CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 18

Summarizing Report Components

Objectives

- Compare and contrast the important components of written reports.

Lesson 18

Topic 18A

Identify Report Audience

Identify Report Audience

- One of the important considerations when you are creating a PenTest report is to determine the target audience.

- Different engagements will have different sets of stakeholders from the organization whose information systems are being tested.

- The stakeholders can include:
  - Upper-level managers, IT management and personnel
  - The client's security or IT team along with consultants

Providing Details to the Stakeholders

- **C-Suite** - top-level management personnel, i.e., CEO and CTO who are responsible for making decisions based on the results.
- **Third-Party Stakeholders** - not directly involved with the PenTest
    - May still be involved in a process related to the PenTest report.
    - Providers, investors, regulators, and similar entities.
- **Technical Staff** - personnel that maintains the systems
- **Developers** - personnel responsible for creating solutions

Review Activity: Identify Report Audience

- Explain the importance of identifying the report audience when preparing the PenTest report
- List some of the stakeholders involved in a PenTest

Lesson 18

Topic 18B

List Report Contents

Defining the Executive Summary

- An executive summary is a high-level and concise overview of the penetration test, its findings, and their impact.
  - It can range from two paragraph to two pages, depending on the client’s objective, the industry, the size of the organization, and other factors.
- Provides a summary of the process and results:
  - Brief and simple explanation of the procedure, notable findings expressed in a non-technical manner, and some of their implications.
- It is recommended to end with a conclusion statement

Outlining the Scope Details

- Details the scope that was defined for the activity during the pre-engagement phase.
  - Includes any deviation from the original scope that were requested by the client, or unexpected events that changed the course of action.
- This section is a formality, as the client should already be fully aware of the original scope and any deviations

Stepping through the Methodology

- Methodology is a high-level description of the standards or framework that were followed to conduct the penetration test.
- Outlines the activities performed, usually in a generic manner
- The team might mention some additional details:
  - What is being targeted on each portion of the testing, and what tools, techniques, and procedures were used for each.

Detailing the Attack Narrative

- The attack narrative is a detailed explanation of the steps taken while performing the activities.
- Guides the reader through the process performed by the team
  - It should show correlation between the methodology that was mentioned, and the activities performed.
- In cases where an event occurred that modified the scope, the attack narrative would mention this and show what followed.
  - It will commonly express, in detail, about paths and whether exploits were successful, while only briefly talking about the rest.

Listing the Findings

- This section shows the issues that were identified during the activity. Often presented with a table that identifies:
  - The vulnerability, the threat level, the risk rating
  - Whether the vulnerability was able to be exploited.
- When tailoring the report to the client’s objective and risk appetite:
  - Consider elements such as critical vulnerabilities, attack vectors successfully exploited, and other results.
- This section should include steps that can be independently repeated so the findings can be validated.

Determining Risk Appetite

- Risk appetite refers to the amount and type of potential threats and vulnerabilities the organization is willing to tolerate and endure.
- The key stakeholders need to determine their risk appetite by answering questions such as:
  - What losses would be catastrophic to the organization?
  - What processes, technology, or other assets can be unavailable and still enable the organization to function and for how long?
- Your PenTest report should account for the client's risk appetite.

Risk Rating (Reference Framework)

- Risk rating is the process of assigning quantitative values to the identified risks.
  - Usually done by following a *reference framework*, which is a method to consistently rate findings.
- To achieve consistency, relevant elements need to be considered,
  - Exploit ability and the location where the vulnerability is located.
- There are established systems that can further enhance risk ratings,
  - CVSS, as well as cybersecurity frameworks such as NIST CSF

Prioritizing Risk

- Risk prioritization is the process of adjusting the final rating of vulnerabilities to the client needs.
- Depending on their industry and other factors, you and the client need to work together to prioritize the results of your testing.
- You may need to consider items that include:
  - PII and PHI in addition to other factors such as network accessibility, building accessibility, and the like.
- These can all influence how you prioritize the results of the PenTest.

Analyzing Possible Business Impact

- A business impact analysis (BIA) involves estimating the possible effects to the client
  - If issues identified were to be targeted by a malicious actor.
- This section of the report will provide a better understanding of the relationship between the findings and their implications
- Will allow the client to better determine the priority given to allocating resources to implement resolutions to the findings.

Defining Metrics and Measures

- Metrics are *quantifiable* measurements of the status of results or processes.
  - An example of a metric related to PenTesting is the criticality of vulnerability findings. This metric can be expressed on a scale, for example, from 1 to 10.
- Metrics and measures can be shown as tables or graphs to better display the results and allow for easy analysis
  - Such as year-to-year changes in the number of successfully exploited attack vectors.

Suggesting Remediation

- Remediation defines possible solutions to issues identified during the PenTest.
- Present as many options as you can when listing recommendations.
- Giving the client options enables them to choose the solution that is right for them and their organization. For example:
    - Weak password complexity - Configure minimum password requirements.
    - No multi-factor authentication Implement MFA in applicable systems.

Outlining the Final Report Sections

- Conclusion - wraps up the report. Key elements include:
  - A general summary statement about failures and successes, with supporting evidence that can be written in a sentence or two.
  - A statement of the PenTest goals and whether those goals were met.
- Appendix - any supporting evidence, or attestation of findings.
  - Can include printouts of test results, screenshots of network activity, and other evidence you obtained during testing.
  - Can include full versions of some of the highlights done in the report or a reference to a file if provided as attachment.

Review Activity: List Report Contents

- Outline what’s included in the Executive Summary
- Explain how to present the Scope Details
- Review what’s included in the methodology section
- Discuss the significance of the attack narrative
- Describe how best to present the findings
- List ways the team can determine the client’s risk appetite

Review Activity: List Report Contents

- Explain the concept of rating and prioritizing risks
- Outline how a business impact analysis (BIA) factors into the PenTest
- Compare how Metrics and Measures are used during the PenTest
- Describe how the team can present remediation recommendations
- List components in the final report sections

Lesson 18

Topic 18C

Define Best Practices for Reports

Storing Reports

- Depending on different factors, you will need to define storage time for reports and supporting documentation.
  - Best practice is to maintain document control of stored reports, as well as other relevant information.
- In general, you should consider implementing the following components into the reports:
  - Cover page, Document properties, and Version control

Securing Report Distribution

- PenTest reports contain highly detailed information about the areas that are vulnerable to attack
    - Take precautions to prevent the reports from falling into the wrong hands.
    - If possible, store the reports on a secure server so that only the appropriate personnel can view the details of the full report.
- There are likely some parts of the report that need to be made available to additional personnel.
    - For this reason, consider storing reports in repositories where parts of the report can be secured with varying levels of access.

Best Practices for Handling Reports

- Maintain the confidentiality and integrity of reports
- Ensure reports are available to the relevant audience
- Minimize the transmission of reports across a public network
- Maintain audit logs for users accessing reports.
- Maintain a chain of custody when transferring ownership of reports.
- Maintain version control for changes to reports.

Taking Notes

- Note taking helps keep track of details that occurred during the activities that you do not want to miss mentioning in the report.
- Notes are generally for internal use it tends to be more flexible regarding the needs of each penetration testing team
    - If asked about the engagement, you can refer to your notes for any additional information that you may need.
- It will be important to tailor your note taking depending on your needs and the client’s.

Ongoing Documentation During Tests

- Documenting during the tests will help you greatly when writing your penetration testing report
  - Due to its importance, it is commonly regarded as a mandatory process.
- Documenting your findings can be invaluable as proof to show the client and to prove your findings.
- Alternately, and notably, not being able to provide evidence for the claims in the report will greatly reduce its credibility.
  - This could translate, in worst cases, to your client failing a cybersecurity recertification process.

Grabbing Screenshots

- Screenshots are a key component of ongoing documentation.
  - From these you can provide both evidence that an attack path was successful as well as provide a different insight on the attack rather than just text.
- Grab only the relevant sections to minimize capturing information that is not needed for the report.
  - Work with the client to determine how to properly handle those events.

Recognizing Common Themes/Root Causes

- As you analyze vulnerability scan results, you can encounter recurring conditions and/or common themes. These can include:
    - Lax physical security or use of obsolete cryptographic protocols
    - Employees not following corporate policy or best practices, or lack of adequate cybersecurity training
- Identifying common themes provides you with a more complete picture of your target environment and its weaknesses.

Identifying Vulnerabilities

- The full list of vulnerabilities that were identified can be useful not only to the client but also to the team itself.
  - The information can provide insight on which high-rated vulnerabilities were not successfully exploited by the team and do further research on those.
  - It can also provide useful information to the team regarding which are the most exploited vulnerabilities as discussed in Common Themes/Root Causes.
- You can always provide the full vulnerability details in the appendix of the report or as a separate file to keep the report concise.

Outlining Best Practices

- Using Vulnerabilities and Common Themes/Root Causes:
  - The team can derive a consistent list of best practices and show where clients usually lack these controls.
  - It is also common to find industry-related best practices for the client and keep track of these during the activities

Providing Observations

- Observations include general details about the PenTest:
  - Conclusions made from information we gathered
  - Important highlights of issues found
  - Actions taken to resolve them
  - Notes to keep in mind for the next retest.
  - Statements such as deviations from scope, changes in priority
  - Other elements that should be considered for the report

Review Activity: Define Best Practices for Reports

- Discuss different factors to consider when storing and distributing the PenTest reports
- List some best practices for handling reports
- Review reasons the team might take notes and grab screenshots
- Describe the importance of providing ongoing documentation
- Explain how the team can identify common themes/root causes
- Outline how best to present the vulnerabilities identified
- List examples of observations on details about the PenTest

Lesson 18

Summary