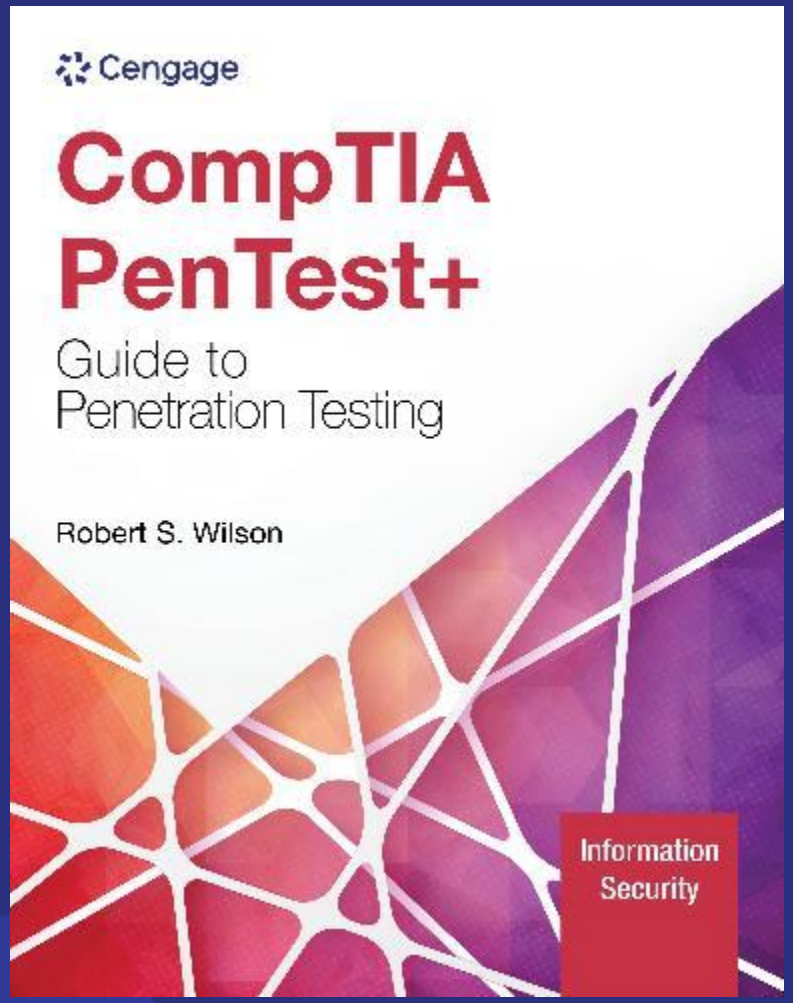


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 12: Reporting and Communication

Module Objectives (1 of 2)

By the end of this module, you should be able to:

1. Explain the importance of communication during the pen-testing process
2. Describe situations that may necessitate communication
3. Explain the importance of a well-defined communication path and the different contacts involved
4. Explain communication triggers
5. Explain various events and milestones that necessitate communication

Module Objectives (2 of 2)

By the end of this module, you should be able to:

6. Explain the types of controls that can be used to remediate vulnerabilities
7. Describe the most common pen-testing finds and mitigation strategies
8. Explain the importance of a pen-testing report, its various components, and its secure handling and destruction requirements
9. Describe pen-testing post-engagement activities

Communicating in Real Time during a Pen Test (1 of 5)

- Active two-way communication between pen tester and client stakeholders is essential during testing
- Communication occurs at regular intervals but may also be driven by events requiring immediate confirmation or if concerns need to be addressed
- Events requiring real-time communication include:
  - Discoveries requiring immediate attention – critical vulnerabilities requiring immediate remediation
  - Scope or ROE changes – discovery of new testing conditions or systems may change ROE

Communicating in Real Time during a Pen Test (2 of 5)

- Events requiring real-time communication include:
  - Business impact – testing activities that may impact business
  - Data gathering – questions to which pen testers need client response in order to proceed with pen testing
  - Determining false positives – ensuring security discovery is legitimate or a potential false positive
  - Scheduling specific activities – physical attacks and social engineering may require coordination with target

Communicating in Real Time during a Pen Test (3 of 5)

Having a Well-Defined Communication Path

- Pen-testing results contain sensitive and potentially confidential info
- Nondisclosure agreements are common and must be followed
- A defined communication path ensures appropriate info shared with correct personnel and not with those unauthorized
  - Primary contact(s)
  - Technical contact(s)
  - Emergency contact(s) and security operations center (SOC)

Communicating in Real Time during a Pen Test (4 of 5)

Communication Triggers

- Communication trigger – event initiating immediate communication

Indicators of Prior Compromise

- Evidence of breach that has already occurred

Critical Findings

- Security issues discovered that may result in harm if left unaddressed

Stage Completion

- Notification to appropriate stakeholders as pen-test stages complete

Communicating in Real Time during a Pen Test (5 of 5)

Other Reasons for Communication

- Situational awareness – information updates between pen-test team and client such as status meetings or updates on upcoming events
- De-escalation – communication to reduce disruption to performance of business systems; rescheduling of activities
- De-confliction – may solve problems caused by client security team detecting and blocking necessary or planned pen-testing activities
- Goal reprioritization – new information may require changes in scope, work, or goals

Discussion Activity 12-1

Real-time communication during a pen test is critical to the overall success of the penetration test and to ensure client needs are met.

What potential issues may arise with lack of proper communication with clients during the phases of a penetration test?

Communicating Findings and Recommending Remediation (1 of 29)

Recommending Controls

- Motivation for pen test is to find vulnerabilities and suggest remediation methods and mechanisms
- Three important questions to consider for each vulnerability:
  1. How was the vulnerability discovered?
  2. What was required to exploit this vulnerability?
  3. What controls could have prevented the discovery and exploitation of this vulnerability?

Communicating Findings and Recommending Remediation (2 of 29)

Recommending Controls

Most controls fall into these categories:

- Technical controls – software or hardware solutions employing security intelligence to detect and remediate security threats
  - Unified threat management (UTM) devices or firewall
- Administrative controls – formal processes and policies to improve security
  - Secure software development, password policies, access control rules, and enforcing policies

Communicating Findings and Recommending Remediation (3 of 29)

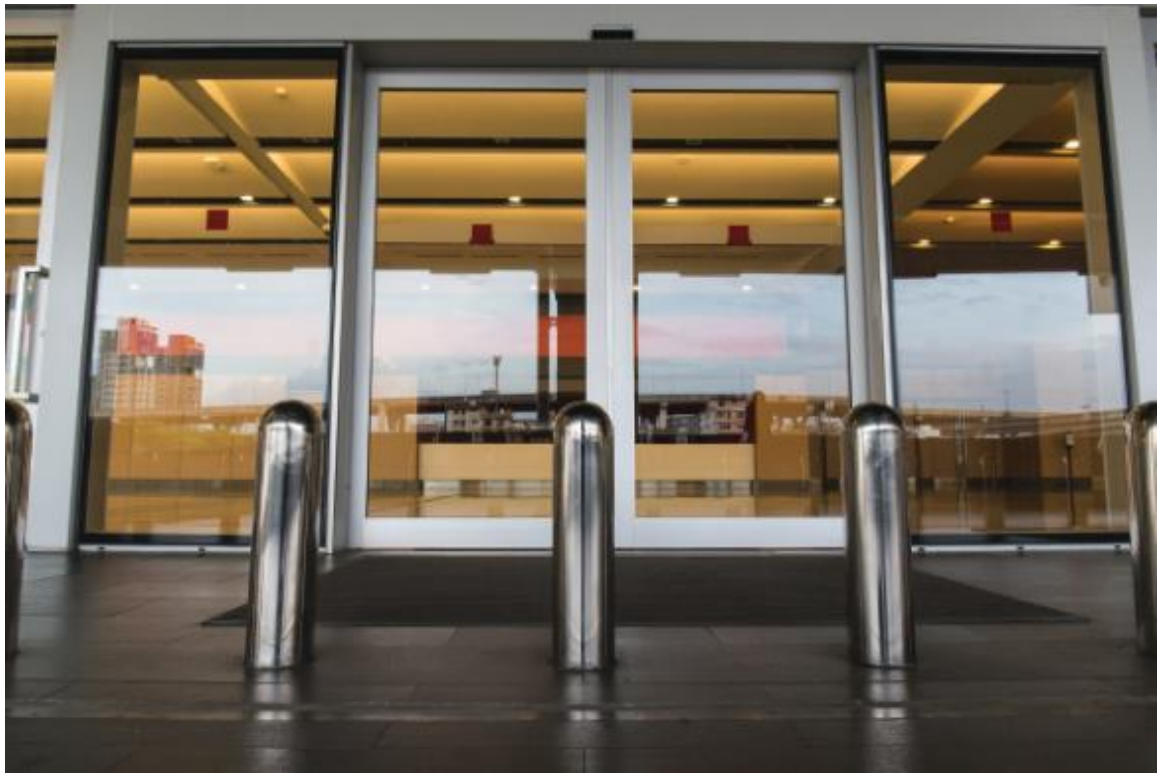
Recommending Controls

- Operational controls – standard procedures for personnel to improve security
  - User training, time-of-day restrictions, mandatory vacations, and job rotation
- Physical controls – tools that prevent threat actors from gaining physical access or damaging a facility
  - Security guards, surveillance systems, mantraps, bollards, and biometric access controls for facility entrance

Communicating Findings and Recommending Remediation (4 of 29)

Recommending Controls

- Controls are commonly combined to solve security issues
- Phishing controls
  - Employee training on phishing (operational)
  - Phishing email report button (technical)



Bollards protecting an entryway

Communicating Findings and Recommending Remediation (5 of 29)

Recommending Controls

- Looking at remediation strategies commonly boils down to three areas:
  - People – weakest link in security and can be best line of defense
    - Formal security training and awareness programs provide results
  - Processes – organizations may operate in ways counter to security practices
  - Technologies – often first controls thought of, but may not protect from problems arising with underlying people and processes

Communicating Findings and Recommending Remediation (6 of 29)

Common Pen-Testing Findings and Mitigation Strategies

Shared Local Administrator Credentials

- Each administrator should use unique admin credentials
- Systems should have unique, strong, and complex admin passwords
- Separate admin accounts for classes of systems
  - Use different admin credentials for servers, desktops, infrastructure devices, etc.
- Randomized passwords created via generator can be a good choice

Communicating Findings and Recommending Remediation (7 of 29)

Common Pen-Testing Findings and Mitigation Strategies

Shared Local Administrator Credentials

- Password management tools may be used but must store data in secure, encrypted local storage
- Administrator passwords should be changed frequently
- Microsoft's Local Administrator Password Solution (LAPS) tool can manage local accounts of domain-joined computers
  - Can set local admin to unique values, perform other security actions

Communicating Findings and Recommending Remediation (8 of 29)

Common Pen-Testing Findings and Mitigation Strategies

Weak Password Complexity

- Simple passwords are cracked easily
- Technical controls can enforce minimum password requirements

Plain Text Passwords

- Passwords not stored using encryption or hashing are vulnerable if discovered by attacker
- All systems should be configured to store passwords properly using strong encryption or hashing

Communicating Findings and Recommending Remediation (9 of 29)

Common Pen-Testing Findings and Mitigation Strategies

No Multifactor Authentication

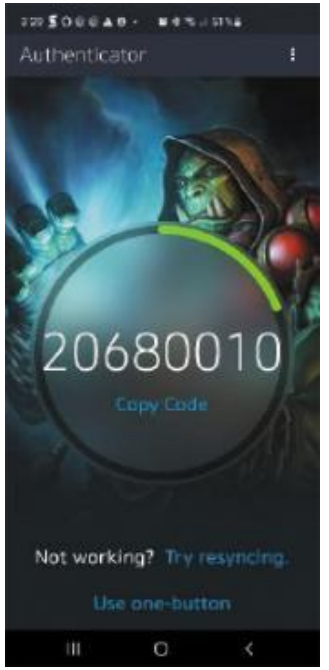
- Requiring an additional factor to the username and password for authentication greatly improves security
- Factors for authentication fall into these categories:
  - Something you know – username, password, MFA, or PIN
  - Something you have – physical object such as authentication token or smartphone app
  - Something you are – biometric techniques like fingerprint and retina

Communicating Findings and Recommending Remediation (10 of 29)

Common Pen-Testing Findings and Mitigation Strategies

No Multifactor Authentication

- One-time passwords (OTP) are increasingly used as "something you have" factor
- MFA implements two or more factors
- If threat actor acquires username and passwords, authentication will not occur without another required factor
  - Can greatly improve authentication security



Battle.net Authenticator app

Communicating Findings and Recommending Remediation (11 of 29)

Common Pen-Testing Findings and Mitigation Strategies

SQL Injection Vulnerabilities

- Websites and servers vulnerable to SQL injection are common findings

Unnecessary Open Services

- Scanning systems for open or listening ports may identify services that are open to communication without business needing to be open
  - Administrators may be unaware of open ports due to complex software installation of network tools and services

Communicating Findings and Recommending Remediation (12 of 29)

Writing a Pen-Test Report

Normalization of Data

- Pen-test report will contain numeric data from various sources
  - Sources may use different scales, 1 to 5, 1 to 10, 1 to 100, to show testing results, vulnerability severity, and other data
  - Some tools may use higher numbers for severity (10) while others may use lower numbers (1); converting is necessary
- Choosing a single scale and converting all numeric data to that scale will aid clients in best understanding results

Communicating Findings and Recommending Remediation (13 of 29)

Writing a Pen-Test Report

Risk Appetite

- The amount of risk an organization is willing to accept in specific areas is referred to as “risk appetite”
- An organization may have a high-risk appetite in certain areas but very low in others

Communicating Findings and Recommending Remediation (14 of 29)

Writing a Pen-Test Report

Report Structure

- Pen-test reports will vary from one pen tester to another
- Format may include the following sections:

1. Title Page and Table of Contents
2. Executive Summary
3. Scope Details
4. Methodology
5. Findings and Remediation
6. Conclusion
7. Appendices

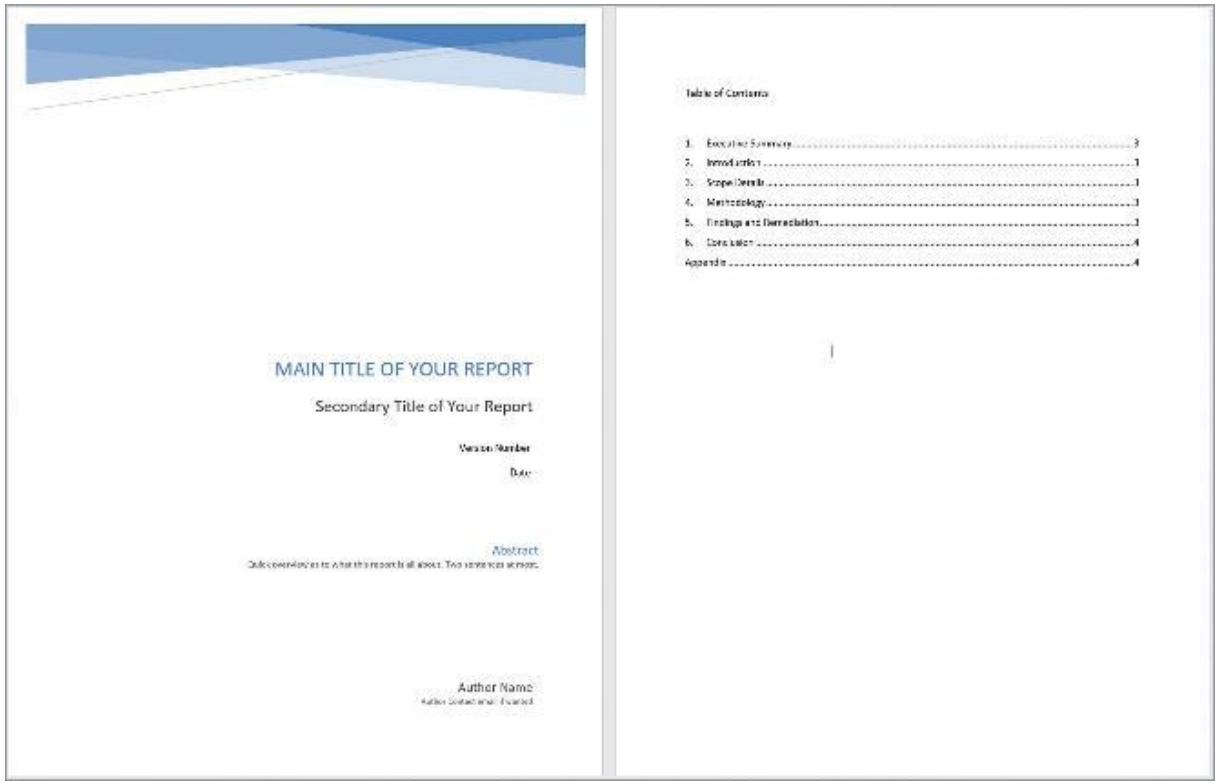
Communicating Findings and Recommending Remediation (15 of 29)

Writing a Pen-Test Report

Title Page and Table of Contents

- Should contain title such as “Enterprise Penetration Report for ACME Corporation”
  - Version number, date, author name
  - Secondary title and abstract if needed
- Table of contents immediately follows title page with references to later pages and sections
  - Each page of report should be numbered

Communicating Findings and Recommending Remediation (16 of 29)



Title page and table of contents

Communicating Findings and Recommending Remediation (17 of 29)

Writing a Pen-Test Report

Executive Summary

- Concise overview of issues discovered during pen testing
- Target audience are C-suite executives of client organization
- Executives may have varying levels of tech savvy
- Business impact details often included here
  - Real world examples from peer organizations often included

Communicating Findings and Recommending Remediation (18 of 29)

Writing a Pen-Test Report

Scope Details

- Section captures planning details during initial development of scope with client
- Scope of work may change during the pen test
- Including changes in scope is important

Communicating Findings and Recommending Remediation (19 of 29)

Writing a Pen-Test Report

Methodology

Technical details of the tests performed:

1. The types of tests performed
2. The steps taken during various tests and phases
3. How attacks were carried out
4. What tools were used
5. What observations were made

Communicating Findings and Recommending Remediation (20 of 29)

Writing a Pen-Test Report

Methodology

- Audience includes tech staff and developers, others who will review and take actions on findings
- Enough tech detail so results can be replicated is necessary, but not overwhelm the reader
- Risk rating metric using impact and probability is useful

		Probability		
		Low (1)	Medium (2)	High (3)
Impact	Low (1)	1	2	3
	Medium (2)	2	4	6
	High (3)	3	6	9

Risk rating table

Communicating Findings and Recommending Remediation (21 of 29)

Writing a Pen-Test Report

Findings and Remediation

- Section covers security issues found and steps suggest to fix each; often the largest section, as it covers bulk of pen-test efforts
- Security issues should be expressed separately with description and remediation steps
- Business impact analysis on organization's specific circumstances may be included

Communicating Findings and Recommending Remediation (22 of 29)

Writing a Pen-Test Report

Findings and Remediation – Sample Vulnerability Finding

Vulnerability Finding #42: No MFA on AWS root accounts
Impact: Medium
Probability: Medium
Risk Rating: 4
Description: While assessing AWS cloud security, it was discovered that root-level account logins were not secured with multifactor authentication. Using MFA with root-level accounts is an AWS suggested best practice.
Remediation: Implement MFA for all AWS root accounts

Communicating Findings and Recommending Remediation (23 of 29)

Writing a Pen-Test Report

Conclusion

- Summary of overall test results; wraps up report for reader
- Describes any root causes to address to improve overall security
- May identify future testing recommendations
- Could include overall risk score for pen test, discussion of risk ratings, or comparison to other organizations in same sphere of operations

Communicating Findings and Recommending Remediation (24 of 29)

Writing a Pen-Test Report

Appendices

- Bulk data from scans or lengthy code listings can be included here
- Technology definitions also included in appendices

Communicating Findings and Recommending Remediation (25 of 29)

Secure Handling and Destruction of Reports

- Sensitive information about client organization is included in reports
  - Vulnerabilities and exploitation details
  - System IP addresses
  - Reconnaissance data
  - Employee and executive names
- Threat actor that obtains pen-test report could use it to attack
- Protection and control of access to electronic and physical copies is critical responsibility of pen tester

Format

- Digital reports should be encrypted, physical copies stored securely

Communicating Findings and Recommending Remediation (26 of 29)

Secure Handling and Destruction of Reports

Storage Time

- Pen testers should agree upon how long they will keep report copies

Delivering the Report

- Meeting between pen testers and appropriate stakeholders should be held to formally deliver the report

Client Acceptance

- Formal acceptance and client sign off on report signifies completion of work

Communicating Findings and Recommending Remediation (27 of 29)

Secure Handling and Destruction of Reports

Post-Engagement Cleanup

- Pen testers are responsible for removing all traces of pen-test activities
- Post engagement cleanup may include:
  - Removing shell programs
  - Removing tester-created credentials
  - Removing tools

Communicating Findings and Recommending Remediation (28 of 29)

Secure Handling and Destruction of Reports

Follow-Up Actions and Retesting

- Some report discoveries may necessitate retesting or other follow-up
- Follow-up actions should be well-defined and scheduled

Attestation of Findings

- Compliance or regulatory testing may require formal document from pen-test team
- Document will vary depending on client need and regulations used

Communicating Findings and Recommending Remediation (29 of 29)

Secure Handling and Destruction of Reports

Data Destruction and Retention

- SOW should spell out details regarding retention and destruction of data created during pen test
- These should be followed explicitly following the completion of test

Lessons Learned

- After formal completion of pen test project, the testing team should meet to discuss project and identify weak areas to improve
- Areas of success should be especially noted and reviewed

Discussion Activity 12-2

The proper handling of penetration reports and all data collected during a pen test is a critical responsibility of the pen-test team. Organizations might have different needs for retention of the report once client sign-off has occurred.

What factors may influence how long a pen-test team may retain copies of the data and report for the pen test? How might the factors influencing client retention of pen-test documents be similar or different from those of the pen-test team?

Summary (1 of 2)

By the end of this module, you should be able to:

1. Explain the importance of communication during the pen-testing process
2. Describe situations that may necessitate communication
3. Explain the importance of a well-defined communication path and the different contacts involved
4. Explain communication triggers
5. Explain various events and milestones that necessitate communication

Summary (2 of 2)

By the end of this module, you should be able to:

6. Explain the types of controls that can be used to remediate vulnerabilities
7. Describe the most common pen-testing finds and mitigation strategies
8. Explain the importance of a pen-testing report, its various components, and its secure handling and destruction requirements
9. Describe pen-testing post-engagement activities