

5.0 Reporting and Communications

CompTIA PenTest+ Exam Prep (PT0-001)

Report Writing

Episode 1

PENTEST+ EXAM OBJECTIVES

DOMAIN	PERCENTAGE OF EXAM
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
TOTAL	100%

PEN TEST REPORT

- Communicate findings AND recommendations
- Primary deliverable
- Only chance to make your points
- Digest of all activities and conclusions
 - Some conclusions are drawn during tests
 - Some result from post-test analysis

5.1 Given a scenario, use report writing and handling best practices

SAMPLES AND TEMPLATES

- <http://www.pentest-standard.org/index.php/Reporting>
- <https://github.com/juliocesarfort/public-pentesting-reports>
- <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>
- http://www.niiconsulting.com/services/security-assessment/NII_Sample_PT_Report.pdf

5.1 Given a scenario, use report writing and handling best practices

TIPS FOR WRITING A REPORT

- Start writing early
 - Don't wait until the end of the project
 - Write what you can up front
 - Add to the report as you go – editing is easy
- Tell your story
- Know your audience(s)
 - Executive 1-page summary
 - Technical/management
 - Motivation – audit?
- Leave the reader with a call to action
 - Include steps to fix the issues

5.1 Given a scenario, use report writing and handling best practices

TIPS FOR WRITING A REPORT

- Your report will be your voice after you leave
- Try to answer any questions that may arise
 - What did you do?
 - Why did you make the choices you made?
 - What did you find, and how did your findings affect your conclusions?
- After settling on format, you need data
- Mostly presentation and summary of data
- Collect data
 - Transform as needed into a common format (normalization)
 - Don't spend too much time on this, but try to harmonize data format
 - Use tools like MS Excel
 - Easier to read and analyze

5.1 Given a scenario, use report writing and handling best practices

COMMON SECTIONS

- Executive summary
 - 1 page max - High level summary
 - Targeted at executives – few details
 - State the test goals and general findings
- Methodology
 - Your approach to the overall test activities
 - Tools and techniques
 - Why you did what you did
 - And why you didn't do more

5.1.2 Written report of findings and remediation

5.1.2.1 Executive summary

5.1.2.2 Methodology

COMMON SECTIONS

- Findings and remediation
 - Ranked list (more details than Executive summary)
 - What you found (important findings first)
 - What you recommend the client does – provide options as appropriate
- Metrics and measures
 - Details of what you found
 - How you assessed each finding
 - Risk rating - <http://www.pentest-standard.org/index.php/Reporting>
- Conclusion
 - Wrap up, summary, and call to action

5.1.2 Written report of findings and remediation

5.1.2.3 Findings and remediation

5.1.2.4 Metrics and measures

5.1.2.4.1 Risk rating

5.1.2.5 Conclusion

BEST PRACTICES

- Risk appetite
 - Amount of risk client is willing to accept
 - Tone of the entire report is based on the company's appetite for risk
 - Risk appetite statement should appear in the report introduction
- Report storage
 - Reports should become part of the organization's document repository
 - Used as input for future pen tests and other assessments
 - Security policy should state how long reports are kept
- Report handling and disposition
 - Security policy should state how assessment reports are stored
 - At end of life, how are reports disposed of?

5.1.3 Risk appetite

5.1.4 Storage time for report

5.1.5 Secure handling and disposition of reports

Post-Report Activities

Episode 2

POST-REPORT DELIVERY ACTIVITIES

- Delivering the report isn't the end
 - There is more work to do
 - Delivering may include presenting the report
- Post-report delivery activities – clean up any changes you made
 - Removing all of these
 - Shells
 - Tester-created credentials
 - Tools
 - Clean up history
 - Leaving artifacts can weaken the client

5.2 Explain post-report delivery activities.

5.2.1 Post-engagement cleanup

5.2.1.1 Removing shells

5.2.1.2 Removing tester-created credentials

5.2.1.3 Removing tools

POST-REPORT DELIVERY ACTIVITIES

- Client acceptance
 - Formal cessation of project activities and acceptance of deliverable
 - The client formally says “You’re done.”
 - Client should sign an statement of acceptance
- Lessons learned
 - Crucial step in project closure
 - Helps to continuously improve
- Follow-up actions/retest
 - Client may need more actions based on findings
 - Be careful to avoid extending the project scope here without a change process
- Attestation of findings
 - Independent review and assurance of findings (i.e. third party)

5.2 Explain post-report delivery activities.

5.2.2 Client acceptance

5.2.3 Lessons learned

5.2.4 Follow-up actions/retest

5.2.5 Attestation of findings

Mitigation Strategies

Episode 3

RECOMMENDED MITIGATION STRATEGIES

- Nearly every pen test will discover multiple vulnerabilities
- A pen test report should contain recommendations to mitigate each vulnerability
- Solutions vary, depending on the vulnerability
- People – behavior changes
 - Social engineering
 - Passwords
- Process – how things are done
 - Backup media handling
 - ID management
- Technology
 - Controls based on hardware and/or software

5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities

5.3.1 Solutions

5.3.1.1 People

5.3.1.2 Process

5.3.1.3 Technology

COMMON FINDINGS

- Shared local administrator credentials
 - Randomize credentials/LAPS
- Weak password complexity
 - Minimum password requirements/password filters
- Plain text passwords
 - Encrypt the passwords
- No multifactor authentication
 - Implement multifactor authentication
- SQL injection
 - Sanitize user input/parameterize queries
- Unnecessary open services
 - Disable or remove unneeded services (system hardening)

5.3.3 Remediation

5.3.3.1 Randomize credentials/LAPS

5.3.3.2 Minimum password requirements/password filters

5.3.3.3 Encrypt the passwords

5.3.3.4 Implement multifactor authentication

5.3.3.5 Sanitize user input/parameterize queries

5.3.3.6 System hardening

Communication

Episode 4

IMPORTANCE OF COMMUNICATION

- Good communication is critical to the penetration test success
- Most penetration tests should be conducted openly
 - Unless discretion is a stated goal
- Cooperation is enhanced with communication
- Who authorizes the project and provides funding?
 - Project sponsor
- Who should be contacted if unexpected consequences occur?
- Who will resolve conflicts?
- Who will provide required technical assistance?
- How will you escalate issues that are not resolved in a timely manner?

5.4 Explain the importance of communication during the penetration testing process.

5.4.1 Communication path

IMPORTANCE OF COMMUNICATION

- Communication timing and frequency
- Communication triggers
 - Critical findings – something that really can't wait
 - Stages – moving from one phase to another
 - Indicators of prior compromise – finding evidence that an attacker has already been here
 - Other defined milestones or events
 - Periodic reports
 - Critical tests started/completed
 - Obstacles put in place/removed (i.e. affect on operations)

5.4 Explain the importance of communication during the penetration testing process.

5.4.2 Communication triggers

5.4.2.1 Critical findings

5.4.2.2 Stages

5.4.2.3 Indicators of prior compromise

REASONS FOR COMMUNICATION

- Situational awareness
 - Most common recurring reason
- De-escalation
 - Information or action is needed to reduce critical risk
- De-confliction
 - Resolve conflict of any type
 - Pen test team vs. operations/users
 - Pen test team vs. service provider
 - Pen test team vs. management

5.4.3 Reasons for communication

5.4.3.1 Situational awareness

5.4.3.2 De-escalation

5.4.3.3 De-confliction

5.4.4 Goal reprioritization

REASONS FOR COMMUNICATION

- Goal reprioritization
 - Changes to pen testing plan
 - Unexpected impact
 - Unexpected findings
 - Organizational changes – management change, merger, acquisition
 - Conflict with team, management, resources, etc.
- All changes must follow change procedures

5.4.3 Reasons for communication

5.4.3.1 Situational awareness

5.4.3.2 De-escalation

5.4.3.3 De-confliction

5.4.4 Goal reprioritization

PENTEST+ EXAM OBJECTIVES

DOMAIN	PERCENTAGE OF EXAM
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
TOTAL	100%

SUMMARY

- You're ready for the test!
- Review the material we covered
 - 1.0 Planning and Scoping
 - 2.0 Information Gathering and Vulnerability Identification
 - 3.0 Attacks and Exploits
 - 4.0 Penetration Testing Tools
 - 5.0 Reporting and Communication
- Practice, practice, practice!

Summary