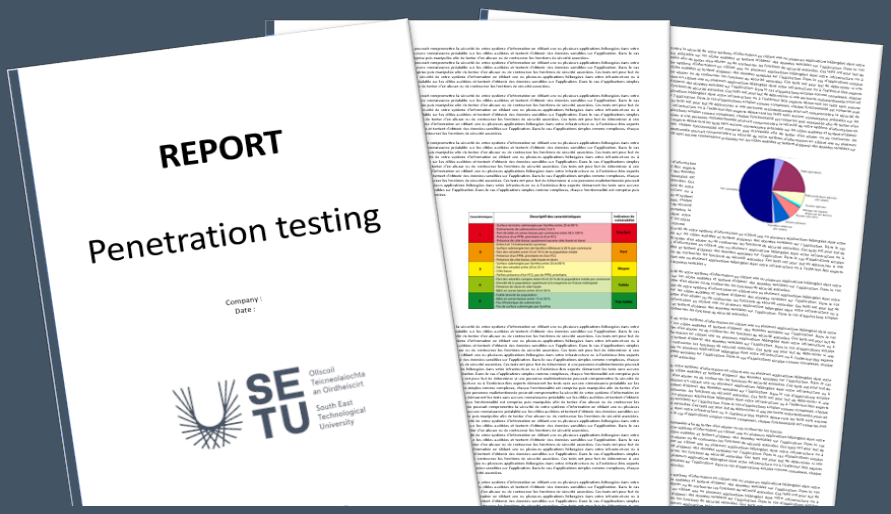
Cybersecurity for Industrial Networks

Topic 9
Penetration Test
Writing the Report



Dr Diarmuid Ó Briain

Version: 1.0

SE TU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Objectives

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

- Write a Penetration Testing (pentest) Report.

2 Introduction

This topic highlights the critical, yet often overlooked, aspect of report writing within the pentest domain. While numerous resources exist to guide the technical execution of pentests, a significant gap remains that can undermine the pentest exercise.

A pentest report is a formal documentation of findings, presenting the results of the pentest while also capturing specific details where definitive information is required. A pentest, without a tangible report to convey the test's outcome to clients or executive stakeholders, loses its purpose. The report meticulously details all the test's findings and, if applicable, propose concrete recommendations for securing high-risk systems.

The significance of pentest report writing extends beyond merely fulfilling a deliverable requirement. It becomes an essential component for service providers, particularly within the realm of IT and OT services. The well-known adage in the consulting industry in particular is: "*If you do not document it, it did not happen*".

A well-structured pentest report should outline the methodology employed but also comprehensively detail the findings of the vulnerability assessment and pentest conducted on the target system. Furthermore, the report should provide specific and actionable recommendations to assist in mitigating identified risks.

It is essential to acknowledge that the target audience for a pentest report can vary. The executive summary is typically geared towards senior management, providing a high-level overview of the findings. Conversely, the technical details contained within the report are intended for operations personnel and information security professionals.

3 Report Development Stages

Figure 1: Report Development Stages

This topic proposes a conventional approach to developing a comprehensive pentest report, encompassing a series of distinct stages including:

- Report Planning,
- Information Collection,
- Writing the First Draft,
- Reviewing and Finalisation.

By adhering to this structured approach, pentesters can ensure the creation of professional and informative reports, ultimately enhancing the value derived from the pentest exercise itself.

4 Report Planning

4.1 Report Objectives

Report objectives explain why the pentesting activity is conducted and the benefit of it. These objectives can typically be found in the Request for Proposal (RFP), be a sub-section of risk analysis, be part of compliance or to know the current status of the target testing environment.

4.2 Pentest Window

Pentesting requires a defined testing window for several critical reasons:

- **Mission-Critical Infrastructure**: During testing of critical systems, key Information Technology (IT) personnel need to be readily available. This ensures they can address any unforeseen issues, like server crashes, that might arise during the test.
- **Dynamic IT Environments**: If the IT infrastructure undergoes frequent changes, it's crucial to freeze the scope of the pentest. This ensures the test accurately reflects the current state of the IT systems being assessed.
- **Time-Bound Risk Assessment**: While perfect security does not exist, the pentest report identifies vulnerabilities within the defined testing window. New risks may emerge after this period due to changes in the IT infrastructure or configuration.

4.3 Plan for Effective Pentest 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.

By following these steps, a penetration test report can be delivered efficiently and meet the client's expectation. Some tips to consider, write the report with:

- **a Clear and Concise title**: Focuses on planning the report writing.
- **a Strong opening**: Emphasises the importance of planning for report delivery.
- **Actionable steps**: Provides a three-step approach for effective report writing.
- **a Focus on Benefits**: Highlights the advantages of structured planning.
- **a Formal tone**: Maintain a professional tone suitable for pentest reports.

4.4 Tailor Pentest Reports for Diverse Audiences

Penetration testing 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. It is therefore important to understanding the potential audience when designing the report format and style, consider the following characteristics of your target audience:

- **Purpose**: Identify how each audience member will utilise the report (e.g., operational planning, resource allocation, approval).
- **Organisational Role**: Tailor content based on the recipient's position (e.g., Information Security Manager, Chief Information Security Officer (CISO), Information Technology Manager, technical teams).
- **Technical Expertise**: Assess their prior knowledge of pentesting concepts.
- **Decision-Making Authority**: Emphasise findings relevant to their decision-making capabilities.

The Scope of Work (SoW) 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.

4.5 Pentest Report Confidentiality

Pentest reports contain sensitive information, including:

- Server Internet Protocol (IP) addresses and details,
- Application information,
- Vulnerabilities,
- Threats,
- Exploits.

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.

4.6 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**: The scope of work should define the number of report copies printed (hardcopy) or distributed electronically (softcopy).
- **Report Format**: The scope of work will also specify whether a hardcopy or softcopy format is preferred.
- **Delivery Procedures**: A secure delivery method should be established to ensure reports reach authorised personnel.

4.6.1 Hardcopy Distribution

Copy Number	Department	Name	Date

Figure 2: Pentest Report Distribution Control

For hardcopies, limiting the number printed and maintaining a record of recipients with copy numbers enhances control as illustrated in Figure 2. Each recipient should formally acknowledge receipt of the hardcopy.

4.6.2 Softcopy Distribution

Softcopies require careful control. Here are some best practices:

- **Secure Storage**: Store softcopies on a secure server managed by the department requesting the penetration test.
- **Access Controls**: Limit access to authorised personnel only. The report owner holds responsibility for managing access.
- **Data Erasure**: After report submission, pentesters should delete all copies of the report and related information.

4.6.3 Ethical Considerations

A Service Level Agreement (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.

4.7 Comprehensive Information Gathering in the Pentest

Effective pentesting hinges on thorough information collection throughout the entire process. This ensures all necessary details are readily available for report writing and analysis.

4.7.1 Importance of Information Collection

Streamlined Report Writing: Having all information documented at each stage simplifies report generation.

Enhanced Analysis: Captured data facilitates in-depth analysis of findings and vulnerabilities.

Collaboration (For Teams): In a team setting, a centralised and secure information repository fosters collaboration.

4.7.2 Information Gathering Strategies

Pentesters should meticulously collect information at every stage of the test, including:

- **Scanning Results**: Document the output of vulnerability scanning tools.
- **Vulnerability Assessments**: Record the details and severity of identified vulnerabilities.
- **Exploit Findings**: If applicable, capture successful exploitation attempts (with proper authorisation).
- **Screenshots**: Take screenshots to visually document findings.
- **Detailed Notes**: Maintain comprehensive notes throughout the testing process.
- **Activity Logs**: Logging all activities provides an audit trail, especially valuable in critical infrastructure testing.

4.8 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**: This stage prioritises capturing all the information gathered. Proofreading and editing come later.
- **Time Allocation**: Allocate approximately 60% of report writing time is dedicated to crafting the initial draft.
- **Using Placeholders**: It's helpful to use placeholders, such as "#" or highlights, to mark areas that need further editing or verification. Simply remove these markers once the edits are complete.

4.8.1 Tips for a Smooth Drafting Process:

- **Structure**: Consider outlining your report beforehand to ensure a logical flow of information.
- **Clarity and Conciseness**: Strive to write clearly and concisely, avoiding unnecessary jargon.
- **Supporting Evidence**: Integrate the information you collected (e.g., scan results, vulnerability assessments) to support your findings.

5 Report Format

This section describes the pentest report format and why each subsection is required. Report planning should include page design decisions to establish the report's visual style. This encompasses elements like header and footer content, fonts, and colour scheme. Ideally, these design choices should align with the service provider's existing branding guidelines.

5.1 Cover Page

The cover page will show:

- The report name,
- Pentest report version,
- Date,
- Aauthor/service provider name,
- Serial number
- Target organisations name.

For example:

Penetration Test Report for Delta Corporation

Version 1.0
April 5, 2024

Theta Limited

Serial No. PEN-2024-001

Delta Corporation

5.2 Document Properties and Version Control

On the first page, in two small tables. In the first, list the document title, version, author, pentesters name, name of persons whom reviewed the report, approved by whom and the document classification. In the second table list the Version Control for the report to include the version, date of change, Author and Description.

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	4 April 2024	Ada Lovelace	Initial Document

5.3 Table of Contents

The table of contents is 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.

5.3.1 List of Figures

If there are tables or charts included in the report, list them in this section with page numbers.

5.4 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.

5.5 Scope of Work

The SoW clearly identifies the scope of the project, equipment and IP addresses of that equipment that was subject to tested. The type of pentest performed and any other information that affected the time and budget of the project.

5.6 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. For example:

- **Evaluate Security Posture**: Assess the security posture of Delta Corp's manufacturing zone. This likely involves testing for vulnerabilities and misconfigurations that could be exploited by attackers.
- **Identify Exploitable Vulnerabilities**: Focus on identifying vulnerabilities that could be immediately exploited by attackers. This prioritises critical vulnerabilities due to the limited time available for the assessment.
    - **Risk Assessment**: Assign risk ratings to identified vulnerabilities based on a combination of factors:
    - **Threat**: The likelihood of an attacker attempting to exploit the vulnerability.
    - **Vulnerability**: The severity and ease of exploitation of the vulnerability.
    - **Impact**: The potential consequences of a successful attack exploiting the vulnerability.

5.7 Assumptions

Should there be some assumptions that the pentester is forced to consider before or during the pentest, then these assumptions need to be clearly listed in the report. Providing the assumptions will guide the report audience to understand why pentest followed a specific direction.

5.8 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

5.9 Summary of Findings

In a dashboard style view illustrate the number of discovered risks based on priorities. When the report of findings is written, be careful to avoid statements that are inflammatory, unsupported by the evidence, speculative, or overly frightening.

For Example:

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

The penetration test identified security gaps in Delta Corp's Operational Technology (OT) environment. Specifically through the test, access was gained to a server within a short timeframe, highlighting the need for a more robust Defence-in-Depth (DiD) strategy. This approach should encompass multiple security layers to safeguard Delta Corp's critical OT assets. Beyond technical measures, it's essential to strengthen processes and employee security awareness. Implementing system and network hardening practices along with secure configurations will reinforce Delta Corp's overall security posture. In short, a layered defence across technology, procedures, and personnel is crucial for Delta Corp to achieve a stronger security level.

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.

5.10 Summary of Recommendation

Based on the analysis of risks and the high level finding, the high level recommendations for the target organisation must be described. For example:

Following a thorough risk analysis and penetration testing, the following high-level recommendations are presented to strengthen Delta Corp's OT security posture:

Implement a Defence-in-Depth Firewall Strategy:

- Deploy a robust firewall policy that restricts access to critical systems and services.
- Prioritise essential public services like mail and web access.
- Utilise anti-mapping rules on border routers and primary firewalls to mask the internal network structure from potential attackers.
- Limit access to non-essential services by IP address or disable them altogether to minimise the attack surface.

Enforce Rigorous Patch Management:

- Establish a comprehensive patch management policy that mandates timely updates for all OT systems.
- Ensure consistent enforcement of this policy to address vulnerabilities promptly.

These recommendations focus on fortifying Delta Corp's OT environment by implementing essential security controls.

5.11 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.

5.11.1 Planning

This section details the information gathering and reconnaissance activities conducted prior to active testing.

- **Information Gathering**: Describe the methods used to collect information about the target environment. This may include details on:
  - Scope of the engagement (authorised systems and exclusions)
  - Network topology (high-level overview)
  - Operating Systems and applications identified through Domain Name System (DNS) records, employee interviews, or other means.
- **Detection of Live Systems**: Explain the tools and techniques used to identify active systems within the target network (e.g., ping sweeps, network discovery tools).
- **Reconnaissance and Scanning**: Outline the process of gathering detailed information on identified systems. 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.

5.11.2 Exploitation

This section describes the process of attempting to exploit identified vulnerabilities.

- **Vulnerability Assessment**: Explain how the information gathered in the planning and scanning phases was analysed to assess the severity and potential impact of vulnerabilities. This may involve referencing vulnerability databases or exploit frameworks.
- **Enumeration and Exploitation**: Detail the methods used to exploit vulnerabilities. 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.

5.11.3 Reporting

This section outlines the content and structure of the final Pentest report.

- **Finding Analysis**: Describe how each identified vulnerability is analysed and documented within the report. 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**: Explain the methodology used to calculate risk ratings for identified vulnerabilities. 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**: Briefly describe the structure and content of the final report. 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).

By providing this level of detail within the methodology section, the report offers transparency into the testing process, allowing readers to understand how vulnerabilities were discovered, exploited, and ultimately rated for risk.

5.12 Detailed findings

Pentesting reports should present detailed findings in a clear and concise manner. Each finding should be summarised with its threat level, vulnerability rating, a breakdown of the issue, the potential impact on information assets if exploited, a calculated risk rating, and corresponding recommendations. To enhance readability, consider presenting this data visually using tables, graphs (pie charts, bar charts), or diagrams.

5.12.1 Vulnerabilities

Vulnerabilities within the report should be clearly described, addressing their source (root cause), potential impact, and likelihood of exploitation. Focusing on the root cause, rather than just the symptoms, allows for more effective mitigation strategies that address the underlying issue and prevent the vulnerability from persisting.

5.12.2 Impact

The report should clearly articulate the potential consequences of a successful attack exploiting the identified vulnerability. This explanation should detail the impact on the Safety, Availability, Integrity, and Confidentiality, of the affected information assets.

5.12.3 Likelihood

The report should address the likelihood of a specific vulnerability being exploited, considering factors outlined in industry standards. From a practical standpoint, pentesters often assess this likelihood by considering the combined factors of:

- ease of access to the vulnerability,
- the level of access gained if exploited,
- the difficulty of discovering and exploiting it,
- the value of the targeted asset to the organisation.

Such a comprehensive approach provides a more nuanced understanding of the risk posed by each vulnerability.

5.12.4 Risk evaluation

The report must include clear explanations of how identified risks are assessed and rated. This process involves comparing the estimated risk level (often based on likelihood and impact) against predetermined risk criteria. Risk analysis methodology employed should refer to one of the industry frameworks such as NIST Special Publication 800-30 as an example. This comparison helps determine the overall significance of each risk, enabling prioritised remediation efforts.

5.12.5 Recommendations

A pentest report should not just identify vulnerabilities; it should also provide actionable recommendations for mitigating them. Recommendations should consider the risk rating (likelihood and impact) of the vulnerability and the target OT asset.

For Example:

- **Vulnerability**: Weak authentication protocols for accessing a control system through a web interface.
- **Risk Rating**: High (High likelihood of exploitation and severe potential impact)

Recommendations:

- **Implement Multi-Factor Authentication (MFA)**: This strengthens the login process by requiring a second factor beyond a username and password, such as a security token or biometric authentication. This significantly reduces the risk of unauthorised access even if attacker steals login credentials.
- **Segment Control Systems**: Implement network segmentation to isolate control systems from the Internet and other less secure networks. This limits the attack surface and makes it more difficult for attackers to exploit vulnerabilities in the web interface.
- **Limit Access and Privileges**: Enforce the principle of least privilege – grant users only the minimum level of access required for their role. This minimises the potential damage caused by compromised accounts.

- **Secure Network Communication**: Encrypt communication between the web interface and control systems using secure protocols like HTTPS. This protects data from eavesdropping and man-in-the-middle attacks.

5.13 Additional Resources

The report can reference industry standards such as:

- **ISA/IEC 62443-4-2 - Secure Deployment of Industrial Automation and Control System Devices**: This standard provides guidance on secure deployment practices for OT devices, including secure configuration and access control.
- **ISA/IEC 62443-4-1 - Product Security Requirements for Industrial Automation and Control Systems**: This standard outlines security requirements for OT device manufacturers to consider during development.

5.14 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.

5.15 Appendices

Appendices within a pentest report offer a space for supplementary information that provides valuable context but is not crucial to understanding the core findings. This can include detailed scan results, in-depth vulnerability assessments, or other technical data. 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.

5.16 Glossary

Include a glossary of terms used in the report.