PENETRATION TESTING

ASSESS SYSTEMS FOR SECURITY GAPS & VULNERABILITIES

An in-depth look at the latest
pen testing types, phases, and solutions.

LIFARS
your digital world, **secured**

CONTENTS

OVERVIEW 3

TYPES OF PENETRATION TESTS..... 5

BASED ON LOCATIONS & TYPES..... 5

BASED ON VISABILITY..... 8

BASED ON DEPTH..... 10

PEN TESTING APPROACH 12

PHASES OF PEN TESTING..... 12

TOOLS & TECHNIQUES..... 18

LIFARS PEN TESTING SOLUTION..... 19

OVERVIEW

Penetration Testing Defined

Penetration testing, also known as pen testing, is an authorized attempt into an IT system to evaluate its security by exploiting the existing vulnerabilities in the system. Generally, pen testing is not a one-time procedure. As a common practice, organizations hire security experts to perform pen testing on a regular basis, or outsource it to a service provider. Post testing, reports are generated and used to check the efficiency of the security measures currently employed by the organization.

The following vulnerabilities are checked during the testing:

- Operating systems
- Flaws in services and applications
- Improper system configurations
- Risky end-user behaviors

How it Works

Penetration testing is typically performed using automated or manual tools to systemically compromise various points of exposure such as servers, mobile devices, computers, endpoints, web applications, wireless networks, and other such network devices. If a system is compromised during the testing, testers use this compromised system to exploit other internal resources – to gain access to highly sensitive data.

The generated report is then presented to network engineers to make the required changes in the network. The fundamental purpose of penetration testing is to measure the efficiency of the defense mechanisms put in place by the organization and to evaluate the loss if these mechanisms are breached.

OVERVIEW

Why Pen testing?

The main reasons why an organization should opt for penetration testing services are:

- To identify security risks and prioritize them accordingly
- To avoid network downtime and recurrent losses
- To become compliant with regulatory requirements
- To avoid penalties & fines
- To preserve the loyalty of customers and maintain a good corporate image

The Latest Statistics on Network Vulnerabilities

According to a recent survey conducted by Barkly:

- Of the organizations that suffered cyber-attacks in 2016
  - 52% are making no changes in their cyber security policy
  - 31% are making significant changes in their cyber security policy
  - 45% are expecting to have the same budget for cyber-security
  - 38% are expecting to have an increased budget for the next year
- Over 4000 ransomware attacks have occurred daily since the beginning of 2016

Businesses and organizations hire a pen tester or a service provider as a proactive approach to ensure safety and security of their network and the data associated with it. According to a recent Forbes article on cyber-attacks, 60% of small businesses that suffer a data breach go out of business within six months, while a recent study conducted by IBM suggested that the average cost of a data breach was approximately $4 million in 2016. This study adds that there has been a 29% increase in the total cost of data breaches since 2013. It goes without saying that investing in a penetration test or a service provider to protect against a breach, would cost organizations significantly less.

TYPES OF PEN TESTING

Based on Location & Types

Penetration testing is categorized into different types, such as: External Network Pen Test, Internal Network Pen Test, Web Application Pen Test, Mobile Pen Test, and Social Engineering.

1. External Network Pen Test

In an External Network Pen Test, tests on an organization's network are performed from outside the organization. This type of testing is usually conducted using the Internet or Extranet. Testers may or may not be well-aware of the organization's infrastructure. The disclosure of the information related to the network and the connected devices is completely up to the organization. A tester begins with the information that is already publicly available, and then performs the test on externally visible servers such as the DNS, email server, web server, or firewalls.

External testing is a more traditional and the most common type of penetration testing. It depends completely on the ability of the tester to attack an organization's network from the outside. To access a particular network or the VPN, a tester needs to exploit an existing vulnerability in the system or trick a user in giving up personal information such as username and password.

2. Internal Network Pen Test

Internal Pen Test takes a completely different approach from external testing. It is somewhat similar to an insider's attack. In this testing, a tester has some authorized access to the organization's internal network. Often times, the person behind the insider's attack is either a disgruntled employee or a visitor with standard user privileges. The objective of this type of testing is to check for any threats to the organization if the network perimeter is successfully penetrated by an attacker.

TYPES OF PEN TESTING

In Internal Pen Test, a tester has knowledge of what is considered important information within the network. The tester has good knowledge of the end points where the attack should take place. For these reasons, an insider's attack can potentially be even more dangerous than other types of attack. Although the techniques used in internal testing are similar to the ones used in external testing, the results can vary a great extent.

3. Web Application Pen Test

Web Application Pen Test focuses only on the security of the web applications of an organization. This process involves checking a web application for weaknesses, vulnerabilities, and other such technical flaws. The issues found during a Web Application Pen Test are presented to the system administrator along with the measured impacts of each issue.

4. Mobile Pen Test

Most businesses and employees use mobile phones as part of their work devices. For example, various teams working together keep track of work progress using tools like Trello and Asana. However, as businesses embrace the benefits of new technologies, they may also open themselves to risks. Just as other devices connected to the network of an organization are tested, mobile devices used within the organization should also be tested.

TYPES OF PEN TESTING

4. Social Engineering

Social engineering is part of a strategy cyber attackers use that relies mostly on human interaction. It usually involves attackers misleading people to break standard security practices. In social engineering, a tester focusses on the technical, psychological, and physiological aspects of a person. Social engineering generally involves three methodologies: phishing, vishing, and impersonation. For example, an attacker calls an employee and identifies him or herself to be calling from a bank and requires a few details about the company's account. The employee might share information that is confidential. Hence, the best way to prevent leakage of any sensitive data through social engineering is regular awareness sessions.

TYPES OF PEN TESTING

Based on Visibility

Penetration testing is categorized also into Overt, Covert, Exercise, and Automated Pen Tests.

1. Overt Pen Test

In Overt Pen Test, the testers work with an organization's IT team to identify potential threats. The main benefit of this type of testing is that testers have complete access to an insider's knowledge. A tester can try to attack the network without any fear of getting blocked.

One of the disadvantages of overt tests is that it might not effectively test an organization's incident response policy, or test the efficiency of intrusion systems. In overt systems—some penetration testing steps, such as intelligence gathering, are not performed.

2. Covert Pen Test – Red Team Pen Test Exercise

Unlike overt testing, authorized Covert Pen Test involves the simulation of a real attack. No one in the organization is aware of the tests being conducted. This exercise is to test the ability of the IT security team and evaluate how they detect and respond to a cyber-attack. Compared to overt testing, covert testing requires more skilled testers, it is more time-consuming, and will have a higher fee.

Generally, covert testing is preferred over overt testing, as it is an authorized real-life attack on an organization. In covert testing, a tester does not only try to find vulnerabilities in the system but also tries to attempt to find the easiest way to gain undetected access to a system. A Covert Pen Test may also be referred to as a Red Team Pen Test Exercise. A Red Team is an organization that challenges the security of a company to improve its policies.

TYPES OF PEN TESTING

3. Automated Pen Test

While performing penetration tests, the testers conduct deliberate attacks on the network of an organization. The reason behind conducting such tests is to assume the mindset of a hacker. The testers use the same techniques and tools as used by real attackers.

Since the nature of penetration testing is manual, many organizations try to automate certain parts of the testing procedure. For example, the testers use various vulnerability scanners to test multiple systems at once.

TYPES OF PEN TESTING

Based on Depth

Penetration testing is categorized into three types: Black Box, White Box, and Gray Box. Depth implies the level of knowledge the testers have of the organization.

1. Black Box Testing

In Black Box Pen Testing, the testers have no specific knowledge of the internal workings of an organization's systems. They do not have access to the source code and are unaware of the architecture.

Similar to covert testing, this type of penetration testing resembles a real attack. Since the testers have no knowledge of the internal systems in place, finding bugs and vulnerabilities in a system takes a significant amount of time. In practical use, black box testing is limited to dynamic analysis by using automated scanning tools and manual pen testing.

2. White Box Testing

In White Box Pen Testing, the testers have full knowledge of the system and have access to the entire network. The complete knowledge of an organization's network makes it easier for the testers to find vulnerabilities since they don't have to use the hit and trial method of black box testing. Also, since the testers know what must be tested, the entire network is covered during this test.

However, considering the complexity of network architectures deployed these days, white box testing introduces several challenges for testers performing various tests and analyzing results. To make this easier, the testers use a number of specialized tools such as, source code analyzers and debuggers.

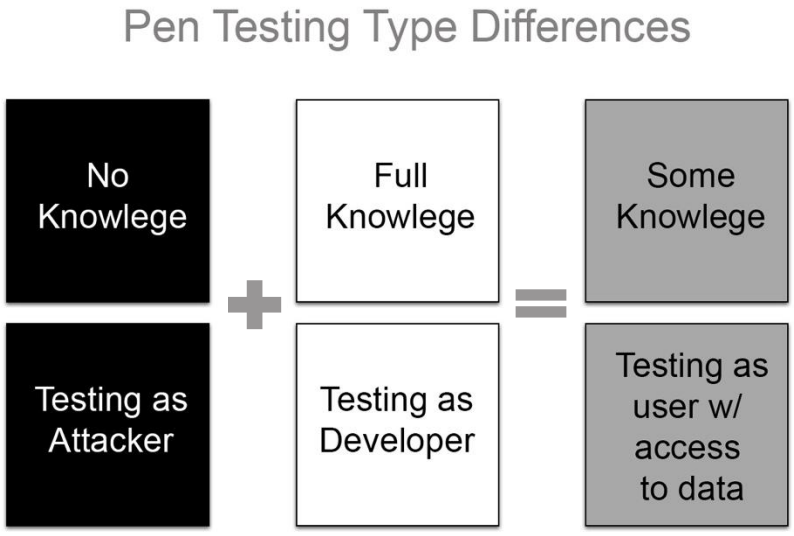
TYPES OF PEN TESTING

3. Gray Box Testing

In Grey Box Pen Testing, the testers have at least some knowledge of the internals of an organization's system. Gray box testing is a combination of both black and white black box testing.

It allows the testers to run automated tests using specialized tools and manual penetration tests against a network or a target application. The testers try to gain access to more sensitive and critical data about the target with the help of already available information. This increment in knowledge is then used to identify vulnerabilities in the target.

With the help of gray box testing, testers can find vulnerabilities in the target system with a comparatively less amount of effort.

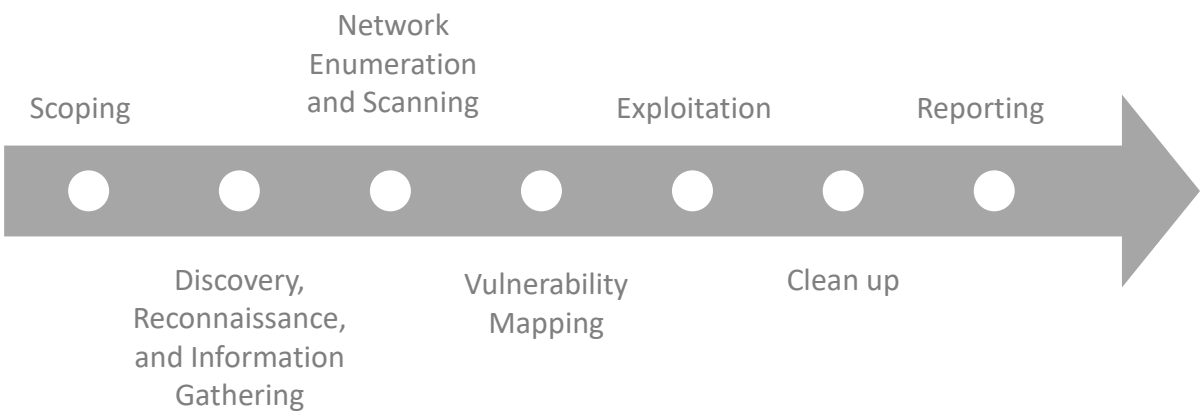


PEN TESTING APPROACH

Phases of Penetration Testing

There are seven industry accepted phases of penetration testing:

(1) Scoping, (2) Discovery, Reconnaissance, and Information Gathering, (3) Network Enumeration and Scanning, (4) Vulnerability Mapping, (5) Exploitation, (6) Clean up, and (7) Reporting.



PEN TESTING APPROACH

Phases of Penetration Testing

1. Scoping

The first phase of a penetration test involves the planning and preparation required to carry out a successful test. Together the tester and the organization define and agree upon the goals and objectives for the test.

The most common objectives of penetration testing are:

- Identifying vulnerabilities in the systems and improving the security
- Involving a third-party to perform the tests to assume a hacker-like mindset
- Checking the response time of the internal IT team

2. Discovery, Reconnaissance, and Information Gathering

In this phase, the main objective is to gather information about the target. This information is then used to plan more effective attacks on the systems. The testers perform the task of information gathering either actively or passively, i.e. being directly connected to the target network or being connected through an intermediary.

To discover information about an organization's systems, a tester uses automated tools to scan the target. The target is scanned using a number of tools for discovering existing vulnerabilities. The tools being used to carry out these scans have a database of their own, which provides details about the latest vulnerabilities.

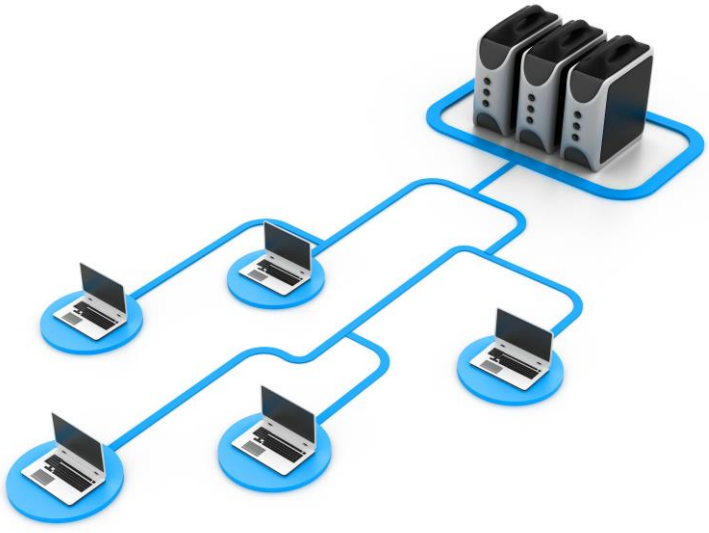
PEN TESTING APPROACH

Phases of Penetration Testing

While performing these discovery, reconnaissance, and information gathering scans, a tester would be able to find the followings:

- **Network Discovery**: Discovering systems, servers, and other network devices connected to the network
- **Host Discovery**: Finding the open ports on the network devices
- **Service Fingerprinting**: Performing scans over open ports to discover the services and the versions running on them

This phase plays an important role in the entire testing process as the information gathered in this phase is used in the next phases, which perform a specific task such as covering tracks or maintaining the presence inside a network.



PEN TESTING APPROACH

Phases of Penetration Testing

3. Network Enumeration and Scanning

The third phase of penetration testing overlaps with the second phase to an extent. In the second phase, the testers try to get as much as information about an organization, while the third phase is only limited to its network. Using Network Enumeration, the testers discover hosts and devices on the network. Various overt discovery protocols such as ICMP and SNMP are used to scan the network. The hosts and devices are fingerprinted such that testers are on the lookout for well-known services.

After discovering the services running on a host or a device, tester check for any existing vulnerability in those services. A good example of this phase is using a vulnerability scanner on the target network or using a Network Mapper to find the versions of the services running on a host.

4. Vulnerability Mapping

In this phase, the results of all automated and manual tests and scans that have been performed are analyzed. This process enables testers to follow a systematic approach in identifying, quantifying, and ranking vulnerabilities.

After mapping and ranking is complete, testers select the most critical vulnerabilities to be exploited in the next phase.

PEN TESTING APPROACH

Phases of Penetration Testing

5. Exploitation

This phase is the most important phase in the entire testing scenario as it is indicative of the test's success (or failure). Testers focus on gaining access to a system or a resource by exploiting the vulnerabilities or bypassing the security restrictions. The activities in the exploitation phase are well planned and precisely carried out with the help of information gathered from the systems in previous phases. Once testers gain entry into a system, they try to identify the high-value assets of an organization.

While attacking a network, testers also simulate the infrastructure of the organization to ensure that the exploitation of the vulnerabilities is successful. The tools and techniques used in the second phase (Discovery, Reconnaissance and Information Gathering) play an important role in successful Exploitation since the exploits are customized according to the vulnerabilities found in the system.

These customized exploits are the publicly available exploits that are used to target specific versions of operating system or services. Testers should be able to customize these publicly available exploits and deploy them to different operating systems to successfully compromise the systems.

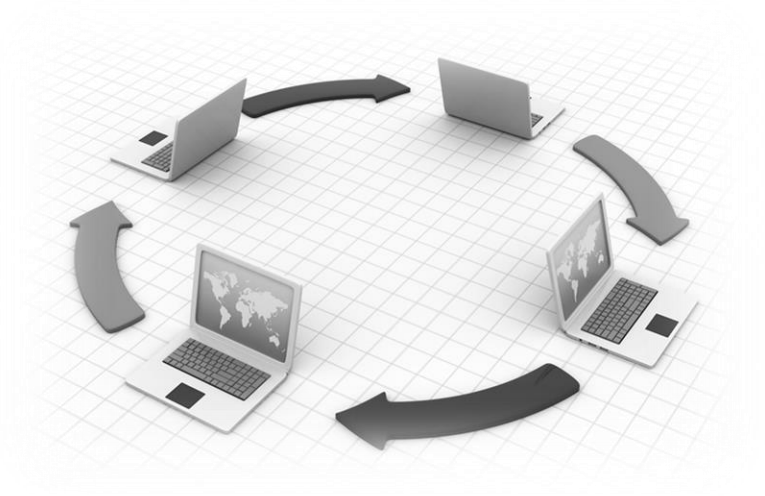
PEN TESTING APPROACH

Phases of Penetration Testing

6. Clean up

After gaining access to a network, maintaining it is also a crucial task. Testers try to extract as much data as possible, but during this entire process they must remain stealthy so their presence remains undetected. To maintain the access, testers use a wide range of techniques such as—privilege escalation, installing a backdoor, sending phishing emails, etc.

If a tester does not want to be caught while performing tests on a network, he must ensure that his digital footprints cannot be found inside the network. In other words, he has to hide the intrusion, delete the necessary logs on his intrusion and the downloaded backdoor, and get rid of any other digital evidence related to the test.



PEN TESTING APPROACH

Phases of Penetration Testing

7. Reporting

The activities from the previous six phases are documented properly and presented to the organization (the client). The report includes scope, information, attack path, vulnerabilities, attack vectors uses, and suggestions & remediation.
The report provided by the testers may include the following sections:

- **Introduction** – This section includes basic information of the test: objective, scope, approach, strength, threats, contact information, etc.
- **Information Gathering** – The second section of the report specifies how the information was gathered. The information is then divided into various types of intelligence such as active, passive, corporate, and personnel.
- **Vulnerability Assessment & Confirmation –** The third section outlines the procedure used by the testers to find the vulnerabilities in the various systems. The testers also confirm the presence of existing vulnerabilities, if any.
- **Risk & Exposure** – For all the vulnerabilities mentioned in the previous section, the testers, in this section, specify the risks associated with each of the noted vulnerabilities. After completing the risk analysis part, testers list the various types of losses that can occur due to such vulnerabilities. These losses vary from financial losses to loss of customer base.
- **Conclusion** – This is the last section of the report and it is an overall and a final overview of the entire testing procedure. This section informs the management about the basic requirements for improving the security of IT infrastructure of their organization. It is ideal to end this section of a positive note by providing suitable guidelines for the future.

PEN TESTING APPROACH

Tools & Techniques

Ransomware or other cyber virus attacks are more common these days and can affect millions of company computers. For businesses, the key to fighting and protecting themselves against these attacks is to conduct pen tests throughout the year. Penetration testing is the only way to simulate real-world attacks and discover the vulnerabilities in your system before a hacker does. Even if one vulnerability is discovered by a hacker, the consequences are costly.

According to the recent pen testing report conducted by CTF365, 99.99% of testers prefer Kali Linux Operating System while performing penetration tests over a network. The table given below displays some of the recommended tools for carrying out a penetration test over a network.

Objective	First Choice	Second Choice
Pen testing framework	Metasploit	Core Impact
Password Crackers	John the Ripper	Hydra
Network Scanners	nmap	netcat
Packet Sniffing	Wireshark	Ettercap
Wi-Fi Pentest	aircrack-ng	KisMet
Bluetooth Pentest	BlueScanner	FTS4BT
Website Scanning	Burp Suite	Nessus

** Please note that the given tools have not been classified as first choice or second choice on the basis of their quality or any such factor, they have been put into two different categories on the basis of the number of testers preferring one over the other.*

LIFARS PEN TESTING SOLUTION

EXPERIENCED TEAM

LIFARS seasoned penetration testing team is one of the best in the space. Each of our senior staff has 10+ years of experience in security assessments and an average of two decades of IT-related experience, delivering the best quality of service in the industry.

CLOUD TESTING

LIFARS' expert team excels in navigating the security assessment peculiarities of a shared provider tenant model. Whether you deploy to IaaS, PaaS, or SaaS, we will work with you and your provider to identify and assess relevant layers in scope.

APPLICATION TESTING

Our tests are expertly designed to detect information security vulnerabilities within computer software–including web-based applications, bespoke software applications, Linux, Windows, and Mac software, databases, mobile operating systems and apps, and other programs.

WEBSITE TESTING

LIFARS' seasoned penetration testers can identify security flaws within your website or web application software by simulating an attack. As a result, we are able to thoroughly test your website for SQL injections, cross-site scripting vulnerabilities, server configuration problems, sensitive data leaks, and other weaknesses in your configuration.

HYBRID TESTING MODEL

We offer time or subscription based cost-effective models. Our hybrid approach integrates automation with manual testing by LIFARS' application security experts. We offer very high quality, scalability, and cost effectiveness.

SECURE CODE REVIEW

Besides dynamic testing, such as penetration testing, organizations should also consider Static Source Code Analysis. Secure Code Review is the industry standard for static Source Code Analysis. It is a process of auditing the application source code and identifying security gaps within an application, as a part of the secure SDLC process. The secure code review is a combination of human effort and the proficient use of security tools by our LIFARS certified experts.

LIFARS

your digital world, **secured**

Contact Us to Learn More

www.lifars.com | 212.222.7061 | info@lifars.com | Twitter: @LIFARSLLC

LIFARS is an Elite Cybersecurity Intelligence firm based in New York City specializing in: Incident Response, Digital Forensics, and Cybersecurity Intelligence.