

EHE

Ethical Hacking Essentials

Module 12

Penetration Testing Fundamentals

Module Objectives

- 1 Understanding Penetration Testing and its Benefits
- 2 Understanding Types of Penetration Testing
- 3 Understanding Phases of Penetration Testing
- 4 Overview of Penetration Testing Methodologies
- 5 Overview of Guidelines and Recommendations for Penetration Testing
- 6 Understanding Risks Associated with Penetration Testing



Module Flow

01

**Understand Fundamentals
of Penetration Testing and
its Benefits**

02

**Discuss Strategies and Phases
of Penetration Testing**

03

**Guidelines and Recommendations
for Penetration Testing**



PENETRATION TEST

What is Penetration Testing?

1

Penetration testing is a type of security testing that evaluates an **organization's ability** to protect its infrastructure such as network, applications, systems, and users against external as well as internal threats

2

It is an effective way of determining the efficacy of the organization's security policies, controls, and technologies

3

It involves the active evaluation of the security of the organization's infrastructure by **simulating an attack** similar to those performed by real attackers

Benefits of Conducting a Penetration Test



1

Reveal vulnerabilities

2

Show real risks

3

Ensure business continuity

4

Reducing client-end attacks

5

Establishing the status of the company in terms of security

6

Guard the reputation of the company

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing



Security Audit

- ❑ A security audit checks whether an organization follows a set of standard **security policies and procedures**



Vulnerability Assessment

- ❑ A vulnerability assessment focuses on **discovering the vulnerabilities in an information system** but provides no indication of whether the vulnerabilities can be exploited or of the amount of damage that may result from the successful exploitation of the vulnerabilities



Penetration Testing

- ❑ Penetration testing is a methodological approach to security assessment that **encompasses a security audit** and vulnerability assessment, and it demonstrates whether the vulnerabilities in a system can be successfully exploited by attackers

Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented

Goal-oriented/Objective-oriented Penetration Testing

- ❑ This type of assessments is **driven by goals**. The objectives of the penetration test are defined, rather than defining the scope of targets
- ❑ The goal of penetration assessment is defined before it begins
- ❑ The job of the pen tester to check whether he/she can **achieve the goal** and to determine the different ways to achieve the goal

Examples



Gain remote access to an internal network



Gain access to credit-card information



Deface a website



Gain domain administrator access



Create a denial of service (DoS) condition against a website

Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented (Cont'd)



Compliance-oriented Penetration Testing

- ❑ This type of assessments is driven by **compliance requirements**. It is testing against adherence to compliance requirements
- ❑ It entails conducting an assessment against the compliance requirements of cyber security standards, frameworks, laws, acts, etc.
- ❑ For example, an organization may ask to perform a security assessment against **PCI-DSS requirements**

Types of Penetration Assessment: Goal-oriented vs. Compliance-oriented vs. Red-team-oriented (Cont'd)

Red-team-based Penetration Testing

- ❑ Red-team-based penetration testing is an **adversarial goal-based assessment** in which the pen tester must mimic the behavior of a real attacker and target the environment
- ❑ This type of assessment has no specific driver
- ❑ For example, an organization may ask to conduct a security assessment for **evaluating its overall security**. It may include assessing people, networks, applications, physical security, etc.



Module Flow

01

**Understand Fundamentals
of Penetration Testing and
its Benefits**

02

**Discuss Strategies and Phases
of Penetration Testing**

03

**Guidelines and Recommendations
for Penetration Testing**

Strategies of Penetration Testing

Penetration testing strategies are broadly classified as follows:

Black box

White box

Gray box



- ❑ Each test strategy takes a **different approach** for assessing the security of an organization's infrastructure



Penetration Testing Process



Defining the Scope

- **Extent** of testing
- What will be tested
- Where testing will be performed from
- Who will perform testing



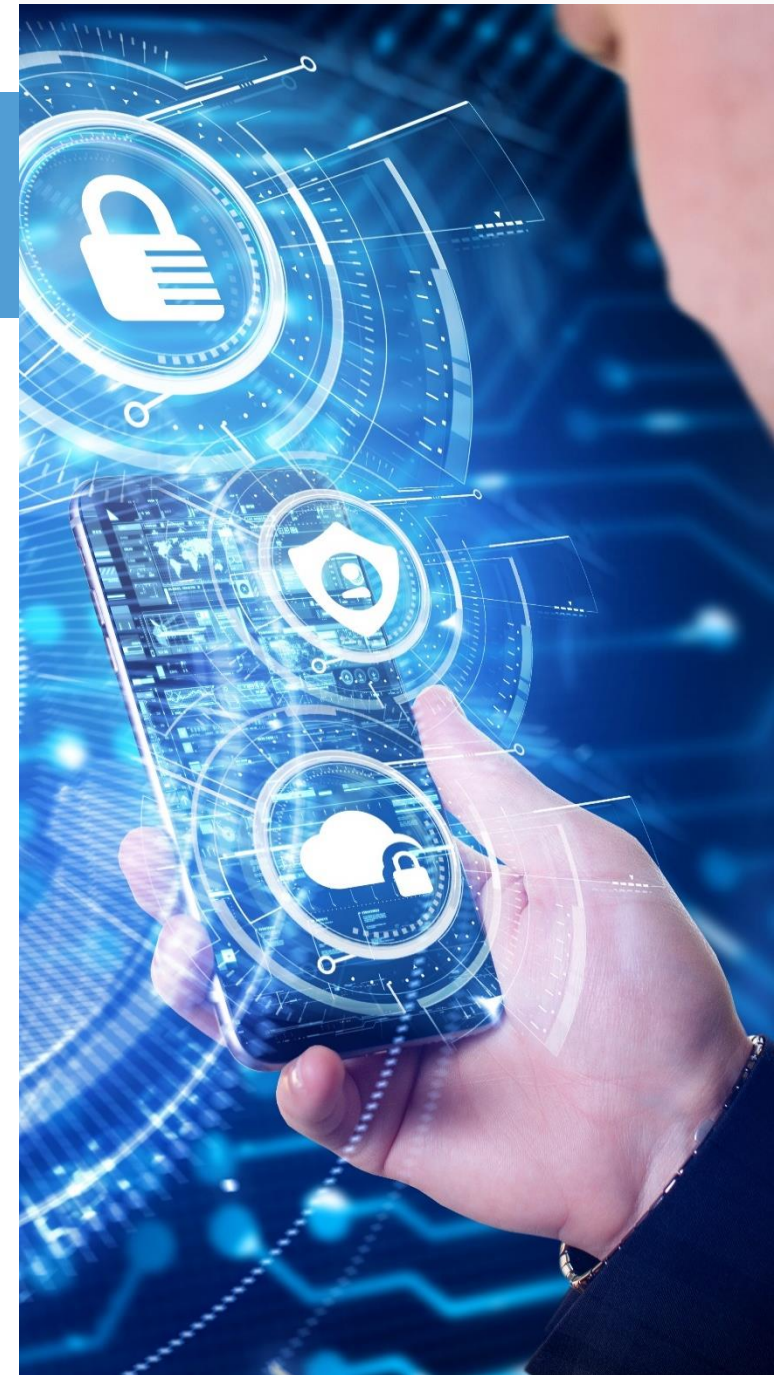
Performing the Penetration Test

- Involves **gathering all information** significant to security vulnerabilities
- Involves **testing the targeted environment** such as network configuration, topology, hardware, and software



Reporting and Delivering Results

- Listing **vulnerabilities**
- Categorizing risks as **high**, medium, or low
- Recommending repairs if vulnerabilities are found



Phases of Penetration Testing

01

Pre-Attack Phase

Research (Information Gathering)



02

Attack Phase

Testing/Exploitation



03

Post-Attack Phase

Documentation and Reporting



Penetration Testing Methodologies



Various penetration testing **frameworks** and **methodologies** exist to help organizations choose the best method to conduct a successful penetration test

Most commonly used methodologies:

Proprietary Methodologies

- 1 EC-Council's LPT
- 2 IBM
- 3 ISS
- 4 McAfee Foundstone



Open-source Methodologies

- 1 OSSTMM
- 2 ISSAF
- 3 NIST
- 4 OWASP
- 5 CREST

Module Flow

01

**Understand Fundamentals
of Penetration Testing and
its Benefits**

02

**Discuss Strategies and Phases
of Penetration Testing**

03

**Guidelines and Recommendations
for Penetration Testing**

Characteristics of a Good Penetration Test



Establishing the parameters of the penetration test such as **objectives**, limitations, and justification of procedures



Hiring skilled and experienced professionals to perform the test



Choosing a suitable set of **tests** that balance cost and benefits



Following a **methodology** with proper planning and documentation



Documenting the **result** carefully and making it comprehensible for the client



When should Pen Testing be Performed?

Pen testing is generally performed in the following cases:

01

Changes have been made in the organization's infrastructure



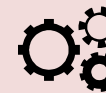
02

A **new threat** to the organization's infrastructure has been discovered



03

Hardware or software has been **updated** or **reinstalled**



04

The organization's **policy** has changed





Ethics of a Penetration Tester

- 01 Perform penetration testing with the express **written permission** of the client
- 02 Work according to the **non-disclosure** and liability clauses of a contract
- 03 Test tools in an isolated laboratory prior to an actual penetration test
- 04 Inform the client about any possible risks that might emanate from the tests
- 05 Notify the client at the first discovery of any highly vulnerable flaws
- 06 Deliver social engineering test results only in a summarized and statistical format
- 07 Try to maintain a **degree of separation** between the criminal hacker and the security professional

Evolving as a Penetration Tester

1

Technologies evolve and change

2

Look outside the workplace to expand knowledge

3

Attend **conferences**, **workshops**, and **training**

4

Join various security groups and discuss current security related topics

5

Keep your career alive by constantly updating your area of knowledge and skill set

6

Read books, journals, and trade magazines

7

Visit various security **websites** and **forums**

8

Visit **libraries** and **bookstores** to glean information

Qualification, Experience, Certifications, and Skills Required for a Pen Tester



- ❑ The quality of penetration testing depends on the **tester's qualifications**
- ❑ Penetration testing skills cannot be obtained without **years of experience** in IT fields such as development, systems administration, or consultancy
- ❑ The tester should possess security certifications such as CEH, CPENT, CISSP, and CISA

1

Networking – Transmission Control Protocol/Internet Protocol (TCP/IP) concepts and cabling techniques

2

Ethical Hacking techniques – exploits, hacking tools, etc.

3

Open source technologies – MySQL and Apache

4

Wireless protocols and devices – 802.11x and Bluetooth

5

Troubleshooting skills

6

Routers, firewalls, and intrusion detection systems (IDS)

7

Databases – Oracle and MSSQL

8

Operating system skills – Windows, Linux, Mainframe, and Mac

9

Web application architecture and Hypertext Transfer Protocol (HTTP) request and response concepts

10

Web servers, mail servers, Simple Network Management Protocol (SNMP) stations, access devices

Communication Skills of a Penetration Tester



A penetration tester should have strong **interpersonal** and **communication skills**



They must have a proven ability to explain the **output of a penetration test** to a nontechnical client



They must have good **presentation** and **report-writing skills**



Profile of a Good Penetration Tester

■ A good penetration tester's résumé should include any/all of the points listed below:



- Conducted research and development in security



- Published **research papers**



- Presented at various local and international seminars

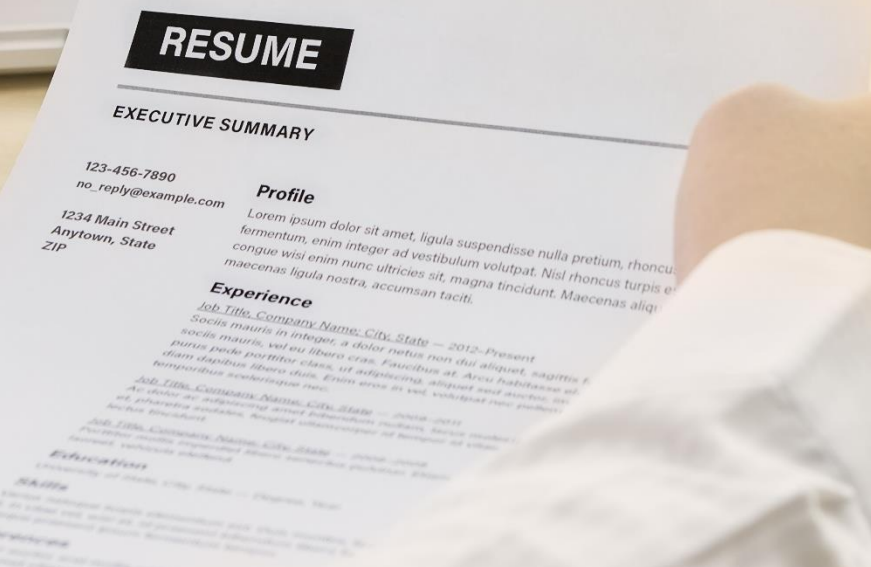


- Holds various **certifications**

- Member of reputed organizations such as **IEEE**

- Written and published **security-related books**

■ The tester needs to market themselves through these activities if they want organizations to consider them as a pen tester



Responsibilities of a Penetration Tester



Risks Associated with Penetration Testing

- ❑ Some of the risks arising from penetration testing are as follows:
 - ✓ Testers can gain access to **protected/sensitive data** after a successful penetration test attempt
 - ✓ Testers can obtain information about the **vulnerabilities** existing in the organizational infrastructure
 - ✓ DoS penetration tests can **take down** the organization's **services**
 - ✓ Using certain **pretexts in a social engineering** penetration attempt can make employees feel uneasy
- ❑ Organizations can avoid such risks by **signing a nondisclosure agreement (NDA)** and other legal documents, which include what is allowed and not allowed for the penetration testing team



Types of Risks Arising from Penetration Testing



Technical Risks

- ❑ This type of risks directly arises with targets in the production environment
- ❑ Examples:
 - ✓ Failure of the target
 - ✓ Disruption of service
 - ✓ Loss or exposure of sensitive data



Organizational Risks

- ❑ This type of risks can occur as a side effect of penetration testing
- ❑ Examples:
 - ✓ Repetitive and unwanted triggering in the incident handling processes
 - ✓ Negligence towards monitoring and responding incidents
 - ✓ Disruption in business continuity
 - ✓ Loss of reputation



Legal Risks

- ❑ This type of risks arises from legal obligations
- ❑ Examples:
 - ✓ Violation of laws and clauses in the rules of engagement (ROE)



Addressing Risks Associated with Penetration Testing and Avoiding Potential DoS Conditions



Module Summary



This module has discussed the fundamentals of penetration testing and its benefits



It has covered various types of penetration testing



It also discussed strategies and phases of penetration testing in detail



This module also discussed various penetration testing methodologies



Finally, this module ended with a detailed discussion on guidelines and recommendations for penetration testing