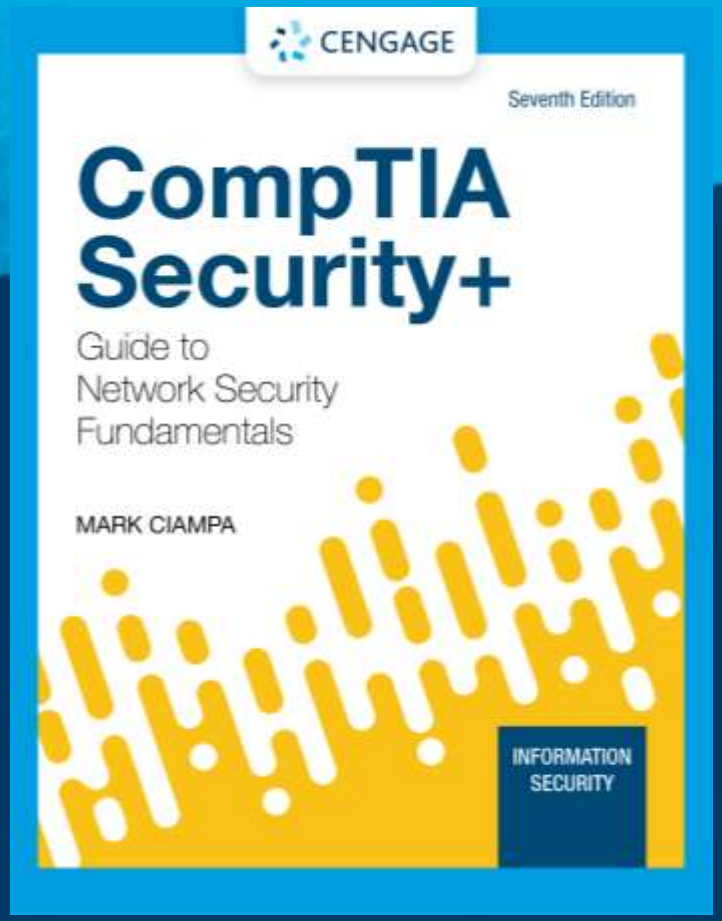


# CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

## Module 2: Threat Management and Cybersecurity Resources

CENGAGE

# Module Objectives

By the end of this module, you should be able to:

1. Explain what a penetration test is

2. Identify the rules of engagement and how to perform a pen test

3. Define vulnerability scanning

4. Describe different cybersecurity resources

# Penetration Testing

- Studying penetration testing involves:
  - Defining what it is and why such a test should be conducted
  - Examining who should perform the tests and the rules for engagement
  - Knowing how to perform a penetration test

# Defining Penetration Testing

- **Penetration testing** attempts to exploit vulnerabilities in order to help:
  - Uncover new vulnerabilities
  - Provide a clearer picture of their nature
  - Determine how they could be used against the organization
- The most important element in a “pen test” is the first step: *planning*
  - A lack of planning can result in *creep*, which is an expansion beyond the initial set of the test’s limitations
  - The most dangerous result of poor planning is creating unnecessary legal issues

# Why Conduct a Test?

- A scan of network defenses usually finds only surface problems to be addressed
  - Many network scans are *automated* and provide only limited verification of vulnerabilities
- A penetration test can find *deep* vulnerabilities and attempts to exploit vulnerabilities using manual techniques
- The attacks:
  - Must be the same as those used by a threat actor
  - Should follow the thinking of threat actors

# Who Should Perform the Test? (1 of 3)

- Internal Security Personnel
  - Advantages to using internal employees include:
    - There is little or no additional cost
    - The test can be conducted much more quickly
    - An in-house pen test can be used to enhance the training of employees and raise the awareness of security risks
  - Disadvantages of using internal security employees:
    - *Inside knowledge*
    - *Lack of expertise*
    - *Reluctance to reveal*

# Who Should Perform the Test? (2 of 3)

- External Pen Tester Consultants
  - Contracting with an external pen testing consultant offers the following advantages:
    - *Expertise*
    - *Credentials*
    - *Experience*
    - *Focus*
  - A disadvantage of using external consultants is the usage of the information uncovered
    - A contractor who conducts a pen test learns all about an organization's network and may receive extremely sensitive information about systems and how to access them
    - This knowledge could be sold to a competitor

# Who Should Perform the Test? (3 of 3)

- Crowdsourced Pen Testers
  - A **bug bounty** is a monetary reward given for uncovering a software vulnerability
  - Bug bounty programs take advantage of *crowdsourcing*, which involves obtaining input into a project by enlisting the services of many people through the internet
  - Advantages of crowdsourced pen testers include the following:
    - Faster testing, resulting in quicker remediation of vulnerabilities
    - Ability to rotate teams so different individuals test the system
    - Option of conducting multiple pen tests simultaneously

# Knowledge Check Activity 1

What is the first step in penetration testing and what is its importance?

a. Planning, because a lack of planning can result in legal issues.

b. Targeting, because the pen tester must know which systems to attempt to penetrate.

c. Targeting; the targets will determine which tools are needed for the pen test.

d. Planning, but this step can often be skipped if the tester is in a hurry.

# Knowledge Check Activity 1: Answer

What is the first step in penetration testing and what is its importance?

**Answer: a. Planning, because a lack of planning can result in legal issues.**

**Planning is the first step and is not an optional step. A lack of planning can result not only in a poorly defined penetration test but also in legal issues.**

# Rules of Engagement (1 of 5)

- Rules of engagement in a penetration test are its limitations or parameters
- Categories for rules of engagement are:
  - Timing
  - Scope
  - Authorization
  - Exploitation
  - Communication
  - Cleanup
  - Reporting

# Rules of Engagement (2 of 5)

- Timing
  - The *timing* parameter sets when the testing will occur
  - Some considerations include: the start and stop dates of the test and should the active portions of the pen test be conducted during normal business hours
- Scope
  - Scope involves several elements that define the relevant test boundaries:
    - *Environment*
    - *Internal targets*
    - *External targets*
    - *Target locations*
    - *Other boundaries*

# Rules of Engagement (3 of 5)

- Authorization
  - *Authorization* is the receipt of prior written approval to conduct the pen test
    - A formal written document must be signed by all parties before a pen test begins
- Exploitation
  - The *exploitation level* in a pen test should be part of the scope that is discussed in the planning stages
- Communication
  - The pen tester should communicate with the organization during the following occasions:
    - *Initiation*
    - *Incident response*
    - *Status*
    - *Emergency*

# Rules of Engagement (4 of 5)

- Cleanup
  - The pen tester must ensure that everything related to the pen test has been removed
  - Cleanup involves removing all software agents, scripts, executable binaries, temporary files, and backdoors from all affected systems
  - Any credentials that were changed should be restored and any usernames created should be removed
- Reporting
  - Once the pen test is completed, a report should be generated to document its objectives, methods used, and results
  - The report should be divided into two parts:
    - An executive summary designed for a less technical audience
    - A more technical summary written for security professionals

# Rules of Engagement (5 of 5)

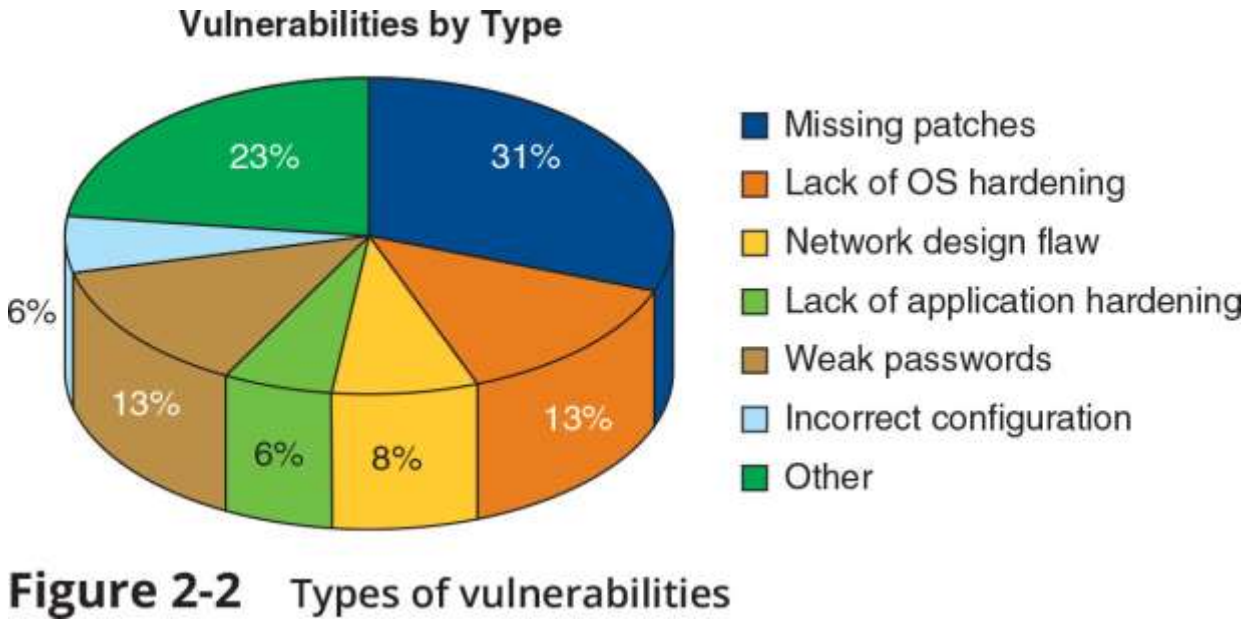


**Figure 2-2** Types of vulnerabilities

Figure 2-2 Types of vulnerabilities

# Performing a Penetration Test (1 of 4)

- Performing a successful pen test involves *determination, resolve, and perseverance*
- A variety of actions take place when performing a pen test, however, they can be grouped into two phases:
  - Reconnaissance
  - Penetration

# Performing a Penetration Test (2 of 4)

- Phase 1: Reconnaissance
  - The first task is to perform preliminary information gathering from outside the organization (called **footprinting**)
  - Information can be gathered using two methods: **active reconnaissance** and **passive reconnaissance**
  - Active reconnaissance involves directly probing for vulnerabilities and useful information
    - **War driving** is searching for wireless signals from an automobile or on foot while using a portable device
    - **War flying** uses drones, which are officially known as **unmanned aerial vehicles** (**UAVs**)
  - A disadvantage of active reconnaissance is that the probes are likely to alert security professionals that something unusual is occurring

# Performing a Penetration Test (3 of 4)

- Phase 1: Reconnaissance (continued)
  - Passive reconnaissance occurs when the tester uses tools that do not raise any alarms
  - This may include searching online for publicly accessible information called **open source intelligence** (**OSINT**) that can reveal valuable insight about the system
- Phase 2: Penetration
  - A pen test is intended to simulate the actions of a threat actor
  - The initial system compromised usually does not contain the data that is the goal of the attack
  - That system usually serves as a gateway for entry into an organization network
  - Once inside the network, threat actors turn to other systems to be compromised until they reach the ultimate target

# Performing a Penetration Test (4 of 4)

- Phase 2: Penetration (continued)
  - Lessons to be learned from how threat actors work include:
    - When a vulnerability is discovered, the pen tester must determine how to pivot (turn) to another system using another vulnerability to continue moving toward the target
    - Vulnerabilities that are not part of the ultimate target can still provide a gateway to the target
    - Pen tests are manual, therefore, a pen tester needs to design attacks carefully
    - Pen testers must be patent and persistent, just like the threat actors

# Knowledge Check Activity 2

What are the two primary phases of penetration testing in order?

a. Penetration, escalation
b. Penetration, pivoting
c. Reconnaissance, footprinting
d. Reconnaissance, penetration

# Knowledge Check Activity 2: Answer

What are the two primary phases of penetration testing in order?

**Answer: d. Reconnaissance, penetration**

**Reconnaissance is a necessary first phase because proper reconnaissance gathers the information needed to perform a proper penetration test. Reconnaissance is followed by the second phase; the actual attempt at penetration.**

# Vulnerability Scanning

- **Vulnerability scanning** in some ways complements pen testing
- Studying vulnerability scanning involves understanding:
  - What it is
  - How to conduct a scan
  - How to use data management tools
  - How threat hunting can enhance scanning

# What is a Vulnerability  Scan?

- A penetration test is a single event using a manual process often performed only after a specific amount of time has passed
- A **vulnerability scan** is a frequent and ongoing process that continuously identifies vulnerabilities and monitors cybersecurity progress

# Conducting a Vulnerability Scan (1 of 6)

- Conducting a vulnerability scan involves:
  - Knowing what to scan and how often
  - Selecting a type of scan
  - Interpreting vulnerability information
- When and What to Scan
  - Two primary reasons for not conducting around-the-clock vulnerability scans:
    - *Workflow interruptions*
    - *Technical constraints*
  - A more focused approach is to know the location of data so that specific systems with high-value data can be scanned more frequently

# Conducting a Vulnerability Scan (2 of 6)


**Figure 2-4** Nessus hardware asset management

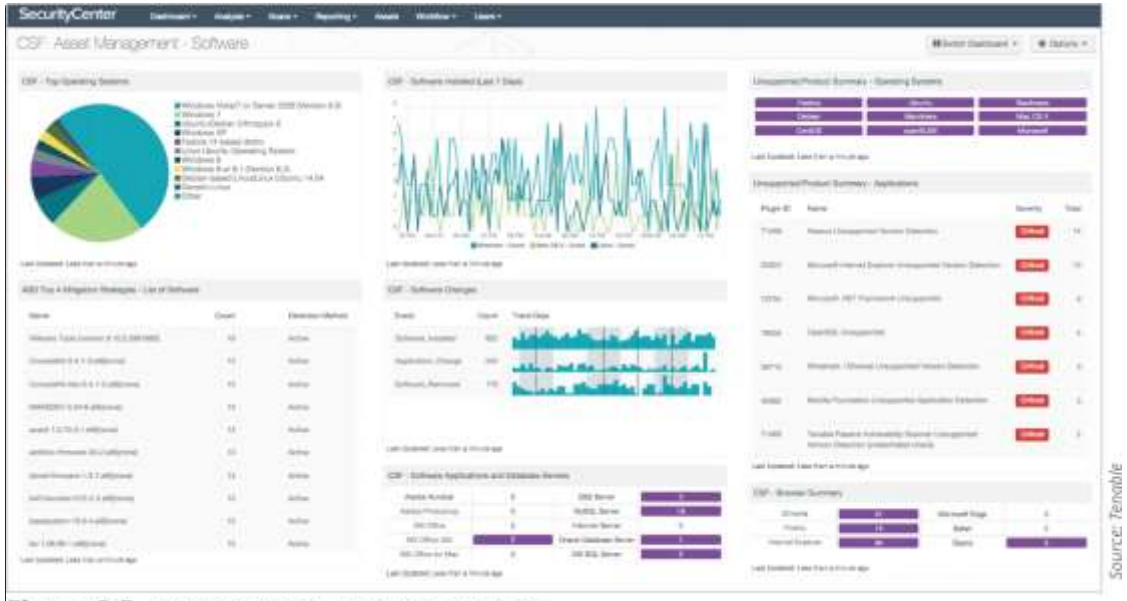


**Figure 2-5** Nessus software asset management

# Conducting a Vulnerability Scan (3 of 6)

- Because a vulnerability scan should be limited, a configuration review of software settings should be conducted
  - Define the group of target devices to be scanned
  - Ensure that a scan should be designed to meet its intended goals
  - Determine the sensitivity level or the depth of a scan
  - Specify the data types to be scanned

# Conducting a Vulnerability Scan (4 of 6)

- Types of Scans
  - Two major types of scans are credentialed scans and intrusive scans
  - In a **credentialed scan**, valid authentication credentials are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials
  - A **non-credentialed scan** provides no such authentication information
  - An **intrusive scan** attempts to employ any vulnerabilities that it finds
  - A **nonintrusive scan** does not attempt to exploit the vulnerability but only records that it was discovered
- Vulnerability Information
  - Vulnerability scanning software compares the software it scans against a set of known vulnerabilities
  - Vulnerability information is available to provide updated information to scanning software about the latest vulnerabilities

# Conducting a Vulnerability Scan (5 of 6)

- Examining Results
  - When examining the results of a vulnerability scan, you should assess the importance of vulnerability as well as its accuracy
  - Questions that may help identify which vulnerability needs early attention:
    - Can the vulnerability be addressed in a reasonable amount of time?
    - Can the vulnerability be exploited by an external threat actor?
    - If the vulnerability led to threat actors infiltrating the system, would they be able to pivot to more important systems?
    - Is the data on the affected device sensitive or is it public?
    - Is the vulnerability on a critical system that runs a core business process?
  - Another part of prioritizing is making sure that the difficulty and time for implementing the correction is reasonable

# Conducting a Vulnerability Scan (6 of 6)

- Examining Results (continued)
  - Another consideration when examining results is accuracy
  - Be sure to identify **false positives**, which is an alarm raised when there is no problem
  - A means to identify false positives is to correlate the vulnerability scan data with several internal data points
    - Most common are related to log files
    - **Log reviews**, or an analysis of log data, can be used to identify false positives

# Data Management Tools (1 of 3)

- Two data management tools are used for collecting and analyzing vulnerability scan data:
  - **Security Information and Event Management (SIEM)**
  - **Security Orchestration, Automation, and Response (SOAR)**
- Security Information and Event Management (SIEM)
  - A SIEM typically has the following features:
    - *Aggregation*
    - *Correlation*
    - *Automated alerting and triggers*
    - *Time synchronization*
    - *Event duplication*
    - *Logs*

# Data Management Tools (2 of 3)


**Figure 2-8** SIEM dashboard

Figure 2-8 SIEM dashboard

# Data Management Tools (3 of 3)

- SIEMS can also perform **sentiment analysis**, which is the process of computationally identifying and categorizing opinions to determine the writer's attitude toward a particular topic
  - Sentiment analysis has been used when tracking postings threat actors make in discussion forums with other attackers to better determine the behavior and mindset of threat actors
- Security Orchestration, Automation, and Response (SOAR)
  - A SOAR is similar to a SIEM in that it is designed to help security teams manage and respond to security warnings and alarms
  - SOARs combine more comprehensive data gathering and analytics to automate incident responses

# Threat Hunting

- **Threat hunting** is proactively searching for cyber threats that thus far have gone undetected in a network
  - It begins with a critical premise: *threat actors have already infiltrated our network*
  - It proceeds to find unusual behavior that may indicate malicious activity
- Threat hunting investigations often use crowdsourced attack data such as:
  - Advisories and bulletins
  - Cybersecurity **threat feeds** – data feeds of information on the latest threats
  - Information from a **fusion center** – a formal repository of information from enterprises and the government used to share information on the latest attacks

# Knowledge Check Activity 3

Which of the following is NOT typically a feature of a SIEM?

a. Aggregation
b. Remediation
c. Correlation
d. Event duplication

# Knowledge Check Activity 3: Answer

Which of the following is NOT typically a feature of a SIEM?

**Answer: b. Remediation**

**The typical features found in a SIEM are aggregation, correlation, automated triggers and alerts, time synchronization, event duplication, and logs. A SIEM provides analysis and reporting but does not commonly provide remediation of security events.**

# Cybersecurity Resources

- External cybersecurity resources are available to organizations:
  - Frameworks
  - Regulations
  - Legislation
  - Standards
  - Benchmarks/secure configuration guides
  - Information sources

# Frameworks (1 of 3)

- A **cybersecurity framework** is a series of documented processes used to define policies and procedures for implementing and managing security controls in an enterprise environment
- The most common frameworks are from the:
  - National Institute of Standards and Technology (NIST)
  - International Organization for Standardization (ISO)
  - American Institute of Certified Public Accountants (AICPA)
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)

# Frameworks (3 of 3)


Source: NIST

**Figure 2-9** NIST Cybersecurity Framework (CSF) functions

Figure 2-9 NIST Cybersecurity Framework (CSF) functions

# Regulations

- The process of adhering to regulations is called *regulatory compliance*
- **Industry regulations** are typically developed by established professional organizations or government agencies using the expertise of seasoned security professionals
- Sample of cybersecurity regulations categories:
  - *Broadly applicable regulations*
  - *Industry-specific regulations*
  - *U.S. state regulations*
  - *International regulations*

# Legislation

- Specific legislation can also be enacted by governing bodies
  - These include national, territorial, and state laws
- Due to a lack of comprehensive federal regulations for data breach notification, many states have amended their breach notification laws from the basic definitions
  - No two state laws are the same

# Standards

- A standard is a document approved through consensus by a recognized standardization body
  - It provides for framework, rules, guidance, or characteristics for products or related processes and production methods
- One cybersecurity standard is the Payment Card Industry Data Security Standard (PCI DSS)

# Benchmarks/Secure Configuration Guides

- **Benchmark/secure configuration guides** are usually distributed by hardware manufacturers and software developers
  - They serve as guidelines for configuring a device or software so that it is resilient to attacks
- Usually, they are usually **platform/vendor-specific guides** that only apply to specific products
- Guides are available for:
  - Network infrastructure devices
  - OSs
  - Web servers
  - Application servers

# Information Sources

- There are a variety of information sources including:
  - Vendor websites
  - Conferences
  - Academic journals
  - Local industry groups
  - Social media
- A specialized research source is a **Request for comments** (**RFC**)
  - Which are white papers documents that are authored by technology bodies employing specialists, engineers, and scientists who are experts in their field

# Discussion Activity

1. Many schools, especially high schools, restrict IT students from accessing the tools used to perform penetration testing and vulnerability scanning for fear that students will use them for nefarious purposes. Is this a valid concern? Why or why not? Is there a way students can learn about these tools in a manner that is safe and that will ease school administrators' concerns?
2. Each student should provide a response to the question.
3. If this is an online class, responses can be posted in the discussion board and each student should respond with a minimum of 100 words. To encourage interaction, each student should post a minimum 25-word response to another student's post.

# Self-Assessment

1. Complete Case Project 2-2 and Case Project 2-3 from the book. Based on your research, consider the following question and use the knowledge you gained from this module to formulate an answer: If a company has sufficient budget for either a good Pen Test product or a good Vulnerability Scanner, which should they choose and why?

# Summary (1 of 2)

- Penetration testing attempts to exploit vulnerabilities just as a threat actor would
- Using internal employees to conduct a penetration test has advantages in some cases
- The rules of engagement in a penetration test are its limitations or parameters
- The first phase of a penetration test is reconnaissance, also called footprinting
- A penetration test is a single event using a manual process that is usually performed only after a specific amount of time has passed
- The best approach for vulnerability scanning is not to scan all systems all the time
- Vulnerability information is available to provided updated information to scanning software about the latest vulnerabilities

# Summary (2 of 2)

- Two data management tools are used for collecting and analyzing data: the Security Information and Event Management (SIEM) tool and a Security Orchestration, Automation, and Response (SOAR) tool
- A cybersecurity framework is a series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment
- Regulations are another cybersecurity resource
- A standard is a document approved through consensus by a recognized standardization body
- Deep vulnerabilities can only be exposed through actual attacks that use the mindset of a threat actor