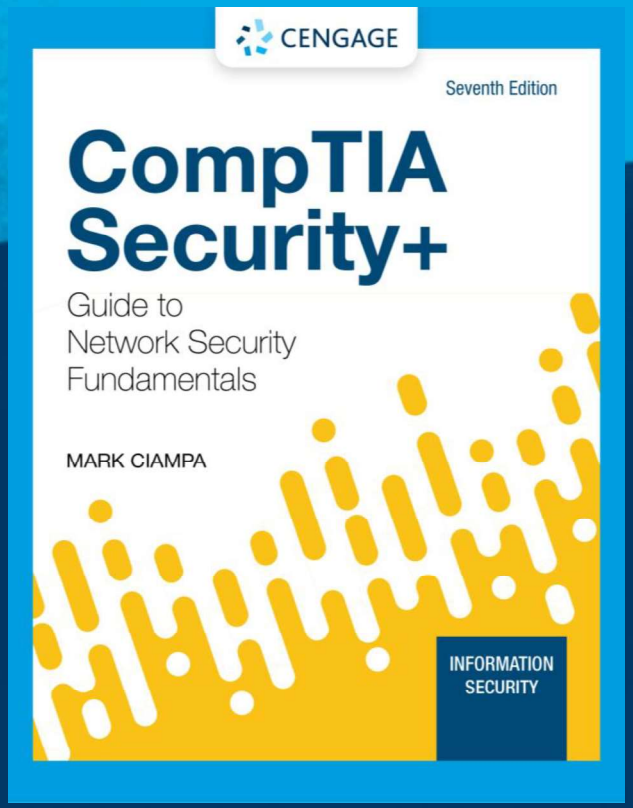

CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

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)

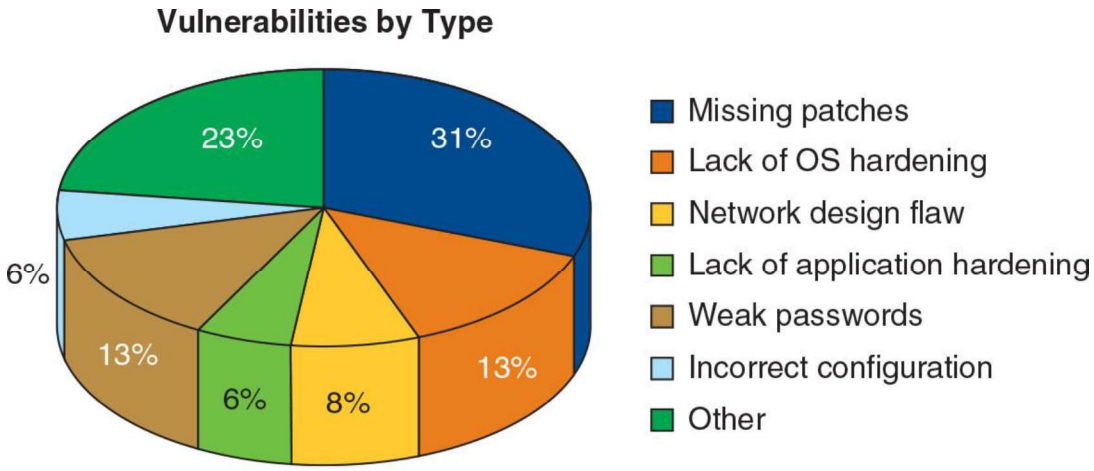

Figure 2-2 Types of vulnerabilities

Figure 2-2 Types of vulnerabilities