

CHAPTER 10

Post-Engagement Activities



Episode 10.01 – Report Writing

Objective 4.1 Compare and contrast important components of written reports

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

SAMPLES AND TEMPLATES

- <http://www.pentest-standard.org/index.php/Reporting>
- <https://github.com/juliocezarfort/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

TIPS FOR WRITING A REPORT

- 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
- Your report will be your voice after you leave

TIPS FOR WRITING A REPORT

- 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?

TIPS FOR WRITING A REPORT

- After settling on format, you need data
- Mostly presentation and summary of data
- Collect data
 - Transform as needed into a common format
 - Don't spend too much time on this, but try to harmonize data format
 - Use tools like MS Excel
 - Easier to read and analyze

COMMON SECTIONS

- Executive summary
 - 1 page max - High level summary
 - Targeted at executives – few details
 - State the test goals and general findings

COMMON SECTIONS

- Methodology
 - Your approach to the overall test activities
 - Tools and techniques
 - Why you did what you did
 - And why you didn't do more

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

COMMON SECTIONS

- 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

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

BEST PRACTICES

- 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?

QUICK REVIEW

- The Pen Test report is your best opportunity to leave a lasting message
- Start writing your report early in the testing project
- Write to your audiences (executive vs. technical)
- Provide a definite "call to action" with remediation recommendations



Episode 10.02 - Important Components of Written Reports

Objective 4.1 Compare and contrast important components
of written reports

IMPORTANT COMPONENTS OF WRITTEN REPORTS

- Note taking
 - Do not rely on memory for any meetings or activities
 - Ongoing documentation during tests
 - Screenshots

IMPORTANT COMPONENTS OF WRITTEN REPORTS

- Common themes/root causes
 - Vulnerabilities
 - Use common vulnerability entries
 - Observations
 - Capture environment and any noticeable conditions
 - Lack of best practices
 - Document any procedures that deviate from well-known best practices

QUICK REVIEW

- Keep careful notes of all activities
- Include screenshots in notes
- Document recurring trends
- Note lack of best practices



Episode 10.03 - Mitigation Strategies

Objective 4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report

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

MITIGATION STRATEGY CATEGORIES

- People – behavior changes
 - Social engineering
 - Passwords
- Process – how things are done
 - Backup media handling
 - ID management
- Technology
 - Controls based on hardware and/or software

COMMON FINDINGS

- Shared local administrator credentials
 - Randomize credentials/LAPS
- Weak password complexity
 - Minimum password requirements/password filters
- Plain text passwords
 - Encrypt the passwords

COMMON FINDINGS

- No multifactor authentication
 - Implement multifactor authentication
- SQL injection
 - Sanitize user input/parameterize queries
- Unnecessary open services
 - Disable or remove unneeded services (system hardening)

QUICK REVIEW

- Recommend mitigation activities for each identified vulnerability
- Suggest different classes of mitigations (technical, administrative, etc.)
- Know common findings and mitigations for the PenTest+ exam



Episode 10.04 – Technical and Physical Controls

Objective 4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report

TECHNICAL CONTROL RECOMMENDATIONS

- Process-level remediation
 - Recommend procedure changes to increase security
- Patch management
 - Plan, test, execute, and manage recurring patch activity
- Key rotation
 - Document key rotation cycles and validate that procedures are followed

TECHNICAL CONTROL RECOMMENDATIONS

- Certificate management
 - Ensure that certificates are managed properly and securely
- Secrets management solution
 - Document how IP and other sensitive data is handled and managed
- Network segmentation
 - Review network segmentation policy and procedures for validating compliance

PHYSICAL CONTROL RECOMMENDATIONS

- Access control vestibule
 - Inner and outer doors
 - Allows personnel or automated controls to determine authorization prior to opening inner door
 - Organization can help separate subjects during authorization

PHYSICAL CONTROL RECOMMENDATIONS

- Biometric controls
 - What you are or what you do
 - Characteristics associated with the subject
 - Harder to spoof
 - Lower requirements

PHYSICAL CONTROL RECOMMENDATIONS

- Video surveillance
 - Helps detect unusual behavior
 - Can provide valuable evidence during a post-incident investigation

QUICK REVIEW

- Recommend controls at multiple layers
- Technical controls rely on hardware, software, and settings
- Physical controls are things you can touch



Episode 10.05 – Administrative and Operational Controls

Objective 4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report

ADMINISTRATIVE CONTROL RECOMMENDATIONS

- Role-based access control
 - Define policies for determining roles and permissions required for each role
- Secure software development lifecycle
 - Implement SCM, SDLC, or other formal development lifecycle

ADMINISTRATIVE CONTROL RECOMMENDATIONS

- Minimum password requirements
 - Develop password policy based on best practices and organizational needs
 - Balance security and usability requirements
- Policies and procedures
 - Use best practices and popular security frameworks to validate that all necessary policies and procedures are in place

OPERATIONAL CONTROL RECOMMENDATIONS

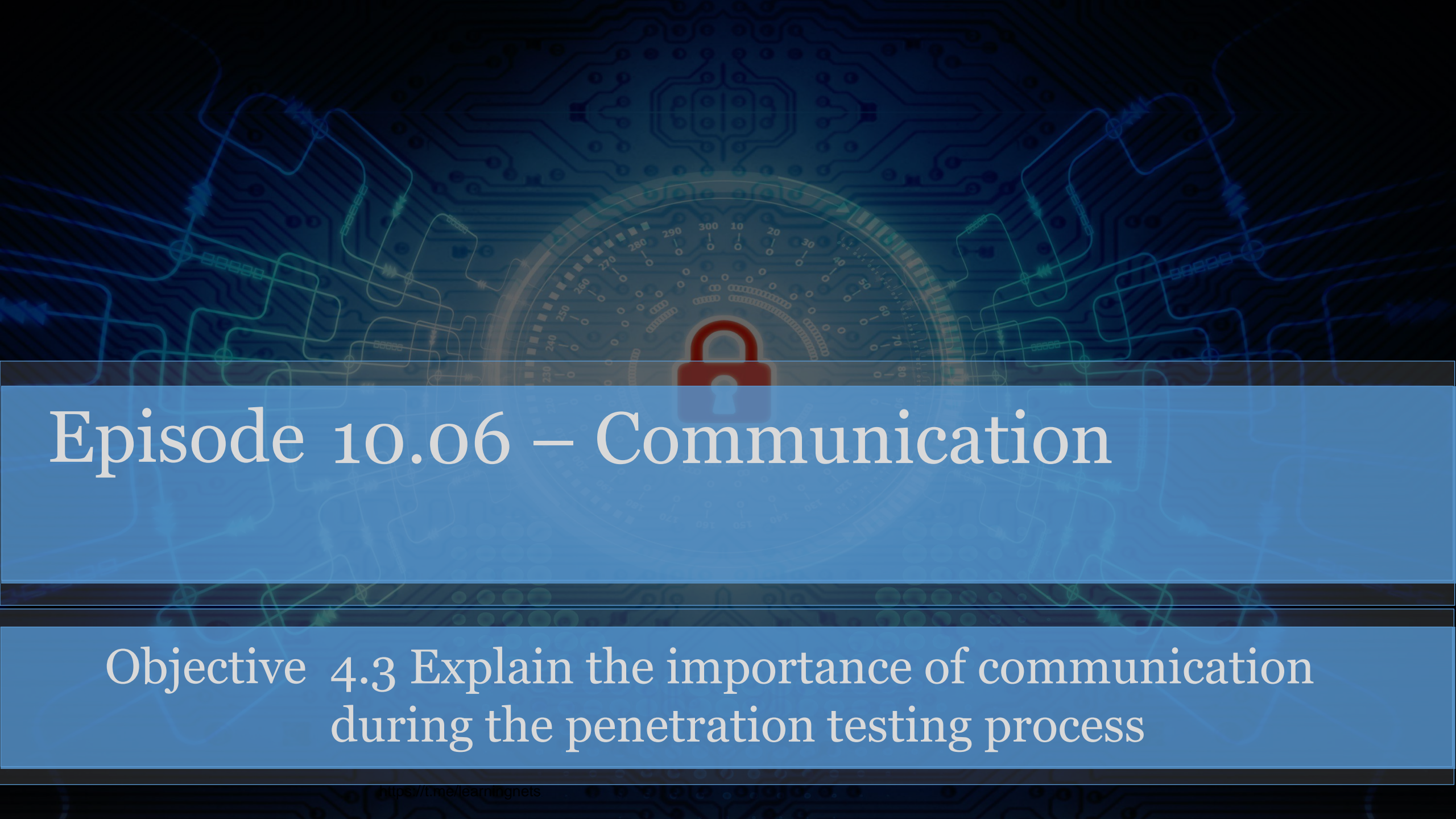
- Job rotation
 - Helpful to identify personnel taking advantage of privilege
- Time-of-day restrictions
 - Limit resource and facility access to align with work duty hours

OPERATIONAL CONTROL RECOMMENDATIONS

- Mandatory vacations
 - Scheduled work activity pauses for audits
- User training
 - Ensure recurrent training on security awareness and procedures

QUICK REVIEW

- Administrative controls focus on policies and procedures
- Operational controls govern how day-to-day activities are managed



Episode 10.06 – Communication

Objective 4.3 Explain the importance of communication during the penetration testing process

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

IMPORTANCE OF 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?

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)

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

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

QUICK REVIEW

- Good communication is critical to pen test project success
- Managing communication expectations, including frequency, reduces conflict
- Define triggers that initiate communication



Episode 10.07 - Presentation of Findings

Objective 4.3 Explain the importance of communication during the penetration testing process

PRESENTATION OF FINDINGS

- Executive
 - High-level bullet points
 - Align every point with a strategic objective
 - Use business language, not technical

PRESENTATION OF FINDINGS

- Management
 - Focus on high-level goals to satisfy business objectives
 - Align technical recommendations with business goals

PRESENTATION OF FINDINGS

- Technical
 - Summary section focuses on actions to implement
 - Details section provides lots of technical info to carry out recommended actions

QUICK REVIEW

- Change your presentation based on the audience
- Executives only want to see summaries and how findings impact the business
- Management needs more details, but still at a high level
- Technical presentations should include details



Episode 10.08 - Post-Report Activities

Objective 4.4 Explain post-report delivery activities

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

- 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

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

POST-REPORT DELIVERY ACTIVITIES

- 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)

QUICK REVIEW

- Remove all test activity artifacts
- Get formal client acceptance
- Conduct "lessons learned" sessions with client and capture the findings
- Follow up on client add-on requests



Episode 10.09 - Data Destruction Process

Objective 4.4 Explain post-report delivery activities

DATA DESTRUCTION PROCESS

- Testing agreements should include destruction expectations
 - Follow and document adherence with expectations
- Identify what information collected is in scope
- Document procedures followed to dispose of covered data
- Provide all data to client in a secure manner and then dispose

QUICK REVIEW

- Pentests generate a lot of data
- Define the usable lifetime of all data
- Document procedures to dispose of the data
- Deliver pentest data securely and then delete it