Chapter 6

System Hacking

Theory

Ethical Hacking

System Hacking

System hacking is the process of trying to compromise the target system with the help of the information we collect from the pre-attack phases (Footprinting and scanning).

Metasploit

Metasploit is a Framework used for developing and executing exploit code against a remote target machine. Metasploit Framework contains following modules

- Exploits
- Payloads
- Auxiliary
- Encoders
- Post
- Nop’s

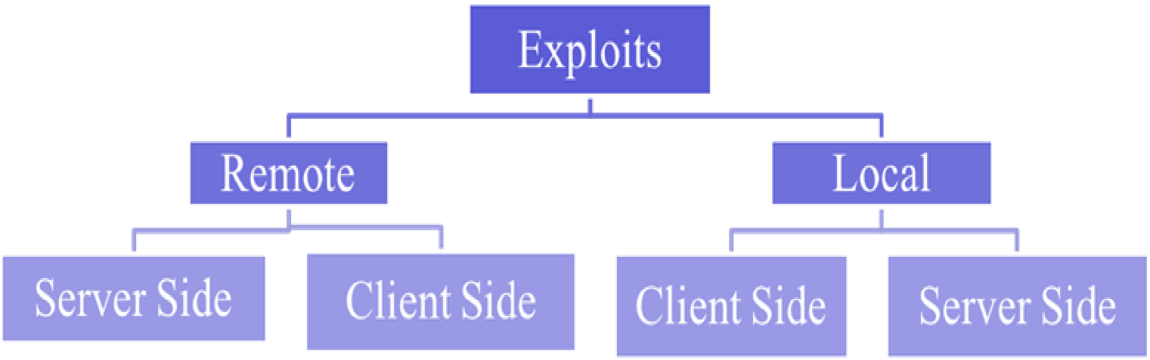
Components of the Metasploit:

- Msfconsole
- Msfvenom
- Armitage

Exploit

Exploits can help gain superuser-level access to a computer system. Hackers manage to gain low-level access; then they try to escalate privileges to the highest level (root). The exploit becomes unusable; once the vulnerability is fixed through a patch

Exploits are Classified based on how the exploit communicate with the vulnerable software.



- A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system.
- A local exploit requires prior access to the vulnerable system and escalate the privileges of the person running the exploit.

Payload

The payload is the piece of code in the exploit which performs a malicious action, i.e., deleting data, providing the remote connection, sending spam or encrypting data.

Types of Payload

The Metasploit framework has three different types of payloads

1. Singles
2. Stagers
3. Stages

Single Payload

Singles are self-contained payloads. They perform a simple task like adding a user to the target computer and running executable files in the victim's computer. These kinds of payloads can be caught with non-Metasploit handlers such as netcat. These payloads are more stable because they contain everything in one.

Stager payload

Stager payloads are used to set up a network connection between the attacker and victim and provide the remote connection to execute commands. It is difficult to do both of these well, so the result is multiple similar stagers. Metasploit will use the stagers to create the buffer memory in a small portion of memory; these stagers are responsible for downloading a large payload (the stage), injecting it into memory, and passing execution to it.

Stage payload

Stage Payloads are the components of the stagers that are downloaded in the exploited pc by the Stagers. The various payload stages provide the advanced features with no size limit such as Meterpreter, VNC injection, etc.

Escalating Privileges

Privilege escalation is a technique to exploit existing vulnerabilities in design, misconfigurations in an operating system or in any installed applications to gain elevated access to resources that are usually protected from an application or user.

Vertical Privilege Escalation

The attacker grants himself higher privileges. Privilege escalation is typically achieved by performing kernel-level operations that allow the attacker to run unauthorized code.

Horizontal Privilege Escalation

Attacker’s use the same level of privileges he already has been granted, but assume the identity of another user with similar privileges.

Password Cracking

In password cracking, hackers use a different kind of attacks to know the target computer login password so that they can gain complete access.

Types of passwords

Passwords with only letters	Ex: admin
Passwords with letters and numbers	Ex: admin123
Passwords with letters and special characters	Ex: admin@
Passwords with only numbers	Ex: 6842
Passwords with only special characters	Ex: @!#$%%^
Passwords with numbers and special characters	Ex: 1234!@#$
Passwords with letters, numbers and special characters	Ex: admin@123

Methods To Crack password

Password Guessing – Not a technique, but usually the first thing that every criminal will try to do.

Brute Force Attack – All possible permutations & combinations of the keyboard are tried as the victim's password. All passwords have to be some permutation or combination of victim's keyboard characters.

Dictionary Based Attack – All words in the dictionary are tried as the victim’s password.

Syllable attack – Combination of both, brute force attack and a dictionary attack. This is often used when the password is a nonexistent word.

Default Passwords – Manufacturers configure the hardware or software with default passwords and settings. We can get default passwords online for devices (http://defaultpassword.us/).

Data Sniffing – Data sniffer to record passwords being sent across the LAN network in plaintext format.

Countermeasures

- Keep Operating system software updated (patched).
- Use stronger authentication methods.
- Enable security auditing to help monitor attacks.
- Avoid storing user names/password on disk.
- Change passwords on a frequent basis.
- Build user awareness on social engineering attacks.