Chapter 6
Comparing Threats, Vulnerabilities, and Common Attacks

CompTIA Security+ objectives covered in this chapter:

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.

- Viruses, Crypto-malware, Ransomware, Worm, Trojan, Rootkit, Keylogger, Adware, Spyware, Bots, RAT, Logic bomb, Backdoor

1.2 Compare and contrast types of attacks.

- Social engineering (Phishing, Spear phishing, Whaling, Vishing, Impersonation, Dumpster diving, Shoulder surfing, Hoax, Watering hole attack), Principles (reasons for effectiveness), (Authority, Intimidation, Consensus, Scarcity, Familiarity, Trust, Urgency), Application/service attacks (DoS, DDoS)

1.3 Explain threat actor types and attributes.

- Types of actors (Script kiddies, Hacktivist, Organized crime, Nation states/APT, Insiders, Competitors), Attributes of actors (Internal/external, Level of sophistication, Resources/ funding, Intent/motivation), Use of open-source intelligence

1.6 Explain the impact associated with types of vulnerabilities.

- Resource exhaustion, Untrained users

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Mail gateway (Spam filter)

2.3 Given a scenario, troubleshoot common security issues.

- Personnel issues (Insider threat, Social engineering, Social media)

2.4 Given a scenario, analyze and interpret output from security technologies.

- Antivirus, File integrity check, Advanced malware tools, Data

execution prevention

3.9 Explain the importance of physical security controls.

- Screen filters

**

Organizations need to understand and protect themselves from many different types of threat actors, so it's valuable to know a little about them, their attributes, and the types of attacks they are likely to launch. Malicious software (malware) and social engineering are two common attack categories that any organization will face, but there are some complexities to each category. Attackers are becoming more and more sophisticated with these attacks, so it's important to know how to reduce the success of attackers.

Understanding Threat Actors

When considering attacks, it's important to realize that there are several different types of threat actors, and they each have different attributes. Don't let the phrase threat actors confuse you. It's just a fancier name given to attackers—anyone who launches a cyberattack on others.

One common method that attackers often use before launching an attack is to gather information from ***open-source intelligence***. This includes any information that is available via web sites and social media. For example, if attackers want to get the name of the chief executive officer (CEO) of a company, they can probably find it on the company's web site. Similarly, many organizations post information on social media sites such as Facebook and Twitter.

A ***script kiddie*** is an attacker who uses existing computer scripts or code to launch attacks. Script kiddies typically have very little expertise or sophistication, and very little funding. Many people joke about the bored teenager as the script kiddie, attacking sites or organizations for the fun of it. However, there isn't any age limit for a script kiddie. More important, they can still get their hands on powerful scripts and launch dangerous attacks. Their motivations vary, but they are typically launching attacks out of boredom, or just to see what they can do.

A ***hacktivist*** launches attacks as part of an activist movement or to further a cause. Hacktivists typically aren't launching these attacks for their own benefit, but instead to increase awareness about a cause. As an example, Deric Lostutter (known online as KYAnonymous) was upset about the rape of a Steubenville, Ohio, high school girl, and what he perceived as a lack of justice. He later admitted to participating in several efforts to raise awareness

of the case, including targeting a web site ran by one of the high school's football players. Eventually, two high school football players were convicted of the rape. One was sentenced to a year in juvenile detention and served about 10 months. The other one was sentenced to two years and served about 20 months. Lostutter was ultimately sentenced to two years in federal prison.

An ***insider*** is anyone who has legitimate access to an organization's internal resources. Common security issues caused by insider threats include loss of confidentiality, integrity, and availability of the organization's assets. The extent of the threat depends on how much access the insider has. For example, an administrator would have access to many more IT systems than a regular user.

Malicious insiders have a diverse set of motivations. For example, some malicious insiders are driven by greed and simply want to enhance their finances, while others want to exact revenge on the organization. They may steal files that include valuable data, install or run malicious scripts, or redirect funds to their personal accounts.

Remember this

A script kiddie is an attacker who uses existing computer scripts or code to launch attacks. Script kiddies typically have very little expertise, sophistication, and funding. A hacktivist launches attacks as part of an activist movement or to further a cause. An insider is anyone who has legitimate access to an organization's internal resources, such as an employee of a company.

Competitors can also engage in attacks. Their motivation is typically to gain proprietary information about another company. Although it's legal to gather information using open- source intelligence, greed sometimes causes competitors to cross the line into illegal activity. This can be as simple as rummaging through a competitor's trash bin, which is known as dumpster diving. In some cases, competitors hire employees from other companies and then get these new employees to provide proprietary information about their previous employer.

Organized crime is an enterprise that employs a group of individuals working together in criminal activities. This group is organized with a hierarchy with a leader and workers, like a normal business. Depending on how large the enterprise is, it can have several layers of management. However, unlike a legitimate business, the enterprise is focused on criminal

activity. As an example, Symantec reported on Butterfly, a group of well-organized and highly capable attackers who steal market-sensitive information on companies and sell that information to the highest bidder. They have compromised some large U.S. companies, including Apple, Microsoft, and Facebook. Additionally, they have steadily increased their targets to include pharmaceutical and commodities-based organizations.

The primary motivation of criminals in organized crime is money. Almost all their efforts can be traced back to greed with the goal of getting more money, regardless of how they get it. However, because there isn't a defined size for organized crime, their sophistication, resources, and motivations can vary widely. Imagine a group of 10 individuals decides to target a single company. They will probably have significantly less sophistication and resources than the criminals within Butterfly.

Some attackers are organized and sponsored by a nation-state or government. An advanced persistent threat (***APT***) is a targeted attack against a network. The attacks are typically launched by a group that has both the capability and intent to launch sophisticated and targeted attacks. They often have a significant amount of resources and funding. Additionally, individuals within an APT group typically have very specific targets, such as a specific company, organization, or government agency. Successful attacks often allow unauthorized access for long periods of time, allowing attacks to exfiltrate a significant amount of data.

Remember this

Organized crime elements are typically motivated by greed and money but often use sophisticated techniques. Advanced persistent threats (APTs) are sponsored by governments and they launch sophisticated, targeted attacks.

As an example, Mandiant concluded that the group they named APT1 operates as Unit 61398 of the People's Liberation Army (PLA) inside China. Mandiant estimates that APT1 includes

over 1,000 servers and between dozens and hundreds of individual operators and has:

- Released at least 40 different families of malware
- Stolen hundreds of terabytes of data from at least 141 organizations
- Maintained access to some victim networks for over four years before being detected
- Established footholds within many networks after email recipients opened malicious files that installed backdoors, allowing attackers remote access

Chinese officials have denied these claims.

More recently, the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint analysis report (JAR-16-20296A), named GRIZZLY STEPPE, that provides detailed information on these APTs. They are nicknamed Fancy Bear (APT 28) and Cozy Bear (APT 29). The joint report states that these groups have targeted many government organizations, think tanks, universities, and corporations around the world. GRIZZLY STEPPE also indicates these two APTs compromised and exploited networks associated with the 2016 U.S. presidential election.

Cybersecurity firms such as CrowdStrike, SecureWorks, ThreatConnect, and FireEye's Mandiant have all indicated that APT 28 is sponsored by the Russian government and has probably been operating since the mid-2000s. Similarly, CrowdStrike has suggested that APT 29 is associated with Russian agencies. Symantec believes the organization has been attacking government and diplomatic organizations since at least 2010.

Russian officials have denied these claims.

Chapter 7, "Protecting Against Advanced Attacks," discusses many different types of attacks in detail. Two generic types of attacks are denial-of-service (***DoS***) attacks and distributed denial- of-service (***DDoS***) attacks. A DoS attack is from one attacker against one target. A DDoS attack is an attack from two or more computers against a single target. DDoS attacks often include sustained, abnormally high network traffic on the network interface card of the attacked computer.

DoS and DDoS attacks often attempt to overload an application or

service on a computer. As an example, a web server responds to Hypertext Transfer Protocol (HTTP) requests to serve web pages. A DDoS attack can overload the web server by sending thousands of HTTP requests to the server a second. These requests overload the resources (such as the processor and memory) and lead to ***resource exhaustion***. At some point, the attacked computer is no longer able to keep up with the requests. The attacked computer typically slows down significantly, preventing legitimate users from viewing web pages. In extreme cases of resource exhaustion, the attacked computer might crash.

Remember this

A denial-of-service (DoS) attack is an attack from a single source that attempts to disrupt the services provided by another system. A distributed denial-of-service (DDoS) attack includes multiple computers attacking a single target. DDoS attacks typically include sustained, abnormally high network traffic.

Determining Malware Types

Malware (malicious software) includes a wide range of software that has malicious intent. Malware is not software that you would knowingly purchase or download and install. Instead, it is installed onto your system through devious means. Infected systems give various symptoms, such as running slower, starting unknown processes, sending out email without user action, rebooting randomly, and more.

You might hear people use the term virus to describe all types of malware, but that isn't accurate. A virus is a specific type of malware, and malware includes many other types of malicious software, including worms, logic bombs, Trojans, ransomware, rootkits, spyware, and more.

It's also worth stressing that malware continues to evolve. In its 2017 report, "Cybersecurity Predictions 2017," Panda Security wrote that PandaLabs detected over 200,000 new malware samples a day in 2016. Most of these aren't completely new. Instead, they are slightly modified versions of existing malware.

Viruses

A ***virus*** is malicious code that attaches itself to a host application. The host application must be executed to run, and the malicious code executes when the host application is executed. The virus tries to replicate by finding other host applications to infect with the malicious code. At some point, the virus activates and delivers its payload.

Typically, the payload of a virus is damaging. It may delete files, cause random reboots, join the computer to a botnet, or enable backdoors that attackers can use to access systems remotely. Some older viruses merely displayed a message at some point, such as "Legalize Marijuana!" Most viruses won't cause damage immediately. Instead, they give the virus time to replicate first. A user will often execute the virus (though unknowingly), but other times, an operating system will automatically execute it after user interaction. For example, when a user plugs in an infected USB drive, the system might automatically execute the virus, infecting the system.

Worms

A ***worm*** is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction. A worm resides in memory and can use different transport protocols to travel over the network.

One of the significant problems caused by worms is that they consume network bandwidth. Worms can replicate themselves hundreds of times and spread to all the systems in the network. Each infected system tries to locate and infect other systems on the network, and network performance can slow to a crawl.

Remember this

Malware includes a wide variety of malicious code, including viruses, worms, Trojans, ransomware, and more. A virus is malicious code that attaches itself to an application and runs when the application is started. A worm is self-replicating and doesn't need user interaction to run.

Logic Bombs

A ***logic bomb*** is a string of code embedded into an application or script that will execute in response to an event. The event might be a specific date or time, or a user action such as when a user launches a specific program.

There's an often-repeated story about a company that decided it had to lay off an engineer due to an economic downturn. His bosses didn't see him doing much, so they thought they could do without him. Within a couple of weeks after he left, they started having all sorts of computer problems they just couldn't resolve.

They called him back, and within a couple of weeks, everything was fine. A few months later, they determined they had to lay him off again. You guessed it. Within a couple of weeks, things went haywire again.

The engineer had programmed a logic bomb that executed when the payroll program ran. It checked for his name on the payroll, and when it was there, things were fine, but when his name wasn't there, ka-boom—the logic bomb exploded.

Remember this

A logic bomb executes in response to an event, such as when a specific application is executed or a specific time arrives.

Backdoors

A ***backdoor*** provides another way of accessing a system, similar to how a backdoor in a house provides another method of entry. Malware often installs backdoors on systems to bypass normal authentication methods.

While application developers often code backdoors into applications, this practice is not recommended. For example, an application developer might create a backdoor within an application intended for maintenance purposes. However, if attackers discover the backdoor, they can use it to access the application.

Effectiveaccountmanagementpolicieshelppreventex-employeesfromcreatingbackdoors after they are fired. For example, if an employee loses network access immediately after being fired, the employee cannot create a backdoor account. In contrast, if an administrator retains

network access, he might create another administrative account. IT personnel might disable his account after they learn he has been fired, but he can still use this new backdoor account. That's exactly what a Fannie Mae Unix engineer did after being told he was fired.

Fannie Mae's account management policy did not revoke his elevated system privileges right away, giving him time to create a backdoor account. After going home, he accessed the system remotely and installed a logic bomb script scheduled to run at 9:00 a.m. on January 31. If another administrator hadn't discovered the logic bomb, it would have deleted data and backups for about four thousand servers, changed their passwords, and shut them down.

Remember this

A backdoor provides another way to access a system. Many types of malware create backdoors, allowing attackers to access systems from remote locations. Employees have also created backdoors in applications and systems.

Trojans

A ***Trojan***, also called a Trojan horse, looks like something beneficial, but it's actually something malicious. Trojan horses are named after the infamous horse from the Trojan War. In Greek mythology, the Achaeans tried to sack the city of Troy for several years, but they simply couldn't penetrate the city's defenses. At some point, someone got the idea of building a huge wooden horse and convincing the people of Troy that it was a gift from the gods. Warriors hid inside, and the horse was rolled up to the gates.

The people of Troy partied all day and all night celebrating their good fortune, but when the city slept, the warriors climbed down from inside the horse and opened the gates. The rest of the warriors flooded in. What the Greek warriors couldn't do for years, the Trojan horse helped them do in a single day.

In computers, a Trojan horse can come as pirated software, a useful utility, a game, or something else that users might be enticed to download and try. Attackers are increasingly using drive-by downloads to deliver Trojans. In a drive-by download, web servers include malicious code that attempts to download and install itself on user computers after the user visits. Here are the typical steps involved in a drive-by download:

1. Attackers compromise a web site to gain control of it.
2. Attackers install a Trojan embedded in the web site's code.
3. Attackers attempt to trick users into visiting the site. Sometimes, they simply send the link to thousands of users via email hoping that some of them click the link.
4. When users visit, the web site attempts to download the Trojan onto the users' systems.

Another Trojan method that has become popular in recent years is rogueware, also known as scareware. Rogueware masquerades as a free antivirus program. When a user visits a site, a message on the web page or a pop-up appears indicating it detected malware on the user's system. The user is encouraged to download and install free antivirus software.

On the surface, this free antivirus software looks useful. However, it isn't. If a user installs and runs it on a system, it appears to do a system scan. After the scan completes, it reports finding multiple issues, such as infections by dozens of viruses. The report isn't true. The application reports these issues even on a freshly installed operating system with zero infections.

It then encourages the user to resolve these issues immediately. If the user tries to resolve the issues, the program informs the user that this is only the trial version, and the trial version won't resolve these issues. However, for the small fee of $79.95, users can unlock the full version to remove the threats. Some rogueware installs additional malicious components. For example, it might allow the attacker to take remote control of the infected system.

Many web browser extensions include malicious Trojans. As an example, I once added an extension into my Google Chrome browser so that I could download videos and view them offline. Unfortunately, it modified the browser's behavior. When I went to a page from a Google search and then right-clicked on the page, it took to me to a malicious web site encouraging me to install malware disguised as a Windows Repair tool. At one point after right-clicking, it indicated my Chrome browser was out of date and encouraged me to download and install an update. However, using Chrome's tools, I verified that Chrome was up to date. When I clicked on Extensions to remove it, it redirected me to a malicious web site. I ultimately reset Chrome to the default settings, disabling all the extensions, and deleted the malicious extension.

Remember this

A Trojan appears to be something useful but includes a malicious component, such as installing a backdoor on a user's system. Many Trojans are delivered via drive-by downloads. They can also infect systems from fake antivirus software, pirated software, games, or infected USB drives.

RAT

A remote access Trojan (***RAT***) is a type of malware that allows attackers to take control of systems from remote locations. It is often delivered via drive-by downloads. Once installed on a system, attackers can then access the infected computer at any time, and install additional malware if desired.

Some RATs automatically collect and log keystrokes, usernames and passwords, incoming and outgoing email, chat sessions, and browser history as well as take screenshots. The RAT can then automatically send the data to the attackers at predetermined times.

Additionally, attackers can explore the network using the credentials of the user or the user's computer. Attackers often do this to discover, and exploit, additional vulnerabilities within the network. It's common for attackers to exploit this one infected system and quickly infect the entire network with additional malware, including installing RATs on other systems.

Ransomware

A specific type of Trojan is ***ransomware***. Attackers encrypt the user's data or take control of the computer and lock out the user. Then, they demand that the user pay a ransom to regain access to the data or computer. Criminals often deliver ransomware via drive-by downloads or embedded in other software delivered via email. Attackers originally targeted individuals with ransomware. However, they have increasingly been targeting organizations demanding larger and larger ransoms.

Many organizations indicate that ransomware attacks continue to grow and are becoming one of the greatest cyber threats:

- Symantec reported that ransomware attacks grew by 35 percent in

2015 (compared with 2014).

- The Cyber Threat Alliance (CTA) reported that CryptoWall 3, a specific version of ransomware, resulted in $325 million in losses in 2015 alone. It's difficult to know how much money has been lost by all versions of ransomware.
- In a public service announcement (Alert Number I-091516-PSA), the FBI reported that a single variant of ransomware infected as many as 100,000 computers a day in the first quarter of 2016.
- In their 2017 Annual Threat Report, SonicWall reported that the number of ransomware attacks observed by the SonicWall GRID Threat Network increased from 4 million in 2015 to 638 million in 2016.

Ransomware types continue to evolve. In early versions, they sometimes just locked the user out of the system. However, this is rarely done anymore. Instead, attackers typically encrypt the user's data to ensure that users can't retrieve it. Ransomware that encrypts the user's data is sometimes called ***crypto-malware***.

Remember this

Ransomware is a type of malware that takes control of a user's system or data. Criminals then attempt to extort payment from the victim. Ransomware often includes threats of damaging a user's system or data if the victim does not pay the ransom. Ransomware that encrypts the user's data is sometimes called crypto-malware.

Some ransomware has added in a new blackmail technique called doxing. If the user doesn't pay the ransom to decrypt the files, the attacker threatens to publish the files along with the victim's credentials. Malware that uses doxing is sometimes called doxingware.

Keylogger

A ***keylogger*** attempts to capture a user's keystrokes. The keystrokes are stored in a file, and are either sent to an attacker automatically, or the attacker may manually retrieve the file.

While a keylogger is typically software, it can also be hardware. For example, you can purchase a USB keylogger, plug it into the computer, and

plug the keyboard into the USB keylogger. This hardware keylogger will record all keystrokes and store them within memory on the USB device.

Spyware

Spyware is software installed on users' systems without their awareness or consent. Its purpose is often to monitor the user's computer and the user's activity. Spyware takes some level of control over the user's computer to learn information and sends this information to a third party. If spyware can access a user's private data, it results in a loss of confidentiality.

Some examples of spyware activity are changing a user's home page, redirecting web browsers, and installing additional software within the browser. In some situations, these changes can slow a system down, resulting in poorer performance. These examples are rather harmless compared with what more malicious spyware (called privacy-invasive software) might do.

Privacy-invasive software tries to separate users from their money using data-harvesting techniques. It attempts to gather information to impersonate users, empty bank accounts, and steal identities. For example, some spyware includes keyloggers. The spyware periodically reads the data stored by the keylogger, and sends it to the attacker. In some instances, the spyware allows the attacker to take control of the user's system remotely.

Spyware is often included with other software like a Trojan. The user installs one application but unknowingly gets some extras. Spyware can also infect a system in a drive-by download. The user simply visits a malicious web site that includes code to automatically download and install the spyware onto the user's system.

Remember this

Keyloggers capture a user's keystrokes and store them in a file. This file can be automatically sent to an attacker or manually retrieved depending on the keylogger. Spyware monitors a user's computer and often includes a keylogger.

Adware

When adware first emerged, its intent was primarily to learn a user's habits for the purpose of targeted advertising. As the practice of gathering

information on users became more malicious, more people began to call it spyware. However, some traditional adware still exists. Internet marketers have become very sophisticated and use a combination of web analytics with behavioral analytics to track user activity. They then provide targeted ads based on past user activity.

The term adware also applies to software that is free but includes advertisements. The user understands that the software will show advertisements and has the option to purchase a version of the software that does not include the ads. All of this is aboveboard without any intention of misleading the user.

Bots and Botnets

Generically, ***bots*** are software robots. For example, Google uses bots as search engine spiders to crawl through the Internet looking for web pages. However, attackers also use bots for malicious purposes. A botnet combines the words *robot* and *network*. It includes multiple computers that act as software robots (bots) and function together in a network (such as the Internet), often for malicious purposes. The bots in a botnet are often called zombies and they will do the bidding of whoever controls the botnet.

Bot herders are criminals who manage botnets. They attempt to infect as many computers as possible and control them through one or more servers running command-and-control software. The infected computers periodically check in with the command-and-control servers, receive direction, and then go to work. The user is often unaware of the activity.

Most computers join a botnet through malware infection. For example, a user could download pirated software with a Trojan or click a malicious link, resulting in a drive-by download. The malware then joins the system to a botnet.

Bot herders have been using Mirai to create large botnets. Mirai infects Linux systems that are running out-of-date versions of Linux and join them to a botnet. This includes Linux software running on Internet of things (IoT) devices such as digital cameras connected to the Internet. Infected devices search for other IoT devices on the Internet and infect them. Attackers have published the source code for Mirai in public forums, making it easily accessible by many attackers.

A Mirai botnet launched an attack in October 2016 against Domain

Name System (DNS) servers. It included about 100,000 simple devices such as digital cameras and printers that were connected to the Internet. The bot herders directed the devices to repeatedly query DNS servers in a protracted distributed denial-of-service (DDoS) attack. This attack overwhelmed the DNS servers and prevented users in the United States and Europe from accessing many common web sites, such as Amazon, Second Life, Twitter, CNN, BBC, Fox News, Tumblr, Reddit, and many more.

Similarly, Wordfence discovered attacks coming from a botnet of approximately 10,000 separate IP addresses in April 2017. After investigating the attacks, they learned that the attacking systems were typically home routers that had a known vulnerability, named the Misfortune Cookie by Checkpoint Software Technologies. Interestingly, Checkpoint reported the vulnerability in 2005. However, this attack showed that a specific Internet Service Provider (ISP) in Algeria was issuing these unpatched routers to its customers.

Botnet herders sometimes maintain complete control over their botnets. Other times, they rent access out to others to use as desired. Some of the instructions sent by the command-and- control servers include:

- Send spam.
- Launch a distributed denial-of-service attack.
- Download additional malware, adware, or spyware such as keyloggers.

Rootkits

A ***rootkit*** is a group of programs (or, in rare instances, a single program) that hides the fact that the system has been infected or compromised by malicious code. A user might suspect something is wrong, but antivirus scans and other checks indicate everything is fine because the rootkit hides its running processes to avoid detection.

In addition to modifying the internal operating system processes, rootkits often modify system files such as the Registry. In some cases, the rootkit modifies system access, such as removing users' administrative access.

Rootkits have system-level access to systems. This is sometimes called root-level access, or kernel-level access, indicating that they have the same level of access as the operating system. Rootkits use hooked processes, or

hooking techniques, to intercept calls to the operating system. In this context, *hooking* refers to intercepting system-level function calls, events, or messages. The rootkit installs the hooks into memory and uses them to control the system's behavior.

Antivirus software often makes calls to the operating system that could detect malware, but the rootkit prevents the antivirus software from making these calls. This is why antivirus software will sometimes report everything is OK, even if the system is infected with a rootkit. However, antivirus software can often detect the hooked processes by examining the contents of the system's random access memory (RAM).

Another method used to detect rootkits is to boot into safe mode, or have the system scanned before it boots, but this isn't always successful. It's important to remember that rootkits are very difficult to detect because they can hide so much of their activity. A clean bill of health by a malware scanner may not be valid.

It's important to remember that behind any type of malware, you'll likely find an attacker involved in criminal activity. Attackers who have successfully installed a rootkit on a user's system might log on to the user's computer remotely, using a backdoor installed by the rootkit. Similarly, attackers might direct the computer to connect to computers on the Internet and send data. Data can include anything collected from a keylogger, collected passwords, or specific files or file types stored on the user's computer.

Remember this

Rootkits have system-level or kernel access and can modify system files and system access. Rootkits hide their running processes to avoid detection with hooking techniques. Tools that can inspect RAM can discover these hidden hooked processes.

Recognizing Common Attacks

In addition to malware, it's important to understand some other common attacks. Social engineering includes several techniques attackers use to trick users. Additionally, many attackers use email, instant messaging, and the phone to deliver attacks.

Social Engineering

Social engineering is the practice of using social tactics to gain information. It's often low- tech and encourages individuals to do something they wouldn't normally do, or cause them to reveal some piece of information, such as user credentials. Some of the individual methods and techniques include:

- Using flattery and conning
- Assuming a position of authority
- Encouraging someone to perform a risky action
- Encouraging someone to reveal sensitive information
- Impersonating someone, such as an authorized technician
- Tailgating or closely following authorized personnel without providing credentials

In the movie *Catch Me If You Can*, Leonardo DiCaprio played Frank Abagnale Jr., an effective con artist. He learned some deep secrets about different professions by conning and flattering people into telling him. He then combined all he learned to impersonate pilots and doctors and perform some sophisticated forgery.

Social engineers con people in person, as Frank Abagnale Jr. did, and they use other methods as well. They may use the phone, send email with phishing tactics, and even use some trickery on web sites, such as fooling someone into installing malware.

As an example of a social engineer using the phone, consider this scenario. Maggie is busy working and receives a call from Hacker Herman, who identifies himself as a member of the IT department.

Hacker Herman: "Hi, Maggie. I just wanted to remind you, we'll be taking your computer down for the upgrade today, and it'll be down for a few hours."

Maggie: "Wait. I didn't hear anything about this. I need my computer to finish a project oday."

Hacker Herman: "You should have gotten the email. I'm sorry, but I have to get the last few computers updated today."

Maggie: "Isn't there any other way? I really need my computer."

Hacker Herman: "Well…it is possible to upgrade it over the network while you're still working. We don't normally do it that way because we need the user's password to do it."

Maggie: “If I can still work on my computer, please do it that way.”

Hacker Herman: “OK, Maggie. Don’t tell anyone I’m doing this for you, but if you give me your username and password, I’ll do this over the network.”

This is certainly a realistic scenario, and many end users will give out their passwords unless security-related awareness and training programs consistently repeat the mantra: “Never give out your password.”

Attackers aren’t always so blatant though. Many times, instead of asking you for your password outright, they ask questions they can use in a password reset system to reset your password. A skilled con man can ask these questions as though he’s generally interested in you. Before you know it, you’ve told him the name of your first dog, your childhood best friend, the name of your first boss, and more. When people post this information in social media, attackers don’t even need to ask.

The following sections describe many common security issues related to social engineering.

Remember this

Social engineering uses social tactics to trick users into giving up information or performing actions they wouldn’t normally take. Social engineering attacks can occur in person, over the phone, while surfing the Internet, and via email.

Impersonation

Some social engineers often attempt to impersonate others. The goal is to convince an authorized user to provide some information, or help the attacker defeat a security control.

As an example, an attacker can impersonate a repair technician to gain access to a server room or telecommunications closet. After gaining access, the attacker can install hardware such as a rogue access point to capture data and send it wirelessly to an outside collection point. Similarly, attackers impersonate legitimate organizations over the phone and try to gain information. Identity verification methods are useful to prevent the success of impersonation attacks.

Shoulder Surfing

Shoulder surfing is simply looking over the shoulder of someone to gain information. The goal is to gain unauthorized information by casual observation, and it's likely to occur within an office environment. This can be to learn credentials, such as a username and password, or a PIN used for a smart card or debit card. Recently, attackers have been using cameras to monitor locations where users enter PINs, such as at automatic teller machines (ATMs).

A simple way to prevent shoulder surfing is to position monitors and other types of screens so that unauthorized personnel cannot see them. This includes ensuring people can't view them by looking through a window or from reception areas.

Another method used to reduce shoulder surfing is to use a ***screen filter*** placed over the monitor. This restricts the visibility of the screen for anyone who isn't looking directly at the monitor.

Remember this

A social engineer can gain unauthorized information just by looking over someone's shoulder. This might be in person, such as when a user is at a computer, or remotely using a camera. Screen filters help prevent shoulder surfing by obscuring the view for people unless they are directly in front of the monitor.

Tricking Users with Hoaxes

A ***hoax*** is a message, often circulated through email, that tells of impending doom from a virus or other security threat that simply doesn't exist. Users may be encouraged to delete files or change their system configuration.

An older example is the teddy bear virus (*jdbgmgr.exe*), which was not a virus at all. Victims received an email saying this virus lies in a sleeping state for 14 days and then it will destroy the user's system. It then told users that they can protect their system by deleting the file (which has an icon of a little bear), and provided instructions on how to do so. Users who deleted the file lost some system capability.

More serious virus hoaxes have the potential to be as damaging as a real virus. If users are convinced to delete important files, they may make their systems unusable. Additionally, they waste help-desk personnel's time

due to needless calls about the hoax or support calls if users damaged their systems in response to the hoax.

Tailgating and Mantraps

Tailgating is the practice of one person following closely behind another without showing credentials. For example, if Homer uses a badge to gain access to a secure building and Francesca follows closely behind Homer without using a badge, Francesca is tailgating.

Employees often do this as a matter of convenience and courtesy. Instead of shutting the door on the person following closely behind, they often hold the door open for the person. However, this bypasses the access control, and if employees tailgate, it's very easy for a nonemployee to slip in behind someone else. Often, all it takes is a friendly smile from someone like Francesca to encourage Homer to keep the door open for her.

Chapter 9, "Implementing Controls to Protect Assets," discusses physical security controls such as mantraps and security guards. A simple ***mantrap*** can be a turnstile like those used in subways or bus stations. Imagine two men trying to go through a turnstile like this together. It's just not likely. Security guards can check the credentials of each person, and they won't be fooled by a smile as easily as Homer.

Dumpster Diving

Dumpster diving is the practice of searching through trash or recycling containers to gain information from discarded documents. Many organizations either shred or burn paper instead of throwing it away.

For example, old copies of company directories can be valuable to attackers. They may identify the names, phone numbers, and titles of key people within the organization. Attackers may be able to use this information in a whaling attack against executives or social engineering attacks against anyone in the organization. An attacker can exploit any document that contains detailed employee or customer information, and can often find value in seemingly useless printouts and notes.

On a personal basis, preapproved credit applications or blank checks issued by credit card companies can be quite valuable to someone attempting to gain money or steal identities. Documentation with any type of Personally Identifiable Information (PII) or Protected Health Information (PHI) should

be shredded or burned.

Remember this

Dumpster divers search through trash looking for information. Shredding or burning papers instead of throwing them away mitigates this threat.

Watering Hole Attacks

A ***watering hole attack*** attempts to discover which web sites a group of people are likely to visit and then infects those web sites with malware that can infect the visitors. The attacker's goal is to infect a web site that users trust already, making them more likely to download infected files.

As an example, an attack discovered in late 2016 initially targeted Polish banks. The attack was discovered by a single Polish bank that discovered previously unknown malware on internal computers. Symantec reported the source of the attack was servers at the Polish Financial Supervision Authority. This is a well-trusted institution by Polish bank employees, and they are likely to visit the organization's web sites often.

This isn't an isolated incident though. Symantec reported over 100 similar attacks located in over 30 countries.

Attacks via Email and Phone

Attackers have been increasingly using email to launch attacks. One of the reasons is because they've been so successful. Many people don't understand how dangerous a simple email can be for the entire organization. Without understanding the danger, they often click a link within a malicious email, which gives attackers access to an entire network. Email attacks include spam, phishing, spear phishing, and whaling.

Spam

Spam is unwanted or unsolicited email. Depending on which study you quote, between 80 percent and 92 percent of all Internet email is spam. Some spam is harmless advertisements, while much more is malicious. Spam can include malicious links, malicious code, or malicious attachments. Even when it's not malicious, when only 1 of 10 emails is valid, it can waste a lot

of your time.

In some cases, legitimate companies encourage users to opt in to their email lists and then send them email about their products. When users opt in to a mailing list, they agree to the terms. On the surface, you'd think that this means that you agree to receive email from the company and that's true. However, terms often include agreeing to allow their partners to send you email, which means the original company can share your email address with others.

Legitimate companies don't send you malicious spam, but they might send you more email than you want. Laws require them to include the ability to opt out, indicating you don't want to receive any more emails from them. Once you opt out, you shouldn't receive any more emails from that company.

Criminals use a variety of methods to collect email addresses. They buy lists from other criminals and harvest them from web sites. Some malware scans address books of infected computers to collect email. Because they are criminals, they don't care about laws, but they might include opt-out instructions in spam they send. However, instead of using this to remove you from their email list, attackers use this as confirmation that your email address is valid. The result is more spam.

Malspam (Sidebar)

In late 2016, some bad actors launched three malicious spam (malspam) campaigns that attempted to install the Cerber ransomware onto victims' computers. Each campaign followed a similar pattern, with each wave targeting domain administrators:

- The subject line included **Domain Abuse Notice** for the targeted domain.
- The body indicated that the targeted domain had been repeatedly used to send spam and spread malware.
- In some emails, it indicated this was a final notice and the domain would be suspended after 24 hours if it wasn't resolved.
- The body included at least one link labeled Click Here or Click Here to Download your Report.

The links were malicious and attempted to download Cerber ransomware. Some linked to a malicious JavaScript file (such as

Domain_Abuse_Report_Viewer.js) and others linked to an infected Word document (such as *Invoice_349KL.doc*) with a malicious macro. These malicious documents were hosted on different servers for each wave.

Phishing

Phishing is the practice of sending email to users with the purpose of tricking them into revealing personal information or clicking on a link. A phishing attack often sends the user to a malicious web site that appears to the user as a legitimate site.

The classic example is where a user receives an email that looks like it came from eBay, PayPal, a bank, or some other well-known company. The "phisher" doesn't know if the recipient has an account at the company, just as a fisherman doesn't know if any fish are in the water

where he casts his line. However, if the attacker sends out enough emails, the odds are good that
someone who receives the email has an account.

The email may look like this:

> "We have noticed suspicious activity on your account. To protect your privacy, we will suspend your account unless you are able to log in and validate your credentials. Click here to validate your account and prevent it from being locked out."

The email often includes the same graphics that you would find on the vendor's web site or an actual email from the vendor. Although it might look genuine, it isn't. Legitimate companies do not ask you to revalidate your credentials via email. If you go directly to the actual site, you might be asked to provide additional information to prove your identity beyond your credentials, but legitimate companies don't send emails asking you to follow a link and input your credentials to validate them.

Remember this

Spam is unwanted email. Phishing is malicious spam. Attackers

attempt to trick users into revealing sensitive or personal information or clicking on a link. Links within email can also lead unsuspecting users to install malware.

Beware of Email from Friends

Criminals have become adept at impersonating your friends. They scan social media sites and identify your friends and family. They then send emails to you that look like they are from your friends or family members, but they really aren't. This has become a common security issue related to social media.

As an example, imagine you are friends with Lisa Simpson and her email address is lisa@simpsons.com. You might receive an email that includes "Lisa Simpson" in the From block. However, if you look at the actual email address, you'd find it is something different, such as homer@moes.com. The underlying email address might belong to someone, but the forgery doesn't mean that they sent the email. To identify the actual sender, you often need to look at the full header of the email address.

I see emails such as this quite often lately. They seem to be related to comments or Likes that I make on Facebook. For example, after Liking a Facebook post on Lisa Simpson's Facebook page, I later receive an email with Lisa Simpson in the From block and a forged email address. These emails typically include a single line such as "I thought you might like this" and a malicious link. Clicking the link often takes the user to a server that attempts a drive-by download. This is a common way users inadvertently install ransomware on their systems.

Another possible scenario is that an attacker has joined your friend's computer to a botnet.
A bot herder is now using your friend's computer to send out phishing emails.

Phishing to Install Malware

One phishing email looked like it was from a news organization with headlines of recent news events. If the user clicked anywhere in the email, it showed a dialog box indicating that the user's version of Adobe Flash was too old to view the story. It then asked, "Would you like to upgrade your version of Adobe Flash?" If the user clicked Yes, it downloaded and installed malware.

Another email had the subject line "We have hijacked your baby" and

the following content: “You must pay once to us $50,000. The details we will send later. We have attached photo of your family.”

The English seems off, and the receiver might not even have a baby, making this look bogus right away. However, the attackers are only trying to pique your curiosity. The attached file isn’t a photo. Instead, it’s malware. If a user clicks on the photo to look at it, it installs malware on the user’s system.

Phishing to Validate Email Addresses

A simple method used to validate email addresses is the use of beacons. A beacon is a link included in the email that links to an image stored on an Internet server. The link includes unique code that identifies the receiver’s email address.

For the email application to display the image, it must retrieve the image from the Internet server. When the server hosting the image receives the request, it logs the user’s email address, indicating it’s valid. This is one of the reasons that most email programs won’t display images by default.

Phishing to Get Money

The classic Nigerian scam (also called a 419 scam) continues to thrive. You receive an email from someone claiming a relative or someone else has millions of dollars. Unfortunately, the sender can’t get the money without your help. The email says that if you help retrieve the money, you’ll get a substantial portion of the money for your troubles.

This scam often requires the victim to pay a small sum of money with the promise of a large sum of money. However, the large sum never appears. Instead, the attackers come up with reasons why they need just a little more money. In many cases, the scammers request access to your bank account to deposit your share, but instead they use it to empty your bank account.

There are countless variations on this scam. Lottery scams inform email recipients they won. Victims sometimes have to pay small fees to release the funds or provide bank information to get the money deposited. They soon learn there is no prize.

Spear Phishing

Spear phishing is a targeted form of phishing. Instead of sending the email out to everyone indiscriminately, a spear phishing attack attempts to target specific groups of users, or even a single user. Spear phishing attacks may target employees within a company or customers of a company.

As an example, an attacker might try to impersonate the CEO of an organization in an email. It's relatively simple to change the header of an email so that the From field includes anything, including the CEO's name and title. Attackers can send an email to all employees requesting that they reply with their password. Because the email looks like it's coming from the CEO, these types of phishing emails fool uneducated users.

One solution that deters the success of these types of spear phishing attacks is to use digital signatures. The CEO and anyone else in the company can sign their emails with a digital signature. This provides a high level of certainty to personnel on who sent the email. Chapter 10, "Understanding Cryptography and PKI," covers digital signatures in great depth.

Whaling

Whaling is a form of spear phishing that attempts to target high-level executives. Las Vegas casinos refer to the big spenders as whales, and casino managers are willing to spend extra time and effort to bring them into their casinos. Similarly, attackers consider high-level executives the whales, and attackers are willing to put in some extra effort to catch a whale because the payoff can be so great. When successful, attackers gain confidential company information that they might not be able to get anywhere else.

As an example, attackers singled out as many as 20,000 senior corporate executives in a fine-tuned phishing attack. The emails looked like official subpoenas requiring the recipient to appear before a federal grand jury and included the executive's full name and other details, such as their company name and phone number. The emails also included a link for more details about the subpoena. If the executives clicked the link, it took them to a web site that indicated they needed a browser add-on to read the document. If they approved this install, they actually installed a keylogger and malware. The keylogger recorded all their keystrokes to a file, and the malware gave the attackers remote access to the executives' systems.

Similar whaling attacks have masqueraded as complaints from the Better Business Bureau or the Justice Department. Executives are sensitive to issues that may affect the company's profit, and these attacks get their

attention. Although not as common, some whaling attacks attempt to reach the executive via phone to get the data. However, many executives have assistants who screen calls to prevent attackers from reaching the executive via phone.

Remember this

A spear phishing attack targets specific groups of users. It could target employees within a company or customers of a company. Digital signatures provide assurances to recipients about who sent an email, and can reduce the success of spear phishing. Whaling targets high-level executives.

Vishing

Vishing attacks use the phone system to trick users into giving up personal and financial information. It often uses Voice over IP (VoIP) technology and tries to trick the user similar to other phishing attacks. When the attack uses VoIP, it can spoof caller ID, making it appear as though the call came from a real company.

In one form, a machine leaves a phone message saying that you need to return the call concerning one of your credit cards. In another form, you receive an email with the same information. If you call, you'll hear an automated recording giving some vague excuse about a policy and prompting you to verify your identity. One by one, the recording prompts you for more information, such as your name, birthday, Social Security number, credit card number, expiration date, and so on. Sometimes, the recording asks for usernames and passwords. If you give all the requested information, the recording indicates they have verified your account. In reality, you just gave up valuable information on yourself.

Another example of vishing is just a regular phone call from a criminal. A popular ploy is a call from a company claiming to be "Credit Services" and offering to give you lower credit card rates. They play around with caller ID and have it display anything they want. A common ploy is to display a number similar to yours, making them appear local. They often announce, "This is your second and final notice," trying to evoke a sense of urgency.

If you answer, the automated system forwards you to a live person who begins asking a series of "qualifying" questions, such as how much credit

card debt you have and what your interest rates are. They then promise that they can help you lower your debt and get you a better rate. Next, they start asking some personal questions. They might ask for the last four digits of your Social Security number so they can "verify your account is in good standing." They might ask you for the code on your credit card "to verify you still have it."

Eventually, they hope to get your credit card number, expiration date, and code so that they can use it to post fraudulent charges. Some people have reported similar callers trying to get their bank information so that they can transfer money out of the accounts.

They hang up right away if you ask them to take you off their list, or stop calling. Similarly, they hang up when they hear words such as *criminal*, *thief*, and other words I'll leave out of this book. Some even reply with insults. They've called me so often, I've played along a few times. I love it when they ask for information on my credit card. I respond by saying, "Can you hold on so I can get it?" I then put the phone in a drawer and go back to work. Once, they stayed on the line for more than three hours waiting for me.

Remember this

Vishing is a form of phishing that uses the phone system or VoIP. Some vishing attempts are fully automated. Others start automated but an attacker takes over at some point during the call.

One Click Lets Them In

It's worth stressing that it only takes one click by an uneducated user to give an attacker almost unlimited access to an organization's network. Consider Figure 6.1. It outlines the process APTs have used to launch attacks.

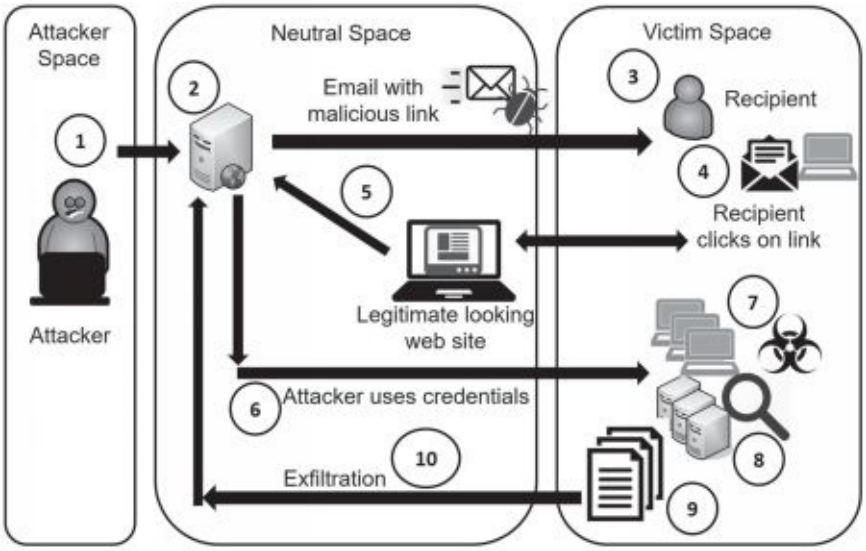

Figure 6.1: Steps in an attack

Note that the attacker (located in the attacker space) can be located anywhere in the world, and only needs access to the Internet. The neutral space might be servers owned and operated by the attackers. They might be in the same country as attackers, or they might be in another country. In some cases, the attackers use servers owned by others, but controlled by the attackers, such as servers in a botnet. The victim space is the internal network of the target. Refer to Figure 6.1 as you read the following steps in an attack:

1. The attacker uses open-source intelligence to identify a target. Some typical sources are social media sites and news outlets. Other times, attackers use social engineering tactics via phone calls and emails to get information on the organization or individuals employed by the organization.
2. Next, the attacker crafts a spear phishing email with a malicious link. The email might include links to malware hosted on another site and encourage the user to click the link. In some cases, this link can activate a drive-by download that installs itself on the user's computer without the user's knowledge. Cozy Bear (APT 29) used this technique and at least one targeted individual clicked the link. Similarly, criminals commonly use this technique to download ransomware onto a user's computer. In other cases, the email might indicate that the user's password has expired and the user needs to change the password or all access will be suspended. Fancy Bear (APT 28) used a similar technique.

3. The attacker sends the spear phishing email to the recipient from a server in the neutral space. This email includes a malicious link and uses words designed to trick the user into clicking it.
4. If the user clicks on the link, it takes the user to a web site that looks legitimate. This web site might attempt a drive-by download, or it might mimic a legitimate web site and encourage the user to enter a username and password.
5. If the malicious link tricked the user into entering credentials, the web site sends the information back to the attacker. If the malicious link installed malware on the user's system, such as a RAT, the attacker uses it to collect information on the user's computer (including the user's credentials, once discovered) and sends it back to the attacker.
6. The attacker uses the credentials to access targeted systems. In many cases, the attacker uses the infected computer to scan the network for vulnerabilities.
7. The attacker installs malware on the targeted systems.
8. This malware examines all the available data on these systems, such as emails and files on computers and servers.
9. The malware gathers all data of interest and typically divides it into encrypted chunks.
10. These encrypted chunks are exfiltrated out of the network and back to the attacker. Privilege escalation occurs when a user or process accesses elevated rights and permissions. Combined, rights and permissions are privileges. When attackers first compromise a system, they often have minimal privileges. However, privilege escalation tactics allow them to get more and more privileges. The recipient shown in Figure 6.1 might have minimal privileges, but malware will use various privilege escalation techniques to gain more and more privileges on the user's computer and within the user's network.

If users are logged on with administrative privileges, it makes it much easier for the malware to gain control of the user's system and within the network. This is one of the reasons organizations require administrators to have two accounts. Administrators use one account for regular use and one for administrative use. The only time they would log on with the administrator account is when they are performing administrative work. This

reduces the time the administrative account is in use, and makes it more difficult for the malware to use privilege escalation techniques.

Blocking Malware and Other Attacks

The previous sections described several different methods attackers and criminals use to launch new attacks. However, organizations and individuals can prevent many of these attacks from succeeding with just a few steps. These steps include using anti-malware software and educating users.

Protecting Systems from Malware

Malware is a significant threat for any organization. Administrators commonly implement layered security, or a defense-in-depth plan, to protect against malware. The following bullets list some common security controls used to protect against malware:

- **Spam filter on mail gateways.** Phishing attacks are delivered as malicious spam. Spam filters on mail gateways (email servers) detect and filter spam before it ever gets to users. Some networks route email through another device first to filter out spam. If users never receive a malicious email, there isn't any chance of them clicking on a malicious link in that email.
- **Anti-malware software on mail gateways.** Malicious email often includes malware as attachments. Anti-malware software on the mail server can detect and block it. The software strips potentially malicious attachments off the email, and typically sends a notification to the user explaining what was removed and why.
- **All systems.** All workstations and servers have anti-malware software installed. Servers may have additional, specialized anti-malware software installed depending on the applications running on the servers.
- **Boundaries or firewalls.** Many networks include detection tools that monitor network traffic through the firewall. For example, unified threat management (UTM) inspects network traffic to reduce the risk of malware entering the network. Chapter 3, "Exploring Network Technologies and Tools," covers UTM systems.

Antivirus and Anti-Malware Software

Anti-malware software provides protection against many types of malware. You'll often hear the term ***antivirus*** software indicating it only protects against viruses. However, the lines have blurred. Viruses aren't the only threats. Attackers have changed their methodologies using different types of malware, and antivirus software vendors have adapted by including methods to detect and block these new threats. Most antivirus software detects, blocks, and removes several different types of malware, such as viruses, Trojans, worms, rootkits, spyware, and adware. Antivirus software provides real-time protection and can perform both scheduled and manual scans. The real-time protection continuously monitors the system. For example, when a user visits a web site, antivirus software scans the downloaded web site files and attempts to block malicious code. Similarly, when a user downloads or opens a file, antivirus software scans it before opening it. Scheduled scans occur regularly, such as once a week. If users or technicians
detect suspicious activity, they can perform manual scans to check the system.

If the antivirus software detects malware, it will typically quarantine it and notify the user. However, the exact way antivirus software does so varies from one vendor to another. The key to analyzing and interpreting the output from the antivirus software is to recognize the alert and read it. Some people just click OK without paying attention to alerts and can inadvertently override the antivirus software.

Antivirus software detects viruses using either signature-based detection or heuristic- based detection.

Signature-Based Detection

Viruses and other malware have known patterns. Signature files (also called data definition files) define the patterns, and the antivirus software scans files for matching patterns. When the software identifies a matching pattern, it reports it as an infection and takes action, such as deleting or quarantining the file.

A quarantined virus is not harmful to the system while it is in quarantine, but it's still available for analysis. As an example, a security professional could release a quarantined virus into an unprotected but isolated virtual machine environment for research and study.

Malware developers constantly release new viruses, so it's important to update signature definition files regularly. Most antivirus software includes the ability to automate the process of checking and downloading updated signature definition files. They typically check for updates several times a day.

It's also possible to download and install signature files manually. Administrators do this when updating systems that do not have Internet access. When doing so, it's important for administrators to ensure the signature file has not lost data integrity by comparing the hash of the signature file posted on the antivirus vendor's web site with the hash of the downloaded file.

Heuristic-Based Detection

Some antivirus software includes heuristic-based detection. Heuristic-based detection attempts to detect viruses that were previously unknown and do not have signatures. This includes zero-day exploits, mentioned later in this chapter.

Heuristic-based analysis runs questionable code in a sandbox or virtualized environment specifically designed to protect the live environment, while it observes the code's behavior. Most viruses engage in viral activities—actions that can be harmful, but are rarely performed by legitimate programs. The heuristic-based analysis detects these viral activities.

As an example, polymorphic malware adds variations to files when it creates copies. It's highly unusual for any application to add variations in files like this, and heuristic methods are often successful at detecting polymorphic malware.

Remember this

Antivirus software detects and removes malware, such as viruses, Trojans, and worms. Signature-based antivirus software detects known malware based on signature definitions. Heuristic-based software detects previously unknown malware based on behavior.

Checking File Integrity

Some antivirus scanners use file integrity checkers to detect modified

system files. A file integrity checker calculates hashes on system files as a baseline. It then periodically recalculates the hashes on these files and compares them with the hashes in the baseline. If the hashes are ever different, it indicates the system files have been modified. When an antivirus scanner detects a modified file, it sends an alert. Many times, these alerts can detect rootkit infections.

It's also possible to check file integrity with command-line tools. For example, the Microsoft File Checksum Integrity Verifier (*fciv.exe*) tool can verify the integrity of all files within a folder, or a group of nested folders. Check out the lab Using the File Checksum Integrity Verifier in the labs for this chapter at *http://gcgapremium.com/501labs/.*

The *fciv.exe* allows you to create a data file listing all the hashes for files within a directory. You can then run the command later to verify the hashes are the same. Normally, you'll see the following message indicating the files haven't lost integrity: "All files verified successfully." However, if the application detects a file has a different hash, you'll see a message similar to this:

```
List of modified files:
----------------------
exefiles\md5Sum.exe
    Hash is: 08ab4b9b40448d77079f61751f989702bbebe2ed
    It should be: 7648ec1a2d8c8b65a024973d30b4b2dc48ad0cec
```

In this example, it indicates that the file *md5sum.exe* has been modified. Because executable files aren't normally modified, this indicates the file has likely been infected with malware and it shouldn't be used.

Data Execution Prevention

Data execution prevention (DEP) is a security feature that prevents code from executing in memory regions marked as nonexecutable. It helps prevent an application or service from executing code from a nonexecutable memory region. The primary purpose of DEP is to protect a system from malware.

DEP is enforced by both hardware and software. Advanced Micro Devices (AMD) implement DEP using the no-execute page-protection (NX) feature. Intel implements DEP using the Execute Disable Bit (XD) feature. Both are enabled in the Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI). Within Windows, DEP is enabled in the System

Properties – Performance Settings.

If DEP is not enabled in the BIOS or UEFI, but you try to install Windows, you will typically see an error message such as "Your PC's CPU isn't compatible with Windows." The solution is to enable DEP in BIOS or the UEFI.

Advanced Malware Tools

Many vendors have begun developing advanced malware tools. These go beyond just examining files to determine if they are malware. As an example, Cisco's Advanced Malware Protection (AMP) combines multiple technologies to protect a network before an attack, during an attack, and after an attack.

AMP analyzes a network to prevent attacks using threat intelligence and analytics. It collects worldwide threat intelligence from Cisco's Security Intelligence organization, Talos Security Intelligence and Research Group, and Threat Grid intelligence feeds. This information helps it detect and alert on malware similar to any antivirus software.

During an attack, AMP uses a variety of techniques to detect and block emerging threats before they infiltrate a network, or contain and remediate malware that gets into a network. AMP uses continuous analysis to detect suspicious file and network activity within a network, which helps it detect malware operating within the network.

Security administrators view logs and alerts to analyze and interpret the output from advanced malware tools such as AMP. For example, administrators might see an alert indicating that encrypted data is being sent out of the network. This is a serious red flag and indicates malware is collecting data and sending it to an attacker.

Spam Filters

Organizations often implement a multipronged approach to block spam. For example, many UTM systems include spam filters to detect and block spam. The output of the UTM goes to an email server. Email servers also have methods of detecting and blocking spam. The email server sends all email to the users, except for what it detects as spam. User systems also have anti-spam filters, or junk mail options, as a final check.

The challenge with any ***spam filter*** is to only filter out spam, and never

filter out actual email. For example, a company wouldn't want a spam filter to filter out an email from a customer trying to buy something. Because of this, most spam filters err on the side of caution, allowing spam through rather than potentially marking valid email as spam. Although the science behind spam filtering continues to improve, criminals have also continued to adapt.

Spam filters typically allow you to identify email addresses as safe, or to be blocked. You can add these as individual addresses or entire domains. For example, if you want to ensure you get email from Homer when he sends email from *springfield.com*, you can identify *homer@ springfield.com* as a safe email address. If you want to ensure you get all email from *springfield.com*, you can designate *springfield.com* as a safe domain. Similarly, you can block either the single email address *homer@springfield.com* or the entire domain *springfield.com.*

Educating Users

Untrained users provide a significant risk to any organization and are often one of the largest vulnerabilities. They don't need to be malicious insiders. They can simply be unaware of the risks. Think back to the Fancy Bear and Cozy Bear APT attacks mentioned in this chapter. No matter how much money an organization is spending on technology, it can all be bypassed by a single user clicking on a malicious link in an email. The impact can be the infection of an entire network.

The single best protection against many attacks, such as social engineering and phishing attacks, is to train and raise the security awareness of users. Many users simply aren't aware of the attackers' methods. However, once they understand the risks and methods used by social engineers and other attackers, they are less likely to fall prey to these attacks. Similarly, raising users' security awareness helps them recognize and respond appropriately to new threats and security trends.

Security-related awareness and training programs take many forms. Some common methods include formal classes, short informal live training sessions, online courses, posters, newsletters, logon banners, and periodic emails. These programs often keep users aware of new threats and new security trends and alerts, such as new malware, current phishing attacks, and zero-day exploits.

New Viruses

Criminals are constantly releasing new viruses and some prove to be exceptionally damaging. Many of these require administrators to take quick action to mitigate the threat. For example, when vendors discover a vulnerability that attackers can exploit, they release patches and updates to remove the vulnerability. Administrators then need to evaluate, test, and implement the patches or upgrades to servers. Similarly, home users should keep their systems and applications up to date.

Phishing Attacks

In addition to releasing new viruses regularly, criminals are also launching new phishing attacks. Some new attempts are tricky and fool many people. The best way to prevent successful attacks is to educate people about what the criminals are doing now.

As an example, criminals crafted a sophisticated attack on Gmail users that fooled even tech-savvy users. Once they had captured the Gmail credentials of one user, they quickly logged on to that user's account and scoured it for sent emails, attachments, and subject lines.

They then used this account to send emails to people this person previously emailed, often using similar subject lines. Additionally, they often include what looks like a thumbnail of a document. Typically, clicking the thumbnail provides a preview of the document. However, this instead opened up another tab within the browser with a URL like this:
data:text/html,https://accounts.google.com/ServiceLogin?service=mail…

When users see *accounts.google.com*, it looks legitimate. Additionally, the page shows a sign-in page that looks exactly like the Google sign-in page. It isn't, though. Users who were tricked into "logging on" on this bogus but perfectly created web page were compromised. Attackers quickly logged on to this account and started the process all over again, hoping to snare other unsuspecting users.

In one publicized example, the attackers used a compromised account to resend a team practice schedule to all the members of the team. It included a similar subject line and screenshot of the original attachment. Some recipients who received the email clicked the thumbnail and were taken to the same URL with *accounts.google.com* in it. Some were tricked and entered their credentials to apparently log on to Google. Attackers quickly logged on

to the newly compromised accounts and started the process again.

Zero-Day Exploits

Chapter 4, “Securing Your Network,” discusses zero-day vulnerabilities and zero-day exploits. As a reminder, a ***zero-day vulnerability*** is a vulnerability or bug that is unknown to trusted sources, such as operating system and antivirus vendors. Operating system vendors write and release patches once they know about them, but until the vendors know about them, the vulnerability remains. As an example, the Heartbleed vulnerability existed for a couple of years before it was widely published. Up until the time that OpenSSL developers released a fix, everyone using it was vulnerable.

Users might adopt the idea that up-to-date antivirus software will protect them from all malware. This simply isn’t true. No matter how great an antivirus company is at identifying new malware, there is always going to be a lag between the time when criminals release the malware and the antivirus company releases new signatures to discover it. This is especially true when attackers are releasing more than 200,000 new variants of malware daily. This includes malware designed to take advantage of zero-day vulnerabilities.

Remember this

Educating users about new viruses, phishing attacks, and zero-day exploits helps prevent incidents. Zero-day exploits take advantage of vulnerabilities that aren’t known by trusted sources, such as operating system vendors and antivirus vendors.

With this in mind, users need to practice safe computing habits. They can’t depend on the antivirus software and other technical controls to protect them. Some basic guidelines are:

- Don’t click on links within emails from unknown sources (no matter how curious you might be).
- Don’t open attachments from unknown sources. Malware can be embedded into many different files, such as Portable Document Format (PDF) files, Word documents, Zipped (compressed) files, and more.
- Be wary of free downloads from the Internet. (Trojans entice you

with something free, but they include malware.)

- Limit information you post on social media sites. (Criminals use this to answer password reset questions.)
- Back up your data regularly (unless you're willing to see it disappear forever).
- Keep your computer up to date with current patches (but beware of zero-day exploits).
- Keep antivirus software up to date (but don't depend on it to catch everything).

Why Social Engineering Works

Social engineers typically use one or more psychology-based principles to increase the effectiveness of their attacks. In addition to teaching users about the different social engineering

tactics, it's also useful to teach them about these underlying principles. The following sections introduce these topics.

Authority

Many people have grown up to respect authority and are more likely to comply when a person of authority says to do so. As an example, volunteers participating in the Milgram experiment continued to send shocks to unseen subjects even though they could hear them scream in pain, simply because a man in a lab coat told them to continue. They weren't actually sending shocks and the screams were fake, but everything seemed real to the volunteers. Psychologists have repeated these experiments and have seen similar results. Using authority is most effective with impersonation, whaling, and vishing attacks:

- **Impersonation.** Some social engineers impersonate others to get people to do something. For example, many have called users on the phone claiming they work for Microsoft. The Police Virus (a form of ransomware) attempts to impersonate a law enforcement agency. Other times, social engineers attempt to impersonate a person of authority, such as an executive within a company, or a technician.
- **Whaling.** Executives respect authorities such as legal entities. As an example, the "Whaling" section mentioned how many executives were tricked into opening infected PDF files that looked like official subpoenas.
- **Vishing.** Some attackers use the phone to impersonate authority figures.

Intimidation

In some cases, the attacker attempts to intimidate the victim into taking action. Intimidation might be through bullying tactics, and it is often combined with impersonating someone else. Using intimidation is most effective with impersonation and vishing attacks.

For example, a social engineer might call an executive's receptionist with this request: "Mr. Simpson is about to give a huge presentation to potential customers, but his files are corrupt. He told me to call you and get you to send

the files to me immediately so that I can get him set up for his talk." If the receptionist declines, the social engineer can use intimidation tactics by saying something like: "Look, if you want to be responsible for this million-dollar sale falling through, that's fine. I'll tell him you don't want to help."

Note that this tactic can use multiple principles at the same time. In this example, the attacker is combining intimidation with urgency. The receptionist doesn't have much time to respond.

Consensus

People are often more willing to like something that other people like. Some attackers take advantage of this by creating web sites with fake testimonials that promote a product. For example, criminals have set up some web sites with dozens of testimonials listing all the benefits of their fake antivirus software. If users search the Internet before downloading the fake antivirus software, they will come across these web sites, and might believe that other real people are vouching for the product.

Using consensus, sometimes called social proof, is most effective with Trojans and hoaxes. Victims are more likely to install a Trojan if everyone seems to indicate it's safe. Similarly, if a person suspects a virus notice is just a hoax, but everyone seems to be saying it's real, the victim is more likely to be tricked.

Scarcity

People are often encouraged to take action when they think there is a limited quantity. As an example of scarcity, think of Apple iPhones. When Apple first releases a new version, they typically sell out quickly. A phishing email can take advantage of this and encourage users to click a link for exclusive access to a new product. If the users click, they'll end up at a malicious web site. Scarcity is often effective with phishing and Trojan attacks. People make quick decisions without thinking them through.

Urgency

Some attacks use urgency as a technique to encourage people to take action now. As an example, the ransomware uses the scarcity principle with a countdown timer. Victims typically have 72 hours to pay up before they lose all their data. Each time they look at their computer, they'll see the timer counting down.

Using urgency is most effective with ransomware, phishing, vishing, whaling, and hoaxes. For example, phishing emails with malicious links might indicate that there are a limited number of products at a certain price, so the user should "Click Now." Executives might be tricked into thinking a subpoena requires immediate action. Many virus hoaxes have a deadline such as at 4:00 p.m. when the hoax claims the virus will cause the damage.

Remember this

Many of the reasons that social engineers are effective are because they use psychology-based techniques to overcome users' objections. Scarcity and urgency are two techniques that encourage immediate action.

Familiarity

If you like someone, you are more likely to do what the person asks. This is why so many big companies hire well-liked celebrities. And, it's also why they fire them when they become embroiled in a scandal that affects their credibility.

Some social engineers attempt to build rapport with the victim to build

a relationship before launching the attack. This principle is most effective with shoulder surfing and tailgating attacks:

- **Shoulder surfing.** People are more likely to accept someone looking over their shoulder when they are familiar with the other person, or they like them. In contrast, if you don't know or don't like someone, you are more likely to recognize a shoulder surfing attack and stop it immediately.
- **Tailgating.** People are much more likely to allow someone to tailgate behind them if they know the person or like the person. Some social engineers use a simple, disarming smile to get the other person to like them.

Trust

In addition to familiarity, some social engineers attempt to build a trusting relationship between them and the victim. This often takes a little time, but the reward for the criminal can be worth it. Vishing attacks often use this method.

As an example, someone identifying himself as a security expert once called me. He said he was working for some company with "Secure" in its name, and they noticed that my computer was sending out errors. He stressed a couple of times that they deploy and support Windows systems. The company name and their experience was an attempt to start building trust.

He then guided me through the process of opening Event Viewer and viewing some errors on my system. He asked me to describe what I saw and eventually said, "Oh my God!" with the voice of a well-seasoned actor. He explained that this indicated my computer was seriously infected. In reality, the errors were trivial.

After seriously explaining how much trouble I was in with my computer, he then added a smile to his voice and said, "But this is your lucky day. I'm going to help you." He offered to guide me through the process of fixing my computer before the malware damaged it permanently.

All of this was to build trust. At this point, he went in for the kill. He had me open up the Run window and type in a web site address and asked me to click OK. This is where I stopped. I didn't click OK.

I tried to get him to answer some questions, but he was evasive.

Eventually, I heard a click.

My "lucky day" experience with this social engineering criminal was over.

The link probably would have taken me to a malicious web site ready with a drive-by download. Possibly the attacker was going to guide me through the process of installing malware on my system. If my system objected with an error, I'm betting he would have been ready with a soothing voice saying "That's normal. Just click OK. Trust me." He spent a lot of time with me. I suspect that they've been quite successful with this ruse with many other people.

Chapter 6 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Understanding Threat Actors

- Script kiddies use existing computer scripts or code to launch attacks. They typically have very little expertise or sophistication, and very little funding.
- A hacktivist launches attacks as part of an activist movement or to further a cause.
- Insiders (such as employees of a company) have legitimate access to an organization's internal resources. They sometimes become malicious insiders out of greed or revenge.
- Competitors sometimes engage in attacks to gain proprietary information about another company.
- Organized crime is an enterprise that employs a group of individuals working together in criminal activities. Their primary motivation is money.
- Some attackers are organized and sponsored by a nation-state or government.
- An advanced persistent threat (APT) is a targeted attack against a network. An APT group has both the capability and intent to launch sophisticated and targeted attacks. They are sponsored by a nation-state and often have a significant amount of resources and funding.
- A common method attackers often use before launching an attack is to gather information from open-source intelligence, including any information available via web sites and social media.

Determining Malware Types

- Malware includes several different types of malicious code, including viruses, worms, logic bombs, backdoors, Trojans, ransomware, rootkits, and more.
- A virus is malicious code that attaches itself to a host application. The code runs when the application is launched.

- A worm is self-replicating malware that travels throughout a network without user intervention.
- A logic bomb executes in response to an event, such as a day, time, or condition. Malicious insiders have planted logic bombs into existing systems, and these logic bombs have delivered their payload after the employee left the company.
- Backdoors provide another way of accessing a system. Malware often inserts backdoors into systems, giving attackers remote access to systems.
- A Trojan appears to be one thing, such as pirated software or free antivirus software, but is something malicious. A remote access Trojan (RAT) is a type of malware that allows attackers to take control of systems from remote locations.
- Drive-by downloads often attempt to infect systems with Trojans.
- Ransomware is a type of malware that takes control of a user's system or data. Criminals attempt to extort payment as ransom combined to return control to the user. Crypto- malware is ransomware that encrypts the user's data. Attackers demand payment to decrypt the data.
- Spyware is software installed on user systems without the user's knowledge or consent and it monitors the user's activities. It sometimes includes a keylogger that records user keystrokes.
- A botnet is a group of computers called zombies controlled through a command-and- control server. Attackers use malware to join computers to botnets. Bot herders launch attacks through botnets.
- Rootkits take root-level or kernel-level control of a system. They hide their processes to avoid detection. They can remove user privileges and modify system files.

Recognizing Common Attacks

- Social engineering is the practice of using social tactics to gain information or trick users into performing an action they wouldn't normally take.
- Social engineering attacks can occur in person, over the phone, while surfing the Internet, and via email. Many social engineers attempt to impersonate others.
- Shoulder surfing is an attempt to gain unauthorized information

through casual observation, such as looking over someone's shoulder, or monitoring screens with a camera. Screen filters can thwart shoulder surfing attempts.

- A hoax is a message, often circulated through email, that tells of impending doom from a virus or other security threat that simply doesn't exist.
- Tailgating is the practice of one person following closely behind another without showing credentials. Mantraps help prevent tailgating.
- Dumpster divers search through trash looking for information. Shredding or burning documents reduces the risk of dumpster diving.
- Watering hole attacks discover sites that a targeted group visits and trusts. Attackers then modify these sites to download malware. When the targeted group visits the modified site, they are more likely to download and install infected files.
- Spam is unwanted or unsolicited email. Attackers often use spam in different types of attacks.
- Phishing is the practice of sending email to users with the purpose of tricking them into revealing sensitive information, installing malware, or clicking on a link.
- Spear phishing and whaling are types of phishing. Spear phishing targets specific groups of users and whaling targets high-level executives.
- Vishing is a form of phishing that uses voice over the telephone and often uses Voice over IP (VoIP). Some vishing attacks start with a recorded voice and then switch over to a live person.

Blocking Malware and Other Attacks

- Antivirus software can detect and block different types of malware, such as worms, viruses, and Trojans. Antivirus software uses signatures to detect known malware.
- When downloading signatures manually, hashes can verify the integrity of signature files.
- Antivirus software typically includes a file integrity checker to detect files modified by a rootkit.
- Data execution prevention (DEP) prevents code from executing in memory locations marked as nonexecutable. The primary purpose of DEP is to protect a system from malware.

- Advanced malware tools monitor files and activity within the network.
- Anti-spam software attempts to block unsolicited email. You can configure a spam filter to block individual email addresses and email domains.
- Security-related awareness and training programs help users learn about new threats and security trends, such as new viruses, new phishing attacks, and zero-day exploits. Zero- day exploits take advantage of vulnerabilities that are not known by trusted sources.
- Social engineers and other criminals employ several psychology-based principles to help increase the effectiveness of their attacks. They are authority, intimidation, consensus, scarcity, urgency, familiarity, and trust.

Online References

- Have you done the online labs? They might help you understand some key content. Check out the online content to view some extra materials at *http://gcgapremium.com/501-extras*.

Chapter 6 Practice Questions

1. The Marvin Monroe Memorial Hospital recently suffered a serious attack. The attackers notified management personnel that they encrypted a significant amount of data on the hospital's servers and it would remain encrypted until the management paid a hefty sum to the attackers. Which of the following identifies the MOST likely threat actor in this attack?

   A. Organized crime
   B. Ransomware
   C. Competitors
   D. Hacktivist

2. Dr. Terwilliger installed code designed to enable his account automatically if he ever lost his job as a sidekick on a television show. The code was designed to reenable his account three days after it is disabled. Which of the following does this describe?

A. Logic bomb
B. Rootkit
C. Spyware
D. Ransomware

3. Lisa recently developed an application for the Human Resources department. Personnel use this application to store and manage employee data, including PII. She programmed in the ability to access this application with a username and password that only she knows, so that she can perform remote maintenance on the application if necessary. Which of the following does this describe?

A. Virus
B. Worm
C. Backdoor
D. Trojan

4. Dr. Terwilliger installed code designed to run if he ever lost his job as a sidekick on a television show. The code will create a new account with credentials that only he knows three days after his original account is deleted. Which type of account does this code create?

A. Backdoor
B. Logic bomb
C. Rootkit
D. Ransomware

5. Security administrators recently discovered suspicious activity within your network. After investigating the activity, they discovered malicious traffic from outside your network connecting to a server within your network. They determined that a malicious threat actor used this connection to install malware on the server and the malware is collecting data and sending it out of the network. Which of the following BEST describes the type of malware used by the threat actor?

A. APT

B. Organized crime
C. RAT
D. Crypto-malware

6. A security administrator recently noticed abnormal activity on a workstation. It is connecting to systems outside the organization's internal network using uncommon ports. The administrator discovered the computer is also running several hidden processes. Which of the following choices BEST describes this activity?

A. Rootkit
B. Backdoor
C. Spam
D. Trojan

7. Lisa is a database administrator and received a phone call from someone identifying himself as a technician working with a known hardware vendor. The technician said he's aware of a problem with database servers they've sold, but it only affects certain operating system versions. He asks Lisa what operating system the company is running on their database servers. Which of the following choices is the BEST response from Lisa?

A. Let the caller know what operating system and versions are running on the database servers to determine if any further action is needed.
B. Thank the caller and end the call, report the call to her supervisor, and independently check the vendor for issues.
C. Ask the caller for his phone number so that she can call him back after checking the servers.
D. Contact law enforcement personnel.

8. Bart is in a break area outside the office. He told Lisa that he forgot his badge inside and asked Lisa to let him follow her when she goes back inside. Which of the following does this describe?

A. Spear phishing
B. Whaling
C. Mantrap
D. Tailgating

9. While cleaning out his desk, Bart threw several papers containing PII into the recycle bin. Which type of attack can exploit this action?

A. Vishing
B. Dumpster diving
C. Shoulder surfing
D. Tailgating

10. Your organization recently suffered a loss from malware that wasn't previously known by any trusted sources. Which of the following BEST describes this attack?

A. Phishing
B. Zero-day
C. Open-source intelligence
D. Hoax

11. A recent change in an organization's security policy states that monitors need to be positioned so that they cannot be viewed from outside any windows. Additionally, users are directed to place screen filters over the monitor. What is the purpose of this policy?

A. Reduce success of phishing
B. Reduce success of shoulder surfing
C. Reduce success of dumpster diving
D. Reduce success of impersonation

12. Attackers recently sent some malicious emails to the CFO within your organization. These emails have forged From blocks and look like they are coming from the CEO of the organization. They include a PDF file that is described as a funding document for an upcoming project. However, the PDF is infected with malware. Which of the following BEST describes the attack type in this scenario?

A. Phishing
B. Spam
C. Trojan
D. Whaling

13. A recent spear phishing attack that appeared to come from your organization's CEO resulted in several employees revealing their passwords to attackers. Management wants to implement a security control to provide assurances to employees that email that appears to come from the CEO actually came from the CEO. Which of the following should be implemented?

A. Digital signatures

B. Spam filter
C. Training
D. Heuristic-based detection

14. A recent attack on your organization's network resulted in the encryption of a significant amount of data. Later, an attacker demanded that your organization pay a large sum of money to decrypt the data. Security investigators later determined that this was the result of a new employee within your company clicking on a malicious link he received in an email. Which of the following BEST describes the vulnerability in this scenario?

A. Ransomware
B. Untrained user
C. Resource exhaustion
D. Insider threat

15. The CEO of a company recently received an email. The email indicates that her company is being sued and names her specifically as a defendant in the lawsuit. It includes an attachment and the email describes the attachment as a subpoena. Which of the following BEST describes the social engineering principle used by the sender in this scenario?

A. Whaling
B. Phishing
C. Consensus
D. Authority

Chapter 6 Practice Question Answers

1. **A.** This attack was most likely launched by an organized crime group because their motivation is primarily money. While the scenario describes ransomware, ransomware is the malware, not the threat actor. Competitors often want to obtain proprietary information and it would be very rare for a hospital competitor to extort money from another hospital. A hacktivist typically launches attacks to further a cause, not to extort money.

2. **A.** A logic bomb is code that executes in response to an event. In this scenario, the logic bomb executes when it discovers the account is disabled (indicating Dr. Bob Terwilliger is no longer employed at the company). In this scenario, the logic bomb is creating a backdoor. A rootkit includes hidden processes, but it does not activate in response to an event. Spyware is software installed on user systems without their awareness or consent. Its purpose is often to monitor the user's computer and the user's activity. Ransomware demands payment as ransom.

3. **C.** A backdoor provides someone an alternative way of accessing a system or application, which is exactly what Lisa created in this scenario. It might seem as though she's doing so with good intentions, but if attackers discover a backdoor, they can exploit it. A virus is malicious code that attaches itself to an application and executes when the application runs, not code that is purposely written into the application. A worm is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction. A Trojan is software that looks like it has a beneficial purpose but includes a malicious component.

4. **A.** The code is creating a new account that Dr. Terwilliger can use to access as a backdoor. He is creating this with a logic bomb, but a logic bomb is the malware type, not the type of account that he created. Rootkits include hidden processes, but they do not activate in response to events. Ransomware demands payment to release a user's computer or data.

5. **C.** The scenario describes a remote access Trojan (RAT), which is a type of malware that allows attackers to take control of systems from remote locations. While the threat actor may be a member of an advanced persistent threat (APT) or an organized crime group, these are threat actor types, not types of malware. Crypto-malware is a type of ransomware that encrypts data, but there isn't indication that the data is being encrypted in this scenario.

6. **A.** A rootkit typically runs processes that are hidden and it also attempts to connect to computers via the Internet. Although an attacker might have used a backdoor to gain access to the user's computer and install the rootkit, backdoors don't run hidden processes. Spam is unwanted email and is unrelated to this question. A Trojan is malware that looks like it's beneficial, but is malicious.

7. **B.**
Thissoundslikeasocialengineeringattackwherethecallerisattemptingtoget on the servers, so it's appropriate to end the call, report the call to a supervisor, and independently check the vendor for potential issues. It is not appropriate to give external personnel information on internal systems from a single phone call. It isn't necessary to ask for a phone number because you wouldn't call back and give information on the servers. The caller has not committed a crime by asking questions, so it is not appropriate to contact law enforcement personnel.

8. **D.** Tailgating is the practice of following closely behind someone else without using credentials. In this scenario, Bart might be an employee who forgot his badge, or he might be a social engineer trying to get in by tailgating. Spear phishing and whaling are two types of phishing with email. Mantraps prevent tailgating.

9. **B.** Dumpster divers look through trash or recycling containers for valuable paperwork, such as documents that include Personally Identifiable Information (PII). Instead, paperwork should be shredded or incinerated. Vishing is a form of phishing that uses the phone. Shoulder surfers attempt to view monitors or screens, not papers thrown into the trash or recycling containers. Tailgating is the practice of following closely behind someone else, without using proper credentials.

10. **B.** A zero-day exploit is one that isn't known by trusted sources such

as antivirus vendors or operating system vendors. Phishing is malicious spam and it can include malware, but there isn't indication this loss was from an email. Attackers use open-source intelligence to identify a target. Some typical sources are social media sites and news outlets. A hoax is not a specific attack. It is a message, often circulated through email, that tells of impending doom from a virus or other security threat that simply doesn't exist.

11. **B.** Shoulder surfing is the practice of viewing data by looking over someone's shoulder and it includes looking at computer monitors. Positioning monitors so that they cannot be viewed through a window and/or placing screen filters over the monitors reduces this threat. Phishing is an email attack. Dumpster diving is the practice of looking through dumpsters. Social engineers often try to impersonate others to trick them.

12. **D.** Whaling is a type of phishing that targets high-level executives, such as chief financial officers (CFOs) or chief executive officers (CEOs) and this scenario describes an attack targeting the CFO. Because whaling is more specific than phishing, phishing isn't the best answer. Spam is unwanted email, but spam isn't necessarily malicious. While the infected Portable Document File (PDF) might include a Trojan, the scenario doesn't describe the type of malware within the PDF.

13. **A.** A digital signature provides assurances of who sent an email and meets the goal of this scenario. Although a spam filter might filter a spear phishing attack, it does not provide assurances about who sent an email. A training program would help educate employees about attacks and would help prevent the success of these attacks, but it doesn't provide assurances about who sent an email. Some antivirus software includes heuristic-based detection. Heuristic-based detection attempts to detect viruses that were previously unknown and do not have virus signatures.

14. **B.** Of the given choices, an untrained user is the most likely vulnerability in this scenario. A trained user would be less likely to click on a malicious link received in an email. While the attack describes ransomware, ransomware isn't a vulnerability. A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack often results in resource exhaustion, but that is the result of an attack, not a

vulnerability. An insider threat implies a malicious insider, but there isn’t any indication that the new employee was malicious.

15. **D.** The sender is using the social engineering principle of authority in this scenario. A chief executive officer (CEO) would respect legal authorities and might be more inclined to open an attachment from such an authority. While the scenario describes whaling, a specific type of phishing attack, whaling and phishing are attacks, not social engineering principles. The social engineering principle of consensus attempts to show that other people like a product, but this is unrelated to this scenario.