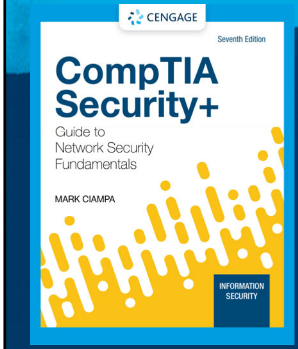


CENGAGE

Seventh Edition

CompTIA Security+

Guide to Network Security Fundamentals

MARK CIAMPA

INFORMATION SECURITY

Module 2
Threat Management and Cybersecurity Resources

Module Objectives

- By the end of this module, you should be able to:
  - Explain what a penetration test is
  - Identify the rules of engagement and how to perform a pen test
  - Define vulnerability scanning
  - Describe different cybersecurity resources

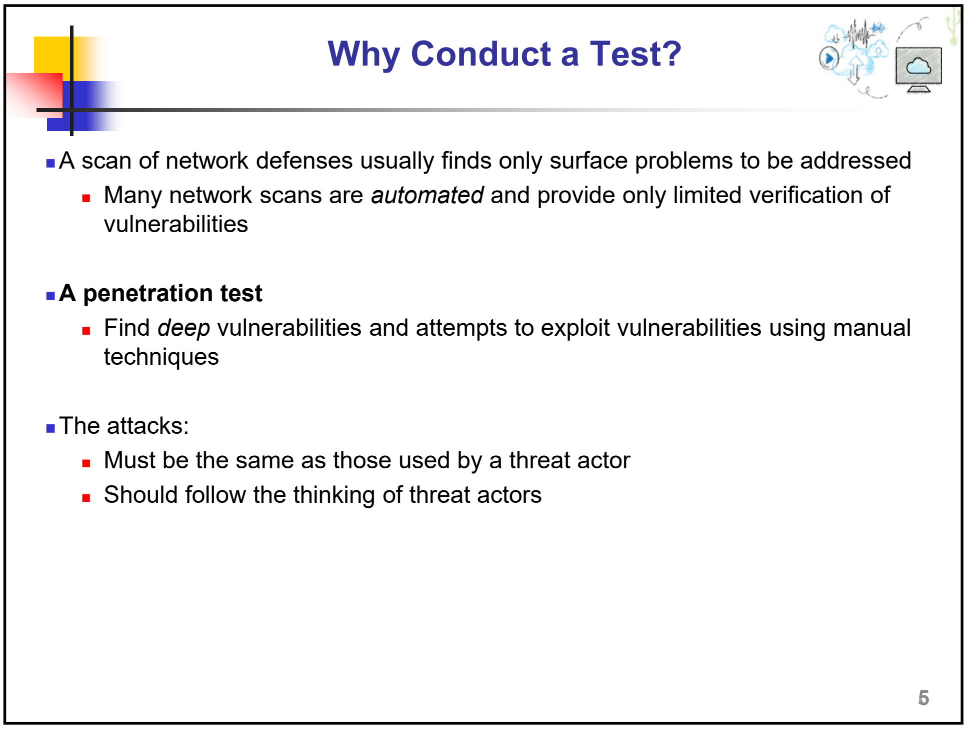
Penetration Testing

- 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

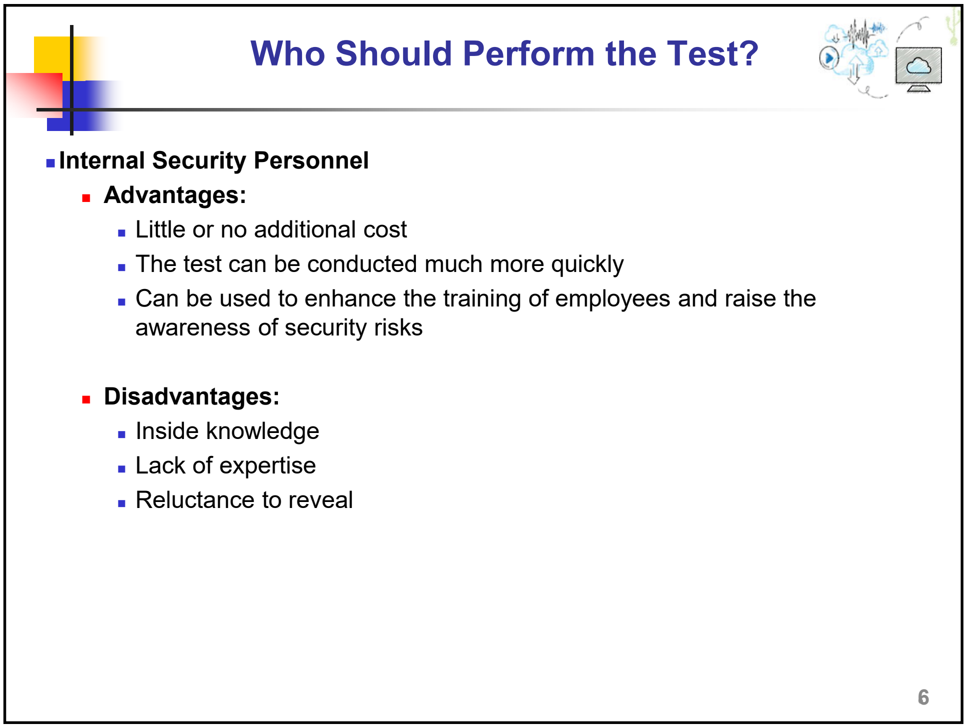
- **Penetration testing** attempts to exploit vulnerabilities in order to help:
  - Uncover new vulnerabilities
  - Provide a clearer picture of their nature
  - Determine how they could be used against the organization

- **Planning:**
  - The first step- Most important element in a “pen test
  - A lack of planning can result in
    - *Scope creep*,
    - Create 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**
  - 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?

- **Internal Security Personnel**
  - **Advantages:**
    - Little or no additional cost
    - The test can be conducted much more quickly
    - Can be used to enhance the training of employees and raise the awareness of security risks
  - **Disadvantages:**
    - Inside knowledge
    - Lack of expertise
    - Reluctance to reveal

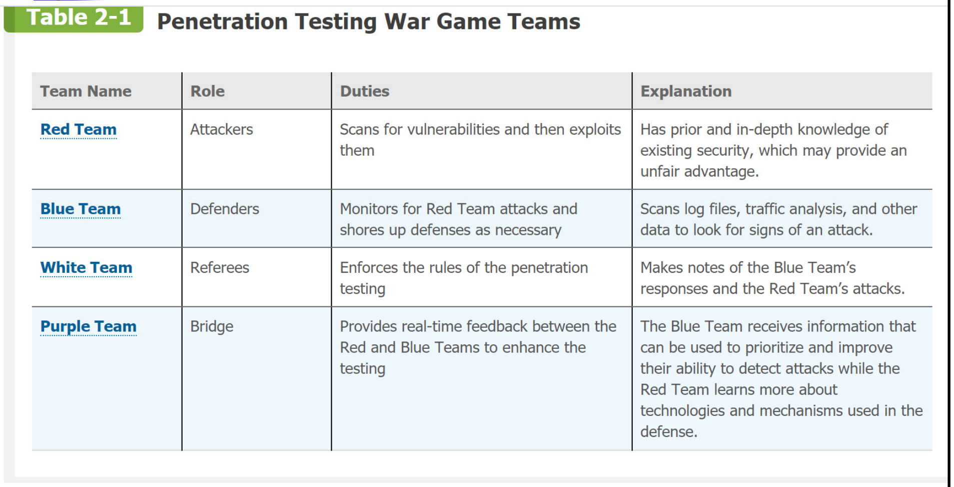


Table 2-1 Penetration Testing War Game Teams

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

Who Should Perform the Test? (contd.)

- **External Pen Tester Consultants**
  - **Advantages:**
    - Expertise
    - Credentials
    - Experience
    - Focus
  - **Disadvantages:**
    - A contractor may learn all about an organization's network
    - May receive extremely sensitive information about systems and how to access them
    - Knowledge could be sold to a competitor

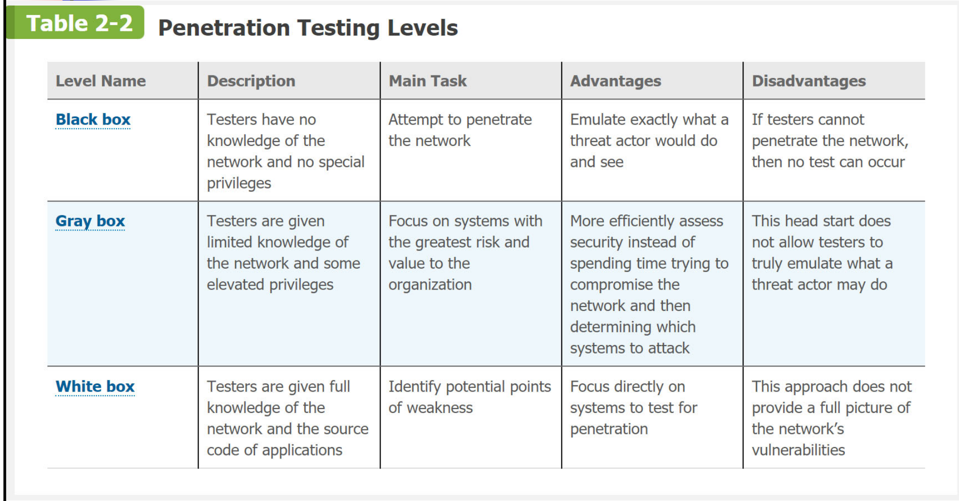
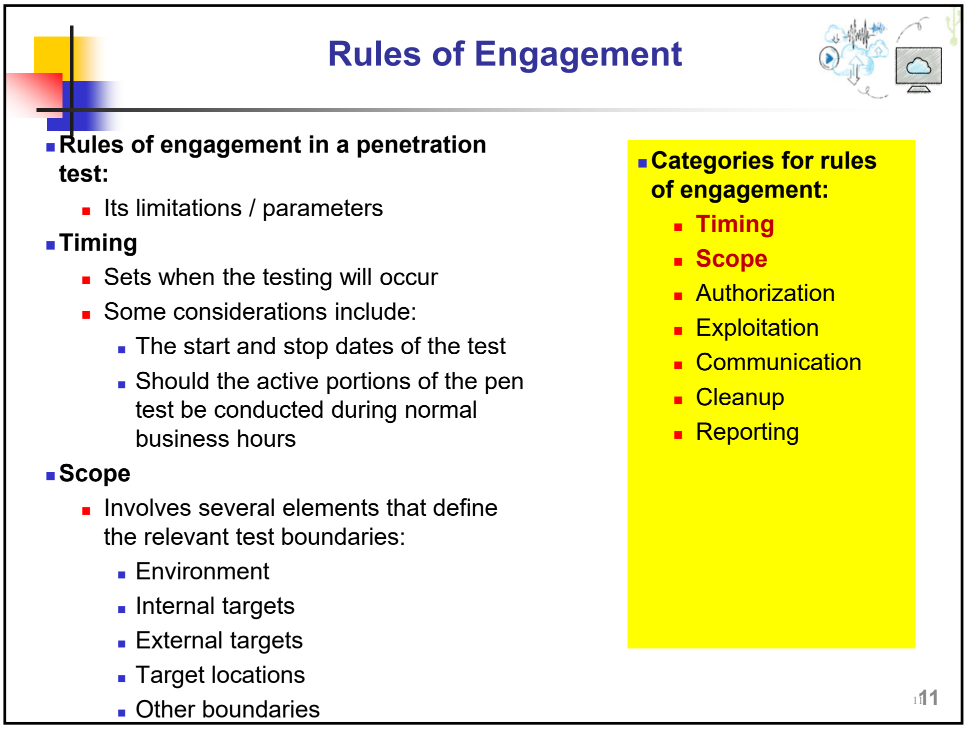


Table 2-2 Penetration Testing Levels

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

Who Should Perform the Test? (contd.)

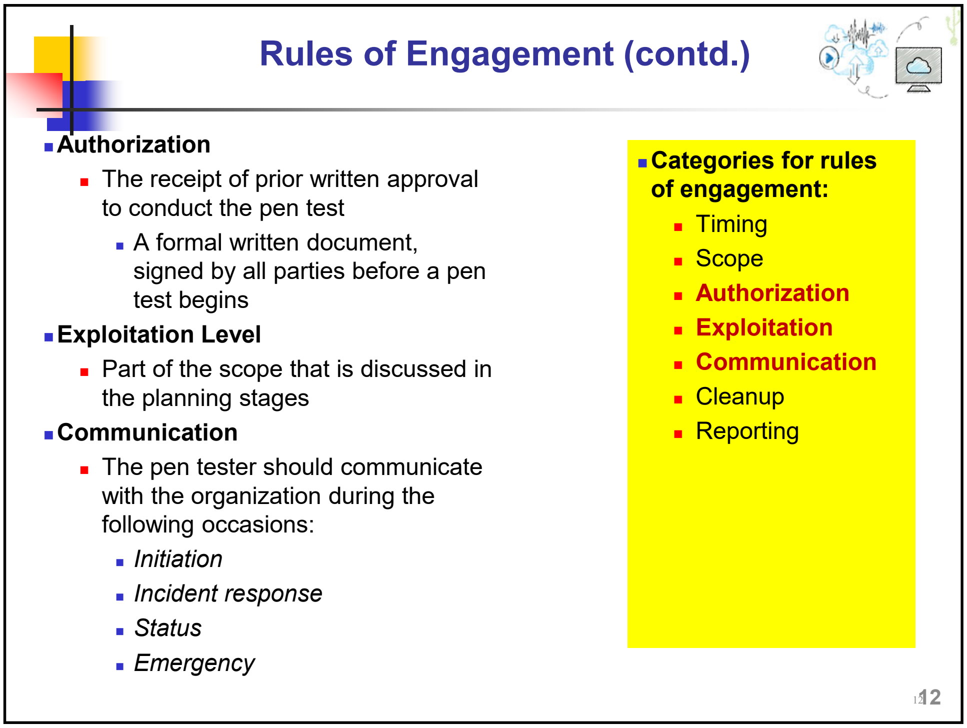
- **Crowdsourced Pen Testers**
  - **Advantages:**
    - Faster testing, resulting in quicker remediation of vulnerabilities
    - Ability to rotate teams so different individuals test the system
    - Option of conducting multiple pen tests simultaneously
  - **Bug bounty**
    - A monetary reward given for uncovering a software vulnerability
    - Take advantage of crowdsourcing, which involves obtaining input into a project by enlisting the services of many people through the internet
    - Facebook
      - https://www.facebook.com/whitehat
    - Google
      - https://www.google.com/about/appsecurity/reward-program/
    - Amazon
      - https://hackerone.com/amazonvrp?type=team



Rules of Engagement

- **Rules of engagement in a penetration test:**
  - Its limitations / parameters
- **Timing**
  - Sets when the testing will occur
  - Some considerations include:
    - The start and stop dates of the test
    - Should the active portions of the pen test be conducted during normal business hours
- **Scope**
  - Involves several elements that define the relevant test boundaries:
    - Environment
    - Internal targets
    - External targets
    - Target locations
    - Other boundaries

- **Categories for rules of engagement:**
  - **Timing**
  - **Scope**
  - Authorization
  - Exploitation
  - Communication
  - Cleanup
  - Reporting



Rules of Engagement (contd.)

- **Authorization**
  - The receipt of prior written approval to conduct the pen test
    - A formal written document, signed by all parties before a pen test begins
- **Exploitation Level**
  - 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*

- **Categories for rules of engagement:**
  - Timing
  - Scope
  - **Authorization**
  - **Exploitation**
  - **Communication**
  - Cleanup
  - Reporting

Rules of Engagement (contd.)

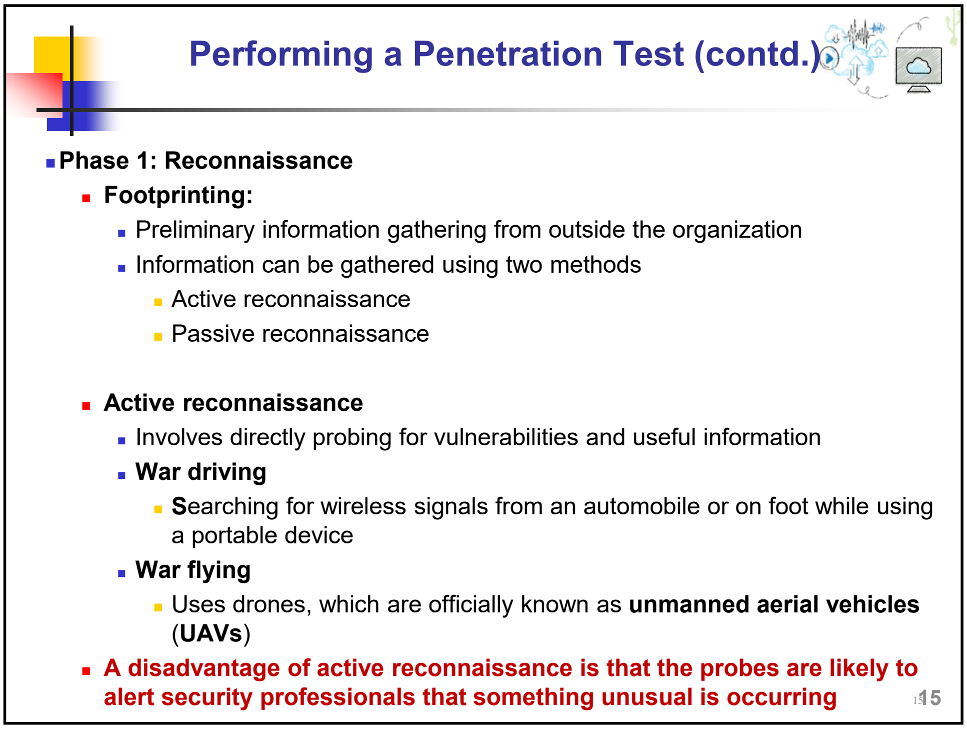
- **Cleanup**
  - The pen tester must ensure that everything related to the pen test has been removed
  - Involves removing all software agents, scripts, executable binaries, temporary files, and backdoors from all affected systems
  - Any credentials that were changed should be restored
  - Any usernames 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

- **Categories for rules of engagement:**
  - Timing
  - Scope
  - Authorization
  - Exploitation
  - Communication
  - **Cleanup**
  - **Reporting**

Performing a Penetration Test

- ***Performing a successful pen test involves***
  - *Determination*
  - *Resolve*
  - *Perseverance*

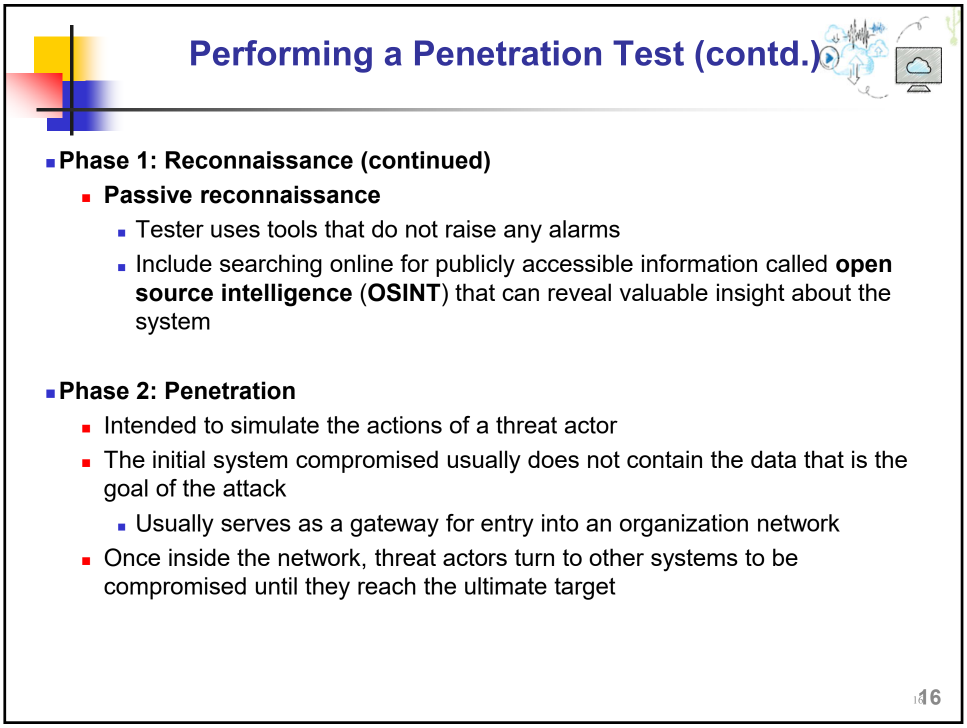
- **Two phases:**
  - Reconnaissance
  - Penetration



Performing a Penetration Test (contd.)

- **Phase 1: Reconnaissance**
  - **Footprinting:**
    - Preliminary information gathering from outside the organization
    - Information can be gathered using two methods
      - Active reconnaissance
      - Passive reconnaissance
  - **Active reconnaissance**
    - Involves directly probing for vulnerabilities and useful information
    - **War driving**
      - **S**earching 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**

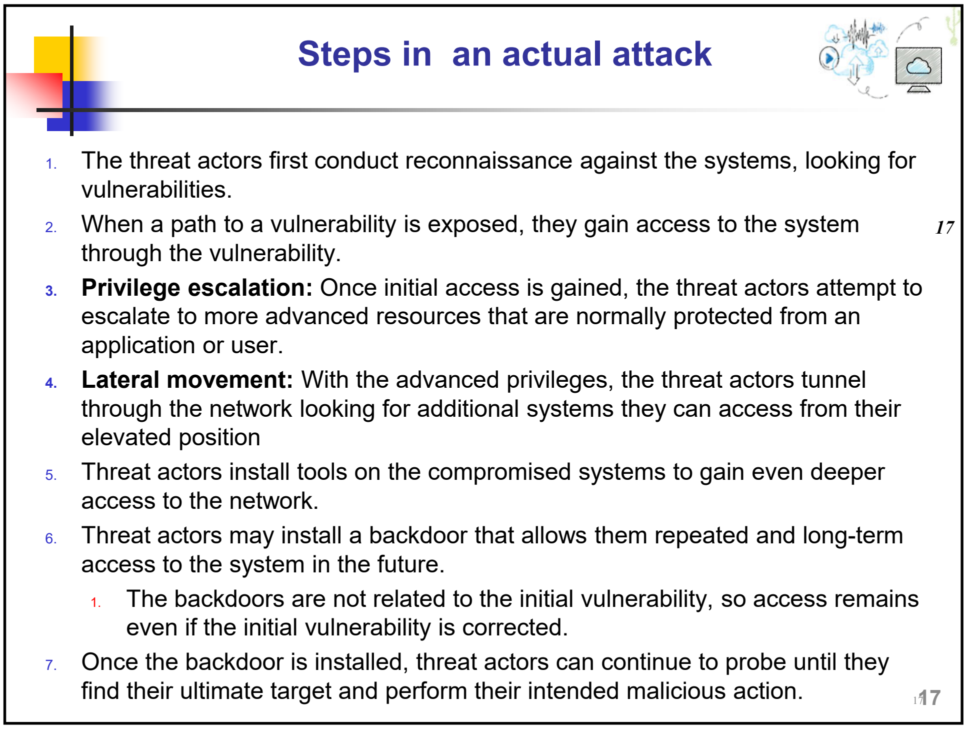
15



Performing a Penetration Test (contd.)

- **Phase 1: Reconnaissance (continued)**
  - **Passive reconnaissance**
    - Tester uses tools that do not raise any alarms
    - Include searching online for publicly accessible information called **open source intelligence** (**OSINT**) that can reveal valuable insight about the system
- **Phase 2: Penetration**
  - 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
    - 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

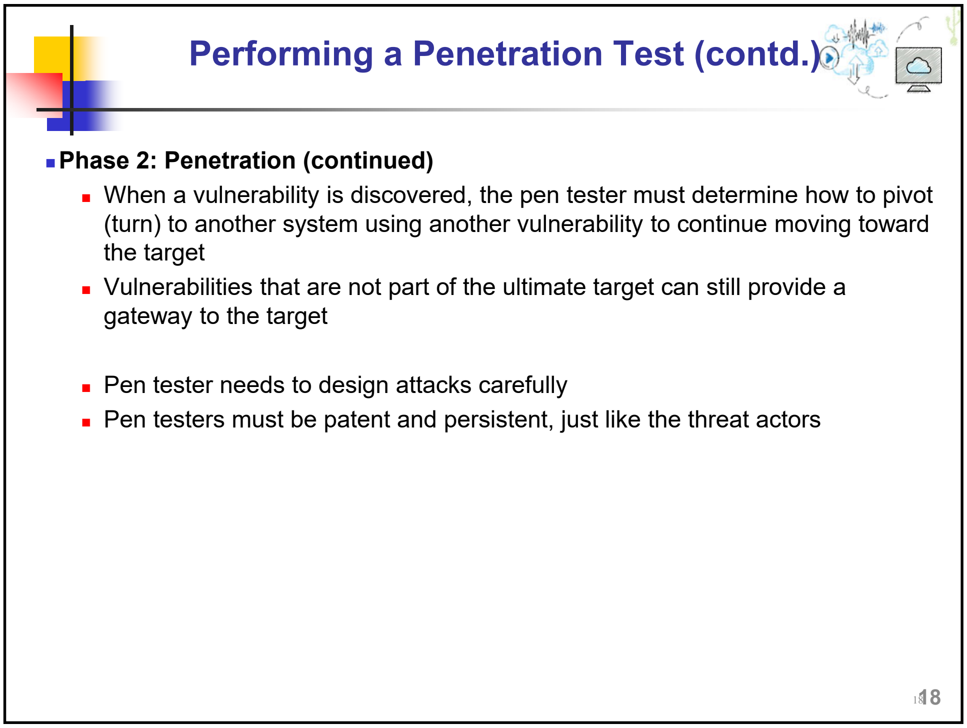
16



Steps in an actual attack

1. The threat actors first conduct reconnaissance against the systems, looking for vulnerabilities.
2. When a path to a vulnerability is exposed, they gain access to the system through the vulnerability. *17*
3. **Privilege escalation:** Once initial access is gained, the threat actors attempt to escalate to more advanced resources that are normally protected from an application or user.
4. **Lateral movement:** With the advanced privileges, the threat actors tunnel through the network looking for additional systems they can access from their elevated position
5. Threat actors install tools on the compromised systems to gain even deeper access to the network.
6. Threat actors may install a backdoor that allows them repeated and long-term access to the system in the future.
    1. The backdoors are not related to the initial vulnerability, so access remains even if the initial vulnerability is corrected.
7. Once the backdoor is installed, threat actors can continue to probe until they find their ultimate target and perform their intended malicious action.

17



Performing a Penetration Test (contd.)

- **Phase 2: Penetration (continued)**
    - 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 tester needs to design attacks carefully
    - Pen testers must be patent and persistent, just like the threat actors

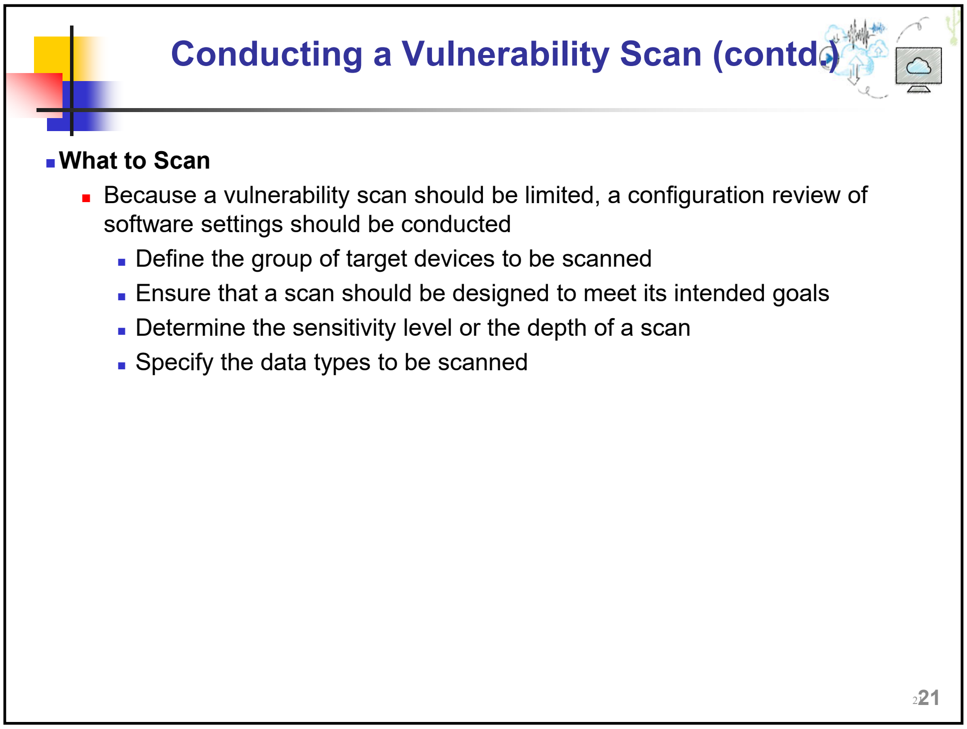
18

Vulnerability Scanning

- **Vulnerability scanning**
  - A frequent and ongoing process that continuously identifies vulnerabilities and monitors cybersecurity progress
  - 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

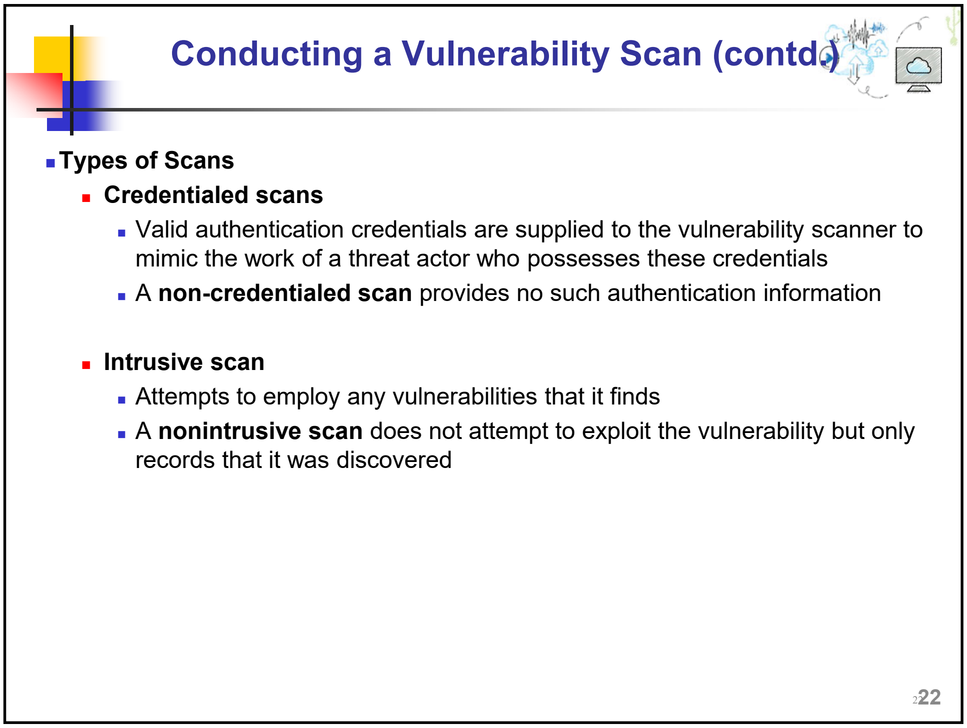
Conducting a Vulnerability Scan

- **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



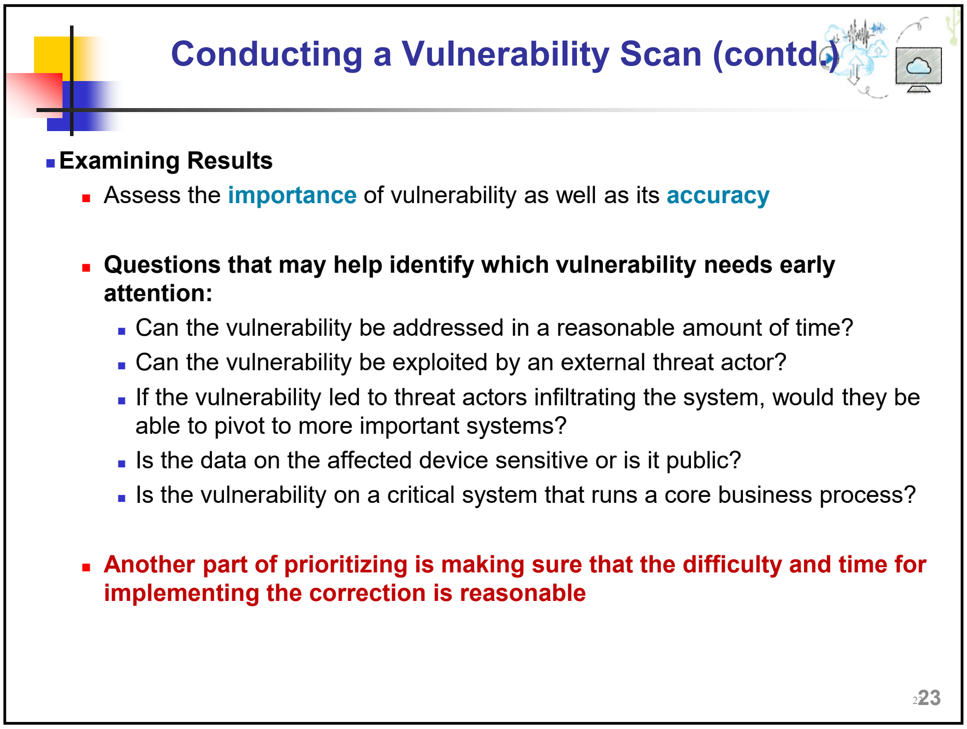
Conducting a Vulnerability Scan (contd.)

- **What to Scan**
  - 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



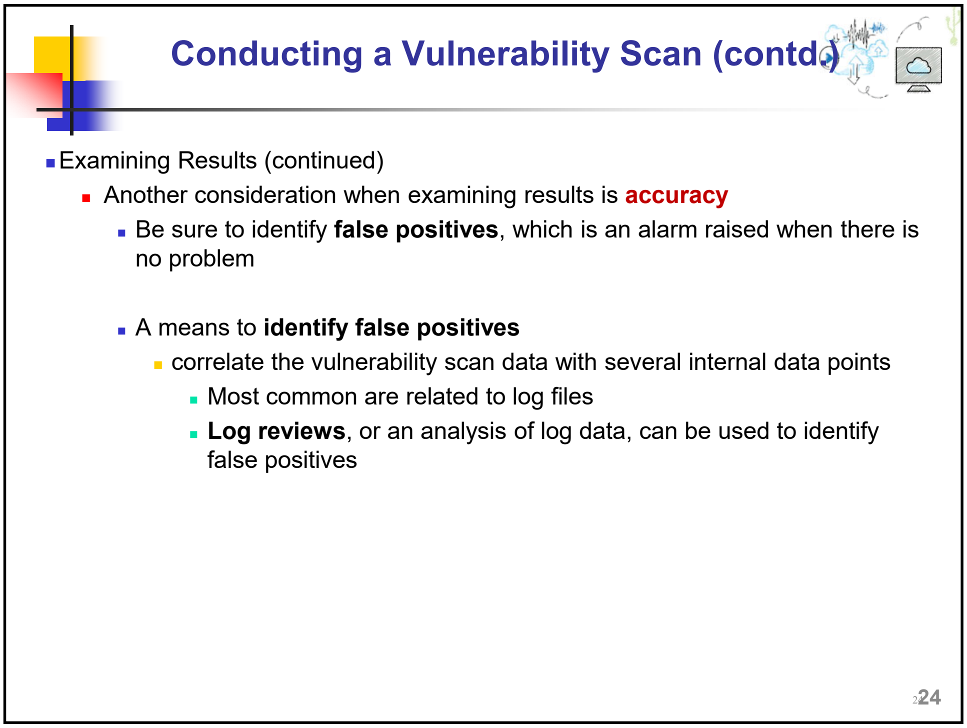
Conducting a Vulnerability Scan (contd.)

- **Types of Scans**
  - **Credentialed scans**
    - 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
  - **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



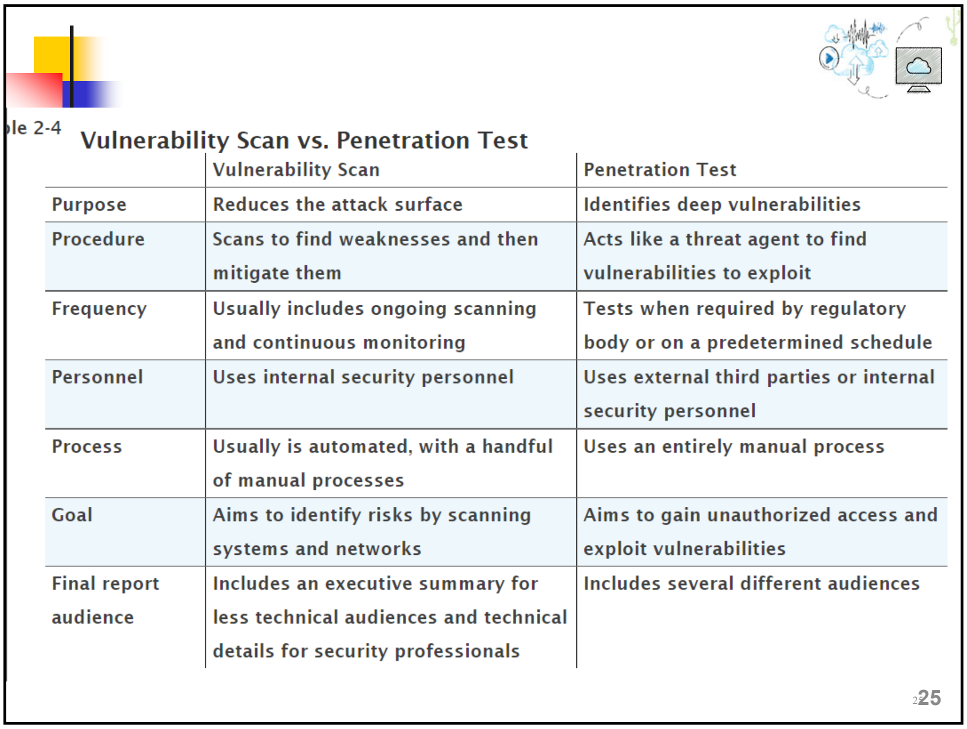
Conducting a Vulnerability Scan (contd.)

- **Examining Results**
  - 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**



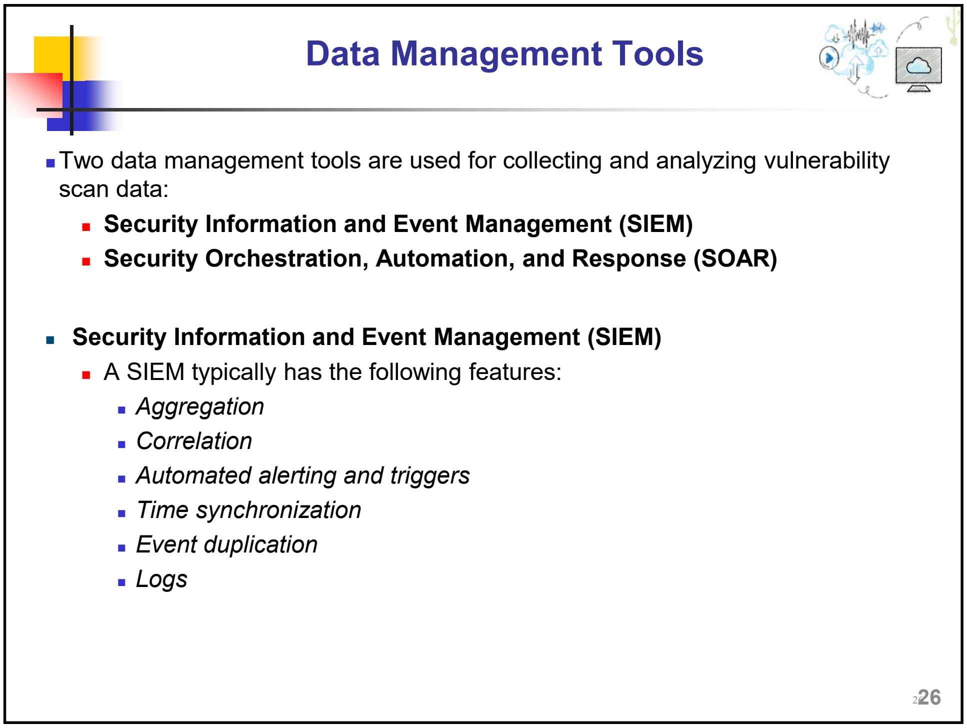
Conducting a Vulnerability Scan (contd.)

- 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**
      - 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



le 2-4 Vulnerability Scan vs. Penetration Test

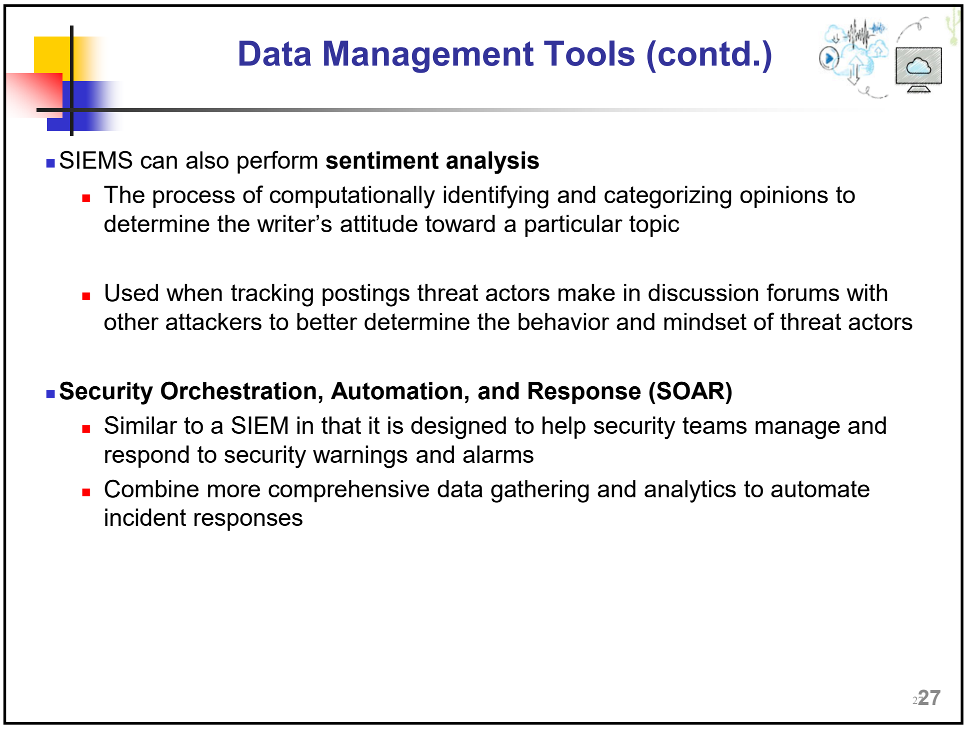
	Vulnerability Scan	Penetration Test
Purpose	Reduces the attack surface	Identifies deep vulnerabilities
Procedure	Scans to find weaknesses and then mitigate them	Acts like a threat agent to find vulnerabilities to exploit
Frequency	Usually includes ongoing scanning and continuous monitoring	Tests when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



Data Management Tools

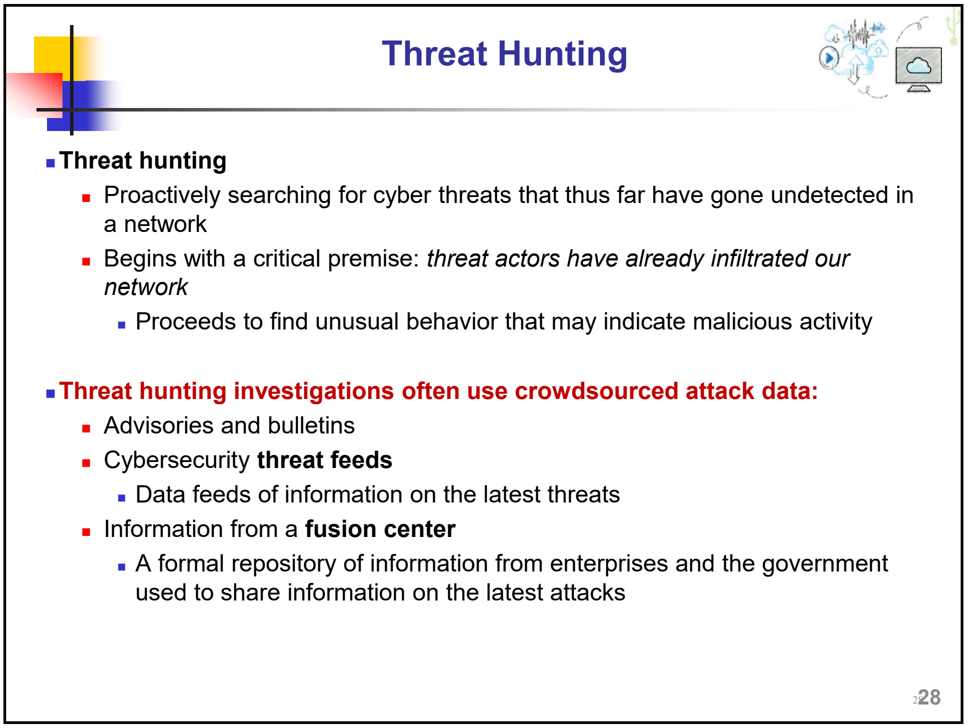
- Two data management tools are used for collecting and analyzing vulnerability scan data:
  - **Security Information and Event Management (SIEM)**
  - **Security Orchestration, Automation, and Response (SOAR)**

- **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 (contd.)

- SIEMS can also perform **sentiment analysis**
  - The process of computationally identifying and categorizing opinions to determine the writer's attitude toward a particular topic
  - 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)**
  - Similar to a SIEM in that it is designed to help security teams manage and respond to security warnings and alarms
  - Combine more comprehensive data gathering and analytics to automate incident responses



Threat Hunting

- **Threat hunting**
  - Proactively searching for cyber threats that thus far have gone undetected in a network
  - Begins with a critical premise: *threat actors have already infiltrated our network*
    - Proceeds to find unusual behavior that may indicate malicious activity
- **Threat hunting investigations often use crowdsourced attack data:**
  - 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

Cybersecurity Resources

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

Frameworks

- A **cybersecurity framework**
  - A series of documented processes used to define policies and procedures for implementing and managing security controls in an enterprise environment

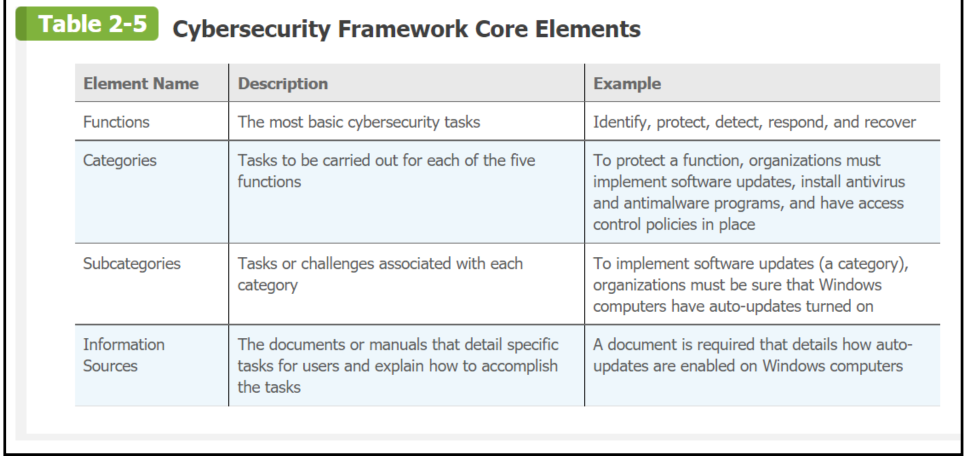
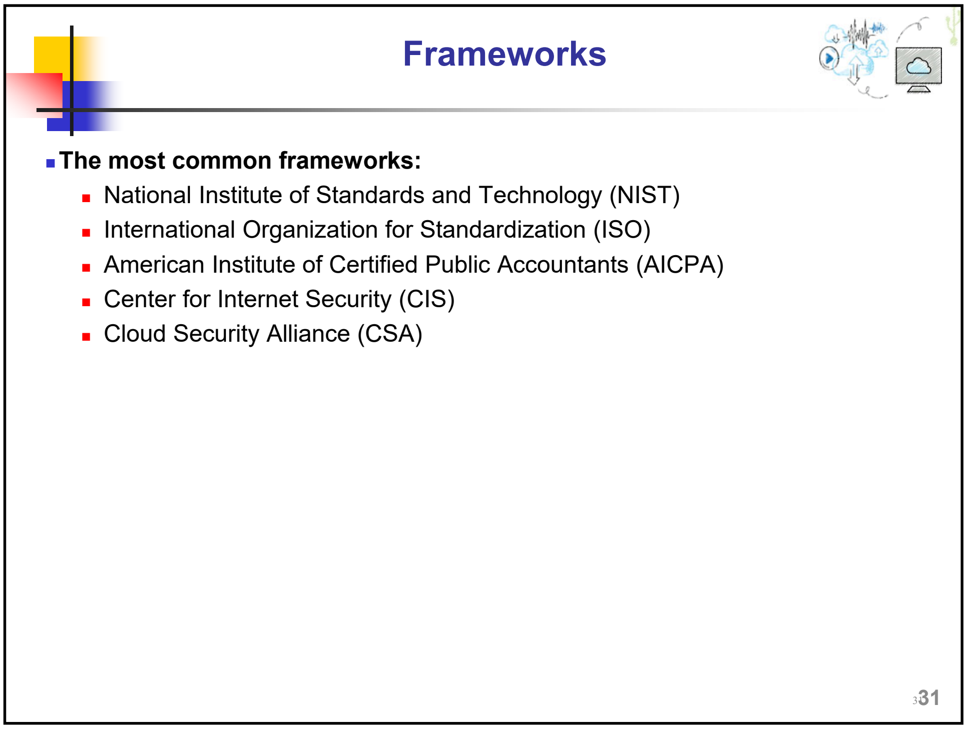


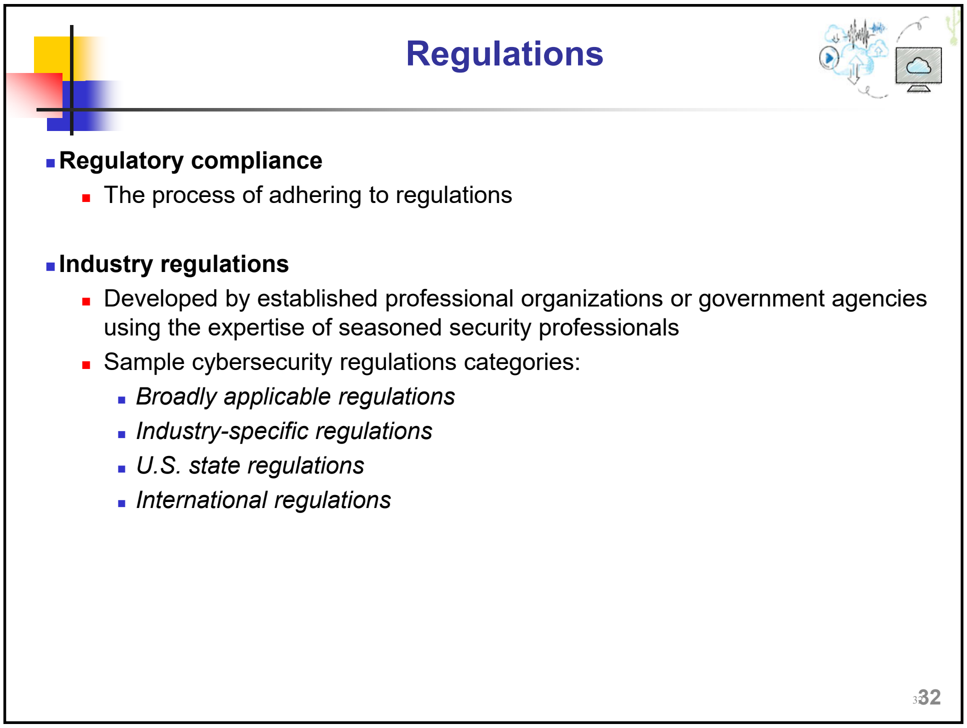
Table 2-5 Cybersecurity Framework Core Elements

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



Frameworks

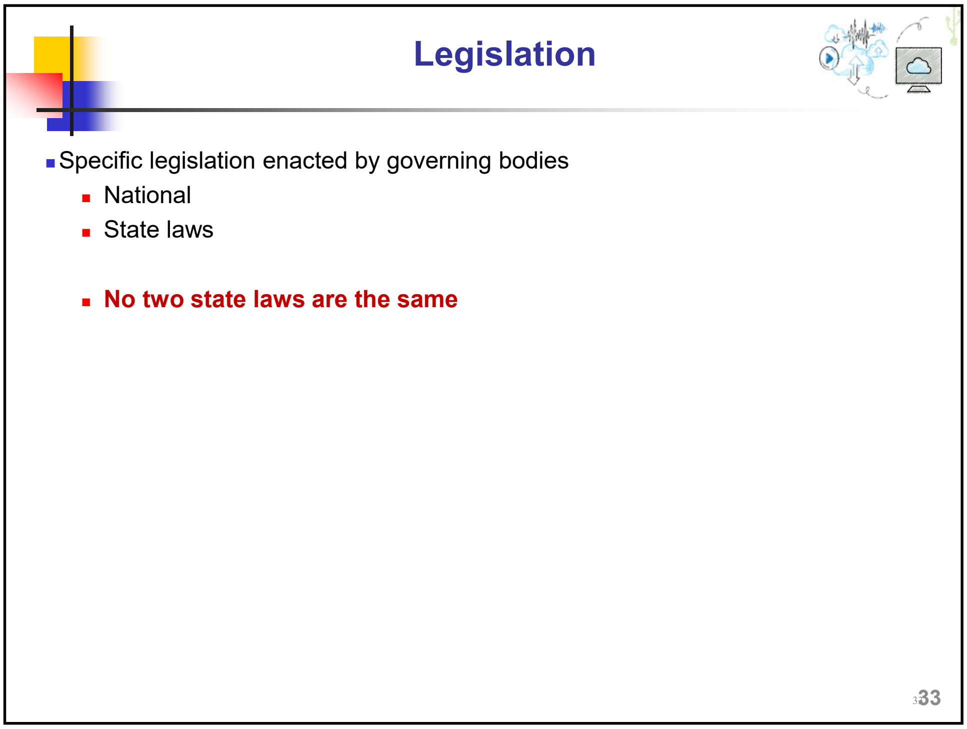
- **The most common frameworks:**
  - National Institute of Standards and Technology (NIST)
  - International Organization for Standardization (ISO)
  - American Institute of Certified Public Accountants (AICPA)
  - Center for Internet Security (CIS)
  - Cloud Security Alliance (CSA)



Regulations

- **Regulatory compliance**
  - The process of adhering to regulations

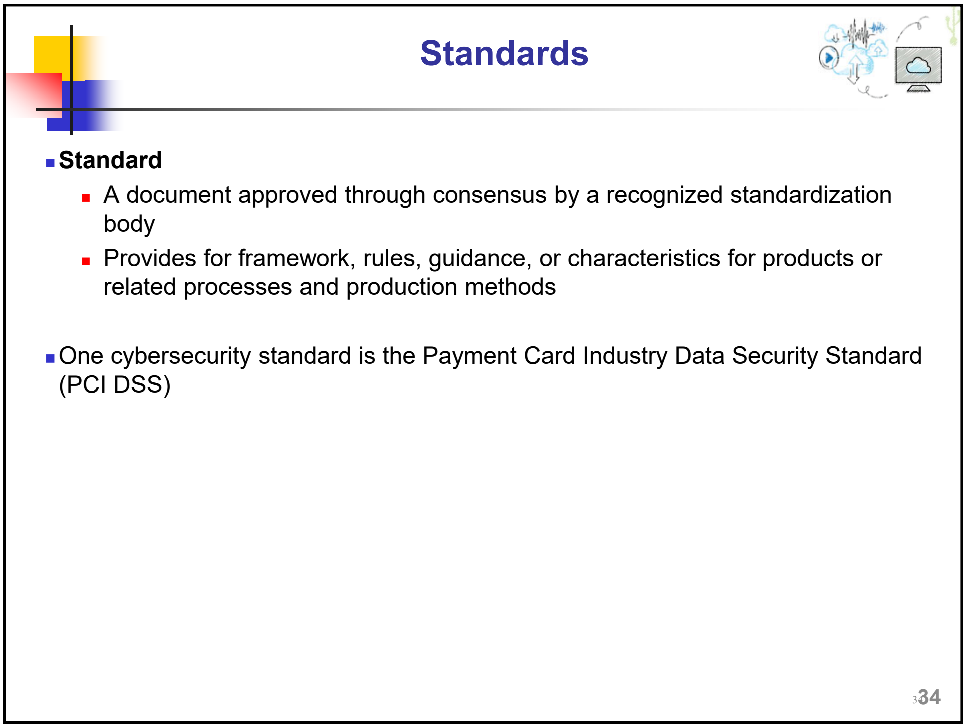
- **Industry regulations**
  - Developed by established professional organizations or government agencies using the expertise of seasoned security professionals
  - Sample cybersecurity regulations categories:
    - *Broadly applicable regulations*
    - *Industry-specific regulations*
    - *U.S. state regulations*
    - *International regulations*



Legislation

- Specific legislation enacted by governing bodies
  - National
  - State laws

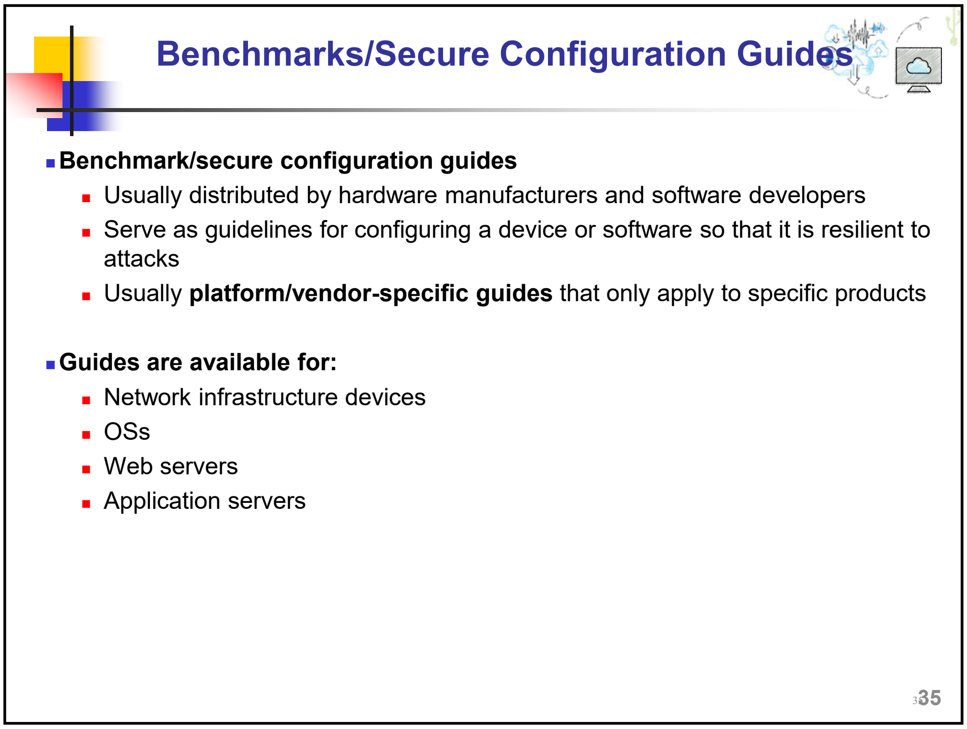
  - **No two state laws are the same**



Standards

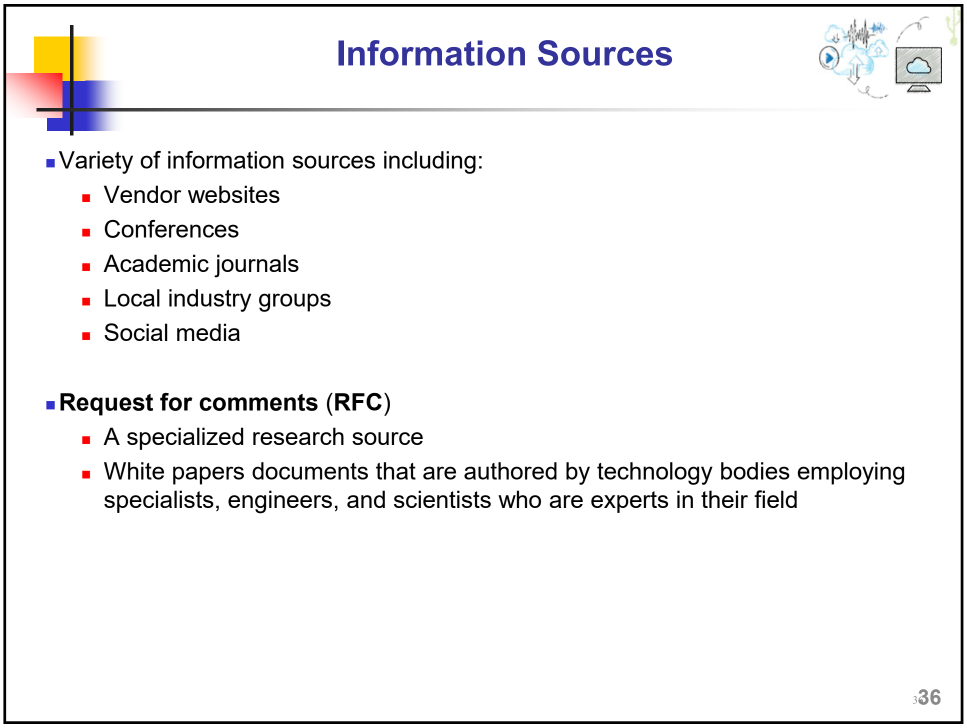
- **Standard**
  - A document approved through consensus by a recognized standardization body
  - Provides for framework, rules, guidance, or characteristics for products or related processes and production methods

- One cybersecurity standard is the Payment Card Industry Data Security Standard (PCI DSS)



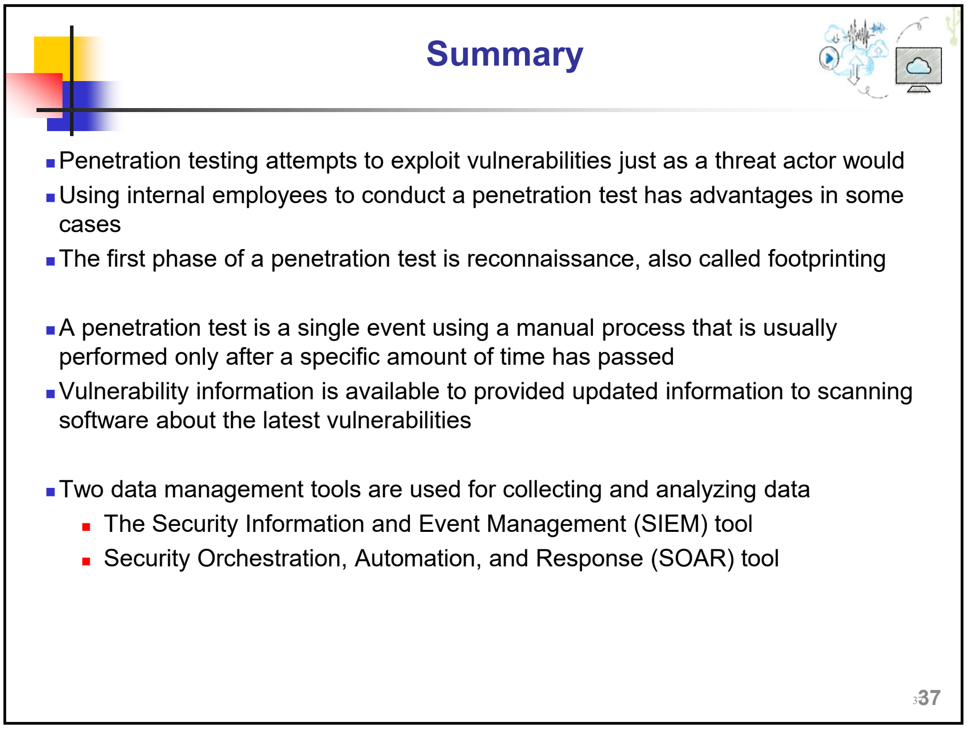
Benchmarks/Secure Configuration Guides

- **Benchmark/secure configuration guides**
  - Usually distributed by hardware manufacturers and software developers
  - Serve as guidelines for configuring a device or software so that it is resilient to attacks
  - 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

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

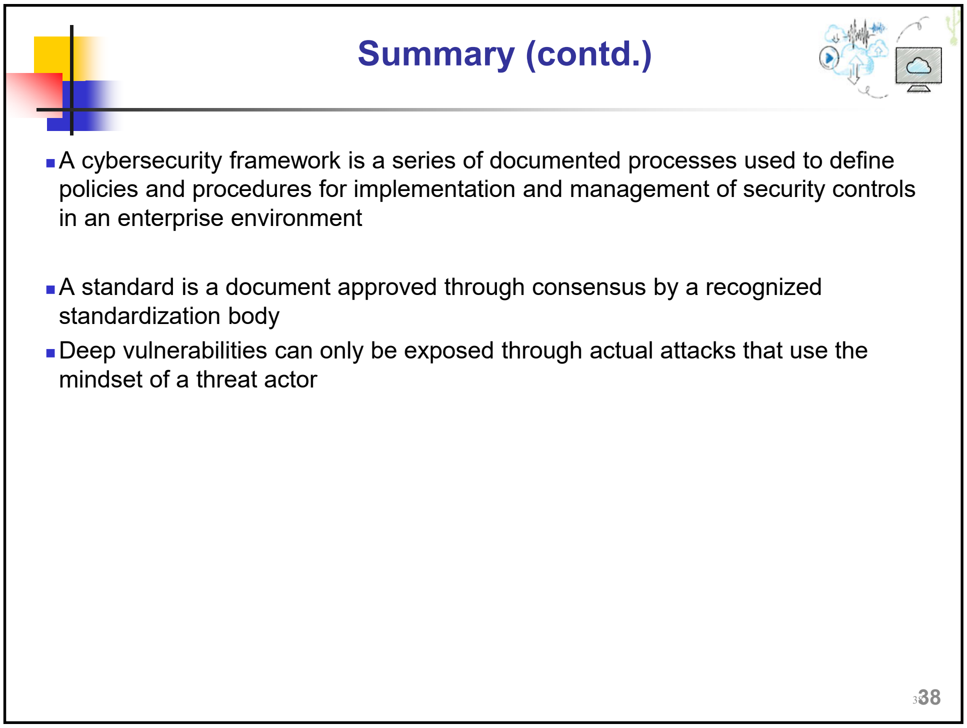


Summary

- 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 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
- Vulnerability information is available to provided updated information to scanning software about the latest vulnerabilities

- Two data management tools are used for collecting and analyzing data
  - The Security Information and Event Management (SIEM) tool
  - Security Orchestration, Automation, and Response (SOAR) tool



Summary (contd.)

- 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

- 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

- InterestingDifficult
- ProposedQuiz

39