**What is Penetration Testing?**

**or**

**Understanding penetration testing**

It’s the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.

The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system. Once the vulnerability is identified it is used to exploit the system in order to gain access to sensitive information.

A penetration test is also known as pen test and a penetration tester is also referred as an ethical hacker

We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing.

A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked.

Causes of vulnerabilities

* **Design and development errors**: There can be flaws in the design of hardware and software. These bugs can put your business-critical data at the risk of exposure.
* **Poor system configuration**: This is another cause of vulnerability. If the system is poorly configured, then it can introduce loopholes through which attackers can enter into the system & steal the information.
* **Human errors**: Human factors like improper disposal of documents, leaving the documents unattended, coding errors, insider threats, sharing passwords over phishing sites, etc. can lead to security breaches.
* **Connectivity**: If the system is connected to an unsecured network (open connections) then it comes in the reach of hackers.
* **Complexity**: The security vulnerability rises in proportion to the complexity of a system. The more features a system has, the more chances of the system being attacked.
* **Passwords**: Passwords are used to prevent unauthorized access. They should be strong enough that no one can guess your password. Passwords should not be shared with anyone at any cost and passwords should be changed periodically. In spite of these instructions, at times people reveal their passwords to others, write them down somewhere and keep easy passwords that can be guessed.
* **User Input**: You must have heard of SQL injection, buffer overflows, etc. The data received electronically through these methods can be used to attack the receiving system.
* **Management**: Security is hard & expensive to manage. Sometimes organizations lack behind in proper risk management and hence vulnerability gets induced in the system.
* **Lack of training to staff**: This leads to human errors and other vulnerabilities.
* **Communication**: Channels like mobile network, internet, telephone opens up security theft scope.

**Why Penetration testing?**

You must have heard of the WannaCry ransomware attack that started in May 2017. It locked more than 2 lakh computers around the world and demanded ransom payments in the Bitcoin cryptocurrency. This attack has affected many big organizations around the globe.

With such massive & dangerous cyber-attacks happening these days, it has become unavoidable to do penetration testing on regular intervals to protect the information systems against security breaches.

So, penetration testing is mainly required because:

– Financial or critical data must be secured while transferring it between different systems or over the network.  
– Many clients are asking for pen testing as part of the software release cycle.  
– To secure user data.  
– To find security vulnerabilities in an application.  
– To discover loopholes in the system.  
– To assess the business impact of successful attacks.  
– To meet the information security compliance in the organization.  
– To implement effective security strategy in the organization.

It’s very important for any organization to identify security issues present in internal network and computers. Using this information organization can plan a defense against any hacking attempt. User privacy and data security are the biggest concerns nowadays. Imagine if any hacker manages to get user details of social networking site like Facebook. The organization can face legal issues due to a small loophole left in a software system. Hence, big organizations are looking for PCI (Payment Card Industry) compliance certifications before doing any business with third-party clients.

What should be tested?

* Software (Operating system, services, application)
* Hardware
* Network
* Processes
* End-user behaviour

Penetration Testing Types:

**1) Social Engineering Test:**

In this test, attempts are being made to make a person reveal the sensitive information like password, business-critical data, etc. These tests are mostly done through phone or internet and it targets certain helpdesks, employees & processes.

Human errors are the main causes of security vulnerability. Security standards and policies should be followed by all staff members to avoid social engineering penetration attempt. Example of these standards includes not to mention any sensitive information in the email or phone communication. Security audits can be conducted to identify and correct process flaws.

**2) Web Application Test:**

Using software methods one can verify if the application is exposed to security vulnerabilities. It checks the security vulnerability of web apps and software programs positioned in the target environment.

**3) Physical Penetration Test:**

Strong physical security methods are applied to protect sensitive data. This is generally used in military and government facilities. All physical network devices and access points are tested for possibilities of any security breach. This test is not much relevant to the scope of software testing.

**4) Network Services Test**:

This is one of the most commonly performed penetration tests where the openings in the network are identified by which entry is being made in the systems on the network to check what kind of vulnerabilities are there. It can be done locally or remotely.

**5) Client-side test**:

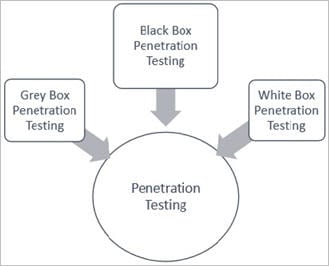
It aims to search and exploit vulnerabilities in client-side software programs.

**6) Remote dial-up war dial**:

It searches for modems in the environment and tries to login to the systems connected through these modems by password guessing or brute forcing.

**7) Wireless security test**: It discovers the open, unauthorized and less secured hotspots or Wi-Fi networks and connects through them.

The above 7 categories we have seen is one way of categorizing the types of pen tests. We can also organize the types of penetration testing into three parts as seen below:

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2012/06/Penetration-Testing.jpg)

**Let’s discuss this testing approaches one by one:**

* **Black Box Penetration Testing**: In this approach, the tester assesses the target system, network or process without the knowledge of its details. They just have very high level of inputs like URL or company name using which they penetrate into the target environment. No code is being examined in this method.
* **White Box Penetration Testing**: In this approach, the tester is equipped with complete details about the target environment – Systems, network, OS, IP address, source code, schema, etc. It examines the code and finds out design & development errors. It is a simulation of internal security attack.
* **Grey Box Penetration Testing**: In this approach, the tester has limited details about the target environment. It is a simulation of external security attack.

Pen Testing Techniques:

**1)** Manual penetration test  
**2)** Using automated penetration test tools  
**3)** Combination of both manual and automated process

The third process is more common to identify all kinds of vulnerabilities.

Penetration Testing Tools:

Automated tools can be used to identify some standard vulnerability present in an application. Pentest tools scan code to check if there is malicious code present which can lead to the potential security breach. Pentest tools can verify security loopholes present in the system by examining data encryption techniques and figuring out hard-coded values like username and password.

Criteria to select the best penetration tool:

– It should be easy to deploy, configure and use.  
– It should scan your system easily.  
– It should categorize vulnerabilities based on severity that needs an immediate fix.  
– It should be able to automate verification of vulnerabilities.  
– It should re-verify exploits found previously.  
– It should generate detailed vulnerability reports and logs.

Once you know what tests you need to perform you can either train your internal test resources or hire expert consultants to do the penetration task for you.

**Examples of Free and Commercial Tools:**

=> [Try the best Pen Test Tool Here](https://bit.ly/2G2N6hw)

* [Nmap](http://nmap.org/)
* [Nessus](http://www.nessus.org/)
* [Metasploit](http://www.metasploit.com/)
* [Wireshark](http://www.wireshark.org/)
* [OpenSSL](http://www.openssl.org/)
* [Cain & Abel](http://www.oxid.it/cain.html)
* THC Hydra
* [w3af](http://w3af.sourceforge.net/)

**Commercial services:**

* [Pure Hacking](http://www.purehacking.com/)
* [Torrid Networks](http://www.torridnetworks.com/)
* [SecPoint](http://www.secpoint.com/)
* [Veracode](http://www.veracode.com/)

You can also refer to the below list available at STH that talks about 37 powerful penetration testing tools: [37 Powerful Penetration Testing Tools For Every Penetration Tester](https://www.softwaretestinghelp.com/penetration-testing-tools/)

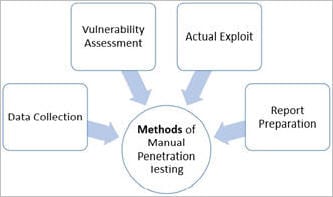
**Limitations of Pentest tools:** Sometimes these tools can flag false positive output which results in spending more developer time on analyzing such vulnerabilities which are not present.

Manual Penetration Test:

It’s difficult to find all vulnerabilities using automated tools. There are some vulnerabilities which can be identified by manual scan only. Penetration testers can perform better attacks on application based on their skills and knowledge of the system being penetrated. The methods like social engineering can be done by humans only. Manual checking includes design, business logic as well as code verification.

**Penetration Test Process:**  
Let’s discuss the actual process followed by test agencies or penetration testers. Identifying vulnerabilities present in the system is the first important step in this process. Corrective action is taken on these vulnerability and same penetration tests are repeated until the system is negative to all those tests.

We can categorize this process in following methods:

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2012/06/Methods-of-manual-penetration-testing.jpg)

**1) Data collection:** Various methods including Google search are used to get target system data. One can also use the web page source code analysis technique to get more info about the system, software and plugin versions. There are many free tools and services available in the market which can give you information like database or table names, DB versions, software versions, hardware used and various third-party plugins used in the target system.

**2) Vulnerability Assessment:** Based on the data collected in the first step one can find the security weakness in the target system. This helps penetration testers to launch attacks using identified entry points in the system.

**3) Actual Exploit:** This is a crucial step. It requires special skills and techniques to launch an attack on the target system. Experienced penetration testers can use their skills to launch an attack on the system.

**4) Result analysis and report preparation:** After completion of penetration tests detailed reports are prepared for taking corrective actions. All identified vulnerabilities and recommended corrective methods are listed in these reports. You can customize vulnerability report format (HTML, XML, MS Word or PDF) as per your organization needs.

Penetration testing sample test cases (test scenarios):

Remember this is not functional testing. In Pentest your goal is to find security holes in the system. Below are some generic test cases and not necessarily applicable for all applications.

**1)** Check if the web application is able to identify spam attacks on contact forms used on the website.  
**2)** Proxy server – Check if network traffic is monitored by proxy appliances. Proxy server makes it difficult for hackers to get internal details of the network thus protecting the system from external attacks.  
**3)** Spam email filters – Verify if incoming and outgoing email traffic is filtered and unsolicited emails are blocked. Many email clients come with inbuilt spam filters which need to be configured as per your needs. These configuration rules can be applied to email headers, subject or body.  
**4)** Firewall – Make sure entire network or computers are protected with Firewall. A Firewall can be a software or hardware to block unauthorized access to a system. A Firewall can prevent sending data outside the network without your permission.  
**5)** Try to exploit all servers, desktop systems, printers and network devices.  
**6)** Verify that all usernames and passwords are encrypted and transferred over secured connection like https.  
**7)** Verify information stored in [website cookies](https://www.softwaretestinghelp.com/website-cookie-testing-test-cases/). It should not be in readable format.  
**8)** Verify previously found vulnerabilities to check if the fix is working.  
**9)** Verify if there is no open port in the network.  
**11)** Verify all telephone devices.  
**12)** Verify WIFI network security.  
**13)** Verify all HTTP methods. PUT and Delete methods should not be enabled on a web server.  
**14)** Verify if the password meets the required standards. The password should be at least 8 characters long containing at least one number and one special character.  
**15)** Username should not be like “admin” or “administrator”.  
**16)** Application login page should be locked upon few unsuccessful login attempts.  
**17)** Error messages should be generic and should not mention specific error details like “Invalid username” or “Invalid password”.  
**19)** Verify if special characters, HTML tags and scripts are handled properly as an input value.  
**20)** Internal system details should not be revealed in any of the error or alert messages.  
**21)** Custom error messages should be displayed to end user in case of web page crash.  
**22)** Verify use of registry entries. Sensitive information should not be kept in the registry.  
**23)** All files must be scanned before uploading to the server.  
**24)** Sensitive data should not be passed in URLs while communicating with different internal modules of the web application.  
**25)** There should not be any hardcoded username or password in the system.  
**26)** Verify all input fields with long input string with and without spaces.  
**27)** Verify if reset password functionality is secure.  
**28)** Verify application for[SQL Injection](https://www.softwaretestinghelp.com/sql-injection-%E2%80%93-how-to-test-application-for-sql-injection-attacks/).  
**29)** Verify application for [Cross Site Scripting](https://www.softwaretestinghelp.com/security-testing-of-web-applications/).  
**31)** Important input validations should be done at server side instead of JavaScript checks at the client side.  
**32)** Critical resources in the system should be available to authorized persons and services only.  
**33)** All access logs should be maintained with proper access permissions.  
**34)** Verify user session ends upon log off.  
**35)** Verify that directory browsing is disabled on the server.  
**36)** Verify that all applications and database versions are up to date.  
**37)** Verify URL manipulation to check if a web application is not showing any unwanted information.  
**38)** Verify memory leak and buffer overflow.  
**39)** Verify if incoming network traffic is scanned to find Trojan attacks.  
**40)** Verify if the system is safe from Brute Force Attacks – a trial and error method to find sensitive information like passwords.  
**41)** Verify if system or network is secured from DoS (denial-of-service) attacks. Hacker can target network or a single computer with continuous requests due to which resources on target system gets overloaded resulting in the denial of service for legit requests.  
**42)** Verify application for HTML script injection attacks.  
**43)** Verify against COM & ActiveX attacks.  
**44)** Verify against spoofing attacks. Spoofing can be of multiple types – IP address spoofing, Email ID spoofing, ARP spoofing, Referrer spoofing, Caller ID spoofing, Poisoning of file-sharing networks, GPS spoofing.  
**45)** Check for uncontrolled format string attack – a security attack that can cause the application to crash or execute the harmful script on it.  
**46)** Verify XML injection attack – used to alter the intended logic of the application.  
**47)** Verify against canonicalization attacks.  
**48)** Verify if the error pages are displaying any information that can be helpful for a hacker to enter into the system.  
**49)** Verify if any critical data like the password is stored in secret files on the system.  
**50)** Verify if the application is returning more data than it is required.

These are just the basic test scenarios to get started with Pentest. There are hundreds of advanced penetration methods which can be done either manually or with the help of automation tools.