

Metasploit

Metasploit is an open-source penetration testing framework used for developing, testing, and executing exploits against remote targets. It is widely regarded as a powerful tool for cybersecurity professionals, ethical hackers, and penetration testers to identify, validate, and exploit vulnerabilities in a network or system.

Key Functionalities

- **Exploitation:** Automates the process of exploiting known vulnerabilities in various systems.
- **Post-Exploitation:** Facilitates further exploitation and information gathering after initial access is gained.
- **Payload Generation:** Generates custom payloads that can be used with exploits to control the compromised system.
- **Auxiliary Tools:** Offers tools for network discovery, fingerprinting, brute-forcing, and vulnerability scanning.
- **Database Integration:** Supports integration with databases like PostgreSQL to store scan results, information about targets, and track the progress of penetration testing engagements.

How to Use Metasploit

1. **Install Metasploit:** It can be installed on various operating systems, including Kali Linux, Ubuntu, and Windows.
2. **Start the Framework:** Use `msfconsole`, the command-line interface of Metasploit, to start the framework.
3. **Search for Exploits:** Use the `search` command to find exploits for specific vulnerabilities.
4. **Configure the Exploit:** Set the necessary options, such as the target IP address and payload.
5. **Run the Exploit:** Use the `run` or `exploit` command to execute the exploit against the target.
6. **Post-Exploitation Activities:** Perform further actions like privilege escalation, data exfiltration, or maintaining access.

Advantages

- **Comprehensive:** Contains a large number of pre-built exploits and payloads.
- **Extensible:** Users can write and integrate their modules.
- **Community-Driven:** Regularly updated by a large community of contributors.
- **Cross-Platform:** Works on different operating systems and targets.

Disadvantages

- **Risk of Misuse:** Can be used by malicious actors for unethical purposes.
- **Resource-Intensive:** Some operations may consume significant system resources.
- **Requires Expertise:** Understanding the framework and its modules requires a good grasp of cybersecurity concepts.

Commands:

- Command: ***search ssh_version***

This command searches for the ssh versions available in Metasploit

```
msf6 > search ssh_version

Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/fuzzers/ssh/ssh_version_15     .               normal No     SSH 1.5 Version Fuzzer
1  auxiliary/fuzzers/ssh/ssh_version_2     .               normal No     SSH 2.0 Version Fuzzer
2  auxiliary/fuzzers/ssh/ssh_version_corrupt .               normal No     SSH Version Corruption
3  auxiliary/scanner/ssh/ssh_version         .               normal No     SSH Version Scanner

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ssh/ssh_version
```

use auxiliary/scanner/ssh/ssh_version

used to identify the version of the SSH server running on a remote system.

- **Options**

if we look at **options** then we can see the module options.

```
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > options

Module options (auxiliary/scanner/ssh/ssh_version):

Name           Current Setting  Required  Description
-----
EXTENDED_CHECKS true            yes       Check for cryptographic issues
RHOSTS         22              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          1               yes       The target port
THREADS        1               yes       The number of concurrent threads (max one per host)
TIMEOUT        30              yes       Timeout for the SSH probe

View the full module info with the info, or info -d command.
```

Since RHOST is not set, we set the Ip of the target machine.

```
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.1.100
RHOSTS => 192.168.1.100
```

(Hidden the IP address for safety)

Setting **THREADS** to 100 means that the module will use 100 concurrent threads to perform its operations (like scanning or exploiting).

When 'run' command is given, it starts performing the actions defined by that module — such as scanning for vulnerabilities, gathering information, or exploiting a target.

```
msf6 auxiliary(scanner/ssh/ssh_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/ssh/ssh_version) > run

[*] 192.168.1.100 - Key Fingerprint: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMB0zV03WTEjP4TudJgWkIVNdTq6kboEDjteOfc65TLI7sRvQbWAhQjeeyI1k8T55gMDkOD0akS1SxvLDcmcdY
fxeIF0ZSuT+nKRhij7XS5SA/Oc5QSk3s3/Sinfb78e3anbRHpmk3cVgETJ5WhKobUNf1AKZW++4Xlc63M4KI5cjvMMIPEV0yR3AKmI78Fo3H3jYucg87JjLeC66I7+dLEYX6zT8i1XYwa/LivZ3q53ISGVu8kRPikMv/cNS
vki4j+qDYyZ2E5497W87+Ed46/8P42LNg0V80cX/ro6pAcBEPudUEfkJrq12YXbhvwI30gFMb6wfe5cnQew==
[*] 192.168.1.100 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
[*] 192.168.1.100 - Server Information and Encryption
```

Type	Value	Note
encryption.compression	none	
encryption.compression	zlib@openssh.com	
encryption.encryption	aes128-cbc	Deprecated
encryption.encryption	3des-cbc	Deprecated
encryption.encryption	blowfish-cbc	Deprecated
encryption.encryption	cast128-cbc	Deprecated
encryption.encryption	arcfour128	Deprecated
encryption.encryption	arcfour256	Deprecated
encryption.encryption	arcfour	Deprecated
encryption.encryption	aes192-cbc	Deprecated
encryption.encryption	aes256-cbc	Deprecated
encryption.encryption	rijndael-cbc@lysator.liu.se	Deprecated
encryption.encryption	aes128-ctr	
encryption.encryption	aes192-ctr	
encryption.encryption	aes256-ctr	

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
File Actions Edit View Help

encryption.encryption aes256-ctr
encryption.hmac hmac-md5 Deprecated
encryption.hmac hmac-sha1
encryption.hmac umac-64@openssh.com
encryption.hmac hmac-ripemd160 Deprecated
encryption.hmac hmac-ripemd160@openssh.com
encryption.hmac hmac-sha1-96 Deprecated
encryption.hmac hmac-md5-96 Deprecated
encryption.host_key ssh-rsa
encryption.host_key ssh-dss
encryption.key_exchange diffie-hellman-group-exchange-sha256
encryption.key_exchange diffie-hellman-group-exchange-sha1 Deprecated
encryption.key_exchange diffie-hellman-group14-sha1
encryption.key_exchange diffie-hellman-group1-sha1 Deprecated
fingerprint_db ssh.banner
openssh.comment Debian-8ubuntu1
os.cpe23 cpe:/o:canonical:ubuntu_linux:8.04
os.family Linux
os.product Linux
os.vendor Ubuntu
os.version 8.04
service.cpe23 cpe:/a:openbsd:openssh:4.7p1
service.family OpenSSH
service.product OpenSSH
service.protocol ssh
service.vendor OpenBSD
service.version 4.7p1

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) >
```