Dated 09/01/2022 BWL DAY#3

What is Penetration Testing?

Penetration testing which is also known as pen-test is a part of ethical hacking, where it focuses explicitly on penetrating only the information systems. Now, how is penetration testing different from ethical hacking? Penetration testing focuses exclusively on information systems, while ethical hacking is a broad area to protect the systems.

What is Ethical Hacking?

Ethical hacking is the process of locating weaknesses or vulnerabilities in computers and information systems using the intent and actions of malicious hackers. There are two types of hackers:

1. **Malicious hacker:** This hacker hacks with a malicious intent to do damage to the victim
2. **Ethical hacker:** This hacker hacks using the same method but passes on the vulnerabilities to the security department

  Fig: Difference between a malicious and ethical hacker

Ethical Hacker Responsibilities

Here are some responsibilities of an ethical hacker:

1. Create scripts that test for vulnerabilities
2. Develop tools to increase security
3. Perform risk assessment
4. Setup security policies
5. Train staff for network security

Now that we have seen what ethical hacking and the roles of an ethical hacker is, it’s time to learn about penetration testing.

What is Penetration Testing?

Penetration testing which is also known as pen-test is a part of ethical hacking, where it focuses explicitly on penetrating only the information systems. Now, how is penetration testing different from ethical hacking? Penetration testing focuses exclusively on information systems, while ethical hacking is a broad area to protect the systems. Ethical hacking has more job roles and responsibilities than penetration testing.

Now that we have understood the difference between ethical hacking and penetration testing let’s take a look at the platform used by ethical hackers.

What is Kali Linux

Kali linux is a Debian-based operating system with advanced penetration testing and security auditing features. Most hackers also use this platform. Kali contains hundreds of tools which are used for various information security tasks like computer forensics and reverse engineering. The main features of Kali Linux include:

1. 600+ tools
2. Open-source
3. Mass customization
4. Wide range wireless support
5. Multi-language support
6. Fast injections

Phases of Ethical Hacking and Penetration Testing

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

1. **Reconnaissance**: The attacker uses various hacking tools (NMAP, Hping) to obtain information about the target
2. **Scanning**: Using tools such as NMAP and Nexpose, the attacker tries to spot vulnerabilities in the system
3. **Gain access**: Here, the attacker attempts to exploit the vulnerability using the Metasploit tool
4. **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)
5. **Clear tracks**: In this stage, the attacker clears all evidence of the attack as no attacker likes to get caught
6. **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

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)

Penetration Testing Tools

These are some of the more popular tools that are frequently used by hackers:

1. BeEF
2. Metasploit
3. NMAP
4. Nessus Vulnerability Scanner
5. WIRESHARK
6. SQLMap
7. BackTrack
8. John the Ripper