Learn Penetration Testing

Penetration testing is a type of security testing used to test the insecure areas of the system or application. The goal of this testing is to find all security vulnerabilities that are present in the system being tested. Vulnerability is the risk that an attacker can disrupt or gain authorized access to the system or any data contained within it

Vulnerabilities are usually introduced by accident during software development and implementation phase. Common vulnerabilities include design errors, configuration errors, software bugs etc.

Need of a Penetration testing:

WHY PENETRATION TESTING

???

???

???

7400+ NEW VULNERABILITIES DISCOVERED EVERY YEAR

92%

VULNERABILITIES CAN BE EXPLOITED REMOTELY

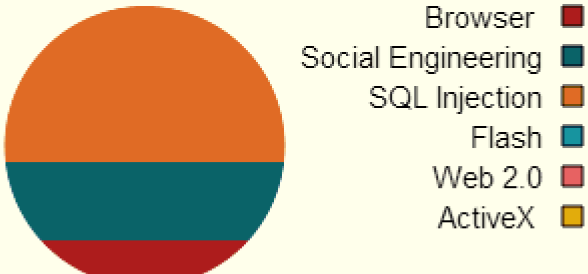
55%

ATTACKS AFFECT WEB APPLICATIONS

74%

VULNERABILITIES DO NOT HAVE A VENDOR PATCH BY END OF YEAR

TOP WEB ATTACK VECTORS



Penetration is essential in an enterprise because -

- Financial sectors like Banks, Investment Banking , Stock Trading Exchanges want their data to be secured , and penetration testing is essential to ensure security
- In case if the software system is already hacked and organization wants to determine whether any threats are still present in the system to avoid future hacks.
- Proactive Penetration Testing is the best safeguard against hackers

Types of Penetration testing:

The type of penetration test selected usually depends on the scope and whether the organization wants to simulate an attack by an employee, Network Admin (Internal Sources) or by External Sources .There are three types of Penetration testing and they are

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

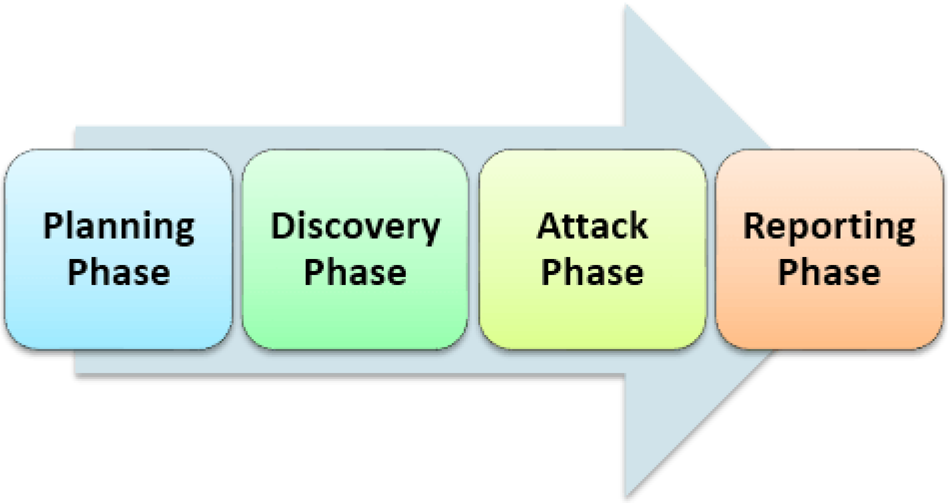
In black box penetration testing, tester has no knowledge about the systems to be tested .He is responsible to collect information about the target network or system.

In a white-box penetration testing, the tester is usually provided with a complete information about the network or systems to be tested including the IP address schema, source code, OS details, etc. This can be considered as a simulation of an attack by any Internal sources (Employees of an Organization).

In a grey box penetration testing, tester is provided with partial knowledge of the system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Steps in Penetration testing:

Following are activities needs to be performed to execute Penetration Test -



1. Planning phase
   1. Scope & Strategy of the assignment is determined
   2. Existing security policies, standards are used for defining the scope
2. Discovery phase
   1. Collect as much information as possible about the system including data in the system, user names and even passwords. This is also called as **FINGERPRINTING**
   2. Scan and Probe into the ports
   3. Check for vulnerabilities of the system
3. Attack Phase
   1. Find exploits for various vulnerabilities You need necessary security Privileges to exploit the system
4. Reporting Phase
   1. Report must contain detailed findings
   2. Risks of vulnerabilities found and their Impact on business
   3. Recommendations and solutions, if any

The prime task in penetration testing is to gather system information. There are two ways to gather information -

- 'One to one' or 'one to many' model with respect to host: A tester performs techniques in a linear way against either one target host or a logical grouping of target hosts (e.g. a subnet).
- 'Many to one' or 'many to many' model :The tester utilizes multiple hosts to execute information gathering techniques in a random, rate-limited, and in non-linear.

Tools of Penetration testing:

There is a wide variety of tools that are used in penetration testing and the important tools are:

1. NMap- This tool is used to do port scanning, OS identification, Trace the route and for Vulnerability scanning.
2. Nessus- This is traditional network based vulnerabilities tool.
3. Pass-The-Hash - This tool is mainly used for password cracking.
4. Cain and Abel- This tool mainly used for Password recovery, Network sniffing, Wireless scanning and VoIP.

Role and Responsibilities of Penetration Testers:

Penetration Testers job is to:

- Testers should collect required information from the Organization to enable penetration tests
- Find flaws that could allow hackers to attack a target machine
- Pen Testers should think & act like real hackers albeit ethically.
- Work done by Penetration testers should be reproducible so that it will be easy for developers to fix it
- Start date and End date of test execution should be defined in advance.
- Tester should be responsible for any loss in the system or information during the testing
- Tester should keep data and information confidential

Manual Penetration vs. automated penetration testing:

1. Manual testing requires expert professionals to run the tests whereas Automated test tools provides clear reports with less experienced professionals
2. Manual Testing requires excel and other tools to track it , but automation has centralized and standard tools -
3. In Manual testing, results vary from test to test but not in the case of Automated tests
4. Memory Cleaning up should be remembered by users , but automated testing will have comprehensive clean ups.

Limitations of Penetration testing:

Penetration Testing cannot find all vulnerabilities in the system .There are limitations of time , budget , scope , skills of Penetration Testers

Following will be side effects when we are doing penetration testing:

- Data Loss and Corruption
- Down Time
- Increase costs

Conclusion:

Testers should act like a real hacker and test the application or system and needs to check whether code is securely written. A penetration test will be effective if there is a well-implemented security policy. Penetration testing policy and methodology should be a place to make penetration testing more effective.