Penetration Testing Process

Dr. Zahid H. Qaisar

Penetration Testing Process

Scanning & discovery

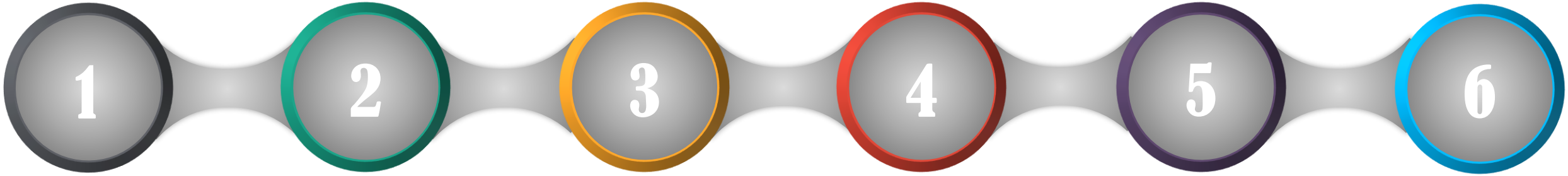
Scan the target host for vulnerabilities, perform port scan, network scan, Vulnerabilities scan

Maintaining Access

Maintain access to the system using backdoor or by other means

Report generation

Report the vulnerabilities identified during the process along with exploit details, impact and remediation.



Reconnaissance & Planning

Planning and gather information as much about the target

Exploitation

Exploit vulnerabilities and gain access to target host

Clearing Tracks

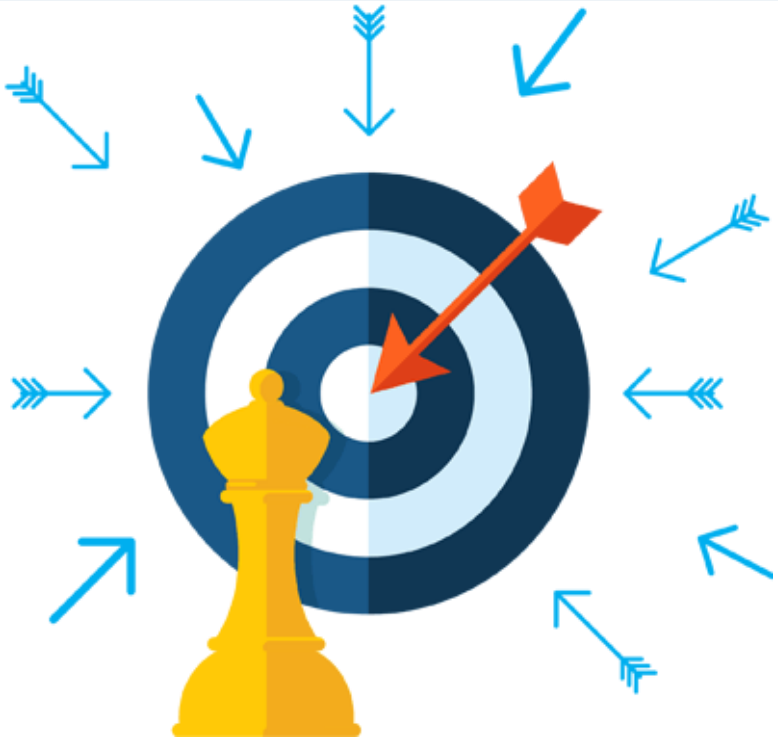
Delete logs and stuff that were used during process to avoid and tracking detection

Reconnaissance & Planning

- **Reconnaissance & Planning**
- First step, the attacker gathers as much publicly available information about the target as possible. The data can be IP addresses, domain details, mail servers, network topology, etc. In this phase, he also defines the scope and goals of a test, including the systems to be addressed and the testing methods to be used. An expert penetration tester will spend most of the time in this phase, this will help with further phases of the attack.

Scanning & discovery

- Based on the data collected in the first step, the attacker will interact with the target with an aim to identify the vulnerabilities. This helps a penetration tester to launch attacks using vulnerabilities in the system. This phase includes the use of tools such as port scanners, ping tools, vulnerability scanners, and network mappers.
- While testing web applications, the scanning part can be either dynamic or static.
- In **static scanning**, the aim is to identify the vulnerable functions, libraries, and logic implementation
- **Dynamic analysis** is the more practical way of scanning compared to static analysis where the tester will pass various inputs to the application and record the responses

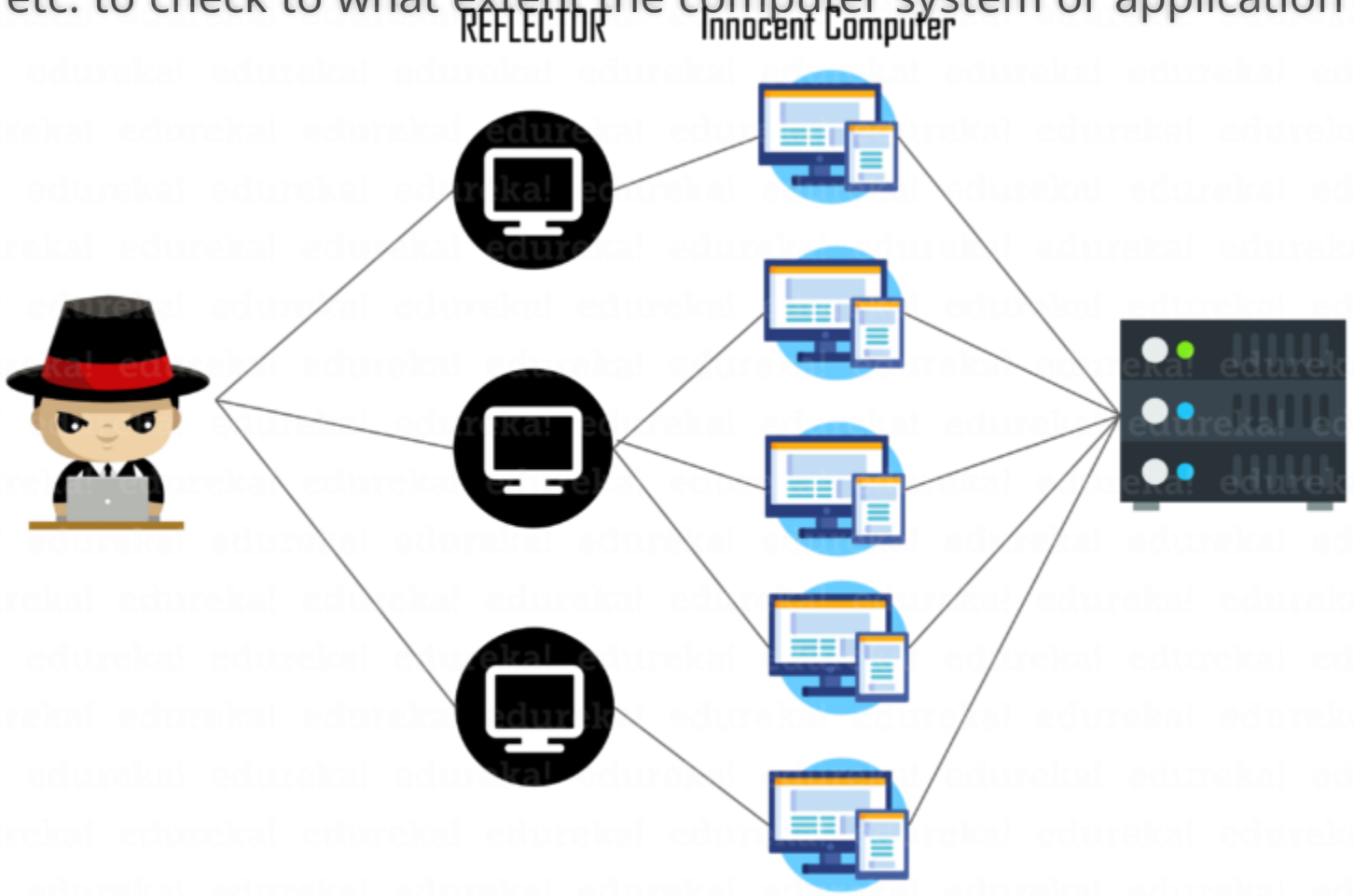


```
Starting Nmap 7.90 ( https://nmap.org ) at year-mo-day hh:mm EDT
Nmap scan report for site.domain (xx.xx.xx.xx)
Host is up (0.15s latency).
Not shown: 89 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
```

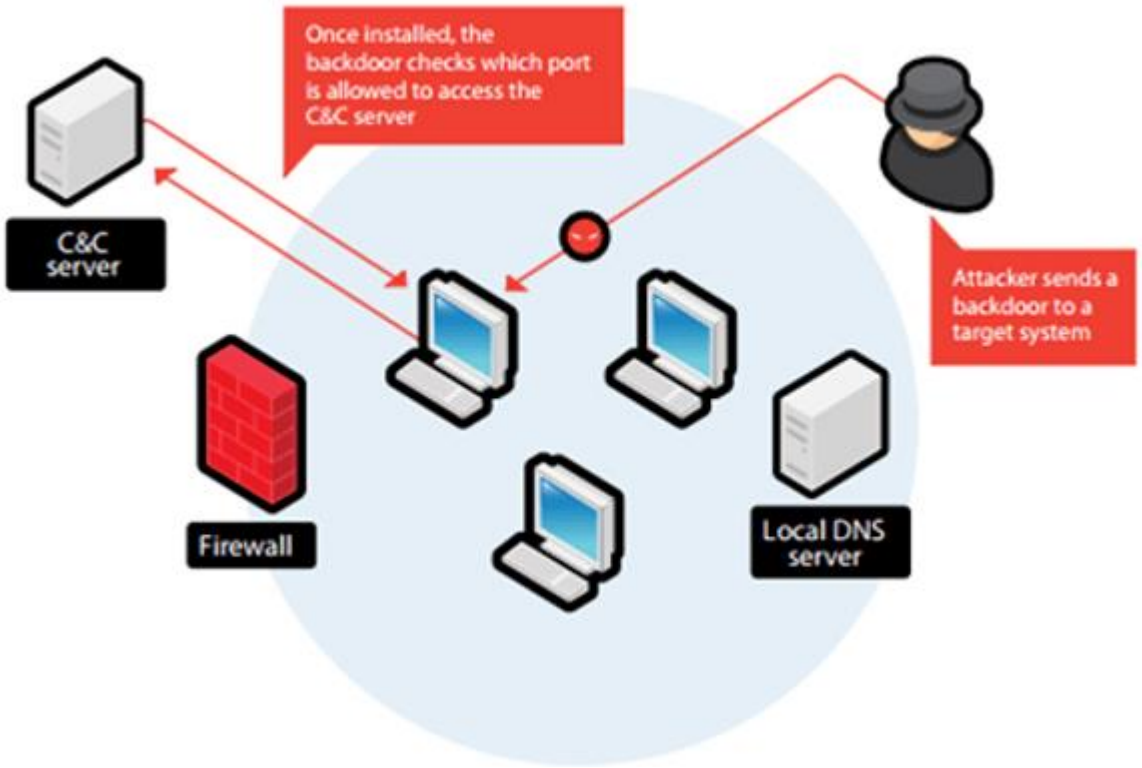
Exploitation

- This is the crucial phase that has to be performed with due care. This is the step where the actual damage is done. Penetration Tester need to have some special skills and techniques to launch an attack on the target system. Using these techniques an attacker will try to get the data, compromise the system, launch dos attacks, etc. to check to what extent the computer system or application or a network can be compromised.



Maintaining Access

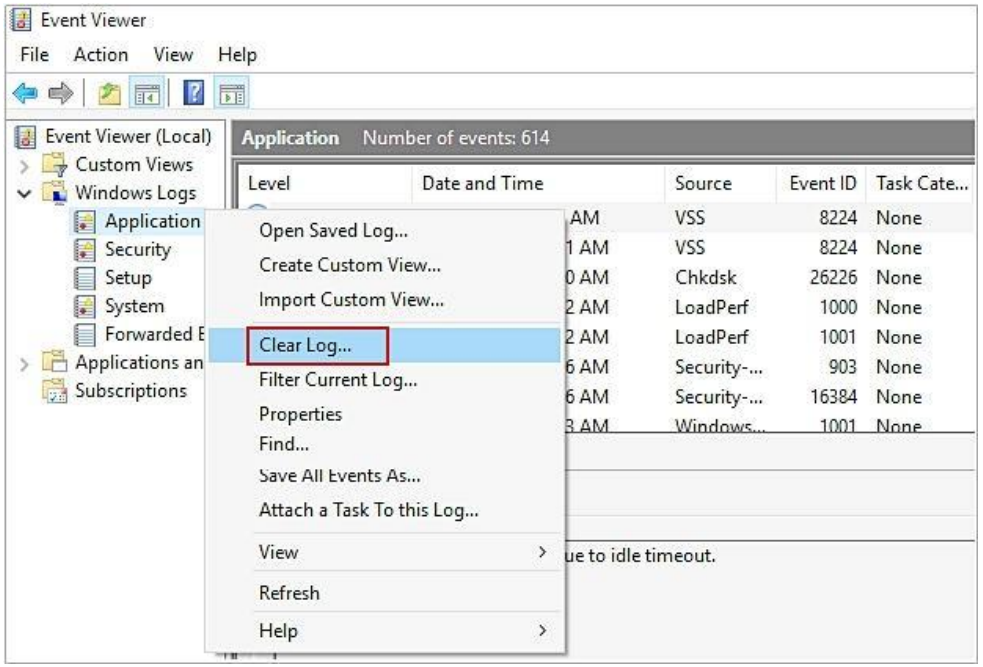
- After successfully compromising a host, if the rules of engagement permit it, it is frequently a good idea to ensure that you will be able to maintain your access for further examination or penetration of the target network. The attacker may install software like **backdoor** or **keyloggers** etc, which allows the hacker to remotely log into a server or computer without detection.



Clearing Tracks

- It is very important, after gaining access and misusing the network, that the attacker cover the tracks to avoid being traced and caught. To do this, the attacker clears all kinds of logs and malicious malware related to the attack. During this phase, the attacker will disable auditing and clear and manipulate logs.

```
meterpreter > run event_manager -c
[-] You must specify and eventlog to query!
[*] Application:
[*] Clearing Application
[*] Event Log Application Cleared!
[*] HardwareEvents:
[*] Clearing HardwareEvents
[*] Event Log HardwareEvents Cleared!
[*] Internet Explorer:
[*] Clearing Internet Explorer
[*] Event Log Internet Explorer Cleared!
[*] Key Management Service:
[*] Clearing Key Management Service
[*] Event Log Key Management Service Cleared!
[*] Security:
[*] Clearing Security
[*] Event Log Security Cleared!
[*] System:
[*] Clearing System
[*] Event Log System Cleared!
```



Report Generation

- Now, this is the final and the most important step. In this step, the results of the penetration test are compiled into a detailed report. This report usually has the following details:
- Recommendations made in the previous phase
- Vulnerabilities that were discovered and the risk levels they posses
- Overall summary of the penetration test
- Suggestions for future security

Thank you