Chapter 8

Using Risk Management Tools

CompTIA Security+ objectives covered in this chapter:

1.4 Explain penetration testing concepts.

- Active reconnaissance, Passive reconnaissance, Pivot, Initial exploitation, Persistence, Escalation of privilege, Black box, White box, Gray box, Penetration testing vs. vulnerability scanning

1.5 Explain vulnerability scanning concepts.

- Passively test security controls, Identify vulnerability, Identify lack of security controls, Identify common misconfigurations, Intrusive vs. non-intrusive, Credentialed vs. non- credentialed, False positive

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

- SIEM (Aggregation, Correlation, Automated alerting and triggers, Time synchronization, Event deduplication, Logs/WORM)

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Protocol analyzer, Network scanners (Rogue system detection, Network mapping), Wireless scanners/cracker, Password cracker, Vulnerability scanner, Configuration compliance scanner, Exploitation frameworks, Banner grabbing, Passive vs. active, Command line tools (Tcpdump, nmap, netcat)

2.3 Given a scenario, troubleshoot common security issues.

- Unencrypted credentials/clear text, Logs and events anomalies

3.2 Given a scenario, implement secure network architecture concepts.

- Security device/technology placement

o Correlation engines

3.8 Explain how resiliency and automation strategies reduce risk.

- Automation/scripting (Continuous monitoring, Configuration validation)

4.4 Given a scenario, differentiate common account management practices.

- General Concepts (Permission auditing and review, Usage auditing and review)

5.3 Explain risk management processes and concepts.

- Threat assessment (Environmental, Manmade, Internal vs. external), Risk assessment (SLE, ALE, ARO, Asset value, Risk register, Likelihood of occurrence, Supply chain assessment, Impact, Quantitative, Qualitative), Testing (Penetration testing authorization, Vulnerability testing authorization), Risk response techniques (Accept, Transfer, Avoid, Mitigate)

**

As a security professional, you need to be aware of the different security issues associated with threats, vulnerabilities, and risks, and the tools available to combat them. This chapter digs into risk management concepts, including risk assessment methods. You'll learn about vulnerability scanners and penetration testers, including key differences between them. This chapter also covers some specific tools used to assess networks and manage risks.

Understanding Risk Management

Risk is the likelihood that a threat will exploit a vulnerability. A vulnerability is a weakness, and a threat is a potential danger. The result is a negative impact on the organization. Impact refers to the magnitude of harm that can be caused if a threat exercises a vulnerability.

For example, a system without up-to-date antivirus software is vulnerable to malware. Malware written by malicious attackers is the threat. The likelihood that the malware will reach a vulnerable system represents the risk. Depending on what the malware does, the impact may be an unbootable computer, loss of data, or a remote-controlled computer that has joined a botnet. However, the likelihood of a risk occurring isn't 100 percent. An isolated system without Internet access, network connectivity, or USB ports has a very low likelihood of malware infection.

The likelihood significantly increases for an Internet-connected system, and it increases even more if a user visits risky web sites and downloads and installs unverified files.

It’s important to realize that you can’t eliminate risk. Sure, you can avoid information technology (IT) risks completely by unplugging your computer and burying it. However, that wouldn’t be very useful. Instead, users and organizations practice risk management to reduce the risks.

You probably practice risk management every day. Driving or walking down roads and streets can be a very dangerous activity. Car-sized bullets are speeding back and forth, representing significant risks to anyone else on the road. However, you mitigate these risks with caution and vigilance. The same occurs with computers and networks. An organization mitigates risks using different types of security controls.

Threats and Threat Assessments

A ***threat*** is a potential danger. Within the context of risk management, a threat is any circumstance or event that can compromise the confidentiality, integrity, or availability of data or a system. Threats come in different forms, including the following:

- **Malicious human threats.** Chapter 6, “Comparing Threats, Vulnerabilities, and Common Attacks,” discusses various types of threat actors. They include relatively inexperienced script kiddies, dedicated criminals working within an organized crime group, and sophisticated advanced persistent threats (APTs) sponsored by a government. These are all malicious human threats. Malicious human threats regularly launch different types of attacks, including network attacks, system attacks, and the release of malware.
- **Accidental human threats.** Users can accidentally delete or corrupt data, or accidentally access data that they shouldn’t be able to access. Even administrators can unintentionally cause system outages. The common cause is by a well-meaning administrator making a configuration change to fix one problem but inadvertently causing another one.
- **Environmental threats.** This includes long-term power failure, which could lead to chemical spills, pollution, or other possible threats to the environment. It also includes natural threats such as hurricanes, floods, tornadoes, earthquakes, landsides, electrical storms, and other similar events.

A ***threat assessment*** helps an organization identify and categorize threats. It attempts to predict the threats against an organization's assets, along with the likelihood the threat will occur. Threat assessments also attempt to identify the potential impact from these threats. Once the organization identifies and prioritizes threats, it identifies security controls to protect against the most serious threats.

Organizations have limited resources, so it's not possible to protect against all threats. However, threat assessments improve the security posture of any system or application by ensuring that the resources aren't squandered on low-priority threats. Some common types of threat assessments are:

- **Environmental.** An environmental threat assessment evaluates the likelihood of an environmental threat occurring. For example, I live in Virginia Beach, Virginia, and while we're concerned about the natural threat of hurricanes during the hurricane season, we aren't very concerned about earthquakes. My sister is a business continuity expert and she lives near San Francisco and works in Silicon Valley. She helps companies prepare for risks associated with earthquakes there, but she spends very little time or energy considering the risk of a hurricane hitting San Francisco.
- **Manmade.** A manmade threat assessment evaluates all threats from humans. These include both malicious human threats and accidental human threats. A malicious human threat refers to any potential attack from a person or group of people. An accidental human threat refers to any potential loss caused by a person or group accidentally.
- **Internal.** An internal threat assessment evaluates threats from within an organization. This includes threats from malicious employees and threats from accidents. It also includes threats related to hardware failure.
- **External.** An external threat assessment evaluates threats from outside an organization. This includes any threats from external attackers. It also includes any natural threats, such as hurricanes, earthquakes, and tornadoes.

Remember this

A threat is a potential danger and a threat assessment evaluates potential threats. Environmental threats include natural threats such as weather events. Manmade threats are any potential dangers from people and can be either malicious or accidental. Internal threats typically refer to employees within an organization, while external threats can come from any source outside the organization.

Vulnerabilities

A ***vulnerability*** is a flaw or weakness in software or hardware, or a weakness in a process that a threat could exploit, resulting in a security breach. Examples of vulnerabilities include:

- **Lack of updates.** If systems aren't kept up to date with patches, hotfixes, and service packs, they are vulnerable to bugs and flaws in the software.
- **Default configurations.** Hardening a system includes changing systems from their default hardware and software configurations, including changing default usernames and passwords. If systems aren't hardened, they are more susceptible to attacks. Chapter 5, "Securing Hosts and Data," covers hardening systems in more depth.
- **Lack of malware protection or updated definitions.** Antivirus and anti-spyware methods protect systems from malware, but if they aren't used and kept up to date, systems are vulnerable to malware attacks. Chapter 6 covers malware types and methods used to protect systems from malware attacks.
- **Lack of firewalls.** If personal and network firewalls aren't enabled or configured properly, systems are more vulnerable to network and Internet-based attacks.
- **Lack of organizational policies.** If job separation, mandatory vacations, and job rotation policies aren't implemented, an organization may be more susceptible to fraud and collusion from employees.

Not all vulnerabilities are exploited. For example, a user may install a wireless router using the defaults. It is highly vulnerable to an attack, but that doesn't mean that an attacker will discover it and attack. In other words, just because the wireless router has never been attacked, it doesn't mean that it isn't vulnerable. At any moment, a war driving attacker can drive by and exploit the vulnerability.

Risk Management

Risk management is the practice of identifying, monitoring, and limiting risks to a manageable level. It doesn't eliminate risks, but instead identifies methods to limit or mitigate them. The amount of risk that remains after managing risk is residual risk.

The primary goal of risk management is to reduce risk to a level that the organization will accept. Senior management is ultimately responsible for residual risk. Management must choose a level of acceptable risk based on their organizational goals. They decide what resources (such as money, hardware, and time) to dedicate to mitigate the risk.

There are multiple ***risk response techniques***, or risk management methods, available to an organization. They include:

- **Avoid.** An organization can avoid a risk by not providing a service or not participating in a risky activity. For example, an organization may evaluate an application that requires multiple open ports on the firewall that it considers too risky. It can avoid the risk by purchasing a different application that doesn't require opening any additional firewall ports.
- **Transfer.** The organization transfers the risk to another entity, or at least shares the risk with another entity. The most common method is by purchasing insurance. Another method is by outsourcing, or contracting a third party.
- **Mitigate.** The organization implements controls to reduce risks. These controls either reduce the vulnerabilities or reduce the impact of the threat. For example, up-to-date antivirus software mitigates the risks of malware. Similarly, a security guard can reduce the risk of an attacker accessing a secure area.
- **Accept.** When the cost of a control outweighs a risk, an organization will often accept the risk. For example, spending $100 in hardware locks to secure a $15 mouse doesn't make sense. Instead, the organization accepts the risk of someone stealing a mouse. Similarly, even after implementing controls, residual risk remains and the organization accepts this residual risk.

Remember this

It is not possible to eliminate risk, but you can take steps to manage it. An organization can avoid a risk by not providing a service or not participating in a risky activity. Insurance transfers the risk to another entity. You can mitigate risk by implementing controls, but when the cost of the controls exceeds the cost of the risk, an organization accepts the remaining, or residual, risk.

Risk Assessment

A ***risk assessment***, or risk analysis, is an important task in risk management. It quantifies or qualifies risks based on different values or judgments. A risk assessment starts by first identifying assets and asset values.

An asset includes any product, system, resource, or process that an organization values. The ***asset value*** identifies the worth of the asset to the organization. It can be a specific monetary value or subjective value, such as Low, Medium, and High. The asset value helps an organization focus on the high-value assets and avoid wasting time on low-value assets.

After identifying asset values, the risk assessment then identifies threats and vulnerabilities and determines the likelihood a threat will attempt to exploit a vulnerability. A risk assessment attempts to identify the impact of potential threats and identify the potential harm, and prioritizes risks based on the likelihood of occurrence and impact. Last, a risk assessment includes recommendations on what controls to implement to mitigate risks.

A risk assessment is a point-in-time assessment, or a snapshot. In other words, it assesses the risks based on current conditions, such as current threats, vulnerabilities, and existing controls. For example, consider a library computer that has up-to-date antivirus protection and cannot access the Internet. Based on these conditions, the risks are low. However, if administrators connect the system to the Internet, or fail to keep the antivirus software up to date, the risk increases.

It’s common to perform risk assessments on new systems or applications. For example, if an organization is considering adding a new service or application that can increase revenue, it will often perform a risk assessment. This helps it determine if the potential risks may offset the potential gains.

Risk assessments use quantitative measurements or qualitative measurements. Quantitative measurements use numbers, such as a monetary figure representing cost and asset values. Qualitative measurements use judgments. Both methods have the same core goal of helping management make educated decisions based on priorities.

Quantitative Risk Assessment

A ***quantitative risk assessment*** measures the risk using a specific monetary amount. This monetary amount makes it easier to prioritize risks. For example, a risk with a potential loss of $30,000 is much more important than a risk with a potential loss of $1,000.

The asset value is an important element in a quantitative risk assessment. It may include the revenue value or replacement value of an asset. A web server may generate $10,000 in revenue per hour. If the web server fails, the company will lose $10,000 in direct sales each hour it's down, plus the cost to repair it. It can also result in the loss of future business if customers take their business elsewhere. In contrast, the failure of a library workstation may cost a maximum of $1,000 to replace it.

One commonly used quantitative model uses the following values to determine risks:

- **Single loss expectancy (SLE).** The ***SLE*** is the cost of any single loss.
- **Annual rate of occurrence (ARO).** The ***ARO*** indicates how many times the loss will occur in a year. If the ARO is less than 1, the ARO is represented as a percentage. For example, if you anticipate the occurrence once every two years, the ARO is 50 percent or.5.
- **Annual loss expectancy (ALE).** The ***ALE*** is the value of SLE × ARO.

Imagine that employees at your company lose, on average, one laptop a month. Thieves have stolen them when employees left them in conference rooms during lunch, while they were on-site at customer locations, and from training rooms.

Someone suggested purchasing hardware locks to secure these laptops for a total of $1,000. These locks work similar to bicycle locks and allow employees to wrap the cable around a piece of furniture and connect into the laptop. A thief needs to either destroy the laptop to remove the lock or take the furniture with him when stealing the laptop. Should your company purchase them? With a little analysis, the decision is easy.

You have identified the average cost of these laptops, including the hardware, software, and data, is $2,000 each. This assumes employees do not store entire databases of customer information or other sensitive data on the systems, which can easily result in much higher costs. You can now calculate the SLE, ARO, and ALE as follows:

- **SLE.** The value of each laptop is $2,000, so the SLE is $2,000.
- **ARO.** Employees lose about one laptop a month, so the ARO is 12.
- **ALE.** You calculate the ALE as SLE × ARO, so $2,000 × 12 = $24,000.

Security experts estimate that these locks will reduce the number of lost or stolen laptops from 12 a year to only 2 a year. This changes the ALE from $24,000 to only $4,000 (saving $20,000 a year). In other words, the organization can spend $1,000 to save $20,000. It doesn't take a rocket scientist to see that this is a good fiscal decision, saving a net of $19,000. Buy them.

Managers use these two simple guidelines for most of these decisions:

- If the cost of the control is less than the savings, purchase it.
- If the cost of the control is greater than the savings, accept the risk.

The organization might be considering other controls, such as a combination of hardware locks, biometric authentication, LoJack for Laptops, and more. The final cost of all of these controls is $30,000 per year. Even if a laptop is never stolen again, the company is spending $30,000 to save $24,000, resulting in a higher net loss—they're losing $6,000 more a year.

Admittedly, a company could choose to factor in other values, such as the sensitivity of data on the laptops, and make a judgment to purchase these additional controls. However, if they're using a quantitative risk assessment, these values would need to be expressed in monetary terms.

Although you would normally know the SLE and ARO and use these to calculate the ALE, you might occasionally have the SLE and ALE, but not know the ARO. Using basic algebra, you can reformat the formula. Any of these are valid:

- ALE = SLE × ARO
- ARO = ALE / SLE
- SLE = ALE / ARO

Remember this

A quantitative risk assessment uses specific monetary amounts to identify cost and asset values. The SLE identifies the amount of each loss, the ARO identifies the number of failures in a year, and the ALE identifies the expected annual loss. You calculate the ALE as SLE × ARO. A qualitative risk assessment uses judgment to categorize risks based on likelihood of occurrence and impact.

Qualitative Risk Assessment

A ***qualitative risk assessment*** uses judgment to categorize risks based on ***likelihood of occurrence*** (or probability) and impact. The likelihood of occurrence is the probability that an event will occur, such as the likelihood that a threat will attempt to exploit a vulnerability. ***Impact*** is the magnitude of harm resulting from a risk. It includes the negative results of an event, such as the loss of confidentiality, integrity, or availability of a system or data.

Notice that this is much different from the exact numbers provided by a quantitative assessment that uses monetary figures. You can think of quantitative as using a quantity or a number, whereas qualitative is related to quality, which is often a matter of judgment.

Some qualitative risk assessments use surveys or focus groups. They canvass experts to provide their best judgments and then tabulate the results. For example, a survey may ask the experts to rate the probability and impact of risks associated with a web server selling products on the Internet and a library workstation without Internet access. The experts would use words such as low, medium, and high to rate them.

They could rate the probability of a web server being attacked as high, and if the attack takes the web server out of service, the impact is also high. On the other hand, the probability of a library workstation being attacked is low, and, even though a library patron may be inconvenienced, the impact is also low.

It’s common to assign numbers to these judgments. For example, you can use terms such as low, medium, and high, and assign values of 1, 5, and 10, respectively. The experts assign a probability and impact of each risk using low, medium, and high, and when tabulating the results, you change the words to numbers. This makes it a little easier to calculate the results.

In the web server and library computer examples, you can calculate the risk by multiplying the probability and the impact:

- **Web server.** High probability and high impact: 10 × 10 = 100
- **Library computer.** Low probability and low impact: 1 × 1 = 1

Management can look at these numbers and easily determine how to allocate resources to protect against the risks. They would allocate more resources to protect the web server than the library computer.

One of the challenges with a qualitative risk assessment is gaining consensus on the probability and impact. Unlike monetary values that you can validate with facts, probability and impact are often subject to debate.

Documenting the Assessment

The final phase of the risk assessment is the report. This identifies the risks discovered during the assessment and the recommended controls. As a simple example, a risk assessment on a database-enabled web application may discover that it's susceptible to SQL injection attacks. The risk assessment will then recommend rewriting the web application with input validation techniques or stored procedures to protect the database.

Management uses this to decide which controls to implement and which controls to accept. In many cases, a final report documents the managerial decisions. Of course, management can decide not to implement a control, but instead accept a risk.

Think how valuable this report will be for an attacker. They won't need to dig to identify vulnerabilities or controls. Instead, the report lists all the details. Even when management approves controls to correct the vulnerabilities, it may take some time to implement them. Because of this, the results of a risk assessment are highly protected. Normally, only executive management and security professionals will have access to these reports.

Risk Registers

Some risk assessments use a ***risk register***. There are different definitions for a risk register, depending on which standard you're following. For example, ISO 73:2009 defines it as a "record of information about identified risks." Projects IN Controlled Environments (PRINCE2), a detailed project management method, defines a risk register as a "repository for all risks identified and includes additional information about each risk."

An easy way to create a risk register is in a table format. As an example, imagine you are evaluating risks related to a new e-commerce web site that accesses a back-end database. Your risk register might include the following columns:

- **Category.** Risk categories could include downtime due to hardware failures, outages from an attack, downtime to database server failure, data breaches, and more.
- **Specific risk.** One of the risks related to hardware failures could be hard drive failure. Of course, there are other potential hardware failures, but the remaining columns for this risk will focus on hard drive failure. For this example, imagine that one drive holds the operating system and applications. A second drive holds data.
- **Likelihood of occurrence.** Medium. This assumes that the installed hard drives are not currently using a redundant array of inexpensive disks (RAID) disk subsystem.
- **Impact.** High. If a hard drive fails, it will probably disable the entire web site.
- **Risk score.** 50 (out of 100). This assumes a score of Medium has a value of 5 and a score of High has a value of 10 (5 × 10 = 50). Note that organizations can assign any desired values to the likelihood of occurrence and impact. The values used here are simply an example.
- **Security controls or mitigation steps.** Implement a RAID-1 to protect the hard drive hosting the operating system. Implement a RAID-6 to protect the data.
- **Contingencies.** Ensure backups exist and are kept up to date.
- **Risk score with security controls.** 10 (out of 100). With the RAID-1 and RAID-6 in place, the likelihood of occurrence is now Low, but the impact remains High. The new score assumes a score of Low has a value of 1 and a score of High has a value of 10 (1 × 10 = 10).
- **Action assigned to.** A risk register may document who has responsibility for implementing the security control.
- **Action deadline.** The deadline identifies when the security control should be implemented.

Organizations might use columns such as these or modify them as they see fit. The key is that the risk register documents relevant risks based on the needs of the organization.

Supply Chain Assessment

A supply chain includes all the elements required to produce and sell a product. As a simple example, consider the Lard Lad Donuts store. They require a steady supply of flour, sugar, eggs, milk, oil, and other ingredients. They also require equipment such as refrigerators to store raw materials, space to manufacture the donuts, and fryers to cook them. Last, they need a method to sell the donuts to customers. If any of these items fail, the company won't be able to make and sell donuts.

It's important to realize that the supply chain isn't only the supply of raw materials. It also includes all the processes required to create and distribute a finished product.

A ***supply chain assessment*** evaluates these elements—the raw materials supply sources and all the processes required to create, sell, and distribute the product. In some cases, the assessment focuses on identifying risks. For example, are there any raw materials that come from only a single source? It would also examine processes and identify any tasks or steps that represent a single point of failure. If the donut store has only one fryer, it is a single point of failure. If it breaks, all sales stop.

Many organizations have mature supply chains. In other words, they have multiple sources in place for all raw materials. The failure of any single supply source will not affect the organization's ability to create and sell its products. Similarly, they have built-in redundancies in their processes. If any internal processes fail, they have alternative methods ready to implement and keep the organization operating.

Organizations with mature supply chains still perform supply chain assessments. The goal of these assessments is to look for methods to improve the supply chain.

Remember this

A risk register is a comprehensive document listing known information about risks. It typically includes risk scores along with recommended security controls to reduce the risk scores. A supply chain assessment evaluates everything needed to produce and sell a product. It includes all the raw materials and processes required to create and distribute a finished product.

Comparing Scanning and Testing Tools

Security administrators use tools to test their networks. Two common categories of tools are vulnerability scanners, which check for weaknesses and penetration tests, which attempt to exploit the vulnerabilities. This section covers vulnerability scanners and penetration tests in more depth.

Checking for Vulnerabilities

Vulnerabilities are weaknesses, and by reducing vulnerabilities, you can reduce risks. That sounds simple enough. However, how do you identify the vulnerabilities that present the greatest risks? Common methods are vulnerability assessments and various scans such as network scans and vulnerability scans.

The overall goal of a vulnerability assessment is to assess the security posture of systems and networks. They identify vulnerabilities, or weaknesses, within systems, networks, and organizations, and are part of an overall risk management plan.

Vulnerability assessments can include information from a wide variety of sources. This includes reviewing security policies and logs, interviewing personnel, and testing systems. Assessments often use a variety of scans and penetration tests, all discussed in this section. A vulnerability assessment typically includes the following high-level steps:

- Identify assets and capabilities.
- Prioritize assets based on value.
- Identify vulnerabilities and prioritize them.
- Recommend controls to mitigate serious vulnerabilities.

Many organizations perform vulnerability assessments internally. Organizations also hire external security professionals to complete external assessments. The following sections discuss many of the common tools used for vulnerability assessments and vulnerability scans.

Password Crackers

A ***password cracker*** attempts to discover a password. Passwords are typically encrypted or hashed so that they aren't easily readable. Chapter 10, "Understanding Cryptography and PKI," covers both encryption and hashing methods. Some methods are stronger than others. If passwords are protected with weak methods, a password cracker can discover the password.

As an example, Message Digest 5 (MD5) is a hashing algorithm. When executed against a passwordofP@ssw0rd, it creates the following MD5hash:161ebd7d45089b3446ee4e0d86dbcf92. A password cracker can analyze the MD5 hash of 161ebd7d45089b3446ee4e0d86dbcf92 and discover the actual password of P@ssw0rd. Chapter 7, "Protecting Against Advanced Attacks," discusses many of the common methods used to crack passwords. The point here is that password crackers are one of the tools security administrators use during a vulnerability assessment.

There are two categories of password crackers—offline and online:

- An offline password cracker attempts to discover passwords by analyzing a database or file containing passwords. For example, attackers often obtain large volumes of data during a data breach. This includes files that include hashed or encrypted passwords. They can then analyze the protected passwords to discover the actual passwords. A key benefit of an offline password cracking attack is that attackers have unlimited time to analyze the passwords.
- An online password cracker attempts to discover passwords by guessing them in a brute force attack. For example, some online password crackers attempt to discover the passwords for specific accounts by trying to log on to the accounts remotely. Other online password crackers collect network traffic and attempt to crack any passwords sent over the network.

Network Scanners

A ***network scanner*** uses various techniques to gather information about hosts within a network. As an example, Nmap (covered in more depth later in this chapter) is a popular network scanning tool that can give you a lot of information about hosts within a network. Other popular network scanning tools are Netcat and Nessus. Network scanners typically use the following methods:

- **Ping scan.** A ping scan (sometimes called a ping sweep) sends an

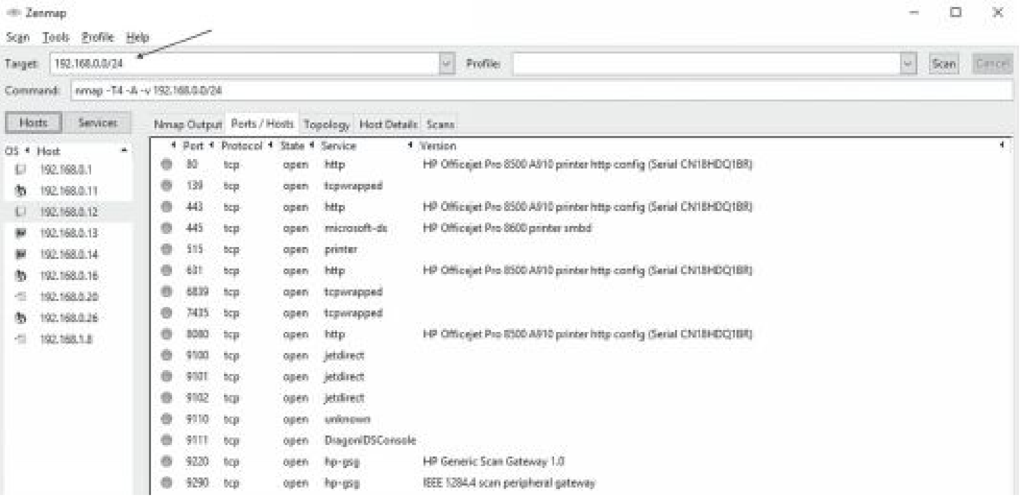
Internet Control Message Protocol (ICMP) ping to a range of IP addresses in a network. If the host responds, the network scanner knows there is a host operational with that IP address. A problem with ping scans is that firewalls often block ICMP, so it can give inconsistent results.

- **Arp ping scan.** Chapter 1, "Mastering Security Basics," discusses the Address Resolution Protocol (ARP) and how systems use it to resolve IP addresses to media access control (MAC) addresses. Any host that receives an ARP packet with its IP address responds with its MAC address. If the host responds, the network scanner knows that a host is operational with that IP address.
- **Syn stealth scan.** Chapter 3, "Exploring Network Technologies and Tools," discusses the Transmission Control Protocol (TCP) three-way handshake. As a reminder, one host sends out a SYN (synchronize) packet to initiate a TCP session. The other host responds with a SYN/ACK (synchronize/acknowledge) packet. The first host then completes the handshake with an ACK packet to establish the connection. A syn stealth scan sends a single SYN packet to each IP address in the scan range. If a host responds, the scanner knows that a host is operational with that IP address. However, instead of responding with an ACK packet, a scanner typically sends an RST (reset) response to close the connection.
- **Port scan.** A port scan checks for open ports on a system. Each open port indicates the underlying protocol is running on the system. For example, if port 80 is open, it indicates the host is running HTTP and it is likely running a web server. A port scan typically uses the ports identified as well-known ports by the Internet Assigned Numbers Authority (IANA).
- **Service scan.** A service scan is like a port scan, but it goes a step further. A port scan identifies open ports and gives hints about what protocols or services might be running. The service scan verifies the protocol or service. For example, if a port scan identifies port 80 is open, a service scan will send an HTTP command, such as "Get /." If HTTP is running on port 80, it will respond to the Get command providing verification that it is a web server.

- **OS detection.** Operating system (OS) detection techniques analyze packets from an IP address to identify the OS. This is often referred to as

TCP/IP fingerprinting. As a simple example, the TCP window size (the size of the receive window in the first packet of a TCP session) is not fixed. Different operating systems use different sizes. Some Linux versions use a size of 5,840 bytes, Cisco routers use a size of 4,128 bytes, and some different Windows versions use sizes of 8,192 and 65,535. OS detection techniques don't rely on a single value but typically evaluate multiple values included in responses from systems.

Figure 8.1 shows the result of a scan using Zenmap (the graphical version of Nmap). After starting it, I entered 192.168.0.0/24 as the Target. Nmap then scanned all the IP addresses from 192.168.0.1 to 192.168.0.254. After the scan completed, I selected the host with the IP address of 192.168.0.12 and selected the Ports/Hosts tab. Nmap discovered that this is a printer, the name and serial number of the printer, and that the printer is hosting an embedded web site running on port 80.



Target: 192.168.0.0/24

Command: nmap -T4 -A -v 192.168.0.0/24

OS	Host
	192.168.0.1
	192.168.0.11
	192.168.0.12
	192.168.0.13
	192.168.0.14
	192.168.0.16
	192.168.0.20
	192.168.0.26
	192.168.1.8

Port	Protocol	State	Service	Version
80	tcp	open	http	HP Officejet Pro 8500 A910 printer http config (Serial CN18HDQ1BR)
139	tcp	open	tcpwrapped	
443	tcp	open	http	HP Officejet Pro 8500 A910 printer http config (Serial CN18HDQ1BR)
445	tcp	open	microsoft-ds	HP Officejet Pro 8600 printer smbd
515	tcp	open	printer	
631	tcp	open	http	HP Officejet Pro 8500 A910 printer http config (Serial CN18HDQ1BR)
6839	tcp	open	tcpwrapped	
7435	tcp	open	tcpwrapped	
8080	tcp	open	http	HP Officejet Pro 8500 A910 printer http config (Serial CN18HDQ1BR)
9100	tcp	open	jetdirect	
9101	tcp	open	jetdirect	
9102	tcp	open	jetdirect	
9110	tcp	open	unknown	
9111	tcp	open	DragonIDSConsole	
9220	tcp	open	hp-gsg	HP Generic Scan Gateway 1.0
9290	tcp	open	hp-gsg	IEEE 1284.4 scan peripheral gateway

Figure 8.1: Zenmap scan

Remember this

Password crackers attempt to discover passwords and can identify weak passwords, or poorly protected passwords. Network scanners can detect all the hosts on a network, including the operating system and services or protocols running on each host.

Network Mapping

Network mapping discovers devices on the network and how they are connected with each other. It is often done as part of a network scan, but it only focuses on connectivity. In contrast, a full network scan also includes additional scans to identify open ports, running services, and OS details.

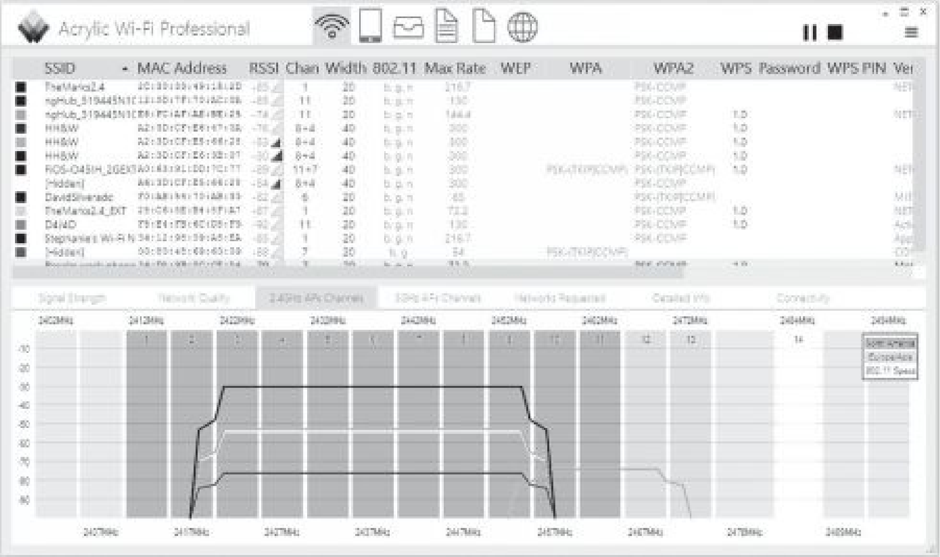
Some tools, such as Zenmap, provide you with a graphical representation of the network. To see how this looks, look at the Nmap and Zenmap labs available at http://gcgapremium.com/501labs/.

Wireless Scanners/Cracker

Chapter 4, “Securing Your Network,” discusses how administrators often perform site surveys while planning and deploying a wireless network. Security personnel periodically repeat the site survey to verify the environment hasn’t changed.

Wireless scanners can typically use both passive and active scans. When using a passive scan, a scanner just listens to all the traffic being broadcast on known channels within the 2.4 GHz and 5 GHz frequency ranges.

Figure 8.2 shows a screenshot from Acrylic Wi-Fi Professional, a wireless scanner with many capabilities. As with many scanners, it can collect and report quite a bit of information on local APs.



SSID	MAC Address	RSSI	Chan	Width	802.11	Max Rate	WEP	WPA	WPA2	WPS	Password	WPS PIN	Ver
TheMarks2.4	[illegible]	-65	1	20	b, g, n	216.7			PSK-CCMP				NET
ngHub_319445N1C	[illegible]	-85	11	20	b, g, n	130			PSK-CCMP				
ngHub_319445N1C	[illegible]	-74	11	20	b, g, n	144.4			PSK-CCMP	1.0			NET
HH&W	[illegible]	-76	8+4	40	b, g, n	300			PSK-CCMP	1.0			
HH&W	[illegible]	-53	8+4	40	b, g, n	300			PSK-CCMP	1.0			
HH&W	[illegible]	-30	8+4	40	b, g, n	300			PSK-CCMP	1.0			
FiOS-O45IH_2GEXT	[illegible]	-29	11+7	40	b, g, n	300		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			NET
[Hidden]	[illegible]	-54	8+4	40	b, g, n	300			PSK-CCMP				
DavidSilverado	[illegible]	-62	6	20	b, g, n	65			PSK-(TKIP|CCMP)				MI
TheMarks2.4_EXT	[illegible]	-87	1	20	b, g, n	72.2			PSK-CCMP	1.0			NET
D4AD	[illegible]	-92	11	20	b, g, n	130			PSK-CCMP	1.0			Acti
Stephanie's Wi-Fi N	[illegible]	-85	1	20	b, g, n	216.7			PSK-CCMP				Appl
[Hidden]	[illegible]	-88	7	20	b, g	54		PSK-(TKIP|CCMP)					CO

Figure 8.2: Acrylic Wi-Fi Professional

The following bullets describe some of the columns in Figure 8.2:

- **SSIDs.** A scanner will detect the service set identifier (***SSID***) of all access points within range of the scanner.
- **MAC addresses.** It shows the MAC, or hardware address of the AP.

- **Signal strength.** The signal strength typically identifies how near (or how far away) the AP is in relation to the computer performing the scan.
- **Channels.** This helps administrators determine if nearby APs are broadcasting on the same channel, causing interference.
- **Channel widths.** A channel is typically 20 MHz wide, but when an AP is using two channels, it is 40 MHz. The scanner will show this information.
- **Security.** The scanner will show if the AP is in Open mode or using one of the other wireless cryptographic protocols: Wi-Fi Protected Access (***WPA***) or Wi-Fi Protected Access II (***WPA2***). Chapter 4 discusses these modes in more depth.

When using an active scan, a wireless scanner acts like a scanner/cracker and can gain more information about an AP by sending queries to it. As an example, Chapter 4 discusses various attacks, including Wi-Fi Protected Setup (***WPS***) attacks. A WPS attack keeps guessing PINs until it discovers the eight-digit PIN used by an AP. It can then use this to discover the pre-shared key (PSK) used by the AP. Various wireless scanners have other capabilities, including password crackers using other methods.

Rogue System Detection

Chapter 4 discusses rogue APs, which are APs placed into service without authorization. As long as an administrator knows what APs are authorized, it’s easy to discover rogue APs with a wireless scan. Administrators often perform site surveys while planning and deploying a wireless network. As an example, Figure 8.2 (the screenshot from Acrylic Wi-Fi Professional in the previous section) shows all the SSIDs it has detected.

Administrators can investigate any unknown SSIDs. The received signal strength indicator (RSSI) shows the strength of the signal. A lower negative number (closer to zero) is stronger than a higher negative number. By installing the wireless scanner on a laptop and walking around an organization, you can locate rogue APs. As you move closer to a rogue AP, the signal becomes stronger. As you move farther away from it, the signal becomes weaker.

Banner Grabbing

Banner grabbing is a technique used to gain information about remote systems and many network scanners use it. It is often used to identify the operating system along with information about some applications. If successful, the server returns a Hypertext Markup Language (HTML) banner providing information on the server. The banner might look something like the following:

```
<!DOCTYPE HTML PUBLIC“-//IETF//DTD HTML 2.0//EN”>
<html><head><title>501 Method Not Implemented</title></head>
<body>
<h1>Method Not Implemented</h1>
<p>GET to /index.html not supported.<br /></p>
<p>Additionally, a 404 Not Found error was encountered.</p><hr>
  <address>Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.0-fips
mod_auth_ passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
Server at 72.52.230.233 Port 80
  </ address>
</body></html>
```

Most of this is formatting. However, the information in the address section provides a lot of information on the web server. It shows this is a Unix server running the Apache web server software along with additional information. The command-line tool Netcat can be used for banner grabbing, as shown later in this chapter. You can also check out the Banner Grabbing Lab in the online exercises for this book at *http://gcgapremium.com/501labs/.*

Remember this

Wireless scanners can detect rogue access points on a network and sometimes crack passwords used by access points. Netcat can be used for banner grabbing to identify the operating system and some applications and services on remote servers.

Vulnerability Scanning

A key part of a vulnerability assessment is a vulnerability scan. Security administrators often use a ***vulnerability scanner*** to identify which systems are susceptible to attacks. Vulnerability scanners identify a wide range of weaknesses and known security issues that attackers can exploit. Most vulnerability scanners combine multiple features into a single package. A vulnerability scan often includes the following actions:

- Identify vulnerabilities
- Identify misconfigurations
- Passively test security controls
- Identify lack of security controls

Identifying Vulnerabilities and Misconfigurations

Vulnerability scanners utilize a database or dictionary of known vulnerabilities and test systems against this database. For example, the MITRE Corporation maintains the Common Vulnerabilities and Exposures (CVE) list, which is a dictionary of publicly known security vulnerabilities and exposures. This is similar to how antivirus software detects malware using virus signatures. The difference is that the CVE is one public list funded by the U.S. government, whereas antivirus vendors maintain proprietary signature files.

Other standards used by vulnerability scanners include the Security Content Automation Protocol (SCAP). SCAP utilizes the National Vulnerability Database (NVD), which includes lists of common misconfigurations, security-related software flaws, and impact ratings or risk scores. The risk scores quantify risks, allowing security experts to prioritize vulnerabilities. The SCAP also includes risk scores for items in the CVE.

Additionally, attackers often look for systems that are misconfigured and vulnerability scanners can detect some common misconfiguration settings. Some of the vulnerabilities and common misconfigurations discovered by a vulnerability scanner include:

- **Open ports.** Open ports can signal a vulnerability, especially if administrators aren’t actively managing the services associated with these ports. For example, all web servers do not use File Transfer Protocol (FTP), so if TCP ports 20 and 21 are open, it indicates a potential vulnerability related to FTP. Similarly, Telnet uses port 23, so if this port is open, an attacker can try to connect to the server using Telnet.
- **Weak passwords.** Many scanners include a password cracker that can discover weak passwords or verify that users are creating strong passwords in compliance with an organization’s policy. It is more efficient to use a technical password policy to require and enforce the use of strong passwords. However, if this isn’t possible, administrators use a separate password cracker to discover weak passwords.

- **Default accounts and passwords.** Operating systems and applications can have default usernames and passwords. Basic operating system and application hardening steps should remove the defaults, and a scan can discover the weaknesses if operating systems and applications aren't secured properly. For example, some SQL database systems allow the sa (system administrator) account to be enabled with a blank password. Scanners such as Nessus will detect this.
- **Sensitive data.** Some scanners include data loss prevention (DLP) techniques to detect sensitive data sent over the network. For example, a DLP system can scan data looking for patterns such as Social Security numbers or key words that identify classified or proprietary data.
- **Security and configuration errors.** Vulnerability scans can also check the system against a configuration or security baseline to identify unauthorized changes.

Administrators can scan specific systems or an entire network. For example, many organizations perform periodic scans on the entire network to detect vulnerabilities. If an administrator makes an unauthorized change resulting in a vulnerability, the scan can detect it. Similarly, if a rebuilt system is missing some key security settings, the scan will detect them. It's also possible to scan a new system before or right after it's deployed.

Passively Testing Security Controls

An important point about a vulnerability scan is that it does not attempt to exploit any vulnerabilities. Instead, a vulnerability scan is a passive attempt to identify weaknesses. This ensures that the testing does not interfere with normal operations. Security administrators then assess the vulnerabilities to determine which ones to mitigate. In contrast, a penetration test (covered later in this chapter) is an active test that attempts to exploit vulnerabilities.

Identifying Lack of Security Controls

Vulnerability scanners can also identify missing security controls, such as the lack of up-to- date patches or the lack of antivirus software. Although many patch management tools include the ability to verify systems are up to date with current patches, vulnerability scanners provide an additional check to detect unpatched systems.

Remember this

A vulnerability scanner can identify vulnerabilities, misconfigured systems, and the lack of security controls such as up-to-date patches. Vulnerability scans are passive and have little impact on a system during a test. In contrast, a penetration test is intrusive and can potentially compromise a system.

False Positive

Unfortunately, vulnerability scanners aren't perfect. Occasionally, they report a vulnerability when it doesn't actually exist. In other words, the scan indicates a system has a known vulnerability, but the report is false. As an example, a vulnerability scan on a server might report that the server is missing patches related to a database application, but the server doesn't have a database application installed.

This is similar to false positives in an intrusion detection system (IDS) where the IDS alerts on an event, but the event isn't an actual intrusion. Similarly, an antivirus scanner can identify a useful application as malware, even though the application does not have any malicious code. False positives can result in higher administrative overhead because administrators have to investigate them.

Credentialed Versus Non-Credentialed

Vulnerability scanners can run as a credentialed scan using the credentials of an account, or as non-credentialed without any user credentials. Attackers typically do not have credentials of an internal account, so when they run scans against systems, they run non-credentialed scans.

Security administrators often run credentialed scans with the privileges of an administrator account. This allows the scan to check security issues at a much deeper level than a non- credentialed scan. Additionally, because the credentialed scan has easier access to internal workings of systems, it results in a lower impact on the tested systems, along with more accurate test results and fewer false positives.

It's worth mentioning that attackers typically start without any credentials but use privilege escalation techniques to gain administrative access. This allows them to run a credentialed scan against a network if desired. Similarly, even though a credentialed scan is typically more accurate, administrators often run non-credentialed scans to see what an attacker without credentials would see.

Remember this

A false positive from a vulnerability scan indicates the scan detected a vulnerability, but the vulnerability doesn't exist. Credentialed scans run under the context of a valid account and are typically more accurate than non-credentialed scans.

Configuration Compliance Scanner

A ***configuration compliance scanner*** verifies that systems are configured correctly. They will often use a file that identifies the proper configuration for systems. When running the scan, the scanner will verify that systems have the same configuration defined in the configuration file. This is also known as configuration validation. Security administrators often configure these tools to use automation or scripting methods so that they automatically run on a set schedule.

As an example, Nessus, a vulnerability scanner developed by Tenable Network Security, uses plug-ins to perform configuration compliance scans. They currently have plug-ins used to perform against both Windows and Unix systems. Administrators can also create custom audit files to perform custom compliance configuration scans on Windows and Unix systems. AutoNessus is a free tool that can be used to automate Nessus scans.

Configuration compliance scans typically need to be run as credentialed scans. This helps ensure they can accurately read the configuration of systems during the scan.

Obtaining Authorization

It's important to obtain vulnerability testing authorization and penetration testing authorization before performing any vulnerability testing or penetration testing. In most cases, this consent is in writing. If it isn't in writing, many security professionals won't perform the test. A penetration test without consent is an attack. An organization may perceive a well-meaning administrator doing an unauthorized penetration test as a black hat or gray hat attacker. The administrator might be updating his résumé after running an unauthorized scan or penetration test.

Many organizations use a written rules-of-engagement document when hiring outside security professionals to perform the test. The rules-of-engagement document identifies the boundaries of the penetration test. If testing does result in an outage even though the testers followed the rules of engagement, repercussions are less likely.

Penetration Testing

Penetration testing actively assesses deployed security controls within a system or network. It starts with passive reconnaissance, such as a vulnerability scan, but takes it a step further and tries to exploit vulnerabilities by simulating or performing an attack.

Security testers typically perform a penetration test to demonstrate the actual security vulnerabilities within a system. This can help the organization determine the impact of a threat against a system. In other words, it helps an organization determine the extent of damage that an attacker could inflict by exploiting a vulnerability.

Although it’s not as common, it’s also possible to perform a penetration test to determine how an organization will respond to a compromised system. This allows an organization to demonstrate security vulnerabilities and flaws in policy implementation. For example, many organizations may have perfect policies on paper. However, if employees aren’t consistently following the policies, a penetration test can accurately demonstrate the flaws.

Because a penetration test can exploit vulnerabilities, it has the potential to disrupt actual operations and cause system instability. Because of this, it’s important to strictly define boundaries for a test. Ideally, the penetration test will stop right before performing an exploit that can cause damage or result in an outage. However, some tests cause unexpected results.

Testers sometimes perform penetration tests on test systems rather than the live production systems. For example, an organization may be hosting a web application accessible on the Internet. Instead of performing the test on the live server and affecting customers, penetration testers or administrators configure another server with the same web application. If a penetration test cripples the test server, it accurately demonstrates security vulnerabilities, but it doesn't affect customers.

Many penetration tests include the following activities:

- Passive reconnaissance
- Active reconnaissance
- Initial exploitation
- Escalation of privilege
- Pivot
- Persistence

Remember this

A penetration test is an active test that can assess deployed security controls and determine the impact of a threat. It starts with a vulnerability scan and then tries to exploit vulnerabilities by actually attacking or simulating an attack.

Passive Reconnaissance

Passive reconnaissance collects information about a targeted system, network, or organization using open-source intelligence. This includes viewing social media sources about the target, news reports, and even the organization's web site. If the organization has wireless networks, it could include passively collecting information from the network such as network SSIDs. Note that because passive reconnaissance doesn't engage a target, it isn't illegal.

Passive reconnaissance does not include using any tools to send information to targets and analyze the responses. However, passive reconnaissance can include using tools to gather information from systems other than the target. For example, you can sometimes gain information about a domain name holder using the Whois lookup site (*https://www.whois.com*). Other times, you can gain information by querying Domain Name System (DNS) servers.

Active Reconnaissance

Active reconnaissance includes using tools to send data to systems and analyzing the responses. It typically starts by using various scanning tools such as network scanners and vulnerability scanners. It's important to realize that active reconnaissance does engage targets and is almost always illegal. It should never be started without first getting explicit authorization to do so.

The "Network Scanners" section earlier in this chapter discussed how tools such as Nmap and Nessus can gather a significant amount of information about networks and individual systems. This includes identifying all IP addresses active in a network, the ports and services active on individual systems, and the operating system running on individual systems.

Remember this

Penetration tests include both passive and active reconnaissance. Passive reconnaissance uses open-source intelligence methods, such as social media and an organization's web site. Active reconnaissance methods use tools such as network scanners to gain information on the target.

Initial Exploitation

After scanning the target, testers discover vulnerabilities. They then take it a step further and look for a vulnerability that they can exploit. For example, a vulnerability scan may discover that a system doesn't have a patch installed for a known vulnerability. The vulnerability allows attackers (and testers) to remotely access the system and install malware on it.

With this knowledge, the testers can use known methods to exploit this vulnerability. This gives the testers full access to the system. They can then install additional software on the exploited system.

Escalation of Privilege

In many penetration tests, the tester first gains access to a low-level system or low-level account. For example, a tester might gain access to Homer's computer using Homer's user account. Homer has access to the network, but doesn't have any administrative privileges. However, testers use various techniques to gain more and more privileges on Homer's computer and his network.

Chapter 6 discusses privilege escalation tactics that attackers often use. The "One Click Lets Them In" section discusses how advanced persistent threats (APTs) often use remote access Trojans (RATs) to gain access to a single system. Attackers trick a user into clicking a malicious link, which gives them access to a single computer. Attackers then use various scripts to scan the network looking for vulnerabilities. By exploiting these vulnerabilities, the attackers gain more and more privileges on the network.

Penetration testers typically use similar tactics. Depending on how much they are authorized to do, testers can use other methods to gain more and more access to a network.

Pivot

Pivoting is the process of using various tools to gain additional information. For example, imagine a tester gains access to Homer's computer within a company's network. The tester can then ***pivot*** and use Homer's computer to gather information on other computers. Homer might have access to network shares filled with files on nuclear power plant operations. The tester can use Homer's computer to collect this data and then send it back out of the network from Homer's computer.

Testers (and attackers) can use pivoting techniques to gather a wide variety of information. Many times, the tester must first use escalation of privilege techniques to gain more privileges. However, after doing so, it's possible that the tester can access databases (such as user accounts and password databases), email, and any other type of data stored within a network.

Remember this

After exploiting a system, penetration testers use privilege escalation techniques to gain more access to target systems. Pivoting is the process of using an exploited system to target other systems.

Persistence

Attackers often use various threats that allow them to stay within a network for weeks, months, or even years without being detected. Penetration testing techniques use similar techniques to maintain persistence within the network.

A common technique used to maintain persistence is to create a backdoor back into the network. For example, a tester may be able to create alternate accounts that can be accessed remotely. In some cases, it's also possible to install or modify services to connect back into a system. For example, a tester may be able to enable Secure Shell (SSH) and then create a method used to log on to a system using SSH.

White, Gray, and Black Box Testing

It’s common to identify testing based on the level of knowledge the testers have prior to starting the test. These testers could be internal employees or external security professionals working for a third-party organization hired to perform the test. The three types of testing are:

- **Black box testing.** Testers have zero knowledge of the environment prior to starting a ***black box test***. Instead, they approach the test with the same knowledge as an attacker. When testing new applications, black box testers wouldn’t have any prior experience with the application. When testing networks, they aren’t provided any information or documentation on the network before the test. Black box testers often use fuzzing to check for application vulnerabilities.
- **White box testing.** Testers have full knowledge of the environment before starting a ***white box test***. For example, they would have access to product documentation, source code, and possibly even logon details.
- **Gray box testing.** Testers have some knowledge of the environment prior to starting a ***gray box test***. For example, they might have access to some network documentation, but not know the full network layout.

Remember this

Black box testers have zero prior knowledge of the system prior to a penetration test. White box testers have full knowledge, and gray box testers have some knowledge. Black box testers often use fuzzing.

You may also come across the terms black hat, white hat, and gray hat. These aren’t referring to testers but instead to different types of attackers. They are reminiscent of the Wild West, where you could easily identify the good guys and the bad guys by the color of their hat. Black hat identifies a malicious attacker performing criminal activities. White hat identifies a security professional working within the law. Gray hat identifies individuals who may have good intentions, but their activities may cross ethical lines. For example, an activist, sometimes called a hacktivist, may use attack methods to further a cause, but not for personal gain.

Hackers and crackers are terms you may also come across. Originally, a hacker indicated someone proficient with computers who wanted to share knowledge with others. They weren’t malicious. In contrast, a cracker was a proficient hacker who used the knowledge for malicious purposes. However, English is a living language that continues to evolve and the media consistently uses the term hacker to identify malicious attackers. This book often uses the term attacker to identify an individual attacking a system for malicious purposes.

Intrusive Versus Non-Intrusive Testing

Scans can be either intrusive or non-intrusive. You can also think of these terms as invasive and non-invasive, respectively. Tools using intrusive methods can potentially disrupt the operations of a system. In contrast, tools using non-intrusive methods will not compromise a system. These terms also apply to penetration testing (intrusive) and vulnerability scanning (non-intrusive).

When comparing penetration testing and vulnerability scanning, it’s important to remember that penetration tests are intrusive and more invasive than vulnerability scans. They involve probing a system and attempting to exploit any vulnerabilities they discover. If they successfully exploit a vulnerability, a penetration test can potentially disrupt services and even take a system down.

Vulnerability scans are generally non-intrusive and less invasive than penetration tests. They never attempt to exploit a vulnerability. Because of this, a vulnerability scan is much safer to run on a system or network because it is significantly less likely that it will affect services.

Passive Versus Active Tools

In the context of tools used to discover security threats and vulnerabilities, it’s important to understand the difference between passive tools and active tools. A passive tool tests systems in a non-intrusive manner and has little possibility of compromising a system. An active tool uses intrusive and invasive methods and can potentially affect the operations of a system.

The “Vulnerability Scanning” section earlier in this chapter mentioned that vulnerability scanning is passive, and penetration testing is active. In this context, passive doesn’t mean that a vulnerability scanner isn’t doing anything. It certainly is probing systems to identify vulnerabilities and other problems. However, it does not take any action to exploit these vulnerabilities.

That doesn’t mean that you can feel free to run a vulnerability scanner on any network simply because it is passive and non-intrusive. If your actions are discovered, you might be identified as an attacker and face legal action.

Remember this

A vulnerability scanner is passive and non-intrusive and has little impact on a system during a test. In contrast, a penetration test is active and intrusive, and can potentially compromise a system. A penetration test is more invasive than a vulnerability scan.

Exploitation Frameworks

An exploitation framework is a tool used to store information about security vulnerabilities. It is often used by penetration testers (and attackers) to detect and exploit software. ***Exploitation frameworks*** typically include tools used to check for vulnerabilities and execute exploits on any discovered vulnerabilities. Chapter 4 discusses intrusion detection systems (IDSs) and many IDSs use information from an existing framework to detect attacks. Some commonly used exploitation frameworks are:

- **Metasploit Framework.** Metasploit is an open source project that runs on Linux systems. It has data on over 1,600 exploits and includes methods to develop, test, and use exploit code. Rapid7 acquired Metasploit in 2009. While the framework is still free and open source, there are more advanced editions available for purchase.
- **BeEF (Browser Exploitation Framework).** BeEF is an open source web browser exploitation framework. It focuses on identifying web browser vulnerabilities. Successful attacks allow testers (and attackers) to launch attacks from within an exploited web browser.

- **w3af (Web Application Attack and Audit Framework).** This open source framework focuses on web application vulnerabilities. The stated goal is to find and exploit all web application vulnerabilities and make this information known to others. Web application developers can then ensure their web applications are not vulnerable to the exploits.

Using Security Tools

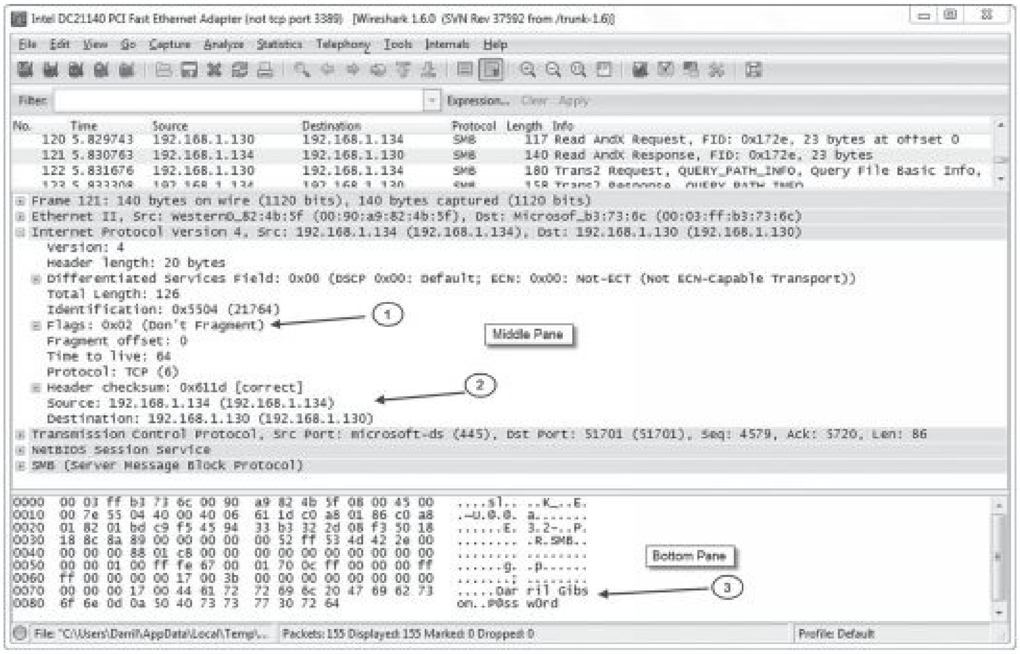
Several tools are available for use by security professionals and attackers alike. Vulnerability scanners were discussed at length earlier in this chapter, including their use as ping scanners and port scanners. However, other tools are available. This section discusses tools such as protocol analyzers, command-line tools, logs, and audits.

Sniffing with a Protocol Analyzer

A ***protocol analyzer*** can capture and analyze packets on a network. The process of using a protocol analyzer is sometimes referred to as sniffing or using a sniffer. Both administrators and attackers can use a protocol analyzer to view IP headers and examine packets. For example, administrators can use a protocol analyzer to troubleshoot communication issues between network systems, or identify potential attacks using manipulated or fragmented packets.

Attackers can use a protocol analyzer to capture data sent across a network in cleartext. For example, unencrypted credentials are usernames and passwords sent across a network in cleartext. One of the ways attackers can view this data is by connecting an unauthorized switch within a network to capture traffic and forward it to a system running a protocol analyzer. If cabling isn't protected, they might be able to simply connect a switch above a drop-down ceiling. Wireshark is a free protocol analyzer that you can download from the Wireshark site: *http://www.wireshark.org/.*

Figure 8.3 shows Wireshark after it captured packets transmitted over the network. It includes about 150 packets and has packet 121 selected in the top pane. The top pane shows the source and destination IP addresses and the Server Message Block (SMB) protocol. Many networks use SMB to send files over the network, and this packet includes the contents of that file. The middle pane shows details from this packet with the Internet Protocol version 4 header information partially expanded. The bottom pane shows the entire contents of the packet (including the unencrypted credentials) displayed in hexadecimal and ASCII characters.


Intel DC21140 PCI Fast Ethernet Adapter (not tcp port 3389) [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
Middle Pane
Bottom Pane
1
2
3

```
No.  Time        Source          Destination     Protocol Length Info
  120 5.829743   192.168.1.130   192.168.1.134   SMB      117 Read AndX Request, FID: 0x172e, 23 bytes at offset 0
  121 5.830763   192.168.1.134   192.168.1.130   SMB      140 Read AndX Response, FID: 0x172e, 23 bytes
  122 5.831676   192.168.1.130   192.168.1.134   SMB      180 Trans2 Request, QUERY_PATH_INFO, Query File Basic Info,
  123 5.833308   192.168.1.134   192.168.1.130   SMB      158 Trans2 Response, QUERY_PATH_INFO
```

```
⊞ Frame 121: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)
⊞ Ethernet II, Src: WesternD_82:4b:5f (00:90:a9:82:4b:5f), Dst: Microsof_b3:73:6c (00:03:ff:b3:73:6c)
⊟ Internet Protocol Version 4, Src: 192.168.1.134 (192.168.1.134), Dst: 192.168.1.130 (192.168.1.130)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 126
    Identification: 0x5504 (21764)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
  ⊞ Header checksum: 0x611d [correct]
    Source: 192.168.1.134 (192.168.1.134)
    Destination: 192.168.1.130 (192.168.1.130)
⊞ Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 51701 (51701), Seq: 4579, Ack: 5720, Len: 86
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
```

```
0000  00 03 ff b3 73 6c 00 90  a9 82 4b 5f 08 00 45 00   ....sl.. ..K_..E.
0010  00 7e 55 04 40 00 40 06  61 1d c0 a8 01 86 c0 a8   .~U.@.@. a.......
0020  01 82 01 bd c9 f5 45 94  33 b3 32 2d 08 f3 50 18   ......E. 3.2-..P.
0030  18 8c 8a 89 00 00 00 00  00 52 ff 53 4d 42 2e 00   ........ .R.SMB..
0040  00 00 00 88 01 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 01 00 ff fe 67 00  01 70 0c ff 00 00 00 ff   ......g. .p......
0060  ff 00 00 00 00 17 00 3b  00 00 00 00 00 00 00 00   .......; ........
0070  00 00 00 17 00 44 61 72  72 69 6c 20 47 69 62 73   .....Dar ril Gibs
0080  6f 6e 0d 0a 50 40 73 73  77 30 72 64               on..P@ss w0rd
```

File: "C:\Users\Darril\AppData\Local\Temp\... Packets: 155 Displayed: 155 Marked: 0 Dropped: 0 Profile: Default

Figure 8.3: Wireshark capture

Although it can be tedious to analyze a packet capture, there is a lot of information in it for anyone willing to take the time to do so. Occasionally, attackers manipulate flags (arrow 1) within the headers for different types of attacks, and the protocol analyzer allows you to verify header manipulation attacks. You can also see the source and destination IP addresses (arrow 2) within the IP header field. You can expand the Ethernet II section to show the media access control (MAC) addresses of the source and destination computers.

Notice that you can view the unencrypted credentials—username (Darril) and password (P@ssw0rd)—in the bottom pane (arrow 3) because SMB sends it in cleartext. However, if an application encrypted the data before sending it across the network, it would not be readable.

Although this packet capture only includes about 150 packets, a packet capture can easily include thousands of packets. Wireshark includes filters that administrators use to focus on specific types of traffic. These filters also allow them to quantify the traffic. For example, they can determine the percentage of SMTP traffic or HTTP traffic on the network.

In addition to seeing a capture using the Wireshark graphical interface, you can also view them as text files. The information in the text file is usually limited using filters, but normally includes the time, source information labeled as src, destination information labeled as dst, and sometimes protocol information. Here's an example:

```
22:33:44, src 192.168.5.55:3389, dst 192.168.7.17:8080,
syn/ack
```

The time is shown in a 24-hour clock as 10:33 p.m. and 44 seconds. Notice the source and destination includes an IP address and a port number. This reiterates the importance of knowing commonly used ports mentioned in Chapter 3. It also shows you how you can identify the source of traffic. For example, if an attacker is manipulating or fragmenting packets as part of an attack, you can use the src IP address to identify the potential source of the attack.

It's worth noting that the source IP address doesn't always identify the actual attacker. For example, attackers often take control of other computers and launch attacks from them without the knowledge of the owner. Similarly, Port Address Translation (PAT) translates public and private IP addresses. If the traffic goes through a device using PAT, the protocol analyzer only captures the translated IP address, not the original IP address.

When using a protocol analyzer, you need to configure the network interface card (NIC) on the system to use promiscuous mode. Normally, a NIC uses non-promiscuous mode and only processes packets addressed directly to its IP address. However, when you put it in promiscuous mode, it processes all packets regardless of the IP address. This allows the protocol analyzer to capture all packets that reach the NIC.

Remember this

Administrators use a protocol analyzer to capture, display, and analyze packets sent over a network. It is useful when troubleshooting communications problems between systems. It is also useful to detect attacks that manipulate or fragment packets. A capture shows information such as the type of traffic (protocol), flags, source and destination IP addresses, and source and destination MAC addresses. The NIC must be configured to use promiscuous mode to capture all traffic.

Command-Line Tools

Chapter 1 introduces some command-line tools available on Windows and Linux systems. Some tools are useful when performing vulnerability scans and penetration tests. Three tools discussed in this section are tcpdump, Nmap, and Netcat.

As with any command-line tools, it's best to dig in and give them a try. I strongly encourage you to check out the free online labs at *http://gcgapremium.com/501labs/* and do each of them.

Tcpdump

Tcpdump is a command-line packet analyzer (or protocol analyzer). It allows you to capture packets like you can with Wireshark (mentioned in the "Sniffing with a Protocol Analyzer" section). The difference is that Wireshark is a Windows-based tool and tcpdump is executed from the command line. Many administrators use tcpdump to capture the packets and later use Wireshark to analyze the packet capture. One of the online labs for this chapter shows how to do this.

Kali Linux includes tcpdump, but you won't find it on Windows systems. As with most Linux command-line tools, tcpdump is case sensitive. You need to enter tcpdump in all lowercase. Additionally, the switches must be entered with the proper case. For example, -c (lowercase c) represents count and indicates the capture should stop after receiving the specified number of packets. However, -C (uppercase C) represents file size and indicates the maximum size (in millions of bytes) of a packet capture. When the file reaches this size, tcpdump closes it and starts storing packets in a new file.

Nmap

Nmap is a network scanner and was discussed earlier in the "Network Scanners" section. The graphical side of Nmap is Zenmap, and Figure 8.1 showed a screenshot from Zenmap. Additionally, online labs show you how to install and use Nmap and Zenmap.

It includes many capabilities, including identifying all the active hosts and their IP addresses in a network, the protocols and services running on each of these hosts, and the operating system of the host. When running the command, you include the scan type(s), optional options, and target specifications. As an example, consider the following command:

```
nmap -T4 -A -v 192.168.0.0/24
```

Notice that it has three switches, -T4, -A, and -v:

- **T4.** T4 refers to the speed of the scan. Valid switches are T0 through T5 with T0 being the slowest and T5 being the fastest. Faster scans are likely to be detected, while slower scans may not be detected.
- **A.** The -A switch indicates the scan should include OS detection, version detection, script scanning, and traceroute.
- **-v.** The -v switch indicates the verbosity level. You can get more data output by using
  -vv or -vvv.

Netcat

Chapter 3 discusses ***Netcat*** and how administrators often use it for remotely accessing Linux systems. It doesn't include native encryption so it's common to use SSH to secure the session. Additionally, the "Banner Grabbing" section earlier in this chapter mentioned that Netcat can easily be used for banner grabbing. The following is a sample command used for banner grabbing:

```
echo “” | nc -vv -n -w1 72.52.206.134 80
```

It uses the netcat command (nc) along with some switches: -vv for a verbose output, -n to not resolve host names, -w1 to wait no more than 1 second for a reply. The command connects to port 80 of the system with an IP address of 72.52.206.134. The echo “” sends a blank command to the server and the pipe symbol (|) tells Netcat to send the command after establishing the connection.

Some other uses of Netcat include:

- **Transferring files.** One of the online labs for Chapter 3 shows how to create a chat session between two systems. Once this session is open, you can use the connection to copy files between the systems.
- **Port scanner.** You can use Netcat to run a port scan against a single IP address. It allows you to specify the range of ports, such as 10 through 1024 and randomize the ports scanned to evade detection. It also supports waiting longer periods of time between port checks, again, to evade detection.

Remember this

Tcpdump is a command-line protocol analyzer. It can create packet captures that can then be viewed in Wireshark. Nmap is a sophisticated network scanner that runs from the command line. Netcat can be used to remotely administer systems and also gather information on remote systems.

Monitoring Logs for Event Anomalies

Logs have the capability to record what happened, when it happened, where it happened, and who did it. One of the primary purposes of logging is to allow someone, such as an administrator or security professional, to identify exactly what happened and when.

Many times, security administrators are searching the logs looking for event anomalies. As a simple example, attackers sometimes try to log on to accounts by guessing passwords. Security logs will record these attempts as failed logons, which is an event anomaly. After investigating the failed logons, administrators can determine if the failed logons were part of normal operation, or a security incident.

It's tempting to set up logging to record every event and provide as much detail as possible—most logs support a verbose mode that will log additional details. However, a limiting factor is the amount of disk space available. Additionally, when logging is enabled, there is an implied responsibility to review the logs. The more you choose to log, the more you may have to review. The goal is to strike a balance between what is needed and the amount of available space for storage. The following sections cover some commonly used logs.

Operating System Event Logs

Operating systems have basic logs that record events. For example, Windows systems have several common logs that record what happened on a Windows computer system. These logs are viewable using the Windows Event Viewer. One of the primary logs in a Windows system is the Security log and it functions as a security log, an audit log, and an access log.

The Security log records auditable events, such as when a user logs on or off, or when a user accesses a resource. Some auditing is enabled by default in some systems, but administrators can add additional auditing. The Security log records audited events as successes or failures. Success indicates an audited event completed successfully, such as a user successfully logging on or successfully deleting a file. Failure indicates that a user tried to perform an action but failed, such as failing to log on or trying to delete a file but receiving a permission error instead. Some additional logs in a Windows system include:

- **Application.** The Application log records events recorded by applications or programs running on the system. Any application has the capability of recording errors in the Application log.
- **System.** The operating system uses the System log to record events related to the functioning of the operating system. This can include when it starts, when it shuts down, information on services starting and stopping, drivers loading or failing, or any other system component event deemed important by the system developers.

If a system is attacked, you may be able to learn details of the attack by reviewing the operating system logs. Depending on the type of attack, any of the operating system logs may be useful.

Firewall and Router Access Logs

You can typically manipulate firewalls and routers to log specific information, such as logging all traffic that the device passes, all traffic that the device blocks, or both. These logs are useful when troubleshooting connectivity issues and when identifying potential intrusions or attacks.

Firewall and router logs include information on where the packet came from (the source) and where it is going (the destination). This includes IP addresses, MAC addresses, and ports.

Linux Logs

The CompTIA Security+ exam includes several Linux-based commands. Understanding this, it’s valuable to know about some common Linux logs. You can view logs using the System Log Viewer on Linux systems or by using the cat command from the terminal. For example, to view the authentication log (auth.log), you can use the following command:

```
cat /var/log/auth.log
```

Some of the Linux logs administrators often look at include:

- **var/log/messages.** This log contains a wide variety of general system messages. It includes some messages logged during startup, some messages related to mail, the kernel, and messages related to authentication. It stores general system activity log entries.
- **var/log/boot.log.** Log entries created when the system boots are contained here.
- **var/log/auth.log.** The authentication log contains information related to successful and unsuccessful logins.
- **var/log/faillog.** This log contains information on failed login attempts. It can be viewed using the faillog command.
- **/var/log/kern.log.** The kernel log contains information logged by the system kernel, which is the central part of the Linux operating system.
- **/var/log/httpd/.** If the system is configured as an Apache web server, you can view access and error logs with this directory.

Some Linux distributions include the utmp, wtmp, and btmp files (or the utmpx, wtmpx, and btmpx variants). They are created so that administrators can answer questions such as who is currently logged in, who has logged in recently, and what accounts have failed login attempts. They are typically within the /var/log folder but might be elsewhere. The following bullets describe these files:

- The utmp file maintains information on the current status of the system, including who is currently logged in. The who command queries this file to display a list of users currently logged in.
- The wtmp file is an archive of the utmp file. Depending on how it is implemented, it can be a circular file, overwriting itself when it reaches a predetermined size. The last command queries this file to show the last logged-in users.
- The btmp file records failed login attempts. The lastb command shows the last failed login attempts.

Other Logs

In addition to the basic operating system logs and firewall and router access logs, administrators use other logs when maintaining systems and networks. These include:

- **Antivirus logs.** Antivirus logs log all antivirus activity, including when scans were run and if any malware was detected. These logs also identify if malware was removed or quarantined.

- **Application logs.** Many server applications include logging capabilities within the application. For example, database applications such as Microsoft SQL Server or Oracle Database include logs to record performance and user activity.
- **Performance logs.** Performance logs can monitor system performance and give an alert when preset performance thresholds are exceeded.

Remember this

Logs record what happened, when it happened, where it happened, and who did it. By monitoring logs, administrators can detect event anomalies. Additionally, by reviewing logs, security personnel can create an audit trail.

SIEM

A security information and event management (***SIEM***) system provides a centralized solution for collecting, analyzing, and managing data from multiple sources. They combine the services of security event management (SEM) and security information management (SIM) solutions. A SEM provides real-time monitoring, analysis, and notification of security events, such as suspected security incidents. A SIM provides long-term storage of data, along with methods of analyzing the data looking for trends, or creating reports needed to verify compliance of laws or regulations.

SIEMs are very useful in large enterprises that have massive amounts of data and activity to monitor. Consider an organization with over 1,000 servers. When an incident occurs on just one of those servers, administrators need to know about it as quickly as possible. The SIEM provides continuous monitoring and provides real-time reporting. For example, in a large network operations center (NOC), the SIEM might display alerts on a large heads-up display. A benefit is that the monitoring and reporting is automated with scripts with the SIEM.

Vendors sell SIEMs as applications that can be installed on systems, and as dedicated hardware appliances. However, no matter how a vendor bundles it, it will typically have common capabilities. This starts with a database that can be easily searched and analyzed. The SIEM collects log data from devices throughout the network and stores these logs in the database.

The following bullets outline some additional capabilities shared by most SIEMs:

- **Aggregation.** Aggregation refers to combining several dissimilar items into a single item. A SIEM can collect data from multiple sources, such as firewalls, intrusion detection systems, proxy servers, and more. Each of these devices formats the logs differently. However, the SIEM can aggregate the data and store it in such a way that it is easy to analyze and search.
- **Correlation engine.** A correlation engine is a software component used to collect and analyze event log data from various systems within the network. It typically aggregates the data looking for common attributes. It then uses advanced analytic tools to detect patterns of potential security events and raises alerts. System administrators can then investigate the alert.
- **Automated alerting.** A SIEM typically comes with predefined alerts, which provide notifications of suspicious events. For example, if it detects a port scan on a server, it might send an email to an administrator group or display the alert on a heads-up display. SIEMs also include the ability to create new alerts.
- **Automated triggers.** Triggers cause an action in response to a predefined number of repeated events. As an example, imagine a trigger for failed logons is set at five. If an attacker repeatedly tries to log on to a server using Secure Shell (SSH), the server’s log will show the failed logon attempts. When the SIEM detects more than five failed SSH logons, it can change the environment and stop the attack. It might modify a firewall to block these SSH logon attempts or send a script to the server to temporarily disable SSH. A SIEM includes the ability to modify predefined triggers and create new ones.
- **Time synchronization.** All servers sending data to the SIEM should be synchronized with the same time. This becomes especially important when investigating an incident so that security investigators know when events occurred. Additionally, large organizations can have locations in different time zones. Each of these locations might have servers sending data to a single centralized SIEM. If the server logs use their local time, the SIEM needs to ensure that it

compensates for the time offset. One method is to convert all times to Greenwich Mean Time (GMT), which is the time at the Royal Observatory in Greenwich, London.

- **Event deduplication.** Deduplication is the process of removing duplicate entries. As an example, imagine 10 users receive the same email and choose to save it. An email server using deduplication processing will keep only one copy of this email, but make it accessible to all 10 users. Imagine a NIDS collects data from a firewall and a SIEM collects data from the NIDS and the firewall. The SIEM will store only a single copy of any duplicate log entries, but also ensure that the entries are associated with both devices.
- **Logs/WORM.** A SIEM typically includes methods to prevent anyone from modifying log entries. This is sometimes referred to as write once read many (WORM). As logs are received, the SIEM will aggregate and correlate the log entries. After processing the logs, it can archive the source logs with write protection.

The location of the SIEM (and the location of its correlation engine) varies based on how the SIEM is used. However, it’s common to locate the SIEM within the private network, even if it is collecting some data from the demilitarized zone (DMZ). The internal network will provide the best protection for the log data. In very large organizations, aggregation processes and the correlation engine can consume a lot of processing power, so organizations sometimes off-load these processes to another server. The primary SIEM appliance can then focus on alerts and triggers.

Continuous Monitoring

It’s important to realize that there is never a time that security professionals can say, “Now that we’ve implemented this security measure, we can sit back knowing that we’re safe.” In other words, security is never finished. Instead, security professionals must continuously monitor their environment for emerging threats and new vulnerabilities.

Continuous security monitoring includes monitoring all relevant security controls, with the goal of ensuring that they help an organization maintain a strong security posture. There are many methods of monitoring, including performing periodic threat assessments, vulnerability assessments, and risk assessments. Many organizations perform routine vulnerability scans, such as once a week, and infrequent penetration tests. Additionally, organizations perform routine audits and reviews, such as usage auditing reviews and permission auditing reviews, which are discussed in the next section.

Remember this

A security information and event management (SIEM) system provides a centralized solution for collecting, analyzing, and managing data from multiple sources. It typically includes aggregation and correlation capabilities to collect and organize log data from multiple sources. It also provides continuous monitoring with automated alerts and triggers.

Usage Auditing and Reviews

Usage auditing refers to logging information on what users do. For example, if Homer accesses a file on a network server, the log entry would show his identity, when he accessed the file, what file he accessed, and what computer he used to access the file. He would not be able to refute the recorded action because auditing provides non-repudiation.

Auditing can include much more than when a user accessed a file. It can also include when a user logs on, accesses a network share, reads a file, modifies a file, creates a file, prints a file, accesses a web site via a proxy server, and much more.

Configuring logging of logon attempts is an important security step for system monitoring. After configuring logging, a system records the time and date when users log on, and when they access systems within a network. When users first log on to their account, it’s recorded as a logon action. Additionally, when users access a resource over the network (such as a file server), it is also recorded as a logon action. Many systems utilize single sign-on (SSO), so users don’t have to provide their credentials again. However, their access is still recorded as a logon action.

A usage auditing review looks at the logs to see what users are doing. For example, an organization might have a network share filled with files on a proprietary project. A usage auditing review might look at audit logs for these files to see who is accessing the files and what they are doing with the files.

Logs create an audit trail of what happened. Usage auditing reviews are often done to re- create the audit trail, or reconstruct what happened in the past. For example, if someone leaks proprietary information outside the organization, investigators can look at the auditing files to see who accessed the information, what they did with it (such as printing it), and when they did so.

Determining Actions from Auditing (Sidebar)

Reality Leigh Winner was arrested in 2017 on suspicion that she leaked an intelligence report to a news web site. She allegedly printed the document and sent it to The Intercept. The Intercept scanned the document, creating a five-page PDF file and included it in a story they published. The file was slightly redacted, but still gave investigators enough information to arrest Winner shortly after The Intercept published the story.

How did investigators identify Winner?

The PDF showed creases, indicating it was printed. After a little investigation, they discovered the file was printed by only six people. This indicates that the file likely had advanced auditing set on it. Advanced auditing can record any access on the file, including if the file is printed.

Ms. Winner was one of those six people. The PDF also included printer steganography tracking dots that provide another method of auditing. These coded dots identified the date and time when the file was printed and the printer model and serial number where it was printed. Access to this printer likely made it easy for investigators to rule out the other five people.

Permission Auditing and Review

A ***permission auditing review*** looks at the rights and permissions assigned to users and helps ensure the principle of least privilege is enforced. Chapter 2, “Understanding Identity and Access Management,” discusses the principle of least privilege in more depth, but in short it simply means that users have the rights and permissions they need, but no more. This includes ensuring users can access only the resources they need to perform their job.

Permission auditing reviews identify the privileges (rights and permissions) granted to users, and compares them against what the users need. It can detect privilege creep, a common problem that violates the principle of least privilege.

Privilege creep (or permission bloat) occurs when a user is granted more and more privileges due to changing job requirements, but unneeded privileges are never removed. For example, imagine Lisa is working in the Human Resources (HR) department, so she has access to HR data. Later, she transfers to the Sales department and administrators grant her access to sales data. However, no one removes her access to HR data even though she doesn't need it to perform her job in the Sales department.

Organizationscommonlyusearole-basedaccesscontrolmodelwithgroup-basedprivileges, as described in Chapter 2. For example, while Lisa is working in the HR department, her account would be in appropriate HR department security groups to grant her appropriate privileges for the HR job. When she transfers to the Sales department, administrators would add her to the appropriate Sales department groups, granting her privileges for her new job. An organization should also have account management controls in place to ensure that administrators remove her account from the HR department security groups. The permission auditing review verifies that these account management practices are followed.

Most organizations ensure that permission auditing reviews are performed at least once a year, and some organizations perform them more often. The goal is to do them often enough to catch potential problems and prevent security incidents. However, unless they can be automated, they become an unnecessary burden if security administrators are required to do them too often, such as daily or even once a week.

Remember this

Usage auditing records user activity in logs. A usage auditing review looks at the logs to see what users are doing and it can be used to re-create an audit trail. Permission auditing reviews help ensure that users have only the access they need and no more and can detect privilege creep issues.

Chapter 8 Exam Topic Review

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

Understanding Risk Management

- A risk is the likelihood that a threat will exploit a vulnerability. A threat is a potential danger that can compromise confidentiality, integrity, or availability of data or a system. A vulnerability is a weakness.
- Impact refers to the magnitude of harm that can be caused if a threat exercises a vulnerability.
- Threat assessments help an organization identify and categorize threats. An environmental threat assessment evaluates the likelihood of an environmental threat, such as a natural disaster, occurring. Manmade threat assessments evaluate threats from humans.
- Internal threat assessments evaluate threats from within an organization. External threat assessment evaluates threats from outside an organization.
- A vulnerability is a flaw or weakness in software or hardware, or a weakness in a process that a threat could exploit, resulting in a security breach.
- Risk management attempts to reduce risk to a level that an organization can accept, and the remaining risk is known as residual risk. Senior management is responsible for managing risk and the losses associated from residual risk.
- You can avoid a risk by not providing a service or participating in a risky activity. Purchasing insurance, such as fire insurance, transfers the risk to another entity. Security controls mitigate, or reduce, risks. When the cost of a control outweighs a risk, it is common to accept the risk.
- A risk assessment quantifies or qualifies risks based on different values or judgments. It starts by identifying asset values and prioritizing high-value items.
- Quantitative risk assessments use numbers, such as costs and asset

values. The single loss expectancy (SLE) is the cost of any single loss. The annual rate of occurrence (ARO) indicates how many times the loss will occur annually. You can calculate the annual loss expectancy (ALE) as SLE × ARO.

- Qualitative risk assessments use judgments to prioritize risks based on likelihood of occurrence and impact. These judgments provide a subjective ranking.
- Risk assessment results are sensitive. Only executives and security professionals should be granted access to risk assessment reports.
- A risk register is a detailed document listing information about risks. It typically includes risk scores along with recommended security controls to reduce the risk scores.
- A supply chain assessment evaluates a supply chain needed to produce and sell a product. It includes raw materials and all the processes required to create and distribute a finished product.

Comparing Scanning and Testing Tools

- A port scanner scans systems for open ports and attempts to discover what services and protocols are running.
- Network mapping identifies the IP addresses of hosts within a network. Network scanners expand on network mapping. They identify the operating system running on each host. They can also identify services and protocols running on each host.
- Wireless scanners can detect rogue access points (APs) in a network. Many can also crack passwords used by the APs.
- Banner grabbing queries remote systems to detect their operating system, along with services, protocols, and applications running on the remote system.
- Vulnerability scanners passively test security controls to identify vulnerabilities, a lack of security controls, and common misconfigurations. They are effective at discovering systems susceptible to an attack without exploiting the systems.
- A false positive from a vulnerability scan indicates the scan detected a vulnerability, but the vulnerability doesn’t exist. Credentialed scans run under the context of an account and can be

more accurate than non-credentialed scans, giving fewer false positives.

- Penetration testers should gain consent prior to starting a penetration test. A rules-of- engagement document identifies the boundaries of the test.
- A penetration test is an active test that attempts to exploit discovered vulnerabilities. It starts with a vulnerability scan and then bypasses or actively tests security controls to exploit vulnerabilities.
- Passive reconnaissance gathers information from open-source intelligence. Active reconnaissance uses scanning techniques to gather information.
- After initial exploitation, a penetration tester uses privilege escalation techniques to gain more access. Pivoting during a penetration test is the process of using an exploited system to access other systems.
- In black box testing, testers perform a penetration test with zero prior knowledge of the environment. White box testing indicates that the testers have full knowledge of the environment, including documentation and source code for tested applications. Gray box testing indicates some knowledge of the environment.
- Scans can be either intrusive or non-intrusive. Penetration testing is intrusive (also called invasive) and can potentially disrupt operations. Vulnerability testing is non-intrusive (also called non-invasive).
- Exploitation frameworks store information about security vulnerabilities. They are often used by penetration testers (and attackers) to detect and exploit software.

Using Security Tools

- Protocol analyzers (sniffers) can capture and analyze data sent over a network. Testers (and attackers) use protocol analyzers to capture cleartext data sent across a network.
- Administrators use protocol analyzers for troubleshooting communication issues by inspecting protocol headers to detect manipulated or fragmented packets.
- Captured packets show the type of traffic (protocol), source and destination IP addresses, source and destination MAC addresses, and

flags.

- Tcpdump is a command-line protocol analyzer. Captured packet files can be analyzed in a graphical protocol analyzer such as Wireshark.
- Nmap is a sophisticated network scanner run from the command line. Netcat is a command-line tool used to remotely administer servers. Netcat can also be used for banner grabbing.
- Logs record events and by monitoring logs, administrators can detect event anomalies. Security logs track logon and logoff activity on systems. System logs identify when services start and stop.
- Firewall and router logs identify the source and destination of traffic.
- A security information and event management (SIEM) system can aggregate and correlate logs from multiple sources in a single location. A SIEM also provides continuous monitoring and automated alerting and triggers.
- Continuous security monitoring helps an organization maintain its security posture, by verifying that security controls continue to function as intended.
- User auditing records user activities. User auditing reviews examine user activity. Permission auditing reviews help ensure that users have only the rights and permissions they need to perform their jobs, and no more.

Online References

- Don’t forget to check out the online resources at *http://gcgapremium.com/501-extras.* It includes additional free practice test questions, labs, and other resources to help you pass.

Chapter 8 Practice Questions

1. A security expert is performing a risk assessment. She is seeking information to identify the number of times a specific type of incident occurs per year. Which of the following BEST identifies this?

A. ALE
B. ARO
C. SLE
D. WORM

2. Lisa needs to calculate the ALE for a group of servers used in the network. During the past two years, five of the servers failed. The hardware cost to repair or replace each server was
$3,500 and the downtime resulted in $2,500 of additional losses for each outage. What is the ALE?

A.
$7,000
B.
$8,000
C.
$15,000
D.
$30,000

3. Martin is performing a risk assessment on an e-commerce web server. While doing so, he created a document showing all the known risks to this server, along with the risk score for each risk. What is the name of this document?

A. Quantitative risk assessment
B. Qualitative risk assessment
C. Residual risk
D. Risk register

4. Your organization includes an e-commerce web site used to sell digital products. You are tasked with evaluating all the elements used to support this web site. What are you performing?

A. Quantitative assessment
B. Qualitative assessment

C. Threat assessment
D. Supply chain assessment

5. A penetration tester is running several tests on a server within your organization’s DMZ. The tester wants to identify the operating system of the remote host. Which of the following tools or methods are MOST likely to provide this information?

A. Banner grabbing
B. Vulnerability scan
C. Password cracker
D. Protocol analyzer

6. You need to perform tests on your network to identify missing security controls. However, you want to have the least impact on systems that users are accessing. Which of the following tools is the BEST to meet this need?

A. A syn stealth scan
B. Vulnerability scan
C. Ping scan
D. Penetration test

7. You periodically run vulnerability scans on your network, but have been receiving many false positives. Which of the following actions can help reduce the false positives?

A. Run the scans as credentialed scans.
B. Run the scans as non-credentialed scans.
C. Run the scans using passive reconnaissance.
D. Run the scans using active reconnaissance.

8. Your organization has a legacy server running within the DMZ. It is running older software that is not compatible with current patches, so management has decided to let it remain unpatched. Management wants to know if attackers can access the internal network if they successfully compromise this server. Which of the following is the MOST appropriate action?

A. Perform a vulnerability scan.
B. Perform a port scan.
C. Perform a black box test.
D. Perform a penetration test.

9. A penetration tester has successfully attacked a single computer

within the network. The tester is now attempting to access other systems within the network via this computer. Which of the following BEST describes the tester’s current actions?

A. Performing reconnaissance
B. Performing the initial exploitation
C. Pivoting
D. Escalating privileges

10. You are troubleshooting issues between two servers on your network and need to analyze the network traffic. Of the following choices, what is the BEST tool to capture and analyze this traffic?

A. Network mapper
B. Protocol analyzer
C. Network scanner
D. SIEM

11. A penetration tester is tasked with gaining information on one of your internal servers and he enters the following command:

echo “” | nc -vv -n -w1 72.52.206.134 80

What is the purpose of this command?

A. Identify if a server is running a service using port 80 and is reachable.
B. Launch an attack on a server sending 80 separate packets in a short period of time.
C. Use Netcat to remotely administer the server.
D. Use Netcat to start an RDP session on the server.

12. You suspect that an attacker has been sending specially crafted TCP packets to a server trying to exploit a vulnerability. You decide to capture TCP packets being sent to this server for later analysis and you want to use a command-line tool to do so. Which of the following tools will BEST meet your need?

A. Wiredump
B. Tcpdump
C. Netcat
D. Nmap

13. You suspect someone has been trying a brute force password attack on a Linux system. Which of the following logs should you check to view failed authentication attempts by users?

A. /var/log/btmp
B. /var/log/fail
C. var/log/httpd
D. /var/log/kern

14. An organization has a large network with dozens of servers. Administrators are finding it difficult to review and analyze the logs from all the network devices. They are looking for a solution to aggregate and correlate the logs. Which of the following choices BEST meets this need?

A. Nmap
B. Netcat
C. Wireshark
D. SIEM

15. Lisa has recently transferred from the HR department to payroll. While browsing file shares, Lisa notices she can access the HR files related to her new coworkers. Which of the following could prevent this scenario from occurring?

A. Permission auditing and review
B. Continuous monitoring
C. Vulnerability scan
D. Penetration testing

Chapter 8 Practice Question Answers

1. **B.** The annual rate of occurrence (ARO) is the best choice to identify how many times a specific type of incident occurs in a year. Annual loss expectancy (ALE) identifies the expected monetary loss for a year and single loss expectancy (SLE) identifies the expected monetary loss for a single incident. ALE = SLE × ARO and if you know any two of these values, you can identify the third value. For example, ARO = ALE / SLE. Write once read many (WORM) is a term sometimes used with archived logs indicating they cannot be modified.

2. **C.** The annual loss expectancy (ALE) is $15,000. The single loss expectancy (SLE) is $6,000 ($3,500 to repair or replace each server plus $2,500 in additional losses for each outage). The annual rate of occurrence (ARO) is 2.5 (five failures in two years or 5 / 2). You calculate the ALE as SLE × ARO ($6,000 × 2.5).

3. **D.** A risk register lists all known risks for an asset, such as a web server, and it typically includes a risk score (the combination of the likelihood of occurrence and the impact of the risk). Risk assessments (including quantitative and qualitative risk assessments) might use a risk register, but they aren't risk registers. Residual risk refers to the remaining risk after applying security controls to mitigate a risk.

4. **D.** A supply chain assessment evaluates all the elements used to create, sell, and distribute a product. Risk assessments (including both quantitative and qualitative risk assessments) evaluate risks, but don't evaluate the supply chain required to support an e-commerce web site. A threat assessment evaluates threats.

5. **A.** Banner grabbing is a technique used to gain information about a remote server and it will identify the operating system of the system in the demilitarized zone (DMZ). A vulnerability scanner checks for vulnerabilities. A password cracker attempts to discover passwords. A protocol analyzer collects packets sent across a network and can be used to analyze the packets.

6. **B.** A vulnerability scanner is passive and has the least impact on systems, and it can detect systems that are lacking specific security

controls. Network scanners use methods such as a syn stealth scan and a ping scan to discover devices on a network, but they don't identify missing security controls. A penetration test is invasive and does not have the least impact on systems.

7. **A.** Running the scans as credentialed scans (within the context of a valid account) allows the scantoseemoreinformationandtypicallyresultsinfewerfalsepositives. Non-credentialed scans run without any user credentials and can be less accurate. Passive reconnaissance collects information on a target using open-source intelligence. All vulnerability scans use active reconnaissance techniques.

8. **D.** A penetration test attempts to exploit a vulnerability and can determine if a successful attack will allow attackers into the internal network. A vulnerability scan is passive. It does not attempt to compromise a system, so it cannot verify if an attacker can access the internal network. A port scan only identifies open ports. A black box test only refers to the knowledge of the testers and indicates they have zero knowledge prior to starting a test.

9. **C.** Pivoting is the process of accessing other systems through a single compromised system. Reconnaissance techniques are done before attacking a system. A successful attack on a single computer is the initial exploitation. Escalating privileges attempts to gain higher privileges on a target.

10. **B.** A protocol analyzer (also called a sniffer) is the best choice to capture and analyze network traffic. A network mapper can detect all the devices on a network, and a network scanner can detect more information about these devices, but neither of these tools is the best choice to capture and analyze traffic for troubleshooting purposes. A security information and event management (SIEM) system aggregates and correlates logs from multiple sources, but does not capture network traffic.

11. **A.** This command sends a query to the server over port 80 and if the server is running a service on port 80, it will connect. This is a common beginning command for a banner grabbing attempt. It does not send 80 separate packets. Netcat is often used to remotely

administer servers, but not using port 80. Remote Desktop Protocol (RDP) uses port 3389 and is not relevant in this scenario.

12. **B.** The tcpdump command-line tool is the best choice of the given answers. It is a command- line packet analyzer (or protocol analyzer) and its primary purpose is to capture packets. Wiredump isn't a valid tool name. Wireshark (not included as an answer choice) is a graphic-based packet analyzer that can be started from the command line, but tcpdump includes more command-line options than Wireshark. Netcat is useful for remotely accessing systems and can be used for banner grabbing, but it doesn't capture packets. Nmap analyzes packets during a scan. It can also use Npcap, the Nmap Project's packet sniffing library, but Nmap isn't the best choice to capture packets.

13. **A.** The /var/log/btmp log contains information on user failed login attempts. While not available as an answer, /var/log/auth also includes information on failed login attempts. While the /var/log/faillog log includes information on failed logins, /var/log/fail isn't a valid log name in Linux. The /var/log/httpd directory includes logs from the Apache web server, when it's installed. The /var/log/kern log contains information logged by the system kernel.

14. **D.** A security information and event management (SIEM) system provides a centralized solution for collecting, analyzing, and managing data from multiple sources and can aggregate and correlate logs. None of the other choices aggregate and correlate logs. Nmap is a network scanner that can discover and map devices on a network. Netcat is a command-line tool that can be used to connect to servers. Wireshark is a graphical-based protocol analyzer.

15. **A.** A permission auditing and review process verifies that the principle of least privilege is followed. This includes ensuring users can access only the resources they need to perform their job. Continuousmonitoringincludesmonitoringallrelevantsecuritycontrols, but isn't the best choice for this specific scenario. A vulnerability scan will discover vulnerabilities on a system or network and a penetration test will scan a system or network and attempt to exploit vulnerabilities. However, vulnerability scans and penetration tests cannot verify a user has the appropriate privileges.