

Role of Pen Tester in Ethical Hacking

(A Better way to increase Security)



Authors

Rahil Karedia,

Team Lead - Threat Intelligence,
Network Intelligence (I) Pvt, Ltd., India.

SK. Niamathulla,

Product Manager – Content Research,
EC-Council, India.

Table of Content

Penetration Testing and Ethical Hacking	04
Introduction to Penetration Testing	04
Why Perform a Penetration Testing	05
When to Perform Penetration Testing?	05
Methodologies of Penetrating Testing	05
Penetration Testing Process	06
Test Preparation	06
What are FIVE Phases in Penetration Testing	06
1. Information Gathering	06
2. Scanning:	06
3. Discover Vulnerability:	06
4. Exploitation:	06
5. Report Generation:	06
Penetration Analysis	07
Top 7 Steps to Conduct Penetration Testing	09
Top 8 Penetration Testing Tools	10
Why you need a Penetration Testing from a Business Perspective	12
Why you need a Penetration Testing from an Operational Perspective	12
Tools for Penetration Testing	12
Role of a Pen Tester	13
Area of Penetration Testing	13
Infrastructure Penetration Testing? And Its Types?	14

Qualification & Certification of Pen Testers	16
Top 5 Variety of Tailored Pen Testing Services	16
Professional Standards and Technical Competency	17
Top 12 Benefit of Penetration Testing	18
ETHICAL HACKING	19
What do Ethical Hackers do?	19
Laws Against Hacking	19
Categories of Hackers	20
Black Hat hackers	20
White hat hacker	20
Grey hat hackers	20
Phases of Ethical Hacking	20
Reconnaissance	20
Scanning	20
Gaining Access	20
Maintaining Access	21
Clearing tracks	21
Rules for ethical hacking	21
Some ethical hacking tools	21
Required skills of an ethical hacker	22
Pros & Cons of Ethical Hacking	22
Penetration vs Ethical Hacking	23



Introduction to Penetration Testing

Penetration testing is more of an art than a science. It is the process of trying to gain unauthorized access to authorized resources. To put simply, Penetration testing is “breaking into your system” to see how hard it is to do.

It is the main branch of network security evaluation; the main aim of penetration testing is to provide analysis to discover the vulnerabilities and security threats in a network.

The purpose of penetration testing is to understand the technique of gaining access to a system by using standard PT tools and techniques developed by hackers. After vulnerability assessments, which are being used to identify and inventory various exposures within the organization’s systems. Penetration testing attempts to exploit anyone of the vulnerabilities to gain unauthorized access.

Why Perform a Penetration Testing

- If the vulnerability is utilized by an unauthorized individual to access company resources, the primary objective of a penetration test is to focus on vulnerabilities before they can be utilized.
- Penetrating testing is a valuable assurance. The assessment tool that benefits both business and its operations.
- The main goal of a vulnerability assessment is to identify controlled security vulnerabilities Conditions that can be terminated before unauthorized users exploited them.
- Computing Systems use penetration testing to solve problems of the high severity vulnerabilities.

When to Perform Penetration Testing?

Penetration Testing plays a vital role in every organization; it is an essential feature that needs to be performed regularly for protecting the functioning of a network. In addition to this, it should be performed penetration testing whenever:

1. You update your system or install the software
2. You add a new network infrastructure
3. You relocate your office

Methodologies of Penetrating Testing

Penetration Testing Methodology includes 3 types:

A Zero-Knowledge Test (Black Box)	The Penetration Test team has no information about the test target environment.
A Full Knowledge Test (White Box)	The Client organization provides the necessary information to the test team.
A Partial Knowledge Test (Grey Box)	The Penetration test team has partial disclosure of information about the target environment.

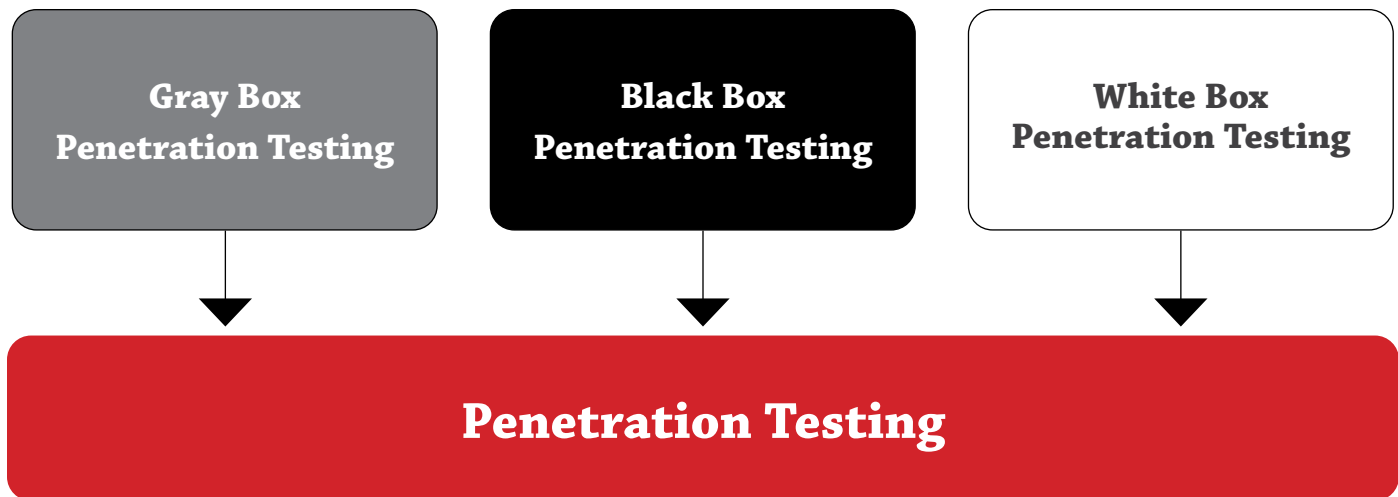


Fig-1: Methodologies of Penetration testing

Penetration Testing Process

To conduct a penetration test and document its outcome, a systematic approach which is circulated to different organization units and management levels in the organization is required. Penetration testing is conducted in three phases:

1. Test Preparation	2. Test Testing	3. Test Analysis
---------------------	-----------------	------------------

Test Preparation

In this preparation process, the documents are collected and finalized. In this phase, the scope of the system components, objective of the test, test duration, and time are identified, agreed, and documented. Due to predicted incidents like information leakage, downtime is defined and recorded in the legal documents, then they are agreed upon and signed by both sides.

FIVE Phases in Penetration Testing

Penetration Testing is a proof-of-concept approach to explore and exploit vulnerabilities. The process of Pen tester confirms whether the vulnerability really exists and further proves that exploiting it can result in damage to the network. The results of a Penetration testing is, typically, evidence in the form of a log, which confirms the finding and can be a useful aid towards remediation. These are the steps involved in the PT process:

1. Information Gathering
2. Scanning
3. Discover Vulnerability
4. Exploitation
5. Report Generation

Penetration Testing Stages

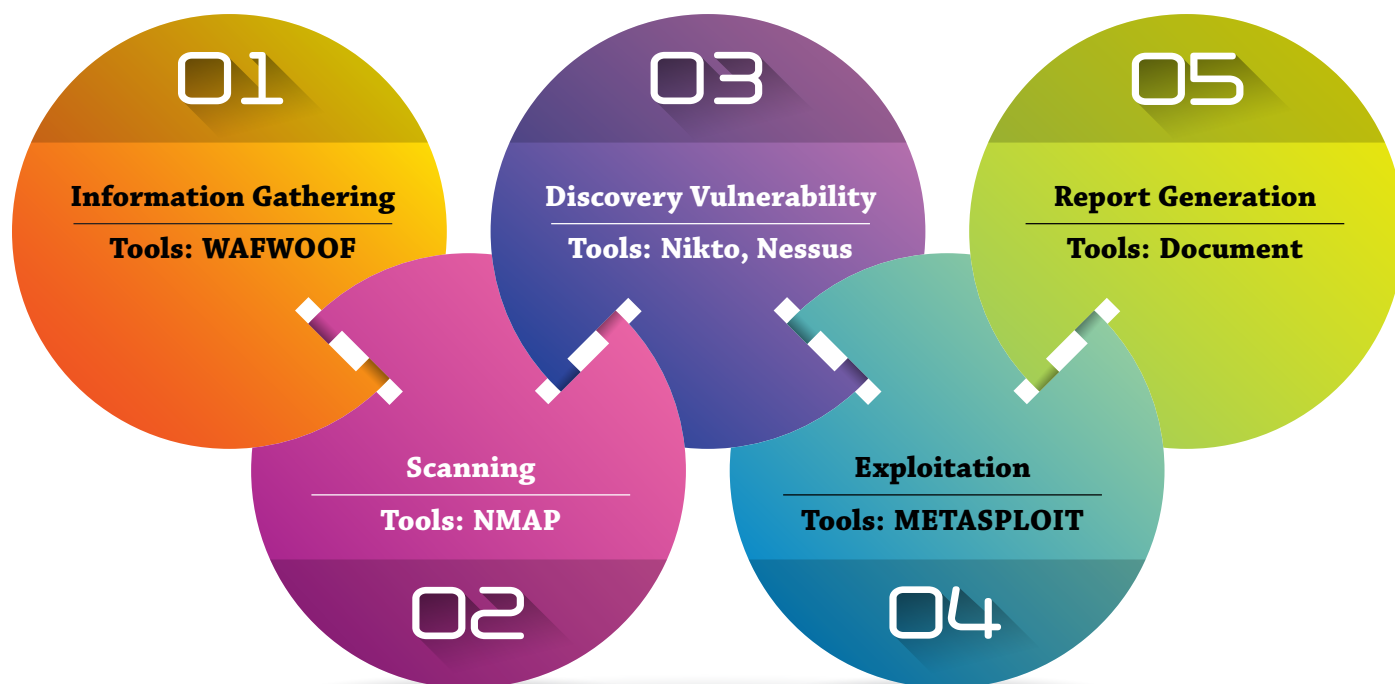


Fig -2: Phases of Penetration Testing

1. Information Gathering

In this Information gathering phase, Pen-tester gathers all information related to server like:

- What is the correct domain of web server and
- How many sub-domains are connected to this domain
- Is any firewall is set up for web server or not?

In this phase, we found that the web server's IP – 123.456.78.911. For detection of the firewall, we will use the tool WAFWOOF (web application firewall detection tool)

2. Scanning:

Pen-tester identifies

- What type of services is running on the web-server.
- What are the functions of that particular service?
- On which port this service is running.
- All assistance is running on which operating system.

To do this NMAP (Network Mapper) tool and Metasploit's Auxiliary facility is used.

3. Discover Vulnerability:

To find the vulnerability in the webserver or any network pen-tester, Nikto, Nessus is mainly used.

In this step, the penetration tester will receive the challenge of evaluating and finding the necessary security defeats from the target. This task focusses on the process of the pen-testing. It is essential to ensure that each task, functions, and processes is done accurately. This phase expands into two main procedures:

- a. Code Analysis
- b. Vulnerability Analysis

Code Analysis

It is used to find security flaws by analyzing source code. It is usually analyzed like this would automatically find security flaws with a high degree.

Vulnerability Analysis

This vulnerability analysis is classified into two areas identifying and reducing the number of vulnerabilities before the software is installed. With identifying vulnerability, it strives to help security engineers understand how vulnerabilities are created and found.

The main goal is that, with this education, security engineers will learn how to detect and eliminate the vulnerabilities in software products before the products are shipped into the system. The reality is that many software products are being dispatched with new vulnerabilities that attackers may be able to exploit.

This vulnerability remediation process involves a comprehensive approach to securing the network using the below equation:

$$\text{Total Vulnerability} = \text{CA} + \text{VA}$$

Where CA = Code Analysis

VA = Vulnerabilities Analysis

4. Exploitation:

After finding the vulnerability, a pen-tester primary goal is breaching all types of security and take the remote access of the server. For doing this, the pen-tester uses the METASPLOIT tool.

5. Report Generation:

In this report generation phase, Pen-tester will generate a full report on the testing process.

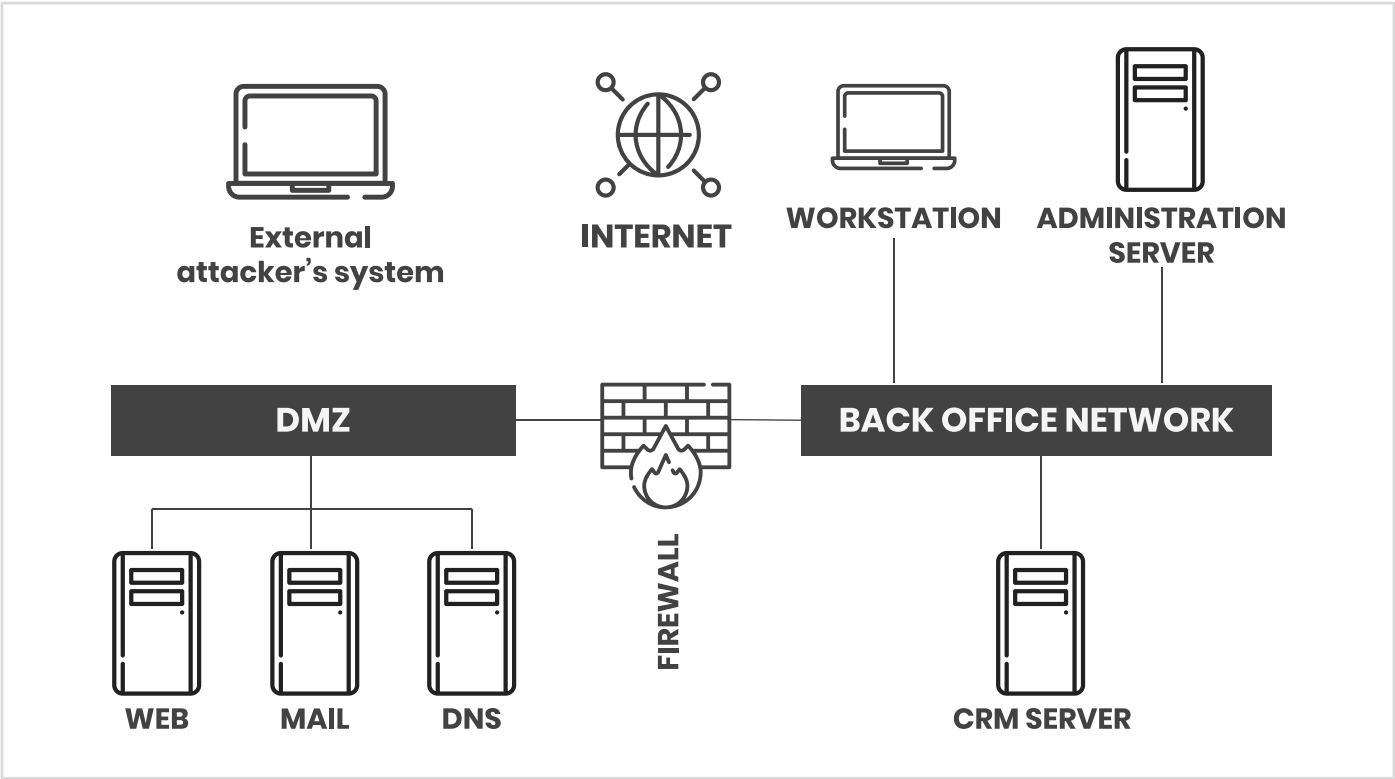
Penetration Analysis

Once the penetration testing process has been compiled, the next process is to prepare a report. The report is provided to advisory and various senior management through the reporting process. IT networking staff, IT management will all likely see the final report or at least part of it.

The report section consists of a core summary, technical details, an overview of risk level indication, assessment finding, budget information, and time estimation, etc.

By using this final report, Pen-tester can represent the entire process to the IT department so that the final result can be obtained and implemented. A mitigation plan is prepared after the penetration testing.

The advisory team plays a vital role in the final phase of the penetration model includes security solutions and patched information against all found risks such as preparation of countermeasures, Budget Estimation, Time Estimation, Creation Advisory Map, Recheck the implemented solution, etc. In this task, penetration tester must provide a definitive and conclusive advisory report for various solutions and the cost. In many instances, when penetration testing is completed, the client needs to install the suitable patches. In such cases, the security solution should be provided in both open source and paid solutions. The advisory phase is depended on the reporting phase because advisory must be prepared after a complete review of all different reports.



Top 7 Steps to Conduct Penetration Testing

Penetration Testing provides clear and concise direction on how to secure your organization's information and network from real-world attacks. One of the critical factors in the process of penetration testing is its underlying methodology.

Generally, Penetration testing has Three Phases

1. Test Preparation

2. Test Examination

3. Test Analysis

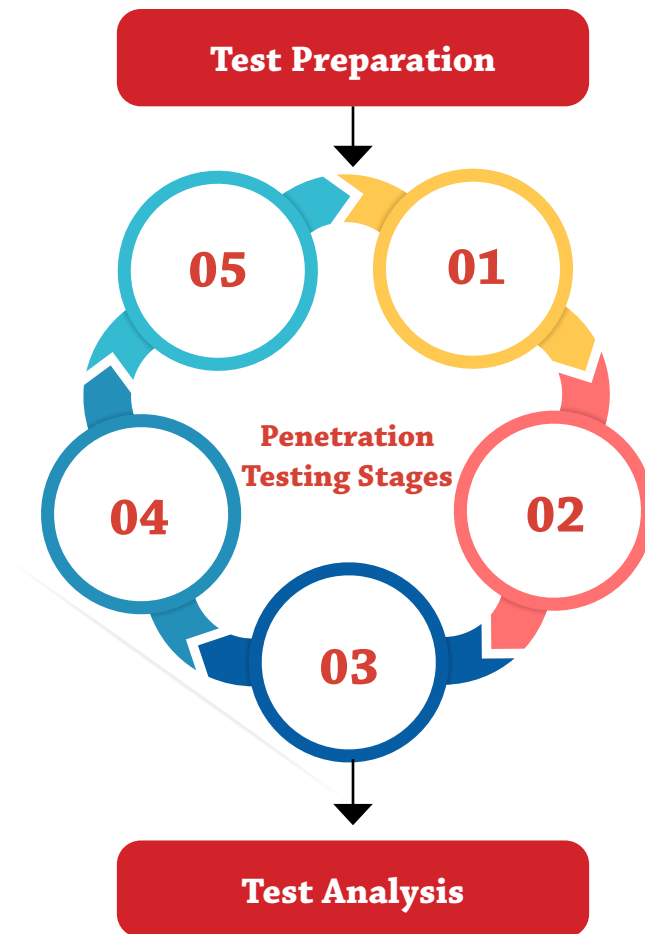


Fig – 3: Phases of Penetration Testing

Step - 1:	All the necessary documents for the test are organized and finalized during the test preparation phase.
Step - 2:	The Pen-testers and the organization meet to decide the scope, objectives, timing, and duration of the test.
Step - 3:	The information leakages and downtime are resolved and put into the legal agreement document.
Step - 4:	Information gathering from the physical and logical areas of the test target.
Step - 5:	Identify all pertinent information needed in the vulnerability analysis phase
Step - 6:	Depending upon the information gathered, the pen-tester then analyses the vulnerabilities within the targets system, application, etc.
Step - 7:	The pen-tester may opt to use the manual method or automated method by using tools (Tools shown in the below table - 1)



Penetration Testing Tools

Name of the Tools	Specific Purpose	Portability
Nmap	Network Scanning, Port Scanning OS Detection	Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac
Hping	Port Scanning, Remote OS fingerprinting	OpenBSD, Solaris, Mac OS X Linux, Free BS, NetBSD
SuperScan	Detect open TCP/UDP ports Run queries like whois, ping, and hostname lookups	Windows 2000, XP, Vista, Windows 7
Xprobe	Remote active OS fingerprinting	Linux and all updated OS
pOF	OS Fingerprinting Firewall detection	Linux, NetBSD OpenBSD, FreeBSD, Mac OS X, Solaris
Httpprint	Web server fingerprinting Detect web-enabled devices	Linux, Mac OS X, Free BSD, Win32
Nessus	Detect vulnerabilities that allow a remote cracker to access or control sensitive data Detect misconfiguration	Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows, Apple
Scanner	Detect network vulnerabilities	Windows but can scan servers built on any platform

Why you need a Penetration Testing from a Business Perspective

From a professional perspective -

- To protect against failure through prevention of financial loss
- To prove appropriate diligence and compliance for industry regulators, customers, and shareholders
- To protect the corporate image
- Rationalization of information security
- To identify and find out risks before safety violations
- Increase awareness about the importance of security at all levels of the organization
- Investment Cost- The organization spends millions of dollars to recover from cyberattack costs, corrective efforts, and reduction in revenue.

Why you need a Penetration Testing from an Operational Perspective

From the operational point of view –

- Quickly and accurately identify the real and potential weaknesses
- Active elimination or mitigation of identity Risk
- Implementation of corrective measures
- An increase in IT knowledge
- Effectively and efficiently – by providing various information and priority vulnerabilities.
- Well-organized and tested configuration changes to end the identified risks
- Determine the effectiveness and probability of an organization vulnerabilities

Tools for Penetration Testing

There are a wide variety of tools that are used in Penetration Testing and the important tools are:

NMap:

Nmap (a.k.a Network Mapper) is used to develop network services and maps. Nmap sends specifically crafted packets to the target host and then analyses the responses. Nmap supports the scanning of the various types of protocols and most of the existing systems.

BeEF:

BeEF (a.k.a Browser Exploitation Framework) focuses on the web browser. It works on Linux, Apple Mac OS X, and Microsoft Windows. BeEF allows the professional pen tester to assess the actual security posture of a target environment. It investigates the exploitability in the context of web browsers.

Metasploit:

Metasploit is a tool that tests for weaknesses in operating systems and applications. This penetration testing tool is based on the concept of 'exploit'. It runs a set of codes on the test target creating a framework for penetration testing. It works on Linux, Apple Mac OS X, and Microsoft Windows.

Nessus

Nessus is a penetration testing tool and remote security scanner, typically run on one machine to scan the services offered by a remote machine. Nessus is the world's most popular vulnerability scanner that is used in over 75,000 organizations worldwide. Nessus tool allows the user to script and run specific vulnerability checks. These checks provide a lot of control where most products do not.

Cain and Abel:

Cain and Abel mostly used for password cracking. It uses network sniffing, Dictionary attack, Brute-force, and cryptanalysis attacks, and routing protocol analysis methods to accomplish this. This is entirely for Microsoft operating systems.

Role of a Pen Tester

The role of a Pen Tester are:

1. Testing across internal security networks.
2. Identifying exposures to protect the most critical data.
3. Discovering vulnerabilities and risks throughout the IT infrastructure.
4. Prioritizing remediation recommendations to ensure that the certified security team is utilizing their time most effectively while protecting the most significant security gaps.
5. Reporting.

Area of Penetration Testing

Penetration Testing is generally done in the following three areas:

1. Network Penetration Testing
2. Application Penetration Testing
3. The response of the system

In-Network Penetration Testing, the network's physical structure needs to be tested to identify the vulnerability and risk. In the networking infrastructure, a Pentester discovers security flaws in the design, implementation, operation part of the respective organization's network.

In the application Penetration Testing, the logical structure of the system needs to be tested to identify vulnerability and risk in an application. The firewall and other monitoring systems are utilized to protect the security system, but sometimes, it needs to be focused on testing, especially when traffic can pass through the firewall.

The response of the system, in this area, Social Engineering gathers information on human interaction to obtain information about an organization its system. It is valuable to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this penetration test is exclusively designed for the workflow of the organization.



Infrastructure Penetration Testing? And Its Types?

Infrastructure Penetration Testing includes, (a) All Internal systems (B) External devices (C) Internet networking (D) Cloud & Virtualization testing.

Hidden on your internal network from public view, there is always a possibility that a criminal can leverage, which can damage your Network infrastructure. Therefore, it is better to be safe than sorry.

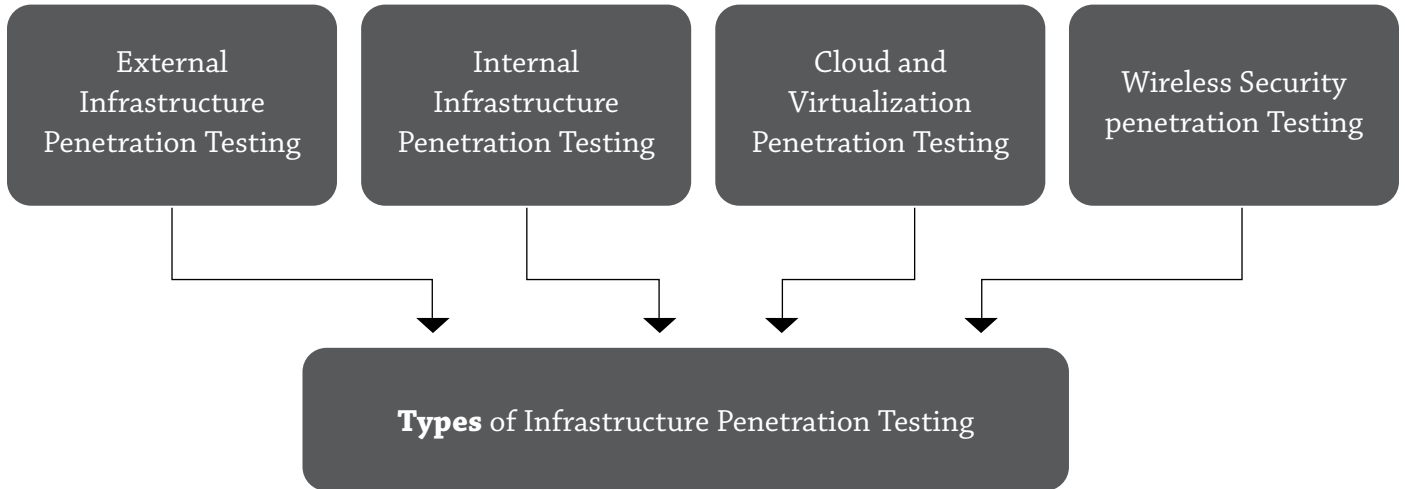






Fig – 4: Types of Infrastructure Penetration Testing



Types of Infrastructure Penetration Testing

Penetration Test		Objective	Benefit
	External Penetration Tests	Identify and exploit vulnerabilities on networks, applications, exposed to the internet. The external test is performed over the internet bypassing the firewall	Understand the risk of assets exposed to the internet.
	Internal Penetration Tests	Insider attacker that has gained access to an end-user system, including escalating privileges installing custom-crafted malware. The internal test is performed by connecting to the internal LAN	Understand risk to organization from a breach
	Cloud & Virtualization Penetration Tests	Identifying the attacker in a cloud environment is challenging. Further, identifying the attacker in a cloud environment is difficult. A criminal attacker can also buy hosting a cloud facility to get access to a user's new cloud data. Most of the cloud hosting is implemented on virtual infrastructure, causing virtualizing risk that an attacker can easily access.	Discovers real risks within the virtual environment and suggests the methods and costs fix the threats and flaws.
	Wireless Security Penetration Test	<u>Wireless technology of your handheld devices provides easy and flexible access to various networks. The easily accessible technologies are vulnerable to unique risks. A criminal hacker can hack from the remote location. WSPT is necessary for every organization.</u>	To find the potential risk and to protect from the external threats.

Qualification & Certification of Pen Testers

Qualification of Pen Testers:

Penetration testing can be performed only by a qualified and certified penetration tester. Therefore, certification of a penetration tester is essential.

A certified internal and external pen-testers are organizationally independent to perform the penetration testing; It means that the Pen-tester must be organizationally independent of the management of the target systems. Here are some certifications that will help you while calling a pen tester.




Certification



Qualified and certified pen tester can perform penetration testing. Certification like C | EH held by the tester is an indication of his practical skill sets and penetration testing.

Here are the few vital penetration testing certifications:

- Certified Ethical Hacker (C | EH)
- Certified Ethical Hacker (Practical & Master)

Top 5 Variety of Tailored Pen testing Services

Types of Penetration Testing			
Penetration Test		Objective	Benefit
	External Penetration Tests	Identify and exploit vulnerabilities on networks, applications, exposed to the internet. The external test is performed over the internet bypassing the firewall.	Understand the risk of assets exposed to the internet.
	Internal Penetration Tests	Insider attacker that has gained access to an end-user system, including escalating privileges installing custom-crafted malware. The internal test is performed by connecting to the internal LAN.	Understand risk to organization from a breach
	Mobile Device Assessments	Systematically assess the security of handheld devices and installed applications.	Understand the risk introduced to an organization through newly developed mobile applications

	Web Application Assessments	Systematically assess web applications for weaknesses that can lead to unauthorized access or data exposure.	To find the potential risk and to protect from the external threats.
	Phishing & Social Engineering attacks	Assess the security awareness and training on security controls concerning human manipulation and spam email identification.	Understand an organization reacts to the exploitation of employees

Professional Standards and Technical Competency

Professional bodies set industrial standards to distinguish members and non-members. It is called a code of conduct and mark as a guide to the penetration tester. The standard codes of conducts are: EC-Council

All testers and personals involved in the PEN test have to keep up their knowledge and update on the tests and development. It is essential to continually develop skills and understanding of the new system that is being developed and used. OSSTMM (Open Source Security Testing Methodology Manual) is used in developing technical skills and knowledge. OWASP Open Web Application Security Project is used for internet-based applications.



Top 12 Benefit of Penetration Testing

01. A Penetration test is used to identify the risks that may occur when an attacker gets access to the system and networks.

02. Performing a Pen test will help estimate the mitigation plan to close security gaps before the actual attack happens.

03. Conducting a Pen test helps organizations to reduce financial and information loss that would have caused a loss in customer trust due to security breaches.

04. Penetration testing safeguards the organizations against failure through preventing financial loss and provide compliance to industry regulators, customers, and shareholders.

05. Penetration testing helps in developing trust, corporate image, and rationalize IT security investments.

06. Penetration Testing is a proactive process, it provides unassailable information that helps the organization to meet the auditing or compliance aspects of regulations.

07. Penetration testing helps adhere to the audit regulatory standards like PCI DSS, HIPAA, and GLBA. This avoids the huge fines for non-compliance.

08. One of the main objectives of PEN testing is to create IT security and its importance at all levels in an organization through structured training and awareness programs to avoid security incidents that may cause damage in terms of confidentiality, integrity, relationship, and customer trust.

09. Penetration testing helps an organization to evaluate the level of security awareness among its employees, the effectiveness of the existing security policy and process, and the efficiency of its products.

10. Penetration testing helps in the decision-making to evaluate the organization's security and hence plan for the security investment and IT strategy.

11. Penetration testing also helps in shaping the important aspects of information security strategy by identifying the vulnerabilities quickly and accurately.

12. Penetration helps in business to evaluate the impacts and likelihood of the vulnerabilities.

13. Penetration testing consumes lots of time, effort, and knowledge depending on the complexity of the business. Therefore, penetration testing supports the enhancement of the knowledge and competency of the persons involved in the process.

ETHICAL HACKING

Hacking is detecting imperfection in the system or network to exploit its weakness to gain access or simply unauthorized access to anyone's system. The first known hacking event took place in 1960 at MIT, and at the same time, the term "hacker" was originated. Users who attack someone else system for their gain or to fulfil their agenda are known as hackers. Hackers are also called as crackers, intruders or attackers.

Ethical Hacking

It is just inverse of criminal hacking. Its goal is to prove a service for a client to test his environment on which it will cope with the hacker's attack; the output of ethical hack is a detailed report about the detected problems, vulnerabilities, and reports. It often has instructions on how to vanish those vulnerabilities. Independent computer security professionals breaking into the computer system with legal permission of the system owner are ethical hackers. Big organizations like Facebook, Google, and yahoo hire ethical hackers to tell them the weakness in their network or any small loophole. If someone wants to attack an ethical hackers system, it will bounce back and go back to them. Ethical hacking is also called as penetration hacking.

What do Ethical Hackers do?

A Certified Ethical Hacker tries to find the answers to the following questions –

1. Vulnerabilities that an attacker can hit
2. What can an attacker see on the target system?
3. What can an attacker do with that confidential information?

Ethical hacker – (a) Address vulnerabilities and risks (b) Explain and suggest the avoidance procedures (c) Finally, prepare a final report of all ethical activities that he did and observed while performing penetration testing.

Laws Against Hacking

Computer Fraud & Abuse Act (CFA)

It makes illegal the distribution of computer code i.e., placing computer code on a computer system or network that can be used to cause damage all economic loss.

Economic Espionage Act (EEA) Used both domestically and internationally to make illegal the theft of trade secrets.

The Wire Fraud Act (WFA) It makes illegal to misuse the wire communications.

The Identity Theft & Assumption Deterrence Act (ITADA)

Protect individuals who are victims of fraud when it comes to hacking.

Father of Hacking

In 1971 John Draper aka Captain Crunch was the first phone hacker and was called the father of hacking.



Categories of Hackers

There are mainly three types of hackers.

Black Hat hackers

These attackers are those who harm anyone for their good to earn money or any other personal benefits. They are criminal hackers.

Bad intention + without permission = black hat hacker

White hat hacker

They are trained professionals hired by the company to hack into their network and find the bloopers and try to give solutions to those peoples. They work in a novel way and are known as white hat hackers or ethical hackers.

Good intention + with permission = white hat hacker.

Grey hat hackers

These hackers have characteristics of both black and white hat hackers. They don't have a personal conflict with the party they are attacking but instead they do it for fun, but without permission. Unlike white hat, grey hat hackers often publicize systems vulnerability.

No bad intentions + without permission = grey hat Hacker.

Phases of Ethical Hacking

Reconnaissance

It's the first and most extended phase of ethical hacking, sometimes lasting weeks or months. In this attacker, gather (collect) the sufficient information from many sources before the attack. This can be performed either actively or passively. E.g., it's easy to find the OS version number and the type of web server that a company's uses with this the hacker can find a vulnerability in that OS version and exploit it to gain access. The tools used in this phase are NMAP, Hping, Google Dorks, Maltego.

Scanning

It is the second phase of ethical hacking. In this, after gathering all the information, the hacker begins the process of scanning perimeter and internal network devices looking for weaknesses in them. It examines all the open as well as close ports. The tools involved during scanning are dialers, sweepers, ports scanner, and network mappers, etc.

Gaining Access

It is the third phase of ethical hacking. Here real hacking takes place. All the information gathers during reconnaissance and scanning are misused to gain access. E.g., Stack-based buffer overflows, Does, and

password cracking. The method used by the hackers to establish a connection for intruding in someone else system can be LAN, local access to a pc, offline, and internet. The foremost tool used in this phase is Metasploit.

Maintaining Access

After gaining access, the hacker inserts some backdoors, Trojan, rootkits in the owned system for future access. The owned system also called a zombie system.

Clearing tracks

In this phase, to hide his wrong deeds, the attacker drops out all the activity logs perform during hacking. He removes all the pieces of evidence the can be harmful to him in the future. The activity done during this phase include altering log files, use of tunneling protocols, and steganography Reporting; Reporting is the last step of the ethical hacking process. Here detailed documentation such as tools used vulnerabilities found, the success rate, and exploit methods.

Rules for ethical hacking

1. The hacker must have expressed (often written) permission to inquest (investigate) the network and seek to identify potential security.
2. You should respect the individual or company's privacy.
3. You should closeout work after completing the task anything open for you or anybody else to exploit later.
4. You let the IT hardware manufacturer or software developer know of any security vulnerabilities you find in their software or hardware, if not known by the organization.

Some ethical hacking tools

Samspace

Samspace is a tool that provides information about a particular host. Example: the address, phone no. etc

Email Tracker& Visual Route

As you know we frequently received many spam messages in our mailbox but we don't know where it comes from. An email tracker is a tool that shows us the actual location of the spam messages server. The email tracker uses a received message header which is associated with it to find the real location.

NMAP (Network Mapper)

NMAP is an open-source and free utility for network assessment, exploration, and security auditing. It uses raw IP packet to determine the hosts which are available on the network, services offered by the network, and operating system used by them.

Metasploit

Metasploit has a bunch of very powerful exploit tools, with it, you can even build your custom tools using its infrastructure. It is free of cost and the most popular cybersecurity tool. It is used for exploit development vulnerability scanning at a different platform, collecting information.

Wire-Shark

It is a well-known tool in the cyber world used by thousands of security professionals for analyzing networks, live packet capturing, and intensive scanning of protocols. It's commonly known as a packet crafting tool.

Required skills of an ethical hacker

He must know these given parameters:

Parameters	Required Skills
Project Management	Planning, organizing and controlling a penetration testing
Network Protocol	TCP/IP protocols and their functions and its manipulation
Microsoft	Operation configuration and management
Routers	Knowledge of routers, routing protocols, and access control list
Firewalls	Deep knowledge about configuration and operation of IDS/IPS
Linux	Knowledge of Linux/Unix, security setting, configuration and services

Pros & Cons of Ethical Hacking

Pros of Ethical Hacking

1. We can find the weakness in our network system through ethical tools & ethical hacking concepts before the hacker's attack which will make our information secure.
2. Using hacking techniques, we can prepare a high-level model through which we can strongly secure our valuable system at its best. III. A brief report on strong and weak security measures can be prepared because the hackers attack these weak security links to gain access & these weak points are made strong using ethical hacking.

Cons of Ethical hacking

1. If an ethical hacker turns out to be a greedy man and his wishes were not fulfilled by the company then he can leak the crucial data to destroy the organization by allowing the company's finance and banking details to be exposed.
2. If the ethical hackers get caught while sending malicious code, malware, and viruses in the company's system then he will be sent to prison and even his license as an ethical hacker will be banned.

Penetration vs Ethical Hacking

Penetration Testing	Ethical Hacking
A Narrow term focusses on penetration testing – To secure the security system	Comprehensive term and penetration testing are some of its features.
Required to have complete knowledge of only the specific area for which he conducts pen testing	Required knowledge on software programming as well as hardware
A pen tester not necessarily required to be a good report writer	An ethical hacker essentially needs to be an expert on report writing
A Pen tester can perform penetration testing with some necessary inputs	An ethical hacker required to be an expert professional in the subject, who has the obligatory certification (C EH) of ethical hacking to be effective
Paperwork is less compared to Ethical hacker	Paperwork is required including legal agreement etc.
Pen tester required less time to perform testing	Ethical hacking involves a lot of time and effort
Normally, Pen tester doesn't require accessibility of systems and its infrastructure and it requires accessibility only for the part for which the tester performing pen-testing.	It normally requires a whole range of accessibility all systems and its infrastructure (as per the situation)






FAQ:

What are the best Penetration Testing Tools?

1. The Network Mapper (NMAP)
2. Metasploit
3. Wireshark

Read more: <https://blog.eccouncil.org/6-essential-skills-needed-for-advanced-penetration-testing/>

What are the types of Penetration Testing?

Penetration Test		Objective
	External Penetration Tests	Identify and exploit vulnerabilities on networks, applications, exposed to the internet. The external test is performed over the internet bypassing the firewall.
	Internal Penetration Tests	Insider attacker that has gained access to an end-user system, including escalating privileges installing custom-crafted malware. The internal test is performed by connecting to the internal LAN.
	Mobile Device Assessments	Systematically assess the security of handhold devices and installed applications.
	Web Application Assessments	Systematically assess web applications for weaknesses that can lead to unauthorized access or data exposure.
	Phishing & Social Engineering attacks	Assess the security awareness and training on security controls concerning human manipulation and spam email identification.

Read more: <https://edm-image.s3-us-west-2.amazonaws.com/Forms/Blog/Cyber-Research/WIRELESS-PENETESTING-TO-PROTECT-WIRELESS-NETWORKS-Whitepaper.pdf>

Why do you need Penetration Testing?

If the vulnerability is utilized by an unauthorized individual to access company resources, the primary objective of a penetration test is to focus on vulnerabilities before they can be utilized. Penetrating testing is a valuable assurance. The assessment tool that benefits both business and its operations. Penetration testing is to identify controlled security vulnerabilities conditions that can be terminated before unauthorized users exploited them.

Read more: <https://blog.eccouncil.org/what-is-penetration-testing-how-does-it-differ-from-ethical-hacking/>

EC-Council