SECURITY FUNDAMENTALS

Relentless is perhaps the best way to describe today's cyberattacks. These attacks, directed against devices ranging from huge cloud computing servers to tiny Internet of Things (IoT) sensors, are designed to steal or manipulate the sensitive data stored in them. The modules in Part 1 introduce security and outline the causes of these attacks. The modules also discuss how to perform security evaluations to identify the weaknesses that need to be addressed to repel attacks.

PART 1

MODULE 1

INTRODUCTION TO SECURITY

After completing this module, you should be able to do the following:

1. Define information security and explain why it is important
2. Identify threat actors and their attributes
3. Describe the different types of vulnerabilities and attacks
4. Explain the impact of attacks

Front-Page Cybersecurity

Threat actors have a long history of using current events to take advantage of distracted and unsuspecting users. For example, whenever a natural disaster such as a hurricane or flood occurs, unscrupulous attackers send out email messages with tempting subject lines such as "Contribute to Disaster Relief Here" or "These Flood Pictures Are Unbelievable!" These messages are, of course, intended to trick a user to open an email attachment that contains malware or click a hyperlink that redirects them to a malicious website.

The 2020 pandemic caused by the coronavirus disease (COVID-19) was no exception. Threat actors used this tragic worldwide event as cover for their attacks. A variety of campaigns distributed malware, stole user credentials, and scammed victims out of their money.

Many email scams offered to sell hard-to-find face masks or even medication to cure COVID-19 infections. Some scams asked for investments in fake companies that claimed to be developing vaccines, while other email scams asked for donations to fictitious charities, such as the World Health Community. (This organization does not exist, but the name is similar enough to the World Health Organization to cause confusion.)

Some malicious emails were designed to infect a victim's computer with malware. Email subject lines such as a "Breaking Coronavirus News Update" or "You Must Do This Right Now!" were common and caused anxious victims to open an attachment that infected their computer. Often emails that pretended to come from the Centers of Disease Control and Prevention (CDC) claimed to contain a list of new COVID-19 cases in the vicinity and included the instructions, "You are instructed to immediately read this list of cases to avoid potential hazards." Unfortunately, opening the attachment installed malware on the computer and stole user passwords.[1]

In one particularly egregious email attack, the threat actors claimed to have access to personal information about the email recipient, including where they lived. The attackers threatened to visit the user to infect them and their family with COVID-19 unless a ransom was paid online. Over a span of two days, this attack was detected more than 1,000 times.

Perhaps the award for the most innovative attack goes to the AI Corona Antivirus website. This site advertised "Corona Antivirus—World's best protection." Downloading and installing its digital "AI Corona Antivirus" would protect the computer

from digital malware infections and keep the user from being infected by the biological COVID-19. In case someone might be skeptical that downloading and installing computer antivirus software would protect them from COVID-19, the website claimed proof that their product actually worked: "Our scientists from Harvard University have been working on a special AI development to combat the virus using a Windows app. Your PC actively protects you against the coronaviruses while the app is running."

However, downloading the AI Corona Antivirus software on a computer did not protect the user from the biological COVID-19—though it took several other actions. It turned the computer into a launching pad to attack other computers. It also took screenshots of what was displayed on the monitor, stole web browser cookies and saved passwords, installed a program to capture keystrokes, and even took any Bitcoin wallets saved on the computer.[2]

How many cyberattacks have you heard about over the past month? The past week? Even today? The number of attacks has reached astronomical proportions. According to one report, the number of new malware releases every month exceeds 20 million, and the total malware in existence is approaching 900 million instances.[3] In 2019, four out of every five organizations experienced at least one successful cyberattack, and more than one-third suffered six or more successful attacks.[4] It is estimated that by 2021, a business will fall victim to a ransomware attack once every 11 seconds. Cybercrime will cost the world $6 trillion annually by 2021, an increase of 100 percent in just six years, representing the greatest transfer of economic wealth in human history.[5] Compounding the problem, 85 percent of organizations are experiencing a shortfall of skilled security professionals.[6] The dismal numbers go on and on.

The need to identify and defend against these constant attacks has created an essential workforce that is now at the core of the information technology (IT) industry. Known as *information security,* personnel in this field are focused on protecting electronic information. Various elements of information security—such as *application security, infrastructure security, forensics and malware analysis,* and *security leadership*, along with several others—make up this workforce.

The information security workforce is usually divided into two broad categories. Information security *managerial personnel* administer and manage plans, policies, and people, while information security *technical personnel* are concerned with designing, configuring, installing, and maintaining technical security equipment. Within these two broad categories are four generally recognized types security positions:

- *Chief information security officer (CISO)*. This person reports directly to the chief information officer (CIO). (Large enterprises may have more layers of management between this person and the CIO.) The CISO is responsible for assessing, managing, and implementing security.
- *Security manager*. The security manager reports to the CISO and supervises technicians, administrators, and security staff. Typically, a security manager works on tasks identified by the CISO and resolves issues identified by technicians. This position requires an understanding of configuration and operation but not necessarily technical mastery.
- *Security administrator*. The security administrator has both technical knowledge and managerial skills. A security administrator manages daily operations of security technology and may analyze and design security solutions within a specific entity as well as identifying users' needs.
- *Security technician*. This position is generally entry level for a person who has the necessary technical skills. Technicians provide technical support to configure security hardware, implement security software, and diagnose and troubleshoot problems.

NOTE 1

The job outlook for security professionals is exceptionally strong. According to the U.S. Bureau of Labor Statistics (BLS) "Occupational Outlook Handbook," the job outlook for information security analysts through 2024 is expected to grow by 18 percent, much faster than the average job growth rate.[8] One report states that by the end of the decade, demand for security professionals worldwide will rise to 6 million, with a projected shortfall of 1.5 million unfilled positions.[9]

As noted earlier, organizations have a desperate need for trained security personnel. The number of unfilled cybersecurity positions has increased by 50 percent since 2015.[7] By some estimates, 3.5 million positions will open by 2021.

When filling cybersecurity positions, an overwhelming majority of enterprises use the Computing Technology Industry Association (CompTIA) Security+ certification to verify security competency. Of the hundreds of security certifications currently available, Security+ is one of the most widely acclaimed security certifications.

Because it is internationally recognized as validating a foundation level of security skills and knowledge, the Security+ certification has become the foundation for today's IT security professionals.

NOTE 2

The value for an IT professional who holds a CompTIA security certification is significant. On average, an employee with a CompTIA certification commands a salary from 5 to 15 times higher than their counterparts with similar qualifications but lacking a certification.[10]

The CompTIA Security+ certification is a vendor-neutral credential that requires passing the current certification exam, SY0-601. A successful candidate has the knowledge and skills required to identify attacks, threats, and vulnerabilities; design a strong security architecture; implement security controls, be knowledgeable of security operations and incident response; and be well versed in governance, risk, and compliance requirements.

NOTE 3

The CompTIA Security+ certification meets the ISO 17024 standard and is approved by U.S. Department of Defense (DoD) to fulfill multiple levels of the DoD 8140 directive, which is an expansion of and replacement for the earlier DoD 8570 directive. This directive outlines which cybersecurity certifications are approved to validate the skills for certain job roles.

This module introduces the security fundamentals that form the basis of the Security+ certification. It begins by defining information security and then examines the attackers and how they function. It also covers vulnerabilities, categories of attacks, and the impacts of attacks.

WHAT IS INFORMATION SECURITY?

The first step in a study of information security is to define exactly what it is. This involves examining the definition of security and how it relates to information security.

Understanding Security

What is *security*? The word comes from Latin, meaning *free from care.* Sometimes security is defined as *the state of being free from danger*, which is the *goal* of security. It is also defined as the *measures taken to ensure safety*, which is the *process* of security. Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal. In this light, security can be defined as *the necessary steps to protect from harm*.

The relationship between *security* and *convenience* is *inversely proportional* (the symbol α), as illustrated in Figure 1-1: as security is increased, convenience is decreased. That is, the more secure something is, the less convenient it may become to use. Consider a house in which the homeowner installs an automated alarm system. The alarm requires a resident to enter a code on a keypad within 30 seconds of entering the house. Although the alarm system makes the house more secure, it is less convenient to race to the keypad than to casually walk into the house.

NOTE 4

Security is often described as *sacrificing convenience for safety.*

Defining Information Security

Several terms describe security in an IT environment: *computer security, IT security, cybersecurity,* and *information assurance*, to name just a few. Whereas each has its share of proponents and slight variations of meanings, the term *information security* may be the most appropriate because it is the broadest: protecting information from harm. Information security is often used to describe the tasks of securing digital information, whether it is manipulated by a microprocessor (such as on a personal computer), preserved on a storage device (such as a hard drive or USB flash drive), or transmitted over a network (such as a local area network or the Internet).

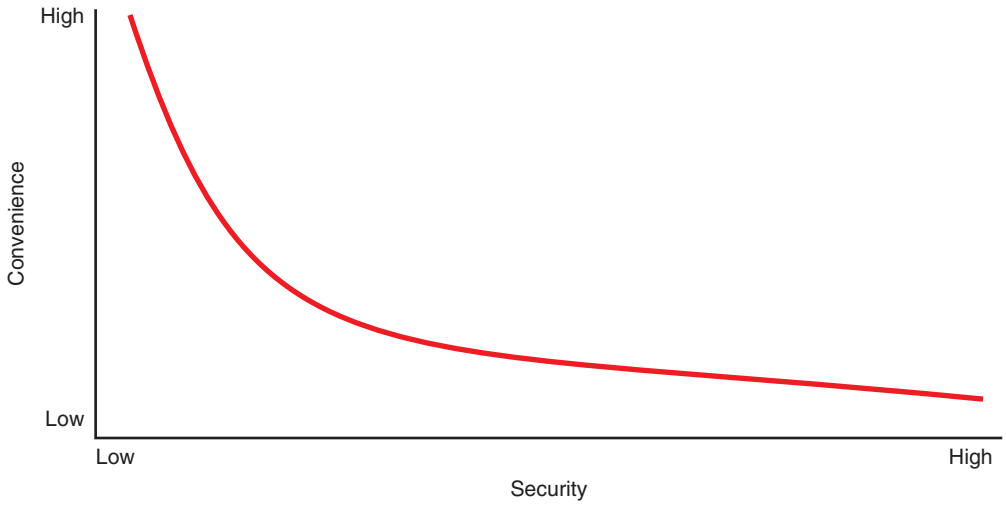


Figure 1-1 Relationship of security to convenience

CAUTION

Information security should not be viewed as a war to win or lose. Just as crimes such as burglary can never be completely eradicated, neither can attacks against technology devices. The goal is not achieving complete victory but instead maintaining equilibrium: as attackers take advantage of a weakness in a defense, defenders must respond with an improved defense. Information security is an endless cycle between attacker and defender.

Information security cannot completely prevent successful attacks or guarantee that a system is totally secure, just as the security measures taken for a house can never guarantee complete safety from a burglar. The goal of information security is to ensure that protective measures are properly implemented to ward off attacks, prevent the total collapse of the system when a successful attack does occur, and recover as quickly as possible. Thus, information security is first *protection*.

Second, information security is intended to protect *information* that provides value to people and enterprises. Known as the *CIA Triad*, three protections must be extended over information:

1. *Confidentiality.* Only approved individuals should be able to access sensitive information. For example, the credit card number used to make an online purchase must be kept secure and unavailable to unapproved entities. *Confidentiality* ensures that only authorized parties can view the information. Providing confidentiality can involve several security tools, ranging from software to encrypt the credit card number stored on the web server to door locks to prevent access to those servers.
2. *Integrity. Integrity* ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of an online purchase, an attacker who could change the amount of a purchase from $10,000.00 to $1.00 would violate the integrity of the information.
3. *Availability.* Information has value if the authorized parties who are assured of its integrity can access the information. *Availability* ensures that data is accessible to only authorized users and not to unapproved individuals. For example, the total number of items ordered as the result of an online purchase must be made available to an employee in a warehouse so that the correct items can be shipped to the customer, but the information should not be available to a competitor.

Because information is stored on computer hardware, manipulated by software, and transmitted by communications, each of these areas must be protected. The third objective of information security is to protect the integrity, confidentiality, and availability of information *on the devices that store, manipulate, and transmit the information.*

Protection is achieved through a process that combines three entities. As shown in Figure 1-2, information and hardware, software, and communications are protected in three layers: *products*, *people*, and *policies and procedures*. The procedures enable people to understand how to use products to protect information.

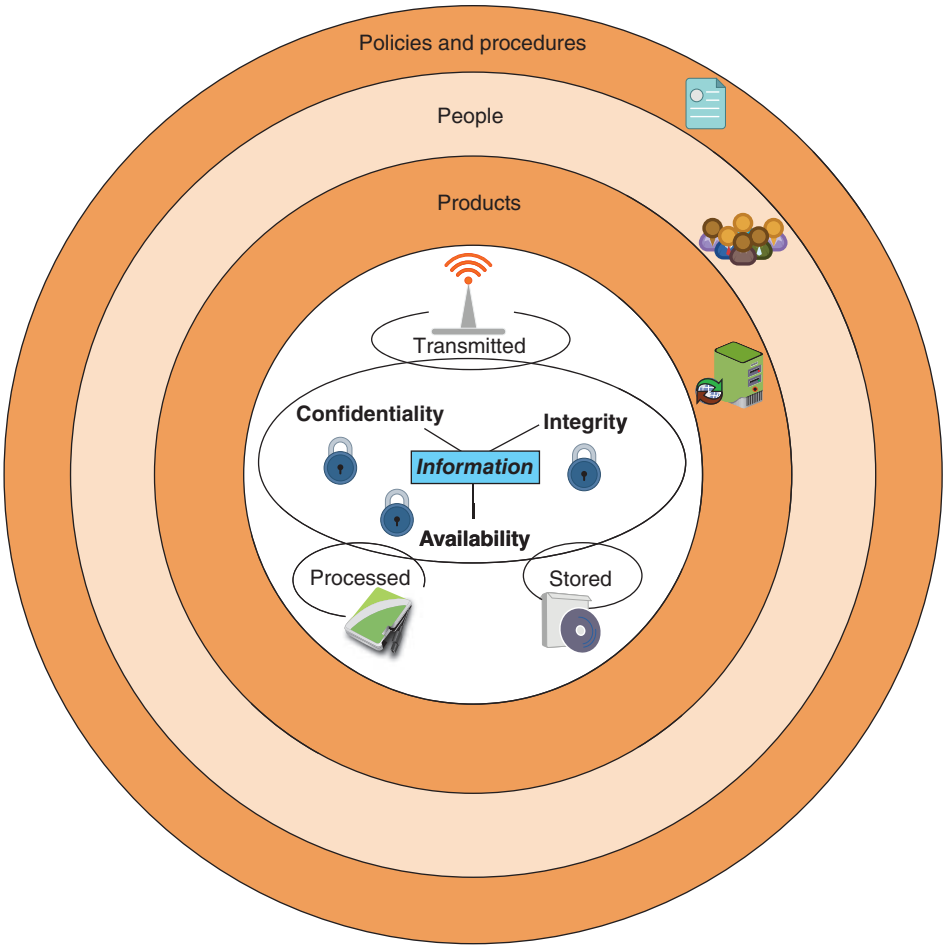


Figure 1-2 Information security layers

Thus, information security may be defined as *that which protects the integrity, confidentiality, and availability of information through products, people, and procedures on the devices that store, manipulate, and transmit the information.*

TWO RIGHTS & A WRONG

1. A security manager works on tasks identified by the CISO and resolves issues identified by technicians.
2. Since 2015, the number of unfilled cybersecurity positions has increased by 10 percent.
3. The relationship between security and convenience is inversely proportional: as security is increased, convenience is decreased.

See Appendix B for the answer.

WHO ARE THE THREAT ACTORS?

CERTIFICATION

1.5 Explain different threat actors, vectors, and intelligence sources.

In cybersecurity, a **threat actor** (also called a *malicious actor*) is an individual or entity responsible for cyber incidents against the technology equipment of enterprises and users. The generic term *attacker* is also commonly used.

The very first cyberattacks were mainly for the threat actors to show off their technology skills (*fame*). However, that soon gave way to threat actors with the focused goal of financial gain (*fortune*). Financial cybercrime is often divided into three categories based on its targets:

- *Individual users*. The first category focuses on individuals as the victims. The threat actors steal and use stolen data, credit card numbers, online financial account information, or Social Security numbers to profit from their victims or send millions of spam emails to peddle counterfeit drugs, pirated software, fake watches, and pornography.
- *Enterprises*. The second category focuses on enterprises and business organizations. Threat actors attempt to steal research on a new product so that they can sell it to an unscrupulous foreign supplier who then builds an imitation model of the product to sell worldwide. This deprives the legitimate business of profits after investing hundreds of millions of dollars in product development, and because these foreign suppliers are in a different country, they are beyond the reach of domestic enforcement agencies and courts.
- *Governments*. Governments are also the targets of threat actors. If the latest information on a new missile defense system can be stolen, it can be sold—at a high price—to that government's enemies. In addition, government information is often stolen and published to embarrass the government in front of its citizens and force it to stop what is considered a nefarious action.

The **attributes**, or characteristic features, of the groups of threat actors can vary widely. Some groups have a high level of power and complexity (called **level of capability/sophistication**) with a massive network of resources, while others are "lone wolves" with minimal skills and no resources. In addition, some groups have deep **resources and funding** while others have none. Whereas some groups of threat actors may work within the enterprise (**internal**), others are strictly outside the organization (**external**). Finally, the **intent/motivation**—that is, the reason for the attacks—of the threat actors also varies widely.

In the past, the term **hacker** referred to a person who used advanced computer skills to attack computers. Because that title often carried a negative connotation, it was qualified in an attempt to distinguish between different types of the attackers. The types of hackers are summarized in Table 1-1.

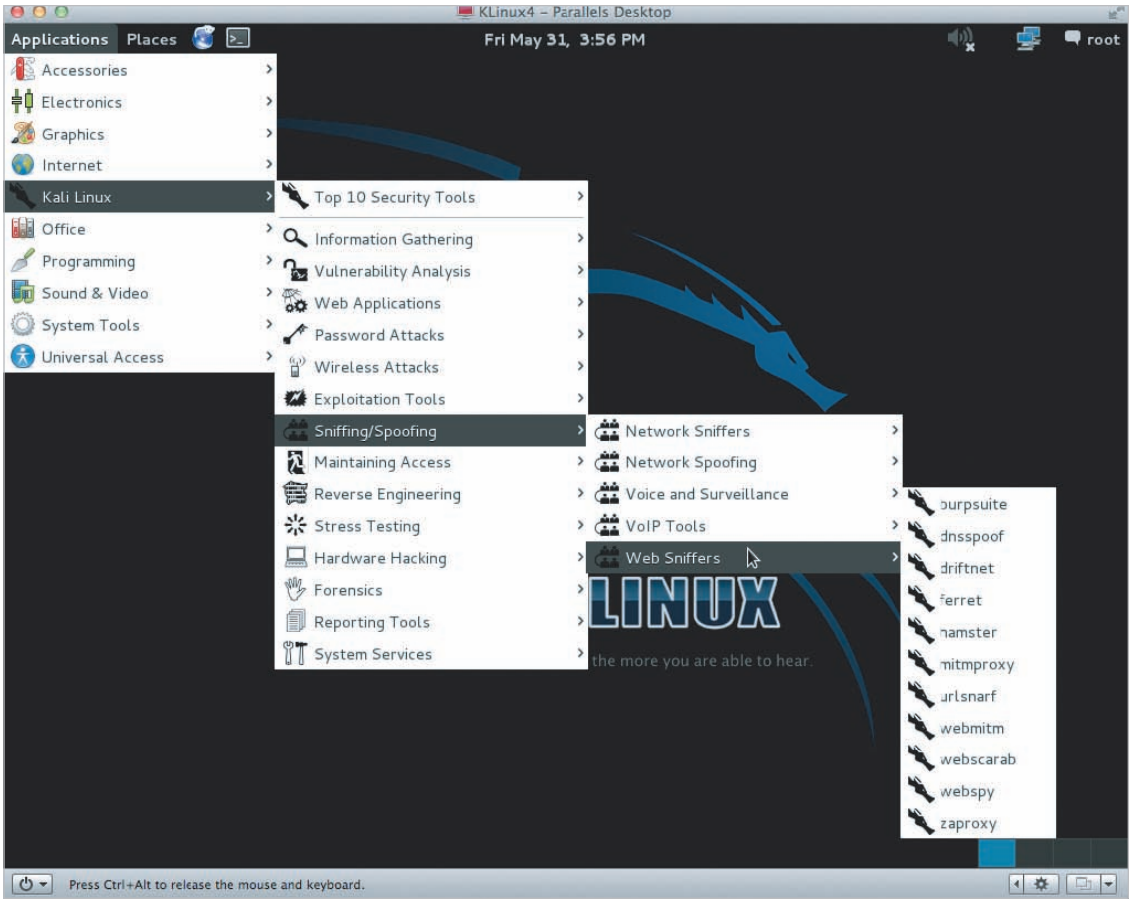
Table 1-1 Types of hackers

Hacker Type	Description
Black hat hackers	Threat actors who violate computer security for personal gain (such as to steal credit card numbers) or to inflict malicious damage (corrupt a hard drive).
White hat hackers	Also known as *ethical attackers*, they attempt to probe a system (with an organization's permission) for weaknesses and then privately provide that information back to the organization.
Gray hat hackers	Attackers who attempt to break into a computer system without the organization's permission (an illegal activity) but not for their own advantage; instead, they publicly disclose the attack in order to shame the organization into taking action.

However, these broad categories of hackers no longer accurately reflect the differences between attackers. Today threat actors are classified in more distinct categories, such as script kiddies, hacktivists, state actors, insiders, and others.

Script Kiddies

Script kiddies are individuals who want to perform attacks, yet lack the technical knowledge to carry them out. Script kiddies instead do their work by downloading freely available automated attack software (*scripts*) and use it to perform malicious acts. Figure 1-3 illustrates a widely available software package that launches a sophisticated attack when a user simply makes selections from a menu. Due to their lack of knowledge, script kiddies are not always successful in penetrating defenses, but when they are, they may end up causing damage to systems and data instead of stealing the data.



Source: Kali Linux

Figure 1-3 Menu of attack tools

Hacktivists

Individuals that are strongly motivated by ideology (for the sake of their principles or beliefs) are **hacktivists** (a combination of the words *hack* and *activism*). Most hacktivists do not explicitly call themselves "hacktivists," but the term is commonly used by security researchers and journalists to distinguish them from other types of threat actors.

In the past, the types of attacks by hacktivists often involved breaking into a website and changing its contents as a means of making a political statement. (One hacktivist group changed the website of the U.S. Department of Justice to read *Department of Injustice*.) Other attacks were retaliatory: hacktivists have disabled a bank's website because the bank stopped accepting online payments deposited into accounts belonging to groups supported by the hacktivists. Today many hacktivists work through disinformation campaigns by spreading fake news and supporting conspiracy theories.

NOTE 5

Hacktivists were particularly active during the coronavirus disease (COVID-19) pandemic of 2020. One large group of what were considered far-right neo-Nazi hacktivists embarked on a months-long disinformation campaign designed to weaponize the pandemic by questioning scientific evidence and research. In another instance, thousands of breached email addresses and passwords from U.S. and global health organizations—including the U.S. National Institutes of Health, CDC, and the World Health Organization—were distributed on Twitter by these groups to harass and distract the health organizations.

State Actors

Instead of using an army to march across the battlefield to strike an adversary, governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes. These attackers are known as **state actors**. Their foes may be foreign governments or even citizens of their own nation that the government considers

hostile or threatening. A growing number of attacks from state actors are directed toward businesses in foreign countries with the goal of causing financial harm or damage to the enterprise's reputation.

Many security researchers believe that state actors might be the deadliest of any threat actors. When fortune motivates a threat actor, but the target's defenses are too strong, the attacker simply moves on to another promising target with less effective defenses. State actors, however, have a specific target and keep working until they are successful. They are highly skilled and have enough government resources to breach almost any security defense.

State actors are often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. The campaigns have created a new class of attacks called **advanced persistent threat (APT)**. The attacks use innovative tools (*advanced*) and once a system is infected, they silently extract data over an extended period of time (*persistent*). APTs are most commonly associated with state actors.

Insiders

Another serious threat to an enterprise comes from its own employees, contractors, and business partners, called *insiders*, who pose an **insider threat** of manipulating data from the position of a trusted employee. For example, a healthcare worker disgruntled about being passed over for a promotion might illegally gather health records on celebrities and sell them to the media, or a securities trader who loses billions of dollars on bad stock bets could use her knowledge of the bank's computer security system to conceal the losses through fake transactions. These attacks are harder to recognize because they come from within the enterprise, yet they may be costlier than attacks from the outside.

Six out of 10 enterprises reported being a victim of at least one insider attack during 2019. The focus of the insiders was intellectual property (IP) theft (43 percent), sabotage (41 percent), and espionage (32 percent).[11] Because most IP thefts occur within 30 days of an employee resigning, the insiders may believe that either the IP belongs to them instead of the enterprise or that they were not properly compensated for their work on the IP. In recent years, government insiders have stolen large volumes of sensitive information and then published it to alert its citizens of clandestine governmental actions.

Other Threat Actors

Other categories of threat actors are summarized in Table 1-2.

Table 1-2 Descriptions of other threat actors

Threat Actor	Description	Explanation
Competitors	Launch attacks against an opponent's system to steal classified information.	May steal new product research or a list of current customers to gain a competitive advantage.
Criminal syndicates	Move from traditional criminal activities to more rewarding and less risky online attacks.	Usually run by a small number of experienced online criminal networks that do not commit crimes themselves but act as entrepreneurs.
Shadow IT	Employees become frustrated with the slow pace of acquiring technology, so they purchase and install their own equipment or resources in violation of company policies.	Installing personal equipment, unauthorized software, or using external cloud resources can create a weakness or expose sensitive corporate data.
Brokers	Sell their knowledge of a weakness to other attackers or governments.	Individuals who uncover weaknesses do not report it to the software vendor but instead sell them to the highest bidder who is willing to pay a high price for the unknown weakness.
Cyberterrorists	Attack a nation's network and computer infrastructure to cause disruption and panic among citizens.	Targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.

CAUTION

Often the perception of an attacker by the general public is a "hacker in a hoodie," a disgruntled teenager looking for an easy target. Nothing could be further from the truth. Threat actors today generally have excellent technology skills, are tenacious, and have strong financial backing. Attackers have even modeled their work after modern economic theories (such as finding the optimum "price point" in which victims will pay a ransom) and software development (attack tools that threat actors sell are often software suites that receive regular updates). It is a serious mistake to underestimate modern threat actors.

TWO RIGHTS & A WRONG

1. Script kiddies are responsible for the class of attacks called advanced persistent threats.
2. Hacktivists are strongly motivated by ideology.
3. Brokers sell their knowledge of a weakness to other attackers or a government.

See Appendix B for the answer.

VULNERABILITIES AND ATTACKS

CERTIFICATION

1.1 Compare and contrast different types of social engineering techniques.

1.5 Explain different threat actors, vectors, and intelligence sources.

1.6 Explain the security concerns associated with various types of vulnerabilities.

When exploiting vulnerabilities, threat actors use several avenues for their attacks. However, one of the most successful types of attack—social engineering—does not even exploit technology vulnerabilities. Regardless of how attacks occur, each successful attack has serious ramifications.

Vulnerabilities

A *vulnerability* (from Latin meaning *wound*) is defined as the state of being exposed to the possibility of being attacked or harmed. Cybersecurity vulnerabilities can be categorized into platforms, configurations, third parties, patches, and zero-day vulnerabilities.

Platforms

Several vulnerabilities are the result of the *platform* being used. (A computer platform is a system that consists of the hardware device and an operating system (OS) that runs software such as applications, programs, or processes.) Although all platforms have vulnerabilities to some degree, some platforms by their very nature have more serious vulnerabilities. These include legacy platforms, on-premises platforms, and cloud platforms.

Legacy Platforms One type of platform that is well known for its vulnerabilities is a legacy platform. A **legacy platform** is no longer in widespread use, often because it has been replaced by an updated version of the earlier technology. Although legacy hardware introduces some vulnerabilities, more often vulnerabilities result from legacy software, such as an OS or program.

Modern OS software, such as Microsoft Windows, Apple macOS, and Linux, continually evolve and are updated with new enhancements and—most critically—fixes to uncovered vulnerabilities. For a variety of reasons—limited hardware capacity, an application that only operates on a specific OS version, or even neglect—an OS may not be updated, thus depriving it of these security fixes. This creates a legacy platform just asking to be attacked.

NOTE 6

Prior to Microsoft Windows 10, all versions of the OS had a *Fixed Lifecycle Policy* with published end-of-support dates. For instance, Windows 7 was first released in October 2009, it was no longer available for purchase in October 2016, and all support ceased in January 2020. Windows 10, however, introduced the *Modern Lifecycle Policy* in which Windows 10 versions receive continuous support and servicing.

On-Premises Platforms Another platform that has significant vulnerabilities is the **on-premises platform**. On-premises ("on-prem") is the software and technology located within the physical confines of an enterprise, which is usually consolidated in the company's *data center*. At one time, the on-premises platform was considered the secure model of computing: an organization's servers and data were protected behind its firewalls to prevent attacks.

However, this model proved to be faulty. Organizations found that they had to add more servers, network resources, support for remote access, and new software to support emerging business processes and user needs. This often resulted in a hodgepodge of resources that were quickly provisioned but not adequately configured for security. In addition, numerous entry points from the outside into the on-premises platform (through USB flash drives, wireless network transmissions, mobile devices, and email messages, for example) made protecting the on-premises platform an ever-changing and never-ending challenge.

Cloud Platforms Forty years ago, as computing technology became widespread, enterprises employed an on-premises model, in which they purchased all the hardware and software necessary to run the organization. As more resources were needed, more purchases were made, and more personnel were hired to manage the technology. Because this resulted in spiraling costs, some enterprises turned to *hosted services*.

In a hosted services environment, servers, storage, and the supporting networking infrastructure are shared by multiple enterprises over a remote network connection that has been contracted for a specific period of time. As more resources are needed (such as additional storage space or computing power), the enterprise contacts the hosted service, negotiates an additional fee, and signs a new contract for those new services.

Today a new model is gaining widespread use. Known as a **cloud platform**, this is a pay-per-use computing model in which customers pay only for the online computing resources they need. As computing needs increase or decrease, cloud computing resources can be scaled up or scaled back.

However, cloud platforms have proven to have significant vulnerabilities. The vulnerabilities are most often based on misconfigurations by the company personnel responsible for securing the cloud platform. Cloud resources are, by definition, accessible from virtually anywhere, putting cloud computing platforms constantly under attack from threat actors probing for vulnerabilities.

Configurations

Modern hardware and software platforms provide an array of features and security settings that must be properly configured to repel attacks. However, the configuration settings are often not properly implemented, resulting in **weak configurations**. Table 1-3 lists several weak configurations that can result in vulnerabilities.

Table 1-3 Weak configurations

Configuration	Explanation	Example
Default settings	Default settings are predetermined by the vendor for usability and ease of use (not for security) so the user can immediately begin using the product.	A router comes with a default password that is widely known.
Open ports and services	Devices and services are often configured to allow the most access so that the user can close ports that are specific to that organization.	A firewall comes with FTP ports 20 and 21 open.
Unsecured root accounts	A root account can give a user unfettered access to all resources.	A misconfigured cloud storage repository could give any user access to all data.

(continues)

Table 1-3 Weak configurations *(continued)*

Configuration	Explanation	Example
Open permissions	Open permissions are user access over files that should be restricted.	A user could be given *Read, Write*, and *Execute* privileges when she should have only *Read* privileges.
Unsecure protocols	Also called *insecure protocols,* this configuration uses protocols for telecommunications that do not provide adequate protections.	An employee could use devices that run services with unsecure protocols such as *Telnet* or *SNMPv1*.
Weak encryption	Users choosing a known vulnerable encryption mechanism.	A user could select an encryption scheme that has a known weakness or a key value that is too short.
Errors	Human mistakes in selecting one setting over another without considering the security implications.	An employee could use deprecated settings instead of current configurations.

Third Parties

Almost all businesses use external entities known as **third parties**. Examples of third parties are marketing agencies, landscapers, shredding contractors, and attorneys.

Many enterprises also use IT-related third parties due to their elevated level of expertise. For example, organizations often contract with third parties to assist them in developing and writing a software program or app. This is called **outsourced code development**. Also, many organizations rely on third-party **data storage** facilities for storing important data. This helps to reduce the capital expenditures associated with purchasing, installing, and managing new storage hardware and software but also can provide remote access to employees from almost any location.

With the sheer number of third parties used, it can be difficult to coordinate their diverse activities with the organization. **Vendor management** is the process organizations use to monitor and manage the interactions with all of their external third parties.

Almost all third parties today require access to the organization's computer network. Access gives external entities the ability to perform their IT-related functions (such as outsourced code development) and even do basic tasks such as submitting online invoices. Connectivity between the organization and the third party is known as **system integration**. However, the organization's systems are often not compatible with the third party's systems, requiring "workarounds," which can create vulnerabilities. In addition, not all organizations are equipped with the expertise to handle system integration (**lack of vendor support**).

One of the major risks of third-party system integration involves the principle of the weakest link. That is, if the security of the third party has any weaknesses, it can provide an opening for attackers to infiltrate the organization's computer network. This can be illustrated by a 2013 attack on the Target retail chain. A refrigeration, heating, and air-conditioning third-party subcontractor that worked at a number of Target stores and other top retailers was provided access to Target's corporate computer network. The access was intended to allow the subcontractor to monitor energy consumption and temperatures in the stores to save on costs and to alert store managers if the temperatures fluctuated outside of an acceptable range. However, threat actors were able to gain access to the third party's computer network and then pivot into the Target network, where they stole 40 million credit card numbers.

Patches

Early OSs were simply program loaders whose job was to launch applications. As more features and graphical user interfaces (GUIs) were added, OSs became more complex. The increased complexity introduced unintentional vulnerabilities that

NOTE 7

One of the most alarming recent unsecured root account vulnerabilities was revealed in 2017 on the Apple macOS High Sierra OS. A user could enter the word *root* in the username field of a login prompt, move the insertion point to the password field, and then press Enter. The user would then be logged in with root privileges.

NOTE 8

Microsoft's first operating system, MS-DOS v1.0, had 4,000 lines of code, while Windows 10 is estimated to have up to 50 million lines.

could be exploited by attackers. In addition, new attack tools made vulnerable what were once considered secure functions and services in operating systems.

To address the vulnerabilities in OSs that are uncovered after the software has been released, software developers usually deploy a software "fix." A fix can come in a variety of formats. A security **patch** is an officially released software security update intended to repair a vulnerability.

However, as important as patches are, they can create vulnerabilities:

- *Difficulty patching firmware*. **Firmware**, or software that is embedded into hardware, provides low-level controls and instructions for the hardware. Updating firmware to address a vulnerability can often be difficult and requires specialized steps. Furthermore, some firmware cannot be patched.
- *Few patches for application software*. Outside of the major application software such as Microsoft Office, patches for applications are uncommon. In most cases, no automated process can identify which computers have installed the application, alert users to a patch, or to distribute the patch.
- *Delays in patching OSs*. Modern operating systems—such as Red Hat Linux, Apple macOS, Ubuntu Linux, and Microsoft Windows—frequently distribute patches. These patches, however, can sometimes create new problems, such as preventing a custom application from running correctly. Many organizations test patches when they are released to ensure that they do not adversely affect any customized applications. In these instances, the organization delays installing a patch from the developer's online update service until the patch is thoroughly tested.

NOTE 9

A variation on a zero-day vulnerability is when the software developer is actively working on a patch, but the vulnerability is discovered by the threat actors who launch an attack before the patch is completed. This could occur when an independent security investigator instead of the software developer uncovers the vulnerability and then alerts the developer who begins work on a patch. However, in the interim, the information about the vulnerability leaks out or is even sold to attackers, who exploit the vulnerability while the developers rush to patch it.

Zero Day

As noted earlier, patches are created and distributed when the software developer learns of a vulnerability and corrects it. What happens if it is not the developer who uncovers the vulnerability, but a threat actor who finds it first? In this case, the vulnerability can be exploited by attackers before anyone else even knows it exists. This type of vulnerability is called a **zero day** because it provides zero days of warning.

Zero-day vulnerabilities are considered extremely serious: systems are open to attack with no specific patches available. However, other protections can mitigate a zero-day attack. For example, some protections use machine learning to collect data from previously detected exploits and create a baseline of safe system behavior that may help detect an attack based on a zero-day vulnerability.

Attack Vectors

An **attack vector** is a pathway or avenue used by a threat actor to penetrate a system. Although there are many specific types of attacks, like vulnerabilities, attack vectors can be grouped into the following general categories:

- *Email*. Almost 94 percent of all malware is delivered through email to an unsuspecting user.[12] The goal is to trick the user to open an attachment that contains malware or click a hyperlink that takes the user to a fictitious website.
- *Wireless*. Because wireless data transmissions "float" through the airwaves, they can be intercepted and read or altered by a threat actor if the transmission is not properly protected.
- *Removable media*. A removable media device, such as a USB flash drive, is a common attack vector. Threat actors have been known to infect USB flash drives with malware and leave them scattered in a parking lot or cafeteria. A well-intentioned employee will find the drive and insert it into his computer to determine its owner. However, once inserted, the USB flash drive will infect the computer.
- *Direct access*. A **direct access** vector occurs when a threat actor can gain direct physical access to the computer. Once the attacker can "touch" the machine, she can insert a USB flash drive with an alternative operating system and reboot the computer under the alternate OS to bypass the security on the computer.

- *Social media*. Threat actors often use social media as a vector for attacks. For example, an attacker may read social media posts to determine when an employee will be on vacation and then call the organization's help desk pretending to be that employee to ask for "emergency" access to an account.
- *Supply chain*. A **supply chain** is a network that moves a product from the supplier to the customer and is made up of vendors that supply raw material, manufacturers who convert the material into products, warehouses that store products, distribution centers that deliver them to the retailers, and retailers who bring the product to the consumer. Today's supply chains are global in scope: manufacturers are usually thousands of miles away overseas and not under the direct supervision of the enterprise selling the product. The fact that products move through many steps in the supply chain—and that some steps are not closely supervised—has opened the door for malware to be injected into products during their manufacturing or storage (called *supply chain infections*). Supply chains also serve as third-party vulnerabilities.

CAUTION

Supply chain infections are considered especially dangerous. Users are receiving infected devices at the point of purchase, unaware that a brand-new device may be infected. Also, there is rarely any way to contact users and inform them of an infected device. Because it is virtually impossible to closely monitor every step in the global supply chain, these infections cannot be easily prevented.

- *Cloud*. As enterprises move their computing resources to remote cloud servers and storage devices, threat actors take advantage of the complexity of these systems to find security weaknesses.

Social Engineering Attacks

Not all attacks rely on technology vulnerabilities; in fact, some cyberattacks use little if any technology to achieve their goals. **Social engineering** is a means of **eliciting information** (gathering data) by relying on the weaknesses of individuals. Information elicitation may be the goal of the attack, or the information may then be used for other attacks. Social engineering is also used as **influence campaigns** to sway attention and sympathy in a particular direction. These campaigns can be found exclusively on social media (**social media influence campaign**) or may be combined with other sources (**hybrid warfare influence campaign**).

Social engineering attacks usually rely on psychological principles. They also can involve physical procedures.

Psychological Principles

Many social engineering attacks rely on psychology to affect others mentally and emotionally rather than physically. At its core, social engineering relies on an attacker's clever manipulation of human nature to persuade the victim to provide information or take actions. Several basic principles make psychological social engineering highly effective. These are listed in Table 1-4 with the example of an attacker pretending to be the chief executive officer (CEO) calling the organization's help desk to reset a password.

Table 1-4 Social engineering effectiveness

Principle	Description	Example
Authority	To impersonate an authority figure or falsely cite their authority	"I'm the CEO calling."
Intimidation	To frighten and coerce by threat	"If you don't reset my password, I will call your supervisor."
Consensus	To influence by what others do	"I called last week, and your colleague reset my password."

(continues)

Table 1-4 Social engineering effectiveness *(continued)*

Principle	Description	Example
Scarcity	To refer to something in short supply	"I can't waste time here."
Urgency	To demand immediate action	"My meeting with the board starts in five minutes."
Familiarity	To give the impression the victim is well known and well received	"I remember reading a good evaluation on you."
Trust	To inspire confidence	"You know who I am."

Another technique is called **prepending**, which is influencing the subject before the event occurs. A common general example is a preview of a soon-to-be-released movie that begins with the statement, "The best film you will see this year!" By starting with the desired outcome ("The best film"), the statement influences the listener to think that way. Threat actors use prepending with social engineering attacks, such as including the desired outcome in a statement that uses the urgency principle, as in "You need to reset my password immediately because my meeting with the board starts in five minutes."

Because many of the psychological approaches involve person-to-person contact, attackers use a variety of techniques to gain trust. For example:

- *Provide a reason*. Many social engineering threat actors are careful to add a reason along with their request. Giving a rationalization and using the word "because" makes it more likely the victim will provide the information. For example, *I was asked to call you because the director's office manager is out sick today.*
- *Project confidence*. A threat agent is unlikely to generate suspicion if she enters a restricted area by calmly walking through the building as if she knows exactly where she going (without looking at signs, down hallways, or reading door labels) and even greeting people she sees with a friendly *Hi, how are you doing?*
- *Use evasion and diversion*. When challenged, threat agents might evade a question by giving a vague or irrelevant answer. They could also feign innocence or confusion, or keep denying allegations, until the victim eventually believes his suspicions are wrong. Sometimes a threat agent can resort to anger and cause the victim to drop the challenge. *Who are you to ask that? Connect me with your supervisor immediately!*
- *Make them laugh*. Humor is an excellent tool to put people at ease and to develop a sense of trust. *I can't believe I left my badge in my office again! You know, some mistakes are too much fun to make only once!*

Social engineering psychological approaches often involve impersonation, phishing, redirection, spam, hoaxes, and watering hole attacks.

Impersonation Social engineering **impersonation** (also called **identity fraud**) is masquerading as a real or fictitious character and then playing the role of that person with a victim. For example, an attacker could impersonate a help desk support technician who calls the victim, pretends that there is a problem with the network, and asks for her username and password to reset the account. Sometimes the goal of the impersonation is to obtain private information (**pretexting**).

CAUTION

Common roles that are often impersonated include a repair person, an IT support technician, a manager, or a trusted third party. Often attackers impersonate individuals whose roles are authoritative because victims generally resist saying "no" to anyone in power. Users should exercise caution when receiving a phone call or email from these types of people asking for something suspicious.

To impersonate real people, the threat actor must know as much about them as possible to appear genuine. This type of **reconnaissance** is called **credential harvesting** and is typically carried out by Internet and social media searches.

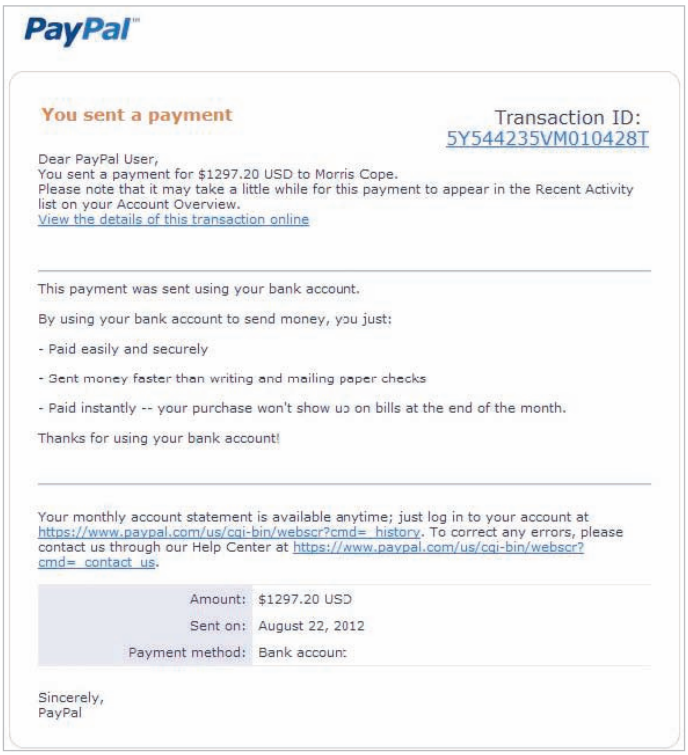
Phishing One of the most common forms of social engineering is phishing. **Phishing** is sending an email message or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user

into surrendering private information or taking action. Users are asked to respond to an email message or are directed to a website where they are requested to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information. However, the email or website is actually an imposter site set up to steal the information the user enters. Users may also receive a fictitious overdue invoice that demands immediate payment and, in haste, make the payment (called an **invoice scam**).

NOTE 10

The word *phishing* is a variation on the word "fishing," to reflect the idea that bait is thrown out knowing that while most will ignore it, some will bite.

Whereas at one time phishing messages were easy to spot due to misspelled words and obvious counterfeit images, that is no longer the case. In fact, one reason that phishing is so successful today is that the emails and the fake websites are difficult to distinguish from legitimate ones: logos, color schemes, and wording seem to be almost identical. Figure 1-4 illustrates an actual phishing email message that looks like it came from a legitimate source.



PayPal

You sent a payment

Transaction ID: 5Y544235VM010428T

Dear PayPal User,
You sent a payment for $1297.20 USD to Morris Cope.
Please note that it may take a little while for this payment to appear in the Recent Activity list on your Account Overview.
View the details of this transaction online

This payment was sent using your bank account.

By using your bank account to send money, you just:

- Paid easily and securely
- Sent money faster than writing and mailing paper checks
- Paid instantly -- your purchase won't show up on bills at the end of the month.

Thanks for using your bank account!

Your monthly account statement is available anytime; just log in to your account at https://www.paypal.com/us/cgi-bin/webscr?cmd=_history. To correct any errors, please contact us through our Help Center at https://www.paypal.com/us/cgi-bin/webscr?cmd=_contact_us.

Amount:	$1297.20 USD
Sent on:	August 22, 2012
Payment method:	Bank accoun:

Sincerely,
PayPal

Source: Email message sent to Dr. Mark Revels

Figure 1-4 Phishing email message

CAUTION

Phishing is also used to validate email addresses. A phishing email message can display an image retrieved from a website and requested when the user opens the email message. A unique code links the image to the recipient's email address, which then tells the phisher that the email address is active and valid. This is the reason most email today does not automatically display images received in emails. Users should be cautious in displaying images in email messages.

The following are several variations on phishing attacks:

- *Spear phishing.* Whereas phishing involves sending millions of generic email messages to users, **spear phishing** targets specific users. The emails used in spear phishing are customized to the recipients, including their names and personal information, to make the message appear legitimate.
- *Whaling.* One type of spear phishing is **whaling**. Instead of going after the "smaller fish," whaling targets the "big fish"—namely, wealthy individuals or senior executives within a business who typically have large sums of money in a bank account that an attacker could access if the attack is successful. By focusing on this smaller

group, the attacker can invest more time in the attack and finely tune the message to achieve the highest likelihood of success.

- *Vishing.* Instead of using email to contact the potential victim, attackers can use phone calls. Known as **vishing** (*v*oice ph*ishing*), an attacker calls a victim who, upon answering, hears a recorded message that pretends to be from the user's bank stating that her credit card has experienced fraudulent activity or that her bank account has had unusual activity. The victim is instructed to call a specific phone number immediately (which has been set up by the attacker). When the victim calls, it is answered by automated instructions telling her to enter her credit card number, bank account number, Social Security number, or other information on the phone's keypad.
- *Smishing.* A variation on vishing uses short message service (SMS) text messages and callback recorded phone messages. This is known as **smishing**. The threat actors first send a text message to a user's cell phone that pretends to come from their bank saying that their account has been broken into or their credit card number has been stolen. Along with the text message is a callback telephone number the customer is instructed to call immediately. That phone number plays a recording telling the customer to enter their Social Security number or credit card number for verification. The attackers then simply capture the information the user enters.

Phishing continues to be a primary weapon used by threat actors. Phishing is considered to be one of the largest and most consequential cyber threats facing both businesses and consumers. During the third quarter of 2019, phishing attacks increased by 46 percent from the previous quarter and almost doubled the number recorded during the fourth quarter of the previous year. One nation saw a 232 percent increase in phishing during 2019.[13] It is estimated that these trends will continue.

CAUTION Although most web browsers automatically block known phishing websites, because so many sites are appearing so rapidly, it is difficult for the browsers to stay up to date. Users should remain constantly vigilant to guard against phishing attacks.

NOTE 11

The cost of typo squatting is significant because of frequent misspellings. In one month, the typo squatting site *goggle.com* received almost 825,000 unique visitors. It is estimated that typo squatting costs the 250 top websites $285 million annually in lost sales and other expenses.[14]

NOTE 12

An increasing number of registered attacker domains are the result of bitsquatting, such as *aeazon.com* (for *amazon.com*) and *microsmft.com* (for *microsoft.com*). Security researchers found that 20 percent of a sample of 433 registered attacker domains were the result of bitsquatting.[15]

Redirection If threat actors cannot trick a user to visit a malicious website through phishing, they can use other tactics to redirect the user.

What happens if a user makes a typing error when entering a uniform resource locator (URL) address in a web browser, such as typing *goggle.com* (a misspelling) or *google.net* (incorrect domain) instead of the correct *google.com*? In the past, an error message like *HTTP Error 404 Not Found* would appear. However, today the user is often directed to a fake lookalike site filled with ads for which the attacker receives money for traffic generated to the site. These fake sites exist because attackers purchase the domain names of sites that are spelled similarly to actual sites. This is called **typo squatting**. A well-known site such as *google.com* may have to deal with more than 1,000 typo squatting domains.

Enterprises have tried to preempt typo squatting by registering the domain names of close spellings of their website. At one time, top-level domains (TLDs) were limited to .com, .org, .net, .int, .edu, .gov, and .mil, so it was fairly easy to register close-sounding domain names. However, today there are more than 1,200 generic TLDs (gTLDs), such as .museum, .office, .global, and .school. Organizations must now attempt to register many sites that are a variation of their registered domain name.

In addition to registering names similar to the actual names (like *goggle.com* for *google.com*), threat actors are registering domain names that are *one bit* different. The billions of devices that are part of the Internet have multiple instances of a domain name in a domain name server (DNS) memory at any time, increasing the likelihood of a RAM memory error that involves a bit being "flipped." Figure 1-5 illustrates that the change of one bit in the letter *g* (0110011*1*) results in the change of the entire character from *g* to *f*. In this example, a threat agent would register the domain *foo.gl* as a variation of the actual *goo.gl*.

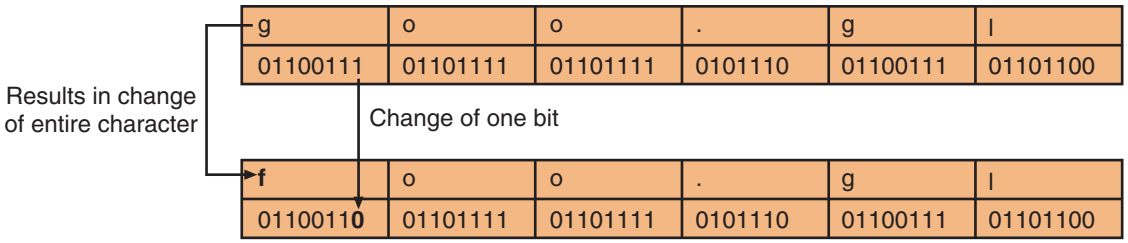


Figure 1-5 Character change by bit flipping

Another redirection technique is **pharming**. Pharming attempts to exploit how a URL such as www.cengage.com is converted into its corresponding IP address *69.32.308.75*. A threat actor may install malware on a user's computer that redirects traffic away from its intended target to a fake website instead. Another technique is to infect a DNS that would direct multiple users to inadvertently visit the fake site.

Spam **Spam** is unsolicited email that is sent to a large number of recipients. Users receive so many spam messages because sending spam is lucrative. It costs spammers very little to send millions of spam email messages. Almost all spam is sent from botnets, and a spammer who does not own his own botnet can lease time from other attackers ($40 per hour) to use a botnet of up to 100,000 infected computers to launch a spam attack. Even if spammers receive only a small percentage of responses, they still make a large profit. For example, if a spammer sent spam to 6 million users for a product with a sale price of $50 that cost only $5 to make, and if only 0.001 percent of the recipients responded and bought the product (a typical response rate), the spammer would still make more than $270,000 in profit.

Text-based spam messages that include words such as *Viagra* or *investments* can easily be trapped by filters that look for these words and block the email. Because of the increased use of these filters, spammers have turned to *image spam*, which uses graphical images of text in order to circumvent text-based filters. Image spam cannot be filtered based on the textual content of the message because it appears as an image instead of text. These spam messages often include nonsense text so that it appears the email message is legitimate (an email with no text can prompt the spam filter to block it). Figure 1-6 shows an example of an image spam.

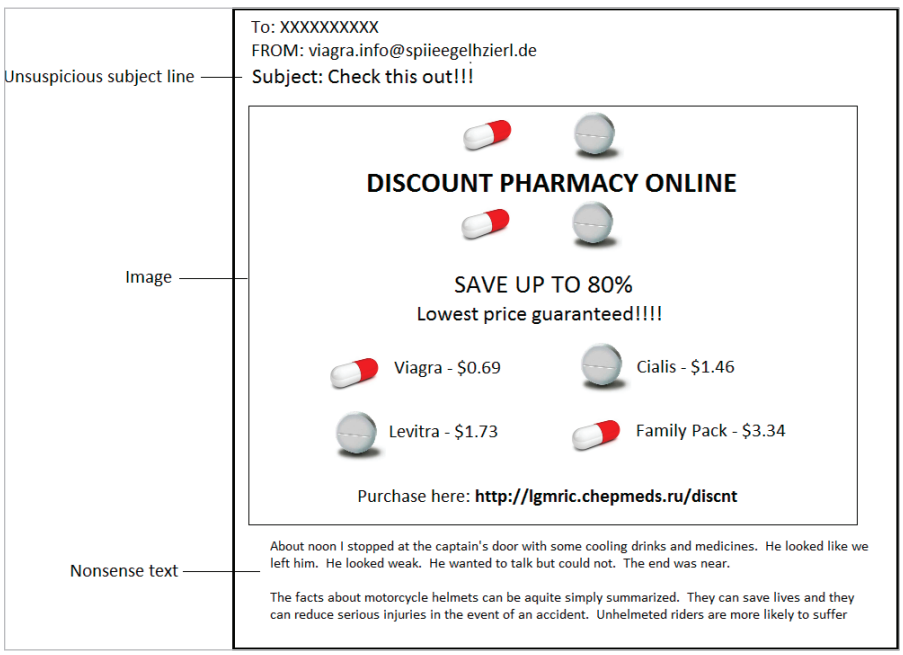


Figure 1-6 Image spam

Spim is spam delivered through instant messaging (IM) instead of email. For threat actors, spim can have even more impact than spam. The immediacy of instant messages makes users more likely to reflexively click embedded links in a spim. Furthermore, because spim may bypass some antimalware defenses, spim can more easily distribute malware. As antispam measures for email are more widely implemented, more spammers may be inclined to migrate to sending spim.

Beyond being annoying and interfering with work productivity as users spend time reading and deleting spam messages, spam and spim can be security vulnerabilities. This is because they can be used to distribute malware. Messages sent with attachments that contain malware are common means by which threat actors distribute their malware today.

Hoaxes Threat agents can use hoaxes as a first step in an attack. A **hoax** is a false warning, often contained in an email message claiming to come from the IT department. The hoax purports that there is a "deadly virus" circulating through the Internet and that the recipient should erase specific files or change security configurations and then forward the message to other users. However, changing configurations allows an attacker to compromise the system. And erasing files may make the computer unstable, prompting the victim to call the phone number in the hoax email message for help, which is actually the phone number of the attacker.

Watering Hole Attack In the natural world, similar types of animals are known to congregate around a pool of water for refreshment. In a similar manner, a **watering hole attack** is directed toward a smaller group of specific individuals, such as the major executives working for a manufacturing company. These executives all tend to visit a common website, such as that of a parts supplier to the manufacturer. An attacker who wants to target this group of executives tries to determine the common website that they frequent and then infects it with malware that will make its way onto the group's computers.

Physical Procedures

While some social engineering attacks rely on psychological manipulation, other attacks rely on physical acts. These attacks take advantage of user actions that can result in compromised security. Three of the most common physical procedures are dumpster diving, tailgating, and shoulder surfing.

Dumpster Diving **Dumpster diving** involves digging through trash receptacles to find information that can be useful in an attack. Table 1-5 lists the different items that can be retrieved—many of which appear to be useless—and how they can be used.

Table 1-5 Dumpster diving items and their usefulness

Item retrieved	Why useful
Calendars	A calendar can reveal which employees are out of town at a particular time.
Inexpensive computer hardware, such as USB flash drives or portal hard drives	These devices are often improperly disposed of and might contain valuable information.
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation.
Organizational charts	These identify individuals within the organization who are in positions of authority.
Phone directories	A phone directory can provide the names and telephone numbers of individuals in the organization to target or impersonate.
Policy manuals	These may reveal the true level of security within the organization.
System manuals	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities.

An electronic variation of physical dumpster diving is to use the Google search engine to look for documents and data posted online that can be used in an attack. This is called *Google dorking*, and it uses advanced Google search techniques to look for information that unsuspecting victims have carelessly posted on the web.

For example, to find on the web any Microsoft Excel spreadsheets (.xlsx) that contain the column heading "SSN" (Social Security number), the Google search term *intext:"SSN" filetype:xlsx* can be used, or to find any Microsoft Word documents (.docx) that contained the word "passwords" as part of the title, the Google search term *allintitle: "passwords" filetype:docx* is used.

NOTE 13

Google dorking is from a slang term that originally was used to refer to someone who is not considered intelligent (a *dork*) and later came to refer to uncovering security vulnerabilities that are the result of the actions of such a person.

Tailgating Organizations can invest tens of thousands of dollars to install specialized doors that permit access only to authorized users who possess a special card or who can enter a specific code. These automated access control systems are designed to restrict entry into an area. However, a weakness of these systems is that they cannot always control *how many* people enter the building when access is allowed; once an authorized person opens the door, one or more individuals can follow behind and also enter. This is known as **tailgating**.

The following are several ways tailgating can occur:

- A tailgater waits at the end of the sidewalk until an authorized user opens the door. She then calls out to him to "Please hold the door!" as she hurries to enter. In most cases, good etiquette wins out over good security practices, and the door is held open for the tailgater.
- A tailgater waits near the outside of the door and then quickly enters once the authorized employee leaves the area. This technique is used most commonly during weekends and at nights, where the actions of the more overt tailgater would be suspicious.
- A tailgater stands outside the door and waits until an employee exits the building. He then slips behind the person as he is walking away and grabs the door just before it closes to gain access to the building.
- An employee conspires with an unauthorized person to allow him to walk in with him through the open door (called *piggybacking*).

Shoulder Surfing If an attacker cannot enter a building as a tailgater without raising suspicion, an alternative is to watch an individual entering the security code on a keypad. Known as **shoulder surfing**, this technique can be used in any setting that allows an attacker to casually observe someone entering secret information, such as the security codes on a door keypad. Attackers are also using webcams and smartphone cameras to "shoulder surf" users of ATM machines to record keypad entries.

CAUTION

A defense against shoulder surfing is an application that uses the computer's web cam to watch if anyone nearby is looking at the computer screen. If someone is detected, the user can be alerted with a popup window message or the screen will automatically blur so that it cannot be read.

Impacts of Attacks

A successful attack always results in several negative impacts. These impacts can be classified as data impacts and effects on the organization.

Data Impacts

Whereas the goal of some attacks may be harm to a system, such as manipulating an industrial control system to shut down a water filtration facility, most attacks focus on data as the primary target. The consequences of a successful attack on data are listed in Table 1-6.

Effects on the Enterprise

A successful attack can also have grave consequences for an enterprise. First, the attack may make systems inaccessible (**availability loss**). This results in lost productivity, which can affect the normal tasks for generating income (**financial loss**).

Table 1-6 Consequences of data attack

Impact	Description	Example
Data loss	Destroying data so that it cannot be recovered	Maliciously erasing patient data used for cancer research
Data exfiltration	Stealing data to distribute it to other parties	Taking a list of current customers and selling it to a competitor
Data breach	Stealing data to disclose it in an unauthorized fashion	Stealing credit card numbers to sell to other threat actors
Identity theft	Taking personally identifiable information to impersonate someone	Stealing a Social Security number to secure a bank loan in the victim's name

One of the most devastating effects is on the public perception of the enterprise (**reputation**). If an organization is the victim of an attack that steals customer data, the public blames the organization and forms a serious negative impression. Many current customers will become disgruntled at the perceived lack of security at the organization and move their business to a competitor.

TWO RIGHTS & A WRONG

1. Spear phishing targets specific users.
2. "I'm the CEO calling" is an example of the psychological principle of authority.
3. The goal of impersonation is often prepending, which is obtaining private information.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in each module in the MindTap.

SUMMARY

- Attacks against information security have grown astronomically in recent years. Eighty percent of organizations have experienced at least one successful attack in a single year, with many organizations suffering multiple successful attacks annually. Compounding the problem is a serious shortfall of skilled security professionals.
- The information security workforce is usually divided into two broad categories. Information security managerial personnel administer and manage plans, policies, and people, while information security technical personnel are concerned with designing, configuring, installing, and maintaining technical security equipment.
- The CompTIA Security+ certification is a vendor-neutral credential that requires passing the current certification exam, SY0-601. A successful candidate has the knowledge and skills required to identify attacks, threats, and vulnerabilities; design a strong security architecture; implement security controls, be knowledgeable of security operations and incident response; and be well versed in governance, risk, and compliance requirements.
- Security can be defined as the necessary steps to protect from harm. The relationship between security and convenience is inversely proportional: as security is increased, convenience is decreased. Information security protects the integrity, confidentiality, and availability of information through products, people, and procedures on the devices that store, manipulate, and transmit the information.
- The threat actors, or individuals behind computer attacks, fall into several categories and exhibit different attributes. Some groups have a high level of power and complexity with a massive network of resources,

while others work alone and have minimal skills and no resources. Some groups have deep resources and funding while others have none. Certain threat actors are internal and work within the enterprise, and others are strictly outside the organization. The intent and motivation, or the reasons for the attacks, vary widely.

- Script kiddies do their work by downloading automated attack software from websites and then using it to break into computers. Hacktivists are strongly motivated by their ideology and often attack to make a political statement. State actors are employed by governments as state-sponsored attackers for launching computer attacks against foes. Other threat actors include competitors, criminal syndicates, shadow IT, brokers, and cyberterrorists.
- Cybersecurity vulnerabilities are often categorized into five broad categories: platforms, configurations, third parties, patches, and zero-day vulnerabilities. Several vulnerabilities are the result of the platform being used. Legacy or outdated platforms have not been updated and are prime targets for attacks. On-premises platforms are located within the physical confines of an enterprise, which are usually consolidated in the company's data center. Due to the rapid provisioning of resources, on-premises platforms are often not adequately configured for security. Cloud platforms are proven to have significant vulnerabilities. These vulnerabilities are most often based on misconfigurations by company personnel responsible for securing the cloud platform.
- Modern hardware and software platforms provide a wide array of features and security settings, and these must be properly configured to repel attacks. Unfortunately, the configuration settings are not always properly implemented, resulting in weak configurations. Many enterprises also use IT-related third parties due to their elevated level of expertise. Almost all third parties require access to the organization's computer network. However, often the organization's systems are not compatible with the third party's systems and require work-arounds, which can create vulnerabilities. A security patch is an officially released software security update intended to repair a vulnerability. However, as important as patches are, they can create vulnerabilities. A zero-day vulnerability has no advance warning because there has been no previous knowledge of the vulnerability.
- An attack vector is a pathway or avenue used by a threat actor to penetrate a system. Although there are many specific types of attacks, vectors can be grouped into general categories. These include email, wireless, removable media, direct access, social media, supply chain, and cloud.
- Social engineering is a means of eliciting information (gathering data) by relying on the weaknesses of individuals. Information elicitation may be the goal of the attack, or the information may be used for other attacks. Many social engineering attacks rely on psychology, which involves taking a mental and emotional approach—rather than a physical approach—to gathering data. At its core, social engineering relies on an attacker's clever manipulation of human nature to persuade the victim to provide information or take actions. Social engineering psychological approaches often involve impersonation, phishing, redirection, spam, hoaxes, and watering hole attacks. Some social engineering attacks rely on physical acts. These attacks take advantage of user actions that can result in compromised security. Three of the most common physical procedures are dumpster diving, tailgating, and shoulder surfing.
- A successful attack always results in several negative impacts. Most attacks focus on data as the primary target. The consequences of a successful attack on data are data loss, data exfiltration, data breach, and identity theft. A successful attack can also have significant consequences for an enterprise. Systems may be rendered inaccessible, which results in lost productivity and impacts the normal tasks for generating income. One of the most devastating effects is on the public perception of the enterprise, or its reputation. An organization that is the victim of an attack in which customer data is stolen faces a serious negative impression in the eye of the public.

Key Terms

advanced persistent threat (APT)
attack vector
attributes
authority
availability loss
black hat hackers
cloud platforms
competitors
consensus
credential harvesting
criminal syndicates
data breach
data exfiltration
data loss
data storage
default settings
direct access
dumpster diving
eliciting information
errors
external

familiarity
financial loss
firmware
gray hat hackers
hacker
hacktivists
hoax
hybrid warfare influence campaign
identity fraud (also called impersonation)
identity theft
impersonation (also called identity fraud)
influence campaigns
insider threat
intent/motivation
internal
intimidation
invoice scam
lack of vendor support
legacy platform
level of capability/sophistication
on-premises platform
open permissions
open ports and services
outsourced code development
patch
pharming
phishing
prepending
pretexting
reconnaissance
reputation
resources and funding
scarcity
script kiddies
shadow IT
shoulder surfing
smishing
social engineering
social media influence campaign
spam
spear phishing
spim
state actors
supply chain
system integration
tailgating
third parties
threat actor
trust
typo squatting
unsecure protocols
unsecured root accounts
urgency
vendor management
vishing
watering hole attack
weak configurations
weak encryption
whaling
white hat hackers
zero day

Review Questions

1. After Bella earned her security certification, she was offered a promotion. As she reviewed the job responsibilities, she saw that in this position she will report to the CISO and supervise a group of security technicians. Which of these generally recognized security positions has she been offered?
   a. Security administrator
   b. Security technician
   c. Security officer
   d. Security manager

2. Which of the following is false about the CompTIA Security+ certification?
   a. Security+ is one of the most widely acclaimed security certifications.
   b. Security+ is internationally recognized as validating a foundation level of security skills and knowledge.
   c. The Security+ certification is a vendor-neutral credential.
   d. Professionals who hold the Security+ certification earn about the same or slightly less than security professionals who have not achieved this certification.

3. Which of the following is true regarding the relationship between security and convenience?
   a. Security and convenience are inversely proportional.
   b. Security and convenience have no relationship.
   c. Security is less important than convenience.
   d. Security and convenience are equal in importance.

4. Which of the following of the CIA Triad ensures that information is correct, and no unauthorized person has altered it?
   a. Confidentiality
   b. Integrity
   c. Availability
   d. Assurance

5. Which of the following is *not* used to describe those who attack computer systems?
   a. Threat actor
   b. Hacker
   c. Malicious agent
   d. Attacker

6. Which of the following is *not* true regarding security?
   a. Security is a goal.
   b. Security includes the necessary steps to protect from harm.
   c. Security is a process.
   d. Security is a war that must be won at all costs.

7. Luna is reading a book about the history of cybercrime. She read that the very first cyberattacks were mainly for what purpose?
   a. Fortune
   b. Fame

c. Financial gain
d. Personal security

8. Which of the following ensures that only authorized parties can view protected information?
a. Authorization
b. Confidentiality
c. Availability
d. Integrity

9. Which type of hacker will probe a system for weaknesses and then privately provide that information back to the organization?
a. Black hat hackers
b. White hat hackers
c. Gray hat hackers
d. Red hat hackers

10. Complete this definition of information security: *That which protects the integrity, confidentiality, and availability of information* _____.
a. *on electronic digital devices and limited analog devices that can connect via the Internet or through a local area network.*
b. *through a long-term process that results in ultimate security.*
c. *using both open-sourced as well as supplier-sourced hardware and software that interacts appropriately with limited resources.*
d. *through products, people, and procedures on the devices that store, manipulate, and transmit the information.*

11. Which of the following groups have the lowest level of technical knowledge?
a. Script kiddies
b. Hacktivists
c. State actors
d. Insiders

12. Which of the following groups use advanced persistent threats?
a. Brokers
b. Criminal syndicates
c. Shadow IT
d. State actors

13. Which of the following is *not* a reason a legacy platform has not been updated?
a. Limited hardware capacity
b. An application only operates on a specific OS version
c. Neglect
d. No compelling reason for any updates

14. How do vendors decide which should be the default settings on a system?
a. Those that are the most secure are always the default settings.
b. There is no reason specific default settings are chosen.
c. Those settings that provide the means by which the user can immediately begin to use the product.
d. The default settings are always mandated by industry standards.

15. Which tool is most commonly associated with state actors?
a. Closed-Source Resistant and Recurrent Malware (CSRRM)
b. advanced persistent threat (APT)
c. Unlimited Harvest and Secure Attack (UHSA)
d. Network Spider and Worm Threat (NSAWT)

16. What is the term used to describe the connectivity between an organization and a third party?
a. System integration
b. Platform support
c. Resource migration
d. Network layering

17. What is an objective of state-sponsored attackers?
a. To right a perceived wrong
b. To amass fortune over of fame
c. To spy on citizens
d. To sell vulnerabilities to the highest bidder

18. Which of the following is *not* an issue with patching?
a. Difficulty patching firmware
b. Few patches exist for application software
c. Delays in patching OSs
d. Patches address zero-day vulnerabilities

19. Which of the following is *not* a recognized attack vector?
a. Supply chain
b. Social media
c. On-prem
d. Email

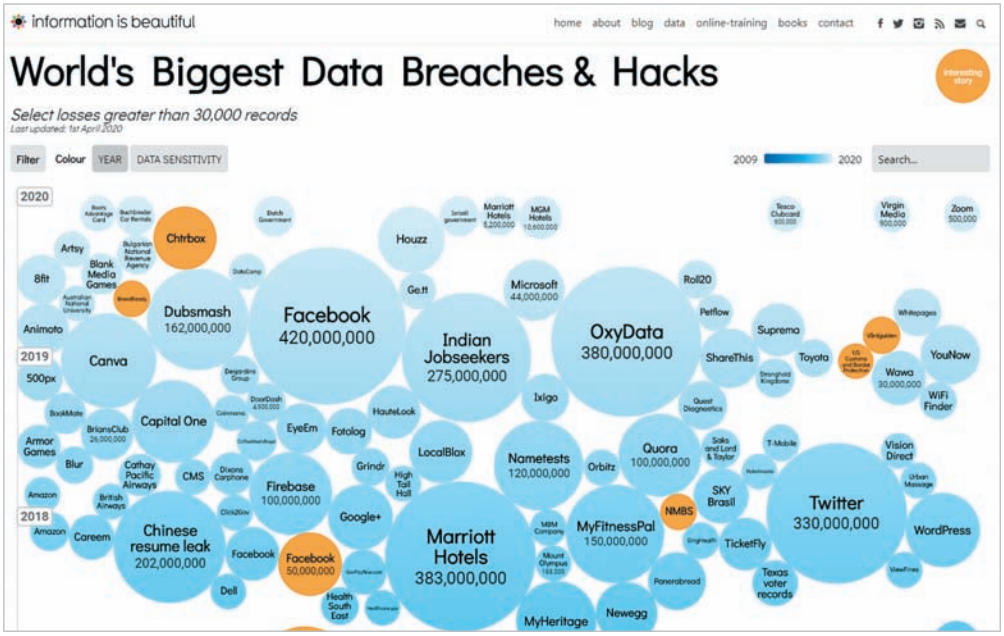
20. What is the category of threat actors that sell their knowledge of vulnerabilities to other attackers or governments?
a. Cyberterrorists
b. Competitors
c. Brokers
d. Resource managers

Hands-On Projects

Project 1-1: Examine Data Breaches—Visual

Time Required: 15 minutes
Objective: Explain the security concerns associated with various types of vulnerabilities.
Description: In this project, you use a visual format to view the biggest data breaches resulting in stolen information.

1. Open your web browser and enter the URL **www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/** (If you are no longer able to access the site through this web address, use a search engine to search for "Information Is Beautiful World's Biggest Data Breaches & Hacks.")
2. This site will display a visual graphic of the data breaches, as shown in Figure 1-7.



Source: Information is Beautiful

Figure 1-7 World's biggest data breaches & hacks webpage

3. Scroll down the page to view the data breaches by year. Note that the size of the breach is indicated by the size of the bubble.
4. Scroll back up to the top.
5. Hover over several of the bubbles to read a quick story of the breach.
6. Note the color of the bubbles that have an "Interesting Story." Click one of the bubbles and read the story. When finished, close only the interesting story tab in your browser.
7. Click the **Data Sensitivity** button on the World's Biggest Data Breaches & Hacks page. Note the color legend from Low to High that indicates how sensitive the data was.
8. Click the **Year** button to return to the original screen.
9. Click the **Filter** button to display the filter menu.
10. Under Sector, click **healthcare** to view those breaches related to the healthcare industry.
11. Click one of the bubbles and read the story.
12. Click **Reset** in the filter menu.
13. Select the sector **financial**.
14. Select the method **poor security**.
15. Click one of the bubbles and read the story.
16. Create your own filters to view different types of breaches. Does this graphic convey a compelling story of data breaches?
17. How does this visualization help you with the understanding of threats?
18. Close all windows.

Project 1-2: Scan for Malware Using the Microsoft Safety Scanner

Time Required: 15 minutes
Objective: Given a scenario, analyze potential indicators to determine the type of attack.
Description: In this project, you download and run the Microsoft Safety Scanner to determine if there is any malware on the computer.

1. Determine which system type of Windows you are running. Click **Start**, **Settings**, **System**, and then **About**. Look under System type for the description.
2. Open your web browser and enter the URL *docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download* (If you are no longer able to access the site through the URL, use a search engine to search for "Microsoft Safety Scanner.")
3. Select either **Download Microsoft Safety Scanner (32-bit)** or **Download Microsoft Safety Scanner (64-bit)**, depending upon which system type of Windows you are running.
4. When the **MSERT.exe** program finishes downloading, launch this program by double-clicking it.
5. If a warning dialog box appears, click **Run anyway**.
6. If a User Account Control dialog box appears, click **Yes.**
7. Click the check box to accept the license terms for this software. Click **Next**.
8. Click **Next**.
9. Select **Quick scan** if necessary.
10. Click **Next**.
11. Depending on your computer, this scan may take several minutes. Analyze the results of the scan to determine if it found any malicious software in your computer.
12. If you have problems, you can click **View detailed results of the scan**. After reviewing the results, click **OK**. If you do not find any problems, click **Finish**.
13. If any malicious software was found on your computer, run the scan again and select **Full scan**. After the scan is complete, click **Finish** to close the dialog box.
14. Close all windows.

Project 1-3: Configure Microsoft Windows Sandbox

Time Required: 15 minutes
Objective: Given a scenario, implement host or application security solutions.
Description: A *sandbox* is an isolated virtual machine: anything run within a sandbox will impact only the virtual machine and not the underlying computer. The Microsoft Windows Sandbox first became available in Windows 10 Version 1903 released in 2019, and additional features have been added with recent Windows 10 updates to provide even more control.

NOTE 14

Although separate programs can perform a sandbox function, the Windows Sandbox has the advantages of being included as part of Windows, so nothing has to be downloaded and installed. It relies on the Microsoft hypervisor to run a separate kernel that isolates the Windows Sandbox from the host. This makes it more efficient since it can take advantage of the Windows integrated kernel scheduler, smart memory management, and a virtual GPU. Once you close the Windows Sandbox, nothing remains on your computer; when you launch Windows Sandbox again, it is as clean as new.

In this project you will configure the Windows Sandbox to use with this book.

CAUTION

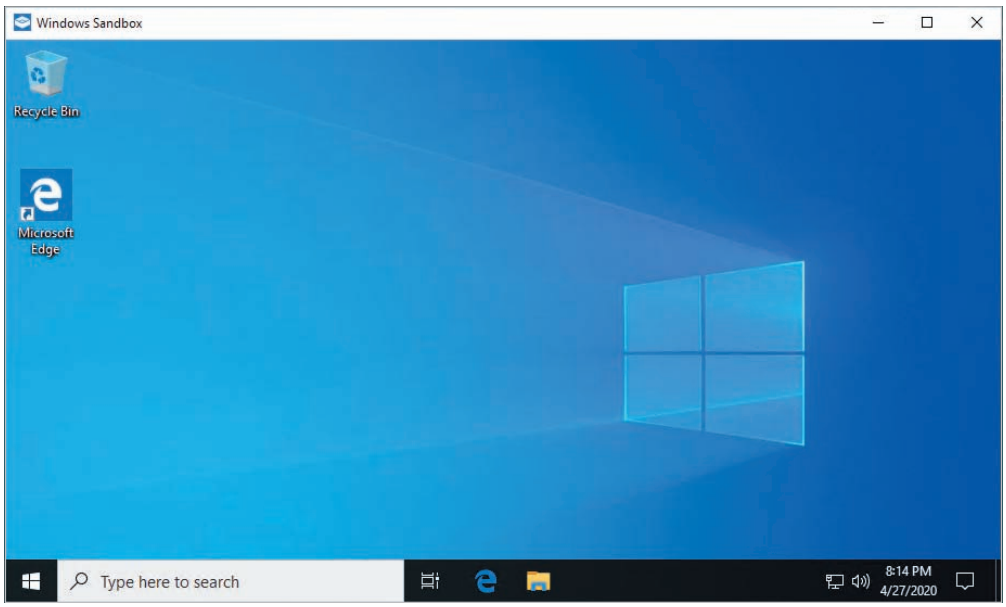
You must be running Windows 10 Professional, Enterprise, or Education (not Home) Version 1903 or higher. To determine which version you are running, click Settings, then System, and then About. If you are not using the correct version, skip to the next project to create a different virtual machine.

1. First check if your system has virtualization turned on. Right-click the taskbar (at the bottom of the screen) and select **Task Manager**.
2. Click the **Performance** tab.
3. Under Virtualization, it must say "Enabled." If it says "Disabled," you will need to reboot and enter your BIOS or UEFI and turn on virtualization.

NOTE 15

With older BIOS, you may also need to disable other settings, such as Hyper-threading.

4. Now enable Windows Sandbox. In the Windows search box on the taskbar, enter **Windows Features** to open the Windows Features window.
5. Click the **Windows Sandbox** check box to turn on this feature.
6. To launch Windows Sandbox, click **Start**, and scroll down to Windows Sandbox, and then click **Windows Sandbox**. A protected virtual machine sandbox that looks like another Windows instance will start, as shown in Figure 1-8.



Source: Used with permissions from Microsoft

Figure 1-8 Windows sandbox

7. Explore the settings and default applications that come with the Windows Sandbox.
8. You can download a program through the Microsoft Edge application in Windows Sandbox. (Edge is included within Windows Sandbox along with a handful of other Windows applications, including access to OneDrive.) Open Edge and go to **www.google.com** to download and install the Google Chrome browser in the Windows Sandbox.

NOTE 16

You can also copy an executable file from your normal Windows environment and then paste it to the Windows Sandbox desktop to launch it.

9. After the installation is complete, close the Windows Sandbox.
10. Now relaunch the Windows Sandbox. What happened to Google Chrome? Why?
11. Close all windows.

Project 1-4: Create a Virtual Machine of Windows 10 for Security Testing—Part 1

Time Required: 25 minutes
Objective: Given a scenario, implement host or application security solutions.
Description: If you were unable to install the Windows Sandbox in Project 1-3, a different virtual machine can be created in which new applications can be installed or configuration settings changed without affecting the base computer. In a virtual machine environment, the "host" computer runs a "guest" operating system. Security programs and testing can be conducted within this guest operating system without affecting the regular host operating system. In this project, you create a virtual machine using Oracle VirtualBox software.

1. Open a web browser and enter the URL **www.virtualbox.org** (If you are no longer able to access the site through this web address, use a search engine to search for "Oracle VirtualBox download.")
2. Click **Downloads** (or a similar link or button).
3. Under VirtualBox binaries, select the latest version of VirtualBox to download for your specific host operating system. For example, if you are running Windows, select the version for "Windows hosts."
4. Under VirtualBox x.x.x Oracle VM VirtualBox Extension Pack, click **All supported platforms** to download the extension package.
5. Navigate to the folder that contains the downloads and launch the VirtualBox installation program **VirtualBox-xxx-nnnnn-hhh.exe**.
6. Accept the default configurations from the installation wizard to install the program.
7. If you are asked "Would you like to install this device software?" on one or more occasions, click **Install**.
8. When completed, click **Finish** to launch VirtualBox.
9. Now install the VirtualBox extensions. Click **File** and then click **Preferences**.
10. Click **Extensions**.
11. Click the **Add a package** icon on the right side of the screen.
12. Navigate to the folder that contains the extension pack downloaded earlier to select that file. Click **Open**.
13. Click **Install**. Follow the necessary steps to complete the default installation.
14. Remain in VirtualBox for the next project to configure VirtualBox and install the guest operating system.

Project 1-5: Create a Virtual Machine of Windows 10 for Security Testing—Part 2

Time Required: 20 minutes
Objective: Given a scenario, implement host or application security solutions.
Description: After installing VirtualBox, the next step is to create the guest operating system. For this project, Windows 10 will be installed. Different options are available for obtaining a copy of Windows:

- A retail version of the software can be purchased.
- If you or your school is a member of the Microsoft Azure Dev Tools for Teaching program, the operating system software and a license can be downloaded. See your instructor or lab supervisor for more information.
- A 90-day evaluation copy can be downloaded and installed from the Microsoft TechNet Evaluation Center (**www.microsoft.com/en-US/evalcenter/evaluate-windows-10-enterprise**).

1. Obtain the ISO image of Windows 10 using one of the preceding options and save it on the hard drive of the computer.
2. Launch VirtualBox.
3. Click **New**.
4. In the Name: box, enter **Windows 10** as the name of the virtual machine.
5. Be sure that the Type: box displays **Microsoft Windows** and the Version: box changes to **Windows 10 (xx-bit)**. Click **Next**.
6. Under Memory size, accept the recommended size or increase the allocation if you have sufficient RAM on your computer. Click **Next**.
7. Under Hard disk, accept **Create a virtual hard drive now**. Click **Create**.
8. Under Hard drive file type, accept the default **VID (VirtualBox Disk Image)**. Click **Next**.
9. Under Storage on physical hard drive, accept the default **Dynamically allocated**. Click **Next**.
10. Under File location and size, accept **Windows 10**. Click **Create**.

11. Now the configuration settings for the virtual machine are set. Next you will load the Windows 10 ISO image. Click **Settings**.
12. In the left pane, click **Storage**.
13. Under Controller: click **Empty**.
14. In the right page under Attributes, click the icon of the optical disc.
15. Click **Choose Virtual Optical Disk File**.
16. Navigate to the location of the Windows 10 ISO file and click **Open**.
17. Click **OK**.
18. Click **Start** to launch the Windows 10 ISO.
19. Follow the Windows 10 installation wizard to complete the installation.
20. To close the Windows 10 guest operating system in VirtualBox, click **File** and then click **Exit**.
21. Close all windows.

Case Projects

Case Project 1-1: Personal Attack Experiences

What type of computer attack have you (or a friend or another student) experienced? When did it happen? What type of computer or device was involved? What type of damage did it inflict? What had to be done to clean up following the attack? How was the computer fixed after the attack? What could have prevented it? List the reason or reasons you think that the attack was successful. Write a one-page paper about these experiences.

Case Project 1-2: Security Podcasts or Video Series

Many security vendors and security researchers now post weekly audio podcasts or video series on YouTube on security topics. Locate two different podcasts and two different video series about computer security. Listen and view one episode of each. Then write a summary of what was discussed and a critique of the podcasts and videos. Were they beneficial to you? Were they accurate? Would you recommend them to someone else? Write a one-page paper on your research.

Case Project 1-3: Phishing Simulators

Search the Internet for three different phishing simulators. Take the phishing challenge on each simulator to determine if you can identify the phishing attacks. Then create a table that lists the features of the phishing simulators, their ease of use, and how accurate you think they were. Would these simulators be helpful in training users about phishing? Write a one-paragraph summary along with your table.

Case Project 1-4: Sources of Security Information

The following is a partial overall list of some of the sources for security information:

- Security content (online or printed articles that deal specifically with unbiased security content)
- Consumer content (general consumer-based magazines or broadcasts not devoted to security but occasionally carry user security tips)
- Vendor content (material from security vendors who sell security services, hardware, or software)
- Security experts (IT staff recommendations or newsletters)
- Direct instruction (college classes or a workshop conducted by a local computer vendor)
- Friends and family
- Personal experience

Create a table with each of these sources and columns that list Advantages, Disadvantages, Example, and Rating. Use the Internet to complete the entire table. The Rating column is a listing from 1 to 7 (with 1 being the highest) of how useful each of these sources is in your opinion. Compare your table with other learners.

Case Project 1-5: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. In order to gain the most benefit from the site, you will need to set up a free account.

Go to **community.cengage.com/infosec2**. Click **Join the Community**. On the Join the Community page, enter the requested information to create your account.

NOTE 17

Your instructor may have a specific naming convention that you should use, such as the name of your course followed by your initials. Check with your instructor before creating your sign-in name.

Explore the various features of the Information Security Community Site and become familiar with it. Visit the blog section and read the blog postings to learn about some of the latest events in IT security.

Case Project 1-6 North Ridge Security

North Ridge Security provides security consulting and assurance services to over 500 clients in more than 20 states and a wide range of enterprises. A new initiative at North Ridge is for each of its seven regional offices to provide internships to students who are in their final year of the security degree program at the local college.

As part of National Cybersecurity Awareness Month, North Ridge is visiting local high schools to talk about careers in cybersecurity. You have been asked to present an introductory session on the need for cybersecurity workers, the types of jobs that are available, what a cybersecurity professional does each day, and the value of security certifications.

1. Use the Internet to research information about working in the cybersecurity field. Then create a PowerPoint presentation that explains why cybersecurity employees are needed, what they do, and the value of security certifications. Your presentation should be seven to 10 slides in length.
2. As a follow-up to your presentation, create a Frequently Asked Questions (FAQ) sheet that outlines working in cybersecurity. Write a one-page FAQ about security employment.

References

1. Shi, Fleming, "Threat spotlight: Coronavirus-related phishing," *Barracuda*, Mar. 26, 2020, accessed Apr. 19, 2020, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/.
2. "Fake 'Corona Antivirus' distributes BlackNET remote administration tool," *MalwareBytes Labs*, Mar. 23, 2020, accessed Apr. 19, 2020, https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/.
3. "McAfee Labs threats report," Dec. 2018, accessed Apr. 21, 2019, www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.
4. "2020 cyberthreat defense report," *Cyberedge Group*, accessed Apr. 20, 2020, https://cyber-edge.com/cdr/.
5. Morgan, Steve, "2019 official annual cybercrime report," *Cybersecurity Ventures*, accessed Apr. 20, 2020, www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.
6. "2020 cyberthreat defense report," *Cyberedge Group*, accessed Apr. 20, 2020, https://cyber-edge.com/cdr/.
7. Hospelhorn, Sarah, "Solving the cybersecurity skills shortage within your organization," *Varonis*, Mar. 29, 2020, accessed Apr. 20, 2020, https://www.varonis.com/blog/cybersecurity-skills-shortage/.
8. "Information security analysts," *Bureau of Labor Statistics*, Apr. 10, 2020, accessed Apr. 30, 2020, www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

9. Morgan, Steve, "One million cybersecurity job openings in 2016," *Forbes*, Jan. 2, 2016, accessed Feb. 16, 2017, www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1118fc737d27.
10. "How CompTIA certifications can earn you higher salary and better opportunities," *Simplilearn*, Aug. 5, 2019, accessed Apr. 20, 2020, www.simplilearn.com/how-comptia-certification-can-earn-higher-salary-rar409-article.
11. "2019 insider threat report," *NucleusCyber*, retrieved Apr. 21, 2020, https://info.nucleuscyber.com/2019-insider-threat-report.
12. Fruhlinger, Josh, "Top cybersecurity facts, figures and statistics for 2020," *CSO,* Mar. 9, 2020, accessed Apr. 21, 2020, www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.
13. "Phishing activity trends report," *Anti-Phishing Working Group*, accessed Apr. 25, 2020, https://apwg.org/trendsreports/.
14. McNichol, Tom, "Friend me on Facebook," *Bloomberg Businessweek*, Nov. 7, 2011.
15. Domabirg, Artem, "Bitsquatting: DNS hijacking without exploitation," *Diaburg.org,* accessed Mar. 27, 2017, dinaburg.org/bitsquatting.html.

MODULE 2

THREAT MANAGEMENT AND CYBERSECURITY RESOURCES

After completing this module, you should be able to do the following:

1. Explain what a penetration test is
2. Identify the rules of engagement and how to perform a pen test
3. Define vulnerability scanning
4. Describe different cybersecurity resources

Front-Page Cybersecurity

"Bug bounties" are monetary rewards given for uncovering a software vulnerability. Although these programs have been in existence since 1995, when Netscape first offered cash to anyone who could find security vulnerabilities in its Netscape Navigator web browser, in recent years bug bounty programs have changed significantly. Not only are exceptionally large rewards now offered, but those paying for rewards are no longer only software developers who want to fix the bugs. The large bounties have resulted in fierce competition over bugs.

Google is typical of the software developers who have bug bounty programs. Starting its program in 2010, Google now pays anywhere from $100 to $31,337 per bug found in their basic software. To date, Google has paid more than $21 million for bug bounties. Google also maintains a leaderboard of the top 10 recipients of bounties. (It is called the "0x0A Leaderboard" because "0x0A" is the number 10 in hexadecimal.) Once a security researcher finds a vulnerability and reports it, Google then immediately works to patch the bug.

Recently, several other players beside software developers have started offering bug bounties. The European Commission (EC), which is part of the European Union (EU) and is responsible for essentially managing the daily affairs of the EU, now offers bug bounties for security vulnerabilities that are uncovered in some of the most popular free and open source software. The EC, which itself has been a victim of cyberattacks that resulted in thousands of diplomatic cables being stolen and published, says that it wants to protect EU citizens (and itself) from attacks by uncovering bugs. Their bug bounties range from €25,000 to €90,000 ($28,600–$103,000).

An entirely new player offering bug bounties is Zerodium. Founded in 2015, Zerodium calls itself the "leading exploit acquisition platform for premium zero-days and advanced cybersecurity capabilities." Zerodium buys bug information and then sells it to "mainly government organizations in need of specific and tailored cybersecurity capabilities and/or protective solutions to defend against zero-day attacks." In other words, the governments may use the knowledge of these zero-day

bugs to defend themselves from future attacks—or they may instead use the information to launch silent attacks against their citizens and other nations. But the price that Zerodium pays has been nothing like the software developers: Zerodium pays up to $2 million for certain types of bugs in Apple products and $1 million for Microsoft Windows bugs.

This has resulted in a price war over bugs. In late 2019, Apple expanded its bug bounty program by opening it to anyone who found a bug. (Previously, Apple's program was invitation-only: they would only accept and pay a bounty from preapproved security researchers.) Apple now pays from $200,000 to $1.5 million per bug and adds a 50 percent bonus on top of the regular payout for any bug reported in an Apple beta release. Other software developers have also raised their prices.

In order to secure an organization from attacks, a concept known as *threat management* is often used. The goal of threat management is to take the appropriate steps needed to minimize hostile cyber actions. It seeks to answer the question, "What threat can take advantage of a vulnerability to bypass our defenses, and how can we prevent it?"

One of the first steps in threat management is to test the defenses to find any weaknesses. However, tests should never be "one-and-done" or conducted only periodically. Instead, because of the nature of today's security attacks, a regular cycle of scans must be conducted. In addition to these tests and scans for defenses, a wealth of cybersecurity information can also be used for defenses.

In this module, you will learn about threat management as it pertains to penetration testing and vulnerability scans. You will also explore cybersecurity standards, regulations, frameworks, and configuration guidelines.

PENETRATION TESTING

CERTIFICATION

1.8 Explain the techniques used in penetration testing.

Studying penetration testing involves defining what it is and why such a test should be conducted. It also examines who should perform the tests and the rules for engagement. Finally, knowing how to perform a penetration test is also useful.

Defining Penetration Testing

Penetration testing attempts to exploit vulnerabilities just as a threat actor would. This helps to uncover new vulnerabilities, provide a clearer picture of their nature, and determine how they could be used against the organization. Kali Linux, a popular penetration testing tool, is shown in Figure 2-1.

Source: Kali Linux

Figure 2-1 Kali Linux penetration testing tool

It is generally recognized that the most important element in a "pen test" (short for "penetration test") is the first step: *planning*. A lack of planning can result in a flawed penetration test that tries to do too little or too much. It can also result in *creep*, which is an expansion beyond the initial set of the test's limitations. In penetration testing, it is often tempting to exploit a vulnerability "down a rabbit hole" and waste valuable time and resources without gaining any significant value.

Yet, the most dangerous result of poor planning is creating unnecessary legal issues. Because the nature of penetration testing is to exploit vulnerabilities, an outsider can easily perceive the testing to be the work of a real threat actor. Breaking into an organization's network and exploiting vulnerabilities is a clear violation of state and national laws. This could easily put a penetration tester in legal peril unless proper planning takes place first.

CAUTION The importance of planning a penetration test should never be underestimated. Planning a pen test is essential; in fact, no pen test should ever occur without a detailed planning phase.

Why Conduct a Test?

By its very nature, a penetration test attempts to uncover vulnerabilities and then exploit them, just as a threat actor would. This involves a significant amount of time and resources. So sometimes asked is the question, "Why spend the time and effort to perform a penetration test? Why can't we just do a scan of our network defenses to find vulnerabilities?"

While a scan of network defenses can help find vulnerabilities, the *type* of vulnerabilities revealed is different from a penetration test. A scan usually finds only *surface* problems to be addressed. This is because many scans are entirely *automated* and provide only a limited verification of any discovered vulnerabilities. A penetration test, on the other hand, can find *deep* vulnerabilities. Penetration tests go further and attempt to exploit vulnerabilities using *manual* techniques.

These deep vulnerabilities can only be exposed through *actual attacks that use the mindset of a threat actor*. Both elements are important. First, the attacks must be the same (or remarkably similar) as those used by a threat actor; anything less will not uncover the deep vulnerabilities that an attacker can find. Second, the attacks should follow the thinking of threat actors. Understanding their thinking helps to better perceive what assets they are seeking, how they may craft the attack, and even how determined they are to obtain assets. Without having an attacker's mindset, it is difficult to find deep vulnerabilities.

NOTE 1

Some security professionals believe organizations that do not have a solid cybersecurity defense should not consider a pen test as the first step. Instead, a general scan should first be conducted to reveal and address surface vulnerabilities. Once this analysis is completed, a more thorough pen test can be performed.

Who Should Perform the Test?

One of the first questions to answer is who should conduct the penetration test. Should it be conducted by in-house employees or an external consultant? Is there another option? What are the advantages and disadvantages to each approach?

Internal Security Personnel

Using internal employees to conduct a penetration test has advantages in some cases. First, there is little or no additional cost. Also, the test can be conducted much more quickly. Finally, an in-house penetration test can be used to enhance the training of employees and raise the awareness of security risks.

When conducting an in-house pen test, an organization often divides security employees into opposing teams to conduct a "war game" scenario. Table 2-1 lists the composition and duties of the teams in a pen test war game.

However, using internal security employees to conduct a penetration test has several disadvantages:

- *Inside knowledge*. Employees often have in-depth knowledge of the network and its devices. A threat actor, on the other hand, would not have the same knowledge, so an attack from employees would not truly simulate that of a threat actor.

Table 2-1 Penetration testing war game teams

Team Name	Role	Duties	Explanation
Red Team	Attackers	Scans for vulnerabilities and then exploits them	Has prior and in-depth knowledge of existing security, which may provide an unfair advantage.
Blue Team	Defenders	Monitors for Red Team attacks and shores up defenses as necessary	Scans log files, traffic analysis, and other data to look for signs of an attack.
White Team	Referees	Enforces the rules of the penetration testing	Makes notes of the Blue Team's responses and the Red Team's attacks.
Purple Team	Bridge	Provides real-time feedback between the Red and Blue Teams to enhance the testing	The Blue Team receives information that can be used to prioritize and improve their ability to detect attacks while the Red Team learns more about technologies and mechanisms used in the defense.

- *Lack of expertise*. Employees may not have the credentials needed to perform a comprehensive test. Their lack of expertise may result in few deep vulnerabilities being exposed.
- *Reluctance to reveal*. Employees may be reluctant to reveal a vulnerability discovered in a network or system that they or a fellow employee has been charged with protecting.

NOTE 2

Sometimes organizations add an incentive called a *capture the flag (CTF)* exercise. A series of challenges with varying degrees of difficulty are outlined in advance. When one challenge is solved, a "flag" is given to the pen tester, and the points are totaled once time has expired. The winning player or team is the one that earns the highest score. CTF events are often hosted at information security conferences or by schools.

External Pen Tester Consultants

Contracting with an external third-party pen testing consultant to conduct a penetration test offers the following advantages:

- *Expertise*. External contractors that conduct penetration tests have the technical and business expertise to conduct a thorough test.
- *Credentials*. Pen test contractors usually employ people who hold several security certifications to validate their pen testing knowledge and experience.
- *Experience.* Because they have conducted numerous penetration tests, contractors know what to look for and how to take advantage of a vulnerability.
- *Focus*. Reputable penetration testing firms generally deliver expert security services and are highly focused on the task.

Penetration testing using external consultants is often classified based on the level of information and access provided in advance of the pen test. These levels are described in Table 2-2.

A disadvantage of using an external consultant is the usage of the information that is uncovered. A contractor who conducts a pen test will not only learn about an organization's network and system vulnerabilities but may also receive extremely sensitive information about these systems and how to access them. Such knowledge could be sold to a competitor by an unscrupulous employee of the third-party contractor. As a protection, most penetration testing contracts contain a *nondisclosure agreement (NDA)* that states all client information related to the test will be treated as highly confidential and that at the end of the test, all data and storage media is either destroyed or given back to the client.

Table 2-2 Penetration testing levels

Level Name	Description	Main Task	Advantages	Disadvantages
Black box	Testers have no knowledge of the network and no special privileges	Attempt to penetrate the network	Emulate exactly what a threat actor would do and see	If testers cannot penetrate the network, then no test can occur
Gray box	Testers are given limited knowledge of the network and some elevated privileges	Focus on systems with the greatest risk and value to the organization	More efficiently assess security instead of spending time trying to compromise the network and then determining which systems to attack	This head start does not allow testers to truly emulate what a threat actor may do
White box	Testers are given full knowledge of the network and the source code of applications	Identify potential points of weakness	Focus directly on systems to test for penetration	This approach does not provide a full picture of the network's vulnerabilities

Crowdsourced Pen Testers

A **bug bounty** is a monetary reward given for uncovering a software vulnerability. Most software developers offer some type of bug bounty, ranging from several thousands of dollars to millions of dollars. Bug bounty programs take advantage of *crowdsourcing*, which involves obtaining input into a project by enlisting the services of many people through the Internet.

Recently some third-party organizations have begun offering crowdsourced pen testing. Instead of contracting with a single external pen tester consulting organization, crowdsourced pen testing involves a large group of individuals who are not regular employees of the contractor. These handpicked crowdsourced members of the security community test the security of the client. Some of the advantages of crowdsourced pen testers are the following:

- Faster testing, resulting in quicker remediation of vulnerabilities
- Ability to rotate teams so different individuals test the system
- Option of conducting multiple pen tests simultaneously

Rules of Engagement

The **rules of engagement** in a penetration test are its limitations or parameters. Without these parameters, a penetration test can easily veer off course and not accomplish the desired results, take too long to produce timely results, or test assets that are not necessary to test. The categories for the rules for engagement are timing, scope, authorization, exploitation, communication, cleanup, and reporting.

Timing

The *timing* parameter sets when the testing will occur. The first consideration for timing is the start and stop dates of the test. When using an external third party, these dates are based on estimates provided by the tester and directly tied to the experience of a tester in a certain area. However, during a penetration test, several events can occur that may slow the testing process. For example, a significant vulnerability may be found that requires immediate attention; multiple meetings may then be necessary with different levels of management and security personnel to address the vulnerability. Such meetings can significantly affect the original estimated completion date. Many pen testers recommend adding up to 20 percent more time to the end date to provide a cushion if any interruptions occur in testing.

The second timing consideration involves when the pen testing should take place. Should the active portions of the pen test—scanning and exploitation—be conducted during normal business hours, which could cause unforeseen interruptions to normal activities? Some organizations choose to have penetration testing conducted after business hours or only on weekends to minimize any impact.

Scope

For a pen test, the *scope* is what should be tested. Scope involves several elements that define the relevant test boundaries. These elements include the following technical boundaries:

- *Environment.* Should the pen test be conducted on the live production environment? This option has the advantage of producing the most accurate test. However, the disadvantage is that it will likely disrupt normal business operations. As an alternative, a simulated environment could be created, but this option comes with additional work and costs.
- *Internal targets*. Before starting a penetration test, all internal targets must be clearly identified for an external third-party gray box test or white box test. (Black box testers are responsible for finding internal targets.) These internal targets are owned by the customer, and information about them may include specific IP addresses, network ranges, or domain names. Also, the scope of internal targets must account for systems such as firewalls, intrusion detection systems, intrusion prevention systems, and networking equipment between the tester and the final target.

CAUTION

Before starting a pen test, all internal targets should be validated to ensure that they are actually owned by the customer. There could be serious legal consequences if a pen tester attacked and successfully penetrated a system—only to discover that it belonged to another organization.

- *External targets*. In some situations, a pen test may include testing a service or an application hosted by a third party. These targets may include cloud service providers or Internet service providers (ISPs).
- *Target locations.* Because laws vary among states, provinces, and countries, testing planners must identify the physical location of the targets and, if necessary, adjust the scope of the test. For instance, countries in the European Union (EU) have more stringent laws surrounding personal privacy, which can change how a social engineering engagement would be executed.
- *Other boundaries*. In addition to technical boundaries, other boundaries should be considered. For example, does the pen test include physical security, such as fencing, cameras, and guards? Are there limitations on who should be targeted by social engineering attacks (such as excluding specific C-suite executives)? Should there be limits on spear-phishing messages, such as those that contain offers for drugs or pornographic material?

CAUTION

The importance of determining the scope of pen testing can be illustrated by an event in 2019. Two security contractors from Coalfire, a penetration testing company that frequently does security assessments for federal agencies and for state and local governments, were arrested in Adel, Iowa, as they attempted to gain access to the Dallas County Courthouse. They claimed to be conducting a penetration test to determine how vulnerable county court records were and to measure law enforcement's response to a break-in. However, because the Iowa state court officials who ordered the test never told county officials about it, the penetration testers were arrested and went to jail. The state officials later apologized to Dallas County, citing confusion over just what Coalfire was going to test, although later both parties said there were "different interpretations" of the scope of the pen test.

Authorization

Authorization is the receipt of prior written approval to conduct the pen test. A formal written document *must* be signed by all parties before a penetration test begins. Naturally, this approval includes people within the organization being tested. However, other levels of authorization are frequently overlooked.

CAUTION

Before performing a pen test against cloud service providers and ISPs, remember that while permission may have been granted by the customer to perform a pen test on external targets, permission must also be obtained from the external targets themselves. Many external targets have specific procedures for penetration testers to follow and may require request forms, scheduling, and explicit permission before testing can begin.

Exploitation

The *exploitation level* in a pen test should also be part of the scope that is discussed in the planning stages. When a vulnerability is uncovered, should it always be exploited? Or are specific areas considered "off limits" so that the tester should not view the related data?

Communication

Communication in penetration testing is particularly important. The pen tester should communicate with the organization on several occasions during the process. These include the following:

- *Initiation*. Once the pen test has started, the organization should be notified that the process has begun.
- *Incident response*. If a pen tester can complete the initial vulnerability assessment without triggering the organization's incident response mechanism, then a critical gap in the security structure has been identified.
- *Status*. Instead of waiting until the pen test is completed, it is better to provide periodic status reports to the organization's management.
- *Emergency*. If the pen tester uncovers a critical vulnerability, it should be immediately reported to the organization's management while the penetration test is paused.

Cleanup

Following the exploitation of the systems outlined in the scope, the pen tester must ensure that everything related to the pen test has been removed. This is called the **cleanup** phase of a pen test and should be clearly outlined in the rules of engagement. Cleanup involves removing all software agents, scripts, executable binaries, temporary files, and backdoors from all affected systems. Also, any credentials that were changed should be restored, and any additional usernames created should be removed. In short, the systems should be returned to their preengagement state.

Reporting

Once the pen test is completed, a report should be generated to document its objectives, methods used, and results. The report should be divided into two parts based on two separate audiences.

The first part of the report should be an executive summary designed for a less technical audience—namely, those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization who may be affected by the identified threats. The executive summary often contains a section that identifies the overall risk of the organization and a breakdown of the types of vulnerabilities that were exploited, as shown in Figure 2-2.

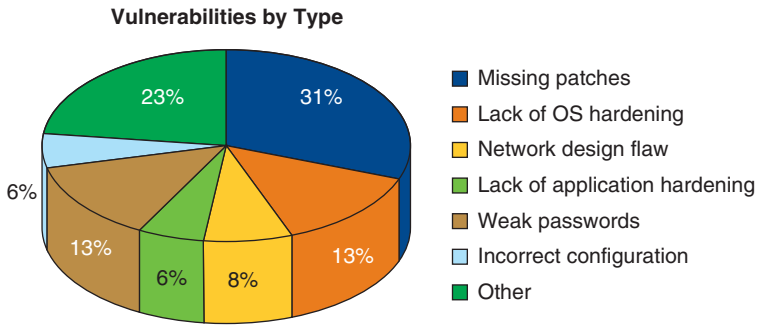


Figure 2-2 Types of vulnerabilities

The second part of the report should be technical in nature and written for security professionals. It should describe in detail the scope of the pen test, the vulnerabilities uncovered, how the vulnerabilities were exploited, the results, and suggested remediation for each vulnerability.

Performing a Penetration Test

Despite how movies portray the ease and speed of breaking into the technology assets of an organization, this is rarely the case in real life. Rather, a great deal of effort and time are needed for performing a penetration test. Many first-time pen testers find the work more difficult than first envisioned.

A key ingredient necessary for performing a successful penetration test is **persistence**, which is defined as *determination, resolve*, and *perseverance*. Pen testers should be prepared for spending long hours and even days searching for vulnerabilities that they might not discover.

Although a variety of actions take place when performing a penetration test, they can be grouped into two phases: reconnaissance and penetration.

Phase 1: Reconnaissance

The first task of the black box and gray box tester is to perform preliminary information gathering from outside the organization. This reconnaissance is called **footprinting**.

Testers gather this information using two methods. **Active reconnaissance** involves directly probing for vulnerabilities and useful information, much like a threat actor would do. For example, unprotected wireless data transmissions from wireless local area networks or Wi-Fi can often be used to gather information or even circumvent security protections. There are different means by which this wireless information can be gathered through active reconnaissance. One means is through **war driving**. War driving is searching for wireless signals from an automobile or on foot while using a portable computing device. To maximize the ability to detect wireless signals, several tools are necessary. These tools are listed in Table 2-3.

Table 2-3 War driving tools

Tool	Purpose
Mobile computing device	A mobile computing device with a wireless NIC can be used for war driving. This includes a standard portable computer, a pad computer, or a smartphone.
Wireless NIC adapter	Many war drivers prefer an external wireless NIC adapter that connects into a USB or other port and has an external antenna jack.
Antenna(s)	Although all wireless NIC adapters have embedded antennas, attaching an external antenna will significantly increase the ability to detect a wireless signal.
Software	Because client utilities and integrated operating system tools provide only limited information about a discovered Wi-Fi, pen testers use more specialized software.
Global positioning system (GPS) receiver	Although this is not required, it does help to pinpoint the location more precisely.

NOTE 3

War driving was originally derived from the term *war dialing*. When telephone modems were popular in the 1980s and 1990s, an attacker could program the device to randomly dial telephone numbers until a computer answered the call. This random process of searching for a connection was known as war dialing, so the word for randomly searching for a wireless signal became known as war driving. However, pen test war driving is not randomly searching for any Wi-Fi signal but is much more focused at finding those associated with the target organization.

However, a more efficient means of discovering a Wi-Fi signal is **war flying**. War flying uses **drones**, which are officially known as **unmanned aerial vehicles (UAVs)**. Because they can quickly cover a wider area, are not limited to streets and sidewalks, and can easily fly over security perimeters such as fences, drones are the preferred means for finding a Wi-Fi signal. A drone is shown in Figure 2-3.

The disadvantage of active reconnaissance in a pen test is that the probes are likely to alert security professionals within the enterprise who do not know about the pen test that something unusual is occurring. This may result in them "locking down" the network to become more restrictive and thus more difficult to probe.

In contrast with active reconnaissance, **passive reconnaissance** takes an entirely different approach: the tester uses tools that do not raise any alarms. This may include searching online for publicly accessible information called **open source intelligence (OSINT)** that can reveal valuable insight about the system.

Source: Kletr/Shutterstock.com

Figure 2-3 Drone

NOTE 4

Active reconnaissance relies on traffic being sent to the targeted system, while passive reconnaissance calls for testers to quietly "make do" with whatever information they can accumulate from public sources.

Phase 2: Penetration

Because a pen test is intended to simulate the actions of a threat actor, the question becomes, "What do threat actors do when they uncover a vulnerability through reconnaissance?" Generally, threat actors follow these steps in an actual attack:

1. The threat actors first conduct reconnaissance against the systems, looking for vulnerabilities.
2. When a path to a vulnerability is exposed, they gain access to the system through the vulnerability.
3. Once initial access is gained, the threat actors attempt to escalate to more advanced resources that are normally protected from an application or user. This is called **privilege escalation**.
4. With the advanced privileges, the threat actors tunnel through the network looking for additional systems they can access from their elevated position (called **lateral movement**).
5. Threat actors install tools on the compromised systems to gain even deeper access to the network.
6. Threat actors may install a backdoor that allows them repeated and long-term access to the system in the future. The backdoors are not related to the initial vulnerability, so access remains even if the initial vulnerability is corrected.
7. Once the backdoor is installed, threat actors can continue to probe until they find their ultimate target and perform their intended malicious action, such as stealing R&D information, password files, or customer credit card numbers.

The initial system that was compromised—the system through which the attackers first gained entry—most often does not contain the data that is the goal of the attack. Rather, this system only serves as a gateway for entry. Once

NOTE 5

Threat actors can exploit *any* vulnerability they uncover, not just a vulnerability on the ultimate target. This means they are not defeated if they cannot find a vulnerability on the target; rather, a remote vulnerability can be used to pivot to the final target.

they are inside the network, the threat actors **pivot**, or turn, to other systems to be compromised, with the goal of reaching the ultimate target.

Several lessons can be learned from how threat actors work, and those lessons can be applied to a penetration test. First, when a vulnerability is discovered during a penetration test, the work is not finished. Instead, the pen tester must determine how to pivot to another system using another vulnerability to continue moving toward the target. Second, vulnerabilities that are not part of the ultimate target can still provide a gateway to that target. This means that no vulnerability is insignificant for a pen tester. Third, unlike some types of automated vulnerability scanning, penetration tests are manual. Therefore, a pen tester needs to design attacks carefully. Finally, because threat actors are patient and persistent, pen testers must also be patient and persistent. A pen test is not a task that should be scheduled for completion quickly; rather, a good pen test may take an extended amount of time to uncover all weaknesses.

CAUTION

Whereas the work of attackers (and pen testers) has generally required manual effort for lateral movement and pivoting, some attackers are now automating their lateral movements within a compromised system.

TWO RIGHTS & A WRONG

1. The Purple Team is made up of the referees who enforce the rules of a pen test.
2. One advantage of using external pen testing consultants is their credentials.
3. White box testers are given full knowledge of the network.

See Appendix B for the answer.

VULNERABILITY SCANNING

CERTIFICATION

1.7 Summarize the techniques used in security assessments.

Like penetration testing, vulnerability scanning is considered an important task in maintaining a cybersecurity defense; in fact, vulnerability scanning in some ways complements pen testing. Studying vulnerability scanning involves understanding what it is, how to conduct a scan, how to use data management tools, and how threat hunting can enhance scanning.

What Is a Vulnerability Scan?

Older model cars typically have a "Needs Service" light on the dashboard that turns on after the car has been driven a certain number of miles, indicating that service such as an oil change is needed. While performing the oil change, a mechanic could note that additional repairs are needed. Newer model cars, on the other hand, usually track mileage automatically. Dealers send the owner monthly email reminders of when the next service is due and even indicate if something is not working properly so the owner can have it taken care of immediately.

The difference between older and newer cars is similar to the difference between a penetration test and a vulnerability scan. A penetration test is a single event using a manual process often performed only after a specific amount of time has passed, such as once a year (and sometimes only to comply with regulatory requirements). A **vulnerability scan**, on the other hand, is a frequent and ongoing process, usually automated, that continuously

identifies vulnerabilities and monitors cybersecurity progress. In other words, a vulnerability assessment is a cyclical process of ongoing scanning and continuous monitoring to reduce the attack surface. Table 2-4 contrasts a vulnerability scan with a penetration test.

Table 2-4 Vulnerability scan vs. penetration test

	Vulnerability Scan	Penetration Test
Purpose	Reduces the attack surface	Identifies deep vulnerabilities
Procedure	Scans to find weaknesses and then mitigate them	Acts like a threat agent to find vulnerabilities to exploit
Frequency	Usually includes ongoing scanning and continuous monitoring	Tests when required by regulatory body or on a predetermined schedule
Personnel	Uses internal security personnel	Uses external third parties or internal security personnel
Process	Usually is automated, with a handful of manual processes	Uses an entirely manual process
Goal	Aims to identify risks by scanning systems and networks	Aims to gain unauthorized access and exploit vulnerabilities
Final report audience	Includes an executive summary for less technical audiences and technical details for security professionals	Includes several different audiences

NOTE 6

A vulnerability scan and a penetration test are similar in some ways. For example, both should be conducted following a data breach, the launch of a new application, or a major change to the network. However, because a vulnerability scan is continuous, it may only need to focus on the new application or change to the network.

Conducting a Vulnerability Scan

Conducting a vulnerability scan involves knowing what to scan and how often, along with selecting a type of scan and interpreting vulnerability information. All vulnerability scans require a close examination of the results.

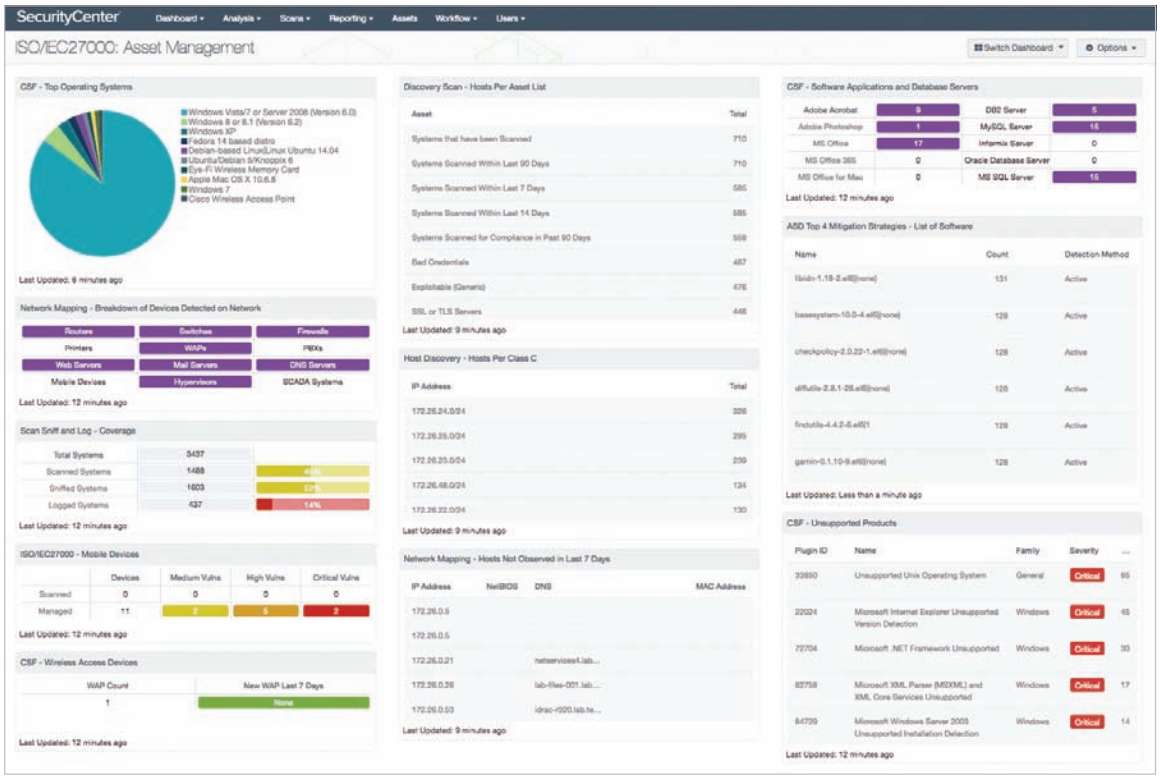
When and What to Scan

It might seem that the optimum approach for vulnerability scanning is simply to scan all systems all the time. However, that approach is usually not practical. There are two primary reasons for not conducting around-the-clock vulnerability scans:

- *Workflow interruptions*. Continual vulnerability scans may impact the response time of a system so that its daily workflow or normal business processes are hindered. Moving the scans to "off hours" such as nights or weekends can limit interruptions.
- *Technical constraints*. Limitations based on technology can dictate how frequently a scan may be performed. For an organization with a large network that contains many devices, it simply may not be possible to scan the entire network within a desired time period. Other technical constraints include limitations on network bandwidth and vulnerability scan software license limitations. When dealing with technical constraints, spreading out the scans to run at specific times may be a necessary alternative.

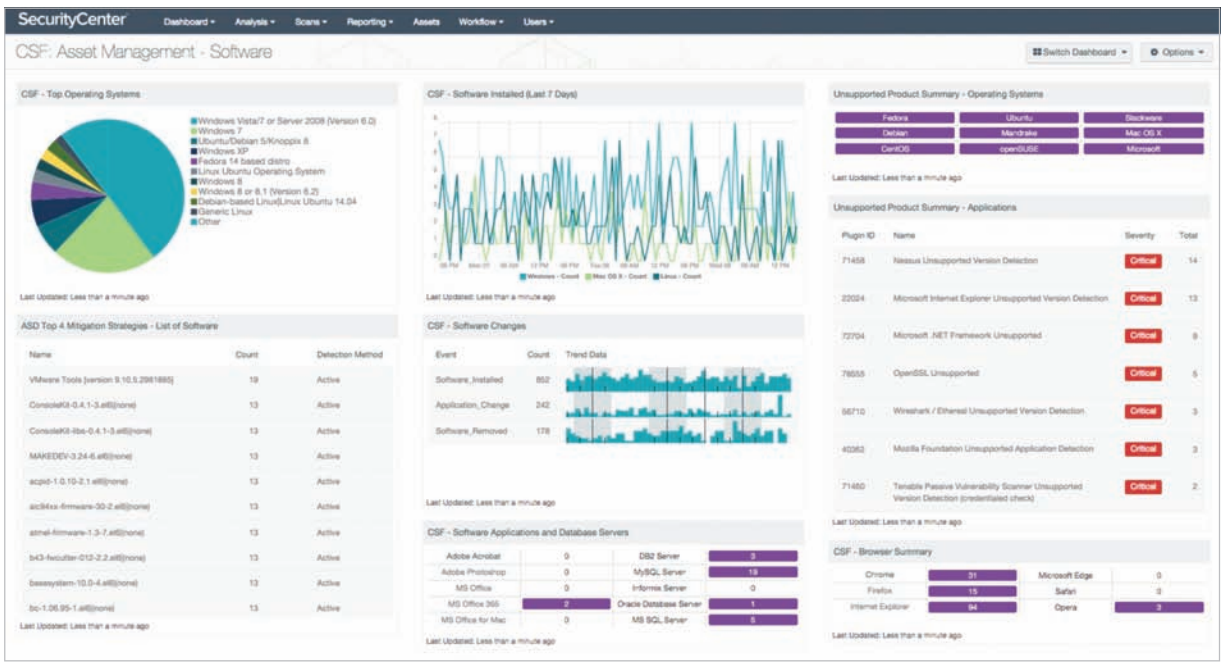
When considering what to scan, the temptation to scan everything is again not practical. Some organizations may instead choose to scan the network, applications, and web applications on a rotating basis. However, running a full vulnerability scan of just the network can take a significant amount of time to find all assets and assess their vulnerabilities.

A more focused approach is to know the location of data so that specific systems with high-value data can be scanned more frequently. Organizations can create a list of systems to be scanned by creating and then consulting an *asset inventory*, a list of all significant assets. If no asset inventory is available, then most vulnerability scanning tools allow for an inventory scan that only searches for devices attached to the network instead of conducting a full vulnerability scan. Figure 2-4 shows the hardware asset management screen of the vulnerability scanner Nessus. Software assets should also be identified and scanned; Figure 2-5 shows the Nessus software asset management screen.



Source: Tenable

Figure 2-4 Nessus hardware asset management



Source: Tenable

Figure 2-5 Nessus software asset management

NOTE 7

While several vulnerability scanning tools are available, Nessus is perhaps the best-known and most widely used vulnerability scanner. It is a product of Tenable and contains a wide array of pre-built templates. Nessus advertises that new information about vulnerabilities are available as soon as 24 hours after a new vulnerability is disclosed. Nessus has a free version called Nessus Essentials that scans 16 IP addresses.

Because a vulnerability scan should be limited, a **configuration review** of the software settings should be conducted. This may include the following tasks:

- Define the group of target devices to be scanned, which may include a range of hosts or subnets.
- Ensure that a scan should be designed to meet its intended goals. If a specific vulnerability for Windows 10 computers is being targeted in the scan, for example, it makes sense to scan only Windows 10 systems.
- Determine the *sensitivity level* or the depth of a scan—in other words, the type of vulnerabilities being searched for. While a general scan may search for all vulnerabilities, a scan often looks for a specific type of vulnerability.
- Specify the data types to be scanned. Like the sensitivity level, this setting can be used to "drill down" when searching for a specific vulnerability in a known file type instead of searching all files on a system.

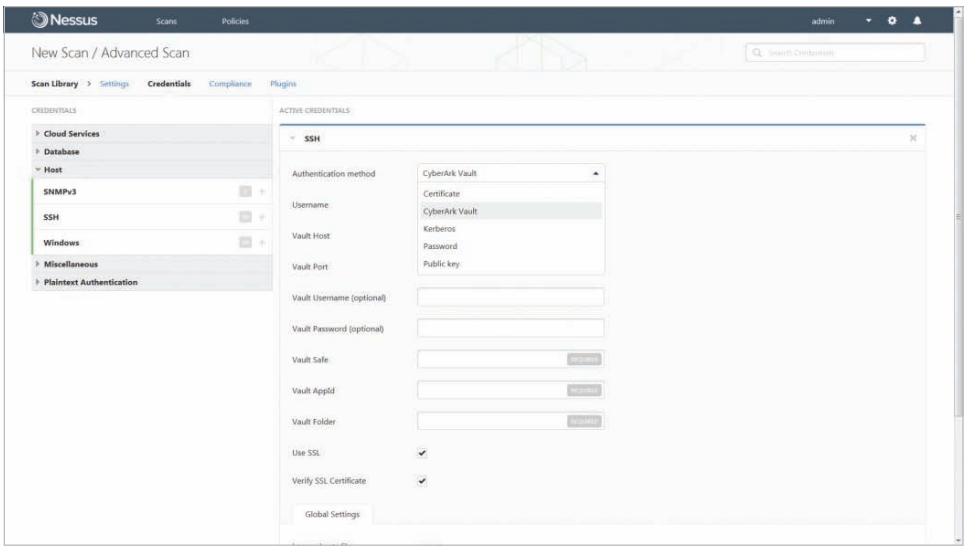
NOTE 8

A configuration review can also reduce the vulnerability scan's impact on overall network performance.

Types of Scans

There are several types of vulnerability scans. Two of the major types of scans are credentialed scans and intrusive scans.

Credentialed vs. Non-credentialed Scans In a **credentialed scan**, valid authentication credentials, such as usernames and passwords, are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials. A **non-credentialed scan** provides no such authentication information. Figure 2-6 shows the credentials that can be entered for a credentialed scan.



Source: Tenable

Figure 2-6 Credentialed scan

NOTE 9

Non-credentialed scans run faster because they perform fundamental actions such as looking for open ports and finding software that will respond to requests. Credentialed scans are slower but can provide a deeper insight into the system by accessing a fuller range of the installed software and examining the software's configuration settings and current security posture.

Intrusive vs. Nonintrusive Scans An **intrusive scan** attempts to employ any vulnerabilities that it finds, much like a threat actor would. A **nonintrusive scan** does not attempt to exploit the vulnerability but only records that it was discovered. While intrusive tests are more accurate, they can impair the target system. In some cases, the system may even become unstable and unusable. However, a nonintrusive scan cannot determine for certain if an installed service is truly vulnerable; rather, it can only indicate that it *might* be vulnerable.

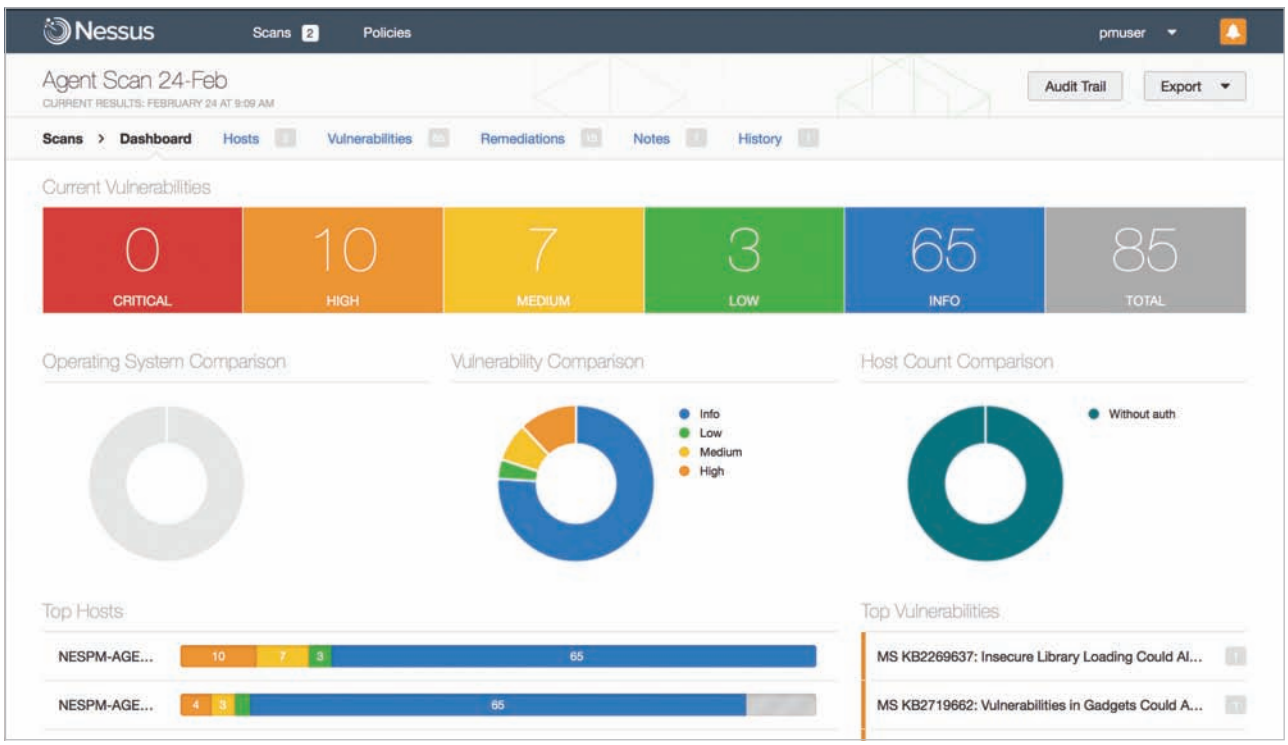
Vulnerability Information

Vulnerability scanning software looks for a vulnerability by comparing the software it scans against a set of known vulnerabilities. Such monitoring requires access to an updated database of vulnerabilities along with a means of actively comparing and matching to known vulnerabilities.

Vulnerability information is available to provide updated information to scanning software about the latest vulnerabilities. Several sources are available. However, the most popular vulnerability feed is the Mitre **Common Vulnerabilities and Exposures (CVE)**. The CVE identifies vulnerabilities in operating systems and application software.

Examining Results

Consider a vulnerability scan that produces the 20 vulnerabilities listed in Figure 2-7. Although the list includes no critical vulnerabilities, others are categorized as high, medium, and low. When addressing these vulnerabilities, where do you begin? Do you start with the high vulnerabilities and work your way down, or is there a better approach to take? How do you know that each is indeed a true vulnerability?



Source: Tenable

Figure 2-7 Results of vulnerability scan

When examining the results of a vulnerability scan, you should assess the importance of vulnerability as well as its accuracy.

Importance Many new security personnel are surprised to learn *it is rarely possible, and often not desirable, to address all vulnerabilities*. Not all vulnerabilities are as potentially damaging as others. Also, although a scanner might assign a medium rating to a vulnerability, not all organizations react to the rating in the same way. To one company, this vulnerability may be critical, but to another, it is not worth the effort to fix. Because many vulnerabilities are complex

to unravel and take an extended amount of time to address, organizations may not have enough time to solve all of them. So, beginning with the high vulnerabilities and working down through the low ones may not always be the best plan of action.

Instead, vulnerabilities need to be prioritized so that the most important ones are addressed early on, while others are delayed until later or are not even addressed. Several criteria are used for prioritizing vulnerabilities.

First, a numeric score is usually assigned to a vulnerability based on the **Common Vulnerability Scoring System (CVSS)**. The numeric scores are generated using a complex formula that considers variables such as the access vector, attack complexity, authentication, confidentiality of the data, and the system's integrity and availability. The vulnerabilities with the highest CVSS scores are generally considered to require early attention.

However, the vulnerabilities with higher CVSS scores may not always be the ones that should be addressed first. Instead, look at scores and the entire vulnerability scan in the context of the organization. These questions about a vulnerability may help in identifying which ones need early attention:

- Can the vulnerability be addressed in a reasonable amount of time, or would it take several days or even a week to fix?
- Can the vulnerability be exploited by an external threat actor, or would exploitation require that the person be sitting at a computer in a vice president's office?
- If the vulnerability led to threat actors infiltrating the system, would they be able to pivot to more important systems, or would they be isolated?
- Is the data on the affected device sensitive or is it public?
- Is the vulnerability on a critical system that runs a core business process, or is it on a remote device that is rarely used?

Prioritizing vulnerabilities is an inexact and sometimes difficult process. However, attention should first be directed toward vulnerabilities deemed to be critical (those that can cause the greatest degree of harm to the organization). Another part of prioritizing is making sure that the difficulty and time for implementing the correction is reasonable.

Accuracy Another consideration when examining results of a vulnerability scan is to review its accuracy. First, be sure to identify false positives. A **false positive** is an alarm raised when there is no problem; a **false negative** is the failure to raise an alarm when there is an issue. Vulnerability scans may produce false positives for several reasons; for example, scan options may not have been well defined or may have been missed in a configuration review, or the scanner might not recognize a control that is already in place to address an existing vulnerability. Security professionals should attempt to identify false positives in a scan report, especially those that would require extensive effort to address.

One means of identifying false positives is to correlate the vulnerability scan data with several internal data points. The most common are related log files. Because a **log** is simply a record of events that occur, system event logs document any unsuccessful events and the most significant successful events. The types of information recorded might include the date and time of the event; a description of the event; its status, error codes, and service name; and the user or system that was responsible for launching the event. **Log reviews**, or an analysis of log data, can be used to identify false positives.

Logs can be particularly helpful internal data points when correlating with vulnerability scan results. For example, if a scan indicates that a vulnerability in a software application was found on a specific device, but a follow-up investigation revealed that the application was no longer vulnerable, log files could indicate whether that program's configuration had been changed between the time of the scan and the follow-up analysis.

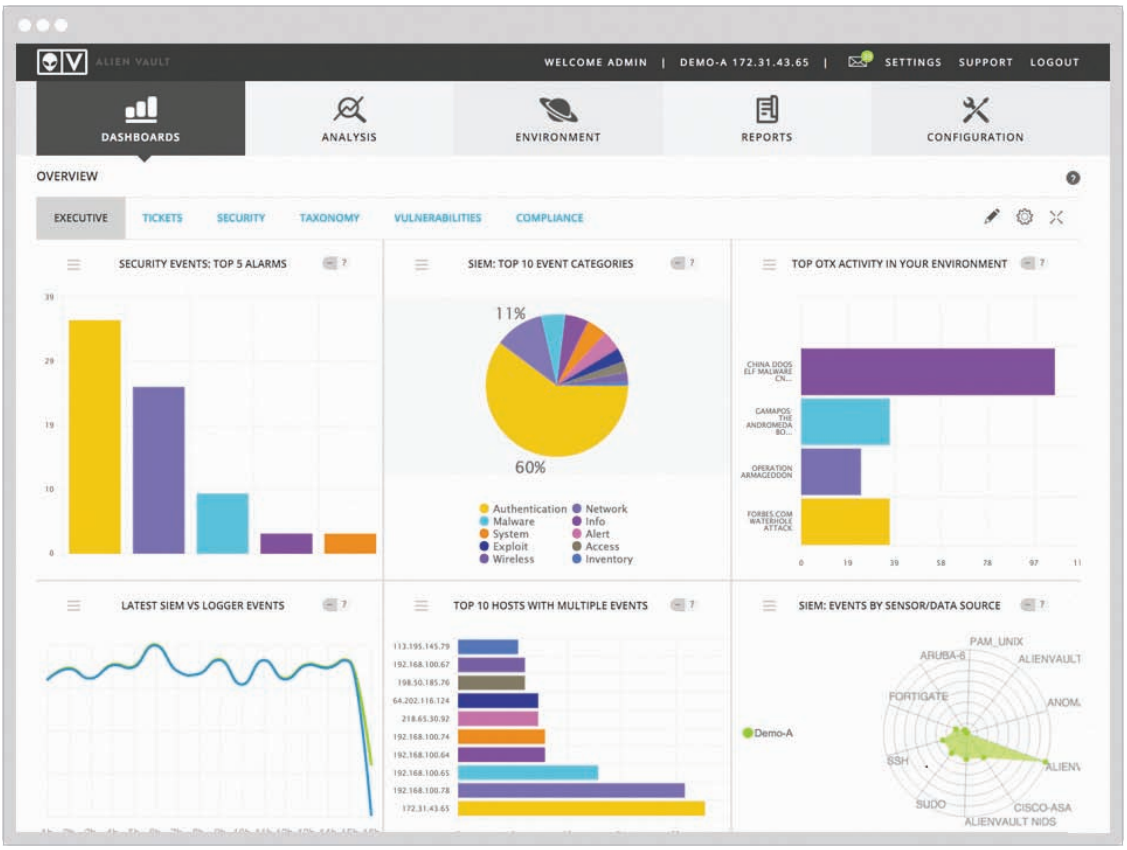
Data Management Tools

In addition to logs, each of the tools for monitoring the security of a network—such as resource monitors, firewalls, and routers—also generate security alerts continuously because an enterprise is the target of continual attacks. How can these alerts, all from different sources and generated at different times, be monitored and managed while searching for evidence of vulnerabilities and attacks?

Two data management tools are used for collecting and analyzing this data. These tools are Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR).

Security Information and Event Management (SIEM)

A **Security Information and Event Management (SIEM)** product (usually pronounced *seem* instead of *sim*) consolidates real-time security monitoring and management of *security information* with analysis and reporting of *security events*. A SIEM product can be a separate device, software that runs on a computer, or even a service provided by a third party. A SIEM dashboard is shown in Figure 2-8.



Source: Alien Vault

Figure 2-8 SIEM dashboard

The starting point of a SIEM is the data input. Data feeds into a SIEM are the standard packet captures of network activity and log collections. Because of the numerous network devices producing logs, SIEMs also perform log aggregation.

A SIEM typically has the following features:

- *Aggregation*. *SIEM aggregation* combines data from multiple data sources—such as network security devices, servers, and software applications—to build a comprehensive picture of attacks.
- *Correlation*. The *SIEM correlation* feature searches the data acquired through SIEM aggregation to look for common characteristics, such as multiple attacks coming from a specific source.
- *Automated alerting and triggers*. *SIEM automated alerting and triggers* can inform security personnel of critical issues that need immediate attention. A sample trigger may be *Alert when a firewall, router, or switch indicates 40 or more drop/reject packet events from the same IP source address within 60 seconds*.
- *Time synchronization*. Because alerts occur over a wide spectrum of time, *SIEM time synchronization* can show the order of the events.
- *Event duplication*. When the same event is detected by multiple devices, each generates an alert. The *SIEM event duplication* feature can help filter the multiple alerts into a single alarm.
- *Logs*. *SIEM logs* or records of events can be retained for future analysis and to show that the enterprise has been in compliance with regulations.

However, a SIEM goes beyond collecting and aggregating data. A SIEM can perform **user behavior analysis**. User behavior analysis looks at the normal behavior of users and how they interact with systems to create a picture of

typical "everyday" activity. A user's account suddenly acting in an unusual fashion, such as a lateral movement between assets, could indicate that a threat actor has compromised that account. A SIEM can generate an alert for further investigation.

SIEMs can also perform **sentiment analysis**. Sentiment analysis is the process of computationally identifying and categorizing opinions, usually expressed in response to textual data, to determine the writer's attitude toward a particular topic. In other words, sentiment analysis is the interpretation and classification of emotions (positive, negative, and neutral) within text data using text analysis techniques. Sentiment analysis has been used when tracking postings threat actors make in discussion forums with other attackers to better determine the behavior and mindset of threat actors. This type of information can be valuable in determining their goals and actions and has even been used as a predictive power to alert against future attacks.

NOTE 10

Sentiment analysis is often used by businesses while conducting online chats with customers or examining Twitter and other social media posts to identify customer sentiment toward products, brands, and services.

Security Orchestration, Automation, and Response (SOAR)

A **Security Orchestration, Automation, and Response (SOAR)** product is similar to a SIEM in that it is designed to help security teams manage and respond to security warnings and alarms. However, SOARs take it a step further by combining more comprehensive data gathering and analytics to automate incident response. While a SIEM tends to generate more alerts than a security team may be able to respond to, a SOAR allows a security team to automate incident responses.

Threat Hunting

It is common today for threat actors to invade a network by slipping past defenses. These threat actors then quietly lurk in "stealth" mode, evading detection, looking for confidential material or stealing login credentials to infiltrate laterally across the network. Attackers can remain unnoticed for weeks, months, and even years before they finally find their valuable treasure.

Vulnerability scans and the SIEM and SOAR tools that provide dashboards of security incidents are considered as *reactive*: during or after an event occurs, something is noticed, and alarms are sounded.

What if instead of being reactive, security tools could be more *proactive*? That is, rather than waiting for an attack to take place, what if the threats could be identified before they occur? That is the principle behind threat hunting. **Threat hunting** is proactively searching for cyber threats that thus far have gone undetected in a network.

Threat hunting begins with a critical major premise: *threat actors have already infiltrated our network.* It proceeds to find unusual behavior that may indicate malicious activity. One means of finding this unusual behavior is for the threat hunter himself to conduct unusual behavior, called **maneuvering**. For example, passwords on an administrator's account are changed every two hours (not a normal activity) to determine if a hidden threat actor is making internal password-cracking attempts. Another maneuver is to clear Domain Name Server (DNS) caches regularly to help detect if the hidden attacker is trying to communicate with an external server.

Threat hunting investigations often use crowdsourced attack data. This data includes *advisories and bulletins*, cybersecurity **threat feeds**, which are data feeds of information on the latest threats, and information from a **fusion center**, which is a formal repository of information from enterprises and the government used to share information on the latest attacks. By learning from others who have been successfully attacked, threat hunters can use this attack data for insight into the attacker's latest tactics, techniques, and procedures. Threat hunting also uses advanced data analytics to sift massive amounts of data to detect irregularities that may suggest potential malicious activity. These anomalies then become hunting leads that skilled analysts investigate to identify the silent threats.

TWO RIGHTS & A WRONG

1. The purpose of a vulnerability scan is to reduce the attack surface.
2. SIEMs generate alerts and automate incident response.
3. The Common Vulnerabilities and Exposures (CVE) vulnerability feed identifies vulnerabilities in operating systems and application software.

See Appendix B for the answer.

CYBERSECURITY RESOURCES

CERTIFICATION

1.5 Explain different threat actors, vectors, and intelligence sources.

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organization security posture.

It would be a sobering task for an organization to attempt to mount a defense against threat actors by itself. Fortunately, that is not necessary. A variety of external cybersecurity resources are available that defenders have at their disposal to help ward off attacks. These resources include frameworks, regulations, legislation, standards, benchmarks/secure configuration guides, and information sources.

Frameworks

A cybersecurity **framework** is a series of documented processes used to define policies and procedures for implementing and managing security controls in an enterprise environment. About 84 percent of U.S. organizations use a security framework, and 44 percent use multiple frameworks.[1] The most common frameworks are from the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), American Institute of Certified Public Accountants (AICPA), Center for Internet Security (CIS), and Cloud Security Alliance (CSA).

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST), operating under the U.S. Commerce Department, created the NIST cybersecurity frameworks as a set of guidelines for helping private companies identify, detect, and respond to cyberattacks. These frameworks also include guidelines for how to prevent and recover from an attack.

The NIST cybersecurity frameworks are divided into three basic parts. The first part is the *framework core*, which defines the activities needed to attain different cybersecurity results. The framework core is further subdivided into four elements, which are listed in Table 2-5.

Table 2-5 Cybersecurity framework core elements

Element Name	Description	Example
Functions	The most basic cybersecurity tasks	Identify, protect, detect, respond, and recover
Categories	Tasks to be carried out for each of the five functions	To protect a function, organizations must implement software updates, install antivirus and antimalware programs, and have access control policies in place
Subcategories	Tasks or challenges associated with each category	To implement software updates (a category), organizations must be sure that Windows computers have auto-updates turned on
Information Sources	The documents or manuals that detail specific tasks for users and explain how to accomplish the tasks	A document is required that details how auto-updates are enabled on Windows computers

The second part of the NIST cybersecurity frameworks is the *implementation tiers*. The NIST framework specifies four implementation tiers that help organizations identify their level of compliance: the higher the tier, the more compliant the organization.

The third and final part is *profiles*. Profiles relate to the current status of the organization's cybersecurity measures and the "road maps" toward compliance with the NIST cybersecurity framework. Profiles are like an executive summary of everything an organization has done for the NIST cybersecurity framework, and they can help demonstrate how each

function, category, or subcategory can increase security. These profiles allow organizations to see their vulnerabilities at each step; once the vulnerabilities are mitigated, the organization can move up to higher implementation tiers.

There are two widely used NIST frameworks:

- *Risk Management Framework (RMF)*. The **NIST Risk Management Framework (RMF)** is considered a guidance document designed to help organizations assess and manage risks to their information and systems. It is viewed as comprehensive road map that organizations can use to seamlessly integrate their cybersecurity, privacy, and supply-chain risk management processes.
- *Cybersecurity Framework (CSF)*. The **NIST Cybersecurity Framework (CSF)** is used as a measuring stick companies can use to compare their cybersecurity practices to the threats they face. The elements of the CSF are shown in Figure 2-9.

Source: NIST

Figure 2-9 NIST Cybersecurity Framework (CSF) functions

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) has created a wide array of cybersecurity standards. The ISO 27000 is a family of 72 standards designed to help organizations keep information assets secure. **ISO 27001** is a standard that provides requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive assets so that they remain secure. These assets include the people, processes, and IT systems used to manage risk. **ISO 27002** is a code of practice for information security management within an organization and contains 114 control recommendations. **ISO 27701**, an extension to ISO 27001, is a framework for managing privacy controls to reduce the risk of privacy breach to the privacy of individuals. **ISO 31000** contains controls for managing and controlling risk.

American Institute of Certified Public Accountants (AICPA)

The American Institute of Certified Public Accountants (AICPA) is the national professional organization for Certified Public Accountants (CPAs) in the United States. The AICPA has created a series of Statements on Standards for Attestation Engagements (SSAE). (An "attestation engagement" is technically "an arrangement with a client where an independent third party investigates and reports on subject matter created by a client" but is better known as an internal controls report or audit.) One AICPA SSAE is a suite of services called the System and Organization Controls (SOCs), which are service offerings that Certified Public Accountants (CPAs) may provide in connection with system-level controls of a service organization or entity-level controls of other organizations. The two primary SOCs that relate to cybersecurity are the following:

- *SSAE SOC 2 Type II.* The **SSAE SOC 2 Type II** report is an internal controls report that reviews how a company safeguards customer data and how well those controls are operating. As an audit, it looks at internal controls, policies, and procedures that directly relate to the security of a system at a service organization. The SOC 2 report is designed to determine if service organizations are compliant with the categories of security, availability, processing integrity, confidentiality, and privacy.
- *SSAE SOC 2 Type III.* The **SSAE SOC 2 Type III** report is the same as a SOC 2 Type II except for its distribution. A SOC 3 report can be freely distributed, whereas a SOC 2 can only be read by the user organizations that rely on the services. While a SOC 3 does not give a description of the service organization's system, it can provide interested parties with the auditor's report on whether an entity maintained effective controls over its systems.

Center for Internet Security (CIS)

The **Center for Internet Security (CIS)** is a nonprofit community-driven organization. It has created two recognized frameworks. The *CIS Controls* are controls for securing an organization and consist of more than 20 basic and advanced cybersecurity recommendations. The *CIS Benchmarks* are frameworks for protecting 48 operating systems and application software.

NOTE 11

Other security frameworks include ISACA Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Open Group Architecture Framework, and AXELOS IT Infrastructure Library (ITIL).

Cloud Security Alliance

The **Cloud Security Alliance (CSA)** is an organization whose goal is to define and raise awareness of best practices to help secure cloud computing environments. Its **Cloud Controls Matrix** is a specialized framework (*meta-framework*) of cloud-specific security controls. These controls are mapped to the leading standards, best practices, and regulations regarding cloud computing and are generally regarded as the authoritative source of information (**reference architecture**) about securing cloud resources. The current version of the Cloud Controls Matrix is v3.0.1 and was released in August 2019.

Regulations

Another cybersecurity resource are *regulations,* and the process of adhering to them is called *regulatory compliance*. Industry **regulations** are typically developed by established professional organizations or government agencies using the expertise of seasoned security professionals. These regulations are followed by companies that have similar business processes, resulting in a common set of tested and approved regulations that are under continual review and revision. Almost every industry has its own set of regulations, and cybersecurity is no exception; several regulations relate to IT and specifically to cybersecurity.

However, organizations face significant challenges to achieve regulatory compliance. First, virtually all organizations must follow multiple regulations from different regulatory bodies. For example, this is a small sample of cybersecurity regulations or related regulations that an organization may be required to follow:

- *Broadly applicable regulations*. Sarbanes-Oxley Act (SOX or Sarbox), Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley (GLB) Act, Electronic Fund Transfer Act, Regulation E (EFTA), Customs-Trade Partnership Against Terrorism (C-TPAT), Free and Secure Trade Program (FAST), Children's Online Privacy Protection Act (COPPA), Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule, Federal Rules of Civil Procedure (FRCP), Computer Fraud and Abuse Act (CFAA), Federal Privacy Act of 1974, Federal Intelligence Surveillance Act (FISA) of 1978, Electronic Communications Privacy Act (ECPA) of 1986, Communications Assistance for Law Enforcement Act (CALEA) of 1994, and the USA Patriot Act of 2001
- *Industry-specific regulations*. Federal Information Security Management Act (FISMA), North American Electric Reliability Corp. (NERC) standards, Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records, Health Insurance Portability and Accountability Act (HIPAA), The Health Information Technology for Economic and Clinical Health Act (HITECH), Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule), and H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation
- *U.S. state regulations*. Massachusetts 201 CMR 17, Nevada Personal Information Data Privacy Encryption Law NRS 603A
- *International regulations*. Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, Federal Law on the Protection of Personal Data Held by Private Parties in Mexico and Safe Harbor Act. An international regulation that has received worldwide attention is the **European Union General Data Protection Directive (GDPR)**. The GDPR is a regulation regarding data protection and privacy in the EU and the European Economic Area (EEA). Its aim is to give individuals control over their personal data, to address the transfer of personal data to areas outside the EU and EEA, and to simplify the regulatory environment for international business by creating a single regulation across all EU members.

CAUTION

With so many regulations that must be followed, organizations often find it difficult to meet all of the requirements. Also, it is not unusual for a requirement in one regulation to adversely impact—or, in some instances, even negate—a requirement in another regulation.

Legislation

Specific legislation or laws can also be enacted by governing bodies that can provide a cybersecurity resource. These include national, territorial, and state laws. However, with the number of different entities involved in passing multiple—and even contradictory—legislation, this often leads to a hodgepodge of legislation and is not always a good cybersecurity resource.

As an example, consider legislation regarding notification for a specific type of cyber incident. The United States does not have a federal law that requires a notification. In that absence, states have legislative mandates for communication. California's Database Security Breach Notification Act was passed in 2003, and by 2018, all other states had passed similar notification laws. Although there is a common core of definitions about personal information and what constitutes a breach of security, due to a lack of comprehensive federal regulations for data breach notification, many states have amended their breach notification laws from the basic definitions shown here. As a result, no two state laws are the same. Table 2-6 lists some of the deviations from these basic definitions, along with examples of states where the deviations occur and expanded definitions of the laws.

Table 2-6 Deviations in state laws from basic definitions

Deviation	Example State	Expanded Definition
Broader definition of personal information	Alabama	A tax identification number; passport number; military identification number; other unique identification number issued on a government document used to verify the identity of a specific individual; any information about an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; a username or email address in combination with a password or security question and answer.
Notification triggered by access to data and not documented theft	Florida	"Breach of security" means unauthorized access to personal information in electronic format.
Breach must satisfy risk-of-harm analysis	Arkansas	Notification is not required if, after a reasonable investigation, the business determines that there is no reasonable likelihood of harm to customers.
Expanded notification beyond impacted citizens	Colorado	Additional notice must be provided to the state attorney general.
Includes encryption safe harbor	Alaska	The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed.
Covers other forms of data	Hawaii	The statute applies to personal information in any form, whether computerized, paper, or otherwise.

Standards

A **standard** is a document approved through consensus by a recognized standardization body. It provides for frameworks, rules, guidelines, or characteristics for products or related processes and production methods. Strictly speaking, compliance is not mandatory, but there may be restrictions for those organizations that do not comply.

One cybersecurity standard is the **Payment Card Industry Data Security Standard (PCI DSS)**. The PCI DSS compliance standard was introduced to provide a minimum degree of security for handling customer card information. Requirement 11 of the latest standard (PCI DSS 3.2.1) states that organizations must *regularly test security systems and processes* using both vulnerability scans and penetration tests. A partial list of the PCI DSS Requirement 11 standards is shown in Table 2-7.

Table 2-7 PCI DSS Requirement 11 standards

Standard	Description	Frequency
11.1	Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points.	Quarterly
11.2	Run internal and external network vulnerability scans to address vulnerabilities and perform rescans as needed until passing scans are achieved. External scans must be performed by an Approved Scanning Vendor (ASV), while scans conducted after network changes and internal scans may be performed by internal staff.	At least quarterly and after any significant change in the network
11.3	Develop and implement a methodology for penetration testing that includes external and internal testing. If segmentation is used to reduce PCI DSS scope, perform penetration tests to verify that the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls.	At least annually and after any significant upgrade or modification; service providers must perform penetration testing at least every six months and after making changes to controls

Benchmarks/Secure Configuration Guides

Benchmark/secure configuration guides are usually distributed by hardware manufacturers and software developers. These serve as guidelines for configuring a device or software so that it is resilient to attacks. Usually, these are **platform/vendor-specific guides** that only apply to specific products. Guides are available for network infrastructure devices, OSs, web servers, and application servers.

Information Sources

There are a variety of information sources that can provide valuable in-depth information. Generic sources include

- Vendor websites
- Conferences
- Academic journals
- Local industry groups
- Social media

There are also specialized research sources that apply specifically to cybersecurity. **Requests for comments (RFCs)** are white papers documents that are authored by technology bodies employing specialists, engineers, and scientists who are experts in those areas. These RFCs describe methods, behaviors, research, or innovations applicable to cybersecurity. *Data feeds* are continually maintained databases of the latest cybersecurity incidences. Common cybersecurity data feeds include **vulnerability feeds** that provide information on the latest vulnerabilities and **threat feeds** that outline current threats and attacks. The **adversary tactics, techniques, and procedures (TTP)** is a database of the behavior of threat actors and how they orchestrate and manage attacks.

TWO RIGHTS & A WRONG

1. The two NIST frameworks are the NIST Risk Management Framework (RMF) and NIST Cybersecurity Framework (CSF).
2. The Center for Internet Security (CIS) has published a Cloud Controls Matrix.
3. The European Union General Data Protection Directive (GDPR) is a regulation regarding data protection and privacy in the EU and the European Economic Area (EEA).

See Appendix B for the answer.

VM LAB You're now ready to complete the live virtual machine labs for this module. The labs can be found in each module in the MindTap.

SUMMARY

- Penetration testing attempts to exploit vulnerabilities just as a threat actor would. This helps to uncover new vulnerabilities, provide a clearer picture of their nature, and determine how they could be used against the organization. The most important element in a pen test is the first step of planning. A lack of planning can result in a flawed penetration test that tries to do too little or too much. A scan of network defenses can help find vulnerabilities, but the types of vulnerabilities revealed are different from a penetration test. A scan usually finds only surface problems to be addressed. This is because many scans are entirely automated and provide only a limited verification of any discovered vulnerabilities. A penetration test can find deep vulnerabilities. Penetration tests go further and attempt to exploit vulnerabilities using manual techniques.
- Using internal employees to conduct a penetration test has advantages in some cases. First, there is little or no additional cost. Also, the test can be conducted much more quickly. However, these employees may lack expertise or have too much inside knowledge to be able to perform a valid pen test. External pen tester consultants have the credentials and experience for conducting a test. Recently, some third-party organizations have begun offering crowdsourced pen testing. Instead of contracting with a single external pen tester consulting organization, crowdsourced pen testing involves a large group of individuals who are not regular employees of an organization.
- The rules of engagement in a penetration test are its limitations or parameters. Without these parameters, a penetration test may not accomplish the desired results, may take too long to produce timely results, or may test assets that are not necessary to test. The categories for the rules for engagement are timing, scope, authorization, exploitation, communication, cleanup, and reporting.
- The first phase of a penetration test is reconnaissance, also called footprinting. Active reconnaissance involves directly probing for vulnerabilities and useful information, much like a threat actor would do. Passive reconnaissance takes an entirely different approach: the tester uses tools that do not raise any alarms. The second phase is penetration by simulating the actions of an attacker. After the initial system is compromised, threat actors then pivot or turn to other systems to be compromised, with the goal of reaching the ultimate target.
- A penetration test is a single event using a manual process that is usually performed only after a specific amount of time has passed, such as once a year (and sometimes only to comply with regulatory requirements). However, a vulnerability scan is a frequent and ongoing process, often automated, that continuously identifies vulnerabilities and monitors cybersecurity progress. A vulnerability assessment is a cyclical and continual process of ongoing scanning and continuous monitoring to reduce the attack surface.
- The best approach for vulnerability scanning is not to scan all systems all the time. Usually, it is not practical to do so. A more focused approach is to know the location of data so that specific systems with high-value data can be scanned more frequently. There are several types of vulnerability scans. A credentialed scan is a scan in which valid authentication credentials, such as usernames and passwords, are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials. A non-credentialed scan provides no such authentication information. An intrusive scan attempts to employ any vulnerabilities it finds, much like a threat actor would. A nonintrusive scan does not attempt to exploit the vulnerability but only records that it was discovered.
- Vulnerability information is available to provide updated information to scanning software about the latest vulnerabilities. The Mitre Common Vulnerabilities and Exposures (CVE) identifies vulnerabilities in operating systems and application software. When examining the results of a vulnerability scan, you should assess the importance of vulnerability as well as its accuracy.

- Two data management tools are used for collecting and analyzing this data. The first is the Security Information and Event Management (SIEM) tool. It consolidates real-time security monitoring and management of security information with analysis and reporting of security events. A SIEM product can be a separate device, software that runs on a computer, or even a service provided by a third party. A Security Orchestration, Automation, and Response (SOAR) tool is similar to a SIEM in that it is designed to help security teams manage and respond to the very high number of security warnings and alarms. However, SOARs combine more comprehensive data gathering and analytics in order to automate incident response. Threat hunting is proactively searching for cyber threats that thus far have gone undetected in a network.
- There are a variety of external cybersecurity resources available that defenders have at their disposal to help ward off attacks. A cybersecurity framework is a series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment. The most common frameworks are from the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), American Institute of Certified Public Accountants (AICPA), Center for Internet Security (CIS), and Cloud Security Alliance (CSA). Regulations are another cybersecurity resource. Industry regulations are typically developed by established professional organizations or government agencies using the expertise of seasoned security professionals. These regulations are followed by companies that have similar business processes, resulting in a common set of tested and approved regulations that are under continual review and revision. Specific legislation or laws can also be enacted by governing bodies that can provide a cybersecurity resource.
- A standard is a document approved through consensus by a recognized standardization body. It provides for frameworks, rules, guidelines, or characteristics for products or related processes and production methods. Strictly speaking, compliance is not mandatory, but there may be restrictions for those organizations that do not comply. Benchmark/secure configuration guides are usually distributed by hardware manufacturers and software developers. These serve as a guideline for configuring a device or software so that it is resilient to attacks. Usually these are platform/vendor-specific guides that only apply to specific products. A variety of information sources can provide valuable information. Some are generic sources while others are specific to cybersecurity.
- Deep vulnerabilities can only be exposed through actual attacks that use the mindset of a threat actor. First, the attacks must be the same (or remarkably similar) as those used by a threat actor; anything less will not uncover the deep vulnerabilities that an attacker can find. Second, the attacks should follow the thinking of threat actors. Understanding their thinking helps to better perceive what assets they are seeking, how they may craft the attack, and even how determined they are to obtain assets. Without having an attacker's mindset, it is difficult to find these deep vulnerabilities.

Key Terms

active reconnaissance
adversary tactics, techniques, and procedures (TTP)
benchmark/secure configuration guides
Black box
Blue Team
bug bounty
Center for Internet Security (CIS)
cleanup
Cloud Controls Matrix
Cloud Security Alliance (CSA)
Common Vulnerabilities and Exposures (CVE)
Common Vulnerability Scoring System (CVSS)
configuration review
credentialed scan
drone
European Union General Data Protection Directive (GDPR)
false negative
false positive
footprinting
framework
fusion center
Gray box
intrusive scan
ISO 27001
ISO 27002
ISO 27701
ISO 31000
lateral movement
log
log reviews
maneuvering
NIST Cybersecurity Framework (CSF)
NIST Risk Management Framework (RMF)
non-credentialed scan
nonintrusive scan
open source intelligence (OSINT)
passive reconnaissance

Payment Card Industry Data Security Standard (PCI DSS)
penetration testing
persistence
pivot
platform/vendor-specific guides
privilege escalation
Purple Team
Red Team
reference architecture
regulations
request for comments (RFC)
rules of engagement
Security Information and Event Management (SIEM)
Security Orchestration, Automation and Response (SOAR)
sentiment analysis
SSAE SOC 2 Type II
SSAE SOC 2 Type III
standard
threat feeds
threat hunting
unmanned aerial vehicle (UAV)
user behavior analysis
vulnerability feeds
vulnerability scan
war driving
war flying
White box
White Team

Review Questions

1. Ebba has received a new initiative for her security team to perform an in-house penetration test. What is the first step that Ebba should undertake?
   a. Approval
   b. Budgeting
   c. Planning
   d. Documentation

2. Which of the following is NOT a characteristic of a penetration test?
   a. Automated
   b. Finds deep vulnerabilities
   c. Performed occasionally
   d. May use internal employees or external consultants

3. Linnea has requested to be placed on the penetration testing team that scans for vulnerabilities to exploit them. Which team does she want to be placed on?
   a. Blue Team
   b. Purple Team
   c. White Team
   d. Red Team

4. Lykke's supervisor is evaluating whether to use internal security employees to conduct a penetration test. Lykke does not consider this a good idea and has created a memo with several reasons they should not be used. Which of the following would NOT be part of that memo?
   a. The employees could have inside knowledge of the network that would give them an advantage.
   b. There may be a lack of expertise.
   c. Employees may have a reluctance to reveal a vulnerability.
   d. They would have to stay overnight to perform the test.

5. What penetration testing level name is given to testers who have no knowledge of the network and no special privileges?
   a. Black box
   b. Gray box
   c. White box
   d. Purple box

6. Which of the following is NOT an advantage of crowdsourced penetration testing?
   a. Faster testing
   b. Less expensive
   c. Ability to rotate teams
   d. Conducting multiple tests simultaneously

7. Tilde is working on a contract with the external penetration testing consultants. She does not want any executives to receive spear-phishing emails. Which rule of engagement would cover this limitation?
   a. Scope
   b. Exploitation
   c. Targets
   d. Limitations and exclusions

8. Which is the final rule of engagement that would be conducted in a pen test?
   a. Cleanup
   b. Communication
   c. Reporting
   d. Exploitation

9. What is another name for footprinting?
   a. High-level reconnaissance
   b. Active reconnaissance
   c. Modeling
   d. Revealing

10. When researching how an attack recently took place, Nova discovered that the threat actor, after penetrating the system, started looking to move through the network with their elevated position. What is the name of this technique?
    a. Jumping
    b. Twirling
    c. Squaring up
    d. Lateral movement

11. What are documents that are authored by technology bodies employing specialists, engineers, and scientists who are experts in those areas?
    a. Cybersecurity feeds
    b. White notebooks
    c. Blue papers
    d. Requests for comments (RFCs)

12. Which of the following is not a general information source that can provide valuable in-depth information on cybersecurity?
    a. Twitter
    b. Conferences
    c. Local industry groups
    d. Vendor websites

13. Which of the following is a standard for the handling of customer card information?
    a. DRD STR
    b. OSS XRS
    c. RMR CDC
    d. PCI DSS

14. Which of the following are developed by established professional organizations or government agencies using the expertise of seasoned security professionals?
    a. Legislation
    b. White papers
    c. Regulations
    d. Benchmarks

15. Which group is responsible for the Cloud Controls Matrix?
    a. CSA
    b. CIS
    c. OSINT
    d. NIST

16. Tuva's supervisor wants to share a recent audit outside the organization. Tuva warns him that this type of audit can only be read by those within the organization. What audit does Tuva's supervisor want to distribute?
    a. SSAE SOC 2 Type II
    b. SSAE SOC 2 Type III
    c. SSAE SOC 3 Type IV
    d. SSAE SOC 3.2 Type X

17. Which ISO contains controls for managing and controlling risk?
    a. ISO XRS
    b. ISO 31000
    c. ISO 271101
    d. ISO 27555

18. Which premise is the foundation of threat hunting?
    a. Cybercrime will only increase.
    b. Threat actors have already infiltrated our network.
    c. Attacks are becoming more difficult.
    d. Pivoting is more difficult to detect than ever before.

19. Which of the following can automate an incident response?
    a. SIEM
    b. SOAR
    c. CVCC
    d. SOSIA

20. Which of the following is NOT something that a SIEM can perform?
    a. User behavior analysis
    b. Sentiment analysis
    c. Log aggregation
    d. Incident response

Hands-On Projects

Project 2-1: Exploring Common Vulnerabilities and Exposures (CVE)

Time Required: 20 minutes
Objective: Summarize the techniques used in security assessments.
Description: Vulnerability feeds are available to provide updated information to scanning software about the latest vulnerabilities. One of the most highly regarded vulnerability feeds is the Mitre Common Vulnerabilities and Exposures (CVE). Feeds can also be manually examined for information on the latest vulnerabilities. In this project, you will learn more about CVE and view CVE information.

1. Open your web browser and enter the URL **https://cve.mitre.org/** (if you are no longer able to access the site through this web address, use a search engine to search for "Mitre CVE").
2. Click **About**.
3. Click **About CVE**.
4. This page gives a brief overview of CVE. Read through the information regarding CVE. In your own words, how would you describe it? How does it work? What advantages does it provide?
5. Point to **About**.
6. Click **FAQs** to display more detailed information on CVE. Who is behind CVE? Who owns it? How is it used? How does CVE compare to a vulnerability database? How would you answer the argument that threat actors could use CVE?
7. Scroll down to **CVE Entries**. Describe the three elements that make up a CVE Entry.
8. Scroll down to **CVE List Basics**. What is the process by which a vulnerability becomes a CVE listing? Who is involved in this process?
9. Click the link **CVE Data Feeds**. Scroll through the newest CVE entries feed. Were you aware of these vulnerabilities? How does the CVE distribute its information? Would you consider it sufficient? How can this be used by security personnel?
10. Click **Search CVE List**.
11. Enter a generic vulnerability such as **passwords** to display the CVE entries. How many are there that relate to this topic?
12. Select several of the CVE entries and read through the material.
13. Locate a CVE entry that contains the tag *Disputed*. Click this entry. Under *Description* click ****DISPUTED**** to read about what constitutes a disputed CVE. Who would dispute a CVE? Why?
14. Click **Search CVE List**.
15. Enter a different vulnerability and select several entries to read through its details.
16. Close all windows.

Project 2-2: Exploring the National Vulnerability Database

Time Required: 20 minutes
Objective: Explain different threat actors, vectors, and intelligence sources.
Description: The National Vulnerability Database (NVD) is managed by the U.S. government as a repository for vulnerability management data and contains software flaws, misconfigurations, product names, and their impacts. In this project, you will explore the NVD.

1. Open your web browser and enter the URL **https://nvd.nist.gov/** (if you are no longer able to access the site through this web address, use a search engine to search for "NIST NVD").
2. Click the plus sign next to **General**.
3. Click **FAQ**.
4. Click **General FAQs**.
5. Read through the material. In your own words, how does the Mitre CVE compare with the NIST NVD? When would you use the CVE? When would you use the NVD? How frequently is the NVD updated? Is this often enough?
6. Return to the home page by clicking the back button as many times as necessary.
7. Click the plus sign next to **General**.
8. Click **NVD Dashboard** to view the latest information. Do the numbers surprise you? How does the number of vulnerabilities under the score distribution compare? Is that what you would have expected?
9. Scroll through the *Last 20 Scored Vulnerability IDs & Summaries*. Have you heard of any of these vulnerabilities? How will they be distributed to the public at large?
10. Return to the home page.
11. Click the plus sign next to **General**.
12. Click **Visualizations** to display graphical information.
13. Click **Vulnerabilities – CVE**.

14. Click **Description Summary Word** to display a bar graph of the most common words used as part of a vulnerability description, as seen in Figure 2-10. Hover over the three highest bars to view the three most frequent words used. Is this what you would have expected?

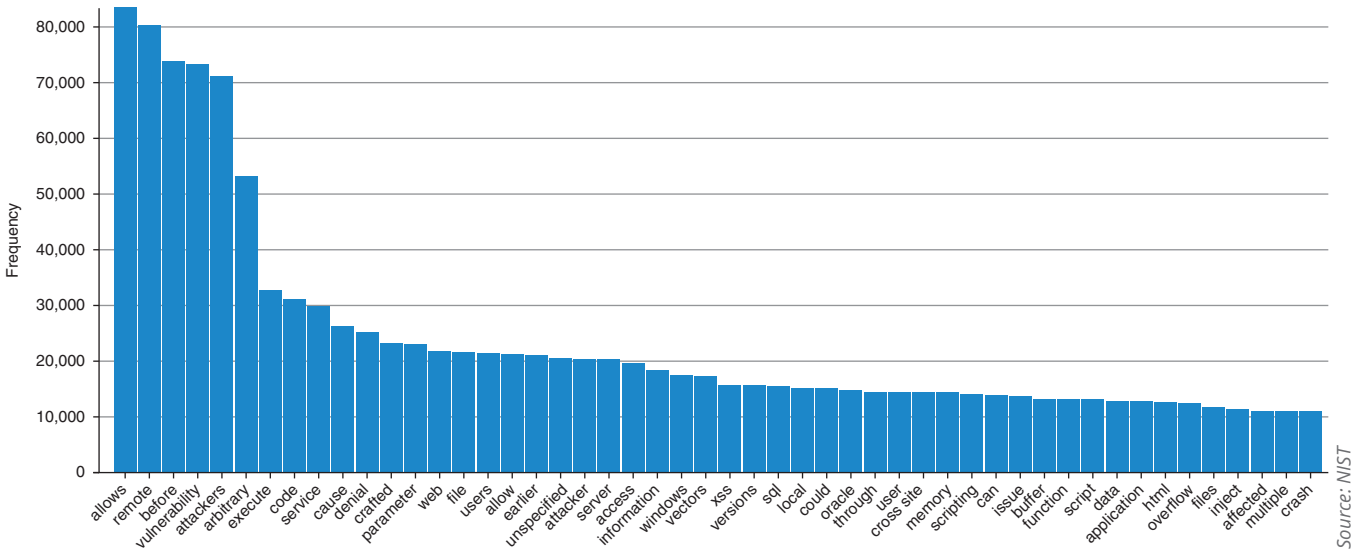


Figure 2-10 NVD Description Summary Word Frequency

15. Return to the Vulnerability Visualizations page. Select each of the other graphs and study the information presented. How could this information be used by a security professional?
16. Return to the NVD Visualizations page. Click **Products – CPE**. Which vendor has the highest number of total products that appears in the NVD? View other vendors by hovering over the bars. What do you find interesting about this distribution?
17. Return to the home page by clicking the back button as many times as necessary.
18. Click the plus sign next to **Other Sites**.
19. Click **Checklist (NCP) Repository**.
20. This page displays a form you can use to search for benchmarks/secure configuration guides. Select different parameters to view different guides, and then select one to view in detail. Is this information helpful?
21. Return to the home page by clicking the back button as many times as necessary.
22. Click the plus sign next to **Search**.
23. Click **Vulnerability Search**.
24. Enter **passwords**. How many vulnerabilities are found? Select several of these to read through the information.
25. Select a different vulnerability to search the NVD database. How useful is this information?
26. Close all windows.

Project 2-3: Sentiment Analysis

Time Required: 20 minutes
Objective: Summarize the techniques used in security assessments.
Description: Sentiment analysis is the process of computationally identifying and categorizing opinions, usually expressed in response to textual data, in order to determine the writer's attitude toward a particular topic. It has been used when tracking postings threat actors make to determine the behavior and mindset of threat actors and has even been used as a predictive power to alert against future attacks. In this project, you will experiment with sentiment analysis to learn of its capabilities.

1. Open your web browser and enter the URL **https://monkeylearn.com/** (if you are no longer able to access the site through this web address, use a search engine to search for "MonkeyLearn").
2. Click **RESOURCES** and then **Guides**. This webpage helps show how sentiment analysis fits into the context of artificial intelligence.

3. Click **Sentiment Analysis** and read through what it is, how it is useful, and how it can be performed.
4. Now create an account. Go to **https://app.monkeylearn.com/accounts/register/** and follow the instructions to create a MonkeyLearn account, and then sign in.
5. Click **Explore**.
6. Click **Sentiment Analysis**.
7. Enter the text **I like sunshine.** and click **Classify Text**. What tag does it provide, and what is the confidence level?
8. Enter several random phrases and perform an analysis on each.
9. Return to the Explore screen.
10. Select **Hotel Aspect**.
11. Search the Internet for two reviews of a hotel—one that you consider would be positive and another that would be negative—and paste the first review into the text box. Click **Classify Text**. Would you agree with the analysis? Then do the same with the second review.
12. Return to the Explore screen.
13. Select **Sentiment Analysis**.
14. Use a search engine to search the Internet for *cybersecurity quotations.* Cut and paste several of these into the text box and analyze them.
15. Now enter statements from threat actors. Go to Google Images (**https://images.google.com**).
16. Enter the search word **ransomware**.
17. Locate ransomware screens that contain messages from threat actors and enter these into the Sentiment Analysis text box for analysis. What is the sentiment analysis for these quotations from threat actors?
18. How could sentiment analysis be useful in identifying a threat actor's mindset? Do you think it could be used for predicting attacks?
19. Close all windows.

Case Projects

Case Project 2-1: False Positives and False Negatives

Use the Internet to research false positives and false negatives. Which is worse? If a doctor gives information to a patient about the results of a diagnostic test, is a false positive or a false negative worse? What about facial recognition scanning for a criminal? Which is worse for a vulnerability scan, a false positive or a false negative? Write a one-page paper on your findings and analysis.

Case Project 2-2: Pen Test Products

Use the Internet to research pen test scanners. Select three scanners and create a table that compares their features. Be sure to include such elements as how often they are updated, the systems they run on, and available tools. Based on your analysis, which would you recommend? Why?

Case Project 2-3: Vulnerability Scanners

Search the Internet for information on Nessus. Then search for two other vulnerability scanners. Create a table that compares their features. Which would you choose? Why?

Case Project 2-4: Threat Actor Tactics

Most users are unaware of how threat actors work and their various tactics. Read the article *Tales From the Trenches; a Lockbit Ransomware Story* at **www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/**. This article contains detailed information about the tactics of threat actors for a particular strain of ransomware. Although some of the information is very technical in nature, it does give a good picture of the advanced skills and strategies used today. Write a one-paragraph summary of what you have learned about their tactics.

Case Project 2-5: Information Security Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. In order to gain the most benefit from the site, you will need to set up a free account.

Go to **community.cengage.com/infosec2**. Create a posting about what you have learned in Module 2. What were your biggest surprises? What did you already know? How could you use this information in your first security job?

Case Project 2-6: North Ridge Security

North Ridge Security provides security consulting and assurance services to more than 500 clients in more than 20 states for a wide range of enterprises. A new initiative at North Ridge is for each of its seven regional offices to provide internships to students who are in their final year of the security degree program at the local college.

North Ridge is preparing a request for proposal (RFP) for a potential new client to perform a penetration test. You have been asked to develop a first draft on the rules of engagement for pen testing a web server running the Apache OS and Apache Tomcat.

1. Use the Internet to research information about Apache OS and Apache Tomcat. Then create a rules of engagement document that contains your recommendations for the seven engagement rules found in this module.
2. As a follow-up to your rules of engagement document, create a PowerPoint presentation for the potential customer on why they should use North Ridge Security instead of internal security personnel or crowdsourced pen testers. Your presentation should be at least seven slides in length.

References

1. Watson, Melanie, "Top 4 Cybersecurity Frameworks," *IT Governance*, Jan. 17, 2019, accessed Sep. 13, 2019, www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks.