Penetration Testing Writing the Report

Dr Diarmuid Ó Briain

26 Apr 2024

Learning objectives

By the end of this topic, you will be able to:

- Write a Penetration Test report.

Report Development Stages

Report Objectives

- Why the pentesting activity is conducted and the benefit of it.
- Typically Report Objectives can be found in:
  - The RFP,
  - A sub-section of risk analysis,
  - Part of compliance,
  - The current status of the target testing environment.

Test Window

- Mission-Critical Infrastructure
  - During testing of critical systems, key IT personnel need to be readily available.
- Dynamic IT Environments
  - If the IT infrastructure undergoes frequent changes, it's crucial to freeze the scope of the pentest
- Time-Bound Risk Assessment
  - Penetration testing report identifies vulnerabilities within the defined testing window
  - New risks may emerge after this period due to changes in the IT infrastructure or configuration.

Plan for Effective Penetration Test Reporting

- During project planning, allocation of sufficient time for report writing is crucial.
- To streamline the process and maintain focus, consider dividing report writing into manageable tasks.
- Consider this recommended approach:
  - **Structure Your Report**: Plan the report structure upfront. This ensures a well-organised and effective final product.
  - **Allocate Time for Writing**: Allocate at least 60% of your time to writing the initial draft.
  - **Factor in Client Acceptance**: Account for the client's acceptance process, as it may extend the overall timeline.

Plan for Effective Penetration Test Reporting

- Some tips to consider, write the report with:
  - A Clear and concise title
  - A Strong opening
  - Actionable steps
  - A Focus on benefits
  - A Formal tone

Tailor PenTest Reports for Diverse Audiences

- Pentests reports cater to various stakeholders within an organisation
- To ensure effective communication, these reports typically adopt a hierarchical structure, presenting information at different levels of detail.
- Consider the following characteristics of your target audience:
  - Purpose
  - Organisational Role
  - Technical Expertise
  - Decision-Making Authority.

Tailor PenTest Reports for Diverse Audiences

- The scope of work document often provides further details regarding the specific target audiences and the depth of technical information required.
- Typical pentest audiences include:
  - Information Security Manager
  - Chief Information Security Officer (CISO)
  - Information Technology Manager
  - Technical Teams.

Penetration Test Report Confidentiality

- Pentest reports contain sensitive information, including:
  - Server Internet Protocol (IP) addresses and details
  - Application information
  - Vulnerabilities
  - Threats
  - Exploits.

Penetration Test Report Confidentiality

- Due to this sensitive nature, these reports warrant a high level of confidentiality.
- The specific classification level to be determined based on the target organisation's information classification policy.
- Typical classifications include:
  - Top Secret (TS)
  - Secret
  - Confidential
  - Restricted
  - Official
  - Unclassified.

Controlled Report Distribution

- Pentest reports contain sensitive information, so strict controls are necessary to ensure they reach the right recipients at the appropriate time.
- These controls typically address:
  - Number of Copies
  - Report Format
  - Delivery Procedures.

Hardcopy

- Limit the number printed and maintaining a record of recipients with copy numbers enhances control
- Each recipient should formally acknowledge receipt of the hardcopy.

Copy Number	Department	Name	Date

Softcopies

- Softcopies require careful control.
- Some best practices:
  - Secure Storage
  - Access Controls
  - Data Erasure.

Ethical Considerations

- An SLA should clearly outline data deletion procedures.
- Pentesters have an ethical obligation to maintain report confidentiality.
- This includes deleting reports and not sharing them with any unauthorised parties.

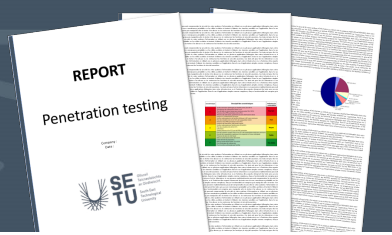
Information Gathering Strategies

- Pentesters should meticulously collect information at every stage of the test, including:
  - Scanning Results
  - Vulnerability Assessments
  - Exploit Findings
  - Screenshots
  - Detailed Notes
  - Activity Logs.

Composing the Initial Report Draft

- Once all the information has been compiled the the first draft of the report can be written.
- Some key points to consider are:
  - Focus on Content, Not Perfection
  - Time Allocation
  - Using Placeholders.

Report Format



Cover Page

- The cover page will show:
  - the report name
  - report version
  - date
  - author/service provider name
  - Serial number
  - Target organisations name.

Penetration Test Report for Delta Corporation

Version 1.0
April 5, 2024

Theta Limited

Serial No. PEN-2024-001

Delta Corporation

Document Properties and Version Control

Document Properties

Title	Penetration Testing Report for Delta Corp
Version	v1.0
Author	Ada Lovelace
Pen-testers	Ada Lovelace and Charles Babbage
Approved By	Luigi Federico Menabrea
Classification	Secret

Version Control

Version	Date	Author	Description
v1.0	27 April 2024	Ada Lovelace	Initial Document

TOC and List of Figures

- Table of Contents
  - Table of contents, a list of all the sections of the report in a sequence with the page numbers.
  - If the report includes some appendices, the titles of these should be listed also.
- List of Figures
  - If there are tables or charts included in the report, list them in this section with page numbers.

Executive Summary

- Leave this section to complete after the remainder of the report is completed.
- This is an executive summary of the report content in a small paragraph containing a statement of the tasks accomplished, methodology used, high level findings and recommendations.
- The executive summery target the executives where high level findings/issues need to be raised and recommended solutions need to be presented.

Scope of Work

- Clearly identify the scope of the project, equipment and IP addresses of that equipment that was subject to tested.
- The type of Pentest perform and any other information that affected the time and budget of the project.

Project Objectives

- List the objectives that the organisation will gain once the have identified the risks related to the penetration of the target equipment, system or application and what the improved cyber posture after mitigating these risks through the implementation of the recommendations in the Pentest report.
- Each pentest objective must to be aligned with the information security objectives, which in turn should be aligned with the organisation's objectives.
- If the Pentest is part of a compliance project, then the report needs to mention this requirement and how the pentesting will help achieve it.

Timeline

Pentest	Start Date – Time	End Date – Time
Test the Firewall from the level 4/5 Enterprise	4/4/24 – 09:30hrs	4/4/24 – 17:30hrs
Test the Scada Server in level 3 MOS	5/4/24 – 09:30hrs	7/4/24 – 17:30hrs
Test the PLCs in level 1 Intelligent Devices	5/4/24 – 09:30hrs	6/4/24 – 17:30hrs
Test the HMIs in level 2 Control Systems	6/4/24 – 09:30hrs	7/4/24 – 17:30hrs

Summary of Findings

Value	Number of Risks	Percentage of the Risk
Low	2	14%
Medium	7	50%
High	4	29%
Critical	1	7%

- Dashboard style
- Narrative beneath.

Summary of Findings

- Here's a breakdown of the key findings and recommended improvements:
  - **Inadequate of Firewall Protection**: Both identified servers lacked sufficent firewall protection, exposing services such as Microsoft Terminal Services presents a significant risk.
  - **Inadequate Patch Management**: Server, D234, IP address: 172.16.23.34, was found running an unpatched Windows 2000 system, creating a high security risk.
  - **Insecure Service Configurations**: Services such as File Transfer Protocol (FTP) were operating with default configurations, lacking proper security measures. Additionally, the web application on D245, IP address: 172.16.23.45, displayed vulnerabilities such as SQL injection and Cross Site Scripting (XSS), potentially compromising customer data.

Methodology

- The methodology section should detail the pen testing approach.
- This includes outlining the information gathering steps, the analysis methods used, the risk rating methodology employed to assess vulnerabilities, and a list of the tools utilised at each stage of the testing process.
- This transparency allows for a better understanding of how the testing was conducted and the rationale behind the findings.

Planning

- This section details the information gathering and reconnaissance activities conducted prior to active testing.
- **Information Gathering**: This may include details on:
  - Scope of the engagement (authorised systems and exclusions)
  - Network topology (high-level overview)
  - Operating Systems and applications identified through DNS records, employee interviews, or other means.
- **Detection of Live Systems**
- **Reconnaissance and Scanning**: This may include:
  - Services and protocols running on target systems
  - Vulnerability scanning tools employed and the types of vulnerabilities scanned for
  - Fingerprinting techniques used to identify specific versions of software and services.

Exploitation

- This section describes the process of attempting to exploit identified vulnerabilities.
  - **Vulnerability Assessment**
  - **Enumeration and Exploitation**: This may include:
    - Manual exploitation techniques leveraging known exploits or privilege escalation methods
    - Automated exploitation tools used for specific vulnerabilities
    - Development of custom exploits for unique vulnerabilities.

Reporting

- This section outlines the content and structure of the final Pentest report.
  - **Finding Analysis**: This may include:
    - Technical details of the vulnerability (e.g., CVE ID, description)
    - Steps taken to exploit the vulnerability (proof of concept)
    - Potential impact of successful exploitation on Safety, Availability, Integrity and Confidentiality.
  - **Risk Calculation and Rating**: This may involve a risk matrix that considers factors such as:
    - Likelihood of exploitation (based on ease of attack and attacker motivation)
    - Impact of a successful attack (severity of consequences)
    - Criticality of the affected asset
  - **Reporting**: This may include:
    - Executive summary highlighting key findings and risks
    - Detailed methodology section outlining the testing approach
    - Findings section with individual vulnerability descriptions, exploit details, impact assessments, and risk ratings
    - Recommendations section outlining mitigation strategies for identified vulnerabilities
    - Appendices containing supplementary information (optional, may include detailed scan results or exploitation scripts)

Detailed Findings

- Pentesting reports should present detailed findings in a clear and concise manner.
- Summaise each finding with:
  - **Threat Level**
  - **Vulnerability Rating**
  - **Potential Impact**
  - **Likelihood**
  - **Risk Rating**
  - **Recommendations.**

References

- Include a section listing precise details of all the work by other authors, which has been referred to within the report. Include:
  - Author's name and initials
  - Date of publication
  - Title of the book, paper or journal
  - Publisher
  - Place of publication
  - Page numbers
  - Details of the journal volume in which the article has appeared.
- References should be listed in alphabetical order of the authors' names. Make sure that references are accurate and comprehensive.

Appendices and Glossary

- **Appendices**
  - A space for supplementary information that provides valuable context but isn't crucial to understanding the core findings.
  - While these appendices can be a valuable resource for readers seeking a deeper understanding, the main report itself should be structured to be self-contained, with all essential findings and recommendations clearly presented without relying on the appendix.
- **Glossary**
  - Include a glossary of terms used in the report.

Learning objectives

- Write a Penetration Test report. ✓

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An Iarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CISSP®

Thank you

TUS