Chapter 5: Security Assessment and Testing

# Vulnerability Management

Use Vulnerability scanning to detect new vulnerabilities as they arise, then assess the priority level.

## Identifying Scan Targets

Identify the systems that will be covered by the vulnerability scanned, you must ask these questions:

* What is the data classification of the information stored, processes, or transmitted by the system?
* Is the system exposed to the internet or other public or semipublic networks?
* What services are offered by the system?
* Is the system a production, test, or development system?

**Asset inventory**: is a list of all the hardware, software, and data that an organization owns or uses.

**asset criticality** refers to the level of importance a particular asset holds to an organization's operations.

## Determining Scan Frequency

Vulnerability scanning tools are usually automated and companies set how many times the tool scans for vulnerability. Automated alerts should also be configured.

Different factors to influence the frequency of vulnerability scans:

* **Risk Appetite:** The willingness to tolerate risks.
* **Regulatory Requirements:** Rules and guidelines that businesses must follow to comply with laws and regulations.
* **Technical Constraints** may limit the frequency.
* **Business Constraints:** Can limit the frequency if it is a high season or a low season.
* **Licensing Limitations**

## Configuring Vulnerability Scans

The parameters of the scan like scheduling and types of reports. Administrators may target a certain area or types of tests. Making sure everything is up to date.

## Scan Sensitivity Levels

Configuring the settings determines the type of test intended to be done. Administrators need to choose which plug-ins to use as it can save time and may affect testing. Best way around this problem is to use test environments.

## Supplementing Network Scans

Doing scans via the network gives the test a more realistic vantage point.

**Credentialed Scans:** Only retrieve information from target servers and has privilege access.

Server-Based Scanning uses **Agent-Based Scanning** which sends agents into every server and conducts scans from inside out.

## Scan Perspective

Conducts the scan from different locations on the network, providing a different view into vulnerabilities.

Internal scans might run from a scanner on the general network providing the view that a malicious insider might encounter.

Scanners in the datacenter are the most accurate and most important.

Controls that might affect a scan results:

* Firewall settings
* Network segmentation
* Intrusion Detection Systems (IDSs)
* Intrusion Prevention Systems (IPSs)

## Scanner Maintenance

Make sure Scanners are up to date.

## Scanner Software

Patching scanners protect organizations from scanner vulnerabilities.

## Vulnerability Plug-in Feeds

Update Plug-ins regularly.

Security Content Automation Protocol (SCAP) Standards:

* Common Configuration Enumeration (CCE): Discussing system configuration issues.
* Common Platform Enumeration (CPE): Describing product names and versions.
* Common Vulnerabilities and Exposure (CVE): Describing security-related software flaws.
* Common Vulnerability Scoring Systems (CVSS): Measuring and describing the severity of the security-related software flaws.
* Extensible Configuration Checklist Description Format (XCCDF): A language for specifying checklists and reporting checklist results.
* Open Vulnerability and Assessment Language (OVAL): A language for specifying low-level testing procedures used by checklists.

## Vulnerability Scanning Tools

Organizations need a network vulnerability scanner, application scanner, and a web application scanner.

## Infrastructure Vulnerability Scanning

Network scanners can probe a wide range of network-connected devices and find their vulnerabilities.

## Application Testing

These tools are usually used during the software development process.

3 common techniques:

* **Static Testing**: Analyze the code without execution.
* **Dynamic Testing:** Execute the code as part of the test.
* **Interactive Testing:** Does static and dynamic testing.

## Web Application Scanning

Scans web applications. Looks for SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) vulnerabilities.

## Reviewing and Interpreting Scan Reports

These reports provide detailed information about each vulnerability that appears.

Report Page Structure/Sections:

* Top of the page vulnerability type.
* “Description” of the vulnerability.
* “Solution” for vulnerability.
* “See Also” references to read.
* “Output” returns information returned by the remote system when probed for the vulnerability.
* “Port/Host” provides details on the servers that contain a vulnerability.
* “Vulnerability Information” is the type of vulnerability known to the community.
* “Risk Information” assessing the severity of the vulnerability.
* “Plugin Details” provides information on the plug-in that found the vulnerability.

## Understanding Common Vulnerability Scoring System (CVSS)

A component of SCAP that asses the severity of the vulnerability.

## Attack Vector Metric (AV)

Table

## Attack Complexity Metric (AC)

Table

## Privileges Required Metric (PR)

Table

## User Interaction Metric (UI)

Table

## Confidentiality Metric (C)

Table

## Integrity Metric (I)

Table

## Availability Metric (A)

Table

## Scope Metric (S)

Table

## Interpreting the CVSS Vector

Each metric will have a score listed.

## Summarizing CVSS Scores

All the scores are calculated and added up to show the severity of a vulnerability.

## Calculation the Impact Sub-Score (ISS)

ISS = 1 – [(1-Confidentiality) \*(1-Integrity) \*(1-Availability)]

## Calculating the Impact Score

If the Scope metric (S) is unchanged: Impact = ISS \* 6.42

If the Scope metric (S) is changed: Impact = 7.52 \* (ISS – 0.029) – 3.25 \* (ISS – 0.02)15

## Calculating the Exploitability Score

Exploitability = 8.22 \* AV \* AC \* PR \* UI

## Calculating the Base Score

Add Impact score and Exploitability.

## Categorizing CVSS Base Scores

Table

## False Positives

This can be caused by interference or by scanners not having sufficient access to the test subject.

**False Positive Error:** When a scanner reports a false positive (false report).

**Positive Error:** When a scanner reports an actual vulnerability (true report).

## Reconciling Scan Results with Other Data Sources

Cybersecurity analysts should investigate other sources while reviewing the report:

* Log Review from servers, applications, etc.
* Security Information and Event Management (SIEM)
* Configuration Management Systems

# Vulnerability Classification

## Patch Management

Applying patches to systems should be a must but is neglected due to lack of resources.

## Legacy Platforms

Software that vendors discontinue support.

## Weak Configuration

* Using default settings.
* Presence of default credentials or unsecured accounts with administrator privileges.
* Open service ports.
* Users have access to information that violates the least privilege principle.

## Error Messages

With debug mode helping coders with error messages that contain crucial information on the structure of the application.

## Insecure Protocols

Protocols that are not encrypted and sending information through open networks.

## Weak Encryption

Encryption protects stored data and data in transit.

2 important choices to implement encryption:

* Algorithm to use.
* Encryption key to use.

## Penetration Testing

When organizations allow skilled people to attack their systems to test their security and find new vulnerabilities.

**Threat Hunting:** is a cybersecurity process that involves searching for and stopping cyberthreats in a network

Penetration Test Types:

* **Physical penetration testing:** testing the security of an organization building.
* **Offensive penetration testing:** security professionals act like attackers to find vulnerabilities.
* **Defensive penetration Testing:** Assessing the effectiveness of security policies, procedures, and technologies.
* **Integrated penetration testing:** Combines offensive and defensive penetration testing.

3 types of information classifications given to the penetration testers:

* **Known Environment:** Having full knowledge of the underlying technology.
* **Unknown Environment:** Having no knowledge of the underlying technology (most likely a real situation).
* **Partially Known Environment:** Mix of known and unknown information.

Rules of Engagement (RoE):

* Timeline
* Locations, systems, applications, and other potential targets.
* Data handling requirements.
* Behaviors to expect from the target.
* Resources
* Legal Concerns.
* When communication will occur for results.

## Reconnaissance

Testers gather as much information as possible about the target organization.

Passive Reconnaissance: gathering information without making direct contact with the target.

Active Reconnaissance: Making direct contact with targets to gather information. Ex. Port scanning and foot printing.

War Driving: drive-by facilities with cars equipped with antennas to connect to wireless networks.

## Running the Test

Key phases:

* Initial access: to get in a system.
* Privilege escalation: to gain privileges.
* Pivoting (lateral movement): move from network to network.
* Persistence: making backdoors to continue hacking.

# Audits and Assessments

3 major components of security assessments:

* Security tests
* Security assessments
* Security audits

## Security Test

Factors:

* Availability of resources.
* Critically of the systems and applications protected by the tested controls.
* Sensitivity of information obtained.
* Likelihood of technical failure.
* Likelihood of a misconfiguration.
* Risk that a system will come under attack.
* Rate of change of the control configuration.
* Other changes that might have an effect.
* Difficulty and time required.
* Impact a test has on business operations.

## Security Assessments

Its an assessment of everything that happened in the test.

## Security Audits

Examinations with a purpose from a 3rd party.

3 types of Audits:

* Internal Audits
* External Audits
* Independent Third-Party Audits: Request comes from a regulator, customer, or other outside entity.

Control Objectives for Information and Related Technologies (COBIT) is the auditing standard.

# Vulnerability Life Cycle

Image

Identification

* Vulnerability scans happen.
* Penetration test happens.
* Report is created.
* Audit is made.

## Vulnerability Analysis

* Confirms the vulnerability exists.
* Categorizing the vulnerability.
* Supplementing the external analysis of the vulnerability

## Vulnerability Response and Remediation

* Apply patches.
* Use network segmentation to isolate the affected system.
* Implement other compensating controls.
* Purchase insurance.
* Grant an exception or exemption to the system as part of a formal risk acceptance strategy.

## Validation of Remediation

Scan everything again after the remediation.

## Reporting

* Summarizing the vulnerabilities identified.
* Providing details on the remediation.
* Highlighting any requirements for further attention.
* Recommendations for improvements.