Chapter 4

Vulnerability Scanning

Outlines

- Regulatory Environment
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Information Security Management Act (FISMA)
- Security and Privacy Controls for Federal Information Systems and Organizations
- Determining Scan Frequency
- Scanner Software
- Scanner Maintenance
- Scan Perspective
- Supplementing Network Scans
- Vulnerability Plug-In Feeds
- Security Content Automation Protocol (SCAP)
- Analyzing and Testing Code
    - Static Code Analysis
    - Dynamic Code Analysis
- Fuzzing
- Web Application Vulnerability Scanning
- Database Vulnerability Scanning
- Developing a Remediation Workflow
- Testing and Implementing Fixes

Regulatory Environment

Many organizations find themselves bound by laws and regulations that govern the ways they store, process, and transmit information. This is especially true when the organization handles sensitive personal information or information belonging to government agencies. Many of these laws are not overly prescriptive and do not specifically address the implementation of a vulnerability management program.

- Health Insurance Portability and Accountability Act (HIPAA) regulates the ways that healthcare providers, insurance companies, and their business associates handle protected health information.
- Gramm-Leach-Bliley Act (GLBA) governs how financial institutions may handle customer financial records.
- Two regulatory schemes, however, do specifically mandate the implementation of a vulnerability management program: the Payment Card Industry Data Security Standard (PCI DSS) and the Federal Information Security Management Act (FISMA).

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS prescribes specific security controls for merchants who handle credit card transactions and service providers who assist merchants with these transactions. This standard includes what are arguably the most specific requirements for vulnerability scanning of any standard.

- Organizations must run both internal and external vulnerability scans (PCI DSS requirement 11.2).
- Organizations must run scans on at least a quarterly basis and "after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)" (PCI DSS requirement 11.2).
- Internal scans must be conducted by qualified personnel (PCI DSS requirement 11.2.1).
- Organizations must remediate any high-risk vulnerabilities and repeat scans to confirm that they are resolved until they receive a "clean" scan report (PCI DSS requirement 11.2.1).
- External scans must be conducted by an Approved Scanning Vendor (ASV) authorized by PCI SSC (PCI DSS requirement 11.2.2).

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 (FISMA) requires that government agencies and other organizations operating systems on behalf of government agencies comply with a series of security standards. The specific controls required by these standards depend on whether the government designates the system as low impact, moderate impact, or high impact

Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary Information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, Organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or Individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and Authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, Organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or Individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or Individuals.

Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or Individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or Individuals.

Security and Privacy Controls for Federal Information Systems and Organizations

a. Scans for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/ application are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and
- Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments to help eliminate similar vulnerabilities in other information systems (i.e. systemic weaknesses or deficiencies)

Corporate Policy

The prescriptive security requirements of PCI DSS and FISMA cover organizations involved in processing retail transactions and operating government systems, but those two categories constitute only a fraction of all enterprises. Cybersecurity professionals widely agree that vulnerability management is a critical component of any information security program, and for this reason, many organizations mandate vulnerability scanning in corporate policy, even if that is not a regulatory requirement.

Determining Scan Frequency

Cybersecurity professionals depend on automation to help them perform their duties in an efficient, effective manner. Vulnerability scanning tools allow the automated scheduling of scans to take the burden off administrators.

Factors influence how often an organization decides to conduct vulnerability scans against its systems

- The organization's risk appetite is its willingness to tolerate risk within the environment. If an organization is extremely risk averse, it may choose to conduct scans more frequently to minimize the amount of time between when vulnerability comes into existence and when it is detected by a scan.
- Regulatory requirements, such as PCI DSS or FISMA, may dictate a minimum frequency for vulnerability scans. These requirements may also come from corporate policies.
- Technical constraints may limit the frequency of scanning. For example, the scanning system may only be capable of performing a certain number of scans per day and organizations may need to adjust scan frequency to ensure that all scans complete successfully.
- Business constraints may prevent the organization from conducting resource-intensive vulnerability scans during periods of high business activity to avoid disruption of critical processes.
- Licensing limitations may curtail the bandwidth consumed by the scanner or the number of scans that may be conducted simultaneously.
- Operational constraints may limit the ability of the cybersecurity team to monitor and react to scan results promptly.

The scope of a vulnerability scan describes the extent of the scan, including answers to the following questions:

- **What systems, networks, services, applications, and protocols will be included in the vulnerability scan?**
- **What technical measures will be used to test whether systems are present on the network?**
- **What tests will be performed against systems discovered by a vulnerability scan?**

Scanner Software

Scanning systems themselves aren't immune from vulnerabilities. Even vulnerability scanners can have security issues! Regular patching of scanner software protects an organization against scanner-specific vulnerabilities and also provides important bug fixes and feature enhancements to improve scan quality.

Scanner Maintenance

Like any technology product, vulnerability management solutions require care and feeding. Administrators should conduct regular maintenance of their vulnerability scanner to ensure that the scanning software and vulnerability feeds remain up to date.

Scan Perspective

Comprehensive vulnerability management programs provide the ability to conduct scans from a variety of scan perspectives. Each scan perspective conducts the scan from a different location on the network, providing a different view into vulnerabilities. Penetration testers must be keenly aware of the network topology of the environments undergoing testing and how the location of their tools on the network may affect scan results.

Supplementing Network Scans

Basic vulnerability scans run over a network, probing a system from a distance. This provides a realistic view of the system's security by simulating what an attacker might see from another network vantage point. However, the firewalls, intrusion prevention systems, and other security controls that exist on the path between the scanner and the target server may affect the scan results, providing an inaccurate view of the server's security independent of those controls.

Vulnerability Plug-In Feeds

Security researchers discover new vulnerabilities every week, and vulnerability scanners can only be effective against these vulnerabilities if they receive frequent updates to their plug-ins. Administrators should configure their scanners to retrieve new plug-ins on a regular basis, preferably daily.

Security Scanner software:

Security Content Automation Protocol (SCAP)

The Security Content Automation Protocol (SCAP) is an effort by the security community, led by the National Institute of Standards and Technology (NIST), to create a standardized approach for communicating security-related information. This standardization is important to the automation of interactions between security components.

- Common Configuration Enumeration (CCE) provides a standard nomenclature for discussing system configuration issues.
- Common Platform Enumeration (CPE) provides a standard nomenclature for describing product names and versions.
- Common Vulnerabilities and Exposures (CVE) Provides a standard nomenclature for describing security-related software flaws.
- Common Vulnerability Scoring System (CVSS) provides a standardized approach for measuring and describing the severity of security-related software flaws.
- Extensible Configuration Checklist Description Format (XCCDF) is a language for specifying checklists and reporting checklist results.
- Open Vulnerability and Assessment Language (OVAL) Is a language for specifying low-level testing procedures used by checklists.

Analyzing and Testing Code

The source code that is the basis of every application and program can contain a variety of bugs and flaws, from programming and syntax errors to problems with business logic, error handling, and integration with other services and systems. It is important to be able to analyze the code to understand what the code does, how it performs that task, and where flaws may occur in the program itself. This information may point to critical undiscovered vulnerabilities that may be exploited during a penetration test.

Static Code Analysis

Static code analysis (sometimes called source code analysis) is conducted by reviewing the code for an application. Since static analysis uses the source code for an application, it can be seen as a type of white box testing with full visibility to the testers. This can allow testers to find problems that other tests might miss, either because the logic is not exposed to other testing methods or because of internal business logic problems. Unlike many other methods, static analysis does not run the program being analyzed; instead it focuses on understanding how the program is written and what the code is intended to do. Static code analysis can be conducted using automated tools or manually by reviewing the code—a process sometimes called "code understanding." Automated static code analysis can be very effective at finding known issues, and manual static code analysis helps to identify programmer-induced errors.

Dynamic Code Analysis

Dynamic code analysis relies on execution of the code while providing it with input to test the software. Much like static code analysis, dynamic code analysis may be done via automated tools or manually, but there is a strong preference for automated testing because of the volume of tests that need to be conducted in most dynamic code testing processes. Penetration testers are much more likely to find themselves able to conduct dynamic analysis of code rather than static analysis because the terms of penetration-testing SOWs often restrict access to source code.

Fuzzing

Fuzz testing, or fuzzing, involves sending invalid or random data to an application to test its ability to handle unexpected data. The application is monitored to determine if it crashes, fails, or responds in an incorrect manner. Fuzzing is typically automated because of the large amount of data that a fuzz test involves, and is particularly useful for detecting input validation and logic issues as well as memory leaks and error handling. Fuzz testing can often be performed externally without any privileged access to systems and is therefore a popular technique among penetration testers. However, fuzz testing is also a noisy testing method that may attract undue attention from cybersecurity teams.

Web Application Vulnerability Scanning

Many of the applications our organizations use today are web-based, and they offer unique opportunities for testing because of the relative standardization of HTML-based web interfaces. Earlier in this chapter, we looked at vulnerability scanning tools like Nessus and Qualys Guard, which scan for known vulnerabilities in systems, in services, and to a limited extent in web applications. Dedicated web application vulnerability scanners provide an even broader toolset specifically designed to identify problems with applications and their underlying web servers, databases, and infrastructure.

Tools:

Acunetix WVS, Arachni, Burp Suite, IBM's AppScan, HP's WebInspect, Netsparker, QualysGuard's Web Application Scanner, and W3AF, Nikto

Nikto: is an open-source web application scanning tool that is freely available for anyone to use.

Database Vulnerability Scanning

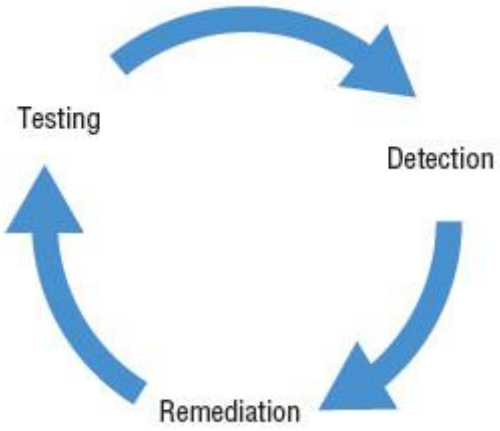
Databases contain some of an organization's most sensitive information and are lucrative targets for attackers. While most databases are protected from direct external access by firewalls, web applications offer a portal into those databases, and attackers may leverage database-backed web applications to direct attacks against databases, including SQL injection attacks.
Database vulnerability scanners are tools that allow penetration testers, other security professionals, and attackers to scan both databases and web applications for vulnerabilities that may affect database security.

Tools:

Sqlmap: is a commonly used open-source database vulnerability scanner that allows security administrators to probe web applications for database vulnerabilities.

Developing a Remediation Workflow

Vulnerability scans often produce a fairly steady stream of security issues that require attention from cybersecurity professionals, system engineers, software developers, network engineers, and other technologists. The initial scans of an environment can produce an overwhelming number of issues requiring prioritization and eventual remediation.



Testing and Implementing Fixes

Before deploying any remediation activity, cybersecurity professionals and other technologists should thoroughly test their planned fixes in a sandbox environment. This allows technologists to identify any unforeseen side effects of the fix and reduces the likelihood that remediation activities will disrupt business operations or cause damage to the organization's information assets.

Questions

1. Ryan is conducting a penetration test and is targeting a database server. Which one of the following tools would best assist him in detecting vulnerabilities on that server?
A. Nessus
B. Nikto
C. Sqlmap
D. OpenVAS
2. Gary is conducting a black box penetration test against an organization and is gathering vulnerability scanning results for use in his tests. Which one of the following scans is most likely to provide him with helpful information within the bounds of his test?
A. Stealth internal scan
B. Full internal scan
C. Stealth external scan
D. Full external scan
3. What tool can white box penetration testers use to help identify the systems present on a network prior to conducting vulnerability scans?
A. Asset inventory
B. Web application assessment
C. Router
D. DLP
4. Tonya is configuring vulnerability scans for a system that is subject to the PCI DSS compliance standard. What is the minimum frequency with which she must conduct scans?
A. Daily
B. Weekly
C. Monthly
D. Quarterly
5. Which one of the following is not an example of a vulnerability scanning tool?
A. QualysGuard
B. Snort
C. Nessus
D. OpenVAS

6. Which one of the following technologies, when used within an organization, is the LEAST likely to interfere with vulnerability scanning results achieved by external penetration testers?
A. Encryption
B. Firewall
C. Containerization
D. Intrusion prevention system
7. Renee is configuring her vulnerability management solution to perform credentialed scans of servers on her network. What type of account should she provide to the scanner?
A. Domain administrator
B. Local administrator
C. Root
D. Read-only
8. Jason is writing a report about potential security vulnerability in a software product and wishes to use standardized product names to ensure that other security analysts understand the report. Which SCAP component can Jason turn to for assistance?
A. CVSS
B. CVE
C. CPE
D. OVAL
9. Ken is planning to conduct a vulnerability scan of an organization as part of a penetration test. He is conducting a black box test. When would it be appropriate to conduct an internal scan of the network?
A. During the planning stage of the test
B. As soon as the contract is signed
C. After receiving permission from an administrator
D. After compromising an internal host
10. Which type of organization is the most likely to face a regulatory requirement to conduct vulnerability scans?
A. Bank
B. Hospital
C. Government agency
D. Doctor's office

11. Which one of the following categories of systems is most likely to be disrupted during a vulnerability scan?
A. External web server
B. Internal web server
C. IoT device
D. Firewall

12. What term describes an organization's willingness to tolerate risk in their computing environment?
A. Risk landscape
B. Risk appetite
C. Risk level
D. Risk adaptation
13. Which one of the following factors is least likely to impact vulnerability scanning schedules?
A. Regulatory requirements
B. Technical constraints
C. Business constraints
D. Staff availability
14. Adam is conducting a penetration test of an organization and is reviewing the source code of an application for vulnerabilities. What type of code testing is Adam conducting?
A. Mutation testing
B. Static code analysis
C. Dynamic code analysis
D. Fuzzing
15. Ryan is planning to conduct a vulnerability scan of a business-critical system using dangerous plug-ins. What would be the best approach for the initial scan?
A. Run the scan against production systems to achieve the most realistic results possible.
B. Run the scan during business hours.
C. Run the scan in a test environment.
D. Do not run the scan to avoid disrupting the business.
16. Which one of the following activities is not part of the vulnerability management life cycle?
A. Detection
B. Remediation
C. Reporting
D. Testing

17. What approach to vulnerability scanning incorporates information from agents running on the target servers?
A. Continuous monitoring
B. Ongoing scanning
C. On-demand scanning
D. Alerting

18. Brian is seeking to determine the appropriate impact categorization for a federal information system as he plans the vulnerability scanning controls for that system. After consulting management, he discovers that the system contains information that, if disclosed improperly, would have a serious adverse impact on the organization. How should this system be categorized?

A. Low impact
B. Moderate impact
C. High impact
D. Severe impact

19. Jessica is reading reports from vulnerability scans run by different parts of her organization using different products. She is responsible for assigning remediation resources and is having difficulty prioritizing issues from different sources. What SCAP component can help Jessica with this task?

A. CVSS
B. CVE
C. CPE
D. XCCDF

20. Sarah is conducting a penetration test and discovers a critical vulnerability in an application. What should she do next?

A. Report the vulnerability to the client's IT manager
B. Consult the SOW
C. Report the vulnerability to the developer
D. Exploit the vulnerability