Introduction to penetration testing

💎 Penetration testing

What is Penetration Testing

"Penetration testing, also called as pen testing, ensures that information security experts use security bugs in a computer program to find and take advantage of them."

These specialists, often classified as white-hat hackers or ethical hackers, make things simpler by detecting attacks by cyber attackers known as black-hat hackers in the modern environment.

⚗Need for Penetration Testing:

The goal of amateur or professional hacker is to steal the sensitive data of your organization. They may be wanted to destroy your company, or they may be after the money. Your company's reputation can be negatively affected by one single incident of system downtime. Your customer or business partner will think twice about their relationship security with your organization.

To secure your system, regular updating your password and window firewall is not enough. Highly skilled hackers can easily access your computer system. They can get any information which they want without even knowing you.

Any organization, corporation or company that depends on IT should have to regularly test the security of their system. To prevent your company from illegal hacking or the negative effect of system downtime, you also have to update your security features.

⚔Benefits of Penetration testing:

1. **Reveal Vulnerabilities**: - The main purpose of penetration testing is to find out the weaknesses of your computer system and network infrastructure. While penetration testing, the actions and habits of employees of your organization will also be researched so that it could lead us to data breaches and malicious infiltration.
2. **Show Real risks: -** Penetration testers will try to exploit identified vulnerabilities. That means you can see the action of the attacker in the real world. The attacker might execute the command of your operating system and access the sensitive data of your system.
3. **Test Cyber-Defence Capability: -**While penetration testing, you should find the attacks and respond adequately on time. When an intrusion is detected, you should begin investigations the intruders, discover and block them. We will block them, whether the intruders are malicious or not. Experts test the effectiveness of your protection strategy.
4. **Third-Party opinion: -**If someone identifies an issue in your organization, your management may not be inclined to act or react. The management faces a bigger impact by the report, which is made by a third party expect. This report may lead to the allocation of additional funds.
5. **Maintain Trust: -**A system breakdown or cyber-attack negatively affects the loyalty of your business partners and customers. You can reassure all your partners if your company is famous for its penetration testing, systematic and strict security.

⚔Areas of Penetration Testing:

1. **Network services**: It finds weaknesses and vulnerabilities in the security of the network infrastructure (for example, firewall testing)
2. **Web application**: Security vulnerabilities or weaknesses will get discovered in web-based applications (for example, Outlook)
3. **Client-side**: It finds vulnerabilities in software on a client computer, such as an employee workstation (for example, media player)
4. **Wireless**: This test examines all the wireless devices which are used in a corporation (for example, tablets or smartphones)
5. **Social engineering**: Getting confidential information by tricking an employee of the corporation to reveal such items (for example, phishing)

🛡Classification of Penetration Tests:

- Blind Tests
- White box Tests
- External tests
- Double-blind tests
- Internal Tests

Let's discuss each one in detail.

- **Blind Tests**: The Companies offers penetration testers with little security details about the device being exploited in a blind test, referred to as a black-box test. The aim is to find vulnerabilities that wouldn't ever be discovered.
- **White box Tests**: A white box test is one where companies offer a range of security details related to their structures to penetration testers to help them improve vulnerabilities.
- **External Tests:** An external test is one where, globally, penetration testers aim to identify vulnerabilities. They are carried out on macro environment-facing software such as domains because of the existence of these kinds of testing.
- **Double-blind Tests**: A double-blind test that is also defined as a covert test is one where sensitive data is not only given to penetration testers by companies. They still may not make the assessments known to their own information security experts. Traditionally, such experiments are strongly regulated by those conducting them.
- **Internal Tests**: An internal examination is one where the examination of penetration exists within the boundaries of an entity. Typically, these checks concentrate on the security weaknesses of which full advantage could be taken by anyone operating from inside an organization.

🛡Phases of Ethical Hacking and Penetration Testing

To carry out a structured attack, ethical hacking employs various phases. These are:

- **Reconnaissance**: The attacker uses various hacking tools (NMAP, Hping) to obtain information about the target
- **Scanning**: Using tools such as NMAP and Nexpose, the attacker tries to spot vulnerabilities in the system
- **Gain access**: Here, the attacker attempts to exploit the vulnerability using the Metasploit tool
- **Maintain access**: Now, the attacker tries to install some backdoors into the victim's system for future access (Metasploit is used again to achieve this)
- **Clear tracks**: In this stage, the attacker clears all evidence of the attack as no attacker likes to get caught
- **Reporting**: Finally, the ethical hacker documents a report which consists of the vulnerabilities spotted, the tools used to exploit, and the success rate of the operation.

🔮Best Penetration Testing Tools and Software

1. Wireshark

Typically named as Ethereal 0.2.0, with 600 contributors, Wireshark is an award-winning network mapper. You can catch and analyze data packets easily with this program. The tool is open-source and is compatible with Windows, Solaris, FreeBSD, and Linux, among other frameworks.

Key Points

- It offers both offline review and options for live-capture.
- Its locating intermediate nodes help you to discover new characteristics, including the protocol of the source and destination.
- It includes the opportunity to inspect the smallest information in a network for operations.
- It contains optional colouring rules for fast, intuitive analysis and are added to the pack.

2. Netsparkar

A common automated application server for penetration testing is the Netsparker vulnerability scanner. From cross-site request to SQL injection, the program can recognize anything from it. This tool can be used by designers on blogs, web infrastructure, and web services.

Key Points

- It can search the web-based applications for 1000 + in less than a day!
- For teamwork and easy discoverability of results, you can add several teammates.
- The Advanced scanning reduces the need for a small set up.
- It can search for SQL and XSS bugs in software applications that are hackable.
- You can create the Legal application of the web and reports of regulatory requirements.
- It has Proof-based screening technology to ensure precise identification.

3. Metasploit

Metasploit is the world's commonly utilized system for vulnerability assessment optimization. Metasploit allows technical experts to validate and manage safety evaluations, enhance visibility, and arm and inspire defenders to remain in the game a point ahead.

Key Points

- It is convenient to use with a scrollable given platform and command-line interface.
- Brute-forcing guides to launch systems to bypass urbanization and modernization, spear spyware, and recognition, an OWASP vulnerability testing app.
- It collects the data from testing for more than 1,500 exploits.
- Meta Modules for experiments of network connectivity.
- This can be used inside infrastructure to discover older vulnerabilities.
- It is also accessible for Mac OS X, Linux and Windows.

4.Aircrack

Aircrack NG is configured to hack vulnerabilities inside the wireless connections by trapping incoming packets for an efficient protocol to be exported for analysis through word documents. Although the program seemed to have been discontinued in 2010, in 2019, Aircrack has modified again.

Key Points

- It is compatible with Solaris, Linux, Windows, OS X, FreeBSD, NetBSD, and OpenBSD.
- To retrieve packages and export data, you will use this method.
- It is intended for wi-fi system testing as well as driver proficiency.
- It focuses on various security fields, such as an attack, surveillance, testing, and cracking.
- In terms of intrusion, you can de-authenticate, establish a fake wireless network and replay attacks.

5.Kali Linux

A Linux operating system used for vulnerability assessments is Kali Linux Specialized Penetration Testing Program. This is the perfect instrument for both extracting and password snipping, many analysts claim. However, to achieve the most of the advantages, you might need experience in both TCP / IP protocols. Tool descriptions, edition management, and meta-packages are supported by an open-source project, Kali Linux.

Key Points

- You will use this technique for brute-force attack password cracking with 64-bit assistance.
- To evaluate the security skills of cybersecurity professionals, Kali uses a live image configured into the RAM.
- Kali Linux contains 600 hacking methods that are ethical.

6.SQLmap

SQLmap is a Database SQL Injection Control Tool. It also enable MySQL, SQLite, Sybase, DB2, Access, MSSQL, PostgreSQL database platforms. SQLmap is open-source and streamlines the mechanism of manipulating the application server and bugs for the Attack vector.

Key Points

- This tool allows you to Detect exploits and monitor them.
- It offers assistance for all aspects of injection: Union, Time, Stack, Error, Boolean.
- It executes a command-line interface and can be configured for Linux, Mac OS, and Windows operating systems.

Advantages of Penetration Testing Tools:

- Meet the needs of tracking and mitigate penalties
- Subvert the channel failure intensity
- Secure brand recognition and corporate image

System hacking:

System hacking is the process of exploiting vulnerabilities in electronic systems for the purpose of gaining unauthorized access to those systems. Hackers use a variety of techniques and methods to access electronic systems, including phishing, social engineering, and password guessing.

Phases of System Hacking (same as above):

Prevention from Hacking:

- Using Firewall.
- Installing Anti-Virus and Anti-Spyware packages.
- Keeping the system up-to-date as security patches updates comes regularly.
- Be Aware of various phishing techniques.

Tool:

Burp Suite Pen Tester

The Burp Suite for programmers has two separate editions. The free version offers appropriate and essential tool for testing operations that are needed. Or, when you need extensive penetration testing, you can go for the second version. For testing web-based applications, this tool is perfect. Tools for mapping the tack substrate and analyzing transactions between the browser and endpoint servers are available.

Key Points

- It is suitable for web-based software scrolling automatically.
- Mac OS X, Linux, and Windows are accessible in this tool

Wireshark

Metasploit

John The Ripper Password Cracker

One of the most common flaws is passwords. To capture information and access sensitive systems, hackers can use credentials. For this reason, John the Ripper is the indispensable tool for password guessing and offers a variety of systems. The pen vulnerability scanner is a free software to use.

Key

- It automatically detects various variations of passwords.
- It also discovers inside databases password vulnerabilities.
- For Linux, Mac OS X, Hash Suite, and Hash Suite Droid, the premium edition is available.
- A personalized cracker is included.
- It helps people to discover online documentation. This provides a description of improvements between variants that are distinct.

🗝What is Social Engineering?

"Social Engineering is a cyber-attack technique where manipulation is the key weapon used by hackers. It exploits any human error to gain access to sensitive information, confidential and private files, etc."

- In Social Engineering attacks, the hackers are usually someone who is known to the victim or lure the victim into exposing data, allowing system access and other malicious activities.
- Social Engineering takes advantage of how users think, act and react to a particular situation.
- Social Engineering is used in the majority of cases or situations where manipulation of human behavior is easy to hack into systems.
- The hackers use this technique to read the behavior of the user.
- Once he gets an idea of what triggers or motivates the user to initiate a specific action, the hacker tries to manipulate and deceive the user.

🔑Characteristics of Social Engineering Attack

Social engineering attack centerson the attacker's use of persuasion and confidence.

High emotions: Emotional manipulation gives attackers the upper hand in any conversation. The below feelings are used equally to explain to you.

- Fear
- excitement
- Curiosity
- Anger
- Crime
- Sadness

Confidence: Credibility is invaluable and necessary for a social engineering attack. If the attacker is lying to us, confidence plays an important role. They have done enough research to prepare a narrative for us that is easy to believe and is unlikely to reduce suspicion.

🔑Types of Social Engineering Attacks: