Task ‘Case Study Reviewing an Assessment Reporting Template’ Unit 5

Case Study: Reviewing an Assessment Reporting Template

PurpleSec

Penetration Testing and Baseline Evaluation Report

Introduction

Penetration testing is a method for assessing IT system's security ethically and in a controlled manner, identifying and testing the exploitability of weaknesses. It is not designed to be used as a vulnerability identification exercise, but as a method to validate security the effectiveness of controls and processes in place. The NCSC recommends penetration testing to be planned and conducted with a clear scope and objectives in mind, to complement security activities, not replace them. Effective testing requires preparation, scoping, and integration into risk management procedures. Without such activities, organizations risk obtaining technical findings without improving security.

(NCSC, 2022).

Objectives and Scope

The primary goal of the assessment was to validate if the PurpleSec’s template defines the right techniques designed to effectively identify weaknesses and measure their exportability. The exercise aimed to determine conformity of the document with the NCSC guidelines. Looking forward to assuring if the information in document provides an effective and ethical pen testing guidelines or not.

(NCSC, 2022).

Methodology and Approach

This analysis will look to identify any gap in the document’s completeness as a penetration testing guide and highlight those in a structured manner.

Compliance with NCSC Principles

The PurpleSec template follows a procedure for scanning for vulnerabilities using Nessus where findings are categorized into Critical, High, Medium, and Low severity levels, providing prioritization guidance and remediation measures to address risks in a proactive manner which is aligned with NCSC recommendations to deliver actionable outcomes; however, it falls short of fully reflecting NCSC guidance on preparation and baseline definition. It presents findings as a point-in-time snapshot rather than validating security controls against a documented reference state.

(NCSC, 2022).

1. Findings and Analysis

1.1. Does the Template Meet the NCSC Baseline Requirement?

The PurpleSec template does not sufficiently meet the NCSC requirement of preparing a baseline reference point for penetration testing here are some of the reasons why:

The report focuses on:

- Scan results.
- Vulnerability focused methodology.
- Findings by severity.
- Risk assessment and remediation.

The report does not focus on:

- Define expected scope of testing for exploitability.
- Provide asset classification.
- Establish measurable baseline metrics.
- Compare results to previous assessments.

This report is a limited snapshot missing requirements for a proper baseline for penetration testing lacks sufficient framing. While some findings and remediation recommendations are solid, other elements are missing. Overall, the report is missing broader coverage of structure and ethical hacking, reducing its effectiveness.

(NCSC, 2022).

1.2. What are the two best lessons/examples presented in the report?

To align with NCSC expectations, the Document needs the following adjustments:

- A baseline definition section. Document requires expected configurations, patch levels, and security standards.
- An asset inventory, classification with Identification of critical systems and expected configurations before testing.

- Incorporate Baseline Metrics with define acceptable vulnerability thresholds and patch compliance rates.
- Comparative analysis that Includes trend data from previous assessments.
- A clear scope alignment that clearly reflects baseline objectives.

These changes make the template a much more baseline-supported assessment suitable for guiding penetration testing.

(NCSC, 2022).

1.3. Best Lessons Presented

Structured Findings by Severity

Categorizing vulnerabilities into Critical, High, Medium, and Low, which provides strong prioritization, this helps risk-based remediation and demonstrates the ability to analyze and manage network threats effectively.

1.4. What two things do you think are unnecessary or could be done more effectively?

The definition of a clear scope and objectives is necessary. So is definition of expectations. This ensures a clear structure and outcome.

Including a list of exploits found and actionable remediation steps will ensure that the report prompts mitigation rather than a simple detection. This aligns with the solutions design that is meant to manage and audit risk.

(NCSC, 2022).

1.5. Areas for Improvement

Excessive Technical Detail in Main Body

The Inclusion of full scanner output reduces clarity for senior stakeholders. Raw data would be better placed in an appendix with executive-level summaries in the core document.

Lack of Contextual and Trend Analysis

The report does not interpret patterns or recurring weaknesses. Adding trend analysis would enhance risk evaluation and demonstrate synthesis of multiple information sources.

2. Reflection

Challenges

One challenge task was distinguishing between a vulnerability assessment and a penetration test structure. Initially, the report appeared comprehensive; however, a deeper analysis of the NCSC guidance revealed some major structural gaps.

(NCSC, 2022).

Overcoming Challenges

The challenge was overcome by examining the NCSC best-practice guidelines, in detail and analyzing the approach to eventually propose a more solid baseline for penetration testing frameworks.

(NCSC, 2022).

Impact on Final Report

This experience will strengthen the final report by ensuring clearer alignment between methodology, scope, and measurable security baselines. Greater emphasis will be placed on analytical insight rather than descriptive findings.

2.2. Learning Outcomes Achieved

This activity had enabled me to differentiate between the identification and analysis of vulnerabilities, in networked systems and the evaluation of appropriate methodologies, as well as the structure of more comprehensive penetration testing. It supported critical examination of a proper reporting structures and strengthened my ability to understand how to improve presentation of information from vulnerability reports to executives and against best practices guidance into a structured security analysis.

(NCSC, 2022).

Conclusion

The PurpleSec template provides a clear exposure categorization and actionable remediation advice to some degree, making it partially effective as a vulnerability assessment report. However, it does not fully meet the NCSC recommendations of a baseline reference establishment for penetration testing. for instance, incorporating baseline pre-requisites, metrics, scoping, reporting and exploitation of a vulnerabilities which would evolve into a stronger assurance tool aligned with NCSC principles.

(NCSC, 2022).

References

NCSC (2022) ‘Advice on how to get the most from penetration testing’. Available at: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed: 16 February 2026].