

## **Ethical Hacking and Countermeasures**

## **Metasploit Cheat Sheet**

4. Using Database i.First Time Setup (Linux command line)



Description

#### Metasploit

Source: https://www.metasploit.com Metasploit is an open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing. It is a tool that provides information about security vulnerabilities and aids in penetration testing. Metasploit framework is also used for developing and executing exploits which promotes in gaining remote access to a system by exploiting any vulnerability present in that server. Meterpreter is a payload inside the framework. The following table lists the various Metasploit commands and their respective scanning methods.

Description

List all sessions

Init database

#### 1.Metasploit General Information

- 2. Executing an Exploit / Scanner / Module
- 3. Session Handling
- 4. Using Database
  - i.First Time Setup (Linux command line)
  - ii. Inside msfconsole
- 5. Meterpreter Session Commands
- i.Base Commands
- ii. Process Commands
- iii. File System Commands

#### iv. Escalate Privileges

- v. Networking Commands vi. Additional Commands
- 6. Session Management
- 7. Interface / Output commands
- 8. Msfvenom Command Options
- 9. Important Auxiliary Modules

#### msfdb Init

**Metasploit Command** 

service postgresql Start

#### ii. Inside msfconsole

Metasploit Command	Description
db_status	Should display connected
hosts	Display hosts in database
services	Show ports in database
vulns	Exhibit all vulnerabilities

# mkdir Make directory rmdir Remove directory

Change directory

Show contents of a file

## edit <FILE> Edit a file in default editor (vi)

upload / download Upload / download a file from target machine

#### 1.Metasploit General Information

Metasploit Command	Description
msfconsole	Launch program
version	Display current version
msfupdate	Pull weekly update
makerc <file.rc></file.rc>	Saves recent commands to file
msfconsole -r <file.rc></file.rc>	Loads resource file

### 5. Meterpreter Session Commands

#### i.Base commands

Metasploit Command	Description
sysinfo	Display system name and OS type
shutdown / reboot	Shutdown system
exit / quit	Exit Meterpreter session

#### iv. Escalate Privileges

**Metasploit Command** 

cd

cat

Metasploit Command	Description
use priv	Load script
getsystem	Gain administrative-level privileges
getprivs	Elevate privileges

#### 2. Executing an Exploit / Scanner / Module

Metasploit Command	Description
use <module></module>	Set the exploit to use
set payload <payload></payload>	Set the payload
show options	Show all options
set <option> <setting></setting></option>	Set setting
exploit or run	Execute exploit

#### ii. Process Commands

Metasploit Command	Description
ps	Show running processes list
kill <pid></pid>	Terminate process
getuid	Show user ID
getpid	Show process ID that Meterpreter is running inside
migrate <pid></pid>	Start another process
execute	Execute given program with the privileges of the process

#### v. Networking Commands

Description  Show network interface information  Manage/view the system's routing table
Manage/view the system's routing table
Forward packets through TCP session
Pivot through session by adding route in MSF
Delete route inside MSF
Allow network sniffing interaction commands
Port forwarding connections
Local host to listen
Local port to listen
Remote port to connect
Remote host to connect

#### 3. Session Handling

Description
List all sessions
Interact to session
Detach from session

#### iii. File System Commands

metaspioit Commana	Description
pwd / lpwd/getwd	Display current working directory (local / remote)



## **Ethical Hacking and Countermeasures**

## 8. Msfvenom Metasplaits Cheat Sheet



#### vi. Additional Commands

Metasploit Command	Description
shell	Drop into a shell on the target machine
hashdump	Show all password hashes in Windows
idletime	Display idle time of the machine
screenshot	Save the screenshot
clearev	Clear the logs
uictl [enable/disable] [keyboard/mouse]	Enable or disable the mouse or keyboard of the machine
use	Extension load
channel	Display active channel
reg	Access machine registry
steal_token	Attempts to steal impersonation token from target
espia	Desktop spying by screenshots
incognito	Impersonation commands
msf> search	Search for any module
msf > use exploit	Specify and exploit to use

#### 6. Session Management

Metasploit Command	Description
msf > exploit -z	Run exploit in background expecting one session
msf > session -i [SessionID]	Interact with backgrounded session
msf > exploit -j	Run exploit in background expecting one or more sessions
msf > sessions -1	List all backgrounded sessions
msf > jobs -l	List all current jobs
msf > jobs -k [JobID]	Kills job
<pre>meterpreter &gt; <ctrl+z> / meterpreter &gt; background</ctrl+z></pre>	Background current interactive session

### 7. Interface / Output Commands

Metasploit Command	Description
enumdesktops	Display all existing desktops
getdesktop	Display current desktop
keyscan_start	Start keylogger in target machine
keyscan_stop	Stop keylogger in target machine

Metasploit Command	Description
set_desktop	Configure desktop
keyscan_dump	Dump keylogger content
-p (Payload option)	Show payload standard options
-l (list type)	List module type
-f (format)	Output format
-e(encoder)	Define which encoder to use
-a (Architecture or platform	Define which platform to use
-s (Space)	Define maximum payload capacity
-b (characters)	Define set of characters not to use
-i (Number of times)	Define number of times to use encoder
-x (File name)	Define a custom file to use as template
-o (output)	Save payload
-h	Help

#### 9. Important Auxiliary Modules

Metasploit Command	Description
msf > use auxiliary/scanner/portscan/tcp msf > set RHOSTS <target IP/Subnet&gt; msf &gt; set PORTS 1-1000 msf &gt; run</target 	Port scanning module
<pre>msf &gt; use auxiliary/gather/dns_enum msf &gt; set DOMAIN target.tgt msf &gt; run</pre>	DNS Enumeration module
<pre>msf &gt; use auxiliary/server/ftp msf &gt; set FTPROOT /tmp/ftproot msf &gt; run</pre>	FTP Server module
<pre>msf &gt; use auxiliary/server/socks4 msf &gt; run</pre>	Proxy Server module
<pre>msf &gt; use auxiliary/scanner/snmp/snmp_en um msf &gt; set RHOSTS <target ip=""> msf &gt; exploit</target></pre>	SNMP Enumeration module
<pre>msf &gt; use auxiliary/scanner/sip/enumerato r msf &gt; set RHOSTS <target ip="" subnet=""> msf &gt; run</target></pre>	SIP Enumeration module
<pre>msf &gt; use auxiliary/scanner/ftp/ftp_versi on msf &gt; set RHOSTS <target ip=""> msf &gt; exploit</target></pre>	FTP Enumeration module

Metasploit Command	Description
msf > use auxiliary/scanner/discovery/ar p_sweep msf > set RHOSTS <target ip-range=""> msf &gt; set SHOSTS <target ip=""> msf &gt; set SHOSTS <target ip=""> msf &gt; set SHOSTS <target ip=""> msf &gt; set THREADS &lt; Number of concurrent threads&gt; msf &gt; run</target></target></target></target>	ARP Sweep module
msf > use auxiliary/scanner/discovery/ipv 6_neighbor msf > set RHOSTS <target IP-Range&gt; msf &gt; set SHOSTS <target ip=""> msf &gt; set SMAC <mac address=""> msf &gt; set THREADS &lt; Number of concurrent threads&gt; msf &gt; run</mac></target></target 	IPV6 Neighbor module
<pre>msf &gt; use auxiliary/scanner/discovery/ud p_probe msf &gt; set RHOSTS <target ip-range=""> msf &gt; set THREADS &lt; Number of concurrent threads&gt; msf &gt; run</target></pre>	UDP Probe module
msf > use auxiliary/scanner/discovery/ud p_sweep msf > set RHOSTS <target IP-Range&gt; msf &gt; set THREADS &lt; Number of concurrent threads&gt; msf &gt; run</target 	UDP Sweep module
<pre>msf &gt; use auxiliary/scanner/scada/modbus _findunitid msf &gt; set RHOSTS <target ip=""> msf &gt; run</target></pre>	Scan and detect Modbus Slaves
<pre>msf &gt; use x86/opty2 msf nop(opty2) &gt; generate -h Usage: generate [options] length</pre>	Generates a NOP sled of a given length