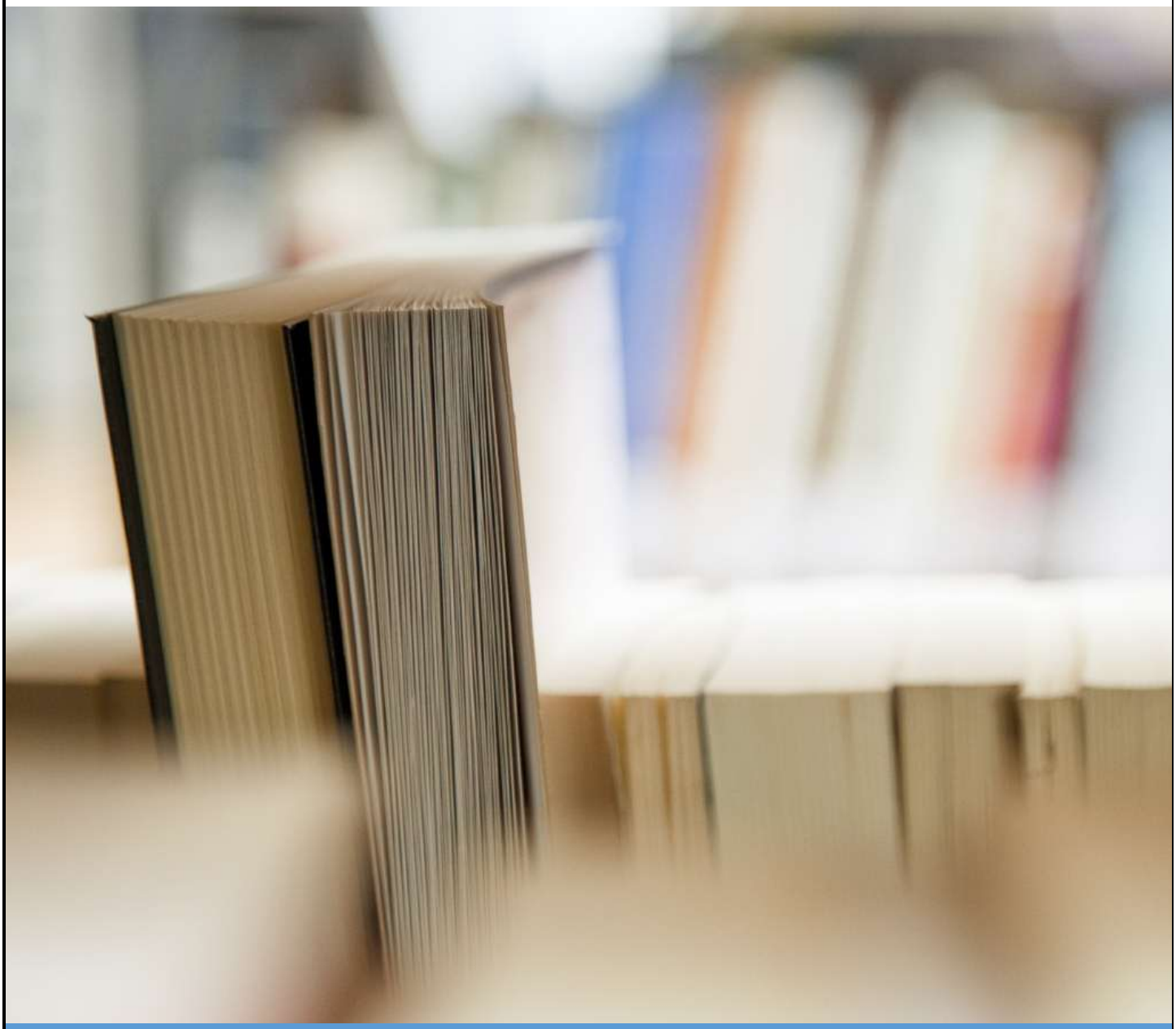


Learn Pen Testing

For Beginners

Rahul K

Table of Contents

Penetration Testing 4
What is Penetration Testing? 4
Why is Penetration Testing Required? 4
When to Perform Penetration Testing? 4
How is Penetration Testing Beneficial? 4
Steps of Penetration Testing Method 5
Planning & Preparation 6
Reconnaissance 6
Discovery 6
Analyzing Information and Risks 6
Active Intrusion Attempts 7
Final Analysis 7
Report Preparation 7
Penetration Testing Vs. Vulnerability 7
Penetration Testing 7
Vulnerability Assessment 7
Which Option is Ideal to Practice? 9
Types of Penetration Testing 9
Types of Pen Testing 9
Black Box Penetration Testing 10
Advantages of Black Box Penetration Testing 10
Disadvantages of Black Box Penetration Testing 10
White Box Penetration Testing 10
Advantages of White Box Penetration Testing 10
Grey Box Penetration Testing 11
Advantages of Grey Box Penetration Testing 11
Areas of Penetration Testing 11
Penetration Testing - Manual & Automated 12
Penetration Testing - Tools 14
Penetration Testing - Infrastructure 16
What is Infrastructure Penetration Testing? 16
Types of Infrastructure Penetration Testing 16
External Infrastructure Testing 16
Internal Infrastructure Penetration Testing 17

Cloud and Virtualization Penetration Testing 17
Wireless Security Penetration Testing 17
Penetration Testing - Testers 18
Qualification of Penetration Testers 18
Certification 18
Past Experience 19
Role of a Penetration Tester 19
Penetration Testing - Report Writing 20
What is Report Writing? 20
Report Writing Stages 20
Report Planning 21
Information Collection 21
Writing the First Draft 21
Review and Finalization 21
Content of Penetration Testing Report 22
Executive Summary 22
Methodology 22
Detail Findings 22
References 22
Penetration Testing - Ethical Hacking 22
Who are Ethical Hackers? 23
Who are Criminal Hackers? 23
What can Criminal Hackers do? 23
What are the Skill-Sets of Ethical Hackers? 24
What do Ethical Hackers do? 24
Types of Hackers 25
Black Hat Hackers 25
White Hat Hackers 25
Grey Hat Hacker 25
Penetration Testing Vs. Ethical Hacking 26
Penetration Testing 26
Ethical Hacking 26
Penetration Testing - Limitations 27
Penetration Testing - Remediation 28
What is Remediation? 28
Penetration Testing - Legal Issues 29

What are the Legal Issues? 29
Five Types of Penetration Test for Successful Pen Testing 30
1. Network Service Tests. 30
2. Web Application Tests. 31
3. Client Side Tests. 31
4. Wireless Network Tests. 31
5. Social Engineering Tests. 31
Remote Tests. 32
Physical Tests. 32
Summary. 32

Penetration Testing

Penetration Testing is used to find flaws in the system in order to take appropriate security measures to protect the data and maintain functionality

What is Penetration Testing?

Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system.

If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.

Why is Penetration Testing Required?

Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because −

- It identifies a simulation environment i.e., how an intruder may attack the system through **white hat attack**.
- It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- It supports to avoid **black hat attack** and protects the original data.
- It estimates the magnitude of the attack on potential business.
- It provides evidence to suggest, why it is important to increase investments in security aspect of technology

When to Perform Penetration Testing?

Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system. In addition to this, it should be performed whenever −

- Security system discovers new threats by attackers.
- You add a new network infrastructure.
- You update your system or install new software.
- You relocate your office.
- You set up a new end-user program/policy.

How is Penetration Testing Beneficial?

Penetration testing offers the following benefits −

- **Enhancement of the Management System** − It provides detailed information about the security threats. In addition to this, it also categorizes the degree of vulnerabilities and suggests you, which one is more vulnerable and which one is less. So, you can

easily and accurately manage your security system by allocating the security resources accordingly.

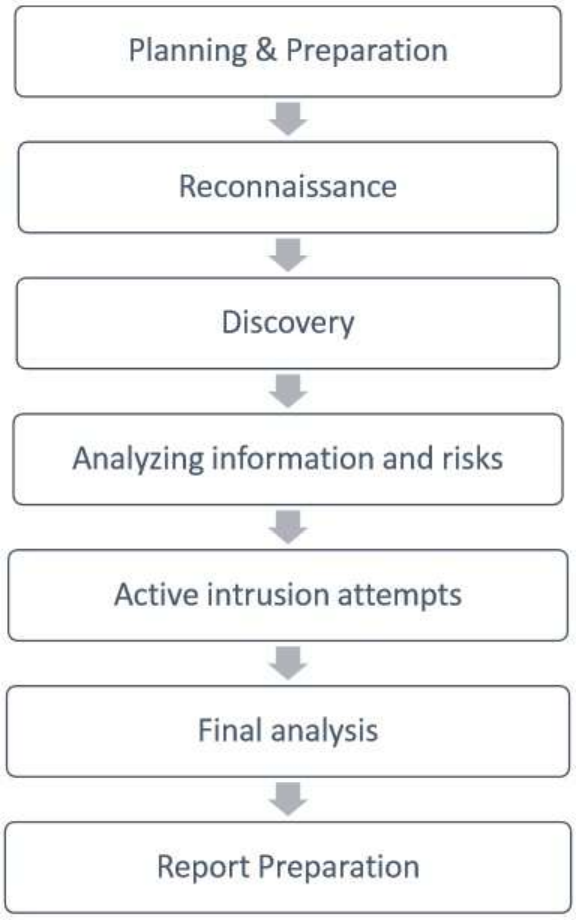
- **Avoid Fines** − Penetration testing keeps your organization's major activities updated and complies with the auditing system. So, penetration testing protects you from giving fines.
- **Protection from Financial Damage** − A simple breach of security system may cause millions of dollars of damage. Penetration testing can protect your organization from such damages.
- **Customer Protection** − Breach of even a single customer's data may cause big financial damage as well as reputation damage. It protects the organizations who deal with the customers and keep their data intact.

Penetration testing is a combination of techniques that considers various issues of the systems and tests, analyzes, and gives solutions. It is based on a structured procedure that performs penetration testing step-by-step.

This chapter describes various steps or phases of penetration testing method.

Steps of Penetration Testing Method

The following are the seven steps of penetration testing −



Planning & Preparation

Planning and preparation starts with defining the goals and objectives of the penetration testing.

The client and the tester jointly define the goals so that both the parties have the same objectives and understanding. The common objectives of penetration testing are −

- To identify the vulnerability and improve the security of the technical systems.
- Have IT security confirmed by an external third party.
- Increase the security of the organizational/personnel infrastructure.

Reconnaissance

Reconnaissance includes an analysis of the preliminary information. Many times, a tester doesn't have much information other than the preliminary information, i.e., an IP address or IP address block. The tester starts by analyzing the available information and, if required, requests for more information such as system descriptions, network plans, etc. from the client. This step is the passive penetration test, a sort of. The sole objective is to obtain a complete and detailed information of the systems.

Discovery

In this step, a penetration tester will most likely use the automated tools to scan target assets for discovering vulnerabilities. These tools normally have their own databases giving the details of the latest vulnerabilities. However, tester discover

- **Network Discovery** − Such as discovery of additional systems, servers, and other devices.
- **Host Discovery** − It determines open ports on these devices.
- **Service Interrogation** − It interrogates ports to discover actual services which are running on them.

Analyzing Information and Risks

In this step, tester analyzes and assesses the information gathered before the test steps for dynamically penetrating the system. Because of larger number of systems and size of infrastructure, it is extremely time consuming. While analyzing, the tester considers the following elements −

- The defined goals of the penetration test.
- The potential risks to the system.
- The estimated time required for evaluating potential security flaws for the subsequent active penetration testing.

However, from the list of identified systems, the tester may choose to test only those which contain potential vulnerabilities.

Active Intrusion Attempts

This is the most important step that has to be performed with due care. This step entails the extent to which the potential vulnerabilities that was identified in the discovery step which possess the actual risks. This step must be performed when a verification of potential vulnerabilities is needed. For those systems having very high integrity requirements, the potential vulnerability and risk needs to be carefully considered before conducting critical clean up procedures.

Final Analysis

This step primarily considers all the steps conducted (discussed above) till that time and an evaluation of the vulnerabilities present in the form of potential risks. Further, the tester recommends to eliminate the vulnerabilities and risks. Above all, the tester must assure the transparency of the tests and the vulnerabilities that it disclosed.

Report Preparation

Report preparation must start with overall testing procedures, followed by an analysis of vulnerabilities and risks. The high risks and critical vulnerabilities must have priorities and then followed by the lower order.

However, while documenting the final report, the following points needs to be considered −

- Overall summary of penetration testing.
- Details of each step and the information gathered during the pen testing.
- Details of all the vulnerabilities and risks discovered.
- Details of cleaning and fixing the systems.
- Suggestions for future security.

Penetration Testing Vs. Vulnerability

Generally, these two terms, i.e., Penetration Testing and Vulnerability assessment are used interchangeably by many people, either because of misunderstanding or marketing hype. But, both the terms are different from each other in terms of their objectives and other means. However, before describing the differences, let us first understand both the terms one-by one.

Penetration Testing

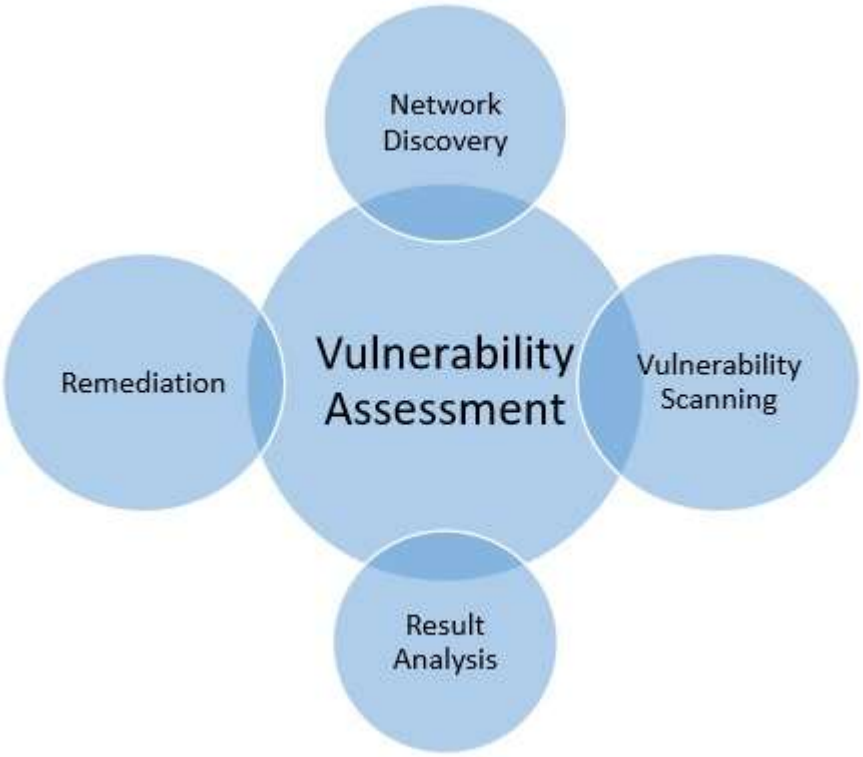
Penetration testing replicates the actions of an external or/and internal cyber attacker/s that is intended to break the information security and hack the valuable data or disrupt the normal functioning of the organization. So, with the help of advanced tools and techniques, a penetration tester (also known as **ethical hacker**) makes an effort to control critical systems and acquire access to sensitive data.

Vulnerability Assessment

On the other hand, a vulnerability assessment is the technique of identifying (discovery) and measuring security vulnerabilities (scanning) in a given environment. It is a comprehensive

assessment of the information security position (result analysis). Further, it identifies the potential weaknesses and provides the proper mitigation measures (remediation) to either remove those weaknesses or reduce below the risk level.

The following diagram summarizes the vulnerability assessment −



The following table illustrates the fundamental differences between penetration testing and vulnerability assessments −

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

Which Option is Ideal to Practice?

Both the methods have different functionality and approach, so it depends upon the security position of the respective system. However, because of the basic difference between penetration testing and vulnerability assessment, the second technique is more beneficial over the first one.

Vulnerability assessment identifies the weaknesses and gives solution to fix them. On the other hand, penetration testing only answers the question that "can anyone break-in the system security and if so, then what harm he can do?"

Further, a vulnerability assessment attempts to improve security system and develops a more mature, integrated security program. On the other hand, a penetration testing only gives a picture of your security program's effectiveness.

As we have seen here, the vulnerability assessment is more beneficial and gives better result in comparison to penetration testing. But, experts suggest that, as a part of security management system, both techniques should be performed routinely to ensure a perfect secured environment.

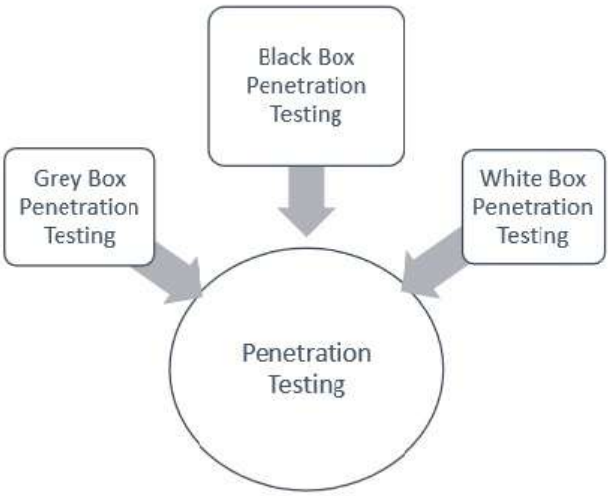
Types of Penetration Testing

The type of penetration testing normally depends on the scope and the organizational wants and requirements. This chapter discusses about different types of Penetration testing. It is also known as **Pen Testing**.

Types of Pen Testing

Following are the important types of pen testing −

- Black Box Penetration Testing
- White Box Penetration Testing
- Grey Box Penetration Testing



For better understanding, let us discuss each of them in detail −

Black Box Penetration Testing

In black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

Advantages of Black Box Penetration Testing

It has the following advantages −

- Tester need not necessarily be an expert, as it does not demand specific language knowledge
- Tester verifies contradictions in the actual system and the specifications
- Test is generally conducted with the perspective of a user, not the designer

Disadvantages of Black Box Penetration Testing

Its disadvantages are −

- Particularly, these kinds of test cases are difficult to design.
- Possibly, it is not worth, incase designer has already conducted a test case.
- It does not conduct everything.

White Box Penetration Testing

This is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc. It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

White box penetration testing examines the code coverage and does data flow testing, path testing, loop testing, etc.

Advantages of White Box Penetration Testing

It carries the following advantages −

- It ensures that all independent paths of a module have been exercised.
- It ensures that all logical decisions have been verified along with their true and false value.
- It discovers the typographical errors and does syntax checking.
- It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

Grey Box Penetration Testing

In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Advantages of Grey Box Penetration Testing

It has the following advantages −

- As the tester does not require the access of source code, it is non-intrusive and unbiased
- As there is clear difference between a developer and a tester, so there is least risk of personal conflict
- You don’t need to provide the internal information about the program functions and other operations

Areas of Penetration Testing

Penetration testing is normally done in the following three areas −

- **Network Penetration Testing** − In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk which ensures the security in a network. In the networking environment, a tester identities security flaws in design, implementation, or operation of the respective company/organization’s network. The devices, which are tested by a tester can be computers, modems, or even remote access devices, etc
- **Application Penetration Testing** − In this testing, the logical structure of the system needs to be tested. It is an attack simulation designed to expose the efficiency of an application’s security controls by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system, but sometime, it needs focused testing especially when traffic is allowed to pass through the firewall.
- **The response or workflow of the system** − This is the third area that needs to be tested. Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the ability of the respective organization to prevent unauthorized access to its information systems. Likewise, this test is exclusively designed for the workflow of the organization/company.

Penetration Testing - Manual & Automated

Both manual penetration testing and automated penetration testing are conducted for the same purpose. The only difference between them is the way they are conducted. As the name suggests, manual penetration testing is done by human beings (experts of this field) and automated penetration testing is done by machine itself.

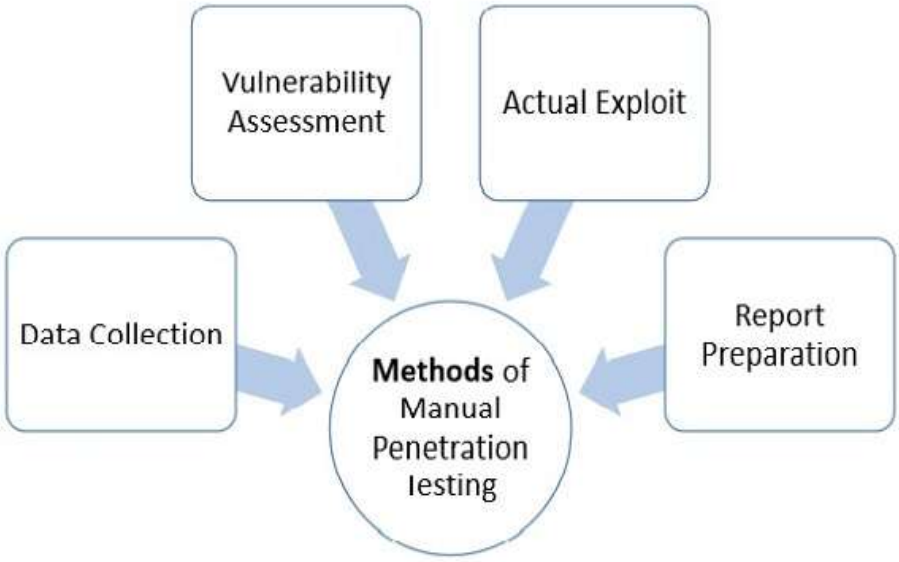
This chapter will help you learn the concept, differences, and applicability of both the terms.

What is Manual Penetration Testing?

Manual penetration testing is the testing that is done by human beings. In such type of testing, vulnerability and risk of a machine is tested by an expert engineer.

Generally, testing engineers perform the following methods −

- **Data Collection** − Data collection plays a key role for testing. One can either collect data manually or can use tool services (such as webpage source code analysis technique, etc.) freely available online. These tools help to collect information like table names, DB versions, database, software, hardware, or even about different third party plugins, etc
- **Vulnerability Assessment** − Once the data is collected, it helps the testers to identify the security weakness and take preventive steps accordingly.
- **Actual Exploit** − This is a typical method that an expert tester uses to launch an attack on a target system and likewise, reduces the risk of attack.
- **Report Preparation** − Once the penetration is done, the tester prepares a final report that describes everything about the system. Finally the report is analyzed to take corrective steps to protect the target system.



Types of Manual Penetration Testing

Manual penetration testing is normally categorized in two following ways −

- **Focused Manual Penetration Testing** − It is a much focused method that tests specific vulnerabilities and risks. Automated penetration testing cannot perform this testing; it is done only by human experts who examine specific application vulnerabilities within the given domains.
- **Comprehensive Manual Penetration Testing** − It is through testing of whole systems connected with each other to identify all sorts of risk and vulnerability. However, the function of this testing is more situational, such as investigating whether multiple lower-risk faults can bring more vulnerable attack scenario, etc

What is Automated Penetration Testing?

Automated penetration testing is much faster, efficient, easy, and reliable that tests the vulnerability and risk of a machine automatically. This technology does not require any expert engineer, rather it can be run by any person having least knowledge of this field.

Tools for automated penetration testing are Nessus, Metasploit, OpenVAs, backtract (series 5), etc. These are very efficient tools that changed the efficiency and meaning of penetration testing.

However, the following table illustrates the fundamental difference between the manual and automated penetration testing −

Manual Penetration Testing	Automated Penetration Testing
It requires expert engineer to perform the test.	It is automated so even a learner can run the test.
It requires different tools for the testing.	It has integrated tools does required anything from outside.
In this type of testing, results can vary from test to test.	It has fixed result.
This test requires to remember cleaning up memory by the tester.	It does not.
It is exhaustive and time taking.	It is more efficient and fast.
It has additional advantages i.e. if an expert does pen test, then he can analyze better, he can think what a hacker can think and where he can attack. Hence, he can put security accordingly.	It cannot analyze the situation.
As per the requirement, an expert can run multiple testing.	It cannot.
For critical condition, it is more reliable.	It is not.

Penetration Testing - Tools

Penetration testing, normally consists of information gathering, vulnerability and risk analysis, vulnerability exploits, and final report preparation.

It is also essential to learn the features of various of tools which are available with penetration testing. This chapter provides information and insights about these features.

The following table collects some of the most significant penetration tools and illustrates their features −

Tool Name	Purpose	Portability	Expected Cost
Hping	Port Scanning Remote OC fingerprinting	Linux, NetBSD, FreeBSD, OpenBSD,	Free
Nmap	Network Scanning Port Scanning OS Detection	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, IRIX, Mac, etc.	Free
SuperScan	Runs queries including ping, whois, hostname lookups, etc. Detects open UDP/TCP ports and determines which services are running on those ports.	Windows 2000/XP/Vista/7	Free
p0f	Os fingerprinting Firewall detection	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, Windows, and AIX	Free
Xprobe	Remote active OS fingerprinting Port Scanning TCP fingerprinting	Linux	Free
Httprint	Web server fingerprinting SSL detection Detect web enabled devices (e.g., wireless access points, switches, modems, routers)	Linux, Mac OS X, FreeBSD, Win32 (command line & GUI	Free

Nessus	Detect vulnerabilities that allow remote cracker to control/access sensitive data	Mac OS X, Linux, FreeBSD, Apple, Oracle Solaris, Windows	Free to limited edition
GFI LANguard	Detect network vulnerabilities	Windows Server 2003/2008, Windows 7 Ultimate/ Vista, Windows 2000 Professional, Business/XP, Sever 2000/2003/2008	Only Trial Version Free
Iss Scanner	Detect network vulnerabilities	Windows 2000 Professional with SP4, Windows Server 2003 Standard with SO1, Windows XP Professional with SP1a	Only Trial Version Free
Shadow Security Scanner	Detect network vulnerabilities, audit proxy and LDAP servers	Windows but scan servers built on any platform	Only Trial Version Free
Metasploit Framework	Develop and execute exploit code against a remote target Test vulnerability of computer systems	All versions of Unix and Windows	Free
Brutus	Telnet, ftp, and http password cracker	Windows 9x/NT/2000	Free

Penetration Testing - Infrastructure

Computer systems and associated networks normally consist of a large number of devices and most of them play a major role in conducting total works and businesses of the respective system. A minor flaw at any point of time, and at any part of these devices may cause great damage to your business. Therefore, all of them are vulnerable to risk and need to be secured properly.

What is Infrastructure Penetration Testing?

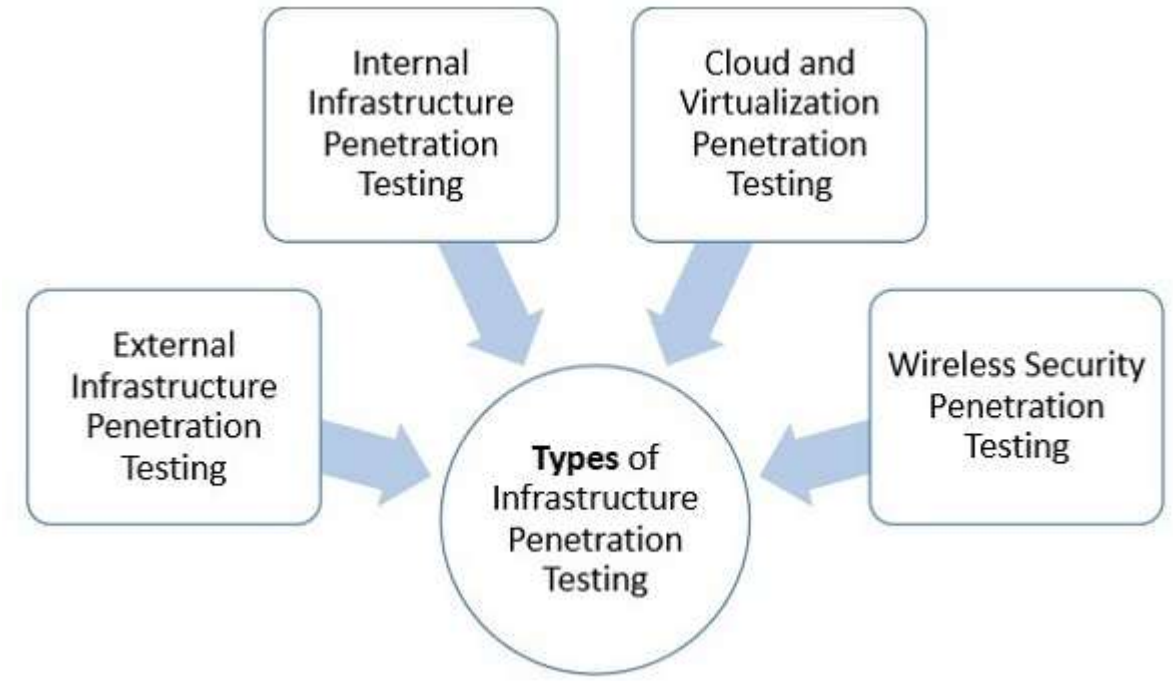
Infrastructure penetration testing includes all internal computer systems, associated external devices, internet networking, cloud and virtualization testing.

Whether hidden on your internal enterprise network or from public view, there is always a possibility that an attacker can leverage which can harm your infrastructure. So, it is better to be safe in advance rather than regret later.

Types of Infrastructure Penetration Testing

Following are the important types of infrastructure penetration testing −

- External Infrastructure Penetration Testing
- Internal Infrastructure Penetration Testing
- Cloud and Virtualization Penetration Testing
- Wireless Security Penetration Testing



External Infrastructure Testing

The penetration test, targeting the external infrastructure discovers what a hacker could do with your networks, which is easily accessible through the Internet.

In this testing, a tester normally replicates the same kind of attacks that the hackers can use by finding and mapping the security flaws in your external infrastructure.

There are various benefits of leveraging external infrastructure penetration testing, as it −

- Identifies the flaws within the firewall configuration that could be misused
- Finds out how information can be leaked out from your system by an attacker
- Suggests how these issues can be fixed
- Prepares a comprehensive report highlighting the security risk of the border networks, and suggests solutions
- Ensures overall efficiency and productivity of your business

Internal Infrastructure Penetration Testing

Due to some minor internal security flaws, hackers are illegally committing frauds in large organizations. So, with internal infrastructure penetration testing, a tester can identify the possibility of a security and from which employee, this problem has occurred.

Internal infrastructure penetration testing benefits as it −

- Identifies how an internal attacker could take advantage of even a minor security flaw.
- Identifies the potential business risk and damage that an internal attacker can inflict.
- Improves the security systems of internal infrastructure.
- Prepares a comprehensive report giving details of the security exposures of internal networks along with the detailed action plan on how to deal with it.

Cloud and Virtualization Penetration Testing

As you buy a public server or wave space, it significantly increases the risks of data breach. Further, identifying the attacker on cloud environment is difficult. An attacker can also buy hosting a Cloud facility to get access to your new Cloud data.

In fact, most of the Cloud hosting is implemented on virtual infrastructure, causing Virtualization risk that an attacker can easily access.

Cloud and Virtualization penetration testing benefits as it −

- Discovers the real risks within the virtual environment and suggests the methods and costs to fix the threats and flaws.
- Provides guidelines and an action plan how to resolve the issue/s.
- Improves the overall protection system.
- Prepares a comprehensive security system report of the Cloud computing and Virtualization, outline the security flaw, causes and possible solutions.

Wireless Security Penetration Testing

Wireless technology of your laptop and other devices provides an easy and flexible access to various networks. The easily accessible technology is vulnerable to unique risks; as physical security cannot be used to limit network access. An attacker can hack from the remote

location. Hence, wireless security penetration testing is necessary for your company/organization.

The following are the reasons for having wireless technology −

- To find the potential risk caused by your wireless devices.
- To provide guidelines and an action plan on how to protect from the external threats.
- To improve the overall security system.
- For preparing a comprehensive security system report of the wireless networking, to outline the security flaw, causes, and possible solutions.

Penetration Testing - Testers

There is the issue of protecting the most critical data of the organization; therefore, the role of a penetration tester is much critical, a minor error can put both the parties (tester and his client) on risk.

Therefore, this chapter discusses various aspects of a penetration tester including his qualification, experience, and responsibilities.

Qualification of Penetration Testers

This test can be performed only by a qualified penetration tester; therefore, qualification of a penetration tester is very important.

Either qualified internal expert or a qualified external expert may perform the penetration test until they are organizationally independent. It means that the penetration tester must be organizationally independent from the management of the target systems. For example, if a third-party company is involved in the installation, maintenance, or support of target systems, then that party cannot perform penetration testing.

Here are some guidelines that will help you while calling a penetration tester.

Certification

A certified person can perform penetration testing. Certification held by the tester is the indication of his skill sets and competence of capable penetration tester.

Following are the important examples of penetration testing certification −

- Certified Ethical Hacker (CEH).
- Offensive Security Certified Professional (OSCP).
- CREST Penetration Testing Certifications.
- Communication Electronic Security Group (CESG) IT Health Check Service certification.

- Global Information Assurance Certification (GIAC) Certifications for example, GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Advance Penetration Tester (GXPN), and GIAC Exploit Researcher.

Past Experience

The following questions will help you to hire an effective penetration tester −

- How many years of experience does the penetration tester has?
- Is he an independent penetration tester or working for an organization?
- With how many companies he worked as penetration tester?
- Has he performed penetration testing for any organization, which has similar size and scope as yours?
- What type of experience does the penetration tester has? For example, conducting network-layer penetration testing etc
- You may also ask for the reference from other customers for whom he worked.

When hiring a penetration tester, it is important to evaluate the past year testing experience of the organization for which he (tester) has worked as it is related to the technologies specifically deployed by him within the target environment.

In addition to the above, for complex situations and typical client requirements, it is recommended to evaluate a tester's capability to handle similar environment in his/her earlier project.

Role of a Penetration Tester

A penetration tester has the following roles −

- Identify inefficient allocation of tools and technology.
- Testing across internal security systems.
- Pinpoint exposures to protect the most critical data.
- Discover invaluable knowledge of vulnerabilities and risks throughout the infrastructure.
- Reporting and prioritizing remediation recommendations to ensure that the security team is utilizing their time in the most effective way, while protecting the biggest security gaps.

Penetration Testing - Report Writing

It is not necessary that an experienced penetration tester can write a good report, as writing report of penetration testing is an art that needs to be learnt separately.

What is Report Writing?

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester's personal experience. Once the report is prepared, it is shared among the senior management staff and technical team of target organizations. If any such kind of need arises in future, this report is used as the reference.

Report Writing Stages

Due to the comprehensive writing work involved, penetration report writing is classified into the following stages −

- Report Planning
- Information Collection
- Writing the First Draft
- Review and Finalization

Report Planning

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing. This part describes why the testing is conducted, what the benefits of pen are testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are −

- **Objectives** − It describes the overall purpose and benefits of pen testing.
- **Time** − Inclusion of time is very important, as it gives the accurate status of the system. Suppose, if anything wrong happens later, this report will save the tester, as the report will illustrate the risks and vulnerabilities in the penetration testing scope during the specific period of time.
- **Target Audience** − Pen testing report also needs to include target audience, such as information security manager, information technology manager, chief information security officer, and technical team.
- **Report Classification** − Since, it is highly confidential which carry server IP addresses, application information, vulnerability, threats, it needs to be classified properly. However, this classification needs to be done on the basis of target organization which has an information classification policy.
- **Report Distribution** − Number of copies and report distribution should be mentioned in the scope of work. It also needs to mention that the hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver's name.

Information Collection

Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the methods, he also needs to mention about the systems and tools, scanning results, vulnerability assessments, details of his findings, etc.

Writing the First Draft

Once, the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

Review and Finalization

Once the report is drafted, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.

Content of Penetration Testing Report

Following is the typical content of a penetration testing report −

Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

Methodology

- Planning
- Exploitation
- Reporting

Detail Findings

- Detailed systems information
- Windows server information

References

- Appendix

Penetration Testing - Ethical Hacking

The fast growth of the internet has changed the way of life for everyone. These days, most of the private and public works are internet dependent. Government's all secret working plans, and operations are internet based. All these things made the life very simple and easily accessible.

But with the good news, there is also a dark face of this development i.e., the criminal hacker. There is no geopolitical limitation of these criminal hackers, they can hack any system from any part of the world. They can damage confidential data and credit history very badly.

Therefore, to protect from the criminal hackers, the concept of the ethical hacker evolved. This chapter discusses the concept and the role of an ethical hacker.

Who are Ethical Hackers?

Ethical hackers are the computer experts who are legally allowed to hack a computer system with the objective to protect from the criminal hackers. An ethical hacker identifies the vulnerabilities and risks of a system and suggests how to eliminate them.

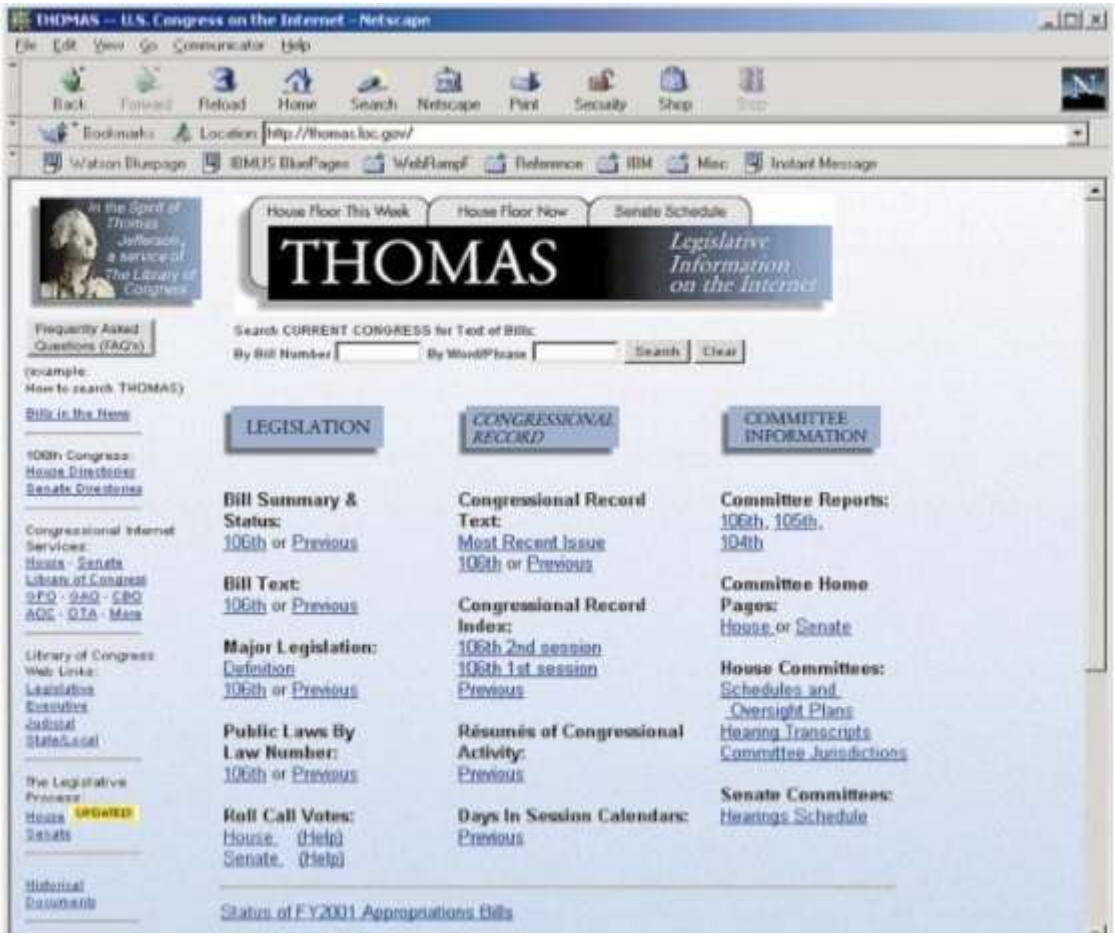
Who are Criminal Hackers?

Criminal hackers are those computer programming experts who hack others systems with the intention to steal data, steal money, defame others credit, destroy others data, blackmail someone, etc.

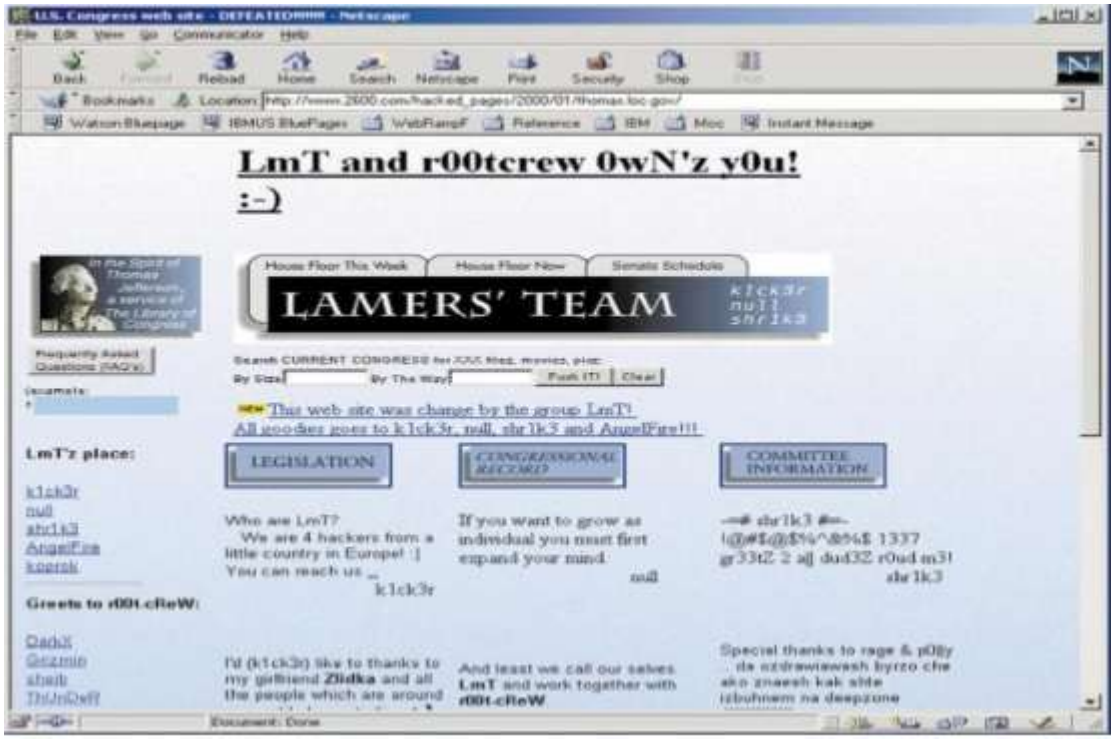
What can Criminal Hackers do?

Once a system is hacked, a criminal hacker can do anything with that system. The following two images C.C. Palmer, which is published on pdf.textfiles.com, illustrates a simple example of a hacked page −

Here is a screenshot of a webpage taken before it was hacked −



And, here is the screenshot of the same webpage after it was hacked −



What are the Skill-Sets of Ethical Hackers?

Expert ethical hackers have the following skill-sets to hack the system ethically

- They must be trustworthy.
- Whatever the risks and vulnerabilities, they discover while testing the system, they have to keep them confidential.
- Clients provide confidential information about their system infrastructure such as IP address, password, etc. Ethical hackers need to keep this information confidential.
- Ethical hackers must have sound knowledge of computer programming, networking and hardware.
- They should have good analytical skills to analyze the situation and speculate the risk in advance.
- They should have the management skill along with patience, as pen testing can take one day, one week, or even more.

What do Ethical Hackers do?

Ethical hackers, while performing penetration testing, basically try to find the answers to the following questions −

- What are the weak points that a criminal hacker can hit?
- What can a criminal hacker see on the target systems?
- What can a criminal hacker do with that confidential information?

Moreover, an ethical hacker is required to address adequately the vulnerabilities and risks, which he found to exist in the target system(s). He needs to explain and suggest the avoidance procedures. Finally, prepare a final report of his all ethical activities that he did and observed while performing penetration testing.

Types of Hackers

Hackers are normally divided into three categories.

Black Hat Hackers

A "black hat hacker" is an individual who has an extensive computer software as well as hardware and his purpose is to breach or bypass internet security of someone else. Black hat hackers are also popular as crackers or dark-side hackers.

White Hat Hackers

The term "white hat hacker" refers to an ethical computer hacker who is a computer security expert, specialized in penetration testing and in other associated testing methodologies. His primary role is to ensure the security of an organization's information system.

Grey Hat Hacker

The term "grey hat hacker" refers to a computer hacker who cracks computer security system whose ethical standards fall somewhere between purely ethical and solely malicious.

Penetration Testing Vs. Ethical Hacking

Penetration testing is very closely related to ethical hacking, so these two terms are often used interchangeably. However there is a thin line of difference between these two terms. This chapter provides insights into some basic concepts and fundamental differences between penetration testing and ethical hacking.

Penetration Testing

Penetration testing is a specific term and focuses only on discovering the vulnerabilities, risks, and target environment with the purpose of securing and taking control of the system. Or in other words, penetration testing targets respective organization's defense systems consisting of all computer systems and its infrastructure.

Ethical Hacking

On the other hand, ethical hacking is an extensive term that covers all hacking techniques, and other associated computer attack techniques. So, along with discovering the security flaws and vulnerabilities, and ensuring the security of the target system, it is beyond hacking the system but with a permission in order to safeguard the security for future purpose. Hence, we can that, it is an umbrella term and penetration testing is one of the features of ethical hacking.

The following are the major differences between Penetration testing and Ethical hacking which is listed in the following table −

Penetration Testing	Ethical Hacking
A narrow term focuses on penetration testing only to secure the security system.	A comprehensive term and penetration testing is one of its features.
A tester essentially does need to have a comprehensive knowledge of everything rather required to have the knowledge of only the specific area for which he conducts pen testing.	An ethical hacker essentially needs to have a comprehensive knowledge of software programming as well as hardware.
A tester not necessarily required to be a good report writer.	An ethical hacker essentially needs to be an expert on report writing.
Any tester with some inputs of penetration testing can perform pen test.	It requires to be an expert professional in the subject, who has the obligatory certification of ethical hacking to be effective.
Paper work in less compared to Ethical hacking.	A detailed paper works are required, including legal agreement etc.
To perform this type of testing, less time required.	Ethical hacking involves lot of time and effort compared to Penetration testing.
Normally, accessibility of whole computer systems and its infrastructure doesn't require. Accessibility is required only for the part for which the tester performing pen testing.	As per the situation, it normally requires a whole range of accessibility all computer systems and its infrastructure.

Since penetration techniques are used to protect from threats, the potential attackers are also swiftly becoming more and more sophisticated and inventing new weak points in the current applications. Hence, a particular sort of single penetration testing is not sufficient to protect your security of the tested systems.

As per the report, in some cases, a new security loophole is discovered and successful attack took place immediately after the penetration testing. However, it does not mean that the penetration testing is useless. It only means that, this is true that with thorough penetration testing, there is no guarantee that a successful attack will not take place, but definitely, the test will substantially reduce the possibility of a successful attack.

Penetration Testing - Limitations

Because of the swift pace of developments in the field of information and technology, the success story of penetration testing is comparatively short-lived. As more protection to the systems is required, more often than you need to perform penetration testing in order to diminish the possibility of a successful attack to the level that is appreciated by the company.

Following are the major limitations of Penetration Testing −

- **Limitation of Time** − As all of us know, penetration testing is not at all time bound exercise; nevertheless, experts of penetration testing have allotted a fixed amount of time for each test. On the other hand, attackers have no time constrains, they plan it in a week, month, or even years.
- **Limitation of Scope** − Many of the organizations do not test everything, because of their own limitations, including resource constraints, security constraints, budget constraints, etc. Likewise, a tester has limited scope and he has to leave many parts of the systems that might be much more vulnerable and can be a perfect niche for the attacker.
- **Limitation on Access** − More often testers have restricted access to the target environment. For example, if a company has carried out the penetration test against its DMZ systems from all across its internet networks, but what if the attackers attack through the normal internet gateway.
- **Limitation of Methods** − There are chances that the target system can crash during a penetration test, so some of the particular attack methods would likely be turned off the table for a professional penetration tester. For example, producing a denial of service flood to divert a system or network administrator from another attack method, usually an ideal tactic for a really bad guy, but it is likely to fall outside of the rules of engagement for most of the professional penetration testers.
- **Limitation of Skill-sets of a Penetration Tester** − Usually, professional penetration testers are limited as they have limited skills irrespective of their expertise and past experience. Most of them are focused on a particular technology and having rare knowledge of other fields.
- **Limitation of Known Exploits** − Many of the testers are aware with only those exploits, which are public. In fact, their imaginative power is not as developed as attackers. Attackers normally think much beyond a tester’s thinking and discover the flaw to attack.

- **Limitation to Experiment** − Most of the testers are time bound and follow the instructions already given to them by their organization or seniors. They do not try something new. They do not think beyond the given instructions. On the other hand, attackers are free to think, to experiment, and to create some new path to attack.

Moreover, penetration testing can neither replace the routine IT security tests, nor it can substitute a general security policy, but rather, penetration testing supplements the established review procedures and discovers new threats.

Penetration Testing - Remediation

Penetration testing efforts − however thorough they may be − cannot always ensure an exhaustive discovery of every instance where a security control's effectiveness is insufficient. Identifying a cross-site scripting vulnerability or risk in one area of an application may not definitely expose all instances of this vulnerability present in the application. This chapter illustrates the concept and utility of remediation.

What is Remediation?

Remediation is an act of offering an improvement to replace a mistake and set it right. Often the presence of vulnerability in one area may indicate weakness in process or development practices that could have replicated or enabled similar vulnerability in other locations. Therefore, while remediating, it is important for the tester to carefully investigate the tested entity or applications with ineffective security controls in mind.

Because of these reasons, the respective company should take steps to remediate any exploitable vulnerability within a reasonable period of time after the original penetration test. In fact, as soon as the company has completed these steps, the pen tester should perform a retest to validate the newly implemented controls which are capable to mitigate the original risk.

The remediation efforts extending for a longer period after the initial pen test possibly require performing a new testing engagement to ensure accurate results of the most current environment. This determination should be made after a risk analysis of how much change has occurred since the original testing was completed.

Moreover, in specific conditions, the flagged security problem may illustrate a basic flaw in respective environment or application. Therefore, the scope of a retest should consider whether any changes caused by remediation identified from the test are classified as significant. All changes should be retested; however, whether an entire system retest is necessary or not will be determined by the risk assessment of the changes.

Penetration Testing - Legal Issues

Before allowing someone to test sensitive data, companies normally take measures regarding the availability, confidentiality, and integrity of data. For this agreement to be in place, legal compliance is a necessary activity for an organization.

The most important legal regulations which have to be observed when establishing and maintaining security and authorization systems are presented below in context for using in implementing penetration tests.

What are the Legal Issues?

Following are some of the issues which may arise between a tester and his client −

- The tester is unknown to his client – so, on what ground, he should be given access of sensitive data
- Who will take the guarantee of security of the lost data?
- The client may blame for the loss of data or confidentiality to tester

Penetration testing may affect system performance, and can raise confidentiality and integrity issues; therefore, this is very important, even in an internal penetration testing, which is performed by an internal staff to get permission in writing. There should be a written agreement between a tester and the company/organization/individual to clarify all the points regarding the data security, disclosure, etc. before commencing testing.

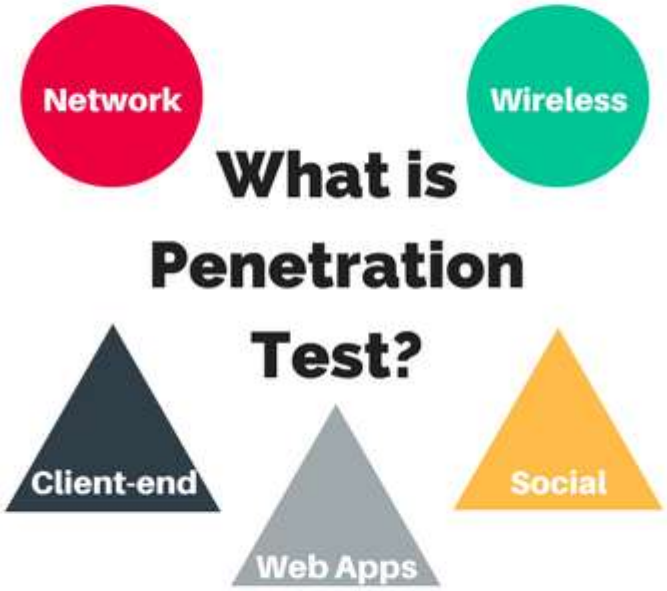
A **statement of intent** should be drawn up and duly signed by both the parties prior to any testing work. It should be clearly outlined that the scope of the job and that, you may and may not be doing while performing vulnerability tests.

For the tester, it is important to know who owns the business or systems which are being requested to work on, and the infrastructure between testing systems and their targets that may be potentially affected by pen testing. The idea is to make sure;

- **the tester** has the permission in writing, with clearly defined parameters.
- **the company** has the details of its pen tester and an assurance that he would not leak any confidential data.

A legal agreement is beneficial for both the parties. Remember, regulations change from country to country, so keep yourself abreast with the laws of your respective country. Sign an agreement only after considering the respective laws.

Five Types of Penetration Test for Successful Pen Testing



1. Network Service Tests.

This type of pen test is the most common requirement for the pen testers. It aims to discover vulnerabilities and gaps in the network infrastructure of the clients. Since the network could have both internal and external access points, so it is mandatory to run tests locally at the client site and remotely from the outer world.

The testers should target the following network areas in their penetration tests.

- Firewall config testing.
- Stateful analysis testing.
- Firewall bypass testing.
- IPS deception.
- DNS level attacks which include.
    - Zone transfer testing.
    - Switching or routing based testing.
    - Any miscellaneous network parameter testing.

Also, there are a set of software modules which the penetration test should cover are as follows.

- SSH client/server tests.
- Network databases like MYSQL/SQL Server.
- Exchange or SMTP mail servers.
- FTP client/server tests.

2. Web Application Tests.

It is more of a targeted test, also, more intense and detailed. Areas like web applications, browsers, and their components like ActiveX, Applets, Plug-ins, Scriptlets fall in the scope of this type of pen testing.

Since this test examines the end points of each web apps that a user might have to interact on a regular basis, so it needs thorough planning and time investment.

Also, with the increase in threats coming from the web applications, the ways to test them are continuously evolving.

3. Client Side Tests.

The goal of these tests is to pinpoint security threats that emerge locally. For example, there could be a flaw in a software application running on the user's workstation which a hacker can easily exploit.

These may be programs or applications like Putty, Git clients, Sniffers, browsers (Chrome, Firefox, Safari, IE, Opera), and even presentation as well as content creation packages like MS Power Point, Adobe Page Maker, Photoshop, and media players.

In addition to third-party software, threats could be home grown. Using uncertified OSS (open source software) to create or extend home made application could cause severe threats that one can't even anticipate. Therefore, these locally developed tools should also pass through the penetration test cycle.

4. Wireless Network Tests.

This test intends to analyze the wireless devices deployed on the client site. The list of devices include items like tablets, laptops, notebooks, iPods, smartphones, etc. Apart from the gadgets, the penetration tester should consider preparing tests for the following.

- Protocols used for configuring Wireless – It'll help find out the weak areas.
- Access points for Wireless setup – It'll enable in identifying the ones violating the access rights.

Usually, such tests should take place at the customer end. The hardware used to run pen tests need to connect with the wireless system for exposing vulnerability.

5. Social Engineering Tests.

This type of test also run as an important part of penetration testing. It paves ways for verifying the "Human Network" of an organization. This pen test imitates attacks which the

employees of a company could attempt to initiate a breach. However, it can further split up into two subcategories.

a. Remote Tests.

It intends to trick an engineer (employee) to compromise confidential data using electronic means. The tester could conduct such an attack via a phishing email campaign.

b. Physical Tests.

This type of test requires a direct contact with the subject to retrieve the sensitive information. It might involve human handling tactics like Dumpster Diving, Imitation, and Intimidation or convince the subject via phone calls.

Please note that you must inform the appropriate people before conducting the social engineering penetration test. Also, remember to emulate real world exploit instead of playing a movie scene.

Summary

Penetration test not only assists in discovering the actual and exploitable security threats but also provides their mitigation. By performing a pen test, we can make sure to identify the vulnerabilities which are critical, which are not significant and which are false positives.