Importance of penetration testing | Step by Step Explained

What is Penetration testing?

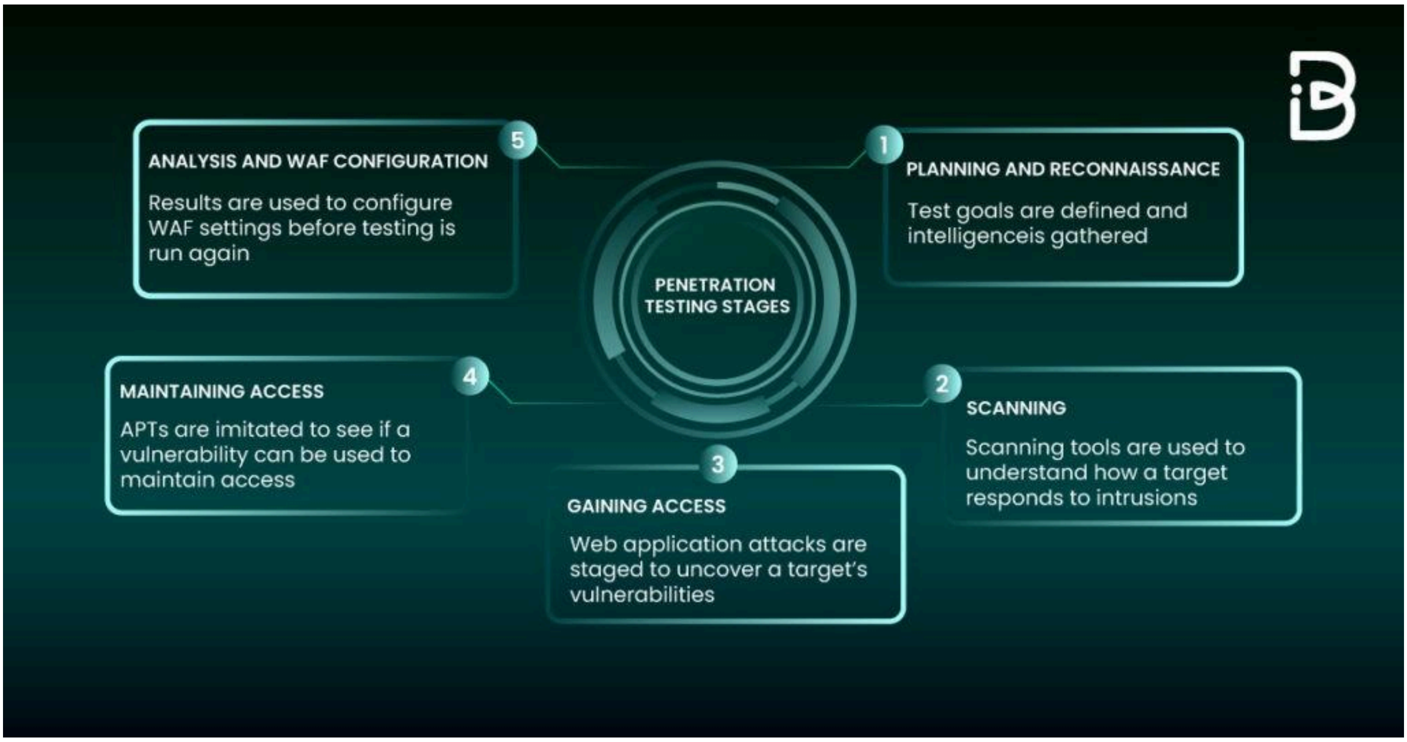
Penetration testing is also known as pen testing or ethical hacking which describes an intentional cyber-attacks that seeks out exploitable vulnerabilities in computer systems, websites, networks, and applications.

Pen testing can include the endeavored breaking of quite a few application frameworks, (e.g., frontend/backend servers, application protocol interfaces (APIs)) to uncover vulnerabilities, for example, unsanitized inputs that are helpless to code infusion assaults.

I hope that made you clear about **what is penetration testing**,
Now Let’s move on to the Next Step which is,

Stages of Penetration Testing :

There are five stages that we need to look at,


PENETRATION TESTING STAGES
1
PLANNING AND RECONNAISSANCE
Test goals are defined and intelligenceis gathered
2
SCANNING
Scanning tools are used to understand how a target responds to intrusions
3
GAINING ACCESS
Web application attacks are staged to uncover a target’s vulnerabilities
4
MAINTAINING ACCESS
APTs are imitated to see if a vulnerability can be used to maintain access
5
ANALYSIS AND WAF CONFIGURATION
Results are used to configure WAF settings before testing is run again

1. **Planning and Reconnaissance** — In this stage, we plan to simulate a malicious attack — this attack is designed to gather as much information on the system as possible. Though it is one of the time-consuming methods as ethical hackers investigate the framework, note the weaknesses, and how the association's tech stack responds to framework breaks.
It must be noticed that the type of data or the profundity of the investigation will rely upon the goals set for the review.
2. **Scanning** — In this stage, the application will react to various intrusive attempts, There are two ways to do this,

- Static Analysis — Assessing an application's code to gauge the manner in which it acts while running. These tools can filter the total of the code in a single pass.
- Dynamic Analysis — Examining an application's code in a running state. This is a more practical approach to filtering, as it gives a continuous view into an application's presentation.

3. **Gaining System Access** — In this stage, Pen testers then penetrate the infrastructure by taking advantage of safety shortcomings. Then, they endeavor to take advantage of the framework further by raising honors to show the way that profound into the objective conditions they can go.
4. **Persistent access** — This pentest step distinguishes the likely effect of a vulnerability exploits by utilizing access privileges. In this pentest stage, we attempt to acquire the most extreme level of privileges, network data, and admittance to however many frameworks as could be allowed by distinguishing which information or potential benefits are accessible to us.
5. **Reporting And Analysis** — This is the final stage where the security team prepares a deeply analyzed report of the entire **penetration testing process**. Some information that is included in the report are:

- The tool that can effectively penetrate the framework
- The reality of the dangers radiating from the vulnerabilities found
- Highlighting those points where security had been implemented perfectly
- And how to avoid future attacks

Importance Of Penetration Testing

1. **Compliance** — Let's say your organization's site utilizes the online methods of payments such as debit or credit cards, you're expected to follow PCI-DSS guidelines. As per these guidelines, you should conduct a yearly pentesting exercise on the site to moderate dangers and safeguard your site's information from hackers.
2. **Crisis Training** — Penetration testing can assist with preparing your security groups to promptly respond to and actually conquer a security break or other emergency. Your network

can be vulnerable to a few distinct sorts of cyberattacks, making it fundamental for your group to figure out how to manage every sort of assault. This will assist your team to be prepared for cyberattacks and, simultaneously, permit them to tweak their reaction to such events.

3. **Building Goodwill** — By doing penetration testing regularly, you can minimize your organization’s risk of losing data or getting hacked and can maintain data protection. Running a penetration test will assist you with measuring the time it would take for a potential hacker to break the security, as well as prepare the security team to answer the assault in time.
4. **Testing New Technology** — The primary objective of the most penetrative test is testing new technologies. They can assist you with making the technology security more powerful, taking into account a more secure, smoother experience for clients. The development stage is the best time to begin penetrative testing so you can dispose of any vulnerability right at the beginning phases.
5. **Verify Security Protocols** — Your security group should be certain of their protocol and ready to face any attack without warning, yet penetrative testing can assist with checking them no different either way. You can distinguish any significant oversights in security and ensure the conventions are improved to be just about as productive as could be expected.

These are the main importance of doing penetration testing while running an organization and doing penetration testing on its own is not so easy.

Hiring a penetration tester will help you save time and give you better results within time.