

## Module 14

### Report Writing and Post Testing Actions

## MODULE OBJECTIVE

Learn how to write a comprehensive penetration testing report for the target audience.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Module Objective

In this module, you will learn about the various components of a penetration test report and learn the process of writing a comprehensive report for the target audience. This module will also discuss various post pen testing activities that penetration testers (also referred to as “pen testers”) should perform to complete the contract with the client. The module also contains post-test activities for organizations that will help improve their security posture.



## Penetration Testing Report: An Overview

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Penetration Testing Report: An Overview

This section provides an overview of the penetration testing report, including its goal, included deliverables, audience types, format, types of reports, characteristics of a good report, common mistakes, and details about writing the final report.

## Goal of the Penetration Testing Report



- The penetration testing report is a **structured report that details the findings of the penetration tests** that are conducted for a client.
- The penetration test report is recorded by the involved pen testers such that a one-to-one correspondence exists between the **documentation** and the **testing process**.



### Goal of the Penetration Testing Report

- 1 Help **executive management** make decisions about implementing **security controls** in the organization.
- 2 Help those responsible for information system security implement security controls and **patch any flaw** discovered during pen testing.
- 3 Assure the organization that the testing team sincerely wishes to **improve the organization's security posture**; bear this in mind when writing the report.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Goal of the Penetration Testing Report

In addition to hacking into the system, explaining the hacking process to the client in a step-by-step manner and recommending how to remove or mitigate the risk is essential. The penetration testing report is a structured report that details the findings of the penetration tests that were conducted for a client. The pen testers record the report in such a way that a direct relationship exists between the documentation and the testing process. The report explains what was done and how. The test report provides information about all the phases starting from the test execution phase. The report should disclose all the technical findings that emerged from the assessment of the client's network and also include remediation plans, suggestions, and recommendations for the client that help them implement security controls. It further explains the process followed and assists the client in understanding how they can reduce their risk.

The team performing the test should set the following main objectives in order to achieve the goal of the test report:

- List the security flaws, vulnerabilities, security misconfigurations, and other exploitable resources found during the testing.
- Analyze the options available to mitigate the vulnerability.
- Suggest solutions for security risks.
- Clarify prioritization of corrections for the client's assets
- Recommend actions to prevent possible future cyberattacks.
- Help executive management make decisions about implementing security controls in the organization.



- Help those responsible for information system security implement security controls and patch any flaw discovered during testing.
- Assure the organization that the testing team sincerely wishes to improve the organization's security posture.

## Penetration Testing Deliverables



 Detailed analysis of the **methodology** used

 Penetration testing **reports**

 Evidence of any **successful penetration**

 Supplementary material to **corroborate** the findings

 Documentation on remediation of any identified **security flaws**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Penetration Testing Deliverables

The penetration testing deliverables are the documents that the pen testing team is advised to submit to the organization after completing the testing process. It is recommended that the following documents be provided as part of the test contract:

- A document that offers a detailed analysis of the methodologies used in the testing such as Penetration Testing Execution Standard (PTES), Information Systems Security Assessment Framework (ISSAF), and Open Source Security Testing Methodology Manual (OSSTMM). Each methodology follows a different approach to testing; including the type of cyberattacks performed, scanning techniques used, etc. is advised.
- A test report with detailed information about all the activities performed and their results in a clear standard format
- Evidence of successful tests of the organizational resources in the form of pictures, videos, and documents. Providing detailed information about the affected resources, cyberattacks performed, tools used, etc. is recommended.
- Documents that corroborate the test findings. These documents can include information on the availability of updates, data from the compromised servers, details of the compromised accounts, etc.
- Documents containing tips for remediating the security flaws, eliminating vulnerabilities, and strengthening the security of the tested components

| Report Audience                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Technicians                                                                                                                                                                                                                                                                                                                                                                                                            | Developers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <ul style="list-style-type: none"><li>Such personnel want to know if the organization is secure.</li><li>Provide clarity about the <b>responsible stakeholders</b> when an issue is found.</li><li>Order of <b>priority for corrections</b> to be provided based on the importance of the identified issues<ul style="list-style-type: none"><li>Specify what needs to be fixed first</li></ul></li><li>Discuss terms, metrics, risk mitigation, and financial loss<ul style="list-style-type: none"><li><b>Graphics and statistics</b> are most effective for this audience.</li></ul></li></ul> | <ul style="list-style-type: none"><li>Such personnel are responsible for fixing the identified technical issues and hence require detailed technical information.</li><li>Offer concise <b>recommendations</b>.</li><li>Describe the steps for <b>remediation</b>.</li><li>Offer a prioritized <b>list of corrections</b>.</li></ul>  | <ul style="list-style-type: none"><li>Such personnel required technically detailed information, so that they can <b>fix the code</b>.</li><li>The report is most efficient when a <b>code review</b> is included in the scope.<ul style="list-style-type: none"><li>Details of the <b>weakness</b> if possible</li></ul></li><li>Provide <b>attack scenarios</b> to enhance the remediation requirements.</li><li>Risk-related data should be <b>prioritized by severity</b> and required remediations.</li></ul> |

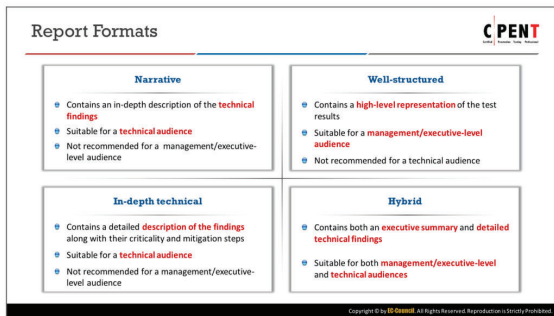
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Report Audience

While developing a penetration testing report, the target audience and their level of understanding of the test results must be considered. Precise reports that describe terms, metrics, risk mitigation, and financial aspects are suitable for a management or executive-level audience. Reports containing in-depth technical descriptions about the findings and their remediation steps are suitable for a technical audience such as IT administrators, network administrators, and developers.

- **Management:** The requirements of the management include the following.
  - Such personnel want to know if the organization is secure.
  - Provide clarity about the responsible stakeholders when an issue is found.
  - Order of priority for corrections to be provided based on the importance of the identified issues
    - Specify what needs to be fixed first.
  - Discuss terms, metrics, risk mitigation, and financial loss.
    - Graphics and statistics are most effective for this audience.
- **Technicians:** The requirements of technicians include the following:
  - Such personnel are responsible for fixing the identified technical issues and hence require detailed technical information.
  - Offer concise recommendations.
  - Describe the steps for remediation.

- Offer a prioritized list of corrections.
- **Developers:** The requirements of developers include the following.
  - Such personnel required technically detailed information, so that they can fix the code.
  - The report is most efficient when a code review is included in the scope.
    - Details of the weakness if possible
  - Provide attack scenarios to enhance remediation requirements.
  - Risk-related data should be prioritized by severity and required remediations.
    - Include effort estimations if available.



## Report Formats

Based on the audience, pen testing reports can be created in four different formats.

- **Narrative:** Narrative reports contain an in-depth description of the technical aspects of the report. Such reports are suitable for a technical audience but not for a management/executive-level audience.
- **Well-structured:** Well-structured reports contain a high-level representation of the test results in the form of charts and graphs. These reports are intended for a management/executive-level audience and are not recommended for a technical audience.
- **In-depth technical:** In-depth technical reports include a detailed description of the findings along with criticality and mitigation steps. Hence, such reports are suitable only for a technical audience.
- **Hybrid:** Hybrid reports contain two sections. The first section includes a summary of the penetration testing project for a management/executive-level audience. The second section includes detailed technical findings intended for a technical audience. Hence, hybrid reports are suitable for all types of audiences.

## Types of Pen Test Reports

|                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Executive Report</b> <ul style="list-style-type: none"><li>It provides a <b>summary</b> of the complete pen testing process, its outcomes, and recommendations.</li></ul>                                                                               | <b>2. Host Report</b> <ul style="list-style-type: none"><li>It provides <b>details</b> of the various <b>hosts</b> that were tested.</li></ul>                                                                               |
| <b>3. Client-Side Test Report</b> <ul style="list-style-type: none"><li>It provides details of the client-side test, including the email template sent, <b>exploits launched</b>, <b>test result</b>, and details about <b>compromised systems</b>.</li></ul> | <b>4. User Report</b> <ul style="list-style-type: none"><li>It provides details of all the users who were <b>identified</b> and <b>targeted</b> during the testing process along with the tasks performed by them.</li></ul> |
| <b>5. Vulnerability Report</b> <ul style="list-style-type: none"><li>It provides details of various <b>vulnerabilities</b> discovered during pen testing.</li></ul>                                                                                           | <b>6. Activity Report</b> <ul style="list-style-type: none"><li>It provides detailed <b>information</b> about all the <b>tasks</b> performed during penetration testing.</li></ul>                                           |

**Note:** All these reports are included in the final penetration testing report.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Types of Pen Test Reports

There are different types of penetrations test reports based on the information they provide.

- **Executive report:** This report is a short briefing of the complete testing process and includes details of the tested components, vulnerabilities, misconfigurations, updates required, and other details that can help the authorities make decisions for securing the target.
- **Host report:** This report provides information about the hosts tested, vulnerabilities found, exploited hosts, etc.
- **Client-side test report:** This report includes the details of the client-side test such as phishing, spear-phishing, spam, and social engineering attacks used during the testing. It also provides detailed information about compromised client-side systems.
- **User report:** This report includes the information of users who were identified and targeted during the testing process along with the tasks performed by them.
- **Vulnerability report:** This report provides detailed information about all the vulnerabilities found during the pen testing process. It is recommended that the report lists the components with vulnerabilities and also offers solutions to eliminate the vulnerabilities.
- **Activity report:** This report includes all the activities that the testing team had performed across the organization and can also include various documents to support the claims.

**Note:** All these reports should be included in the final penetration testing report.

## Characteristics of a Good Pen Testing Report



- The report should be **concise** and **easy to understand**.



- It should be written in a **professional manner** using formal language.



- The final report must clearly state the findings with the help of screenshots showing **Proof of Concepts (PoC)** of the existence of the identified vulnerability and its potential risks.



- It should clearly justify the **recommendations** and **analysis** made by the pen tester.



**Note:** Standard techniques and methodologies should be followed while preparing a report.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Characteristics of a Good Pen Testing Report

A penetration tester must be aware of the process of creating a good penetration testing report. The report must comply with the standard reporting procedures of the client organization and must be acceptable globally.

Characteristics of a good penetration report are as follows:

- It should be written in simple language that everyone can easily understand.
- It should be written in a professional manner using formal language.
- It must be comprehensible to both technical and nontechnical personnel such as security admins and stakeholders.
- It should clearly explain the purpose of the penetration test as well as that of writing the report.
- It should provide complete information to the reader in a clear format and not contain unnecessary information.
- It should be grammatically correct, punctuated appropriately, and free of typographical errors.
- It should provide accurate information and support it with proper evidence, such as screenshots of the test results and stolen credentials.
- It should not contain biased information.
- It must contain information sorted according to the security risks, with the highest risks being prioritized.

- It should be structured logically.
- The style of presentation and the usage of words should be attractive to readers.
- It should contain screenshots and other findings such as obtained open ports information and results obtained from tools, which act as evidence for the identified vulnerabilities and their potential risks.
- It should contain unbiased recommendations and suggestions based on the analysis by the pen testers

**Note:** Standard techniques and methodologies should be followed while preparing a report.



## Common Mistakes



- ✎ Not understanding the scope of the pen testing service
- ✎ Not asking for a retest
- ✎ Not asking for a letter of attestation
- ✎ Using a vendor without creating and signing a contract
- ✎ Not receiving guidance on the type of test to conduct
- ✎ Not asking for a detailed debrief or report walkthrough
- ✎ Not asking for a report with detailed steps and reproducible results

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Common Mistakes

Some of the common mistakes made by organizations initiating a penetration testing process are discussed below:

- Not understanding the scope of the pen testing service
- Not asking for a retest
- Not asking for a letter of attestation
- Using a vendor without creating and signing a contract
- Not receiving guidance on the type of test to conduct
- Not asking for a detailed debrief or report walkthrough
- Not asking for a report with detailed steps and reproducible results
- Using vendors and tools that provide reports with hundreds or thousands of vulnerabilities that are mostly not critical
- Employing an inexperienced pen tester who creates reports using automated tools

### Writing the Final Report

The final penetration testing report is the tangible output of the entire testing process. Without an appropriate report, it is extremely difficult to explain the entire process followed and the criticality of the findings. The final report should be easy to understand for the client's management and information security personnel. The report must meet the requirements of both the management as well as technical personnel. A report that is too technical is of no use to the upper management; however, an overly simplistic report is not recommended, as the

information security personnel may be unable to appropriately implement the recommended changes.

An ideal final report should include the following.

- **Final report delivery date:** The delivery date should be included in the report so that the client organization can have that information for its records.
- **Cover letter:** The cover letter should include the tester's name, the name of the organization the tester works for, and the tester's email address. It should be addressed to the client organization's contact person. An ideal cover letter also includes details about the tester and acknowledges those who helped in the successful completion of the pen test.
- **Executive summary:** The report should include a summary that allows authorized client personnel to make a decision after reading it and the following topics.
  - **Organization synopsis:** This section includes a brief description of the organization and its network.
  - **Purpose for the evaluation:** This section defines the reason for undertaking penetration testing.
  - **System description:** This section includes a brief description of the systems used across the client organization.
  - **Scope of the project:** This section includes the total number of IP addresses, apps, devices, hosts, and other network resources that the organization had mentioned in the contract.
  - **Summary of evaluation:** This section should contain a summary of the tests performed by the pen testers and the results obtained.
  - **Assumptions/Timeline:** This section should specify all the assumptions made during the testing process and include all the commencement and completion dates for each test.
  - **Major findings and recommendations:** This section should include a summary of the major findings and any issues that could lead to future cyberattacks. The testers should also mention any recommended actions to mitigate the vulnerabilities.
  - **Testing methodology:** This section specifies the standard frameworks and techniques followed to perform penetration testing.
  - **Planning:** This section includes the details of the planned penetration testing process and how the actual process was performed.
  - **Exploitation:** This section includes all the detailed exploitation processes followed during the penetration test.
  - **Conclusions:** This is the concluding section of the report. These conclusions include any further suggestions from the testing team.

## Phases of Report Development

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Phases of Report Development

### Report Development Process



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Phases of Report Development

A typical report development process contains the following phases:

- Plan the report
- Collect and document the information
- Write a draft report
- Review and finalize the report

| Plan the Report                                                                   |                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |                                                                                                                                                                                                                    |
| 1. Report Objectives                                                              | Clearly outline the <b>primary goal</b> of writing the report and the main purpose of the security audit.                                                                                                          |
| 2. Target Audience                                                                | Clearly know the <b>target audience</b> for whom the report is being written.                                                                                                                                      |
| 3. Time frame                                                                     | Consider the reporting time frame during the pen test project planning and adhere to the same.                                                                                                                     |
| 4. Confidentiality                                                                | Determine the confidentiality level of the various pen testing reports and identify the controls to maintain the <b>confidentiality</b> of reports, as the reports contain a <b>lot of sensitive information</b> . |
| 5. Format                                                                         | Determine the format of the <b>final report</b> according to the Rules of Engagement (RoE) with the client.                                                                                                        |
| 6. Distribution                                                                   | Consider how the reports will be distributed to the <b>concerned stakeholders</b> .                                                                                                                                |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Plan the Report

It is recommended that the testers plan the report after evaluating the time frame, audience, criticality of the results reported, and format of the report. This will help in avoiding last-minute dilemmas and confusion while creating the report and facilitate the creation of a checklist for report inclusions. The following should be considered while planning the report.

- **Report objectives:** The main objective of creating a report and the primary purpose of the security audit should be defined. The defined objective should act as a guideline that drives the framing and completion of an effective report.
- **Target audience:** The audience of a report can include both technical personnel such as network and security administrators who implement the recommendations and nontechnical personnel such as the stakeholders and CEO who are the primary decision makers. Therefore, identifying the target audience of the test report will help choose a format that both types of audiences can understand without much difficulty. For example, the senior management will review and analyze an executive summary, while the IT development team will focus on the technical details of the report.
- **Time frame:** The time required to create and submit the reports should be evaluated. The report submission is a part of the testing process, and the client will not allot a separate time frame for this. Therefore, it is advised to perform the test and develop the report within the allotted time frame.
- **Confidentiality:** The confidentiality level of the various pen testing reports should be determined, and controls should be identified to maintain the confidentiality of reports, as the reports contain a lot of sensitive information. Reports can contain sensitive information about the client such as vulnerabilities in the networks and systems,

security implemented, and types of storage used. The reports should be secured from unauthorized access, and security controls should be implemented.

- **Format:** The final report should be prepared in a format requested by the client or as per the requirements of the Rules of Engagement (ROE). The client may want the report in a hardcopy or softcopy format. The report should be prepared after identifying the requirement correctly.
- **Distribution:** It is important to consider how the reports will be distributed to the concerned stakeholders. The report should be submitted within the given time frame, and copies should be distributed to the authorized personnel recommended by the client. A systematic approach should be maintained while distributing hard copies of the final report.

## Collect and Document the Information



- It is important to **gather information at every stage of the testing** pertaining to the nature and scope of the security assessment such as documenting every process **with a detailed description** about the methods and tools utilized, key areas where exploits are carried out, outcomes of the scanning, vulnerability evaluation, countermeasures, and recommendations.



### Key guidelines to collect information:

**1** Compile and sort all the information collected during each step of pen testing.

**3** Note the information on activity logs and network traffic.

**2** Prepare notes after each step.

**4** Maintain a list of scanned reports and screenshots for clarity and reference.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Collect and Document the Information

After performing tests at each phase, information should be collected about the complete testing process, and the results should be collected and documented. Every process should be documented with a detailed description of methods and tools utilized, vulnerabilities present, cyberattack surface areas, scanning outcomes, vulnerability evaluation, countermeasures, and recommendations.

It is also recommended to take screenshots of the results, save versions of the tools used for tests, and take videos capturing the process and results if possible. This will help retain critical information safely and create the reports that need to be submitted to the target organization. Such evidence will also act as a proof of the tests and provide a basis for the recommendations.

Key guidelines while collecting the information include the following:

- Compile the information from all the phases of the testing process such as intelligence gathering and footprinting, scanning, and exploitation and sort all the information collected at these phases.
- For each step of the test, prepare notes about the significance and result of the test along with details such as tools and their versions used, vulnerabilities found, and recommendations.
- Document all the activities and gather the network traffic logs as proof.
- Capture the screenshots for different tasks such as the outcome of the tool, scanning results, and traffic sniffed and document them for further reference where possible.
- List the devices, servers, databases, as well as other hardware and software components tested in the test report as evidence. Maintain this list of scanned reports and screenshots for clarity and reference.

## Write a Draft Report



- Gather all the information collected during the pen test and prepare a **rough draft**, including details from the report planning phase to the documentation phase.



- Arrange the information according to a **predetermined report format**.



- Ensure that all the information is gathered and documented appropriately in order to **avoid missing any important information**.



- Create a final draft report keeping the **target audience** in mind and following **standard methodologies**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Write a Draft Report

A draft report refers to the rough copy of a report before finalizing the process flow. This report should utilize the information and documents collected during the test. A rough draft should be prepared, including details from the report planning phase to the documentation phase. The information should be arranged according to the report format that was predetermined during the planning of the report. Information such as the results of various scanning techniques, findings from different tests performed, the output from tools, vulnerabilities identified, and recommendations should be included.

It must be ensured that all the information has been gathered and documented appropriately, and the draft should be checked for missing any important information. A final draft report should be created keeping the target audience in mind and following standard methodologies. The audience of the report may include both technical and nontechnical readers.

## Review and Finalize the Report



- 1 It is highly recommended that the rough draft be first reviewed by peers for a **second opinion**.
- 2 If a team has collectively participated in the documentation process, the **whole team** should **review** and **edit** the report.
- 3 After the documents are reviewed and edited by teams and peers, it is essential to appropriately document and **finalize the changes**.
- 4 Prepare the final report with all the changes in a **specific format** that is widely accepted.
- 5 The final report should be presented in a **professional manner** matching the organization's standards.
- 6 The report should clearly mention the **importance of penetration testing** to the client along with the associated **vulnerabilities** and **risks** to the organization.
- 7 Recommendations should be made depending on the **assessment** and **research** conducted by the team that justify the organization's security needs.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Review and Finalize the Report

In this phase, the report is reviewed for errors, and the necessary corrections are made. It is highly recommended that the rough draft be first reviewed by peers for a second opinion. If a team has collectively participated in the documentation process, the whole team is advised to review and edit the report. After completion of the review, feedback should be collected from the reviewers, and the necessary suggestions should be incorporated in the document before finalizing the report.

The final report should be created carefully without mistakes and in a presentable manner. It should contain all the changes in a widely accepted format. The final report should be presented in a professional manner matching the organization's standards.

The report should clearly mention the importance of penetration testing to the client along with the associated vulnerabilities and risks to the organization. Recommendations should be made based on the assessment and research conducted by the team that justify the organization's security needs.



# Sample Pen Testing Report Format

## 1.0 Report Details

- Document Details
- Version History Information
- Recipient
- Penetration Testing Team Members
- Contact Information

## 2.0 Executive Summary

- Project Objectives
- Project Scope
- Target Systems
- Assumptions and Timeline
- Summary of Evaluations, Findings, and Recommendations
- Testing Methodology
- Planning
- Exploitation
- Reporting

## 3.0 General Opinion

- Personnel
- Policies and Procedures
- Critical Vulnerabilities
- Identification and Authentication
- Intrusion Detection
- Conclusion

## 4.0 Comprehensive Technical Report

- Web Application Assessment
- Security Management
- Security Architecture
- Access Control Methodologies
- Physical and Operational Security
- Telecommunications and Network Security
- Applications and Systems Security
- List of Tests Performed
- Network-Based Tests
- List of IP Addresses Tested
- Specific ISS Tests Conducted during Point Scans
- Specific NetRecon Tests Conducted during Point Scans
- Specific ESM Policy Tests Conducted
- Remote Access Phone Dialing Tests
- Physical Security Tests
- Social Engineering Tests

## 5.0 Result Analysis

## 6.0 Recommendations

## 7.0 Supplemental CD Readme File

## 8.0 Appendix

## 9.0 List of Illustrations

## 10.0 List of Tables

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Sample Pen Testing Report Format

A sample penetration testing report format is shown in the below figure.

- 1.0 Report Details
  - Document Details
  - Version History Information
  - Recipient
  - Penetration Testing Team Members
  - Contact Information
- 2.0 Executive Summary
  - Project Objectives
  - Project Scope
  - Target Systems
  - Assumptions and Timeline
  - Summary of Evaluations, Findings, and Recommendations
  - Testing Methodology
  - Planning
  - Exploitation
  - Reporting
- 3.0 General Opinion
  - Personnel
  - Policies and Procedures
  - Critical Vulnerabilities
  - Identification and Authentication
  - Intrusion Detection
  - Conclusion
- 4.0 Comprehensive Technical Report
  - Web Application Assessment
  - Security Management
  - Security Architecture
  - Access Control Methodologies
  - Physical and Operational Security
  - Telecommunications and Network Security
  - Applications and Systems Security
  - List of Tests Performed
  - Network-Based Tests
  - List of IP Addresses Tested
  - Specific ISS Tests Conducted during Point Scans
  - Specific NetRecon Tests Conducted during Point Scans
  - Specific ESM Policy Tests Conducted
  - Remote Access Phone Dialing Tests
  - Physical Security Tests
  - Social Engineering Tests
- 5.0 Result Analysis
- 6.0 Recommendations
- 7.0 Supplemental CD Readme File
- 8.0 Appendix
- 9.0 List of Illustrations
- 10.0 List of Tables

Figure 14.1: Sample pen test report



## Report Components

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Report Components



1 Cover Letter

6 Executive Summary

2 Document Properties / Version History

7 Comprehensive Technical Report

3 Table of Contents and List of illustrations /  
Final Report-Delivery Date

8 Result Analysis

4 Assessment Information / Contact  
Information

9 Recommendations

5 Distribution List / Confidentiality Statement

10 Appendices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Report Components

This section discusses the following various components of a penetration testing:

- Cover letter
- Document properties/version history
- Table of contents and list of illustrations/final report-delivery date

- Assessment information/contact information
- Distribution list/confidentiality statement
- Executive summary
- Comprehensive technical report
- Result analysis
- Recommendations
- Appendices

## Cover Letter

**Cover Letter** - It contains the report title, details about the author and client organization, date of submission, and a disclaimer.

**The organization synopsis includes the following:**

- 1 A brief description of the **nature, scope, and structure** of the organization's information security system
- 2 The **purpose and need** for undertaking the **vulnerability assessment**
- 3 Views on the **current level of security risks** and threats
- 4 Details about **people involved in the project**, namely, whether a single tester or a team of testers has worked on the project
- 5 The **knowledge and skill set of the pen tester**, with details of prior studies and research conducted in this field

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Cover Letter

A cover letter provides a brief description of the final report submitted. It contains the report title, details of the author and the client organization, date of submission, and a disclaimer. The cover letter should refer to the client organization stakeholder to whom the report is being submitted and should include the details of the authors and the organization for which the work was undertaken and their positions and skills.

It is recommended that the cover letter includes a summary of the target organization comprising the following:

- A brief description of the nature, scope, and structure of the organization's information security system
- The purpose and need for performing the vulnerability assessment
- Views on the current level of security risks and threats
- Details about the people involved in the project, namely, whether a single tester or a team of testers has worked on the project
- The knowledge and skill set of the tester, with details of prior studies and research conducted in this field

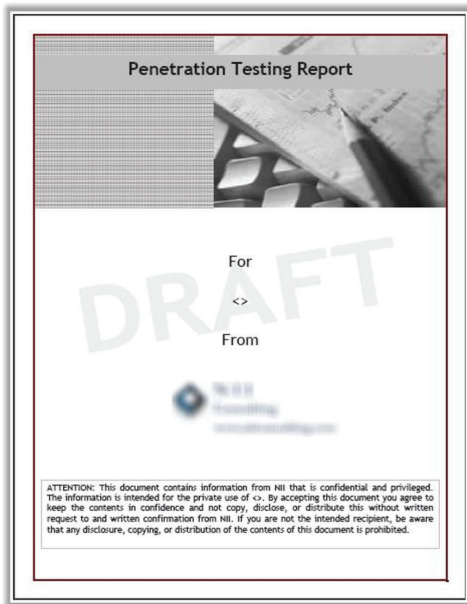


Figure 14.2: Sample cover letter and disclaimer

## Document Properties/Version History



### Document Properties

- Contain valuable information about the report, including **title**, **author**, **version**, **date** and **time**, and **classification** of the document
- Also lists the names of people involved in the **documentation process**, including those of the final draft approver, and in some cases, the names of the people to whom the report will be submitted

A table showing document properties in a report

| Document Properties         |                            |
|-----------------------------|----------------------------|
| Title                       | Penetration Testing Report |
| Classification              | Confidential               |
| Version                     | V 2.3.3                    |
| Date                        | April 24, 2020             |
| Name of Pen Tester/Team     | EC-Council LPT Team        |
| Name of Supervising Officer | *****                      |

### Version History

- A record of all the **version control tracked changes** made on the report, including the names of the people who made revisions, date and time when they made the changes, and a **description of the changes** they made



A table illustrating the version control system in a report

| Date           | Version | Author | Comments                                |
|----------------|---------|--------|-----------------------------------------|
| April 24, 2020 | V 2.3.3 | *****  | Final draft                             |
| April 22, 2020 | V.2.3.2 | *****  | Checked for formatting and proofreading |
| April 20, 2020 | v.2.3.1 | *****  | Edited and made changes to content      |

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Document Properties/Version History

### ■ Document Properties

Document properties refer to the description of the document being submitted to the target organization. The properties include valuable information about the report such as title, author, version, date and time, and classification of the document. The names of the people involved in the documentation process, including those of the final draft approver, and in some cases, the names of the people to whom the report will be submitted, are also listed.

| Document Properties         |                            |
|-----------------------------|----------------------------|
| Title                       | Penetration Testing Report |
| Classification              | Confidential               |
| Version                     | V 2.3.3                    |
| Date                        | April 24, 2020             |
| Name of Pen Tester/Team     | EC-Council LPT Team        |
| Name of Supervising Officer | *****                      |

Table 14.1: A table showing document properties in a report

### ▪ Version History

Version history refers to a record of all the version control tracked changes made on the report, including the names of the people who made the revisions, date and time when they made the changes, and a description of the changes made.

| Date           | Version | Author | Comments                                |
|----------------|---------|--------|-----------------------------------------|
| April 24, 2020 | V 2.3.3 | *****  | Final draft                             |
| April 22, 2020 | V.2.3.2 | *****  | Checked for formatting and proofreading |
| April 20, 2020 | v.2.3.1 | *****  | Edited and made changes to the content  |

Table 14.2: A table illustrating a version control system in a report



## Table of Contents/Final Report



### Table of Contents and List of Illustrations

- This is a list of all the **important points** covered in the report with **page numbers**.
- It also includes a list of illustrations and figures in a **diagrammatic** and **sequential** form such as network application architecture, network diagram, and captured screenshots list.

### Final Report - Delivery Date

- This includes all the **key information** on the report timeline — from the project inception date to the project delivery date along with important dates when the report was reviewed, edited, finalized, etc.
- Testing should be **planned**, **prepared**, and **performed** keeping the delivery date of the report in mind.

### Table of Contents

|                                                 |    |
|-------------------------------------------------|----|
| 1. The Cover Letter                             | 11 |
| 1.1 Document Properties                         | 11 |
| 1.2 Introduction                                | 12 |
| 1.3 Table of Contents and List of Illustrations | 12 |
| 1.4 Assessment Information                      | 13 |
| 1.5 Declaration List                            | 13 |
| 1.6 Confidentiality Statement                   | 14 |
| 1.7 Final Report Delivery Date                  | 14 |
| 2. The Executive Summary                        | 15 |
| 2.1 Scope of the Project                        | 15 |
| 2.2 Purpose for the Evaluation                  | 15 |
| 2.3 System Description                          | 16 |
| 2.4 Assumptions                                 | 16 |
| 2.5 Findings                                    | 17 |
| 2.6 Summary of Evaluation                       | 18 |
| 2.7 Summary of Findings                         | 18 |
| 2.8 Summary of Recommendations                  | 18 |
| 2.9 Testing Methodology                         | 19 |
| 2.10 Planning                                   | 19 |
| 2.11 Implementation                             | 19 |
| 2.12 Reporting                                  | 19 |
| 2.13 Conclusion                                 | 20 |
| 2.14 Appendix                                   | 20 |
| 2.15 Glossary                                   | 20 |
| 2.16 Bibliography                               | 20 |
| 2.17 Index                                      | 20 |
| 2.18 Appendix                                   | 20 |
| 2.19 Appendix                                   | 20 |
| 2.20 Appendix                                   | 20 |
| 2.21 Appendix                                   | 20 |
| 2.22 Appendix                                   | 20 |
| 2.23 Appendix                                   | 20 |
| 2.24 Appendix                                   | 20 |
| 2.25 Appendix                                   | 20 |
| 2.26 Appendix                                   | 20 |
| 2.27 Appendix                                   | 20 |
| 2.28 Appendix                                   | 20 |
| 2.29 Appendix                                   | 20 |
| 2.30 Appendix                                   | 20 |
| 2.31 Appendix                                   | 20 |
| 2.32 Appendix                                   | 20 |
| 2.33 Appendix                                   | 20 |
| 2.34 Appendix                                   | 20 |
| 2.35 Appendix                                   | 20 |
| 2.36 Appendix                                   | 20 |
| 2.37 Appendix                                   | 20 |
| 2.38 Appendix                                   | 20 |
| 2.39 Appendix                                   | 20 |
| 2.40 Appendix                                   | 20 |
| 2.41 Appendix                                   | 20 |
| 2.42 Appendix                                   | 20 |
| 2.43 Appendix                                   | 20 |
| 2.44 Appendix                                   | 20 |
| 2.45 Appendix                                   | 20 |
| 2.46 Appendix                                   | 20 |
| 2.47 Appendix                                   | 20 |
| 2.48 Appendix                                   | 20 |
| 2.49 Appendix                                   | 20 |
| 2.50 Appendix                                   | 20 |
| 2.51 Appendix                                   | 20 |
| 2.52 Appendix                                   | 20 |
| 2.53 Appendix                                   | 20 |
| 2.54 Appendix                                   | 20 |
| 2.55 Appendix                                   | 20 |
| 2.56 Appendix                                   | 20 |
| 2.57 Appendix                                   | 20 |
| 2.58 Appendix                                   | 20 |
| 2.59 Appendix                                   | 20 |
| 2.60 Appendix                                   | 20 |
| 2.61 Appendix                                   | 20 |
| 2.62 Appendix                                   | 20 |
| 2.63 Appendix                                   | 20 |
| 2.64 Appendix                                   | 20 |
| 2.65 Appendix                                   | 20 |
| 2.66 Appendix                                   | 20 |
| 2.67 Appendix                                   | 20 |
| 2.68 Appendix                                   | 20 |
| 2.69 Appendix                                   | 20 |
| 2.70 Appendix                                   | 20 |
| 2.71 Appendix                                   | 20 |
| 2.72 Appendix                                   | 20 |
| 2.73 Appendix                                   | 20 |
| 2.74 Appendix                                   | 20 |
| 2.75 Appendix                                   | 20 |
| 2.76 Appendix                                   | 20 |
| 2.77 Appendix                                   | 20 |
| 2.78 Appendix                                   | 20 |
| 2.79 Appendix                                   | 20 |
| 2.80 Appendix                                   | 20 |
| 2.81 Appendix                                   | 20 |
| 2.82 Appendix                                   | 20 |
| 2.83 Appendix                                   | 20 |
| 2.84 Appendix                                   | 20 |
| 2.85 Appendix                                   | 20 |
| 2.86 Appendix                                   | 20 |
| 2.87 Appendix                                   | 20 |
| 2.88 Appendix                                   | 20 |
| 2.89 Appendix                                   | 20 |
| 2.90 Appendix                                   | 20 |
| 2.91 Appendix                                   | 20 |
| 2.92 Appendix                                   | 20 |
| 2.93 Appendix                                   | 20 |
| 2.94 Appendix                                   | 20 |
| 2.95 Appendix                                   | 20 |
| 2.96 Appendix                                   | 20 |
| 2.97 Appendix                                   | 20 |
| 2.98 Appendix                                   | 20 |
| 2.99 Appendix                                   | 20 |
| 2.100 Appendix                                  | 20 |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Table of Contents/Final Report

### Table of Contents and List of Illustrations

A test report should contain a table of contents, which the readers can use for easily navigating the contents. All the important topics and subtopics of the report should be listed with their page numbers. A list of illustrations, diagrams, charts, and tables should also be included. The table of contents will help the clients learn about the flow of the testing process and also improve the presentation of the report.

A sample format for the table of contents is shown in below figure.

| <b>Table of Contents</b>                        |    |
|-------------------------------------------------|----|
| 1 Cover Letter                                  | 01 |
| 1.1 Document Properties                         | 03 |
| 1.2 Version History                             | 04 |
| 1.3 Table of Contents and List of Illustrations | 06 |
| 1.4 Assessment Information                      | 11 |
| 1.5 Distribution List                           | 12 |
| 1.6 Confidentiality Statement                   | 14 |
| 1.7 Final Report Delivery Date                  | 16 |
| 2 Executive Summary                             | 18 |
| 2.1 Scope of the Project                        | 19 |
| 2.2 Purpose for the Evaluation                  | 21 |
| 2.3 System Description                          | 23 |
| 2.4 Assumption                                  | 26 |
| 2.5 Timeline                                    | 27 |
| 2.6 Summary of Evaluation                       | 28 |
| 2.7 Summary of Findings                         | 32 |
| 2.8 Summary of Recommendations                  | 36 |
| 2.9 Testing Methodology                         | 39 |
| 2.10 Planning                                   | 44 |
| 2.11 Exploitation                               | 45 |
| 2.12 Reporting                                  | 47 |
| 3 Comprehensive Technical Report                | 50 |
| 3.1 Detailed SYSTEMS Information                | 52 |
| 3.2 Windows Server                              | 60 |
| 4 Result Analysis                               | 66 |
| 5 Recommendations                               | 68 |
| 6 Appendices                                    | 75 |
| 6.1 Required Work Efforts                       | 76 |
| 6.2 Research                                    | 80 |
| 6.3 References                                  | 84 |
| 6.4 Glossary                                    | 90 |

Figure 14.3: A sample Table of Contents

#### ▪ **Final Report-Delivery Date**

The final report should include details of the report timeline, which specifies details of the test ranging from the project inception date to the project delivery date along with important dates on which the report was reviewed, edited, and finalized. Planning, preparing, and performing the testing based on the delivery date of the report is advised.

## Assessment Information/Contact Information



- This section covers **details of all the members of the penetration testing team**, including account executive, assessment team members, project manager, etc.



- Include the name of each member and their **role/designation** along with their contact information such as email address and phone number.



- It is recommended to include **client details** such as company name, address, and contact information.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Assessment Information/Contact Information

The test report should contain assessment information that covers details of all the members of the penetration testing team, including account executive, assessment team members, project manager, etc. The name of each member and their role/designation along with their contact information such as email address and phone number should be included.

This section should also contain client details such as company name, address, and contact information.

## Distribution List/Confidentiality Statement

### Distribution List

- Contains details about all the **report audiences**
- Include **each individual's** name, designation, contact details (email address/phone number), date of distribution, and mode of distribution.

### Confidentiality Statement

- Describes the **importance of maintaining** the confidentiality of the information contained in the report
- It also includes **actions to be taken** in case of redistribution, duplication, or misuse of such proprietary and confidential information.

| Individual Name | Designation | Contact Information | Date of Distribution |
|-----------------|-------------|---------------------|----------------------|
| *****           | *****       | *****               | April 28, 2020       |
| *****           | *****       | *****               | April 27, 2020       |
| *****           | *****       | *****               | April 24, 2020       |

A table illustrating distribution list in a report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Distribution List/Confidentiality Statement

### ■ Distribution List

Including a distribution list in the final report is recommended. This list contains details about all the target audiences of the report. Each individual's name, designation, contact details (email address/phone number), date of distribution, and mode of distribution should be included.

| Individual Name | Designation | Contact Information | Date of Distribution |
|-----------------|-------------|---------------------|----------------------|
| *****           | *****       | *****               | April 28, 2020       |
| *****           | *****       | *****               | April 27, 2020       |
| *****           | *****       | *****               | April 24, 2020       |

Table 14.3: A table illustrating the distribution list for a report

### ■ Confidentiality Statement

Including a confidentiality statement in the final pen test report is highly recommended. This statement describes the importance of maintaining the confidentiality of the information contained in the report. It also includes actions to be taken in case of redistribution, duplication, or misuse of such proprietary and confidential information. To distribute or share this document, the client and the penetration testing team need to negotiate a nondisclosure agreement to meet compliance requirements.

## Executive Summary



- 1 The executive summary provides a **high-level view** of the test goals and results in the form of both risks and business impact in a simple and understandable way.
- 2 It is intended for **non-technical readers** such as high-level executives, business leaders, and management.
- 3 They can review this summary and gain insight into the **current security posture** and the concerns highlighted in the document.
- 4 It allows them to **make informed decisions** for improving the security of their company.
- 5 Including **visual communication** while generating an executive summary is highly recommended to simplify complex information.
- 6 Use **graph or chart-based representations** to communicate a summary of the findings and their criticality.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Executive Summary (Cont'd)



### Elements included in the executive summary

- Scope of the project
- Evaluation purpose
- System description
- Assumptions
- Timeline
- Summary of evaluations
- Summary of findings
- Summary of recommendations
- Testing methodology
- Planning
- Exploitation
- Reporting

### Information covered in the executive summary

- Information about the targeted systems and apps such as IP addresses, operating systems, application names, servers, and other target devices targeted
- Details about processes conducted, software tools used, and hardware utilized
- Penetration test results
- Details about all the exploits performed
- Details of the discovered vulnerabilities
- Detailed summary of execution

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Executive Summary

The executive summary provides a high-level view of the test goals and results in the form of both risks and business impact in a simple and understandable way. This summary must be concise and clear. The summary is intended for nontechnical readers such as high-level executives, business leaders, and management (CEO, chairman, and stakeholders). They can review this summary and gain insight into the current security posture and the concerns

highlighted in the document. This summary further allows them to make informed decisions for improving the security posture of their company.

Including visual communication while generating an executive summary is highly recommended to simplify complex information. Graphs or chart-based representations can be used to communicate a summary of the findings and their criticality.

This summary should include very less technical information. It is mandatory to explain to the readers the losses that the organization may face due to the current situation. The target organization stakeholders are responsible for the approval of changes and sanction of finances required to implement the identified changes.

It is recommended that the following elements be included in the executive summary section of the report:

- Scope of the project
- Evaluation purpose
- System description
- Assumptions
- Timeline
- Summary of evaluations
- Summary of findings
- Summary of recommendations
- Testing methodology
- Planning
- Exploitation
- Reporting

The above-specified details must cover the following information:

- Information about the targeted systems and apps such as IP addresses, operating systems, application names, servers, and other target devices
- Details about processes conducted, software tools used, and hardware utilized to perform the test
- Penetration test results
- Details about all the exploits performed and the details of changes made to the environment or any systems during exploitation/testing
- Details of the discovered vulnerabilities
- A detailed summary of execution for an easy understanding of all the testing activities performed.

## Scope of the Project



- The test report should include the scope of the project, which refers to the **total number of IP addresses**, apps, devices, hosts, and other network resources that the organization had **listed in the contract**.



**The scope of the project should also include the following:**

- 1 Examining whether **social engineering** has been employed or not
- 2 Examining whether **public** or **private networks** have been tested or not
- 3 Examining whether **Trojans** and **backdoor** software applications are permitted or not

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Scope of the Project

The test report should include the scope of the project, which refers to the total number of IP addresses, apps, devices, hosts, and other network resources that the organization had listed in the contract, and which had accordingly been tested by the penetration testers. This section should also offer detailed information about the type of tests performed on a device, app, or an employee. This section covers all inclusions and exclusions, i.e. details of the tests performed and those that were not performed along with the reasons and their technical details.

The scope of the project should mention whether the pen tests included the following:

- Analysis of IP address and ports
- Use of social engineering techniques and other attacks targeted towards employees
- Testing of private and public networks
- Use of Trojans, backdoor, and other malware to identify vulnerabilities

## Evaluation Purpose/System Description



### Evaluation Purpose

- This section explains the main **purpose of the test**.
- It lists all **loopholes** and **security flaws** found in the network and the tools used to test the vulnerabilities.
- It explains how the testing was conducted, whether the testing was **successful** or **unsuccessful**, and the reasons behind the successful and failed attempts.
- This section also includes information **about the extent of testing across the organization**.

### System Description

- This section includes a list of all the devices that were used for pen testing **hardware and software devices**, such as the IP address of the system.
- It includes information about the **domain model, Internet service provider, web server, network ports and protocols, system configurations**, etc.
- It also explains the **network architecture, network flow, and information status of the organization** before and after the testing.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Evaluation Purpose/System Description

### ■ Evaluation purpose

The penetration test report must include the main purpose for which the organization had taken up the testing. It should include the number of successful and failed testing attempts along with the reasons for each. This section should include all the loopholes and security flaws found in the network and the tools used to test the vulnerabilities. It should also include information about the extent of testing performed across the organization.

### ■ System description

This section contains a list of all the resources of the organization that were targeted under testing including hardware and software devices such as the hosts, servers, web applications, and IP addresses. It includes information about the domain model, Internet service provider, web server, network ports and protocols, system configurations, etc. Explaining the network architecture, network flow, and information status of the organization before and after the testing is recommended.



## Assumptions/Timeline



### Assumptions

- This section explains the **assumptions made** by the pen tester when facing a roadblock in a **critical situation**.
- These assumptions also **help the reader understand the vulnerabilities** in critical areas, why the pen tester opted for certain testing techniques, and the rationale for them.
- For example**, testing the firewall and other devices to check that alarms and warnings that alert administrators are functioning correctly



### Timeline

- This section includes a record of the duration and **time frames** maintained by the pen tester for every conducted test.
- It contains all the **commencement and completion dates**, along with other important dates in the report.

| Categories   | Initiation Date/Time | Completion Date/Time |
|--------------|----------------------|----------------------|
| Windows      | Mm/dd/yr             | Mm/dd/yr             |
| Linux        | Mm/dd/yr             | Mm/dd/yr             |
| Footprinting | Mm/dd/yr             | Mm/dd/yr             |

A table representing a timeline in a penetration report

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Assumptions/Timeline

### Assumptions

During testing, critical situations would have arisen when the testing process hit a roadblock, such as when the testers could not breach into the systems or bypass the firewall. During these situations, the testers would have made certain assumptions to get past the roadblock. Such assumptions should be included in this section of the report. These assumptions help the readers understand the flow of the testing and the reason for making a testing-related decision. It will help make decisions according to the results provided by the testing team.

Additionally, these assumptions help the reader understand the vulnerabilities in critical areas, why the pen tester opted for certain testing techniques, and the rationale for them such as testing the firewall and other devices to check that alarms and warnings that alert administrators are functioning correctly.



Figure 14.4: The tester performing the pen test and checking firewall

### Timeline

This section of the test report contains a record of the duration and time frames maintained by the tester for every conducted test. It contains all the commencement

and completion dates of each test as well as that of the complete penetration test. It will provide a fair idea about other important dates in the report as well.

| Categories   | Initiation Date/Time | Completion Date/Time |
|--------------|----------------------|----------------------|
| Windows      | Mm/dd/yr             | Mm/dd/yr             |
| Linux        | Mm/dd/yr             | Mm/dd/yr             |
| Footprinting | Mm/dd/yr             | Mm/dd/yr             |

Table 14.4: A table representing a timeline in a report

## Summary of Evaluation



- This is a detailed report on how the **evaluation process** was conducted, which specifically describes each step of the process.
- It also contains the **important findings** and **outcomes** found during the evaluation.



### Host Table

- Include a host table that contains a list of all the hosts and targets that were assessed
- Include a **severity rating** for each discovered target
  - Ideally sorted by priority for remediation



- Specify the **role of the target** within the organization when identified
  - Domain controller
  - Databases
  - Others



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Summary of Evaluation

The summary of evaluation refers to the detailed reports of the evaluations performed along with a description of all the processes. This section also describes the results obtained from each process. It also contains the important findings and outcomes found during the evaluation.

### Host table

The summary of evaluation must also include a host table that contains a list of all the hosts and targets that were assessed. A severity rating for each discovered target should be included, and the host table entries should be sorted based on the priority for remediation. Additionally, when the target is identified, its role within the organization should be specified, e.g., domain controller or databases.

## Summary of Findings



- This is a summary report about the findings, listing the discovered **risks** and **threats** in a specific manner.
- It also sorts all the findings depending on their **priority level**.
- Summarize all your findings in a manner that is understandable to a non-technical audience.
- Colors must be used for findings that highlight the vulnerabilities and risks posed to the applications and systems.
- Include graphs/charts for showing the overall security posture of the organization based on the risk analysis, identified vulnerabilities by severity/host type/device type, etc.

Summary of Findings Table

| Finding Number | Finding Name               | Risk Level | Severity Rating | Risk Description |
|----------------|----------------------------|------------|-----------------|------------------|
| 1              | Insufficient Authorization | Critical   | 9.2             | XXXXXXXX         |
| 2              | SQL Injection              | High       | 8.5             | XXXXXXXX         |
| 3              | LDAP Injection             | Medium     | 6.0             | XXXXXXXX         |

Graphical Summary of Findings



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Summary of Findings

Decision makers such as high-level executives and management do not spend much time going into the details of each finding. Hence, this section must summarize all the pen testing findings in a manner that is understandable to a nontechnical audience.

The summary of findings contains information about the discoveries the testers made during the test, including the risks and threats of all the target devices. It is recommended that the findings be presented after sorting them according to a specified method or by sorting them according to priority. The findings should be supported by including relevant evidence such as text and screenshots. The following details should be covered in the findings table: finding number, severity, brief description of the finding, impacted asset, page numbers to the detailed findings data.

Using a colored table for findings that highlight the vulnerabilities and risks posed to the applications and systems is mandatory (see table below). Graphical/chart representations should be used for summarizing findings. For example, graphs should be included for showing the overall security posture of the organization based on the risk analysis, identified vulnerabilities by severity/host type/device type, etc. Additionally, a table that lists the most significant findings in the report should be included. The findings should be grouped by severity or category (e.g., group by a software issue, network device configuration, password policy, operating system, etc.).

| Finding Number | Finding Name               | Risk Level | Severity Rating | Risk Description |
|----------------|----------------------------|------------|-----------------|------------------|
| 1              | Insufficient Authorization | Critical   | 9.2             | XXXXXX           |
| 2              | SQL Injection              | High       | 8.5             | XXXXXX           |
| 3              | LDAP Injection             | Medium     | 6.0             | XXXXXX           |

Table 14.5: Sample summary of findings table

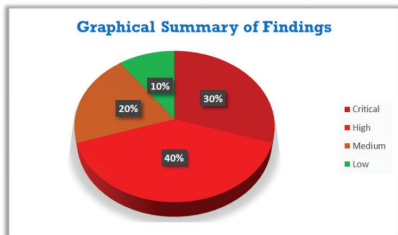


Figure 14.5: Graphical representation of summary of findings

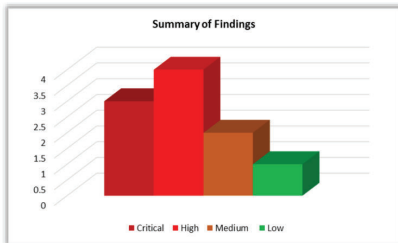


Figure 14.6: Chart representation of summary of findings

## Summary of Strengths and Weaknesses



- Summary of strengths helps the client understand the strengths of their current security environment and **reinforce the security best practices** to build a robust defensive security posture.



- Categorize all the **identified vulnerabilities** as a summary of weaknesses.



- Knowing weaknesses helps the client take **appropriate remediation steps** to secure the enterprise environment.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Summary of Strengths and Weaknesses

Including a summary of the strengths and weaknesses found during the penetration testing process is recommended. The client organization must be aware of both positive findings and weaknesses. This helps them understand the strengths of their current security environment and reinforce the security best practices to build a robust defensive security posture.

For example, in the summary of strengths, findings such as the following can be included:

- Strong inbound firewalls rules for the internal web server, restricted access to only trusted hosts.
- Efficient group management that clearly restricts which users are administrators and which users are allowed to remote login.
- Though your password policy is not strong, users are using strong passwords.

All the identified vulnerabilities must be categorized in the summary of weaknesses. Knowing these weaknesses helps the client organization follow appropriate remediation steps to secure the enterprise environment.

For example, in the summary of weaknesses, findings such as the following can be included:

- Lack of SMB signing allows attackers to impersonate users and execute malicious code on remote machines.
- Misconfiguration of LLMNR and NB-NS protocols allows attackers to gather information passively and perform hash-replay attacks.
- NTLM authentication is enabled.

## Summary of Recommendations



- This is a summary of the recommendations and suggestions made by the team after thoroughly **analyzing the findings** of the organization's information system.



- Recommendations are made after thorough **research** and **investigation**.



- All **security weaknesses** are not necessarily technical and cannot be remediated by security personnel.



- The summary of recommendations offers **strategic steps** that enhance the operational policy of the client to strengthen their overall security posture.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Summary of Recommendations

This section should include all the recommendations for the client about the risks and threats found during the penetration test. These suggested recommendations help the organization remediate the discovered vulnerabilities. The testers are advised to mention appropriate recommendations based on thorough research, investigation, and consideration of the goals of the organization.

All security weaknesses are not necessarily technical and cannot be remediated by security personnel. Clients need to focus on the root causes of such findings and resolve them at their core. The recommendations discussed in this section are strategic steps that enhance the operational policy of the client organization to strengthen their overall security posture.

## Testing Methodology



- Penetration testing is primarily conducted following a **standard framework**. The pen tester may follow a single methodology or can combine various models to provide the output and recommendations that **best suit the client's requirements**.
- A pen tester must follow standards and techniques such as the Information Systems Security Assessment Framework (ISSAF), **Open Web Application Security Project (OWASP)**, Open Source Security Testing Methodology Manual (OSSTMM), **Penetration Testing Execution Standard (PTES)**, and National Institute of Standards and Technology (NIST).
- This section should clearly mention whether any **specific standard open-source, proprietary, or combination** of methodologies was used during pen testing.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Testing Methodology

In penetration testing, methodology refers to a standard framework process that the testers are advised to follow to perform the testing. The testers may follow a single methodology or may combine various models to provide output and recommendations that best suit the client's requirements.

Some of the most commonly followed methodologies are as follows:

- Information Systems Security Assessment Framework (ISSAF)
- PCI Penetration Testing Guide
- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- National Institute of Standards and Technology (NIST)

It is recommended that this section of the test report includes information about the standard framework followed by the testers. It should also clearly mention whether the testers had used any specific standard open-source methodologies, proprietary methodologies, or a combination during the testing process.



## Planning



- This section explains how the pen tester planned the complete **penetration testing process** and how the actual test was performed.
- It explains all-important **strategies** and **tactics** implemented for testing.
- It briefs about every step in a **sequential manner**, explaining them with relevant tables, graphs, diagrams, charts, etc.
- It explains the details of different types of **research** and **investigation** performed by the testers for the whole project.
- It also includes a list of **tools** and **utilities** that were used for testing the organization's information structure.
- It explains the testers' plans for testing **business-critical areas**, how risks were assessed, and the plans for **exploiting vulnerabilities**.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Planning

The penetration testing report should include the details of the planning phase of a test. This section should provide a detailed report of how the testers planned and executed the tests. It should include details of whether the testers were able to conduct the tests according to the plan or had to modify it or create a new plan during the test.

The planning section should contain all the strategies, approaches, and tactics such as different types of networks on which cyber attacks were performed and social engineering attempts targeted at the employees for obtaining crucial information. This section ought to provide details of every step in a sequential manner and explain them with relevant tables, graphs, diagrams, and charts.

The details of different types of research and investigation performed by the testers during the project should be provided. It is advisable to include details of encountered security risks such as code errors, network misconfigurations, and malicious attempts.

This section should include a list of tools and utilities that had been used for testing the organization's information structure. Explaining the testers' plans for testing business-critical areas, the process of analyzing their risks, and the plans for exploiting vulnerabilities is recommended.

## Exploitation



- 1 This section explains how the information security of an **organization was analyzed by the pen tester**, how the penetration testing was carried out, and the obtained testing results.
- 2 This section also lists all the **vulnerabilities found** and the details about the actual exploitation process.
- 3 It also lists how the exploitation was carried out in **critical areas**, the extent to which it was successful, and the successful as well as failed attempts.
- 4 It includes a list of all the **tools and devices** actually used for exploiting the network, systems, applications, etc.
- 5 Finally, it briefly describes the vulnerabilities in the organization's infrastructure and the **exploitation results**.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Exploitation

The exploitation section of a penetration testing report explains the methods and techniques that the testers had adopted to exploit the vulnerabilities across the targets to complete testing. This section should explain the information security analysis process of an organization along with the used testing method as well as their result.

All the vulnerabilities found in this section should be listed, and details should be provided about how they were actually exploited. This section should explain the complete exploitation process carried out by the testers in critical areas along with both successful as well as failed attempts.

Including a list of all the tools and devices the testers had used for exploiting the network, systems, apps, etc. as part of the test process is recommended. It is advised to briefly describe the vulnerabilities in the organization's infrastructure and describe the exploitation results.

## Reporting



- 1 The report section includes details about the **findings** and **assessments** of the vulnerabilities found by the pen tester.
- 2 It explains how the threats and **risks are classified** and how **ratings** are assigned.
- 3 It provides a detailed description of each **risk** and the ratings assigned and lists the **measures/steps** to mitigate them.
- 4 It is a final conclusion about the **organization's information system** that is prepared by the team and submitted to **senior management**.
- 5 The severity/risk level of identified vulnerability should be decided based on **Common Vulnerability Scoring System (CVSS)** ratings.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Reporting (Cont'd)



- CVSS provides an open framework for **communicating the characteristics and impacts** of IT vulnerabilities.
- Its quantitative model ensures repeatable accurate measurement while enabling users to see the **underlying vulnerability characteristics** that were used to **generate the scores**.

CVSS v3.0 and v3.1 Ratings

| Severity | Base Score Range |
|----------|------------------|
| None     | 0.0              |
| Low      | 0.1-3.9          |
| Medium   | 4.0-6.9          |
| High     | 7.0-8.9          |
| Critical | 9.0-10.0         |

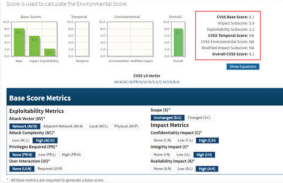
CVSS v2.0 Ratings

| Severity | Base Score Range |
|----------|------------------|
| Low      | 0.0-3.9          |
| Medium   | 4.0-6.9          |
| High     | 7.0-10.0         |

Source: <https://www.first.org>

### Common Vulnerability Scoring System Calculator (version 3) CVE-2017-0144

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Source: <https://nvd.nist.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Reporting

In this section, the testers should present the details of the testing process as assessments and findings of the vulnerabilities. This section contains the details of risks identified during the test and sorts them according to their severity. This section should explain the process of classification of threats and risks as well as the criteria used for grading them.

A detailed description of each risk found during the testing, its severity level, and the measures/steps the organization must mandatorily follow to mitigate them should be listed. In this section, including a conclusion about the organization's information system security that has been prepared and reviewed by the team is recommended.

It is recommended that the testers use commonly available frameworks such as Common Vulnerability Scoring System (CVSS) ratings for grading the severity or risk level of identified vulnerability.

- **CVSS Ratings**

Source: <https://www.first.org>, <https://nvd.nist.gov>

CVSS is an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics used to generate the scores.

| Severity | Base Score Range |
|----------|------------------|
| None     | 0.0              |
| Low      | 0.1–3.9          |
| Medium   | 4.0–6.9          |
| High     | 7.0–8.9          |
| Critical | 9.0–10.0         |

Table 14.6: CVSS version 3.0 and 3.1 ratings

| Severity | Base Score Range |
|----------|------------------|
| Low      | 0.0–3.9          |
| Medium   | 4.0–6.9          |
| High     | 7.0–10           |

Table 14.7: CVSS version 2.0 ratings

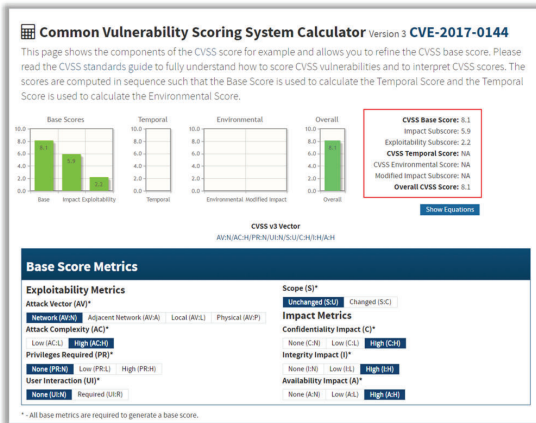


Figure 14.7: CVSS Calculator version 3

## Comprehensive Technical Report



Security | Penetration | Testing | Network

- This is a **detailed technical description** of the sequential process of penetration testing.
- The technical report discusses all the security defects found and precisely describes the technicality of security flaws and the process of their exploitation.
- Include technical details of cyberattacks, findings, vulnerabilities, and recommendations in this section.



- It further explains the technical details of the following:
  - Detailed Systems Information
  - OS Vulnerabilities
  - Web Server Vulnerabilities
  - Database Server Vulnerabilities
  - Application Security Vulnerabilities
  - Network Security Vulnerabilities
  - Vulnerabilities in Business Continuity Policy



Note: The technical report is usually reviewed by the technical department of an organization.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Comprehensive Technical Report

The penetration test report should include a comprehensive technical report that explains the technical details of pen tests. Explaining the step-by-step technical process involved in the scanning of the target, identification of the vulnerabilities, exploitation, cyberattack methodology, and details of data accessible is recommended.

The technical report discusses all the security defects found and precisely describes the technicality of security flaws and the process of their exploitation. Technical details of cyberattacks, findings, vulnerabilities, and recommendations are included in this section. The testing firm or team is advised to prepare the technical report and send it to the technical department of their organization for review.

The technical report further explains the technical details of the following.

- Detailed systems information: It notes the summary of critical issues exposed by the team in system architecture, etc.
- OS vulnerabilities
- Web server vulnerabilities
- Database server vulnerabilities
- Application security vulnerabilities
- Network security vulnerabilities
- Vulnerabilities in business continuity policy

For example, consider the vulnerabilities identified on Windows Server.

- **Windows Server:** This includes the vulnerabilities on the servers that the team had discovered while port scanning.

| Port Number | Service Running | Service Version Details |
|-------------|-----------------|-------------------------|
| 25          | SMTP            | Sendmail                |
| 90          | HTTP            | Apache                  |
| 443         | SSL             | Open SSL                |

Table 14.8: A sample table that clearly explains the comprehensive technical report of an organization

**Note:** The technical report is usually reviewed by the technical department of an organization.

## Result Analysis



The results analyzed should include the following:

1

Domain name



2

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports



3

Details of the test performed



4

IP addresses of the hosts



5

Description of the service



6

Vulnerability analysis



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Result Analysis

The penetration test report should comprise a detailed analysis of the test results and include information such as the threat level, vulnerability rating, and impact of the issue, risk level, and recommendations. This section should include an analysis of the tests, vulnerabilities, and their characteristics. The following details should be provided about each test result that is being analyzed:

- Domain name
- IP addresses of the hosts
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports
- Description of the services
- Details of the tests performed
- Vulnerability analysis



## Recommendations



- This section includes the pen tester's **suggestions or recommendations** for strengthening the organization's security level.
- It includes details about the extensive **research and investigation** conducted before recommendations are made.
- Identifying the vulnerabilities and documenting how to manage them is not sufficient. A pen tester is required to make suggestions that **manage, mitigate, and eliminate the weaknesses in the network security**; hence, this section includes all the security suggestions made by the pen tester to the organization.
- The testers should justify their recommendations and action plan with expert reviews in this section.
  - Indication of priorities and risks** – This subsection clearly explains, recognizes, and specifies the potential threats and prioritizes the risks that jeopardize the organization's information system.



| Category                  | Summary | Level of Threat | Percentage |
|---------------------------|---------|-----------------|------------|
| Number of Live Hosts      | 40      | High            | 60%        |
| Number of Vulnerabilities | 23      | Medium          | 36%        |

Table representing vulnerability assessment at different levels

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Recommendations

Recommendations refer to the suggestions that a tester provides the organization based on the analysis of test reports for mitigating vulnerabilities and strengthening the organization's security level. Testers should extensively research and investigate the process of strengthening the organization's security before suggesting recommendations.

In addition to identifying and documenting vulnerabilities, suggesting a process to manage, mitigate, and eliminate the identified weaknesses is recommended. Hence, this section includes all the security suggestions made by the tester to the organization. The testers should justify their recommendations and action plan with expert reviews in this section.

The section should also include details that indicate priorities and risks, which clearly explain, recognize, and specify potential threats and prioritize the risks that jeopardize the organization's information system.

The issue should be thoroughly analyzed before preparing recommendations, and all possible efforts must be made to cover all the network components specified in the scope. The test report is beneficial only if the suggested recommendations improve the security of the organization.

| Category                  | Summary | Level of Threat | Percentage |
|---------------------------|---------|-----------------|------------|
| Number of Live Hosts      | 40      | High            | 60%        |
| Number of Vulnerabilities | 23      | Medium          | 36%        |

Table 14.9: Table representing vulnerability assessment at different levels

## Appendices



- These include **additional information on pen testing** such as tools and exploits, snapshots, log output, risk assessment methodologies, and vulnerability classification, to provide the organization a clear understanding of the penetration testing report.

### A list of common appendices:

#### Required Work Efforts

- This appendix lists all the constraints faced during the testing and any additional effort required to complete the test than what was anticipated.

#### Research

- This appendix details all the research and investigation activities conducted by the penetration testing team.

#### Tools

- This appendix includes the tools list along with the output of the tools used during testing. Also includes details of exploitation using tools indicated using screenshots.

#### References

- This appendix includes proper references to authors and their works referred during the pen test.

#### Glossary

- This appendix is a detailed list of all the technical terms used in the report.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Appendices

These include additional information on pen testing such as tools and exploits, snapshots, log output, risk assessment methodologies, and vulnerability classification to provide the readers a clear understanding of the penetration testing report. Appendices do not include essential information, but additional information, and the most essential information about the report should not be included in the Appendices.

Common appendices of pen test report include the following.

- Required work effort:** This appendix should include details of all the constraints faced during the testing and any additional effort required to complete the test than what was anticipated.
- Research:** This appendix should include the details of all the research and investigation activities conducted by the testing team.
- Tools:** This appendix should include the tools listed along with the output of the tools used during testing. It should also include details of exploitation using tools indicated using screenshots.
- References:** This appendix should include proper references to authors and their works referred during the testing.
- Glossary:** This appendix should include a detailed alphabetical list of all the technical terms used in the report.

## Sample Appendix



### List of Appendices

|                                                                |     |
|----------------------------------------------------------------|-----|
| Appendix A— Live CD Distributions for Security Testing .....   | A-1 |
| Appendix B— Rules of Engagement Template.....                  | B-1 |
| Appendix C— Application Security Testing and Examination ..... | C-1 |
| Appendix D— Remote Access Testing.....                         | D-1 |
| Appendix E— Resources .....                                    | E-1 |
| Appendix F— Glossary .....                                     | F-1 |
| Appendix G— Acronyms and Abbreviations .....                   | G-1 |

Source: <http://csrc.nist.gov>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Sample Appendix

Source: <https://csrc.nist.gov>

It is recommended that the pen test report includes appendices. An example of an appendix is shown in the below figure.

### List of Appendices

|                                                                |     |
|----------------------------------------------------------------|-----|
| Appendix A— Live CD Distributions for Security Testing .....   | A-1 |
| Appendix B— Rules of Engagement Template.....                  | B-1 |
| Appendix C— Application Security Testing and Examination ..... | C-1 |
| Appendix D— Remote Access Testing.....                         | D-1 |
| Appendix E— Resources .....                                    | E-1 |
| Appendix F— Glossary .....                                     | F-1 |
| Appendix G— Acronyms and Abbreviations .....                   | G-1 |

Figure 14.8: Sample appendix



## Penetration Testing Report Analysis

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Penetration Testing Report Analysis



### Review

- After the pen testing team has completed the **onsite technical evaluation** of the client, all the gathered information should be sent to senior or higher authorities for review and evaluation.



### Determine Security Flaws

- Penetration testing report analysis by the senior testing team helps **determine the security flaws** in the conducted test.



### Analyze the Output

- Conduct a team meeting with peers and **analyze the output** from the conducted tests.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Penetration Testing Report Analysis

The penetration testing report should include an analysis of the report prepared by the pen testing team. The testing organization should have a board of senior members to evaluate the report and provide appropriate suggestions.

Steps to analyze the test report include the following.

- **Review:** After the testing team has completed the onsite technical evaluation of the client, all the gathered information should be sent to senior or higher authorities for review and evaluation.
- **Determine security flaws:** The senior testing team should evaluate the report and spot errors and security flaws in the conducted tests.
- **Analyze the output:** Conducting a team meeting with peers and analyzing the output from the conducted tests is recommended.

## Sections of the Penetration Testing Report



Divide the reports into sessions as follows:

### Network Test Reports

- Includes a detailed report about various tests performed on the **internal** and **external networks** and their components



### Client-Side Test Reports

- Includes details about different tests performed on the **client-side technologies** and their results



### Web Application Test Reports

- Includes a detailed report about various **web application pen tests** performed and their results



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Sections of the Penetration Testing Report

The penetration testing report should be divided into the following sections.

- **Network test reports:** This subsection includes a detailed report about various tests performed on the internal and external networks and their components. The results of the tests and recommendations should be included.
- **Client-side test reports:** The client-side test report contains details about different tests performed on the client-side technologies and their results. This subsection should include details of the vulnerabilities and weaknesses across the client-side technologies that allow the hackers to compromise the server-side technologies.
- **Web application test reports:** This section provides a detailed report about various web application pen tests performed by the testers and provides information about their results.

## Pen Test Team Meeting



 Set up an agenda for the meeting.

 Bring up all the questions about findings.

 Assign different sections of the findings to individual members.

 Create an action plan and set deadlines.

 Consult any additional expertise that might be needed.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Pen Test Team Meeting

The pen test team should conduct a meeting after completing the tests. An agenda should be set for the meeting, and all the team members must be involved to discuss the progress of the testing and develop the final report. During the meeting, bringing up all the questions and doubts about findings, process, or tools and clarifying them with peers is recommended.

This meeting will also help the team managers distribute different sections of the report to the team members for creating an effective report. The pen test team should try to discuss the main goal of the report, create an action plan, and set deadlines. The team meeting will also provide the testers an opportunity to consult any additional expertise required.

## Research Analysis



1

Check the identified **vulnerabilities** and find the latest **fix** or **patch** for each vulnerability.

2

Extensive **research** and **investigation** must be conducted for each vulnerability.

3

Research analysis helps the tester list the **functional anomalies** and performance issues.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Research Analysis

Before developing the report, the tester is advised to perform a research analysis on the vulnerabilities found during the assessment. The vulnerabilities should be analyzed, and their nature, including the reason for the occurrence, their effectiveness, and the process of fixing them, should be understood.

Extensive research and investigation should be conducted for each vulnerability to identify their severity level and the process of mitigation. This research analysis will help list the functional anomalies, performance issues, and gap analysis based on the organization's business needs, security objectives, and policies. The tester should find the patches for each vulnerability present across the target, as it will help make appropriate recommendations to the organization for improving security.



## Pen Test Findings



- Pen test findings are the **security issues uncovered** during the penetration testing.
- The substantive security issues in the pen test findings should be addressed one at a time.



- Each vulnerability must be reported appropriately as follows:
  - A detailed description of the vulnerability with an identifiable name
  - An evaluation in terms of mandatory and enhancement changes
  - References to certain information sources
  - Suggestions for resolving the issues

- The findings are categorized as follows:
  - Critical
  - High
  - Medium
  - Low



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Pen Test Findings

Pen test findings are the security issues uncovered during penetration testing. These findings should be included in the report classified according to their severity so that the readers from the target organization can prioritize working on severities with the highest impact first and then address lower impact vulnerabilities or risks.

Appropriately report each vulnerability as follows:

- A detailed description of the vulnerability with an identifiable name
- An evaluation in terms of mandatory and enhancement changes
- References to certain information sources for better understanding
- Suggestions for resolving the issues

Categorize findings as follows:

- Critical
- High
- Medium
- Low

## Rating Findings

**Extreme Criticality Findings**

- Loss could result in the unauthorized release of information that could have a **disastrous impact** on the organization's reputation or mission or financial assets or result in loss of life.

**High Criticality Findings**

- Loss could result in the unauthorized release of information that could have a **significant impact** on the organization's mission or financial assets or result in loss of life.

**Medium Criticality Findings**

- Loss could result in the unauthorized release of information that could have an **impact** on the organization's mission or financial assets or result in harming an individual.

**Low Criticality Findings**

- Loss could result in the unauthorized release of information that could have **some degree of impact** on the organization's mission or financial assets or result in harming an individual.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Rating Findings

Based on the findings, the vulnerabilities should be analyzed and categorized into the following based on their severity: critical, high, medium, and low. The levels of severity should be defined after discussing the vulnerabilities with the target organization and considering vulnerabilities in the most business-critical components as the highest priority. Each vulnerability should be categorized based on its severity.

- **Extreme criticality findings:** Loss of findings could result in the unauthorized release of information that could have a disastrous impact on the organization's reputation or mission or financial assets or result in loss of life.
- **High criticality findings:** Loss could result in the unauthorized release of information that could have a significant impact on the organization's mission or financial assets or result in loss of life.
- **Medium criticality findings:** Loss could result in the unauthorized release of information that could have an impact on the organization's mission or financial assets or result in harming an individual.
- **Low criticality findings:** Loss could result in the unauthorized release of information that could have some degree of impact on the organization's mission or financial assets or result in harming an individual.

Categorizing the criticality of a finding depends on the impact of these vulnerabilities on the customer business. Determining the criticality involves many factors, but the main point is identifying its effect on the organization.

## Detailed Findings Table



A detailed explanation of each finding consisting of the following:

|                   |                                                                |
|-------------------|----------------------------------------------------------------|
| 1 Finding Number  | 5 Location and Assets Exposed                                  |
| 2 Finding Name    | 6 Severity                                                     |
| 3 CVE Details     | 7 Description                                                  |
| 4 Category        | 8 Analysis/Exposure (research on the specifics of the finding) |
| 9 Recommendations |                                                                |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Detailed Findings Table

Including a detailed findings table in the final report is recommended. This table covers all the technical details of the findings along with their severity level. A detailed explanation for each finding consisting of the following elements should be included:

- Finding Number
- Finding Name
- CVE Details
- Category
- Location and Assets Exposed
- Severity
- Description
- Analysis/Exposure (research on the specifics of the finding)
- Recommendations

## Example of Finding - I



### Finding: SNMP Set password set to public

#### Finding ID #: 1

CVE/CAN: CAN-2014-0517

Category: Identification and Authentication (External Exposure)

Location: 10.0.0.4

Severity: Extreme

#### Discussion:

The Simple Network Management Protocol (SNMP) default public community name is specified, allowing anyone to change the computer's system information if they use this default value. An attacker can use SNMP to obtain valuable information about the system such as information on network devices and current open connections. In this case, the hacker can actually change the system information because the SNMP Set password is set to Public.

#### Recommendations:

Option 1: If the SNMP Service is not necessary, disable or remove it.

Option 2: If the organization requires the use of the SNMP Service, take steps to secure the SNMP community names and the community strings.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Example of Finding - I

### Finding: SNMP Set password set to public

#### Finding ID #: 1

CVE/CAN: CAN-2014-0517

Category: Identification and Authentication (External Exposure)

Location: 10.0.0.4

Severity: Extreme

#### Discussion

The Simple Network Management Protocol (SNMP) default public community name is specified, allowing anyone to change the computer's system information if they use this default value. A hacker may use SNMP to obtain valuable information about the system such as information on network devices and current open connections. In this case, the hacker can actually change the system information because the SNMP Set password is set to *Public*.

#### Recommendations

- Option 1: If the SNMP Service is not necessary, disable or remove it.
- Option 2: If the organization requires the use of the SNMP Service, take steps to secure the SNMP community names and the community strings.

## Example of Finding - II



**Finding: Telnet default account accessible**

**Finding ID #: 2**

CVE/CAN: No common corresponding vulnerability

Category: Technical Finding (System Boundary)

Location: 10.0.0.4

Severity: High

**Discussion:**

An accessible default account was detected through Telnet. Default Telnet accounts allow attackers easy access to remote systems by providing a network-accessible service on the server or printer.

**Recommendations:**

Option 1: Disable the Telnet account/service on each network.

Option 2: Change the password for the account to a strong password.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Example of Finding - II

**Finding: Telnet default account accessible**

**Finding ID #: 2**

CVE/CAN: No common corresponding vulnerability

Category: Technical Finding (System Boundary)

Location: 10.0.0.4

Severity: High

**Discussion**

An accessible default account was detected through Telnet. Default Telnet accounts allow the hackers easy access to remote systems by providing a network-accessible service on the server or printer.

**Recommendations**

- Option 1: Disable the Telnet account/service on each network.
- Option 2: Change the password for the account to a strong password.

## Example of Finding - III



### **Finding: Directory listing enabled**

#### **Finding ID #: 3**

CVE/CAN: CVE-2018-3809

Category: Security Misconfiguration

Location: 10.0.0.4

Severity: Medium

#### **Discussion:**

An enabled directory listing was found on one of the web servers that allow attackers to quickly identify and access the resources available at a given path.

#### **Recommendations:**

Option 1: Configure the web server to prevent directory listings for all paths under the web root.

Option 2: Disable directory listings to prevent access to the directories and files within the specified path.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Example of Finding – III

### **Finding: Directory listing enabled**

#### **Finding ID #: 3**

CVE/CAN: CVE-2018-3809

Category: Security Misconfiguration

Location: 10.0.0.4

Severity: Medium

#### **Discussion**

Web servers provide automatic listing/indexing functionality to list all the files within a requested directory in case a normal base file is not present. When a user browses the home page of a web application, they usually type a URL such as <http://www.clientweb.com/home/>. Such a URL is equivalent to executing commands like "ls" in Unix or "dir" in Windows. An enabled directory listing allows attackers to quickly identify and access the resources available at a given path and perform further attacks.

#### **Recommendations**

- Option 1: Configure the web server to prevent directory listings for all paths under the web root.
- Option 2: Disable directory listings to prevent access to the directories and files within the specified path.

## Analyze



- To analyze the report, compare the initial **goals of the test** to the final results.



- Repeatedly analyze the **findings**.



- This is critical for preparing the **final report**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Analyze

The final outcomes of the penetration tests should be analyzed to ensure that the organization's pen testing goals have been achieved. The findings, including the vulnerabilities, security misconfigurations, etc. should be evaluated repeatedly for verification. This is critical for preparing the final report.

The following steps should be performed during the analysis phase:

- Obtain, verify, and evaluate the client's data to identify vulnerabilities.
- Assess the vulnerabilities for potential defense mechanisms.
- Analyze formerly gathered data that focuses on various diverse areas that are both technical and associated with the guidelines.
- Evaluate the possible monetary loss when the organization suffers from risks.
- Assess the passwords issued to users to authenticate the system.
- Check the consequences affecting a database when affected by errors.
- Observe the effectiveness of the security policy and a framework.

## Prioritize Recommendations



1

Focus on **high-priority** security concerns first.



2

Prioritize recommendations for **mitigating risks** to applications, networks, devices, and other tested components.



3

Develop different strategies to achieve short-term and long-term **security postures**.



4

Consider both required and available **resources** to maintain a consistent **level of information security**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Prioritize Recommendations

Penetration testers must include recommendations that will help the organization to strengthen its security. While including recommendations in the report, focusing on the most critical and high-priority security concerns first is advised because they may impact the organization's business and cause financial and reputational losses. Recommendations should be prioritized for mitigating risks to apps, networks, devices, and other tested components. Different strategies should be developed to achieve long-term and short-term security postures of the organization. Both the required and available resources should be considered to maintain a consistent level of information security. The technology changes that are required for the implementation of recommendations should also be considered.





## Penetration Testing Report Delivery

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Penetration Testing Report Delivery

This section discusses points for consideration while delivering the report, letter of attestation; steps for conducting cleanup and restoration; report retention; destroying the report after the tests, cleanup, restoration, and delivery; and the sign-off document.

## Delivering Penetration Testing Report



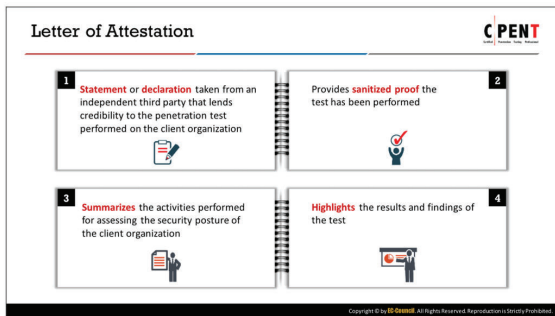
- 1 The report must be presented in **PDF format** unless requested otherwise.
- 2 A **printed report** is the best format.
- 3 Do not send the report to **unapproved staff**.
- 4 Always deliver the report to approved **stakeholders** in the organization in person.
- 5 **Avoid sending** the report by email or CD-ROM.
- 6 Always ask for a **signed acknowledgment** after submitting the report.
- 7 Be **available for 30-60 days after submitting** the report for answering any queries.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Delivering Penetration Testing Report

The final penetration testing report should be delivered personally to prevent the report from being accessed by an unintended third party. Here are some points to keep in mind while delivering the test report:

- Present the report in PDF format, as it has strong security mechanisms and is resistant to viruses, worms, and other malware.
- A printed report is the best format.
- Do not send the report to unapproved staff.
- Always deliver the report to approved stakeholders in the organization in person.
- Avoid sending the report by email or CD-ROM.
- Always ask for a signed acknowledgment after submitting the report.
- Be available for 30–60 days after submitting the report for answering any queries.



## Letter of Attestation

Letter of Attestation is a statement or declaration taken from an independent third party that lends credibility to the penetration test performed on the client organization. Penetration testing uncovers many vulnerabilities related to security posture, compliance, policies, and procedures, etc. that the organization might not have been aware of before the testing. A letter of attestation provides sanitized proof that the test has been performed. It serves as a record for performing a penetration test. The letter summarizes the activities performed for assessing the security posture of the client organization. It highlights the results and findings of the test. After following the test recommendations, the site should have eliminated the significant findings.

## Cleanup and Restoration



- 👉 Clean up all the **disruptions made to the network** while carrying out the penetration audit.



- 👉 **Restore** all the resources after the testing is completed.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Cleanup and Restoration

During pen testing, the testers try to access backdoors, exploit vulnerabilities, steal account credentials, and perform other malicious actions. All these activities may impact the network resources, user accounts, and lead to business disruption if they are not reversed after testing is over. Therefore, pen testers should clean up all the disruptions created during the testing process and restore all the tested systems, servers, apps, accounts, etc. to their original state. The cleanup and restoration process should ensure the following:

- The cleanup and restoration do not impact business operations.
- Ensure complete restoration by requesting the organization staff to check the cleanup process.
- Remove all the executable, scripts, and temporary files from the target systems.
- Use the secure deletion method to remove files and folders.
- Restore the system to the original configuration and settings in case of any changes made earlier.
- Remove all the backdoors and rootkits installed on the target system.
- Delete the temporary user accounts/credentials created for testing purpose.
- Remove the shells, if any, used for gaining backdoor access.
- Remove all the tools installed during the penetration testing process.

## Report Retention



- The pen test information is **sensitive** and **confidential**.
- Store** it only for a certain period (30–60 days is typical).
- Be able to **answer questions** during this period.
- After 30–60 days, **destroy the information** retained in storage.
- This clause is usually pre-determined in the **contract** with the customer before the engagement begins.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Report Retention

Penetration testing reports include sensitive information about the organization such as network infrastructure, database architecture, vulnerability and exploit data, and sensitive storage data, which may result in huge losses if accessible to an unintended third party.

After delivering the report, the organization may ask the testers to clarify doubts, raise issues, or discuss the processes clearly. Having a copy of the report will help the testers in supporting their claims and explaining the processes to the client. However, it is advised to store the report only for a certain duration (30–60 days is typical), which can be predetermined with the organization. During this period, the tester or testing team will be completely responsible for the security of the report and should answer the client's questions.

All the information related to the test and report retained in storage should be destroyed after the completion of the pre-determined duration. Organizations usually mention the duration and process of deleting the test reports and other information in the engagement contract.

## Destroy the Report



After **completing the penetration testing** and **mitigating all the vulnerabilities**, destroy the pen test report.

Based on the **agreement signed** with the company, the testing team may be asked to destroy the following:

|                                                                                                                      |                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Printed and electronic information  | All the penetration reports related to the company  |
| Email correspondence                | Test results                                        |
| Analysis documents                  | Reports                                             |

This applies to every team member of the penetration testing team.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Destroy the Report

The organization needs to take precautions to protect the pen test report from exposure. As part of this, they must ask the testing team to destroy the report after the tests, cleanup, restoration, and delivery of the report. The organization will mention the terms and conditions of destroying the report in the agreement signed during the engagement process.

The pen testing team should destroy the report and other relevant documents. Based on the agreement signed with the organization, the testing team is advised to destroy the following:

- Printed and electronic information
- All the penetration reports related to the organization
- Email correspondence
- Test results
- Analysis documents
- Reports

All the members of the team should remove all the data related to the target organization from their systems and devices used during any of the testing processes. This applies to every team member of the penetration testing team.

## Sign-off Document



1

A written **end-of-contract letter** that both parties are advised to sign after the completion of the penetration testing process



2

At this stage, send the **invoice** for the penetration testing job.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Sign-off Document

The sign-off document refers to a written end-of-contract letter that both parties are advised to sign after the completion of the penetration testing process. This will mark the end of the contract between the organizations and relieve the testing team and their firm from any responsibilities related to the test. The testers can send the invoice for the pen testing job at this stage.

## Sign-off Document Template



| ACCEPTANCE SIGN-OFF LOG |            |              |               |
|-------------------------|------------|--------------|---------------|
| CUSTOMER NAME           |            |              |               |
| PROJECT NAME            |            | PROJECT      |               |
| PROJECT PHASE           |            | DATE         |               |
| PROJECT MANAGER         |            |              |               |
| REF NUMBER              | ISSUE DATE | DELIVERABLES | DATE RECEIVED |
|                         |            |              |               |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Sign-off Document Template

| ACCEPTANCE SIGN-OFF LOG |            |              |               |
|-------------------------|------------|--------------|---------------|
| CUSTOMER NAME           |            |              |               |
| PROJECT NAME            |            | PROJECT      |               |
| PROJECT PHASE           |            | DATE         |               |
| PROJECT MANAGER         |            |              |               |
| REF NUMBER              | ISSUE DATE | DELIVERABLES | DATE RECEIVED |
|                         |            |              |               |

Figure 14.9: Sample sign-off document





## Post-Testing Actions for Organizations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Post-Testing Actions for Organizations

This section helps you understand the processes that the target organization is advised to perform after completing the penetration test.

## Develop an Action Plan



Organizations should develop an action plan to do the following:



Address the **security concerns** on time.



Reduce the **misuse or threat of cyberattacks** on the organization's network.



Identify the **specific areas** of security strengths and weaknesses.



Help the organization **conduct security checks** at regular intervals.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Develop an Action Plan

Post the pen testing process, the organization is advised to build an action plan to eradicate the vulnerabilities and weaknesses as well as implement recommendations to strengthen its security and protect business activities from cyberattacks.

The action plan is a follow-up activity after the testing that helps in providing input into the design of future tests. The organization should formally document, review, and implement the action plan after obtaining the approval of the senior management.

The plan should address security concerns on time, reduce the misuse or threat of cyberattacks on the organization's network, identify the specific areas of security strengths and weaknesses, and help the organization conduct security checks at regular intervals.

The action plan must include the following details mandatorily:

- A detailed description of the action
- Priority and category of action
- Individuals responsible and accountable for the action
- The target date for completion of an action

## Points to Check in Action Plan



- 1 Does the current security situation support the complete **business strategy**; what other technologies might give the organization a competitive edge?
- 2 Is the **current Information Technology** environment conducive to achieving e-business requirements?
- 3 Are the **organization's security-related expenses** included in the overall budget?
- 4 In what ways does the **company manage its risks**, and does it need to perform other tests?
- 5 Are **security, reliability**, and **privacy issues** ensured for the customer's data?
- 6 Are sufficient **resources** allocated to reduce the **business risks** or not?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Points to Check in Action Plan

The action plan should include all the relevant actions to prevent the vulnerabilities identified during testing from reoccurring. They improve the overall performance of the information security program. The following are points to check while developing an action plan:

- Does the current security situation support complete business strategy; what other technologies might give the organization a competitive edge?
- Is the current Information Technology environment conducive to achieving e-business requirements?
- Are the organization's security-related expenses included in the overall budget?
- In what ways does the organization manage its risks, and does it need to perform other tests?
- Are security, reliability, and privacy issues ensured for the customer's data?
- Are sufficient resources allocated to reduce the business risks or not?

## Develop and Implement Data Backup Plan



📌 Develop and implement a data backup plan that clarifies the following:

|                           |                          |
|---------------------------|--------------------------|
| 1 Which Data to Back Up   | 6 Integrity Verification |
| 2 Backup Method           | 7 Backup Security        |
| 3 Backup Schedule         | 8 Backup Restoration     |
| 4 Backup Media            | 9 Backup Responsibility  |
| 5 Backup Media Management | 10 Maintenance           |

📌 Data backups can be used to **recover data** in case of any security incident or accidental data deletion.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Develop and Implement Data Backup Plan

Organizations should develop and implement a data backup plan to recover data in case of any security incident or accidental data deletion. Even though developing a data backup plan requires investment of time and money, it will prevent the organization from the burden of recreating data. The organization is advised to develop and implement a data backup plan that clarifies the following:

- Which data to back up
- Backup method
- Backup schedule
- Backup media
- Backup media management
- Integrity verification
- Backup security
- Backup restoration
- Backup responsibility
- Maintenance

## Create Process for Minimizing Misconfiguration Chances

📌 Create a **configuration management process**.



📌 Create or use **configuration checklists** available from product vendors and security organizations such as **NIST** and **NSA**.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Create Process for Minimizing Misconfiguration Chances

The organization should correct all the misconfigurations mentioned in the report and create a process for minimizing the chances of misconfiguration in the future. Creating a configuration management process that ensures compliance of systems, devices, software, and apps with an organization's policy is recommended.

Organizations are advised to create their own configuration checklists from product vendors and security organizations such as NIST and NSA. These checklists help in maintaining and implementing secure configuration settings.

## Updates and Patches



- Improve the **level of control** for the purchased software by checking for updates and patches from the vendors.



- Create a **policy** for applying patches in an appropriate, timely manner.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Updates and Patches

The organization is advised to install all the new updates and patches, as well as create policies and procedures to regularly check and update all the systems. We recommend that the organization develop the following processes to improve the update and patching process:

- Use alerts from the developers and manufacturers regarding the updates.
- Improve the level of control for the purchased software by checking for updates and patches from the vendors.
- Create a policy for applying patches in an appropriate, timely manner.
- Ensure continuous updates to counter the latest threats.
- Update security processes frequently.
- Apply all updates, regardless of their type on an “as-needed” basis.
- Use virtual patches in the organization, as it provides additional identification/logging capabilities.
- Establish a disaster recovery plan to handle patch management failures.

## Capture Lessons Learned and Best Practices



- Note all the **flaws and weaknesses** found during the pen test and focus on developing an appropriate security strategy that prevents them in future.



- Create guidelines for best practices to be followed based on the **recommendations of the pen test report**.



- Create best practice documents for improving the security of all the components.



- Regular auditing of the organization **reduces exposure** to vulnerabilities.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Capture Lessons Learned and Best Practices

The organization is advised to note all the flaws and weaknesses found during a penetration test and needs to focus on developing an appropriate security strategy that prevents these weaknesses in the future. It is well-advised to create guidelines for best practices to follow based on the recommendations of the report. Policies should be created and implemented to conduct regular auditing of the organization to reduce exposure to the vulnerabilities. The organization should improve the following policies:

- Organizational standards policy
- Acceptable use guidelines
- Roles and responsibilities

The organization is advised to create best practice documents for improving the security of all the components including networks, hardware devices, software programs, servers, databases, etc.

## Create Security Policies



|                                                                                                                     |                                                                                                                     |                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
|  Systems Security Policy           |  Information Classification Policy |  Password Policy                       |
|  Strong Authentication Policy      |  Encryption Policy                 |  Virus Detection and Management Policy |
|  Security Change Management Policy |  Remote Network Access Policy      |  Firewall Security Policy              |
|  Network-connection policy         |  Email security policy             |  Acceptable-use Policy                 |

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Create Security Policies

Security policies are the organization's first line of defense. These help the organization protect its physical and informational security assets from security misconfigurations and setting flaws. The organization should create effective security policies and ensure appropriate implementation of those policies.

The organization is advised to create security policies such as the following:

- Systems security policy
- Information classification policy
- Password policy
- Strong authentication policy
- Encryption policy
- Virus detection and management policy
- Security change management policy
- Remote network access policy
- Firewall security policy
- Network-connection policy
- Email security policy
- Acceptable-use policy



## Conduct Training



- Conduct training for analyzing the **security posture** of a network.
- Conduct technical **security training** programs for people **managing IT**.
- Conduct training for application developers to help them develop **secure code**.



It is necessary to implement security education and awareness programs such as the following:

- General **security awareness** for new employees in the organization
- An awareness program through **e-learning**
- **Employee education** about the importance of **information security**
- Taking measures to **safeguard the privacy and confidentiality** of information, documents, files, email, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Conduct Training

Training should be conducted for analyzing the security posture of a network. A training program allows employees to strengthen the skills that they need to improve. The organization should ensure that all the employees are aware of security settings and comply with the regulations related to their work.

It is recommended that employees be trained in securing the data, systems, accounts, and other important aspects of their work while managing IT. Training should be conducted for app developers to help them develop secure code for app and software programs.

It is necessary to implement security education and awareness programs such as the following:

- General security awareness for new employees and ongoing employee education
- Creating awareness programs through e-learning and conducting training for analyzing the security posture of a network
- Technical security training programs for people managing IT
- Training on taking measures to safeguard the privacy and confidentiality of information, documents, files, email, etc.
- Creating visual aids such as posters to develop security awareness among employees

## Module Summary



- The pen testing report helps executive management make decisions about implementing security controls in the organization.
- The final report must clearly state the findings and map them to the potential risks.
- The scope of the project should include the IP address ranges that are mentioned in the contract and have been tested.
- The summary of findings is a comprehensive report about the findings that lists the discovered risks and threats in a specific manner.
- The report section includes details about the findings and an assessment of vulnerabilities identified by the pen tester.
- The penetration testing report analysis helps determine the security flaws in the conducted test.
- Data backups can be used to recover data in case of any security incident or accidental data deletion.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Module Summary

In this module, you have learned about the components of a pen test report and the process of creating it. Some of the important points to consider in relation to the topics covered are listed below:

- The pen testing report helps executive management make decisions about implementing security controls in the organization.
- The final report must clearly state the findings and map them to the potential risks.
- The scope of the project should include the IP address ranges that are mentioned in the contract and have been tested.
- The summary of findings is a comprehensive report about the findings that lists the discovered risks and threats in a specific manner.
- The report section includes details about the findings and an assessment of the vulnerabilities identified by the tester.
- The penetration testing report analysis helps determine the security flaws in the conducted test.
- Data backups may be used to recover data in case of any security incident or accidental data deletion.