This will enable testers to launch further attacks on the network to further increase the scope of compromised systems.

The post exploitation step will also involve clearing of tracks by conducting activities such as clearing logs and disabling antivirus.As a post-exploitation phase tester, you can demonstrate how an attacker can maintain access to the system through backdoors and rootkits.

Stage 6 – Report generation

After completing the assessment as per the scope of work, final reporting needs to be done covering the following key areas:

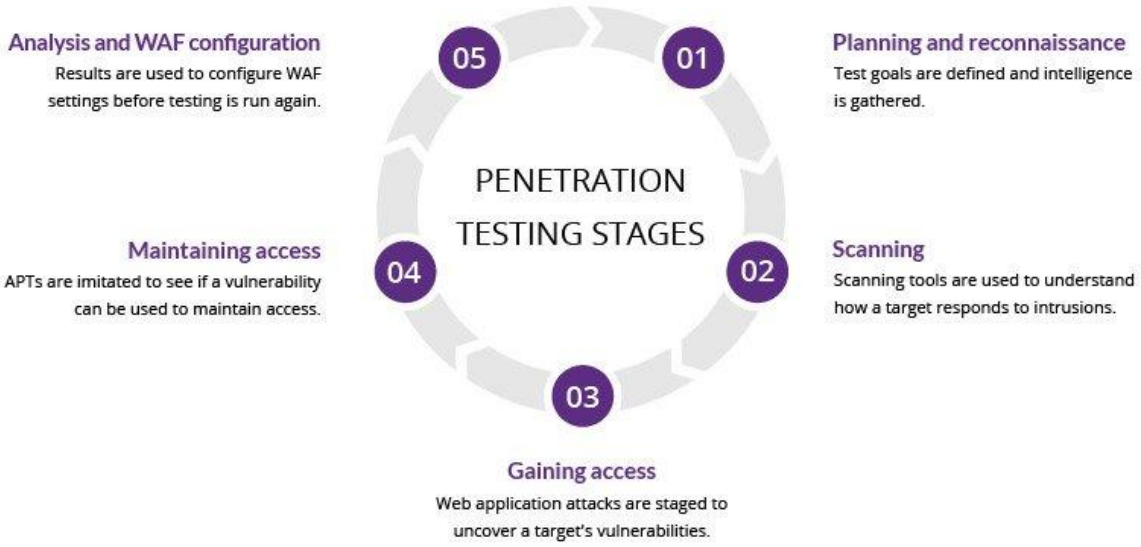
- A brief introduction about the assessment
- The scope of assessment
- The management/executive summary
- A synopsis of findings with risk severity
- Details about each finding with their impact and your recommendations to fix the vulnerability.

What is penetration testing

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.


Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.
05
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
PENETRATION TESTING STAGES
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
04
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.

1. Planning and reconnaissance

The first stage involves:

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

Static analysis – Inspecting an application’s code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Dynamic analysis – Inspecting an application’s code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application’s performance.

3. Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target’s vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization’s most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a report detailing:

Specific vulnerabilities that were exploited

Sensitive data that was accessed

The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise’s WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Penetration testing methods

External testing

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

Internal testing

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn’t necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

Blind testing

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

Double-blind testing

In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

Targeted testing

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

Who performs pen tests?

It's best to have a pen test performed by someone with little-to-no prior knowledge of how the system is secured because they may be able to expose blind spots missed by the developers who built the system. For this reason, outside contractors are usually brought in to perform the tests. These contractors are often referred to as 'ethical hackers' since they are being hired to hack into a system with permission and for the purpose of increasing security.

Many ethical hackers are experienced developers with advanced degrees and a certification for pen testing. On the other hand, some of the best ethical hackers are self-taught. In fact, some are reformed criminal hackers who now use their expertise to help fix security flaws rather than exploit them. The best candidate to carry out a pen test can vary greatly depending on the target company and what type of pen test they want to initiate.

What are the types of pen tests?

White box pen test - In a white box test, the hacker will be provided with some information ahead of time regarding the target company's security info.

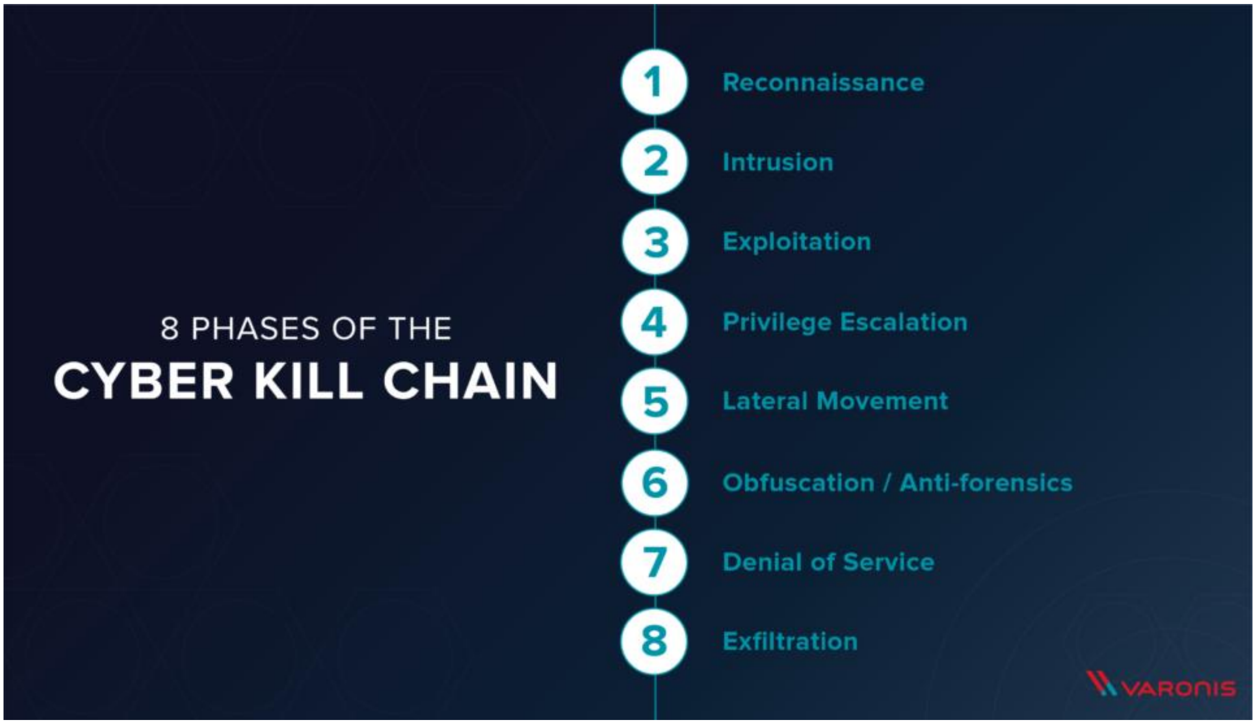
Black box pen test - Also known as a 'blind' test, this is one where the hacker is given no background information besides the name of the target company.

Covert pen test - Also known as a 'double-blind' pen test, this is a situation where almost no one in the company is aware that the pen test is happening, including the IT and security professionals who will be responding to the attack. For covert tests, it is especially important for the hacker to have the scope and other details of the test in writing beforehand to avoid any problems with law enforcement.

External pen test - In an external test, the ethical hacker goes up against the company's external-facing technology, such as their website and external network servers. In some cases, the hacker may not even be allowed to enter the company's building. This can mean conducting the attack from a remote location or carrying out the test from a truck or van parked nearby.

Internal pen test - In an internal test, the ethical hacker performs the test from the company's internal network. This kind of test is useful in determining how much damage a disgruntled employee can cause from behind the company's firewall.

The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).



8 PHASES OF THE

CYBER KILL CHAIN

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement
6. Obfuscation / Anti-forensics
7. Denial of Service
8. Exfiltration

How the Cyber Kill Chain Works

There are several core stages in the cyber kill chain. They range from reconnaissance (often the first stage in a malware attack) to lateral movement (moving laterally throughout the network to get access to more data) to data exfiltration (getting the data out). All of your common attack vectors