Chapter 12

Reporting and Communication

Outlines

- Defining a Communication Path
- Communication Triggers
- Goal Reprioritization
- Recommending Mitigation Strategies
- Finding: Shared Local Administrator Credentials
- Finding: Weak Password Complexity
- Finding: Plain Text Passwords
- Finding: No Multifactor Authentication
- Finding: SQL Injection
- Finding: Unnecessary Open Services
- Writing a Penetration Testing Report
- Structuring the Written Report
- Executive Summary
- Findings and Remediation
- Methodology
- Conclusion
- Secure Handling and Disposition of Reports
- Post-Engagement Cleanup
- Client Acceptance
- Follow-Up Actions/Retesting
- Attestation of Findings

Defining a Communication Path

Penetration testers should clearly define their communication path during the planning stages of an engagement. It’s natural for technologists throughout the organization to be curious about interim results, especially if they are responsible for managing systems and applications that are within the scope of the test. When a communication path is defined in advance, this provides testers with an easy answer to requests for information: “Our contract requires us to keep the results confidential until we release our final report to management, except under very specific circumstances.”

Communication Triggers

- Completion of a testing stage. The penetration testing statement of work should include concrete milestones that indicate the completion of one stage of testing and mark the beginning of the next stage. The completion of a test stage should serve as a trigger for communicating updates to management.
- Discovery of a critical finding. If the penetration test identifies a critical issue with the security of the client’s environment, the testers should not wait for the delivery of their final report to communicate this issue to management. Leaving a critical vulnerability unaddressed may put the organization at an unacceptable level of risk and result in acompromise. Penetration testers who discover and validate the presence of a critical issue should follow the procedures outlined in the statement of work to immediately notify management of the issue, even if this notification reduces the degree of penetration that the testers are able to achieve during the test.
- Discovery of indicators of prior compromise. Penetration testers follow paths of activity that might also be attractive to real-world attackers. This puts them in situations where they are likely to discover evidence left behind by real attackers who compromised a system. When penetration testers discover indicators of an ongoing or past compromise, they should immediately inform management and recommend that the organization activate its cybersecurity incident response process.

Goal Reprioritization

There's a common saying among military planners: "No plan survives first contact with the enemy." In the realm of warfare, this means that the dynamic circumstances of the battlefield often require rapid shifts in plans that may have been in development for years. This same concept is true in the world of penetration testing. As testers conduct their work, they may discover information that causes them to want to reprioritize the goals of the test and perhaps pivot in a new, unforeseen direction. Reprioritizing the goals of a penetration test is an acceptable activity. It's perfectly fine to deviate from the original plan, but this reprioritization requires the input and concurrence of stakeholders. Remember, when you first embarked on a penetration test, you sought agreement from many stakeholders on the rules of engagement and the priorities for the test.

Recommending Mitigation Strategies

The whole point of a penetration test is to discover weaknesses in an organization's security posture so that they can be corrected. Penetration testers who successfully gain access to an organization's computing environment understand the flaws they exploited in more detail than anyone else. This makes them uniquely suited to recommend ways to remediate those flaws.

Security professionals are often quick to jump to technological solutions, but penetration testers should consider the full range of potential remediations for any flaw they discover.

These fit into three categories:

- **People**. Many attacks target individuals, and those attacks are often best addressed by also targeting those individuals with controls. For example, a social engineering attack might seek to convince an employee to approve a wire transfer request received via email. A people-focused control might use an awareness campaign to remind employees that they will never receive a legitimate request to transfer funds over email.
- **Process.** Business processes also are a common target for penetration testers, and process controls can protect against common attacks. Continuing the example of an attack that uses fraudulent emails to request wire transfers, the organization might implement a new process that provides specific approved techniques for requesting wire transfers to remove ambiguity.
- **Technology**. Technological controls also provide effective defenses against many security threats. For example, an organization might implement email content filtering to block inbound messages that appear to come from internal sources without proper authentication. They may also filter out messages containing high-risk keywords or coming from known malicious sources.

The CompTIA PenTest+ exam includes specific coverage of remediation strategies for six different findings that are commonly discovered during penetration tests:

- **Shared local administrator credentials**
- **Weak password complexity**
- **Plain text passwords**
- **No multifactor authentication**
- **SQL injection**
- **Unnecessary open services**

Finding: Shared Local Administrator Credentials

Organizations should randomize the passwords of administrator accounts, setting them to strong, complex passwords that are unique on each system. They may then use a password management tool to track all of those passwords.

In an ideal situation, no human being would have knowledge of those passwords. They may be available for emergency use through the password management tool, but the tool should be implemented in a way that administrators may gain emergency access to systems using the password without learning the password themselves. Additionally, the tool should change passwords to a new random, complex value immediately after their use or disclosure.

Finding: Weak Password Complexity

Organizations that rely upon passwords for authentication should set technical policies that set minimum password requirements governing the length and composition of passwords. Anytime a user is provided with the ability to set or change a password, that password should pass through a password filter to verify that it meets the organization's current complexity requirements.

Finding: Plain Text Passwords

The solution to this issue is to always store passwords in encrypted or hashed form. This prevents an attacker who gains access to the server from easily accessing all of the passwords stored on that server.

Finding: No Multifactor Authentication

Multifactor authentication implementations combine two or more authentication mechanisms coming from different authentication categories (or factors). These include the following categories:
Something you know. Knowledge-based authentication approaches rely upon some fact that the individual memorizes and keeps secret from other parties. This category includes passwords, PINs, and answers to security questions.

- Something you have. Physical objects may also be used as authentication mechanisms. These may include authentication tokens carried on key fobs that generate a one-time password that must be used at login. Other physical approaches include the use of smartphone apps that request confirmation of a login request, such as the Duo application

- Something you are. Biometric authentication techniques measure some attribute of an individual's physical body. Biometric approaches include fingerprint scans, voiceprint analysis, and facial recognition.

Finding: SQL Injection

CompTIA suggests two techniques for remediating SQL injection vulnerabilities:
Sanitizing user input (also known as input validation) and parameterizing queries. We discussed SQL injection vulnerabilities, as well as these remediation strategies, in detail in the section "Injection Attacks" in Chapter 5, "Analyzing Vulnerability Scans."

Finding: Unnecessary Open Services

The solution to unnecessary services is system hardening. When initially configuring a system, administrators should analyze all of the open services on the device and shut down any services that aren't necessary for the proper functioning of the server. They should repeat this process on a periodic basis and reconfigure systems as business needs change.

Writing a Penetration Testing Report

Structuring the Written Report

- Executive summary
- Findings and remediations
- Methodology
- Conclusion

Executive Summary

All of the important conclusions of the report in a clear manner that is understandable to a layperson.
The title of this section also describes the audience: It is being written for executives. These are not necessarily technologists. Executive summaries are often shared with senior leaders, board members, and other people who are busy and lack technical knowledge. Remember this when writing the executive summary.
The executive summary may be the first section to appear in the written report, but it should be the last section that you write. Creating the rest of the penetration testing report helps you finalize your findings, develop remediation recommendations, and provide a sense of context.

Findings and Remediation

The findings and remediation section is the meat and potatoes of a penetration testing report. This is where you describe the security issues that you discovered during the penetration test and offer suggestions on how the organization might remediate those issues to reduce their level of cybersecurity risk.

1. **Critical: SQL injection vulnerabilities allow the exfiltration of sensitive information from a business-critical database.**

2. **The web server located at 10.17.1.1 contains an application named directory.asp that contains SQL injection vulnerability in the lastName variable.**

3. **Users exploiting this vulnerability gain access to the backend database instance “CorporateResources” with administrative privileges.**

4. **The testers demonstrated the ability to use this vulnerability to gain access to employee Social Security numbers, confidential sales figures, and employee salaries. The risk associated with this vulnerability is somewhat mitigated because the web server is not externally accessible, but it poses a critical risk for insider attacks. To reproduce this risk, visit the following URL:https://10.17.1.1/directory.asp?lastName=test’;SELECT%20*%20 FROM&20Employees’—**

5. **We recommend that MCDS immediately remediate this vulnerability by enforcing an input validation policy on the lastName variable in the directory.asp application.**

Methodology

The methodology section of the report is your opportunity to get into the nitty-gritty technical details. Explain the types of testing that you performed, the tools that you used, and the observations that you made. The audience for this section of the report consists of the technologists who will be reviewing your results and taking actions based upon your findings. You want to share enough information to give them confidence in the quality of the test and a strong understanding of the way that you approached your work. Ideally, a skilled security professional should be able to pick up your report, read the methodology section, and use it to reproduce your results.

Conclusion

The conclusion is your opportunity to wrap things up in a tidy package for the reader. You should summarize your conclusions and make recommendations for future work. For example, if your penetration test scope excluded web application testing, you might recommend conducting that testing in a future engagement.
You also may wish to include metrics and measures in your conclusion that help put the information presented in the report in the context of the organization or a peer group of similar organizations or in a global context. Penetration testing providers who conduct many scans annually often conduct normalization of this information to produce an index that summarizes the organization’s level of risk in a score.

Secure Handling and Disposition of Reports

Followed to compromise the organization's security. Those instructions could serve as a road map for an attacker seeking to gain access to the organization. Discovering a copy of a penetration testing report is the ultimate win for an attacker conducting reconnaissance of an organization! It is, therefore, extremely important that anyone with access to the penetration testing report handle it securely. Reports should only be transmitted and stored in encrypted form, and paper copies should be kept under lock and key. Digital and paper copies of the report should be securely destroyed when they are no longer necessary.

Post-Engagement Cleanup

- Removing shells installed on systems during the penetration test
- Removing tester-created accounts, credentials, or back doors installed during the test
- Removing any tools installed during the penetration test

Client Acceptance

You should obtain formal client acceptance of your deliverables. This may simply be a written acknowledgment of your final report, but it more typically includes a face-to-face meeting where the testers discuss the results of the engagement with business and technical leaders and answer any questions that might arise.

Client acceptance marks the end of the client engagement and is the formal agreement that the testers successfully completed the agreed-upon scope of work.

Follow-Up Actions/Retesting

In some cases, the client may wish to have the team conduct follow-up actions after a penetration testing engagement. This may include conducting additional tests using different tools or on different resources than were included in the scope of the original test. Follow-on actions may also include retesting resources that had vulnerabilities during the original test to verify that remediation activities were effective.

Attestation of Findings

If the client conducted the test as part of a regulatory or contractual commitment, they may request that the tester prepare a formal attestation of their work and findings. The level of detail included in this attestation will depend upon the purpose of the request and should be discussed between the client and the tester. It may be as simple as a short letter confirming that the client engaged the tester for a penetration test, or it may require a listing of high-risk findings along with confirmation that the findings were successfully remediated after the test.

Questions

1. Tom recently conducted a penetration test for a company that is regulated under PCI DSS.
Two months after the test, the client asks for a letter documenting the test results for its compliance files. What type of report is the client requesting?

A. Executive summary
B. Penetration testing report
C. Written testimony
D. Attestation of findings

2. Wendy is reviewing the results of a penetration test and learns that her organization uses the same local administrator password on all systems. Which one of the following tools can help her resolve this issue?

A. LAPS
B. Nmap
C. Nessus
D. Metasploit

3. Which one of the following is not a normal communication trigger for a penetration test?

A. Discovery of a critical finding
B. Completion of a testing stage
C. Documentation of a new test
D. Identification of prior compromise

4. Gary ran an Nmap scan of a system and discovered that it is listening on port 22 despite the fact that it should not be accepting SSH connections. What finding should he report?

A. Shared local administrator credentials
B. Unnecessary open services
C. SQL injection vulnerability
D. No multifactor authentication

5. Tom's organization currently uses password-based authentication and would like to move to multifactor authentication. Which one of the following is an acceptable second factor?

A. Security question
B. PIN
C. Smartphone app
D. Passphrase

6. Which one of the following items is not appropriate for the executive summary of a penetration testing report?

A. Description of findings
B. Statement of risk
C. Plain language
D. Technical detail

7. Which one of the following activities is not commonly performed during the post engagement cleanup phase?

A. Remediation of vulnerabilities
B. Removal of shells
C. Removal of tester-created credentials
D. Removal of tools

8. Who is the most effective person to facilitate a lessons learned session after a penetration test?

A. Team leader
B. CIO
C. Third party
D. Client

9. Which one of the following is not a common category of remediation activity?

A. People
B. Process
C. Testing
D. Technology

10. Which one of the following techniques is not an appropriate remediation activity for SQL injection vulnerability?

A. Network firewall
B. Input sanitization
C. Input validation
D. Parameterized queries

11. When should system hardening activities take place?

A. When the system is initially built
B. When the system is initially built and periodically during its life
C. When the system is initially built and when it is decommissioned
D. When the system is initially built, periodically during its life, and when it is decommissioned

12. Biometric authentication technology fits into what multifactor authentication category?

A. Something you know
B. Something you are
C. Somewhere you are
D. Something you have