Chapter 12: Vulnerability Management

Vulnerability Scanning

- Vulnerability scanning is an examination of the organization’s security to uncover weaknesses
- Studying vulnerability scanning involves understanding the following:
  - The basics of a vulnerability scan
  - The sources of data needed for a scan
  - Knowing the decisions that must be made regarding scans
  - Running a scan and analyzing scan reports
  - Addressing the reported vulnerabilities

Vulnerability Scan Basics

- A **vulnerability scan** is an ongoing automated process used to identify weaknesses and monitor information security progress
- One specialized type of vulnerability scan examines applications
  - Many applications use **open-source libraries**
  - Because these libraries are not owned and controlled by a single entity, attackers frequently infect open-source libraries with malware
- Analyzing apps can be done using **package monitoring** tools, which continuously analyze apps for vulnerabilities

Vulnerability Scan Basics

- The following are some challenges associated with vulnerability scanning:
  - Volume of scan data
  - Identification of vulnerabilities
  - Technical limitations
  - Remediations

Sources of Threat Intelligence

- **Threat intelligence** is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors
- Some threat intelligence data is owned by an entity and is not available to outsiders
- Some large enterprises hire security researchers who uncover security bugs in their products (called a **bug bounty program**)
- The web has three levels: the **clear web**, the **deep web**, and the **dark web**

Dark Web


Google
Bing
yahoo!
Clear web
Deep web
Dark web
Records
Academic
Medical
Legal
Scientific
Government
Subscription-only information
Databases
Organization-specific information
Illegal activities
Romolo Tavani/Shutterstock.com

Sources of Threat Intelligence

- Proprietary vulnerability scanners offer their own threat intelligence as a paid subscriptions service (known as **third-party sources**)
- **Information sharing organizations** gather, collate, analyze, and then distribute threat intelligence
- Sharing threat intelligence has the following advantages:
  - Organizations can leverage the collective knowledge, experience, and capabilities of other organizations
  - An organization can enrich its own existing information and make it more actionable

Sources of Threat Intelligence

- A typical threat intelligence information sharing center is the U.S. Dept of Homeland Security Cyber Information Sharing and Collaboration Program (CISCP), which includes the following services:
  - Analyst-to-analyst technical exchanges
  - CISCP analytical products
  - Cross-industry orchestration
  - Digital malware analysis

Sources of Threat Intelligence

- **Automated Indicator Sharing** (**AIS**) enables the exchange of cyber threat indicators between parties through computer-to-computer communication
- The following tools facilitate AIS:
  - **Structured Threat Information Expression** (**STIX**)
  - **Trusted Automated Exchange of Intelligence Information** (**TAXII**)

Sources of Threat Intelligence

- **Open-Source Intelligence** (**OSINT**) is threat intelligence data that has been legally gathered from free and public sources
- OSINT is often used to create cybersecurity **threat maps** that illustrate cyber threats overlaid on a diagrammatic representation of a geographical area
- Threat maps help in visualizing attacks and provide a limited amount of context of the source and the target countries, the attack types, and historical and near real-time data about threats

Threat Map


Check Point
THREATCLOUD
LIVE CYBER THREAT MAP
96,578,678 ATTACKS ON THIS DAY
DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW
TOP TARGETED COUNTRIES
TOP TARGETED INDUSTRIES
TOP MALWARE TYPES
Turkey
India
Brazil

Question?

- Why are open-source libraries vulnerable?

Answer

- Why are open-source libraries vulnerable?
- Because these libraries are not owned and controlled by any single entity, attackers frequently infect open-source libraries with their malware. The malware then replicates whenever a programmer downloads and uses that library in their application.

Scanning Decisions

- What Should Be Scanned?
  - Before performing a vulnerability scan, it is important to know the value of specific data
  - Data should be classified into groups of data that need similar protections
  - Examples of classifications include confidential, private, sensitive, critical, public, and restricted
  - Once data has been identified, its value can be determined, and the type and frequency of a vulnerability scan can be calculated

Scanning Decisions

Asset	Description
Network	Can identify possible network security attacks and vulnerable systems on wired networks
Endpoint	Can locate and identify vulnerabilities in servers, workstations, or other network endpoints and provide visibility into the configuration settings and patch history of the endpoints
Wireless network	Can identify rogue access points and validate that the wireless network is secure
Database	May identify the weak points in a database
Applications	Web applications and other software assets can be scanned in order to detect known software vulnerabilities and erroneous configurations

Scanning Decisions

- How Should It Be Scanned?
  - **Active scanning** sends test traffic transmissions into the network and monitors the responses of the endpoints
  - **Passive scanning** does not send any transmissions but instead only listens for normal traffic to learn the needed information
  - Active scanning can accelerate the collection of data
  - Not all parts of a network may always be available, which can limit the ability to passively monitor traffic

Scanning Decisions

- How Should It Be Scanned?
  - An **internal vulnerability scan** is performed from the vantage point inside the internal network
    - This has the primary benefit of identifying at-risk systems
  - An **external vulnerability scan** is performed from the vantage outside the network
    - It targets specific IP addresses that are within the network to identify vulnerabilities

Scanning Decisions

- When Should It Be Scanned?
  - Spread out scans to run at specific times
  - Move the scans to “off hours” such as nights or weekends
  - Specific regulations can dictate how frequently a vulnerability scan must be preformed
  - The organization’s tolerance for exposure to a vulnerability is known as **risk appetite**
    - Systems with low-risk appetite may be scanned more frequently

Running a Vulnerability Scan

- Vulnerability scanning tools include the following:
  - **Open Vulnerability Assessment Scanner (OpenVAS)**
  - **Invicti** is a tool for scanning website applications for vulnerabilities
  - **Nexpose**
  - **Nessus**
- After selecting a vulnerability scanning tool, the software plug-ins need to be updated and the vulnerability and threat feeds need to be accessed

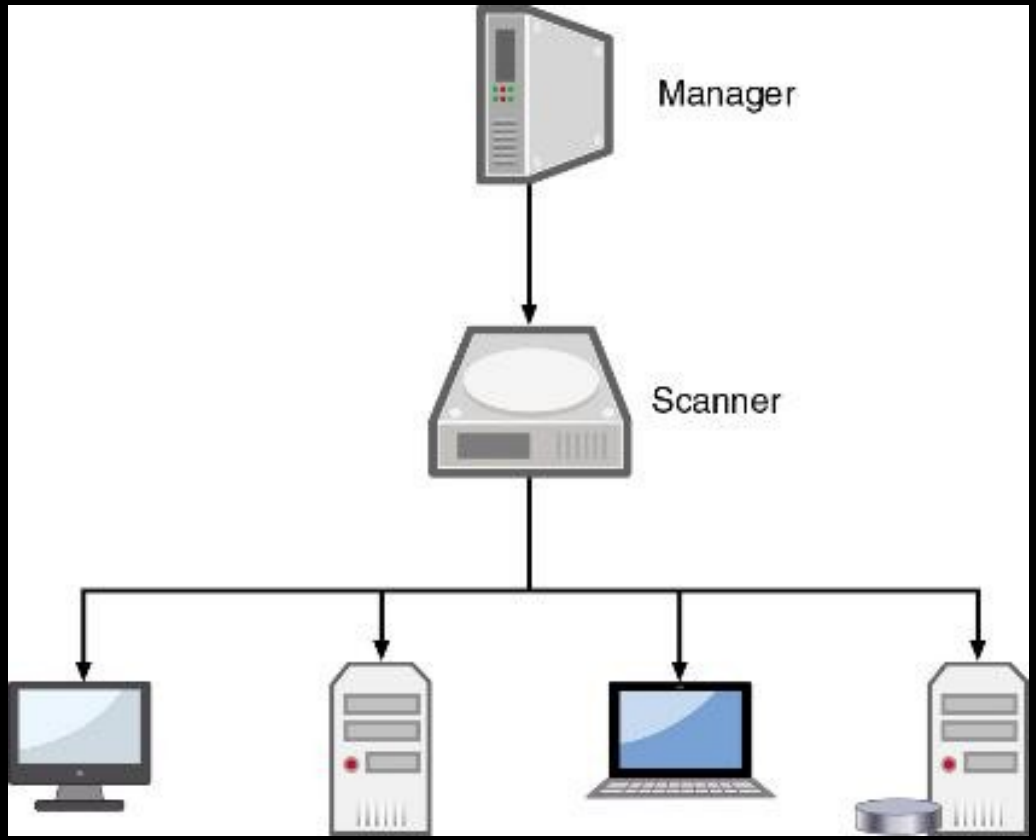
Running a Vulnerability Scan

- The **scope** of a vulnerability scan is the target devices to be scanned
- The scope can be set by using **environmental variables**, which are variables whose values are set outside the program
  - An environmental variable can point to a directory that is to be excluded from a scan
- The **sensitivity level** is the depth of a scan (what type of vulnerabilities are being searched for?)
- You can also specify the data types to be scanned

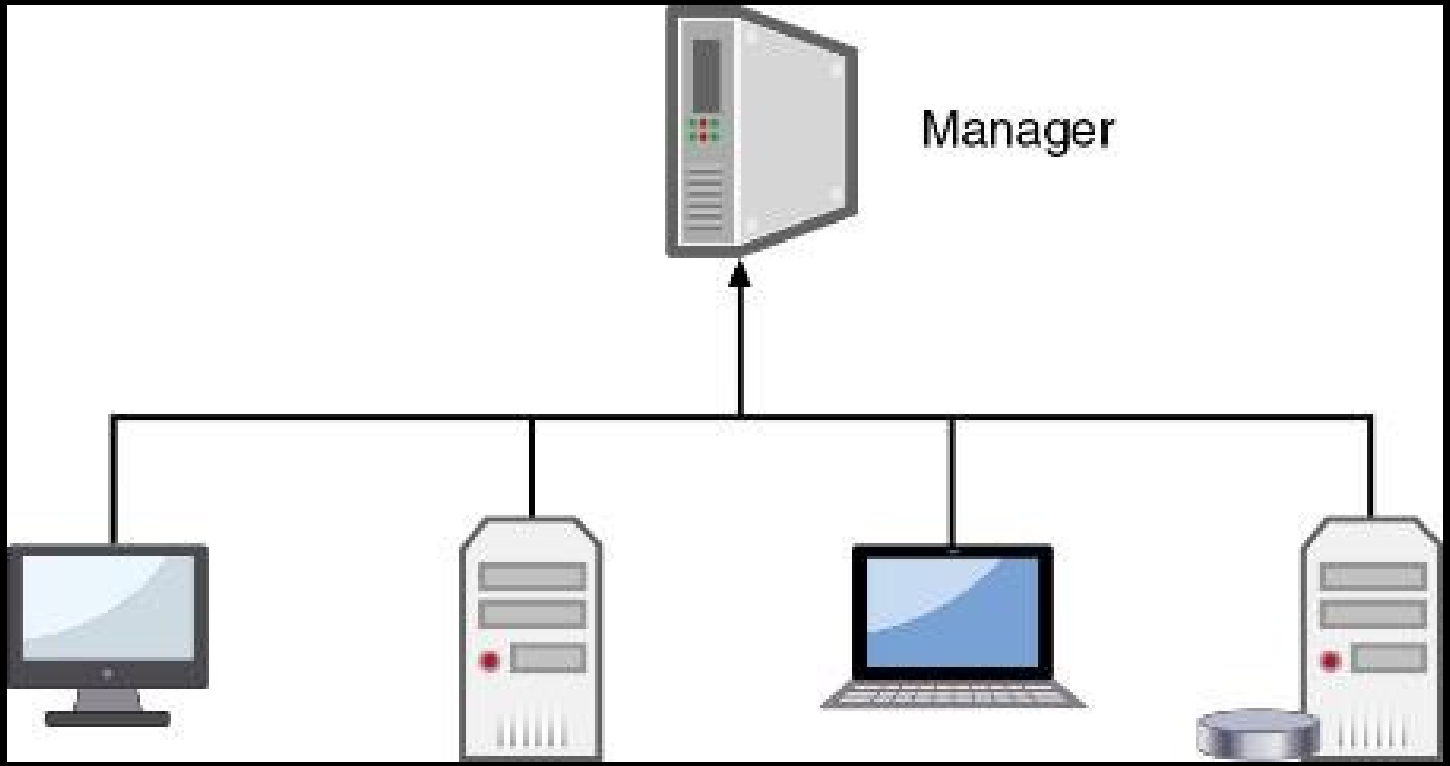
Running a Vulnerability Scan

- Network security would prevent the vulnerability scanner from being able to accurately examine the devices on the network
- Testers should have permissions from internal supervisors to software used to access approved systems
- When a scanner manager connects to a scanner engine that probes each system, it is known as **server-based** (pull) **scanner technology**
- When a software agent resides on a system and sends their information back to the manager, this is known as **agent-based** (push) **scanner technology**

Server-Based Scanner Technology



Agent-Based Scanner Technology



Running a Vulnerability Scan

- Two types of scans include the following:
  - 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

Analyzing Vulnerability Scans

- Vulnerability scan results should be validated for confirmation
- If the scan were 100 percent accurate, then the organization would know that a future attack would accurately trigger an alarm (**true positive**)
- The absence of an attack would not trigger an alarm (**true negative**)
- A **false positive** is an alarm that is raised when there is no problem
- A **false negative** is the failure to raise an alarm when there is an issue

Analyzing Vulnerability Scans

Audience	Level of report	Explanation
Management	A general report that outlines the impact to the organization	Management will be interested in how the latest scan compares with previous scans, how serious are the vulnerabilities, and how long it will take to addresses them
System and network engineers	A technical report that outlines what needs to be addressed	Engineers will want a listing of the devices with vulnerabilities and specific details regarding how to fix the problems
Application developers	A report that lists the applications that contain vulnerabilities and what those vulnerabilities are	Developers will want to know which of their applications are vulnerable and as much as possible the location of that vulnerability in their code
Security teams	A very specific report as it relates to the technical security details	Security teams want to know what systems were vulnerable, the details as to why they could be exploited, and what remediation steps are necessary

Addressing Vulnerabilities

- To remediate vulnerabilities, the first step is to prioritize vulnerabilities
- Criteria used for prioritizing vulnerabilities includes the following:
  - **Common Vulnerability Scoring System** (**CVSS**), which contains numeric scores generated using a complex formula that considers such variables as the access vector, attack complexity, authentication, confidentiality of data, and integrity and availability
  - **Common Weakness Enumeration** (**CWE**), which ranks based on a **vulnerability classification** system

Addressing Vulnerabilities

- Once vulnerabilities are prioritized, take the following action steps:
  - Patch and harden
  - Address difficult vulnerabilities
  - Identify exceptions and exemptions
  - Analyze network segmentation
  - Verify mitigation

Question?

- Levi needs to specify which devices need to be included in the next vulnerability scan. What parameter must he set?

Answer

- Levi needs to specify which devices need to be included in the next vulnerability scan. What parameter must he set?
- Scope, sets the parameter of which devices need to be scanned.

Audits and Assessments

- An **audit** is an examination of results to verify their accuracy
- An **assessment** is a judgement made about those results
  - It involves actions necessary to make what was assessed brought back into conformity with the required standards
- Audits and assessments can be internal and external

Internal Audits

- **Internal audits** (self-assessments) are performed by company employees and are used to identify the actions needed to put what was assessed back into **compliance** to mandated standards
- An audit committee is one of the major operating committees of a company’s board of directors
  - It oversees the organization’s financial statements and reporting by providing proof (**attestation**) that the organization is in compliance with required standards

External Assessments

- **External assessments** are performed by professionals from outside the organization
  - These professionals perform an **independent third-party audit**
- Their assessments of the organization are often to ensure that the company is compliant with **regulatory** requirements as set forth by outside bodies

Penetration Testing

- A **penetration test** attempts to uncover vulnerabilities and then exploit them
- A vulnerability scan is considered a **defensive** assessment, and a penetration test is an **offensive** assessment that probes the system for weakness
- Penetration testing that probes for weaknesses in physical security controls are called **physical penetration testing**
  - Those that probe both technical and physical weaknesses are **integrated penetration tests**

Penetration Testing

- Using internal employees for penetration testing offers the following advantages:
  - Little or no additional cost, the test can be conducted much more quickly, it can be used to enhance the training of employees and raise awareness of security risks
- Internal tests can have several disadvantages:
  - Inside knowledge, lack of expertise, and reluctance to reveal a vulnerability

Penetration Testing

- Contracting with an external third-party pen testing consultant offers the following advantages:
  - Expertise
  - Credentials
  - Experience
  - Focus

Penetration Testing

- One of the first tasks of testers is to perform preliminary information gathering from outside the organization
  - This reconnaissance is called **footprinting**
- **Active reconnaissance** involves directly probing for vulnerabilities and useful information
- **Passive reconnaissance** occurs when the tester uses tools that do not raise any alarms

Pen Test vs Vulnerability Scan

	Vulnerability scan	Penetration test
Purpose	Reduce attack surface	Identify deep vulnerabilities
Procedure	Scan to find weaknesses and then mitigate	Act like a threat agent to find vulnerabilities to exploit
Frequency	Usually ongoing scanning and continuous monitoring	When required by regulatory body or on a predetermined schedule
Personnel	Internal security personnel	External third parties or internal security personnel
Process	Usually automated with handful of manual processes	Entirely manual process
Goal	Identify risks by scanning systems and networks	Gain unauthorized access and exploit vulnerabilities
Final report audience	Executive summary for less technical audience, technical details for security professionals	Several different audiences

Question?

- Carly has been asked to explore part of the web that is the domain of threat actors to look for information about the latest types of attacks. What area of the web will he explore?

Answer

- Carly has been asked to explore part of the web that is the domain of threat actors to look for information about the latest types of attacks. What area of the web will he explore?
- The dark web is like the deep web in that it is beyond the reach of a normal search engine, but it is the domain of threat actors. Using special software such as Tor or I2P (Invisible Internet Project) will mask the user's identity to allow for malicious activity such as selling drugs and stolen personal information and buying and selling malicious software used for attacks.