that is typically part of the phishing email. Secondly, don't click on a link without verifying the URL it points to.
    - Does the URL include a non-secure link? To know if it is a secure link, check that the URL begins with "https".
    - Does the URL direct you to a completely different website? Some URLs intentionally try to look like legitimate ones, for instance this is a fake URL for PayPal: www.paypall.accountlogin.com/signin. Notice the misspelling of "PayPal".

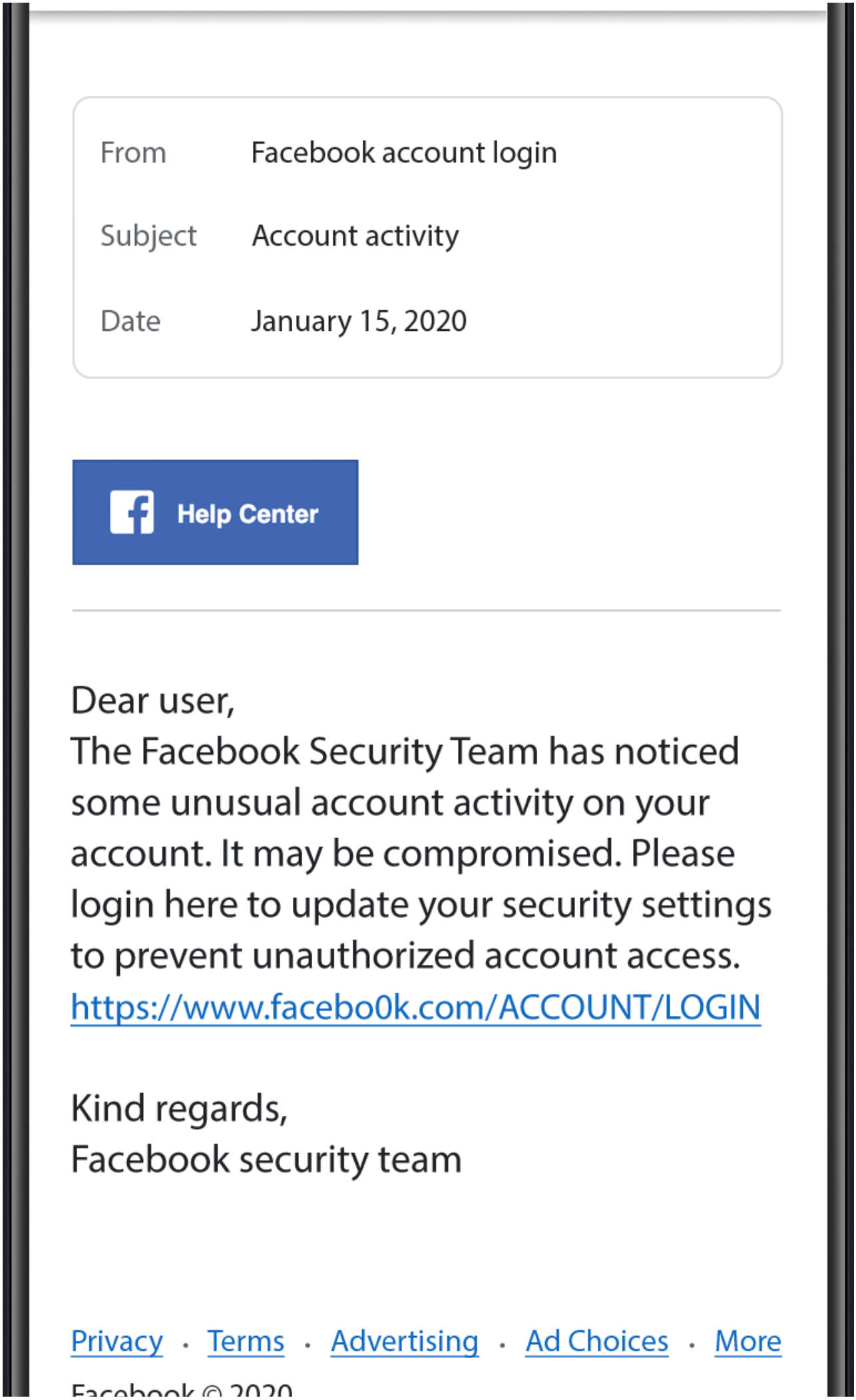
Important Note

If you receive an email that you believe could be phishing, don’t respond in any way and do not click any links or open any attachments. Most email services have a method to report an email as spam.

If you are in any doubt, you can get in touch with the sender via a trusted channel such as a previously saved contact phone number or access the service web address from your records.

Activity

Put on your detective hat and let's say you received this email from Facebook. Take a moment to read and study the email. What signs do you see that indicate this is a phishing email?



From Facebook account login

Subject Account activity

Date January 15, 2020

Help Center

Dear user,
The Facebook Security Team has noticed some unusual account activity on your account. It may be compromised. Please login here to update your security settings to prevent unauthorized account access.
https://www.facebo0k.com/ACCOUNT/LOGIN

Kind regards,
Facebook security team

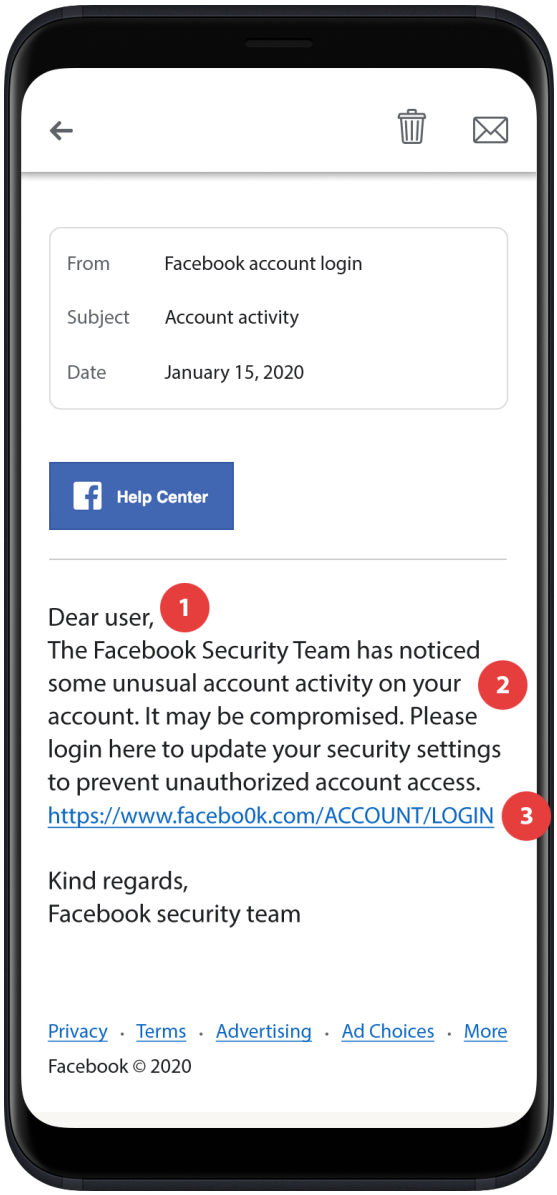
Privacy · Terms · Advertising · Ad Choices · More

Facebook © 2020

When you are ready, click here to reveal the indicators in the email.

There are three giveaways that indicate this is a phishing email attempting to get information from you.

1. It does not use your personal account name.
2. It is an unusual request.
3. The provided link is completely incorrect. Notice the misspelling of "facebook"; facebo0k.com is a known and reported phishing URL.



Open source intelligence

20 Minutes

Open source intelligence (OSINT) has become a major area of interest over the last decade, both within government activities and the private sector. The term "open" is used to refer to intelligence operations using publicly available information, such as information found on the open web, blogs, and websites. OSINT is all information that can be easily collected without any active collection methods, such as hacking, wiretaps, and so on. In this lesson, we will examine the benefits of OSINT, sources, and a few areas of concern for organizations and individuals. You will better understand how attackers can collect information about a targeted organization or individual.

Open source investigations can be conducted by journalists, researchers, and malicious attackers. Here, we will focus on attackers using these approaches as part of a reconnaissance stage for a larger attack.

Comparing OSINT with alternative options

Traditional forms of information gathering such as bugging phones, satellite images, and signal intelligence intercepts tend to be very expensive, complex, and often illegal. In comparison, using open information can be **virtually free** and **considerably easy** to acquire.

> EXAMPLE
> What if a journalist wants to locate where a member of a political party is at any given time? On one hand, they could attempt to illegally place a piece of malware on the individual's mobile phone to acquire GPS co-ordinates. On the other hand, it may be far simpler to keep a close eye on the individual's Twitter account. All it would take is for one of the politician’s aides to post a location tagged message or a photo with a recognizable landmark and they would have their answer. While this example seems simple, the same techniques have been used by military units to track their counterparts in foreign countries.

Another benefit of open source intelligence is that a lot of it is **undetectable to the target**.

> EXAMPLE
> What if an attacker wants to gather information about the control systems inside a power station? If they try to scan the power plant's external network, the attacker may be detected and have the secrecy of their infrastructure compromised. Alternatively, if the attacker finds a system engineer discussing sensitive plans online, while the blogging platform might have access records, the company would not.

Sources of open information

An attacker is about to embark on collecting basic information about an organization or individual, where might the attacker start? Here are some common sources to provide you with illustrative examples. There are *many more* possible sources and new ones are being discovered all the time.

Expand each section to learn more about the sources.

Company website

- Although it might seem too obvious, a company’s website can be revealing in terms of what information it chooses to make publicly available.
- It can reveal helpful information such as points of contact, external social media profiles, building addresses, and much more.
-

Companies might make mistakes with the information they make public, which means information can be placed into the public domain that may be more detailed than the company might like.

- Searches can be augmented with some advanced search features often referred to as "**Google hacking (https://en.wikipedia.org/wiki/Google_hacking)**" to find more advanced information and unintentionally revealed files.
- There are also options to retrieve a company's legacy website, such as using the **Wayback Machine (https://archive.org/web/)**. This can be a powerful tool for attackers to determine what a website was being used for at certain times.

Media and news

- If someone has already done the hard work, then why repeat the effort? There are very good journalists who are skilled at processing open information.
- While it is unlikely that attackers will find an exact match for what they are looking for, it's likely some articles might provide help for further investigations.
- Other sources of pre-processed or foundational information may include industry analysts, rating agencies, and other assessing bodies.

Social media

- In the era of social media, people are happy to share information and make it widely available.
- Social media information can be pieced together quite effectively to get an accurate perspective about an individual's personal and work life. For example, employees have been known to share photos of ID badges, network diagrams, and even sticky notes with passwords.
- For cyber attackers, even small pieces of information can add credibly to a social engineering attack.
    - For example, if an attacker finds out that a target recently attended a conference, then the attacker could start a spear phishing email to share the attacker found the target's name on the attendee list and wants to follow-up.

Government or public records

- Many countries around the world keep detailed records of both citizens and companies. These sources of information can be highly valuable for cyber attackers.
    - For example, a set of hospital records may identify an individual's place and date of birth and an electoral roll may identify someone's address. The availability of this type of information is a key reason why those facts should never form part of a security process without other safeguards.
- For companies, many stock exchanges require a certain amount of financial information to be made available.
    - For example, in the UK companies must provide information to **Companies House (https://www.gov.uk/government/organisations/companies-house)** to operate. All of this information can be of interest to a cyber attacker.

Good rules for gathering open information

If you are conducting an investigation using open information, here are a few simple guidelines to follow. As you become more experienced, you will learn additional tips and tricks, but this should be a good starting point.

1. Get lots of information: Quantity is valuable • The more information, the better. • Analyst tools that look for links between data sets operate better with more information. **Keep in mind**: You never know what the key piece of information will be, so save everything initially before refinement.
2. Get a range: Build a picture from many perspectives • Do not rely on a single source. • Not everything online is true! As a rule of thumb, a single source is easy to falsify (e.g., a social media profile with lots of flattering photos), however falsifying multiple sources is much more difficult to manage. **Keep in mind**: If you discover a target has deleted or attempted to conceal information, then this very fact can be of interest.
3. Do not get stuck: Be prepared to fail and do not get frustrated • While open source intelligence is very powerful, there are many dead ends and there is an element of luck about what a target may choose to share. • You may need to switch to a different approach or a new area to explore. **Keep in mind**: Successful investigations can take teams of trained researchers weeks to complete.

> **Note**: There will be many occasions during an investigation where open information is not obtainable. Some organizations and individuals will not have as much public information as others, for instance due to good operational security.

Why is open source intelligence an area of interest for everyone?

We live in a highly connected world where oversharing is a frequent occurrence. Everyone should be aware that what they share online is virtually permanent.

Even small pieces of information can be combined into revealing something of external interest. This process is called **information aggregation**. While an individual's place of work, commuting information, and typical evening plans may be innocuous in isolation, together they can be used to map someone's life out.

>  EXAMPLE
> This would be problematic in an organization where say hypothetically 100 employees could each reveal 1% of a sensitive piece of information. If the disclosures are combined by an external party, then significant breakthroughs or additional discoveries may be possible to achieve.

For organizations, the OSINT techniques that cyber attackers employ are important to consider when designing information management policies. The bottom line is that information leakage is bad for organizations. Organizations must take action to ensure that as little information as possible is unintentionally disclosed and made vulnerable for collection. Since having information publicly accessible is frequently essential, the scope of the information shared should be logged and understood.

Activity

One of the best ways to get started with open source intelligence is through trial and error. Try looking yourself up online! What open source intelligence could someone find out about you?

- Spend a few minutes now to open new internet browser windows to access Google, social media sites, and so on to run a few searches on your name.
    - If possible, use a fresh web browser with no cookies or history to avoid being steered back to sites based on your previous activity. This can be done using new, private or incognito internet browser windows.
- Could someone find your address, place of work, or other personal information? How private is your social media?
- Once you've done this, you could try asking a friend or family member to repeat the process to see what they find that you did not, and what approaches they took.

What can you conclude? There is no need to overshare. It is important for you to be aware.

Technical scanning

10 Minutes

Technical scanning techniques are an essential part of network administration and for network analysis at organizations. Here, we will turn our attention to how attackers collect information about computers and networks. While investigating a target machine on a network, an attacker may want to learn more information about the technical configuration. This could include details such as:

- What services are running on the machine?
- What operating system is in use?
- Are any of the services vulnerable to well known exploits?

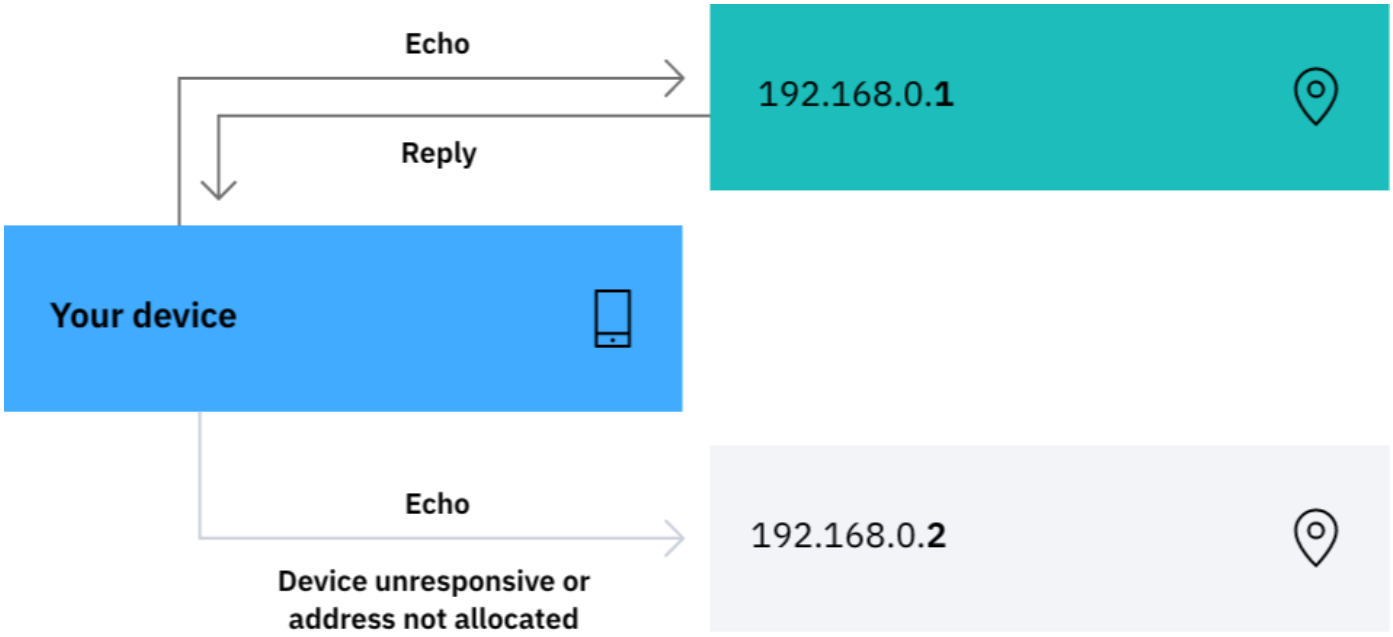
In this lesson, you will be introduced to technical scanning techniques and what attackers use them for. We will focus on how scanning can be used by a malicious outsider during the reconnaissance stage of an attack.

Ping test

What is it?

In a ping test, a scanning machine sends an Internet Control Message Protocol (ICMP) packet to the target machine's Internet Protocol address (IP address). This outbound packet is called an **echo request** packet. A **packet** is a small amount of formatted data, analogous to the digital version of a postcard. If the target machine replies with an **echo reply** packet, then the scanning machine knows the target machine is most likely active and switched on.

This diagram shows a phone "pinging" two IP addresses on its local network and waiting for a response.



What information does it provide?

This is a basic test. It is commonly used by organizations to debug networking issues. It identifies the status of a machine. It also provides an indication of how "far" into a network the machine is located by using a property known as a packet's "time to live" (TTL). Every router which forwards the packet onwards decreases the time to live by one.

> EXAMPLE
> If a packet starts with a time to live of 120 and reached the destination with 108 left, then it went through 12 stages. This feature can be used in the next scan. A ping test can be started using the command *'ping target_name'* on Windows machines.

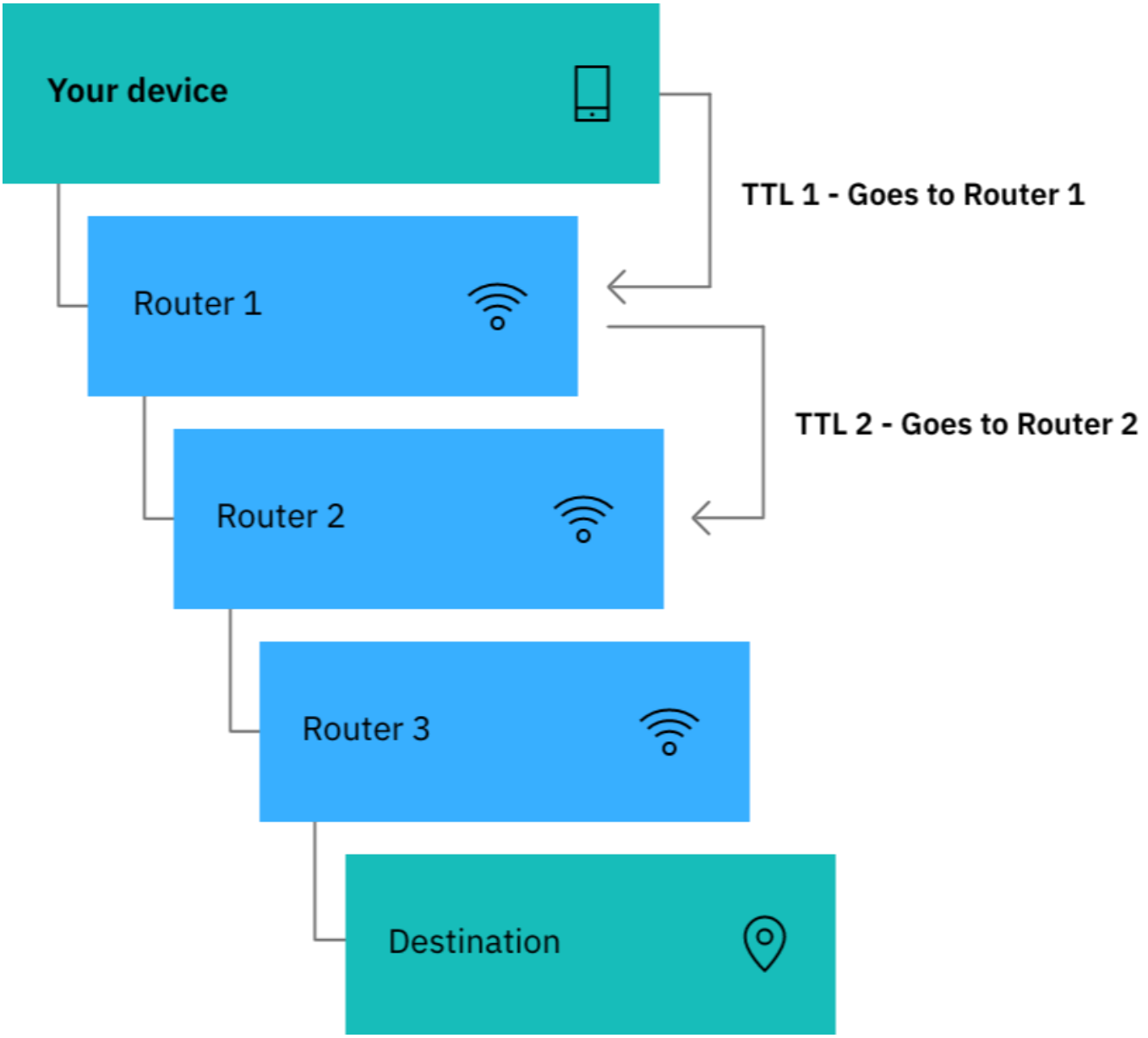
A ping test tells attackers and defenders if a machine is responsive and, when repeated in a sweep, how many devices are on a network.

Traceroute

What is it?

A traceroute between two computers can be calculated by sending out packets that have either increasing or decreasing "times to live" (TTL). When a packet is in transit and its "time to live" is decreased to zero, the machine processing the packet sends back an error message to the source point indicating the destination was not reached.

This diagram shows a device mapping out its connection between itself and a destination address. A physical analogy for this process is skimming a series of stones on a lake with increasing hops each time.



What information does it provide?

This behavior can be used to map out a network and determine how many switches and routers exist between you and your destination.

> EXAMPLE
> Imagine a target is 12 hops away. If a packet with a "time to live" of 11 is sent towards the target, it will fail at the final routing step. An error message packet will be returned to the scanner, but in doing so, it will reveal the IP address of the router 11 steps away. As the "time to live" is reduced down to one over a few new tests, a complete list of the network nodes between the scanner and the target can be produced. A traceroute can be started by using the command *'tracert target_name'* on Windows machines.

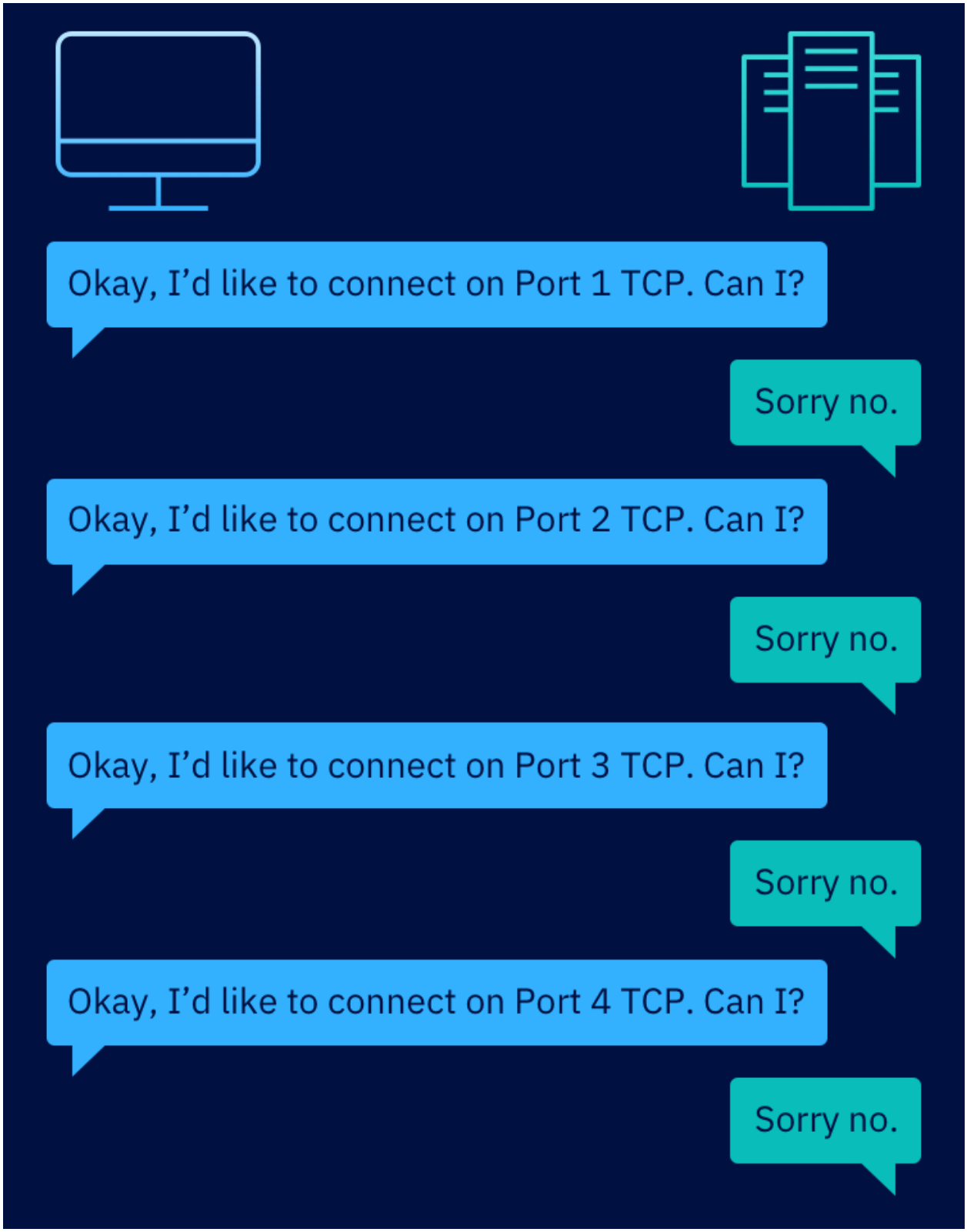
Port scanning

What is it?

In networking, applications make themselves accessible externally through advertising services on digital ports. You can imagine this as floors of a building. The IP address would set the building and each of the floors would be a different port number.

Most port scanning is based around the idea of attempting to open a connection with a certain number of ports on the target machine. Should the port start accepting a connection, the finding is noted by the scanning device and the connection is rejected. A port that accepts a connection is defined as being "open".

This diagram shows a machine scanning a server by systemically testing ports to see if a service is available on each one. After four attempts, the scanner has identified four ports that are rejecting connections and would be defined as "closed" ports.



What information does it provide?

By working through the list of "well known" ports on a target device, a scanner can often work out what the machine is being used for. Within the Transmission Control Protocol (TCP), there are 65,536 total ports of which the first 1,024 are "well known" ports. A "well known" or "system" port has a specific application associated with it that is agreed upon internationally. A common scanner,

such as **Network Mapper (Nmap) (https://nmap.org/)**, typically scans the most common 1,000 ports for a given protocol. This includes some "well known" ports and others will be higher numbered user-related ports (1,024 - 49,151).

> EXAMPLE
> The TCP port 80 is typically set aside for http applications or web servers. The fact that it is "open" on a target machine may be of interest to an investigator, since it shows a web-based application may be in use.

Network vulnerability scanning

What is it?

Another form of testing is vulnerability scanning. There are two main methods:

1. Certain actions are done to exploit the vulnerability, to determine if it exists on the target system. This is often known as **dynamic scanning** if done in real time.
2. The version numbers of software (e.g., a version of Apache or MySQL) are compared against a database containing known application vulnerability information.

Important Note

Please be aware that dynamic scanning may automatically perform actions which are illegal in certain countries. You should only scan targets for which you have the owner’s consent. A network vulnerability scan will often be interpreted as the planning stage of an attack.

What information does it provide?

Network vulnerability scanning is a powerful tool for both organizations to identify vulnerabilities in their own network and for attackers to find potential victims. Certain organizations periodically run such scans to identify mistakes which have been introduced in order to remediate them.

> EXAMPLE
> A scanner may attempt to connect to a server and check if it is running an outdated version of an application. If the application is out-of-date with a known vulnerability, then the scanner may attempt to exploit the vulnerability to confirm its existence and report this finding.

Search engine for the internet

Another tool for technical scanning is the **Shodan search engine (https://www.shodan.io/)**. It describes itself as the world's first search engine for internet-connected devices. It is of interest to malicious attackers and security researchers alike. It offers a vast catalogue of collected scan results spanning billions of records. These stored records can be used to track applications at scale around the world.

CHECK THIS OUT!

If you are interested in researching and spending more time on the topic of scanning, you can explore a popular port scanning site called **Network Mapper (Nmap) (https://nmap.org/)**. It is a free and open-source network scanner. You can start exploring the Intro, Reference Guide, or other online materials.

Go to Nmap (https://nmap.org/)

Case studies

15 Minutes

Cyber attacks are in the news on a daily basis, impacting individuals and organizations, whether in the public or private sector. In this lesson, we will review three high profile case studies of cyber attacks so you can understand the extent of what is possible and going on in the world. Each case study focuses on a different type of threat actor. These three case studies are part of an ever-growing catalogue of security breaches in the international landscape. As a participant within the security community, it is important to learn from examples to guide future decision making.

Stuxnet

Introducing cyber weapons

When Stuxnet was identified in 2010, it was one of the most advanced and targeted malware collections observed within the security community. Stuxnet was designed to target a specific industry control system and modify key settings. It is widely accepted that the malware was designed to target centrifuges used within Iranian uranium processing, which is a precursor for nuclear bomb production.

Entities related to this attack
Source: **StuxNet : A malware that gave the 4th dimension to war (https://medium.com/@shaayaan95/stuxnet-a-malware-that-gave-the-4th-dimension-to-war-5443215e7482)**, Medium by Shayan Anwar, July 2019

Here are a few considerations that made this attack particularly interesting.

- Stuxnet used four previously unidentified vulnerabilities, a pair of compromised digital certificates and concealed itself at a very low level within computing systems. Technically speaking, it was considerably more advanced than any previous malware.
- The malware was spread through infected USB drives. A common mistake within cybersecurity is to assume that if a system is not connected to the wider internet, an adversary could not introduce malware into the local network.
- The authors of the malware were persistent. Their targeted campaign went on for months as they kept tweaking and upgrading the tools they were using.

In many respects, Stuxnet was the definitive example of a cyber weapon being deployed to achieve a tangible military and political objective. It has set the international expectations for future cyber weapons in the future.

Equifax

Preventable large-scale data breach exposes hundreds of millions of people

In 2017, the US credit rating agency, Equifax, was hacked. After the organization failed to apply a security patch to a database, a group of hackers were able to gain access to Equifax's network. Within the network was a set of administrative credentials stored without encryption or basic access controls. Once the attackers had the administrative credentials, they could control most systems and did so undetected for months. According to the US Federal Trade Commission, the attackers stole at least 147 million names and dates of birth, 145.5 million Social Security numbers, and 209,000 payment card numbers and expiration dates. [1]

This case study was made notable for both the impact and scale of the data breach and the basic mistakes made within the organization which made it possible. Due to the scale of the breach, it placed the idea of data breaches into US attention.

[1] **Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related)**, Federal Trade Commission, Press Release, July 2019

National Security Agency

An insider leaks highly sensitive, damaging information

In 2013, a National Security Agency (NSA) subcontractor named Edward Snowden released a significant amount of classified information. He was able to access the information because of his job role, and with few technical tools and techniques.

Once the files were made public, the impact to the US and its international allies was considerable. The leaked files included technical capability overviews, guidance on operations, and other highly sensitive material. Several business arrangements between the NSA and US companies were bought under a high degree of scrutiny as a result.

This is a well known example of a malicious insider. While a public figure for the cost of the damages has not been made available, the general understanding was the data breach was the most damaging set of leaks the US had ever suffered.

SolarWinds

A large-scale supply chain attack affects thousands of organizations

SolarWinds developed software used to manage IT systems, including a product called Orion. In 2020, it was discovered that SolarWinds had been compromised and that malware had then been spread to thousands of SolarWinds' customers. The attackers compromised SolarWinds' update process so when customers updated Orion, they installed the malware as well.

This attack was noteworthy as it highlighted how trusted relations within supply chains can be used by prospective attackers. By compromising SolarWinds, the attacker was able to gain access to thousands of other organizations.

Looking beyond SolarWinds, large-scale supply chain attacks remain thankfully rare. Despite supplier compromises such as this case study, patching software is still recommended as a routine step.

Sources:

- **Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor (https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor)**, Mandiant, December 2020
- **Dealing with the SolarWinds Orion compromise (https://www.ncsc.gov.uk/guidance/dealing-with-the-solarwinds-orion-compromise)**, National Cyber Security Centre, January 2021

Activity

Take a few minutes to investigate a cybersecurity incident of your choosing for your own short case study, like those above. You can search online or access this **"List of cyberattacks" Wikipedia online article (https://en.wikipedia.org/wiki/List_of_cyberattacks)** for a list of many recent, well-known cases that may be of interest to you and provide a start.

Please type your answer to each question in the boxes. Your answers are just for you and are only saved in this course for you. Be sure to click **Save Text**.

1. Which cybersecurity incident did you choose for your case study?

Your text has been saved. Click "X" to continue. ✖

2. What type of attack was it and how was it completed?

Your text has been saved. Click "X" to continue. ✖

3. What were the consequences and what can the cybersecurity community learn from the event?

Save Text