Security Testing

Ethical Hacking:-

1. Ethical Hacking is a process to identify and exploit weakness
2. The Goal of Ethical Hacking is to secure Systems.
3. Example - Weakness of default password.

Types of Hackers:-

1. Black Hat: Work in illegal way
2. White Hat: Work in legal way
3. Gray Hat: Work in legal terms and illegal way

Types of Testing:-

1. Black Box Testing: No Knowledge about Target
2. White Box Testing: Complete Knowledge about Target
3. Gray Box Testing: Partial knowledge about Target

Ethical Hacking Terminologies:-

1. Vulnerability
2. Payload
3. Exploit
4. Penetration
5. Script Kiddie
6. Intermediate Hacker
7. Elite Hacker

Ethical Hacking Terminologies:-

1. Vulnerability – Weakness of a system
2. Payload – Malicious Code to attack on system
3. Exploit – Amethod which contains payload
4. Penetration – Intrude in a system
5. Script Kiddie – unskilled attacker
6. Intermediate Hacker – Better understanding about hacking techniques
7. Elite Hacker – Expert Hackers in Ethical Hacking Area

Virtual Machine:-

1. It is used to run multiple machines on a physical machine.
2. Example – Vmware Workstation, VirtualBox

Footprinting:-

1. Gather information about target.
2. It is first phase in pentesting process.
3. Example - Network Footprinting, Web Footprinting etc.
4. Tools - Dmitry, Nmap, sparta etc.

Dmitry basically search for the onwer of the domain.

1. `sudo apt install dmitry`

2. `dmitry -s [www.zemosolabs.com](http://www.zemosolabs.com/)`

Vulnerability Scanning

1. Gather information about vulnerabilities in target system.

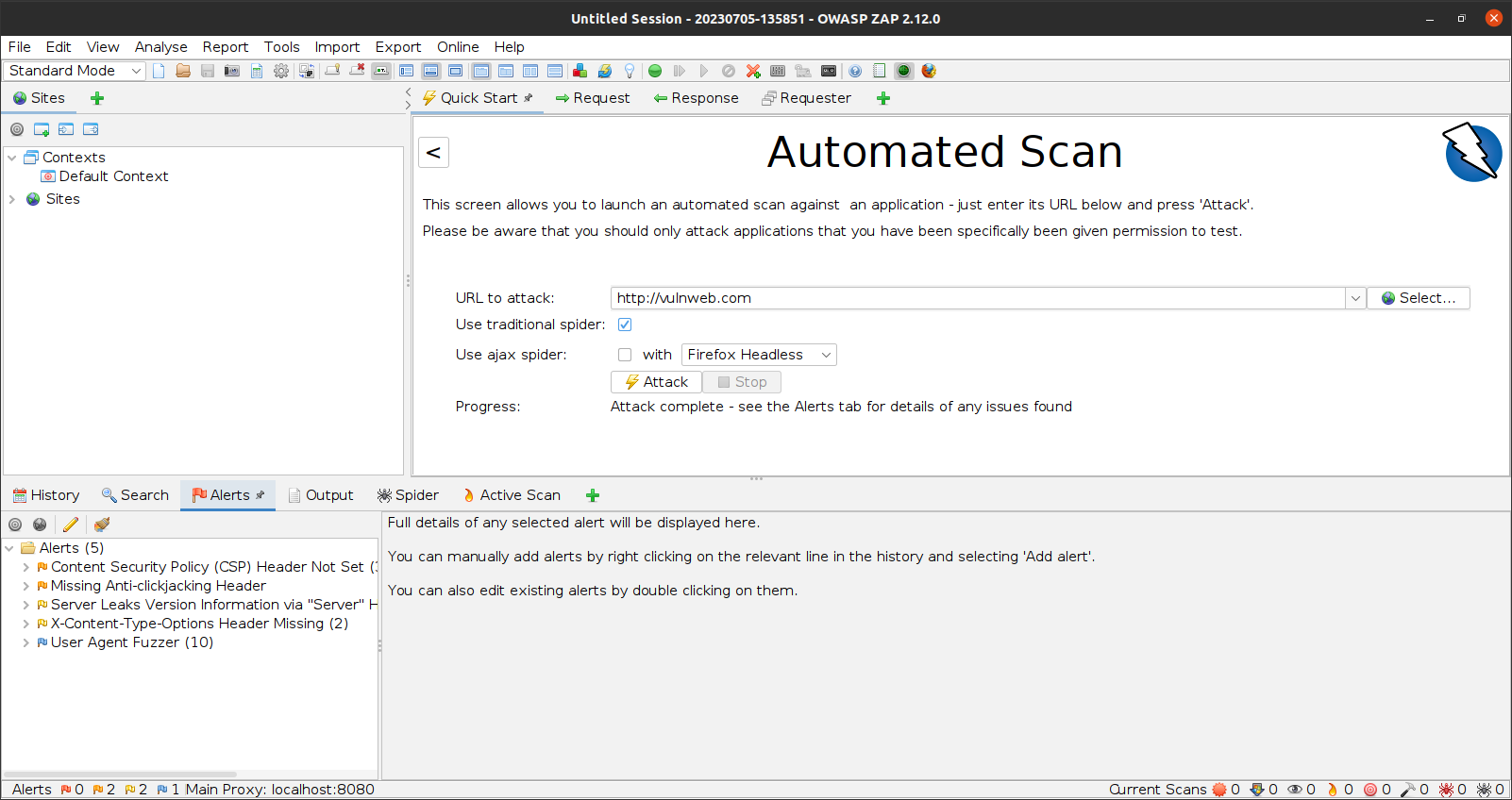
2. Generate a vulnerability scanning report.

3. Example - Network Scanning, Website Scanning etc.

Phase:-

Footprinting --> Vulnerability Scanning --> Exploits

For penetration testing, OWASP ZAP 2.12.0 we are using;

  
Exploits:-

1. Methods to attack on target system.
2. Metasploit Framework contains various exploits.
3. Example – Windows10 exploits

Exploitation Attack Process:-

1. Create a Payload.
2. Transfer it to victim machine.
3. Create a handler in attacker machine.
4. Execute the payload in victim machine.
5. Get access to victim machine.