VIT UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING

Chapter 2: PEN TESTING

By
Dr. Ravi Verma

Contents To Be Discuss

- What Is Penetration Testing?
- Causes of Vulnerability
- Penetration Testing Tools and Companies
- Criteria for selecting the best penetration tool
- Recommended Penetration Testing Tools
- Other Free Tools
- Why Penetration Testing?
- Penetration Testing is mainly required for
- What Should Be Tested?

Contents To Be Discuss Cont. ...

- Penetration Testing Types
- Types of penetration testing into three parts
- Pen Testing Techniques
- We can categorize this process in the following methods
- Conclusion

What Is Penetration Testing?

- We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing.
- A penetration test will tell whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest countermeasures which can be taken to reduce the risk of the system being hacked.

Causes of Vulnerability

- **Design and Development Errors**: There can be flaws in the design of hardware and software. These bugs can put your business-critical data at 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 within the reach of hackers.

Causes of Vulnerability Cont..

- **Complexity**: The security vulnerability rises in proportion to the complexity of a system. The more features a system has, the more are the chances of the system being attacked.
- **Password**: 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.

Causes of Vulnerability Cont..

- **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 networks, internet, telephone opens up security theft scope.

Penetration Testing Tools and Companies

- Automated tools can be used to identify some standard vulnerabilities present in an application. Pentest tools scan code to check if there is a malicious code present which can lead to a 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 usernames and passwords.

Criteria for selecting 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 need an immediate fix.
- It should be able to automate the verification of vulnerabilities.
- It should re-verify the 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.

Recommended Penetration Testing Tools

1) Acunetix

Acunetix WVS offers security professionals and software engineers alike a range of stunning features in an easy, straight-forward, and very robust package.

2) Intruder

is a powerful vulnerability scanner that finds cybersecurity weaknesses in your digital estate, explains the risks & helps with their remediation before a breach can occur. It is the perfect tool to help automate your penetration testing efforts.

Other Free Tools

- Nmap
- Nessus
- Metasploit
- Wireshark
- OpenSSL

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 from 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 at regular intervals to protect the information systems against security breaches.

Penetration Testing is mainly required for

- 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 an effective security strategy within the organization.

What Should Be Tested?

- Software (Operating systems, services, applications
- Hardware
- Network
- Processes
- End-user behavior

Penetration Testing Types

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

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.

Penetration Testing Types Cont..

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 the possibility of any security breach. This test is not very 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. This can be done locally or remotely.

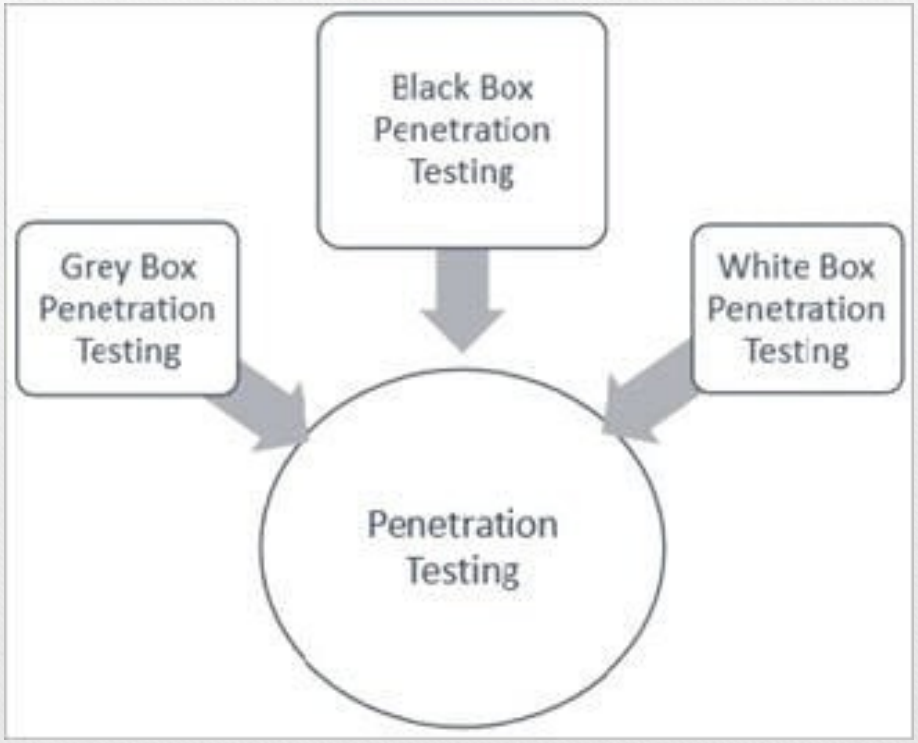
Penetration Testing Types Cont..

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 log in to the systems connected through these modems by password guessing or brute-forcing.

7) Wireless Security Test: It discovers open, unauthorized and less secure hotspots or Wi-Fi networks and connects through them.

Types of penetration testing into three parts



types of penetration testing into three parts

- **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 a very high level of inputs like URL or company name using which they penetrate 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 an 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 attacks.

Pen Testing Techniques

- Manual Penetration Test
- Using automated penetration testing tools.
- Combination of both manual and automated processes.

Pen Testing Techniques Cont..

Manual Penetration Test:

It’s difficult to find all vulnerabilities using automated tools. There are some vulnerabilities that can only be identified by manual scan. Penetration testers can perform better attacks on applications based on their skills and knowledge of the system being penetrated.

Pen Testing Techniques Cont..

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 this vulnerability and the same penetration tests are repeated until the system is negative to all those tests.

We can categorize this process in the following methods

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.
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.

We can categorize this process in the following methods

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 in 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 the vulnerability report format (HTML, XML, MS Word or PDF) as per your organization’s needs.

Conclusion

- Finally, as a penetration tester, you should collect and log all vulnerabilities in the system. Don’t ignore any scenario considering that it won’t be executed by the end-users.
- *If you are a penetration tester, please help our readers with your experience, tips, and sample test cases on how to perform Penetration Testing effectively.*

Question Please?

THANK YOU