Introduction to Penetration Testing

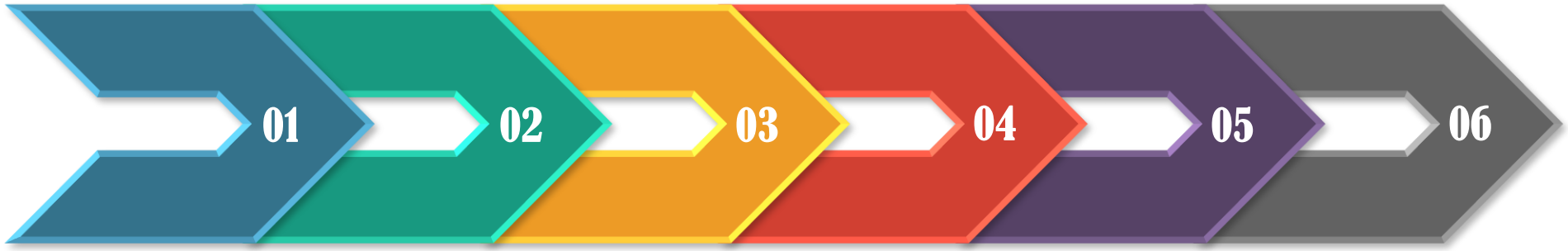
Dr. Zahid H. Qaisar

Course Outline

What is Penetration testing?

Phases of Penetration testing

Metasploit



Types of Penetration testing

Penetration testing tool and Lab

Web Penetration

What is Penetration Testing?

- Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer systems, networks, websites, and applications. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.

- it comprises a set of methods and procedures that

aim at testing/protecting an organization's security.

The penetration tests prove helpful in finding vulnerabilities in an organization and check whether an attacker will be able to exploit them to gain unauthorized access to an asset.

Why perform a Penetration Test?

If a vulnerability is utilized by an unauthorized individual to access company resources, company resources can be compromised. The objective of a penetration test is to address vulnerabilities before that can be utilized. Vulnerabilities could be due to multiple reasons, few basic ones being:

- Flaws in the design of hardware and software
- Usage of unsecured network
- Poorly configured computer systems, networks & applications
- Complex architecture of computer systems
- Plausible human errors

- **What should be tested?**

The core services offered by the company that include: user, system, network, wireless systems or application access. i.e. Mail, DNS, firewall systems, password syntax, web servers, database servers and any other servers.

These include physical access to the computing/network and backup areas in addition to social engineering access attempts.

Basic terms

- ***Asset***

An asset is any data, device, or other component of the environment that supports information related activities that should be protected from anyone besides the people that are allowed to view or manipulate the data/information.

- ***Vulnerability***

Vulnerability is defined as a flaw or a weakness inside the asset that could be used to gain unauthorized access to it. The successful compromise of a vulnerability may result in data manipulation, privilege elevation, etc.

- ***Threat***

A threat represents a possible danger to the computer system. It represents something that an organization doesn't want to happen. A successful exploitation of vulnerability is a threat. A threat may be a malicious hacker who is trying to gain unauthorized access to an asset.

- ***Exploit***

An exploit is something that takes advantage of vulnerability in an asset to cause unintended or unanticipated behavior in a target system, which would allow an attacker to gain access to data or information.

- ***Risk***

A risk is defined as the impact (damage) resulting from the successful compromise of an asset. For example, an organization running a vulnerable apache tomcat server poses a threat to an organization and the damage/loss that is caused to the asset is defined as a risk. Normally, a risk can be calculated by using the following equation:

Risk = Threat * vulnerabilities * impact

Vulnerability Assessments vs Penetration Test

Oftentimes, a vulnerability assessment is confused with a penetration test; however, these terms have completely different meanings.

- In a vulnerability assessment, our goal is to figure out all the vulnerabilities in an asset and document them accordingly.
- In a penetration test, however, we need to simulate as an attacker to see if we are actually able to exploit a vulnerability and document the vulnerabilities that were exploited and the ones that turned out to be false-positive.

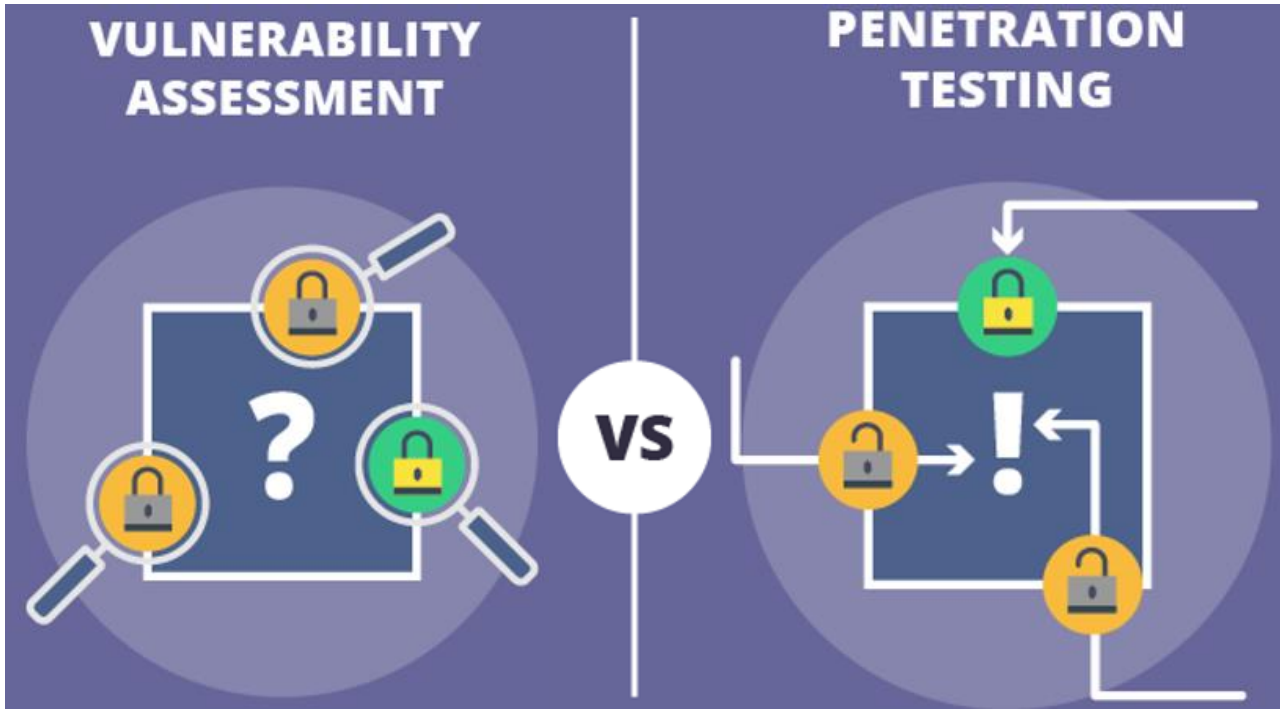


Image source: https://www.scnsoft.com/blog/vulnerability-assessment-vs-penetration-testing

Thank you