



Module 02

Penetration Testing Scoping and Engagement

MODULE OBJECTIVE

Learn how to initiate, engage, and proceed with the penetration testing assignment.

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

Module Objective

In this module, you will learn the process to initiate, engage, and proceed with a penetration testing assignment as well as all the necessary elements that you must consider before implementing a penetration test. The main objective of this module is to guide you in employing a well-planned and scheduled penetration test.

Penetration Testing: Pre-engagement Activities



- Pre-engagement activities set the foundation for managing and successfully executing a penetration testing engagement.



- These pre-engagement activities constitute an important component in penetration testing and **should not be overlooked** by a pen tester or client.



- If the client and pen tester fail to properly follow the pre-engagement activities, they may face issues such as **scope creeping**, **unsatisfied customers**, and even **legal issues** in their penetration testing engagement.



- The pre-engagement activities in a penetration test start with determining the **goal of the test**.



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

Penetration Testing: Pre-engagement Activities

Pre-engagement activities help establish a clear understanding between the client and penetration tester. They set the foundation for managing and successfully executing a penetration testing engagement. These pre-engagement activities constitute an important component in penetration testing and should not be overlooked by a penetration tester or client. If the client and pen tester fail to properly follow the pre-engagement activities, they may face issues such as scope creeping, unsatisfied customers, and even legal issues in their penetration testing engagement. The pre-engagement activities in a penetration test start with determining the goal of the test.

The primary objectives for conducting pre-engagement activities are as follows:

- Evaluate the scope of penetration testing.
- Understand the type of penetration testing required.
- Determine the penetration test procedure.
- Identify the amount of resources needed for the test.
- Outline the rules of engagement (ROE).
- Determine the metrics for estimating the time and cost of the test.
- Estimate the overall cost.
- Ascertain the limits of engagement.
- Learn about the laws in the jurisdiction of the test location.



Request for Proposal

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

Request for Proposal

This section discusses the initial processes related to a penetration testing project and describes the issue of the request for proposal (RFP), proposal submission, and process of evaluating proposals.

Initiation of a Pen Testing Engagement Process



- The client first distributes a **request for proposal (RFP)** document to various penetration testing vendors or publishes one, asking the vendors to submit proposals before a due date.

Contents of a RFP

Purpose of the RFP

- Goals of the organization in relation to penetration testing:
 - Evaluate the security of the organization.
 - Identify any security issues that will impact the business.
 - Submit the findings and recommendations.

Technical & Contractual Contact

- Contact details of individuals to contact for proposal submission, specifications, SOW requirements, contract terms, conditions, etc.

Name	John
Address	
Phone	
Email	

Schedule of Events

- Specifies the timetable for events before engagement

Event	Date
RFP distribution to vendors	
Questions from vendors about scope or approach due	
Responses to vendors about scope or approach due	
Proposal due date	
Target date for review of proposals	
Anticipated decision and selection of vendor(s)	
Anticipated commencement date of work	

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

Initiation of a Pen Testing Engagement Process

An RFP is an invitation to penetration testers to submit their proposals of penetration testing services to the client organization. The client first distributes an RFP document to various penetration testing vendors or publishes one, asking the vendors to submit proposals before a due date. The main purpose of the RFP is to inform the vendors about the penetration testing opportunity and allow them to submit bids on various platforms such as websites, portals, and other applications.

An RFP helps organizations select an appropriate vendor that can meet their requirements and provide quality services. This RFP template also lists a set of questions related to different domains that the organization uses to assess and evaluate the proficiency of vendors.

The following are the contents of an RFP.

■ Purpose of the RFP

The goals of the organization in relation to penetration testing are as follows:

- Evaluate the security of the organization.
- Identify any security issues that will impact the business.
- Submit the findings and recommendations.

■ Technical and contractual contact

This component has contact details of individuals to contact for proposal submission, specifications, SOW requirements, contract terms, conditions, and so on. The following table presents a format that can be used for each contact.

Name	John
Address	
Phone	
Email	

Table 2.1: Contact details

- **Schedule of events**

This component specifies the timetable for events before engagement. The following table presents a sample schedule of events.

Event	Date
RFP distribution to vendors	
Questions from vendors about scope or approach due	
Responses to vendors about scope or approach due	
Proposal due date	
Target date for review of proposals	
Anticipated decision and selection of vendor(s)	
Anticipated commencement date of work	

Table 2.2: Schedule of events

Proposal Submission



A proposal in **response to an RFP** should contain the following elements:



1 Executive Summary: High-level synopsis, features, and benefits of the proposed engagement	5 Approach and Methodology: Detailed testing procedures and technical expertise needed for the engagement
2 Project Deliverables: Types of reports that will be provided (executive summary report, technical report, etc.)	6 Project Management: Method and approach used for project management and how the engagement will proceed from start to end
3 Itemized Pricing: Details on how charges will be calculated	7 References: Relevant references for similar work performed in the past
4 Team Strength: Biographies and relevant experience of team member	8 Company Briefing: Information on the company with its official address, contact details, expertise in offering similar services, etc.

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

Proposal Submission

The RFP provides details of the selection standards and procedures set by the organization. It also includes guidelines for filling the proposal document and the rights of the organization. Before submitting the proposal, the penetration tester should read the document carefully and understand all the conditions and disclaimers mentioned in it.

The organization awards the contract to the penetration tester whose proposal, in response to the RFP, is the most responsive and requires relatively low resources such as time and cost. The organization has the following rights while awarding contracts to vendors:

- It can deny any or all offers and suspend the entire RFP process without any liability to the vendors.
- There is no rule dictating that organization must award the contract to vendor who offered the lowest price. The firm has the right to reject the lowest-price offer and select the vendor as per its requirements.
- The organization can also select the vendor on a first-come-first-serve basis, without considering or waiting for the best offer.
- It can award more than one contract to the same vendor.

A proposal in response to an RFP should contain the following elements.

- Executive summary:** High-level synopsis, features, and benefits of the proposed engagement
- Approach and methodology:** Detailed testing procedures and technical expertise needed for the engagement

- **Project deliverables:** Types of reports that will be provided (executive summary report, technical report, and so on)
- **Project management:** Method and approach used for project management and how the engagement will proceed from start to end
- **Itemized pricing:** Details on how charges will be calculated
- **References:** Relevant references for similar work performed in the past
- **Team strength:** Biographies and relevant experience of team members
- **Company Briefing:** Information on the company with its official address, contact details, expertise in offering similar services, etc.



"Keep the common evaluation criteria in mind before submitting your proposal."

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

"Keep the common evaluation criteria in mind before submitting your proposal."

While filling the RFP and submitting it, the penetration tester must consider the evaluation criteria used by the client to select a proposal. The penetration tester must determine the goal of the client in issuing the RFP and submit a proposal that is aligned with the goal.

Common Evaluation Criteria for Proposals



The decision on selecting a proposal is based on the following:

- What has been taken into consideration while deciding the operational, technical, cost, and management requirements
- Responsiveness to the RFP
- Price quoted for all the items mentioned in RFP



The following primary considerations are also considered for evaluating proposals:

- Completion of the responses mentioned in the RFP in the correct format
- Ability to propose an effective solution based on the stated requirements
- Ability to deliver the proposed service against specifications
- Experience, stability, and past record, etc.
- Ability and availability of sufficient highly skilled team members

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

Common Evaluation Criteria for Proposals

The client evaluates proposals based on the penetration testing organization's considerations in deciding the operational, technical, and management requirements, as well as the total cost incurred for testing the items listed in the RFP.

The client also considers the responsiveness of the penetration testing organization and its interest in the RFP. The main criterion is the price quoted by the organization for completing the project.

The client can also consider the following primary considerations for evaluating proposals:

- Completion of the responses mentioned in the RFP in an organized, detailed, and correct format
- Ability to propose an effective solution based on the stated requirements
- Ability to deliver the proposed service against specifications
- Experience, stability, past record, and results on similar engagements
- Ability and availability of sufficient highly skilled team members
- Experience and qualification of the key personnel assigned
- Ability to propose an effective solution including best-practice methodologies, areas of focus, and proposed tools based on the stated requirements

During evaluation, the client may ask penetration testers for an oral presentation on the proposal. This provides an opportunity for the client to ask any questions they might have on the proposals submitted.



Preparing Response Requirements for Proposal Submission

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

Preparing Response Requirements for Proposal Submission

This section discusses the process of proposal submission, listing the goals of penetration testing, scoping a penetration test, conducting a penetration test scoping meeting, and so on.

Preparing for Proposal Submission



1

Identifying scope, approach, and methodology

4

Understanding staffing requirements

2

Determining project deliverables

5

Proposing detailed and itemized pricing

3

Determining the project schedule

6

Submitting the proposal

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

Sending a Preliminary Information Request Document to the Client



- The preliminary information request document provides guidelines for **gathering basic information** about the client's expectations from the penetration test.
- It contains the **client's contact details**, objectives and scope of pen testing, list of networks and devices to test, etc.



Contact Information		Scope of the Pen Testing/Security Audit		List what needs to be tested	
Company name:		What kind of penetration testing should be included?		Items	Details
Contact name:		☐ Black box (Company will not be provided with any network information)		☐ Servers	
Address:		☐ White box (Company will be supplied with full network information and diagrams)		☐ Workstations	
City:		☐ Gray box (Company will be supplied with limited network information)		☐ Routers	
State:		☐ External testing (Company will conduct tests from outside the perimeter firewall)		☐ Firewalls	
Country:		☐ Internal testing (Company will conduct tests from the internal network. Note that network organization will need to be considered)		☐ Networking devices	
Zip/Postal code:		What kind of penetration testing should be included?			
Email:		☐ Network testing			
Phone:		☐ Firewall/IDS testing			
		☐ Router and switches testing			
		☐ Denial of service testing			
		☐ Database testing			
		☐ VoIP testing			
		☐ Wireless testing			
		☐ Cloud testing			

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

Preparing for Proposal Submission: Identifying Scope, Approach, and Methodology

Sending a Preliminary Information Request Document to the Client

The preliminary information request document provides guidelines for gathering basic information about the client's expectations from the penetration test. It contains the client's

contact details; objectives and scope of penetration testing; a list of networks and devices such as servers, workstations, routers, firewalls, and network devices to test; and so on.

Contact Information	
Company name:	
Contact name:	
Address:	
City:	
State:	
Country:	
Zip/Postal code:	
Email:	
Phone:	

Figure 2.1: Contact information

Scope of the Pen Testing/Security Audit
What kind of penetration testing should be included? ☐ Black box (VampireTech will not be provided with any network information) ☐ White box (VampireTech will be supplied with full network information and diagrams) ☐ Grey box (VampireTech will be supplied with limited network information) ☐ External testing (VampireTech will conduct tests from outside the perimeter firewall) ☐ Internal testing (VampireTech will conduct tests from the internal network. Note that network segmentation will need to be considered) What kind of penetration testing should be included? ☐ Network testing ☐ Firewall/IDS testing ☐ Router and Switches testing ☐ Denial-of-Service testing ☐ Database testing ☐ VoIP testing ☐ VPN Testing ☐ Cloud testing

Figure 2.2: Scope of a penetration test/security audit

List what needs to be tested	
Items	Details
☐ Servers	
☐ Workstations	
☐ Routers	
☐ Firewalls	
☐ Networking devices	

Figure 2.3: List of components to be tested

Listing the Goals of Penetration Testing



1

Identify the organization's goal from the **purpose** section of the RPF and preliminary information request document.

2

Identify **what** the target organization wants tested.

3

Identify the **primary** and secondary goals of the organization.

4

The primary goals are **driven by business risk**, while secondary goals are **driven by compliance**.

Goal	Primary or Secondary?
Protecting stakeholders' data	
Reducing financial liability for noncompliance with regulations (e.g., GDPR)	
Protecting the company's intellectual property	
Ensuring a high level of customer trust	
Reducing the likelihood of a breach to protect brand reputation	
Safeguarding the organization from failure	
Preventing financial loss due to fraud	
Identifying key vulnerabilities	
Improving the security of the technical systems	

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

Listing the Goals of Penetration Testing

The main objective of an organization in conducting a penetration test is to analyze its own security configurations and determine its ability to resist any kind of intrusion attempts. The basic idea of penetration testing is to demonstrate the adequacy of the firm's security levels against the testing objectives. The organization's goal can be identified from the purpose section of the RPF and preliminary information request document.

Through the RFP, the organizations look for a vendor who can perform the following:

- Identify all the vulnerabilities and fix them.
- Find unauthorized ways of accessing the organizational resources and close them.
- Evaluate the security of current network configurations.
- Provide security training to employees.
- Discover issues with compliance.
- Identify the uncertainties associated with organization's web applications.
- Test the functioning of new tools, devices, and technologies.

The main intention of organizations is to fix their vulnerabilities before an attacker finds and exploits them. Firms also get an opportunity to take note of all security loopholes pointed out by the penetration tester and bring these issues to attention of the upper management.

Although the goals of penetration testing might vary based on the organization's requirements and environment under test, the basic idea remains the same. As a part of the proposal submission, the penetration tester should analyze the primary as well as secondary goals of the organization. The primary goals are driven by business risks, while secondary goals are driven by

compliance. The categorization of the goals of penetration testing is summarized in the below table.

Goal	Primary or secondary?
Protecting stakeholders' data	
Reducing financial liability for noncompliance with regulations (e.g., GDPR)	
Protecting the company's intellectual property	
Ensuring a high level of customer trust	
Reducing the likelihood of a breach to protect brand reputation	
Safeguarding the organization from failure	
Preventing financial loss due to fraud	
Identifying key vulnerabilities	
Improving the security of the technical systems	

Table 2.3: Goals of penetration testing



"Clarity of scope is key to getting value from pen testing." - Mike Gillespie

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

"Clarity of scope is key to getting value from pen testing."- Mike Gillespie

Scoping the Penetration Test

■ Scoping is one of the **important parts** of the penetration testing engagement process.

■ It is an **empirical process** that helps in gathering assessment requirements for the penetration test.

■ It further helps in **preparing the test plan**, limitations, business objectives, and time schedule for the proposed pen test.

■ It helps **define clear objectives**, with which the following can be identified:

- What will be tested
- How it should be tested
- What resources will be allocated
- What limitations will be applied
- What business objectives will be achieved
- How the test project will be planned and scheduled

Advantages:

- Scoping ensures the consistency and high success rate of the penetration test.
- A carefully defined scope helps in preventing collateral damage from intrusive scans or exploits.
- A lack of scoping can lead to a huge chance of failure of the penetration test because assessment requirements will have no proper definitions or procedures to follow.
- Scoping helps address all the required attributes to start the penetration testing project in a professionally sound manner.

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

Scoping the Penetration Test

The major goal of penetration testing is to perform a quality test of a realistic target while balancing both the time and resources of the client. To achieve this goal, penetration testers should have complete knowledge of all the possible networks, devices, infrastructure, and security that they need to test. Scoping is one of the important parts of the penetration testing engagement process. Scoping the target organization helps in assessing the possible elements and determining the approach and speed of tests, the tools required, and ROE. It further helps in preparing the test plan, limitations, business objectives, and time schedule for the proposed penetration test.

Scoping helps define clear objectives, with which the following can be identified:

- What will be tested
- How it should be tested
- What resources will be allocated
- What limitations will be applied
- What business objectives will be achieved
- How the test project will be planned and scheduled

The penetration test environment includes networks, applications, systems, servers, databases, new technologies, cloud systems, Internet service providers (ISPs), and managed security service providers (MSSPs). Penetration testers must gather the client requirements through verbal or written communication and assess the limitations of tasks.

The following are some key factors to consider when scoping a penetration test:

- **Target's criticality**

The criticality of a target may vary based on the business services or activities it offers. Penetration testers should determine in advance the mission-critical systems, networks, services, and applications as part of scoping.

- **Test location**

Some clients allow the penetration tester to work on site, while others prefer off-site locations as they do not want their employees to know about the test. The test location helps the penetration tester determine the approach and methodology required as well as gauge the client's requirements.

- **Test volume**

It is important to have an idea of the approximate number of systems involved in the test, number of IP addresses, list of web pages and parameters, and so on as this will help in determining the time and cost of the penetration test.

The advantages of scoping a penetration test are as follows:

- Scoping ensures the consistency and high success rate of the penetration test.
- A carefully defined scope helps in preventing collateral damage from intrusive scans or exploits.
- A lack of scoping can lead to a huge chance of failure of the penetration test because assessment requirements will have no proper definitions or procedures to follow.
- Scoping helps address all the required attributes to start the penetration testing project in a professionally sound manner.

Pen Test Scoping Meeting



- Once the goal is identified, schedule a scoping meeting with the client to define the **scope** of the proposed penetration test.
- In many cases, the scoping meeting can be arranged after the contract has been signed.
- However, there is a chance of the client arranging the scoping meeting before the contract is signed. In such cases, the client may ask the tester to sign an NDA before any in-depth scoping discussion.
- Rules of engagement (ROE)** and **cost** are not discussed in this meeting.

The scoping meeting covers the following discussions:

- Review the RFP Document:** Discuss and confirm information related to the client's expectations for the penetration test such as the client's contact details as well as the scope, type, and category of the pen test.
- Questionnaires:** Ask as many questions as possible so that the scope can be properly estimated.



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

Pen Test Scoping Meeting

Once the goal is identified, a meeting must be scheduled with the client to define the scope of the proposed penetration test. In many cases, the organizations arrange a scoping meeting after signing the contract. However, there is a chance that the client may arrange a scoping meeting before signing the contract. In such a case, the client may ask the tester to sign an NDA before any in-depth scoping discussion.

The main objective of the scoping meeting is to discuss what a penetration tester must test. The penetration tester will not discuss the cost and ROE in this meeting, as discussing these aspects can lead to a loss of focus on the scope. Hence, the penetration tester must moderate the meeting and ensure that the discussions are on topic to avoid distractions.

The scoping meeting covers the following discussions.

■ Review of the RFP document

Discuss and confirm information about the client's expectations from the penetration test such as the client's contact details as well as the scope, type, and category of the penetration test.

■ Questionnaires

Ask as many questions as possible so that the scope can be properly estimated:

- What does the client aim to gain out of the penetration test?
- Which IP ranges are in scope for the engagement?
- Should the test be performed at any particular time of the day?
- Are there any third parties that penetration testers must deal with?

- What are the client's major concerns that led them to initiate this testing process?
What is the most significant risk they are concerned about?
- Does the target environment operate in any other countries?
- What is the source of contact for further queries, if any?

Sample Questionnaires



Network Penetration Test

1. Why is the client having the penetration test performed against their environment?
2. Is the penetration test required to meet a specific compliance requirement?
3. When does the client want the active portions (scanning, enumeration, exploitation, etc.) of the penetration test conducted?
 1. During business hours?
 2. After business hours?
 3. On the weekends?
4. How many IP addresses in total are being tested?
 1. How many internal IP addresses, if applicable?
 2. How many external IP addresses, if applicable?
5. Are there any devices in place that may impact the results of a penetration test such as a firewall, an intrusion detection/prevention system, a web application firewall, or a load balancer?
6. In case a system is compromised, how should the testing team proceed?
 1. Perform a local vulnerability assessment on the compromised machine?
 2. Attempt to gain the highest privilege (root on Unix machines and SYSTEM or Administrator on Windows machines) on the compromised machine?
 3. Perform no, minimal, dictionary, or exhaustive password attacks against the local password hashes obtained (e.g., /etc/shadow on Unix machines)?

Source: <http://www.pentest-standard.org>

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

Sample Questionnaires (Cont'd)



Social Engineering

1. Does the client have a list of email addresses against which a social engineering attack needs to be performed?
2. Does the client have a list of phone numbers against which a social engineering attack needs to be performed?
3. Is the social engineering attack being performed for gaining unauthorized physical access? If so,
 1. How many people will be targeted?



Web Application Penetration Test

1. How many web applications are being assessed?
2. Will the test be executed against a live application or a snapshot of it in a testing environment?
3. How many login systems are being assessed?
4. Approximately how many static pages are being assessed?
5. Approximately how many dynamic pages are being assessed?
6. Will the source code be made readily available?
7. Will there be any kind of documentation?
 1. If yes, what kind of documentation?
8. Will static analysis be performed on this application?
9. Does the client want fuzzing performed against this application?
10. Does the client want role-based testing performed against this application?
11. Does the client want credentialed scans of web applications performed?

Wireless Network Penetration Test

1. How many wireless networks are in place?
2. Is a guest wireless network used? If so,
 1. Does the guest network require authentication?
 2. What type of encryption is used on the wireless networks?
 3. What is the square footage of coverage?
 4. Will enumeration of rogue devices be necessary?
 5. Will the team be assessing wireless attacks against clients?
 6. Approximately how many clients will be using the wireless network?

Source: <http://www.pentest-standard.org>

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

Sample Questionnaires (Cont'd)



Questions for Business Unit Managers

1. Is the manager aware that a test is about to be performed?
2. What is the main type of data that would create the greatest risk to the organization if exposed, corrupted, or deleted?
3. Are testing and validation procedures in place to verify that business applications are functioning properly?
4. Will the testers have access to the quality assurance testing procedures from when the application was first developed?
5. Are disaster recovery procedures in place for the application data?

Questions for Systems Administrators

1. Are there any systems that could be characterized as fragile, e.g., systems with tendencies to crash, with older operating systems (OSes), or that are unpatched?
2. Are there systems on the network that are not owned by the client and require additional approval to test?
3. Are change management procedures in place?
4. What is the mean time to repair system outages?
5. Is any system monitoring software in place?
6. What are the most critical servers and applications?
7. Are backups tested on a regular basis?
8. When was the last time backups were restored?

Source: <http://www.pentest-standard.org>

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

Sample Questionnaires

Source: <http://www.pentest-standard.org>

Network penetration test

- Why is the client having the penetration test performed against their environment?
- Is the penetration test required to meet a specific compliance requirement?
- When does the client want the active portions (scanning, enumeration, exploitation, and so on) of the penetration test conducted?
 - During business hours?
 - After business hours?
 - On the weekends?
- How many IP addresses in total are being tested?
 - How many internal IP addresses, if applicable?
 - How many external IP addresses, if applicable?
- Are there any devices in place that may impact the results of a penetration test such as a firewall, an intrusion detection/prevention system, a web application firewall, or a load balancer?
- In case a system is compromised, how should the testing team proceed?
 - Perform a local vulnerability assessment on the compromised machine?

- Attempt to gain the highest privilege (root on Unix machines and SYSTEM or Administrator on Windows machines) on the compromised machine?
- Perform no, minimal, dictionary, or exhaustive password attacks against the local password hashes obtained (e.g., /etc/shadow on Unix machines)?

Social engineering

- Does the client have a list of email addresses they would like a social engineering attack to be performed against?
- Does the client have a list of phone numbers they would like a social engineering attack to be performed against?
- Is the social engineering attack being performed for gaining unauthorized physical access? If so, how many people will be targeted?

Web application penetration test

- How many web applications are being assessed?
- Will the test be executed against a live application or a snapshot of it in a testing environment?
- How many sign-in systems are being assessed?
- Approximately how many static pages are being assessed?
- Approximately how many dynamic pages are being assessed?
- Will the source code be made readily available?
- Will there be any kind of documentation?
 - If yes, what kind of documentation?
- Will static analysis be performed on this application?
- Does the client want fuzzing performed against this application?
- Does the client want role-based testing performed against this application?
- Does the client want credentialed scans of web applications performed?

Wireless network penetration test

- How many wireless networks are in place?
- Is a guest wireless network used? If so,
 - Does the guest network require authentication?
 - What type of encryption is used on the wireless networks?
 - What is the square footage of coverage?
 - Will enumeration of rogue devices be necessary?
 - Will the team be assessing wireless attacks against clients?
 - Approximately how many clients will be using the wireless network?

Questions for business unit managers

- Is the manager aware that a test is about to be performed?
- What is the main type of data that would create the greatest risk to the organization if exposed, corrupted, or deleted?
- Are testing and validation procedures in place to verify that business applications are functioning properly?
- Will the testers have access to the quality assurance testing procedures from when the application was first developed?
- Are disaster recovery procedures in place for the application data?

Questions for systems administrators

- Are there any systems that could be characterized as fragile, e.g., systems with tendencies to crash, with older operating systems (OSes), or that are unpatched?
- Are there systems on the network that are not owned by the client and require additional approval to test?
- Are change management procedures in place?
- What is the mean time to repair systems outages?
- Is any system monitoring software in place?
- What are the most critical servers and applications?
- Are backups tested on a regular basis?
- When was the last time backups were restored?

Identifying the Types of Penetration Testing Assessment to Perform



- Identify the types of penetration testing assessment that the organization wants performed.

Important point for an objective-based test:

- Clearly understand the goal of the test and ensure that it is **SMARTER**.

S- SPECIFIC

M- MEASURABLE

A- ATTAINABLE

R-RELEVANT

T- TIME-BOUND

E- EVALUATE

R- REEVALUATE



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

Identifying the Types of Penetration Testing Assessment to Perform (Cont'd)



- Important points for a **compliance-based test**:



- Clearly understand the **requirements of standards, frameworks, laws**, acts, etc. with which the organization wishes to comply.

- The organization sets limitations, rules, and policies for compliance scope to avoid any act that can make it noncompliant at any stage during the penetration test.

- In **PCI-DSS**, it is important to limit the PCI-DSS scope by reducing/eliminating cardholder data from the environment. Otherwise, cardholder data may be exposed, making the organization noncompliant.

- The organization must clearly **understand the limitations**, rules, and policies of compliance scope as it needs to monitor and ensure that it remains PCI-DSS compliant.

Examples of limitations, rules, and policies in compliance scope:

- Limitation on the depth of penetration testing after finding a gap, in adherence to requirements
- Limitation on places from which data can accidentally leak
- Limitation on in-scope devices

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

Identifying the Types of Penetration Testing Assessment to Perform (Cont'd)



Important points for a **red-team assessment**:



- 1 Ensure specificity and accuracy in quantifying the testing environment, e.g., IPs within the scope.
- 2 Prioritize testing efforts based on the objectives, importance, and risk level.
- 3 Have a good understanding of the risk threshold.
- 4 Determine whether the budget matches the testing requirements.

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

Identifying the Types of Penetration Testing Assessment to Perform

The organization must identify the types of penetration testing assessment they wish to perform. The following factors help the organization determine the type of penetration testing to consider.

- **Requirement (Outcome):** To identify the type of penetration testing required, the organization must identify the requirement or the expected results of penetration testing. For example, penetration testing can be performed to find vulnerabilities in a system or application, assess the security posture by performing real-time attacks, etc.
- **Budget:** The security budget determines the types of penetration testing assessment to perform.
- **Compliance requirements:** The compliance requirements of the organization widely determine the type of penetration testing to perform. For example, an organization processing card payments must meet PCI DSS compliance requirements; hence, it needs to perform internal and external penetration testing.
- **Objective-based testing:** If the organization identifies that it must follow an objective-based testing approach, then it must clearly understand the goal of the test and ensure that it is specific, measurable, achievable, relevant, time-bound, evaluate, and re-evaluate (SMARTER).

For goal-oriented/objective-oriented penetration testing, SMARTER goals should be set. A goal-oriented approach should be accompanied by a strong testing methodology that includes appropriate techniques to identify risks. The full Open Web Application Security Project (OWASP) Testing Methodology can be used to enhance the efforts to identify the attack vectors.

The goal should be based on the following points.

- **Specific:** The goal must be defined clearly and explicitly. It should determine the expected outcome of the pen test. This will help define real-time goals.
- **Measurable:** The completion criteria and related quantitative or qualitative measurement method must be clearly described. The pen tester should know what will determine the achievement of the goal.
- **Attainable:** The set goal must be achievable. The objective should be realistic. An understanding of the required skills and resources will help in setting an attainable goal.
- **Relevant:** The goal must be relevant to the task the pen tester desires to achieve.
- **Aligned:** The goal must align with the organization's strategy, mission, and priorities.
- **Time-bound:** The time frame to achieve the goal should be set by determining a start and end time. Determining and planning the time frame for achieving critical milestones will enable pen testers to plan and prioritize their activities to achieve the goal within the set time period.
- **Evaluation:** The goal should be assessed periodically to determine whether the set target can be reached. Checkpoints or milestones should be defined, and the expected deliverables should be reviewed. Evaluating the set goal enables pen testers to review the progress of the goal and relieves them of the fear of failing to achieve the goal.
- **Reevaluation:** The goal needs to be re-evaluated regularly based on its evaluation and progress. Pen testers should review the process undertaken to perform specific tasks and the deviation of the actual result from the desired result. The problems should be identified, and appropriate solutions should be devised to reach the goal within the set time frame. Re-evaluation helps define new specific goals to overcome the drawbacks of previously set goals.
- **Compliance-based testing:** If the organization identifies that it needs to follow a compliance-based penetration testing approach, then it must clearly understand the requirements of standards, frameworks, laws, acts, etc. with which it wishes to comply. The organization must set limitations, rules, and policies for compliance scope to avoid any act that can make it noncompliant at any stage during the penetration test.

For example, in PCI DSS, it is important to limit the PCI DSS scope by reducing/eliminating cardholder data from the environment. Otherwise, cardholder data may be exposed, making the organization noncompliant. The organization needs to clearly understand the limitations, rules, and policies of compliance scope as it needs to monitor and ensure that it remains PCI DSS compliant. The following implementations are necessary to limit PCI DSS scope.

- Implement firewalls to restrict inbound and outbound traffic. Firewalls restrict external users from accessing the internal network and limit internal users' access to necessary data.

- Implement point-to-point encryption. Encrypt payment card and cardholder information beginning from the client end throughout the processing of the sensitive data.
- Use devices approved by the PCI Council.
- While using third-party vendors for payment processing, ensure that they are PCI DSS compliant.
- Segment the network and separate the cardholder data environment from the rest of the network.
- Implement methods approved by the PCI Security Council for timely disposal of cardholder information when not in use.
- The following are some of the examples of limitations, rules, and policies in compliance scope, which may include limitations on the depth of the penetration test implemented after finding gaps in adherence to requirement:
 - Limitation on places from which data can accidentally leak
 - Limitation on in-scope devices
- **Red-team assessment approach:** Based on requirements, if the organization identifies that it needs to follow a red-team-based assessment approach, then it should either evaluate the entire network or some portion of it to determine the critical functions to prioritize. Then, it should allocate the needed time and resources to perform penetration testing. The following points are important to implement a successful red-team assessment assignment:
 - Ensure specificity and accuracy in quantifying the testing environment, e.g., IPs within the scope.
 - Prioritize testing efforts based on the objectives, importance, and risk level.
 - Have a good understanding of the risk threshold.
 - Determine whether the budget matches the testing requirements.

Identifying the Testing Strategy



- The appropriate testing strategy **depends on the scenario** in which the testing is to be commissioned.
 - Black-box or white-box testing
 - Announced or unannounced testing
 - Blind or double-blind testing



- **Determine** if the approach is a black-box/white-box/announced/unannounced/blind/double-blind approach **before starting** the pen test.

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

Identifying the Testing Strategy

The main idea behind classifying is to propose a systematic approach to perform a successful penetration test. The selection of white- or black-box testing entirely depends on the testing scenario and environment. The penetration tester must mention if they will perform black-box/white-box/announced/unannounced/blind/double-blind testing before performing the actual test.

■ Black-box testing

Black-box testing, also known as behavioral testing, refers to the process in which the tester has no prior knowledge or information about a system. In this sense, black-box testing simulates a true web-hacking attack, beginning with only the organization's corporate name. From here, the ethical hacker gathers information about the network and business from as many outside sources as possible. This can include publicly available information from sources such as websites and media publications that contain useful information about the business.

To simulate real-world attacks and minimize false positives, penetration testers can choose to undertake black hat testing (or a zero-knowledge attack, with no information or assistance from the client) and map the network while enumerating services, shared file systems, and OSes discreetly. Additionally, the penetration tester can undertake war dialing to detect listening modems and war driving to discover vulnerable access points if it is legal and within the scope of the project.

■ White-box testing

If the organization needs to assess its security against a specific kind of attack or a specific target, it will provide complete information to penetration testers. The information

provided can include network topology documents, asset inventory, and valuation information. Typically, an organization would opt for this strategy when it demands a complete audit of its security.

White-box testing is based on the concept that penetration testers know the system and have full access to system-related information. Nevertheless, white-box testing has fundamental similarities to black-box testing in terms of the type of testing involved, even though the ethical hacker has complete information about the client organization and network infrastructure from the outset.

In this type of test, the tester can access the client's system design and implementation documentation, which may include listings of source code, manuals, and topological diagrams. This helps the ethical hacker adopt a structured formal approach. The tester initially verifies the authenticity of the information provided as input for the network evaluation.

- **Announced testing**

Announced testing refers to tests performed after a proper announcement. Before starting the test, the organization is informed. In this type of test, the organization makes an announcement to all its members, including stakeholders.

- **Advantages**

- This type of test is efficient.
 - The test is team oriented.

- **Disadvantages**

- Security is not tight.
 - This type of test may block penetration that would lead to the discovery of holes.

- **Unannounced testing**

Unannounced testing refers to tests performed without any prior announcement to the organization. This type of test is secretive in nature.

- **Advantages**

- This type of test is secure and reliable.

- **Disadvantages**

- The operation has a large impact.
 - It is relatively less efficient.
 - It requires a strict process.
 - Responses may block penetration.

- **Blind testing**

Blind testing stimulates the methodologies of a real attacker; the penetration testing team is provided limited or no information. It is a time-consuming and expensive process.

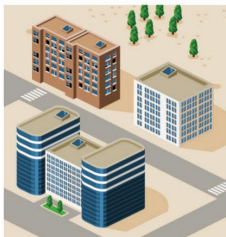
- **Double-blind testing**

Double-blind testing involves the testing of the organization's security monitoring, incident identification, and response procedures.

Identifying the Areas of Infrastructure to Test



- 1 Network Penetration Testing
- 2 Application Penetration Testing
- 3 Social Engineering Penetration Testing
- 4 Wireless Network Penetration Testing
- 5 Mobile Device Penetration Testing
- 6 Cloud Penetration Testing
- 7 Virtual Private Network (VPN) Penetration Testing



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

Identifying the Areas of Infrastructure to Test

▪ Network penetration testing

Network penetration testing includes the detection of vulnerabilities in network, system, and host devices that provide unauthorized access for the organization. This is the most commonly demanded area of infrastructure to test in any organization. This test examines following:

- Intrusion prevention system (IPS) evasion
- Firewall configuration testing
- Firewall bypass testing
- Stateful analysis testing

▪ Application penetration testing

In this growing world, a major part of the business functionality is conducted through web-based applications/mobile applications; accordingly, a major part of the chance of attack occurrence is in these applications. Application penetration tests stop internal or external unauthorized attacks on sensitive data by evaluating various elements such as user authentication, information leakage, privilege escalation, and removal of data.

Some important components of this type of penetration test are as follows:

- Code review
- Functionality testing
 - Input validation

- Transaction testing
- Authorization testing
 - Input validation of sign-in fields
 - Cookie testing
 - Lockout testing

▪ **Social engineering penetration testing**

Social engineering penetration testing works by tricking a human to reveal confidential information of an organization. This includes one of the following methods:

- Physical testing: Presence or physical means is utilized to gather sensitive information from a person. This includes threatening, convincing, and so on.
- Remote testing: Electronic means plays a crucial role in this type to reveal sensitive information; an example is a phishing email campaign.

▪ **Wireless network penetration testing**

Wireless network penetration testing includes examining all wireless networks and devices to discover any loopholes. As signals in wireless technologies propagate beyond the physical boundaries of an organization, the threats associated with wireless networks are unique and difficult to control.

The targets of this type of tests may include the following:

- Sign-in credentials
- Wireless protocols
- Wireless access points

▪ **Mobile device penetration testing**

Mobile device penetration testing involves examining all basic security features in a mobile device. The following elements must be considered while performing mobile device penetration testing:

- Rooting prevention controls
- Password brute force prevention
- Virtual private network (VPN) configuration
- Wireless security

▪ **Cloud penetration testing**

It is important to perform cloud penetration testing as many organizations use cloud services offered by third parties. Usually, cloud penetration testing is an external penetration test. It is necessary to have a clear understanding of the regulations of a service provider before testing an application on the cloud.

- **Virtual Private Network (VPN) Penetration Testing**

The objective of VPN penetration testing is to find any vulnerabilities in VPN configuration and implementation that can be exploited by an attacker to perform malicious activities.

Identifying the Targets to Test

Based on the **initial questionnaire phase** with clients in the scoping meeting, the penetration tester should be able to identify all the required targets for assessment.

They should identify what exactly to test for a specific type of test.

They should **identify targets** in the form of specific IP addresses, network ranges, domain names, devices to be tested, etc.

Examples of targets:

- Network
- Applications
- Users/employees
- Whitelisted/blacklisted IPs configured on IPS/firewall
- Access-control lists (ACLs) assigned on resources
- Organization's security policies
- Certificate pinning



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

Identifying the Targets to Test

The first stage of penetration testing involves information gathering, which helps in identifying all the test targets. Based on the initial questionnaire phase with clients in the scoping meeting, the penetration tester should be able to identify all the required targets for assessment. They should identify targets in the form of specific IP addresses, network ranges, domain names, devices to test, etc.

The following should be considered during the identification of targets:

- Selection of all targets
- Any limitations in the ROE
- Test duration
- End goal of the test

The following are some types of target-based penetration testing.

- **Network penetration testing:** testing the vulnerabilities, system misconfigurations, network, and services
- **Application penetration testing:** testing for vulnerabilities in applications; examples: cross-site scripting (XSS), structured query language (SQL) injection, and authentication and session management issues
- **Employee/user penetration testing:** testing for weaknesses in users and employees to determine whether they are vulnerable to various social engineering attacks such as phishing

- **Whitelist/blacklist of IPs configured on IPS/firewall:** testing the IPS and firewall configurations for whitelisted and blacklisted IP addresses
- **Access-control lists (ACLs) assigned on resources:** testing the ACLs configured on resources as per the security requirements
- **Organization's security policies:** testing the defined security policies for flaws
- **Certificate pinning:** verifying that the certificate is trusted and valid to ensure that Transport Layer Security (TLS) connections are working as intended

Identifying the Internal/External Targets to Test Within/Outside the Organization



- Persistent penetration testing of servers, workstations and desktops, and network devices can benefit enterprises in **hardening the security** and **integrity** of their infrastructure components.



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

Identifying the Internal/External Targets to Test Within/Outside the Organization

The penetration tester should identify all the internal and external targets of the organization that need to be tested. The tester should identify the types of tests required for these targets and determine whether they should conduct the designated tests on these targets from outside the organization's boundaries or from inside.

The test targets may include network devices, components, applications, and other elements within or outside the organization.

The following are some network components that might need to be tested.

- **URLs**
- **Servers**
 - Internet Information Services (IIS) servers
 - Application servers:
 - Client application servers
 - Web application servers
 - Windows servers
 - Unix/Linux servers
- **Workstations and desktops**

This includes the number of workstations per department, in case there are multiple departments in the organization.

- **Network devices**

- Routers
- Hubs
- Switches
- Modems
- Network load balancers
- Local area network (LAN) cards
- Gateways

Identifying any Targets that Require Dealing with Third Parties



- Identify the services or applications hosted by a third party such as **cloud service providers**, Internet service providers (ISPs), and managed security service providers (MSSPs) that need to be tested.



- Special permission should be obtained from such third parties to **avoid any legal issues**.



- Occasionally, the client may ask to test services or applications hosted by third parties.



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

Identifying any Targets that Require Dealing with Third Parties

In penetration testing, there are many cases that involve the testing of a service or an application provided or hosted by a third party such as a cloud service provider, an Internet service provider (ISP), and an managed security service provider (MSSP). In such cases, the penetration tester must take permission from the developer or service provider before starting the test. Failing to obtain the required permissions from third parties can lead to serious legal violations and leave the tester at risk.

For example, when testing an application hosted over a public cloud service, the penetration tester should notify the cloud service provider about the test and include details such as the time and process of the test. Further, the tester should perform comprehensive research on the testing process recommended by cloud services. Moreover, the limitations and regulations of the cloud services must be considered before initiating the test.

The penetration tester should also verify the terms of service of the ISP and test requirements before launching an attack. In many cases, the ISP will shut and block traffic it considers malicious. Therefore, provide clear information to the web hosting provider about the scope and timing of the test. It is always safe to notify MSSPs, especially when testing services and systems that they own.

Identifying any Targets that Require Dealing with Other Countries



- Identify the **countries** where targets, e.g., servers, are located.



- Do not rely on the client taking legal responsibility for any laws violated.



- Review** and **verify** the laws of the country where the targets are located.



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

Identifying any Targets That Require Dealing with Other Countries

The server location may also play a crucial part in launching an attack. The tester must verify the countries hosting the target servers and review all the laws and regulations of that country. The tester should not assume that the firm will take responsibility for any laws violated. It is the responsibility of testers to review and follow the laws of each region as they are responsible for any breach.

Understanding Client Assessment Requirements



- 📁 Create a **checklist** of assessment requirements.



- 📁 Identify the **time frame** and **testing hours**.



- 📁 Identify **who** will be involved in reporting and document delivery.



Items to Be Tested

📁 Servers	Yes ☐	No ☐
📁 Workstations	Yes ☐	No ☐
📁 Routers	Yes ☐	No ☐
📁 Firewalls	Yes ☐	No ☐
📁 Networking devices	Yes ☐	No ☐
📁 Cabling	Yes ☐	No ☐
📁 Databases	Yes ☐	No ☐
📁 Applications	Yes ☐	No ☐
📁 Physical security	Yes ☐	No ☐
📁 Telecommunications	Yes ☐	No ☐

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

Understanding Client Assessment Requirements

To avoid any miscommunications, both the company and penetration tester should sign a contract that contains a list of tasks explaining what the penetration tester will and will not test. The contract should also include the list of IP addresses, networks, subnets, computers, and so on that the penetration tester needs to test. The tester should identify the time frame and testing hours as well as who will be involved in reporting and document delivery.

The following figure shows a sample list of items to test. The penetration tester must maintain a checklist of the servers, workstations, routers, firewalls, networking, cabling, databases, and other company elements for the following reasons:

- To have an understanding of what to deal with
- As a proof, in case the organization blames the tester for accessing unauthorized elements

It is always recommended to note down the range of IP addresses or other elements to which the organization had granted access because there is a chance that the penetration tester might unknowingly access unauthorized IP addresses.

Items to Be Tested			
	Servers	Yes ☐	No ☐
	Workstations	Yes ☐	No ☐
	Routers	Yes ☐	No ☐
	Firewalls	Yes ☐	No ☐
	Networking devices	Yes ☐	No ☐
	Cabling	Yes ☐	No ☐
	Databases	Yes ☐	No ☐
	Applications	Yes ☐	No ☐
	Physical security	Yes ☐	No ☐
	Telecommunications	Yes ☐	No ☐

Figure 2.4: Sample list of items to test

Listing Tests That Will Not be Performed



- Identify the types of tests that should not be performed on the client organization before testing begins.

Examples

Social Engineering Penetration Testing

- Identify the pretexts that should not be used while performing a social engineering penetration test.
- Pretexts related to sex, drugs, porn, etc. may not be allowed in a corporate environment.
- Obtain approval in writing for acceptable pretexts before the test.



Denial of Service (DoS) Testing

- DoS pen testing may render the client organization's services unavailable to its users.
- If the client is an e-commerce company, then they may not want to get a DoS test performed on their website.
- DoS penetration testing should be performed only if the organization explicitly wants its infrastructure to be tested against the availability of services; this test should be approved in writing before it begins.

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

Listing Tests That Will Not be Performed

As requirements vary among companies, constraints in penetration testing change according to the company's domain. That is, a firm that allows penetration testers to access/test its cloud may not allow them to test its database, whereas others may allow them to test either or none of them. Hence, before implementing a penetration test, penetration testers should request the firm for the list of areas/devices that they must not access or test for vulnerabilities.

■ Social engineering penetration testing:

- Identify the pretexts that must not be used while performing a social engineering penetration test against the organization's employees.
- Pretexts related to sex, drugs, porn, etc. may not be allowed in a corporate environment.
- Obtain approval in writing for acceptable pretexts before the test.

■ Denial of Service (DoS) Testing

- Denial of service (DoS) penetration testing may render the client organization's services unavailable to its users.
- If the client is an e-commerce company, then they may not want to get a DoS test performed on their website.
- DoS penetration testing should be performed only if the organization explicitly wants its infrastructure to be tested against the availability of services; this test should be approved in writing before it begins.

Listing Security Exceptions

The pen tester should identify and prepare a list of various security exceptions before performing a penetration test. It enables the tester to restrict the scope of penetration testing. For example, the following tasks may be performed for this purpose:

- Prepare a list of all whitelisted and blacklisted IP addresses in the IDS and firewall to test the IDS and firewall configurations.
- Attempt unauthorized access to the resources in the list of assigned ACLs on various resources.
- List all the defined security policies across the organization and perform penetration testing to bypass the defined policy.
- Identify certificate pinning in the organization and perform testing to check if the certificate is valid or trusted for secure TLS connections.

Obtaining a Detailed Proposal of Tests to Conduct and Not Conduct



- Ask the client to submit a **detailed proposal** for the penetration tests to be conducted and those that should not be conducted.



- This detailed proposal will help in identifying the **nature** and **intensity** of the penetration test assignment.



- The proposal sheet should also specify the **test details** and **scope**, type of test, and number of tests required.



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

Obtaining a Detailed Proposal of Tests to Conduct and Not Conduct

Client organizations should provide detailed information about the nature and scope of the penetration test. The pen tester should ask the client to submit a detailed proposal for the tests to be performed and those that should not be performed. This will help in identifying the nature and intensity of a penetration test assignment.

In the proposal sheet, the pen tester should mention the following details:

- Number of IPs needed for testing
- Type of test
- Number of tests that must be performed
- Is an IDS system installed (Y/N)?

Deciding on the Desired Depth for Penetration Testing



- Decide the depth of the proposed penetration test based on the **scope identified** during the penetration test scoping.



- Consider the following factors for deciding the depth of the proposed penetration test:

- Type of testing** required (black box/white box/announced/unannounced/blind/double blind)
- Areas of infrastructure** to test (network/application/wireless network/cloud/DoS)
- Number of targets** to test (IP addresses, network ranges, domain names, and devices)

- The depth provides an estimate of the **time, resources, and expenses** required for the test.



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

Deciding on the Desired Depth for Penetration Testing

ROE includes the depth of penetration testing and type of testing, including DoS testing, database testing, and firewall testing. The pen tester should decide the depth of the proposed penetration test based on the scope identified during the penetration test scoping. The depth provides an estimate of the time, resources, and expenses required for the test.

The following factors must be considered when determining the depth of the proposed penetration test:

- Type of testing required (black box/white box/announced/unannounced/blind/double blind)
- Areas of infrastructure to test (network/application/wireless network/cloud/DoS)
- Number of targets to test (IP addresses, network ranges, domain names, and devices)

Preparing for Proposal Submission



1

Identifying scope, approach, and methodology

4

Understanding staffing requirements

2

Determining project deliverables

5

Proposing detailed and itemized pricing

3

Determining the project schedule

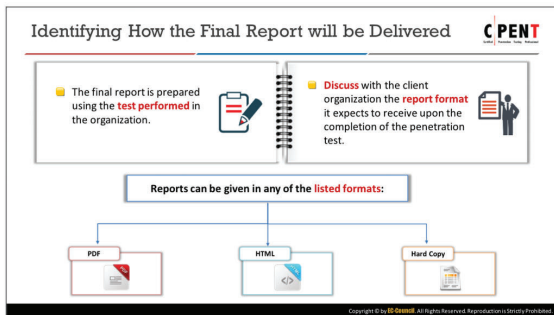
6

Submitting the proposal

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

Preparing for Proposal Submission: Determining Project Deliverables

This section specifies the process by which the pen tester must deliver the penetration testing report to the client as well as the elements that should be included for delivering a detailed report.



Identifying How the Final Report will be Delivered

Preparing the final penetration testing report is important in a penetration testing assignment. The pen tester should discuss with the client organization the report format that they expect to receive upon completion of the penetration test. The final report must be prepared based on the penetration test performed on the organization. The report should not only communicate facts but also present an expert opinion.

The goal of the report is to present all pertinent facts relating to the matter in an impartial and accurate manner and provide responsible, authoritative information to assist in determining whether to take corrective, remedial, or disciplinary action. The report should include related exhibits such as diagrams and pictures.

As much as possible, the report should present facts in the same order as that in which they were observed during the penetration test. It should include an outline or arrangement based on appendices and an exhibit that assists in assembling material for the report. The report should state the vulnerabilities, present the test results, draw conclusions, and propose recommendations. For assembling the facts and evidence, a logical presentation should be followed.

The detailed report should contain the following:

- **Vulnerabilities in the organization**
 - Prepare a pie graph or chart displaying low-, medium-, or high-ranking vulnerabilities.
- **Countermeasures to reduce vulnerabilities**
 - Propose countermeasures and remedies for the vulnerabilities found.

- **Recommendations**
 - Present best practices for the secure configuration of services and devices.
- **Document the result**
 - Prepare a document for the result generated after the penetration testing process.
- **Final summary**
 - Prepare a summary with an exhibit briefing the client on all the vulnerabilities found, its countermeasures, and best practices.

Reports can be presented in any of the following formats:

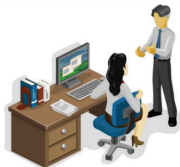
- PDF
- HTML
- Hard copy

Identifying the Reports to Deliver after the Pen Test



- The following are various reports provided after the completion of the penetration testing process:

- 1 Network test reports
- 2 Client-side test reports
- 3 Web-application test reports



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

Identifying the Reports to Deliver after the Pen Test

The reports submitted to the client organization after the completion of the penetration test process must include the following:

- **Network test reports**
 - Provides test reports on attacks over the network
- **Client-side test reports**
 - Provides test reports on attacks over end users
- **Web-application test reports**
 - Provides test reports on attacks over web applications

Preparing for Proposal Submission



1

Identifying scope, approach, and methodology

4

Understanding staffing requirements

2

Determining project deliverables

5

Proposing detailed and itemized pricing

3

Determining the project schedule

6

Submitting the proposal

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

Specifying the Test Duration



- After the scope has been identified, specify and agree on the **start** and **end for an engagement**.



- This allows for ending the engagement at a **predetermined time**.



- It also helps **overcome scope creep**.



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

Preparing for Proposal Submission: Determining the Project Schedule

Specifying the Test Duration

The duration of engagements depends on the scope of the test and size of the environment; it can last from a few days to a few weeks. The time taken to complete the penetration test purely depends on the experience and capabilities of the penetration testers. After the scope has been

identified, the pen tester should specify and agree on the start and end of engagement. This allows them to end the engagement in a finite time. It also helps arrest scope creep.

If the client does not provide sufficient time to penetration testers, then they would struggle to complete the test and might end up providing incomplete reports. If penetration testers ask for more time than needed, then the client may not show interest in offering them the bid. Therefore, penetration testers should analyze the resources, volume of the test, and their own capabilities before specifying the test duration. Note that a test might cross the expected due date in some rare conditions such as an increase in complexity and failure of efforts in covering additional scope.

The penetration tester should have a signed statement of work (SOW) outlining the start and end dates as well as the number of working hours required, in addition to clauses for extending the dates upon the assignment of any additional work.

Preparing for Proposal Submission



1 Identifying scope, approach, and methodology

4 Understanding staffing requirements

2 Determining project deliverables

5 Proposing detailed and itemized pricing

3 Determining the project schedule

6 Submitting the proposal

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

Project Team Staffing



- Identify a **group of experts** required in the penetration testing team based on the area and type of penetration testing.
- Specify the **details of expertise** in the team along with the skills and experience of team members.

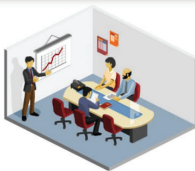
• Network Penetration Testers

• Policy Penetration Testers

• Application Penetration Testers

• Database Penetration Testers

• Report Writers



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

Preparing for Proposal Submission: Understanding Staffing Requirements

Project Team Staffing

The penetration tester should identify a group of experts required in the penetration testing team based on the area and type of penetration testing. Specify the details of expertise in the team along with the skills and experience of team members.

A project team should include the following:

- **Network penetration testers**

A network penetration tester identifies exploitable vulnerabilities in networks, systems, hosts, and network devices. They improve network security and provide protection for the entire network against attacks.

- **Policy penetration testers**

A policy penetration tester determines whether all the policies developed and analyzed are up to date and check for their implementation across the organization.

- **Application penetration testers**

Application penetration testers are proficient in testing vulnerabilities in certain types of applications. There are often multiple application experts on a team, each with expert knowledge about certain applications.

- **Database penetration testers**

Database penetration testers help organize and store data. They are responsible for ensuring the performance of the system and help maintain the database. They help secure and maintain the performance management system. They are responsible for securing confidential data.

- **Report writers**

A report and documentation writer develops manuals, project proposals, technical support documents, online help files, and product instructions.

Preparing for Proposal Submission



1

Identifying scope, approach, and methodology

4

Understanding staffing requirements

2

Determining project deliverables

5

Proposing detailed and itemized pricing

3

Determining the project schedule

6

Submitting the proposal

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

Estimating the Cost of the Pen Test Engagement



- The estimated cost depends on the estimated scope, resources, and time required for the pen test engagement.
- If the estimated scope, resources, and time required are high, then the **cost will also be high**.



Negotiate Per Day/Per Hour Fee for the Penetration Testing Project

- Based on the work performed by the testing team, negotiate the nature of payments as hourly or daily.
- Salary negotiation is handled by the chief penetration tester, and the salary is distributed as per the rules of the client organization.

How Much to Charge?

- Penetration test pricing varies based on the scope and number of man-days required to cover the scope of the project.

Report	Hourly Fees	No. Of Hours required
Network penetration testing report	\$ X	X Hours
Application penetration testing report	\$ X	X Hours
Mobile penetration testing report	\$ X	X Hours
Cloud penetration testing report	\$ X	X Hours

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

Preparing for Proposal Submission: Proposing Detailed and Itemized Pricing

Estimating the Cost of the Pen Test Engagement

Before negotiating the pay, penetration testers should have a clear understanding of their own capabilities, experience, market conditions, and organization policies.

A penetration test firm should provide several choices when with regard to pricing. The target organization should be provided various packages with different pricing options so that it can choose the most appropriate option for the contract it needs to draft.

The estimated cost depends on the estimated scope, resources, and time required for the pen test engagement. If the estimated scope, resources, and time required are high, then the cost will also be high. Pricing usually depends on the number of workdays required to cover the scope of the project. It can also be based on the number of target IP addresses. Another inclusion under the pricing of the test scope is the manpower required to perform the tests.

Target servers incur a higher cost per unit than client terminals because these devices require much deeper penetration and include more information to safeguard as well as analyze.

Pen testers should negotiate a per day/per hour fee for the penetration testing project in the following manner:

- Based on the work performed by the testing team, negotiate the nature of payments as hourly or daily.
- Salary negotiation is handled by the chief penetration tester, and the salary is distributed as per the rules of the client organization.

Penetration test pricing depends on the techniques used to perform the tests such as social engineering, competitive intelligence, device theft, and physical security. The following table presents a sample cost calculation for a penetration testing engagement.

Report	Hourly fee	No. of hours required
Network penetration testing report	\$X	X hours
Application penetration testing report	\$X	X hours
Mobile penetration testing report	\$X	X hours
Cloud penetration testing report	\$X	X hours

Table 2.4: Cost calculation for penetration testing

Preparing for Proposal Submission



1

Identifying scope, approach, and methodology

4

Understanding staffing requirements

2

Determining project deliverables

5

Proposing detailed and itemized pricing

3

Determining the project schedule

6

Submitting the proposal

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

Submitting the Proposal



- Prepare an **executive summary** with a high-level synopsis that briefs the client on the engagement, features, and benefits of the proposed work.



- Before submitting the proposal, have a **discussion** with different **experts in the team** and generate a draft proposal to be sent to the client for discussion.



- Draft the proposal with the expected response requirements.



- Submit the proposal before the due date specified by the client.



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

Preparing for Proposal Submission: Submitting the Proposal

The following are important instructions to bidders for proposal submission:

- Prepare an executive summary with a high-level synopsis that briefs the client on the engagement, features, and benefits of the proposed work.
- Before submitting the proposal, have a discussion with different experts in the team and generate a draft proposal to send to the client for discussion.

- Draft the proposal with the expected response requirements.
- Stick to the ethical standards associated with bidding and contractual processes. Offering any kind of bribe can lead to a criminal investigation against the bidder.
- Instead of simply specifying the total estimated cost for the overall project, bidders must provide a breakdown structure for the bid price. They should also provide financial and insurance documents based on the requirement.
- In addition to the complete project deadline, bidders should provide clear timelines for the core phases of the project such as organizational audits and resource developments.
- Ensure that the bid is submitted in a sealed envelope before the due date



"The bidder will receive a notification from the client upon selection of their proposal."

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

"The bidder will receive a notification from the client upon selection of their proposal."



Setting the Rules of Engagement

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

Setting the Rules of Engagement

This section discusses ROE as well as brainstorming sessions with the top management and technical teams.

Rules of Engagement



ROE

- The rules of engagement (ROE) is the **formal permission** to conduct penetration testing.

Top-level Guidance

- ROE provides "**top-level**" guidance for conducting the penetration test.

ROE's Assistance

- ROE helps testers **overcome legal, federal, and policy-related restrictions** to use different penetration testing tools and techniques.

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

Rules of Engagement (Cont'd)



01

Scoping and **ROE** are two aspects that need to be handled independently while engaging in a penetration testing assignment.

Scoping defines **what should be tested**, while ROE defines the agreement on how testing should be performed within certain limitations and rules during penetration testing.

02

03

The ROE specifies the manner in which the **penetration test** should be conducted.

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

Rules of Engagement

ROE is the formal permission to conduct a penetration test. It provides "top-level" guidance for conducting the penetration test and certain rights and restrictions to the test team for performing the test. It also helps testers to overcome legal and policy-related restrictions and use different penetration testing tools and techniques.

Based on the organization's requirements, the ROE may allow testers to conduct some technical and nontechnical activities such as port scanning, social engineering, and network sniffing and

may restrict certain activities such as password cracking and SQL injection attacks. All the activities that a penetration tester must perform during the test are explicitly defined in the ROE, and therefore, it acts as a guide to penetration testers.

Scoping and ROE

Scoping and ROE are two aspects must be handled independently while engaging in a penetration testing assignment. Scoping defines what should be tested, while ROE defines the agreement on the process of testing that must be performed with certain limitations and rules. The ROE specifies the manner of conducting the penetration test.

Framing an ROE involves the steps listed below:

1. Estimate the cost, time, and effort that the organization can invest.
2. Decide on the desired depth for penetration testing.
3. Conduct precontract discussions with different penetration testers.
4. Conduct brainstorming sessions with the top management and technical teams.

Brainstorming Sessions with the Top Management and Technical Teams



- Conduct a meeting with the top management and technical teams to **discuss the ROE**.



Rules are created based on the following common directives:

Establishing communication lines

- How often and in which manner will the test team and client communicate with each other?
- Who will be the point of contact (POC) for both the client and test team?

Timeline

- When will specific milestones in the engagement be completed?

Time/Location

- When and where will the progress of the test be informed?

Frequency

- What will be the frequency of meetings for briefing the client on the progress of the test?

Evidence handling

- What care should be taken while handling the evidence for the test?

Time of day to conduct testing

- At what time of the day should testing be performed?

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

Brainstorming Sessions with the Top Management and Technical Teams

A meeting should be conducted with the top management and technical teams of the organization to discuss the ROE, including the resources required, type of testing, budget required, and testers needed to perform the penetration testing process.

Rules should be created based on the following common directives:

- Establishing communication lines**
 - How often and in which manner will the penetration test team and client communicate with each other?
 - Who will be the point of contact (POC)? This includes client contact details and those of the penetration test team.
- Timeline**
 - When will specific milestones in the engagement be completed?
- Time/Location**
 - When and where will the progress of the test be informed?
- Frequency**
 - What will be the frequency of meetings for briefing the client on the progress of the test?
- Evidence handling**
 - What care should be taken while handling the evidence for the test?
- Time of day to conduct testing**
 - At what time of the day should testing be performed?



Establishing Communication Lines

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

Establishing Communication Lines

This section explains how to identify the details of the key contact at the client organization. These contacts will be in charge of the penetration testing project, and the pen tester should conduct an initial teleconference with the target POC (TPOC). This section also discusses the process of contacting key personnel at the client organization during the test.

Listing Contacts at the Client Organization in Charge of the Pen Testing Project



- Key personnel will be appointed by the organization to **take the lead of the project** from its side.
- Some important **contacts include** the risk manager, database administrator, network administrator, and system administrator.

A diagram showing the layout of a contact information form. It consists of five rectangular boxes arranged around a central icon of a laptop with a person silhouette. The boxes are labeled: 'Name of the personnel' (top), 'Role and department' (left), 'Personal contact numbers' (right), 'Email address' (bottom), and the central icon represents the contact details.

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

Listing Contacts at the Client Organization in Charge of the Pen Testing Project

Key personnel will be appointed by the organization to take the lead of the project from its side. In addition to the contact details of key personnel, the pen tester should gather the contact details of some other important personnel. These important contact details include those of the following:

- Risk manager, who handles risk in the organization
- Database administrator, who maintains the entire database of the organization
- Network administrator or system administrator, who handles the entire system or network

The contact details mainly include the following information:

- Name of the personnel
- Department
- Role or designation
- Mobile number
- Email address
- Office number

All this information should be gathered to ensure uninterrupted access to a contact from the client organization even if one contact is unavailable.

Obtaining the Details of Personnel to Contact at the Client Organization in Case of an Emergency



- Gather key **contact details** of personnel to approach in case of an emergency.
- Whom to contact in case of an emergency depends upon the **nature of the crisis**.
- A pen tester should be well prepared to ensure a safe and worry-free experience.
- Emergency situations include fire and electric breakdown.



■ Risk manager

■ Database administrator

■ Local security officer

■ ISP

■ Networking administrator

■ System administrator

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

Obtaining the Details of Personnel to Contact at the Client Organization in Case of an Emergency

One of the most important tasks of a penetration tester is to keep themselves safe from any unwanted situations and to concentrate fully on their responsibilities. Regardless of the domain and environment, the penetration tester should keep a record of emergency contact details of the client organization. Whom to contact in the case of an emergency depends on the nature of the crisis. Emergency situations include fire, electric breakdown, etc., and emergency contact details can include the phone number and email address of the human resources (HR) department, risk manager, project manager, ISP, local security officer, networking administrator, database administrator, system administrator, and chief secretary.

The pen tester should ensure that the individuals in the emergency contact list know them and have had a conversation with them at least once. The tester should avoid panic in an emergency condition and attempt to analyze the situation. After deciding who can help in this unexpected situation, the pen tester should contact them immediately. The person to contact can be any employee of the firm, ranging from the HR manager to project manager.

Points-of-Contact Template



- A POC refers to the **identification** and means of **communication** with person(s) and organizations(s) associated with resource(s).
- A POC can be a person or a **department serving** as the coordinator or focal point of information concerning an activity or program.
- POCs are used in many cases in which information is **time sensitive** and **accuracy** is important.

Organization	POC Name	Number/Email Address
Third Party	Name	Mobile/Email
Functional Area	Name	Mobile/Email
Authority Name	Name	Mobile/Email

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

Points-of-Contact Template

A POC refers to the identification and means of communication with person(s) and organizations(s) associated with resource(s). A POC can be a person or a department serving as the coordinator or focal point of information concerning an activity or program. Organizations must use POCs in cases wherein the information is time sensitive and accuracy is important.

The client or the target organization should appoint a primary POC and an alternate POC to provide necessary assistance to the penetration tester. These POCs should have a clear understanding of the scope, timelines, and constraints of the test. The following table presents a template for storing information on POCs.

Organization	POC Name	Number/Email Address
Third party	Name	Mobile/Email
Functional area	Name	Mobile/Email
Authority name	Name	Mobile/Email

Table 2.5: Points-of-contact template

Initial Teleconference with Target Point of Contact



- Obtain the email address of the **target POC (TPOC)** from the **engagement letter (EL)**.
- The pen tester should compose an **email** to the **TPOC** introducing themselves and **requesting a teleconference** at the TPOC's convenience.

The teleconference has the following purposes:



- Obtain the **initial information** needed to set up the engagement documentation.
- If required, **determine** who will provide the NDA and data use agreement (DUA).
- Determine how sensitive information will be transmitted between partners.



Note: The chief penetration tester or engagement team leader (ETL) must conduct a teleconference with the TPOC from time to time to finalize the document.

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

Initial Teleconference with Target Point of Contact

The TPOC email address is available in the EL. The penetration tester should compose an email to the TPOC introducing themselves and requesting a teleconference at the TPOC's convenience.

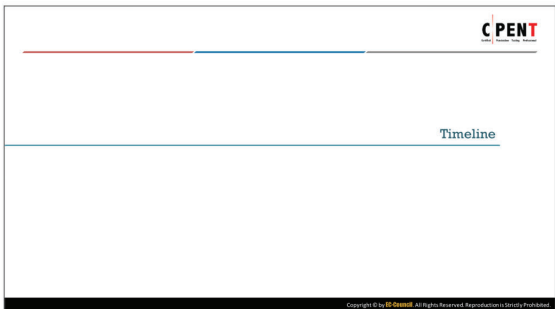
The teleconference has the following purposes:

- Obtain the initial information needed to set up the engagement documentation.
- Determine who will provide NDAs and DUAs (if required).
- Determine how sensitive information will be transmitted between the partners.

The penetration tester should keep the following points in mind during and after conducting the teleconference with the TPOC:

- Note all the points to discuss during the call
- Assign a person to note the key points that will be discussed during the call.
- Ensure that the call is made on time. A delay may lead to a poor impression.
- At the end of the call, provide a quick summary and discuss future steps that the client must implement.

Note: The chief penetration tester or engagement team leader (ETL) must conduct regular teleconferences with the TPOC to finalize the document.



Timeline

This section discusses the process of estimating the timeline for the engagement, metrics for time estimation, work breakdown structure or task list, and so on.

Estimating the Timeline for the Engagement



- 1 Once the scope of the pen test assignment and assessment requirements are clearly determined, the next step is to **plan** and **estimate** how time will be spent on the engagement.
- 2 Scope defines the **start** and **end of engagement**, while ROE defines the timeline for all activities during the engagement.
- 3 The timeline depends on the **canvas of the engagement**.
- 4 Some engagements may take **weeks** or **even months** depending on the canvas of the engagement.

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

Estimating the Timeline for the Engagement

Once the scope of the penetration test assignment and assessment requirements are clearly determined, the next step is to plan and estimate how to spend time on the engagement. Scoping defines the start and end of the engagement, while the ROE defines the timeline for all activities from the start to end of an engagement. Some engagements may take weeks or even months depending on the canvas of the engagement. One can use Gantt charts and work breakdown structures to define the work and the amount of time taken for each piece of work.

Metrics for Time Estimation



- 1 The estimated time depends on the **amount of experience** in the area of testing.



- 2 A pen tester with more years of experience in a specific type of testing may **take less time**.



- 3 Consider the **overhead of time** spent in meeting creeps, site problems, additional service, etc.



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

Metrics for Time Estimation

The experience of the tester plays a crucial part in determining the time required for a penetration testing project. A penetration tester with many years of experience in performing a specific type of testing they may take less time than one with less experience. Note that the tester should also consider the overheads of time spent in meeting creeps, site problems, additional service, and so on for time estimation.

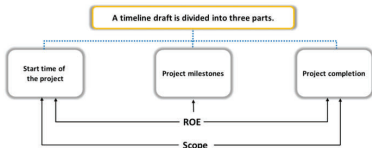
Adding 20% extra time to the estimated time is a good practice as this time could help fill gaps due to any interruptions that may occur during a test. The entire process of adding extra time to the estimated time is called padding. Padding helps in most cases involving new vulnerabilities, a network segment going down, and so on.

The pen tester should determine the last possible date for completing the tests. The signed agreement specifies the work, time of work, and specific date at which testing is to end.

Drafting a Timeline for the Pen Testing Project



- A draft timeline is required at the **beginning of a test** to clearly identify what work needs to be done and who will do it.
- **Gantt charts** and **work breakdown structures** can be used to create a draft timeline that will define the work, time required, and person in charge.



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

Drafting a Timeline for the Pen Testing Project

Before starting any project, it is important to determine a timeline for completion. A draft timeline helps penetration testers clearly identify the work and allocate individuals to it. Gantt charts and work breakdown structures can be used to create a draft timeline that will define the work, time required, and person in charge. This timeline depends on the size of the project and the available resources.

Penetration testers should create the timeline for the completion of testing according to the size of the organization and the number of IPs that they need to test. The client organization needs to define the goal of the testing so that the penetration tester can determine the time.

The timeline is the total time required to finish the project. As shown in the figure, this timeline draft has three parts:

- Start time of the project
- Project milestones
- Project completion

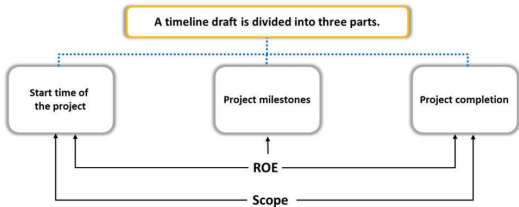


Figure 2.5: Components of the draft timeline

Work Breakdown Structure or Task List



- Developing a task list means breaking down a piece of work into its **component tasks**.
- The task status must be **measurable**.
- Each task must be a **clearly defined event** with a clear start and a clear end.
- Every task must have a **deliverable**.



Example:

- Where the tasks start and end
- Time estimates
- Task dependencies
- Resources assigned to each task



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

Work Breakdown Structure or Task List

A work breakdown structure refers to the breaking down of the entire project into a set of measurable tasks and depicting them as a chart. The task status must be measurable, and each task must be a clearly defined event with a clear start and end. Every task must have a deliverable. The main idea behind creating this graphical chart is to provide a clear view to the project manager.

For example, the chart can contain the following components:

- Where the tasks start and end
- Time estimates
- Task dependencies
- Resources assigned to each task

The work breakdown structure or task list helps the project manager to do the following:

- Analyze the various tasks involved in the penetration testing.
- Define the key objectives and create an associated flow to reach the final goal.
- Make optimal decisions.
- Manage and schedule the activities of the penetration test.
- Allocate necessary resources.
- Avoid redundancy.

The work breakdown chart can be represented as a tree graph in which the key objective is the “trunk” or “root node” and all the necessary steps to achieve the objective are represented as branches of the tree.

Penetration Testing Schedule



- A penetration test schedule **details the timing and duration** of various tasks involved in testing.
- It **provides a thorough design of the tasks** performed during penetration testing.
- Details of the test schedule **must be documented** in a separate deliverable and generated with the assistance of a project scheduling tool .
- The following tools may help in creating a penetration test schedule:
 - Microsoft Project Professional 2016
 - Zoho Projects
 - GanttProject



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

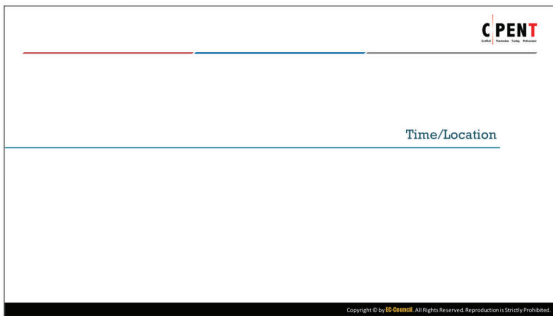
Penetration Testing Schedule

A test schedule includes the scheduled start and end dates of the penetration test, along with the expected dates for meeting any intermediate deadlines. All the elements should be documented in this test schedule as a separate supply of items by using a project scheduling tool.

The test schedule outlines the duration and timings of various penetration testing programs. It also provides a thorough design of every task performed during the test process, along with the time allotted for each. The testers should document details such as the task name, time, and project status after a stipulated duration in a deliverable format.

The following tools may help in creating a penetration test schedule:

- Microsoft Project Professional
- Zoho Projects
- GanttProject



Time/Location

This section discusses the identification of the reporting time scales and work location of the penetration tests.

Identify the Reporting Time Scales



📌 **Reporting time scales** include the following:

01

Normal time scale for the project



02

Local requested time scale for the project



03

Distribution list of the project



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

Identifying the Reporting Time Scales

The time scale defines the time it takes for the organization to conduct its operations. Testers should be prepared to accommodate flexible timings that will not affect the daily activities of the organization. A penetration tester should have attained a clear understanding of the project timeline in the planning phase itself.

The reporting time scales identified by the client organization should include the following.

- **Normal time scale for the project:**
 - Specify the normal duration or time required for completing the project.
- **Local requested time scale for the project:**
 - The local time scale requested by the team to complete the project.
- **Distribution list of the project:**
 - Specify the final distribution of the project.

Identifying the Office Space/Location where the Team will Work



- Identify the best and **most flexible space** that **suits the functional requirements** of the penetration test.

- Penetration testing is a **time-consuming process** depending on the client organization's testing requirements.

- The tester must ensure that the space provided for them and their team at the office premises of the client organization is **comfortable, spacious, and well ventilated**.

- The location should have **easy access** to restrooms and the cafeteria as well as **restricted access** for other employees of the client organization.



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

Identifying the Office Space/Location where the Team will Work

The following steps should be followed when identifying the office space where the penetration test will be conducted.

Before starting the penetration test, a penetration tester should discuss the location of work with the client. They should identify the best and most flexible space that suits the functional requirements of the penetration test. Penetration testing is a time-consuming process depending on the client organization's testing requirements. The tester needs to ensure that the space provided for their team in the client organization's premises is comfortable, spacious, and well ventilated. The location should have easy access to restrooms, and the cafeteria and should have restricted access for other employees of the client organization.

In most cases, the organizations might want tests to be conducted at their other branches across the world. In such cases, instead of travelling to all the locations, the testing team can use VPN connections for testing.



Frequency of meetings

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

Frequency of Meetings

This section provides information on the number of meetings that must be scheduled with the client.

Meeting with the Client



- A pen tester should keep the client **continuously informed** about the project.



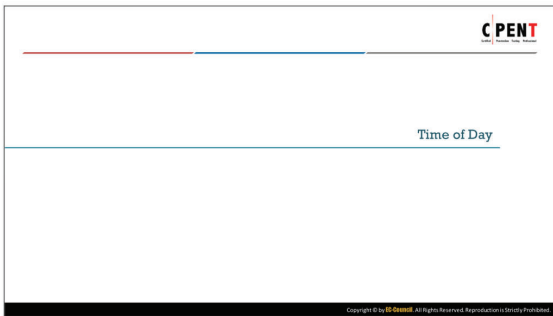
- Decide how often meetings should be held with the client regarding the progress of test: daily, weekly, etc.



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

Meeting with the Client

Penetration testers must schedule regular meetings with the client to keep them informed about the test status. The client should be given a complete and detailed picture of the project as well as timely updates. The tester must decide how often they will meet the client to discuss the progress of test; the meetings can be conducted daily, weekly, etc. In these meetings, the tester must clear any doubts and answer all the questions raised by the client. The tester can discuss the project plans, present critical findings, submit reports, and define problems occurring during the test.



Time of Day

This section discusses the process of deciding the time of day during which the penetration test will be conducted.

Deciding the Time of Day for the Test



Decide the **time of the day** at which testing should be performed.



Business hours



After business hours



Weekends



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

Deciding the Time of Day for the Test

The penetration tester should decide whether testing should be conducted during or after business hours or in the weekends. Client organizations can require penetration testers to run the tests after business hours or mostly during nights or weekends to avoid the disruption of customer services. Penetration testers should ensure that the client clearly communicates test timings prior to initiating the test.

A penetration tester can use Gantt chart tools that are available on the Internet for managing the timelines for every task involved in the penetration test. These tools also help in communicating with high-level management of the client's firm regarding the timelines.



Identifying Personnel for Assistance

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

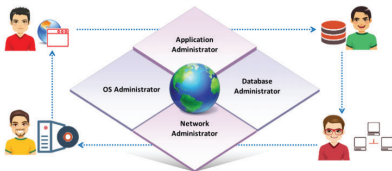
Identifying Personnel for Assistance

This section discusses the method of identifying personnel from the client organization who can help in the penetration testing process. They include the local human resources required for the penetration test. They may include the client's IT security admin, who will help with the penetration test.

Identifying the Local Human Resources Required for the Pen Test



- Study and understand the pen testing requirements to **identify the human resources required** to perform a successful pen test.
- The **local human resource** requirements to perform the penetration testing are as follows:



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

Identifying the Local Human Resources Required for the Pen Test

The pen tester should study and understand the penetration testing requirements to identify the human resources required to conduct a successful penetration test. The list of such human resources is as follows.

- **Application administrator**

The main function of the application administrator is to control the applications available for users and groups.

- **Database administrator**

The main functions of a database administrator include the following:

- Creating and testing backups
- Examining the integrity of data
- Checking the performance of the database

- **Network administrator**

The main function of the network administrator is to control and manage the hardware and software in a network.

- **OS administrator**

The main function of the OS administrator is to create directories, manage OS security, build backups, and restore backups. The functions of the OS administrators are similar to those of database administrators and application administrators. The pen tester must analyze the functions of each role and seek the help of the corresponding personnel based on requirements.

Identifying the Client's IT Security Admin



- ✚ To make the penetration testing successful, the tester must have an understanding of the **security-related issues** of the organization.
- ✚ The information security administrator is the person responsible for the **data and application security** of the organization.
- ✚ The **administrator of the organization** should be identified.
- ✚ The security administrator can provide an understanding of the **core parts of security** and is accountable for network and system updates.
- ✚ Security administrators can **assist in installing tools**, testing services, etc.

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

Identifying the Client's IT Security Admin

To make the penetration testing successful, the tester must have an understanding of the security-related issues of the organization. The information security administrator is the person responsible for the data and application security of the organization. Security administrators are responsible for analyzing, managing, and maintaining the desktop, mobile, and network security of a company. If possible, the administrator of the organization should be identified. The security administrator can provide an understanding of the core parts of security and is accountable for network and system updates. Major works performed by IT security admins are risk assessment, network traffic monitoring, software auditing, and training and awareness programs for other employees. Seek the help of IT security admins whenever needed, as they have clear knowledge on all security operations, tools, and techniques employed in the company.

Selecting Other Internal Employees



- The following internal employees can also **assist in the pen test engagement**.
- They can **provide valuable experience** and pass on their knowledge of the organization.

Internal Employees

Application Administrators

Database Administrators

Network Administrators

OS Administrators

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

Selecting Other Internal Employees

Internal employees

Internal employees play an important role in the penetration testing procedure. They can pass on helpful information on the organization to the penetration tester. If possible, the tester can use an internal employee's expertise while conducting the internal penetration test.

Internal employees can also act as targets in the case of an unannounced penetration test. Penetration testers can target internal employees and use social engineering techniques to obtain valuable information related to the organization and information assets. This exercise should be performed only with the involvement of top management, and its details should be included in the agreement.

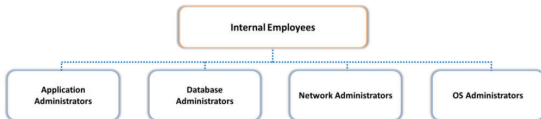


Figure 2.6: Types of internal employees

ROE Document



- ROE is a separate **formalized document** that states the rules to be followed during the execution of the engagement.



- The ROE established between the tester and client should be documented, and **both the parties should sign it.**



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

ROE Document

ROE is a separate formalized document that states rules to be followed by both the client and penetration testing organizations during the engagement. The ROE must be documented, and both organizations must sign it.

ROE template

DATE: [Date]

TO: [Name and Address of the Organization]

FROM: [Name and Address of the Third Party performing the Penetration Test]

CC: [Names and Addresses of Concerned Organization Officials]

RE: Rules of Engagement to Perform a Limited Penetration Test in Support of [required activity]

[Name of requesting organization] to perform an audit of [Name of risk assessment target]. The corresponding task order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the “Rules of Engagement” is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

Penetration test purpose

Penetration test objective

Scope

Timing

Methodology

Assessment tools

Deputy Chief Information Officer for
Information Technology Security

Date

XSECURITY: Sample ROE Document



XSECURITY Consideration Checklist

YES	NO	DESCRIPTION
		Has XSECURITY taken reasonable precautions to ensure that its own employees or the staff of any subcontractor will not take advantage of the opportunity afforded to them by the testing assignment to later initiate an unsanctioned attack against the client?
		Is XSECURITY acceptable to the organization's insurance underwriter (if any)?
		Does XSECURITY agree to be bound by clearly defined (and documented) terms of engagement?
		Does XSECURITY provide any kind of compensation if they, as a result of their testing activities, significantly disrupt the normal operation of the system being tested?
		Does XSECURITY provide any kind of compensation (or guarantee) if they fail to detect a security hole that is later successfully exploited by an intruder?

XSECURITY

Penetration Testing Rules of Engagement

Overview:

Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system, network, considerations, etc.). Penetration testing tools and techniques can be intrusive, however, so these needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools

The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings, updates, network and modulation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/ confidential files, only network/modulation files associated with system configuration and security. The XSECURITY does perform "penetration testing" - that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our team determines what vulnerabilities exist within the agency's network with full disclosure those vulnerabilities.

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

XSECURITY: Sample ROE Document

ROE is used to document various behavior-related elements among employees or team members. The main idea of an ROE is to establish good communication between the team members so that they can work together without any issues. As an example, the following table presents the various basic rules and interactions of a tester with a firm named XSECURITY. All these questions, which are from the tester's perspective, were answered by XSECURITY through the XSECURITY Consideration Checklist. The following table shows a sample ROE document of XSECURITY.

XSECURITY Consideration Checklist		
Yes	No	Description
		Has XSECURITY taken reasonable precautions to ensure that its own employees or the staff of any subcontractor will not take advantage of the opportunity afforded to them by the testing assignment to later initiate an unsanctioned attack against the client?
		Is XSECURITY acceptable to the organization's insurance underwriter (if any)?
		Does XSECURITY agree to be bound by clearly defined (and documented) terms of engagement?
		Does XSECURITY provide any kind of compensation if they, as a result of their testing activities, significantly disrupt the normal operation of the system being tested?
		Does XSECURITY provide any kind of compensation (or guarantee) if they fail to detect a security hole that is later successfully exploited by an intruder?

Table 2.6: XSECURITY consideration checklist

XSECURITY

Penetration Testing Rules of Engagement

Overview:

Security Assessment needs vary from agency to agency. The XSECURITY Penetration Testing Team (XSECURITY) offers several services that can assist COMPANY X in securing their information technology assets. Each of these services requires some degree of support from the COMPANY X (system information, access to agency personnel or facilities, system/network connections, etc.). Penetration testing tools and techniques can be invasive, however, so there needs to be a clear level of understanding of what an assessment entails, what support is required for assessments, and what potential effect each type of assessment may have.

Use of Tools

The Penetration testing activities performed by the XSECURITY Penetration Testing Team include scanning network assets with specific penetration testing tools. These tools check system configurations, default settings, security settings/updates, network and workstation services, open ports, and other specific vulnerabilities that might be utilized by intruders or unauthorized staff to undermine or bypass the security of an agency's network. They do not access user files, data files, or other personal/confidential files, only network/workstation files associated with system configurations and security. The XSECURITY does perform 'penetration testing' – that is, test how deep into your network an intruder can go, retrieve confidential information, or change system configurations. Our scans determine what vulnerabilities exist within the agency network with fully exploiting those vulnerabilities.

Figure 2.7: Sample rules of engagement

Sample ROE Template



Rules of Engagement Template

DATE: [Date]
TO: [Name and Address of NASA Official]
FROM: [Name and Address of Third Party performing the Penetration Testing]
CC: [Name and Address of Interested NASA Officials]
RE: Rules of Engagement to Perform a Limited Penetration Test in Support of [required activity]

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), [Name of requesting organization] to perform an audit of NASA's [Name of risk assessment target]. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.¹¹ Individual organizations may find it necessary to include additional information to supplement what is outlined here.

I. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (in, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, identification of appropriate subgroups for the test system, etc.

1.4. Risks

Identifies risks that arise when conducting information security tests—particularly in the case of sensitive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

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

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

Sample ROE Template

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

The screenshots below show different parts of an ROE document template.

Rules of Engagement Template

DATE: [Date]
TO: [Name and Address of NASA Official]
FROM: [Name and Address of Third Party performing the Penetration Testing]
CC: [Name and Address of Interested NASA Officials]
RE: Rules of Engagement to Perform a Limited Penetration Test in Support of [required activity]

[Name of third party] has been contracted by the National Aeronautics and Space Administration (NASA), [Name of requesting organization] to perform an audit of NASA's [Name of risk assessment target]. The corresponding task-order requires the performance of penetration test procedures to assess external and internal vulnerabilities. The purpose of having the "Rules of Engagement" is to clearly establish the scope of work and the procedures that will and will not be performed, by defining targets, time frames, test rules, and points of contact.

Figure 2.8: Rules of engagement template—part 1

Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.⁴² Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Figure 2.9: Rules of engagement template—part 2

Obtaining the Engagement Letter from the Client



- 1 A pen testing engagement begins with the **receipt of the EL**.



- 2 Once all agreements on **scope** and **ROE** are completed, the client sends the final EL.



- 3 Scan the EL into an electronic format. Produce an **MD5 hash** of the document for integrity purposes.



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

Obtaining the Engagement Letter from the Client

A penetration testing engagement begins with the receipt of the EL. Once the client and penetration testing organization agree on the scope and establish the ROE, then the client sends the final EL to the penetration testing organization. This letter includes a list of all tests and tasks that the organization wants the penetration testers to perform, a timeline for the complete project, goals, legal issues, disclaimers, and waivers.

The EL should be scanned and converted into an electronic format. An MD5 hash of the document should be produced for integrity purposes. The penetration tester should read the EL carefully and plan the project. Furthermore, the EL should be vetted by a lawyer for any legal discrepancies.



Handling Legal Issues in Penetration Testing Engagement

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

Handling Legal Issues in Penetration Testing Engagement

This section discusses the process of handling legal issues that may arise during the penetration testing process as well as the preparation process.

Hiring a Lawyer



- 1 Hire a **lawyer who can understand technology** and related matters.



- 2 **Sign a legal document** related to the penetration testing before starting the penetration testing assignment.



- 3 Have the document **vetted by the lawyer** before signing.



- 4 A **lawyer who understands information technology and the risks** associated with testing can render professional services more efficiently.



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

Hiring a Lawyer

The penetration testing organization or individuals must hire legal help to understand legal liabilities and defend themselves in the case of legal issues in the penetration test process. The organization or individuals must hire a lawyer who can understand information technology, risks associated with penetration testing, and related matters, as such a lawyer can render professional services more efficiently. A legal document related to the penetration test must be signed with the organization before starting the penetration testing assignment. Before signing the document, the lawyer must have read it carefully and examined it for any loopholes that can have an adverse impact and result in legal issues.

Penetration Testing Contract



☑ The penetration testing contract must be **drafted by a lawyer** and **signed** by the penetration tester and the client company.

The contract must clearly state the following:

1	Nondisclosure clause	4	Sensitive information
2	Objective of the penetration test	5	Confidential information
3	Fees and project schedule	6	Indemnification clause
7	Reporting and responsibilities		

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

Penetration Testing Contract

The penetration tester must check for service-level agreements in the project that may affect the scope of the test. Penetration testing involves risk. Both parties involved in testing must prepare, agree, and sign documents defining the scope of the test. Authorities from both organizations such as the director, CEO, CISO, and chief penetration testing officer must draft a penetration testing contract. The legal advisors and lawyers of both firms must examine the contract. The two firms will sign the agreement, which they must not disclose to a third party.

The contract must clearly state the following:

- Nondisclosure clause
- Objective of the penetration test
- Fees and project schedule
- Sensitive information
- Confidential information
- Indemnification clause
- Reporting and responsibilities

The tester should accept a waiver or privilege letter from the contractual partners to perform this test. Prior to the test, both parties should define the rules and principles they must follow. Legal issues that arise during a penetration test include the following:

- Issues that can provoke or trigger businesses or public authorities when conducting penetration tests
- Legal aspects that are the basis of the contract agreement

Drafting Contracts



- The pen test contract is the most important document to **define and regulate the legal relationship** between the penetration tester and client.

It protects both parties from misunderstandings and includes agreements such as the following:

- Scope of the Test
- Performance Standards
- Security and Confidentiality
- Audit Information
- Reporting and Cost
- Ownership and License
- Dispute Resolution and Indemnification



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

Drafting Contracts

The contract is a powerful legal tool that protects both parties from misunderstandings or miscommunications among the penetration tester, client, and third parties. It clearly allocates liability in case of unforeseen or unintended consequences such as a system crash, loss of access, compromised proprietary or sensitive information, and damage to the network or information residing on the network. The contract also helps define and regulate the legal relationship between the penetration tester and customer.

The penetration testing contracts must include the following elements:

- **Scope of the test**

A penetration testing contract should clearly describe the services, activities, and time required to conduct the test, as well as the type of penetration testing, number of target systems, and organization's environment. General terms must not be used in the contract, as they may be vague. For example, if the type of the penetration test is internal, then it should be clearly specified as an "Internal Penetration Test," rather than as a generic term such as "State of the Art."

- **Performance standards**

Organizations must include the minimum performance standards the penetration test must meet. It must also include the metrics used to measure a service level such as the response time of a product/system, errors associated with the product, product review periods, and targets for batch processing.

- **Security and confidentiality**

Organizations should also add details about their security policies in the contract. They should ask the penetration tester to not disclose information about their confidential data

and resources in any situation. It should also prohibit the penetration tester from accessing unallocated resources and data.

- **Audit information**

Many organizations allow its regulatory agencies and penetration tester to access its audit reports whenever needed. The contract must include the audit information that a penetration tester can access. It should also define accessible details such as the audit access frequency and charges applied for accessing the audit (if any).

- **Reporting and cost**

The client should include the type and frequency of reports it will receive in the contract. It should also address the requirements of reports and the fees for generating reports.

The contract should fully describe the fees for services that include any development or conversion, recurring services, and any other special requests. In addition, it should mention the additional costs applicable.

- **Ownership and license**

The contract must clearly mention the ownership of the organization's data, equipment, system documentation, systems, application software, and other intellectual property rights. It must state the rights of penetration testers over the mentioned property and permissions they need to acquire prior to accessing or conducting tests on them.

- **Dispute resolution and indemnification**

Organizations should ensure that the contract discusses the dispute resolution process to help resolve any disputes and resume services.

The contract should also include an indemnification clause, which states that the testing team will not be liable for any damages or loss of information during the test. Indemnification is included to defend the organization against any negligence or disregard of the penetration tester or any accidental loss or damage to the assets of the organization.

Sample Penetration Testing Contract



1

XSECURITY

Penetration Testing Contract

The below text is a sample contract only and does not obligate XSECURITY to perform services under any specified terms or conditions. This contract is for educational purposes only. Only valid signed contracts will be considered binding.

This contract is between XSECURITY (hereinafter referred to as the "provider") and Penetration Testing Services buyer (hereinafter referred to as the "client") for the supply of Penetration Testing services by the provider for the client.

Whereas the provider provides certain computer and systems security consulting and testing services including Penetration Testing services, and

Whereas the client wishes to retain the provider to provide computer and systems security services, specifically Penetration Testing services, therefore

The client does hereby retain the provider for the purpose of providing Penetration Testing services on the client's computer and/or system.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client to close the issues in a planned manner, thus significantly raising the level of their security protection. The client understands that Internet security is a constantly growing and changing field and that testing by XSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs, outputs for each software component in use. Further security breaches can and

- The client understands that Internet security is a continually growing and changing field and that testing by XSECURITY **does not imply that the client's site is secure from every form of attack**. There is no such thing as 100% security testing. For example, **it is impossible to test for vulnerabilities in software or systems** that are not known at the time of testing or to consider a mathematically complete set of all possible inputs/outputs for each software component in use.

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

Sample Penetration Testing Contract (Cont'd)



2

XSECURITY

Penetration Testing Contract

The below text is a sample contract only and does not obligate XSECURITY to perform services under any specified terms or conditions. This contract is for educational purposes only. Only valid signed contracts will be considered binding.

This contract is between XSECURITY (hereinafter referred to as the "provider") and Penetration Testing Services buyer (hereinafter referred to as the "client") for the supply of Penetration Testing services by the provider for the client.

Whereas the provider provides certain computer and systems security consulting and testing services including Penetration Testing services, and

Whereas the client wishes to retain the provider to provide computer and systems security services, specifically Penetration Testing services, therefore

The client does hereby retain the provider for the purpose of providing Penetration Testing services on the client's computer and/or system.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client to close the issues in a planned manner, thus significantly raising the level of their security protection. The client understands that Internet security is a constantly growing and changing field and that testing by XSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs, outputs for each software component in use. Further security breaches can and

- The **provider** shall be **under no liability** whatsoever to the client for any indirect loss and/or expense (including loss of profit) suffered by the client that arises from a breach by the provider of this contract. In the event of any **breach of this contract** by the provider, the remedies of the client shall be limited to a **maximum of the fees paid** by the client.



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

Sample Penetration Testing Contract (Cont'd)



3

XSECURITY

Penetration Testing Contract

The below text is a sample contract only and does not obligate XSECURITY to perform services under any specified terms or conditions. This contract is for educational purposes only. Only valid signed contracts will be considered binding.

This contract is between XSECURITY (hereinafter referred to as the "provider") and Penetration Testing Services buyer (hereinafter referred to as the "client") for the supply of Penetration Testing services by the provider for the client.

Whereas the provider provides certain computer and systems security consulting and testing services including Penetration Testing services, and

Whereas the client wishes to obtain the provider to provide computer and systems security services, specifically Penetration Testing services, and

The client does hereby obtain the provider for the purpose of providing Penetration Testing services on the client's computer and to system.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client to close the issues in a planned manner, thus significantly raising the level of their security protection. The client understands that Internet security is a continuously growing and changing field and that testing by XSECURITY does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or errors that are not known at the time of testing or the mathematically complete set of all possible inputs, inputs for each software component in use. Further security measures can and

- The provider and client have imparted and may from time to time **impart to each other certain confidential information related to each other's business**, including specific documentation. Each party agrees that it shall use **such confidential information solely for the purposes of the service** and that it shall not disclose directly or indirectly to any third party such information either expressed or otherwise.



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

Sample Penetration Testing Contract (Cont'd)



Penetration Testing Agreement

This document serves as a binding agreement between the Business Owner and Data Custodian (see Description page 2), and the client of the following contract(s) of application, the University Chief Information Officer, and the University IT Security Office.

Agreement to be tested:

Testing Time Frame: (begin) (end)

Penetration Testing Component(s) (see Description page 3). Indicate the testing components that are to be completed, by testing:

Component	Business Owner	Data Custodian
Defining Publicly Available Information		
Network Scanning		
Service Scanning		
Service Profiling		
System Profiling		
Vulnerability Identification/Exploitation		
Privilege Escalation		

As parties, by signing below, accept and agree that:

- The IT Security Office will use resources that to generate the operational status of systems, but cannot be generated.
- The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
- Test results are shared as specified below only. They include, but do not and cannot include, the actual details regarding specific vulnerabilities of the application system.
- All information contained in this testing will be treated as highly confidential level II security data, with appropriate protection.

Sign:

(Business Owner)

(Data Custodian)

(CISO)

(CISO)

Testing Complete: Date:

Review/Change Discussion Completed (Date):

Definitions

Data Custodian - The technical contact(s) that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms.

Business Owner - The senior official(s) within a college or departmental unit (or his/her designee) that are accountable for managing information assets.

Penetration Testing Component Descriptions:

- Defining Publicly Available Information** - Researching the environment using publicly available data sources, such as search engines and web sites.
- Network Scanning** - Performing automated sweeps of IP addresses of systems provided and/or discovered, from on-campus and off-campus.
- Service Profiling** - Identification of the operating system and version numbers operating on the system, to focus subsequent tests.
- System Profiling** - Identification of the services and applications as well as their version numbers operating on the system, to further focus testing on vulnerabilities associated with the identified services discovered.
- Vulnerability Identification** - Potential vulnerabilities (control weaknesses) applicable to the system are researched, tested, and identified.
- Vulnerability Validation/Exploitation** - After vulnerabilities are identified, they must be validated to minimize errors (false reports of problems), which involves attempts to exploit the vulnerability.
- Privilege Escalation** - Should exploitation of vulnerability be successful, attempts are made to escalate the privileges to obtain "complete control" of the system.

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

Sample Penetration Testing Contract

Let us consider a penetration testing contract from a firm to demonstrate the method of drafting a penetration testing contract by covering all the elements.

The following are some noticeable elements in a penetration testing contract:

- **Confidentiality**

In most cases, organizations do not want the penetration tester to share contract information or the contract itself with the outside world.

- **Responsibilities of the client**

Penetration testers must clearly mention the requirements for conducting the penetration test, starting from the scope information to emergency contacts.

- **Responsibilities of the tester**

Schedule timings, IP ranges, and other contact reasons can be mentioned in the contract. If needed, the client organization can include the cost, time, and scope limitation liability.

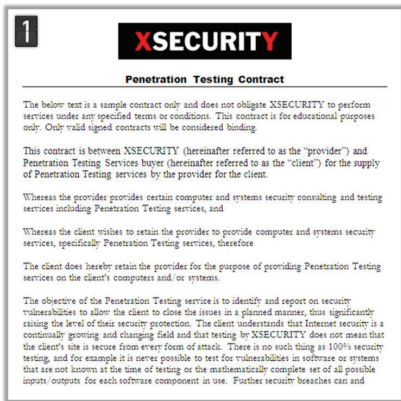


Figure 2.10: Sample penetration testing contract

In the sample contract shown in the above figure, the client understands that Internet security is a continually growing and changing field and that testing by XSECURITY does not imply that the client's site is secure from every form of attack. There is no such thing as 100% security testing. For example, it is impossible to test for vulnerabilities in software or systems that are not known at the time of testing or to consider a mathematically complete set of all possible inputs/outputs for each software component in use.

The provider shall be under no liability whatsoever to the client for any indirect loss and/or expense (including loss of profit) suffered by the client that arises from a breach by the provider of this contract. In the event of any breach of this contract by the provider, the remedies of the client shall be limited to a maximum of the fees paid by the client.

The provider and client have imparted and may from time to time impart to each other certain confidential information related to each other's business, including specific documentation. Each party agrees that it shall use such confidential information solely for the purpose of the service and that it shall not disclose directly or indirectly to any third party such information either expressed or otherwise.

The following figures show a sample agreement template and a description page, respectively. The agreement contains all the necessary fields that both organizations must fill and sign, whereas the "Definitions" page defines the important terms used in the agreement.

Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

- The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
- The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
- Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
- All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: _____ (Business Owner)

_____ (Data Custodian)

_____ (CIO)

_____ (CISO)

Testing Complete: _____ Date: _____

Review/Closeout Discussion Completed (Date): _____

Figure 2.11: Sample penetration testing agreement template

Definitions

Data Custodian - The technical contact(s) that have operational-level responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software platforms.

Business Owner - The senior official(s) within a college or departmental unit (or his/her designee) that are accountable for managing information assets.

Penetration Testing Component Descriptions:

1. Gathering Publicly Available Information - Researching the environment using publicly available data sources, such as search engines and web sites.
2. Network Scanning - Performing automated sweeps of IP addresses of systems provided and/or discovered, from on-campus and off-campus.
3. System Profiling - Identification of the operating system and version numbers operating on the system, to focus subsequent tests.
4. Service Profiling - Identification of the services and applications as well as their version numbers operating on the system, to further focus testing on vulnerabilities associated with the identified services discovered.
1. Vulnerability Identification - Potential vulnerabilities (control weaknesses) applicable to the system are researched, tested, and identified.
2. Vulnerability Validation/Exploitation - After vulnerabilities are identified, they must be validated to minimize errors (false reports of problems), which involves attempts to exploit the vulnerability.
3. Privilege Escalation - Should exploitation of vulnerability be successful, attempts are made to escalate the privileges to obtain "complete control" of the system.

Figure 2.12: Sample "Definitions" page of a penetration testing agreement

Penetration Testing “Rules of Behavior”



- Penetration testing “rules of behavior” is a penetration **testing agreement** that outlines the framework for external and internal penetration testing.



- Prior to testing, this agreement is **signed by representatives** from both the target organization and penetration testing organization to ensure a **mutual understanding** of the limitations, constraints, liabilities, and indemnification considerations.



- A **release and authorization** form may be required (in addition to the **rules of behavior**) that states the penetration testing organization will be held **harmless and not criminally liable** for unintentional interruptions and loss or damage to equipment.



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

Penetration Testing “Rules of Behavior”

Penetration testing “rules of behavior” is a penetration testing agreement that outlines the framework for external and internal penetration testing. Prior to testing, representatives from both the target organization and penetration testing organization sign this agreement to arrive at a mutual understanding of the limitations, constraints, liabilities, and indemnification considerations.

They help in designing test procedures for extracting the maximum or best output from the penetration test while having the least impact on the target resources. These rules assist in addressing unplanned events and accidents with the help of an incident response protocol. The rules of behavior most commonly address some penetration testing elements such as the type of the penetration test, scope of the test, and uncertainties associated with the penetration test.

The rules of behavior should also describe the set of constraints on certain attacks performed by the tester. For example, an e-commerce firm would not allow the penetration tester to implement a DoS attack, as it would disturb the Internet connection, which that firm’s business operations depend upon. Similarly, some other companies restrict the tester from performing war dialing and other attacks that may disturb their business operations. Every firm should create penetration testing rules by keeping the success criteria in mind to achieve the goals.

Penetration testers require a release and authorization form (also to the rules of behavior) that states the penetration testing organization will not be held criminally liable for unintentional interruptions and loss or damage to equipment.

Create a Get-Out-of-Jail-Free Card



- A **get-out-of-jail-free** card is an element that helps a person or organization **emerge from** an undesirable situation.
- The **agreement outlines** the types of **activities** to be performed and indemnifies the tester against any loss or damage that may result from the testing.
- The **get-out-of-jail-free** card entails a **legal agreement** signed by an authorized representative of the organization.
- The card is a **part of the penetration testing contract** and should include an incident response plan and appropriate client contact who can be alerted should an issue arise.

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

Create a Get-Out-of-Jail-Free Card

A get-out-of-jail-free card is an element that helps a person or organization emerge from an undesirable situation. The get-out-of-jail-free card defends the penetration tester from any unexpected/poor results of the penetration test. The client provides this card to the tester after signing a contract, which outlines the list of resources accessible and restricted to the testers. The agreement also outlines the types of activities to be performed and indemnifies the tester against any loss or damage that may result from the testing. Allocating a get-out-of-jail-free card to penetration testers implies that the customer has authorized them to test their systems. The card is a part of the penetration testing contract and should include an incident response plan and appropriate client contact who can be alerted should an issue arise.

Penetration testers should be careful while operating the get-out-of-jail-free card as it could result in legal issues if used inattentively. For example, even if a firm has authorized the tester to test their cloud network, the cloud admin or provider could blame the tester for accessing the cloud. Moreover, penetration testers will be at risk if the organization provides an incorrect range of IP addresses. If the tester attacks systems based on this incorrect IP address range, then they will be liable to legal claims.

Listing the Permitted Items in the Legal Agreement



- Before performing the test, the pen tester must necessarily know and **seek written permission** for the following essential elements:



Attack Methodology	Permitted?
Electronic Mapping – External	Yes
Electronic Mapping – Internal	Yes
Social Engineering by Telephone	Yes
Social Engineering by Mail	No
Adopt Employee Identity – Remote	Yes
Adopt Employee Identity – On Site	No
Break into Employee Workstation?	Yes
Read Corporate Email	No

Attack Methodology	Permitted?
Pretend to Be Technical Supplier	Yes
Dumpster Diving – On Site Outside	No
Dumpster Diving – On Site Inside	Yes
Dumpster Diving – Off Site	Yes
Target Sensitive Corporate Resources	No
Personnel Extortion, Blackmail and Coercion	No
Investigate Personal Backgrounds of Staff	No
Penetration of Business Partners	No

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

Listing the Permitted Items in the Legal Agreement

To avoid miscommunications and risk, penetration testers should list out all the attacks they will perform and send this list to the client organization for approval. On receiving the list, the client needs to approve only those attacks that are within company's limitations.

The following table presents a sample list of tests that a testing agency will perform and the approval obtained from the client. This includes various attack methodologies used by the testing team and requires prior permission from the client organization to perform them. Such permissions will allow the team to perform their testing processes in a hazard-free environment.

Attack methodology	Permitted?
Electronic mapping—External	Yes
Electronic mapping—Internal	Yes
Social engineering by telephone	Yes
Social engineering by mail	No
Adopt employee identity—remote	Yes
Adopt employee identity—on site	No
Break into employee workstation?	Yes
Read corporate email	No
Pretend to be technical supplier	Yes

Dumpster diving—on site outside	No
Dumpster diving—on site inside	Yes
Dumpster diving—off site	Yes
Target sensitive corporate resources	No
Personnel extortion, blackmail, and coercion	No
Investigate personal backgrounds of staff	No
Penetration of business partners	No

Table 2.7: Sample representation of tests

Confidentiality and Nondisclosure Agreement Clauses



- Many documents and other information regarding the pen test contain critical information that could **damage one or both parties** if improperly disclosed.



- The tester also **signs an agreement** guaranteeing that the company's information will be treated confidentially.



- It **provides cover** for a number of other key areas, such as negligence and liability, in the event of an untoward incident.



Agreements are designed to be used by both the parties to **protect sensitive information** from **disclosure**

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

Confidentiality and Nondisclosure Agreement Clauses (Cont'd)



- Both parties **bear the responsibility to protect** tools, techniques, vulnerabilities, and information from disclosure beyond the terms specified by a written agreement.
- NDA's should be **narrowly drawn** to protect sensitive information.



- Specific areas to consider include the following:**
 - Ownership
 - Use of the evaluation reports
 - Results and the use of the testing methodology in client documentation



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

Confidentiality and Nondisclosure Agreement Clauses

The NDA is a security contract signed between two individuals or companies for maintaining the confidentiality of the information shared between them. The parties sign this agreement when they intend to restrict the use of the shared information. NDAs are also known as confidentiality agreements, proprietary information agreements, and secrecy agreements.

Business experts state that NDAs are the best option when an individual or firm makes a contract with another. NDAs are useful when an individual or firm needs to share its confidential information with third parties but does not want them to disclose it. This confidential information can be the pharmaceutical formulas of a pharmaceutical firm, beverage compositions of a beverage firm, list of customers of an e-commerce firm, or some other technical data.

A written NDA is a powerful legal tool stating that neither party will disclose any trade secrets, patents, or other proprietary information to anyone outside the company. A party can initiate legal action against the other for any violation of the documented agreement. The organization can sue for damages and compensation in the case of any violation. Many documents and other information regarding penetration testing contain critical information that could damage one or both parties if improperly disclosed. Therefore, the organizations must create NDA documents to protect sensitive information.

This agreement also covers the key aspects of negligence and liability for many potential issues. The organizations must be careful in wording the agreement because many testing firms would not want to attract legal consequences even in the case of negligence. Both parties bear the responsibility to protect tools, techniques, vulnerabilities, and information from disclosure beyond the terms specified by a written agreement.

The following points should be considered when drafting an NDA document:

- Determine truly valuable information that is important to the company. NDAs should clearly specify that the individual or organization signing the agreement should not disclose its contents.
- NDAs should clearly identify all parties to the agreement; it should specifically include the starting date and length of the nondisclosure period.
- All the parties involved in the NDA should have it reviewed by their respective legal advisors.

Specific areas to consider include the following:

- Ownership
- Use of evaluation reports
- Results and the use of the testing methodology in customer documentation

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

WHEREAS _____ agrees to review, examine, inspect or obtain such confidential information only for the purposes described above, and to otherwise hold such information confidential pursuant to the terms of this Agreement.

1. _____ agrees to hold confidential or proprietary information or trade secrets ("confidential information") in trust and confidence and agrees that it shall be used only for the contemplated purposes, shall not be used for any other purpose, or disclosed to any third party.

2. No copies will be made or retained of any written information or prototypes supplied without the permission of [YOUR NAME].

3. At the conclusion of any discussions, or upon demand by [YOUR NAME], all confidential information, including prototypes, written notes, photographs, sketches, models, memoranda or notes taken shall be returned to [YOUR NAME].

4. Confidential information shall not be disclosed to any employee, consultant or third party unless they agree to execute and be bound by the terms of this Agreement, and have been approved by [YOUR NAME].

5. This Agreement and its validity, construction and effect shall be governed by the laws of [insert jurisdiction].

AGREED AND ACCEPTED BY:

Date: _____

By _____ Witness: _____

Title: _____

Figure 2.13: Confidentiality and nondisclosure agreement

Preparing a Nondisclosure Agreement and Having the Client Sign

1 An NDA is an agreement that **contains confidential information**.

2 The lawyer should **vet the NDA form** before the client is asked to sign it.

3 The NDA should also be aimed at **protecting** the penetration tester's interests.

4 Include clauses highlighting the fact that the tester and their team will **not disclose any information** divulged by the client during the penetration test.

NDA helps in **creating a confidential relationship** between the pen tester and client to protect critical and confidential information or trade secrets.

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

Preparing a Nondisclosure Agreement and Having the Client Sign

The above figure shows a sample NDA. It helps in creating a confidential relationship between the penetration tester and the client to protect critical and confidential information or trade secrets. The following points should be considered after preparing an NDA:

- After preparing the NDA, have it checked by a lawyer before sending it to the client organization.
- Highlight critical words in the document such that neither the company nor the team will disclose information during the process of penetration testing.
- The main purpose of this agreement is to protect essential information.
- Ensure that the prepared document contains only legal information.
- This agreement is valid for a certain period, and both parties should follow the rules and regulations mentioned in the NDA.

Defining Liability Issues



Standards and penalties imposed by federal, state, or local governments 	Other noncontractual civil wrongs (torts) ranging from fraud, invasion of privacy, and conversion to deceptive trade practices and negligence 
Breach of contractual agreements 	Federal and state statutes that may impose criminal penalties as well as form the bases for private lawsuits 

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

Defining Liability Issues

While entering a service relationship, both parties should review their liability issues with respect to the outlined tasks:

- Standards and penalties imposed by federal, state, or local governments
- Other noncontractual civil wrongs (torts) ranging from fraud, invasion of privacy, and conversion to deceptive trade practices and negligence
- Breach of contractual agreements
- Federal and state statutes, which may impose criminal penalties as well as form the bases for private lawsuits

On many occasions, penetration testing leads to unexpected consequences, resulting in the malfunction of the target organization's systems, disruption of its services, and corruption of its information. In case of any such mishap, the testing firm should have a liability waiver, signed by the authorized personnel of the client organization, stating that the it cannot be held responsible for such consequences. To create a liability waiver, both parties must consult their legal advisors and provide appropriate authorization to standardize the agreement.

The following are some aspects a liability waiver should address:

- Damages to systems
- Denial of services
- Information corruption
- Mails to spoof and obtain passwords and account information

- Grounds for recourse and the maximum amount given for damages incurred
- Method of dispute resolution

A letter of authorization is necessary when an outside firm hosts the target organization's network. The testing team may even inadvertently access the networks of other companies hosted by that hosting company. In such a case, this letter would legally protect the testing firm.

A master services agreement is another agreement that serves as a warranty to both parties of the penetration test. It addresses issues such as changes in the work scope, pricing, testing tools, and time frame.

Applicable laws: Computer Fraud and Abuse Act 45

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(a)

Unauthorized attempts to upload information or change information on the websites are strictly prohibited and are subject to prosecution under **the Computer Fraud and Abuse Act** of 1986 and Title 18 U.S.C. Sec. 1001 and 1030+.

Those who knowingly access a computer without authorization or exceed the authorized limits, and by means of such conduct obtain information that has been determined by the **United States Government** pursuant to an Executive order to require protection against unauthorized disclosure for reasons of **national defense** or **foreign relations**, or any restricted data, as defined in paragraph y. of section 11 of the **Atomic Energy Act** of 1954 with the intent to believe that information obtained is used to the injury of the United States or to the advantage of any foreign nation

Unauthorized access in obtaining information contained in a financial record of a financial institution or of a card issuer as defined in section 1602(n) of title 15 defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

Unauthorized access of a computer of a **department** or **agency** of the United States that is for the use of the government of the United States, which affects government operation;

Unauthorized access, with intent to defraud, of a federal interest computer and by means of such conduct furthering the intended fraud and obtaining anything of value unless the object of the fraud and the thing obtained uses a computer;

Unauthorized access of a federal interest computer and by means of one or more instances of conduct **altering, damaging, or destroying** of information, thereby—(A) causing loss of a value aggregating \$1,000 during any one-year period; (B) modifying or impairing the medical examination, medical diagnosis, medical treatment, or **medical care** of individuals;

Unauthorized access to traffic, as defined in section 1029, in any password if—(A) such **trafficking** affects interstate or foreign commerce; (B) such a computer is used by or for the government of the United States; shall be punished as provided in subsection (c) of this section.

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(b)

Imprisonment for not more than **ten years or both**, in the case of an offense under subsection (a) (1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this **subparagraph**; and

Who attempts to commit an offense under subsection (a) of this section will be punished as provided in subsection (c) of this section.

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(c)

A fine under this title or imprisonment for not more than **five years or both**, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(d)

The **United States Secret Service**, in addition to any other agency having such authority, has the authority to investigate offenses under this section. Such authority of the United States Secret Service is exercised in accordance with an agreement, which shall be entered by the Secretary of the Treasury and the Attorney General

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(e)

As used in this section—

1) The term "**computer**" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device

2) The term "**Federal interest computer**" means a computer-- (A) exclusively for the use of a financial institution or the United States Government, and the conduct constituting the offense affects the use of the financial institution operation or the Government's operation of such computer

3) The term "**State**" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States; (4) the term "**financial institution**" means—(A) an institution with deposits insured by the Federal Deposit Insurance Corporation; (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank; (C) a credit union with accounts insured by the National Credit Union Administration

4) The term "**financial institution**" means—

The institution with deposits that are insured by the Federal Deposit Insurance Corporation.

A credit union with accounts insured by the National Credit Union Administration.

(5) The term "**financial record**" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution.

(6) The term "**exceeds authorized access**" means to access a computer authorization and access to obtain or alter information in the computer that the accessed is not entitled.

(7) The term "**department of the United States**" means the legislative or judicial branch of the government or one of the executive departments enumerated in section 101 of title 5.

Computer Fraud and Abuse Act 1986 (US) 18 USC 1030(f)

Lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a **political subdivision** of a State, or of an intelligence agency of the United States are not prohibited.

Defining a Negligence Claim



A negligence claim of liability is based on a **charge that the company** and its officers and directors acted “negligently.”



In law, “negligence” arises when a party owes a legal duty to another and that duty is breached. The breach results in damages to the **injured party** when, for example, a company is required to protect a customer database with reasonable measures.



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

Defining a Negligence Claim

In law, negligence arises when a company breaches a legal duty that it owes to another company, also called the client, and the breach causes damage. The breach results in damages to the injured party when, for example, a company is required to protect a customer database with reasonable measures. A negligence claim of liability is based on a charge that the company, its officers, and directors acted negligently.

In penetration testing, the testing firm is negligent if it fails to exercise the minimum required protective measures or care toward the target organization’s electronic information systems and other assets. If the testing team fails to exert the minimum effort that any reasonable and responsible service provider would have under such circumstances, it is negligent. In such a case, any lawsuit filed against the testing firm to claim damages would be a negligence claim.

The petitioner of a negligence claim should include four important elements:

- **Duty of care**

In this element, the petitioner should be able to prove that the testing firm did not perform necessary actions such as informing the petitioner in time that such damage might occur, which any other responsible service provider might have done.

- **Breach of duty**

In this element, the petitioner can claim that the testing team did not perform remedial action, which any other professional would have performed to mitigate the damage to some extent.

- **Casual occurrence**

The target organization should be able to prove that the damage incurred is not due to any casual coincidence or mishap.

- **Actual loss incurred**

In this element, the petitioner should be able to prove that the actual loss incurred by them is due to the negligence of the testing firm.

The licensed penetration test firm can defend themselves from negligence claims. The firm's defense should be based on the following four elements in the negligence claim:

- They can challenge the petitioner's claim and the duty of care clause.
- They can defend themselves by noting that they acted upon the incident or damage with the appropriate amount of responsibility.
- They can defend themselves by proving that the damage incurred was casual and not due to their negligence.
- They can question whether the plaintiff suffered any actual loss.

Defining Contract Limitations



- The contract should be **confidential** between the parties.



- Information, terms, and fees in the contract should **not be released** by either party.



- The service provider can **employ a team of experts** to test various security aspects.



- Without prior written approval, the provider should **not release** the client's information to third parties.



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

Defining Contract Limitations

The penetration testing contract is between the client and penetration test provider. Both parties should maintain the contract as confidential. Neither party should release information about this contract, contract terms, and the fees. Without any prior written consent, no party should release information about the client's confidential matters, business, or security systems to third parties.

Without the client's prior written approval, the provider may subcontract its obligations to third parties. The provider may employ a team of experts to test various security issues, and all those subcontractors must abide by the terms and conditions of the contract. Both parties agree to use the confidential information for the service and not disclose it to another third party. Every contract is subject to the laws of the state government. Neither the provider nor the contractor is liable for any accidental act of God, fire, strike, war, or other situation beyond the reasonable control of either party.

Having the Engagement Letter Vetted by a Lawyer



- After obtaining the legal document from the client organization, **study** it with the help of a lawyer.
- Based on the documentation provided by the organization, **prepare a penetration testing document and have the appointed lawyer check it.**
- This document contains information related to the **legal aspects of testing** and the scope of the project.

Pen Test Engagement Letter

Dec 20, 2014
ABC Financial Services,
Albuquerque, NM 52200

Dear,

This letter agreement, if acceptable to and countersigned by you, will serve as the agreement ("Agreement") between ABC-COM (ABC Financial Services) and PPT Security Solutions ("PPT") governing PPT's conduct of the Pen Test ("Pen Test") required by the "Pen Test Section" of this Engagement Letter. The effective date of the Agreement (the "Effective Date") will be the date on which this letter agreement is executed by ABC Financial Services, PPT and ABC Financial Services are each referred to herein as a "Party" and collectively, the "Parties."

1. BACKGROUND

The ABC Financial Services board requires, within 45 days of the date of the respective board meeting, to retain an independent consultant to conduct an independent security review of all ABC Financial Services information systems. The review is to include a comprehensive vulnerability and risk assessment, security posture assessment, and assessment of security controls implemented across ABC Financial Services information systems. The Agreement, together with its attachments, constitutes that engagement letter.

2. ORGANIZATION OF THIS AGREEMENT

Section 3 of this document sets forth the scope of pen testing services, section 4 sets the proposed services, section 5 prescribes the timing of pen testing services, section 6 defines reporting requirements and section 7 sets forth the terms and conditions for this pen test assignment.

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

Having the Engagement Letter Vetted by a Lawyer

The engagement letter (EL) is a document authorizing the penetration testing provider to conduct an engagement for the testing organization. It consists of the required updates, plan to conduct the project, schedule, and various portions of the work.

It is always recommended to consult a lawyer and discuss the legal points mentioned in the EL. Based on the documentation given by the client organization, the testing provider should prepare a penetration testing document and check it with the lawyer they appointed. This document contains information related to the legal aspects of testing and the scope of the project. Having a clear understanding of the legal aspects helps the tester exercise caution while dealing with the sensitive aspects of the test.

The following figure shows a sample penetration test EL.

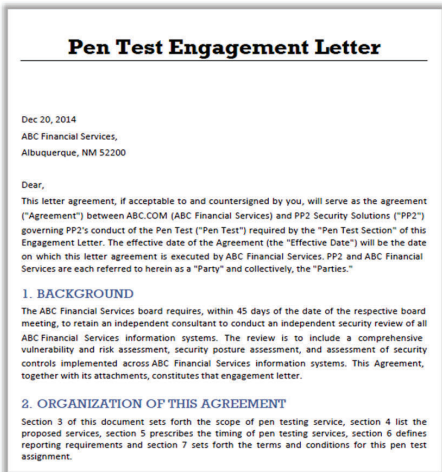


Figure 2.14: Sample penetration test engagement letter

Obtaining Liability Insurance from a Local Insurance Firm



- If possible, the pen tester should obtain **liability insurance** from an insurance company to **protect their interests** in case the client organization files a lawsuit against them for bringing their network down during the penetration testing.



- The insurance will **protect against the risks** that may exist, directly or indirectly, from the organization.



- It is suggested to **take third-party insurance** that covers all losses.



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

Obtaining Liability Insurance from a Local Insurance Firm

The pen tester should attempt to obtain liability insurance from a local insurance company to protect their interests if the client organization files a lawsuit or case against them for bringing their network down or causing a computer system crash during the process of penetration testing.

The insurance protects against direct or indirect risks from the client organization. The third-party insurance should preferably cover all the losses incurred by the tester and the client organization.

Independence Check of Team Members



- Compose an email to all members asking if anyone has a direct or indirect **financial interest** in the client the team is preparing to engage with.



- Delete all emails concerning **independence**; check the inbox, sent items, and other client email folders used.



- Use "**privacy software**" to wipe the free space on the local hard drives of the hosts used.



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

Independence Check of Team Members

The independence of an individual is a state of mind of keeping their professional judgement independent of any financial or other influences of personal gain. Simply put, it is the state of mind of an individual who correctly performs all professional duties without breaking the company's rules under any circumstances.

Before implementing a penetration test, the tester needs to analyze the independence of the client company's staff. To do so, the penetration tester implements the following steps:

- Step 1:** Initially, the penetration tester sends an email to the staff as a third party, offering them some amount (say \$15) to perform an action that is against the company's laws.
- Step 2:** Next, the penetration tester analyzes the replies from the employees and organize them.
- Step 3:** In this step, the penetration tester identifies the emails that are against the independence.
- Step 4:** Finally, the penetration tester gathers the employee IDs based on the email addresses and reports to the firm.

After the independence check, the penetration tester should delete all emails concerning the independence; to do this, they must check the inbox, sent items, and other email client folders used. "Privacy software" should be used to wipe the free space on the local hard drives of the hosts used.

Listing Known Waivers/Exemptions



1

A waiver is a **voluntary relinquishment** or surrender of some known right or privilege.

2

While a waiver is often in writing, a **person's actions** can occasionally act as a waiver.

3

An example of a written waiver is a **disclaimer**, which becomes a waiver when accepted.

4

Waivers are also called **exculpatory clauses**, releases, or hold harmless clauses.

5

Sometimes, the elements "voluntary" and "known" are established by a **legal fiction**.

6

In this case, it is presumed that one knows their rights and that those rights are **voluntarily relinquished** if they are not asserted at the time.

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

Listing Known Waivers/Exemptions

A waiver is the voluntary relinquishment or surrender of some known right or privilege by an organization. While a waiver is often in writing, in individual's actions can occasionally act as a waiver. An example of a written waiver is a disclaimer, which becomes a waiver when accepted. Waivers are also called exculpatory clauses, releases, or harmless clauses.

Sometimes, the elements "voluntary" and "known" are established by a legal fiction. In this case, it is presumed that an individual knows their rights and that those rights are voluntarily relinquished if they are not asserted at the time.

The penetration tester must list all the actions that the organization has waived or exempted from legal issues and define them.

Listing Contractual Constraints in the Penetration Testing Agreement



- Check for **service-level agreements** in the project that may affect the scope of the test.



- Accept a **waiver** or **privilege letter** from the contractual partners to perform this testing.



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

Listing Contractual Constraints in the Penetration Testing Agreement

Penetration testing involves risk. Both parties must agree and sign documents defining the scope of the test. Further, both parties must sign an NDA. The penetration tester should check for service-level agreements in the project that may affect the scope of the test.

The penetration tester should accept a waiver or privilege letter from the contractual partners before performing the testing. Legal issues in a penetration test include the following:

- Issues that can provoke or trigger a business or public authority
- Rules and principles both parties must follow, which are defined prior to the test
- Legal aspects that are the basis of the contractual agreement



Preparing for the Test

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

Preparing for the Test

This section discusses the creation of an engagement log, kickoff meeting, construction of a penetration test plan, penetration testing hardware/software requirements, and so on.

Reviewing the Engagement Letter



- 1 Reviewing the EL helps the team members **set up folders** to store the engagement data.
- 2 The EL is reviewed by the **engagement team leader (ETL)** to determine the services provided to the client.
- 3 The ETL **creates a system** to maintain the data gathered during the engagement process.
- 4 Every document in the engagement process must include the **name of the client**.

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

Reviewing the Engagement Letter

The EL is a document authorizing the penetration testing provider to conduct an engagement for the testing organization. It also includes the required updates, plan to conduct the project, schedule, and various portions of the work. The engagement team leader (ETL) reviews the EL to determine services that the team must provide to the client.

Reviewing the EL helps the team members set up a specified folder to store the data. The ETL or equally designated representative creates a system to maintain the data gathered during the process and makes initial modifications to the standard engagement project plan.

The ETL reviews the EL and removes the information necessary to perform certain tasks. Every document in the engagement process must include the name of the client and location. The EL specifies the ETL and the length of the engagement. As a second part, the ETL removes information on the expected duration and schedule of the test. The third item of importance is the “acceptance of proposed services.” It provides the ETL with details of the services they must provide to the client during the engagement. The ETL maintains control of the EL until the completion of the next task and then scans the EL into an electronic format.

Creating an Engagement Log



- Create an **engagement log** document and record all important activities concerning the engagement in this log file until the **engagement ends**.



- Keep all the engagement documents in a **folder**.



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

Creating an Engagement Log

The penetration tester must create an engagement log document and record all important activities concerning the engagement in this log file until the engagement ends. All engagement documents should be kept in a folder.

The list of network segments to test must be provided to the tester for ensuring that they have a clear view. Furthermore, a network diagram illustrating all the network segments should be provided. It includes the following:

- Dataflow diagram on sensitive authentication data or cardholder data
- List of all exposed ports and expected services
- List of all authorized users along with the privileges of each user to access the sensitive data

This information helps the penetration tester identify the vulnerabilities associated with the target.

Kickoff Meeting



- **First meeting** between the project team and client



Primary Goals

- Outlining the project goals and team members' responsibilities
- Providing information related to the project plan, methodologies, and processes
- Clarifying the expectations of the parties

Attendees

- Executive sponsor
- Key stakeholders involved in the testing
- Tiger team conducting the assessment

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

Kickoff Meeting

A kickoff meeting officially marks the start of the implementation phase of the project. The client holds this meeting in the initial stages of the project after the groundwork for the project is completed. The hardware and software resources required for the project; the development team; and the project layout and design, documentation template, and cost limits and deadlines must all be ready prior to this meeting.

The following are some steps in the preparation of the kickoff meeting:

- Define the project goals, deliverables, and project plan.
- Build a proper project team and assign tasks to the team members.
- Create a team contact list including the name, location, contact number, and email address of each member.
- Prioritize the tasks assigned to the team members and ensure that each member is committed to the success of the project.
- The project plan should be developed such that it helps validate the resources, identify risks, and determine timelines to complete the project.
- Each project team member must know the key success factors for a successful project.
- Communicate to each participant a preferred date and time to conduct the kickoff meeting and send all the materials related to the kickoff meeting including the project agenda, plan draft, and contact information.
- Review the project plan before the kickoff meeting and identify key issues.

The following are the primary goals of the kickoff meeting:

- Outlining the project goals and team members' responsibilities
- Providing information related to project plan, methodologies, and process
- Clarifying the expectations of the parties involved

This meeting should include the following participants:

- **Executive sponsor**

The client is the executive sponsor of the project, and the meeting cannot be conducted without the client. Any doubts can be clarified even at the last moment.

- **Key stakeholders involved in the testing**

This team involves all the key players involved in penetration testing and includes the managers, clients, CEO, and all those who are directly involved in the project.

- **Tiger team conducting the assessment**

The most important element is the tiger team that conducts the assessments and takes the responsibility of testing.

Preparing a Statement of Work



- 1 Penetration testing and other assessment services are based on a **statement of work (SOW)** created by the penetration tester for the client.
- 2 The SOW serves as a **contractual document** signed by the client that authorizes the work to be performed.
- 3 The SOW defines the **test objectives**, the **actions to be performed**, and how the penetration tester and their representatives will interact with the customer.
- 4 The SOW also **defines deliverables** and sets limitations on the penetration tester's liability.
- 5 The penetration tester should understand that there is a **significant risk** to the customer's network and delineate that risk within the SOW.
- 6 In short, the SOW provides **ROE** for the penetration testing service.

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

Preparing a Statement of Work

Penetration testing and other assessment services are based on a statement of work (SOW) created by the penetration tester for the client. The SOW serves as a contractual document signed by the client that authorizes the work to be performed. It is a formal document that captures and defines the work activities, deliverables, and timeline, which the penetration tester will execute as part of the specified work for the client. The SOW includes detailed requirements and pricing, along with standard regulatory and governance terms and conditions. It defines the test's objectives, the actions to be performed, and how the penetration tester and their representatives will interact with the client. The penetration tester should understand that there is a significant risk to the client's network and should delineate that risk within the SOW. In short, the SOW provides ROE for the penetration testing service.

The areas addressed by a SOW are as follows.

- **Purpose:** The purpose statement clarifies why the project is being undertaken.
- **Scope of work:** This describes the work in detail, specifies the hardware and software involved, clarifies the exact nature of the work.
- **Work:** This describes the work location as well as the location of hardware and software and where people will meet to perform the work.
- **Period of performance:** This specifies the allowable time for projects such as the start and finish times, the number of hours billed per week or month, the location of work, and anything else that relates to scheduling.
- **Deliverables schedule:** This part lists the specific deliverables, describing what is due and when.

- **Applicable standards:** This describes any industry-specific standards that penetration testers need to adhere to while fulfilling the contract.
- **Acceptance criteria:** This specifies how the client will determine if the service is acceptable and what objective criteria will determine the work as acceptable.
- **Special requirements:** This specifies any special hardware or software, specialized workforce requirements such as degrees or certifications for personnel, travel requirements, and anything else not covered in the contract specifics.
- **Type of contract/payment schedule:** The project acceptance depends on whether the budget available will be sufficient for the work required. Therefore, at this stage, the parties negotiate the breakdown of payments and determine whether payments will be in advance or in a phased manner.
- **Miscellaneous:** Many items do not form a part of the main negotiations but are nonetheless important to the project. They may seem minor, but overlooking or forgetting them could cause problems for the project.

Identifying the Security Tools Required for the Penetration Test



Example:

Tool Category	Tool Names
Port Scanners	Nmap, NetScanTools Pro, SuperScan, MegaPing
Vulnerability Scanners	QualysGuard Vulnerability Management, Retina Network Security Scanner, GFI LANGuard, SAINT Vulnerability Scanner, Microsoft Baseline Security Analyzer (MBSA)
Application Scanners	AppScan, Acunetix WVS, WebInspect
Firewall Tools	Firewall Builder, Firewall Security Manager
Sniffers	Wireshark, tcpdump, WinDump, Capsa Network Analyzer
Tunneling Tools	Super Network Tunnel, HTTP Tunnel, HTTPort, HTTPHost

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

Identifying the Security Tools Required for the Penetration Test

The following table lists the security tools needed for penetration testing.

Tool Category	Tool Names
Port scanners	Nmap, NetScanTools Pro, SuperScan, MegaPing
Vulnerability scanners	QualysGuard Vulnerability Management, Retina Network Security Scanner, GFI LANGuard, SAINT Vulnerability Scanner, Microsoft Baseline Security Analyzer (MBSA)
Application scanners	AppScan, Acunetix WVS, WebInspect
Firewall tools	Firewall Builder, Firewall Security Manager
Sniffers	Wireshark, tcpdump, WinDump, Capsa Network Analyzer
Tunneling tools	Super Network Tunnel, HTTP Tunnel, HTTPort, HTTPHost

Table 2.8: Security tools for penetration testing

Identifying Hardware and Software Configurations Required for the Penetration Test

Ideal Hardware Configuration

- Processor running at 2 GHz or higher
- 8 GB RAM
- 500 GB storage capacity
- 1 network interface card



Ideal Software Configuration

- IIS server
- Application servers
- MS Office 2016
- OSes: Windows Server 2012, Windows 10, Linux, and Macintosh OS X



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

Identifying Hardware and Software Configurations Required for the Penetration Test

The penetration tester should choose a system with high specifications as it would yield good results and complete the project in relatively less time. The configurations mentioned below are mainly for laptops as most organizations use laptops as personal computers.

- The ideal hardware configuration should contain the following:
 - A 64-bit Intel® Core™ processor, the most secure processor series in the present generation, running at a frequency higher than 2 GHz and having power-saving features
 - At least 8 GB RAM with a hard disk storage capacity of 500 GB
 - One network interface card
- Software plays a key role in any system. The ideal software configuration includes the following:
 - Servers such as an IIS server, an application server, and a database server to store records
 - Windows Server/Windows 10/MacOS/Linux, which are the most secure and convenient OSes

For report writing, penetration testers must have MS Office 2019, which is the latest and has special features for design and implementation.

Preparing the Test Plan



- A project plan is a **crucial part** of project management.
- It **defines** the project, specifies goals and objectives, deadlines, resources required, approach, success factors, assumptions, and financial aspects.
- A **well-developed project plan** is said to be **half** of the **actual task**.



Test Plan Overview	
Company Name	
Project Title	
Authority Name	
Date	
Test Plan Created by	
Scope	
Description	

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

Preparing the Test Plan

A project plan is a crucial part of project management. A penetration test plan is a part of an overall security plan and sets the ground rules of the test. It is vital to set appropriate ground rules for the test. It defines the project, goals and objectives, deadlines, resources required, approach of the project, success factors, assumptions, and financial aspects. A well-developed project plan is said to be half of the actual task.

The following table presents an overview of a test plan.

Test Plan Overview	
Company name	
Project title	
Authority name	
Date	
Test plan created by	
Scope	
Description	

Table 2.9: Test plan overview

Other than basic details such as the company name, project title, authority name, date, creator of the test plan, and scope of the test, the test ground rules established in the penetration test plan are

- Product configuration
- Environment to conduct the testing process
- Resources to perform penetration testing
- Product agenda

Test Plan



- A test plan is a document that **details the structure** of procedures for a penetration test.
- A test plan can be structured according to an **industry standard** or an internal template.
- A penetration test plan **establishes the ground rules**, limits, and scope of testing.
- It enhances the probability of achieving **favorable results** from a penetration test.

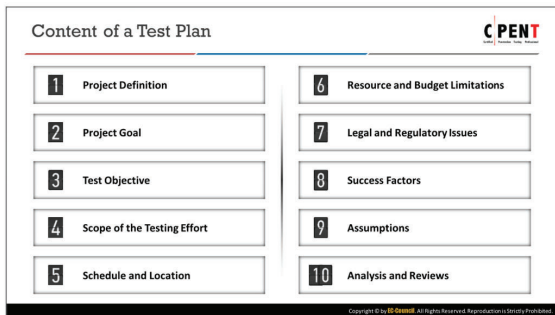
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test Plan

A test plan is a document that details the structure of procedures for a penetration test. It is structured according to an industry standard such as the Institute of Electrical and Electronics Engineers (IEEE) Standard for Software Documentation—Std. 829 or an internal template. The IEEE Standards Association is an organization with members working voluntarily to develop standards for various products. The IEEE defines the standards required for testing various applications. The contents of the IEEE standards are updated over time, and its requirements change.

A penetration test plan establishes the ground rules, limits, and scope of testing. It enhances the probability of achieving favorable results from a penetration test. The following are two types of test plans:

- **Master test plan:** The test lead prepares the master test plan, which depends on the functional specification.
- **Detailed test plan:** The test analyst prepares the detailed test plan, which consists of the main content.



Content of a Test Plan

The test plan must include the following content:

- **Project definition:** The test plan must define the penetration test project.
- **Project goal:** It must provide the details of penetration test goals.
- **Test objective:** It must specify the objectives that each penetration tester must accomplish as part of the project.
- **Scope of the testing effort:** The test plan must determine the scope of the penetration testing process.
- **Schedule and location:** It must provide information about the schedule of test and location at which the team would work.
- **Resource and budget limitations:** It should stipulate the resources and budget required to perform the test process.
- **Legal and regulatory issues:** The plan should define all the legal and regulatory issues that can arise during the process and explain the methods of reducing and handling them.
- **Success factors:** It should give a clear idea of factors that would represent the success of each test.
- **Assumptions:** The plan must explain the assumptions the penetration tester can make on hitting a roadblock or when they are unable to move forward with the test.
- **Analysis and reviews:** It should include an analysis of the penetration test process and periodic reviews on the test process.
- **Change controls, communication, and coordination of key activities:** It should mention the change controls, communication, and key activities in the penetration test process.

Building a Penetration Test Plan



- 1 Set up a test goal
- 2 Define the objects to be tested
- 3 Hire a skilled penetrator
- 4 Bind the penetration analysis resources



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

Building a Penetration Test Plan

Source: <https://www.nasa.gov>

To set appropriate test ground rules, one needs to build a good penetration test plan.

The four major requirements to build a test plan are as follows.

- **Set up a test goal**

The most important goal of penetration testing is to focus on developing adequate evidence of flawlessness and to reach a security assurance level. Other goals include the following:

- Security assurance
- System design research
- Systems training

It is essential to achieve the following goals for a successful penetration test:

- Define the number of errors or flaws present in the system.
- Determine the level set of the penetration test time.
- Use unauthorized means to access dummy target objects.
- Violate and change the security policy.
- Determine the proper usage of resources and money.

Multiple independent penetration testing teams employ some systems to improve the confidence level. Most penetration test processes mainly focus on the design,

implementation, and operational integrity of security parameters to control flaws in the security interface.

- **Define the objects to be tested**

The penetration testing process should be performed in systems that require Trusted Computer Security Evaluation Criteria (TCSEC). Systems with these kinds of evaluation classes are not designed to avoid hostile attacks and penetration. Thus, this kind of attack always exposes vulnerabilities.

A system designed to perform TCSEC evaluation at a high level comes with documentation and a collection of material to support the security claim. The collected security evidence characterizes the penetration testing of a security system. Penetration testing should be performed on a separate copy of the target of evaluation to ensure noninterference with the actual users.

- **Hire a skilled penetrator/bind the penetration analysis resources**

The penetration testing team should have well-qualified professionals. The testing organization should strive to hire certified professionals with relevant experience.

Penetration analysis looks for flaws present in a system without any limitations. The major resource for penetration analysis is the penetration testing team. This team should have adequate knowledge about the target system and spend time collecting security evidence related to the target system. The team should spend a majority of this time in gathering resources (such as security evidence). The team should access various tools such as the following:

- Compilers
- Editors
- Configuration management systems
- Word processors
- Database management systems

Test Plan Identifier



- Each test plan should be **assigned an identifier** that is **unique** in the organization.
- Summarize** the software items and features to be tested.



- References to the following documents are required when developing the highest-level test plan:

- Project authorization
- Quality assurance and project plan
- Configuration management plan
- Relevant policies
- Relevant standards



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

Test Plan Identifier

The penetration tester must assign a unique identifier to each test plan in the organization and summarize the software items and features to be tested. The test plan identifier specifies the scope and purpose, along with the needed resources, activities involved, and scheduling. It identifies the areas that require checking and the team to perform the testing. The test planner should carefully select the required team to ensure the quality of work. The team should be provided the required training if necessary. The test planner should also address various aspects of the project such as the agreement of the project, legal and financial issues involved, time constraints, and any liabilities that may eventually arise. There are various levels in the process of testing.

The planner must include references to the following documents when developing the highest-level test plan:

- Project authorization
- Quality assurance and project plan
- Configuration management plan
- Relevant policies
- Relevant standards

XSECURITY: Test Plan Checklist



Test Identifier	YES	NO
Is the scope of the project defined?		
Are all the test items defined?		
Are the items that are not to be tested identified?		
Are the change control items identified and the members of the change control board (CCB) defined?		
Are the features to be tested identified?		
Are the features that are not to be tested identified?		
Is the test strategy identified and documented?		
Are the test criteria for security testing documented?		
Are the entry criteria defined and documented?		
Are the exit criteria defined and documented?		
Is the list of deliverables documented?		
Is the test environment researched and documented?		

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

XSECURITY: Test Plan Checklist (Cont'd)



TEST PLAN CHECKLIST

DATE: _____

PROJECT NAME: _____ PREPARED BY: _____

1. TEST DESCRIPTION

2. TEST OBJECTIVES

3. TESTING METHODS

☐ Automated Testing
 ☐ Stress Testing
☐ Manual Testing
 ☐ Regression Testing
☐ Compatibility Testing
 ☐ Workflow Testing
☐ Integration Testing
 ☐ Ad-Hoc Testing

4. OTHER TESTING METHODS

5. TEST DELIVERABLES

☐ Test Plan
 ☐ Test Specifications
 ☐ Test Script

Completion Date: _____
 Completion Date: _____
 Completion Date: _____

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

XSECURITY: Test Plan Checklist

Test Identifier	Yes	No
Is the scope of the project defined?		
Are all the test items defined?		

Are the items that are not to be tested identified?		
Are the change control items identified and the members of the change control board (CCB) defined?		
Are the features to be tested identified?		
Are the features that are not to be tested identified?		
Is the test strategy identified and documented?		
Are the test criteria for security testing documented?		
Are the entry criteria defined and documented?		
Are the exit criteria defined and documented?		
Is the list of deliverables documented?		
Is the test environment researched and documented?		

Table 2.10: Test plan checklist

The above table presents a sample test plan checklist of XSECURITY, where each test identified is analyzed and the corresponding result (Yes or No) is recorded. The maximum number of checks in the “Yes” tuple indicates a successful penetration test.

As shown in the figure, XSECURITY’s test plan checklist document contains the project name and the name of penetration tester who prepared it. The following are the other fields included in this document:

- Test description
- Test objectives
- Testing methods
- Other testing methods
- Test deliverables

TEST PLAN CHECKLIST	
DATE: _____	
PROJECT NAME: _____ PREPARED BY: _____	
1. TEST DESCRIPTION	
2. TEST OBJECTIVES	
3. TESTING METHODS	
☐ Automated Testing	☐ Stress Testing
☐ Manual Testing	☐ Regression Testing
☐ Compatibility Testing	☐ Workflow Testing
☐ Integration Testing	☐ Ad-Hoc Testing
4. OTHER TESTING METHODS	
5. TEST DELIVERABLES	
☐ Test Plan	Completion Date: _____
☐ Test Specifications	Completion Date: _____
☐ Test Script	Completion Date: _____

Figure 2.15: Test plan checklist

Penetration Testing Hardware/Software Requirements

Laptop

- Windows 10 and Windows Server 2019
- Linux OS
- Wireless access points
- Wireless cards
- A huge hard disk (preferably 1 TB)



Devices

- Keyloggers
- Jamming devices
- Radio communication interceptors
- Telephone spying devices
- Wireless antennas



Software

- Hacking tools
- Sniffing devices
- Penetration testing tools
- Vulnerability assessment tools



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

Penetration Testing Hardware/Software Requirements

Penetration testing, like any other project, requires certain hardware and software resources. The basic hardware required for conducting penetration testing is a laptop or a computer.

The following should be installed in the computer:

- Windows 10 and Windows Server 2019
- Linux OS
- Wireless access points
- Wireless cards
- A huge hard disk with a capacity of preferably 1 TB
- Keyloggers
- Jamming devices
- Radio communication interceptors
- Telephone spying devices
- Wireless antennas

The following are some software resources required for penetration testing:

- Hacking tools
- Sniffing devices
- Penetration testing tools
- Vulnerability assessment tools

Assign Resources



■ **Break the project task** into small tasks.

■ **Select the resources** for each task.

■ **Assign resources** (equipment and personnel) to project tasks.

■ **Brief the personnel on the task** and provide hardware/software tools if required.



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

Assigning Resources

Penetration testers must break the project into smaller parts and distribute them among the team members. This will help the team members understand the goals better and focus on the assigned task. This will also reduce confusion as to which task they must perform first.

Penetration testers must select the resources, including software and hardware equipment, as well as the personnel required and assign them to the project tasks. The personnel should be provided with proper guidelines regarding the usage of resources. They must be briefed on the process they must follow to complete their tasks; additionally, information about the hardware/software tools can be provided if required.

Sending Internal Control Questionnaires to the Client



- 1 During the initial call with the client, the ETL determines which **OSes other than Microsoft Windows are in use at the client facility.**
- 2 This information is used to determine which **internal control questionnaires (ICQs)** are sent to the client.
- 3 An archive containing the ICQ is sent to the client as part of the **"advance packet"** discussed later.

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

Sending Internal Control Questionnaires to the Client

An internal control is a group of policies and procedures a firm creates, follows, and maintains for effectively handling all its business operations. The main purpose of the internal control is to help the company in achieving its key objectives.

An internal control questionnaire (ICQ) allows the penetration tester to evaluate the internal control of the firm by asking questions on the company's key objectives/goals. Consequently, the tester can obtain what is known as provided-by-client (PBC) information. Some companies provide ICQs with other tools such as flowcharts and documentation, in addition to reports of the organization's internal control. Before implementing the penetration test, the ETL must determine the OSes used in the company. They must determine if there are any OSes in use at client facilities other than Microsoft Windows. An ICQ must be prepared based on the outcomes and sent to the client organization, which helps in evaluating the internal control of the firm. An archive containing the ICQ is sent to the client as part of the "advance packet."

Requesting for Previous Penetration Testing/Vulnerability Assessment Reports



1

Organizations **retain a copy of penetration testing reports** for future reference.



2

Request for **previous penetration testing reports** of the client organization to attain a clear understanding of the problems that existed in the past.



3

Most organizations will not be willing to share their previous penetration test reports.



TRY YOUR LUCK!

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

Requesting for Previous Penetration Testing/Vulnerability Assessment Reports

Organizations retain a copy of penetration testing reports for future reference. The penetration tester can request for the client organization's previous penetration testing report to gain a clear understanding of the problems that existed in the past. The main reason for gathering the previous report is to get an idea of the level of vulnerabilities, threats, or attacks that occurred.

- If the organization provides the report, the penetration tester should check for the following:
 - Compliance of the test
 - Reasons to perform the test
 - Entity that performed the previous penetration test
 - Time of conducting the test

Most organizations will not be willing to share their previous penetration test reports.

Creating a Data Use Agreement



- A data use agreement (DUA) governs the **disclosure** and **use of data** in the nationwide databases of the Healthcare Cost and Utilization Project (HCUP) of US Department of Health & Human Services.



- The DUA is normally required if the client is subject to the **Health Insurance Portability and Accountability Act (HIPAA) regulation**.



- HIPAA also affects **businesses, business associates, and contractors** in other countries who deal with US healthcare services.



- **Sign a separate DUA** for each team member assigned to work on an engagement.



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

Creating a Data Use Agreement

A data use agreement (DUA) governs the disclosure and use of data in the nationwide databases of the Healthcare Cost and Utilization Project (HCUP) of the US Department of Health & Human Services. Established by HCUP, DUA protects the most confidential data from unauthorized access. As HCUP handles large databases that store national-level healthcare data, privacy and protection have become their major concerns. These concerns made them establish a DUA, which restricts the availability of and access to their confidential data resources.

Before starting the penetration test, the HCUP's DUA must be signed by the clients if they follow the Health Insurance Portability and Accountability Act (HIPPA) regulation. HIPPA is a privacy rule that was enacted by the US government to protect confidential information, especially the medical details of patients. HIPAA also affects businesses, business associates, and contractors in other countries who deal with US healthcare services. A separate DUA should be signed for each team member assigned to work on an engagement.

Working Teleconference



- Conduct a working teleconference with the client and **ask if there are any questions** on the engagement documents such as the ICQ, ROE, and NDA. Answer as necessary.



- Ask if there are any questions on the initial **provided-by-client (PBC) list**.



- Determine a **date for delivery** of the final copies of the documentation.



- Determine the **final document delivery method**.



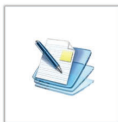
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Working Teleconference

The penetration tester must always conduct either audio or video conferencing with the client and ask if there are any questions on the engagement documents such as the ICQ, ROE, and NDA. The questions should be answered, as necessary. After going through all the agreements, the tester should list out the queries, discuss them with the clients, and give them a chance to raise queries on behalf of their organization. Ask if there are any questions on the initial PBC list.

Both parties must discuss and fix the final delivery date on the call so that the client organization can have that information for its records. The parties can also discuss various delivery-related points such as the delivery code, delivery method, and final delivery report.

Sending the Final Engagement Control Documents to the Client for Signature



On or before the delivery of the final documents to the client, assemble the final copies of **engagement control documents (ECD)**.

Send the final ECDs to the client for signature as modified during the **working teleconference**.

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

Sending the Final Engagement Control Documents to the Client for Signature

After completing the teleconference, the penetration tester must make the necessary changes to the documents (if required) and submit the final engagement control documents (ECDs) to the client. The documents should be easy to understand for the client company's management and information security personnel. A report that is too technical is of no use to the upper management. However, it should not be too simplistic either; otherwise, the information security personnel will be unable to properly implement the recommended changes. The final ECDs are sent to client for signature as modified during the working teleconference.

Obtaining the Penetration Testing Permission from the Company's Stakeholders



- 1 A penetration test can have **diverse effects on individuals**, such as system owners, network security engineers, database administrators, and stakeholders.


- 2 Before starting a penetration test, a pen tester or pen testing party needs to **identify all the individuals** who will be affected by the pen test.


- 3 A corporate stakeholder is a party **who affects or can be affected** by the company's actions.


- 4 The company's stakeholders must **provide permission** for the penetration test; request the client organization to **obtain permission** from the stakeholders to **avoid future litigations**.


- 5 Identifying stakeholders allows the pen tester to **know who needs to be informed** and **when they should** be contacted.


- 6 **Report and document** the **result**, and submit it to the stakeholder.



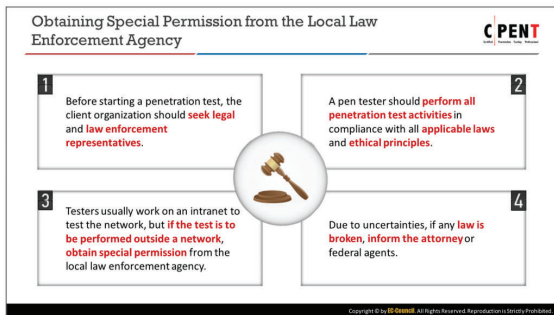
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Obtaining the Penetration Testing Permission from the Company's Stakeholders

Most companies have stakeholders who play a key role and are directly or indirectly involved in the functions of the organization. They can impact all the decisions in an organization, and all the actions performed in the organization affect them. Stakeholders can be employees, directors, government, shareholders, management, system owners, investors, network security engineers, database administrators, and the community.

Before starting a penetration test, a penetration tester or penetration testing party needs to identify all the individuals whom the test will impact. They must request the client organization to obtain permission from the stakeholders to avoid future litigations. Identifying stakeholders allows the penetration tester to know who they must inform and when they can contact them. The penetration tester can write one penetration test report but target numerous readers. For example, a tester can expect the senior management to read and understand the executive summary, while the IT team will read the technical details.

Even before conducting an audit on a web application or network security or any other form of security testing, penetration testers need to create a preliminary penetration test report that would help the planning. Identifying stakeholders allows the penetration tester to know the reporting authority, method, and time of contact. This also helps in creating customized reports to provide a better understanding. The tester reports and documents the result and submits it to the stakeholders.



Obtaining Special Permission from the Local Law Enforcement Agency

Before performing a penetration test, it is important for penetration testers to obtain permission from the people involved, including third parties if a company has outsourced or managed services as part of its IT infrastructure. A pen tester should perform all penetration test activities in compliance with all applicable laws and ethical principles.

This has made it increasingly important for penetration testers to have a clear understanding of who owns the systems they are targeting as well as infrastructure between the testing systems and the targets, which may be affected by the testing.

If a tester performs penetration tests across the Internet, they should notify the relevant ISPs, primarily their own ISP and the client's ISP. This is important for various reasons, including legal, informational, and technical.

Moreover, despite permissions and technical issues, it is important to have a clear understanding of the law, especially when more than one country is involved.

Testers usually work on an intranet to test the network, but if they must perform the test outside a network, then they must obtain special permission from the local law enforcement agency. The permission must be in writing, indicating the reasons, scope, and extent of the test. It must include the tools the penetration testers will use. The test results should be kept confidential and disclosed only to the law enforcement agency and the security administration department. Due to uncertainties, if any law is broken, the tester must inform an attorney or federal agents.

Obtaining Temporary Identification Cards from the Client for Team Members Involved in the Process



1

After being assigned a physical location to conduct the test process, **request the organization to provide a temporary identity card** to all the penetration testers.



2

Use this identity card as an access card to **enter the company's premises**.



3

Ensure that all the testers involved in the penetration testing at the client organization have a **unique identity** or access card.



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

Obtaining Temporary Identification Cards from the Client for Team Members Involved in the Process

After choosing the physical location at the client side, the team should request temporary identification cards for all testers who will be involved in the penetration testing process. The team members must use this access card to enter the client organization's premises. Each team member should receive their own identification card. These identification cards will help the testing team avoid problems with security guards, who usually work in shifts.

Gathering Information on the Client Organization's History and Background



1

Penetration testing assesses the **security model** of an organization.



2

Before starting the penetration testing for an organization, **gather some information** about that company.



3

Search in websites and **gather the history** and **background** of the client organization.



4

Use publicly available tools such as **search engines**, **Whois tools**, and specially crafted requests to gather information.



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

Gathering Information on the Client Organization's History and Background

Penetration testing is a process of assessing the security model of an organization. Before starting the penetration test, the tester should search the Internet and gather information on the history and background of the client organization. This can be done using various search engines, Whois tools, specially crafted requests, and so on. Usually, large organizations have official websites, which can be used as the main source of information. Some organizations release their details in newspapers or magazines that mention their growth and development. The main purpose of gathering information is to give the tester an idea about the company. The following history and background details can be helpful to the tester:

- Foundation of the company
- Objectives of the company
- Products released
- Assets of the organization
- Employee details
- Stakeholders
- Potential business partners
- Clients of the organization

Visiting and Becoming Familiar with the Client Organization's Premises and Environment



- 1** Visit the **premises** of the client organization for more information on its physical infrastructure.
- 2** Check for **facilities** such as car parking levels, restaurant, restroom, elevator, club, and swimming pool.
- 3** Get **acquainted with the organization's premises** to assess the physical security of the client organization.
- 4** Check the **work premises** where most of the employees utilize network equipment such as routers, switches, LAN, hub, and bus.
- 5** Choose a **location** near the network equipment room to perform the test process.

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

Visiting and Becoming Familiar with the Client Organization's Premises and Environment

The pen tester should visit the client organization's premises, including basic facilities such as parking areas and levels, restaurants, restrooms, elevators, clubs, and swimming pools. The entire physical infrastructure of the client organization should be checked. Visiting the premises provides an understanding of the physical security of the company.

The pen tester must make themselves acquainted with the organization's premises to assess the physical security of the client organization.

The tester should check the work premises where most of the employees use network equipment such as routers, switches, LAN, hubs, and bus. Further, they should examine the network equipment room where the routing setup is secured. Alternatively, they can check if the server room is different from the network equipment room. Moreover, the tester should inspect the area where the testing team will work, check whether the server and network rooms have sufficient security, and choose a location near the network equipment room to perform the test process.



Identifying the Local Equipment Required for the Pen Test

The list of local equipment required for performing the penetration testing process is as follows.

- Category 5 (CAT5) taps and speed
- Fiber taps/converter
- Internet access, which should allow the following:
 - Filtered Internet access
 - Unfiltered Internet access
 - Uploads/downloads
- Separate office-space allocation for the testing team
- Ethernet taps and speed
- 24-h power availability with generator facility
- Refreshments including access to the cafeteria, bakes, confectionaries, soft drinks, and so on

Mission Briefing



- The purpose of mission briefing is to give team members the maximum amount of time and **information to prepare for the mission** and perform any necessary equipment maintenance (hardware and software).

1

At the appointed time and date, assemble the members of the engagement team and orally brief them on the mission.



2

Ask for any questions about the contents of the briefing and answer them accordingly.



3

After the briefing, ensure that each team member clearly understands their part of the mission by asking for feedback from each member on their portion of the mission.



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

Mission Briefing

Mission briefing refers to the process of providing detailed information about the penetration test, scope, and goal to the team responsible for performing the tests. The purpose of mission briefing is to provide team members the maximum amount of time and information to prepare for the mission and perform any necessary equipment maintenance (hardware and software).

At the appointed time and date, the ETL should assemble the members of the engagement team and conduct the mission briefing orally. This must include the penetration test plan, hardware devices and software programs included in the scope, responsibilities of each tester, tools they can use, evidences they need to gather, and type and format of the output they must achieve.

The ETL must ask the team for any questions and doubts about the content of the briefing and answer them accordingly. After the briefing, the ETL ensures that each team member clearly understands their part of the mission by asking for feedback from each member on their portion of the mission.



Handling Scope Creeping During Pen Testing

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

Handling Scope Creeping During Pen Testing

This section discusses the process of handling scope creeping during a penetration test. It also provides information about the process of battling scope creeping.



"Scope Creeping: Don't let your penetration test land you in legal hot water."—Michael Kassner

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

"Scope Creeping: Don't let your penetration test land you in legal hot water."—
Michael Kassner



"Don't fall victim when client says, 'Forgotten to include that' in the statement of work. It's a serious trap."

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

"Don't fall victim when the client says, 'Forgotten to include that' in the statement of work. It's a serious trap."

Scope Creeping



- Scope creeping occurs when a client asks to include other tests in between, **beyond the scope** of the initial engagement.
- Scope creeping is common during **penetration testing** engagements.
- Scope creeping can **pose legal problems** and consume a significant part of the estimated time (scope) and resources.

Battling scope creep

- 1 Strive to help the client but ask for payment for any extra help.
- 2 If the client is ready to pay an extra amount for additional tests and legally allows additional time and resources in the pen test engagement, then the pen tester should happily agree to do the extra work.
- 3 If not, the tester should politely refuse.

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

Scope Creeping

Scope creeping is the process of adding new services or objectives to a project that has already been defined. Scope creeping is common during penetration testing engagement, and testers must be able to handle it carefully. It can also pose legal problems and consume a significant part of the estimated time (scope) and resources.

If a client likes penetration testers' work and asks them to take up some additional work, then they should take it as a compliment and analyze the requirement. Based on the requirement, the penetration tester can request for additional funds and extra time for completing the project. If the client refuses to pay the extra amount or offer more time, then there would be no sense in performing that work. In such cases, the penetration tester must reject the work politely.

On the other hand, if the client agrees to pay but expects a discount from the tester, then the penetration tester(s) should use the opportunity and take up the additional work as they can achieve repeat business without hunting for work and going through formal RFP processes. Note that the best source for any form of business is the existing customer; therefore, they should be treated well.

Module Summary



- ❑ The following points should be considered before proceeding to the actual penetration test:
 - The scope of the proposed penetration test should be clearly understood.
 - Both parties should clearly understand and agree on the established ROE and included clauses.
 - The penetration testing contract should be vetted by a lawyer before signing.
 - An SOW and a test plan should be prepared for the proposed penetration test.

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

Module Summary

Let us quickly recap the key steps discussed in this module:

- Gather basic information about the client's expectations from the penetration test based on the preliminary information request document
- Identify the type of testing to conduct: black- or white-box testing
- List the servers, workstations, desktops, and network devices to test
- Clearly understand the scope of the proposed penetration test
- Prepare a penetration testing contract
- Prepare a tiger team
- Review the signed EL
- Create ROE
- Prepare an SOW and a test plan
- Get the penetration testing contract vetted by a lawyer before signing it
- Send the final ECDs to the client for signature
- Conduct a mission briefing