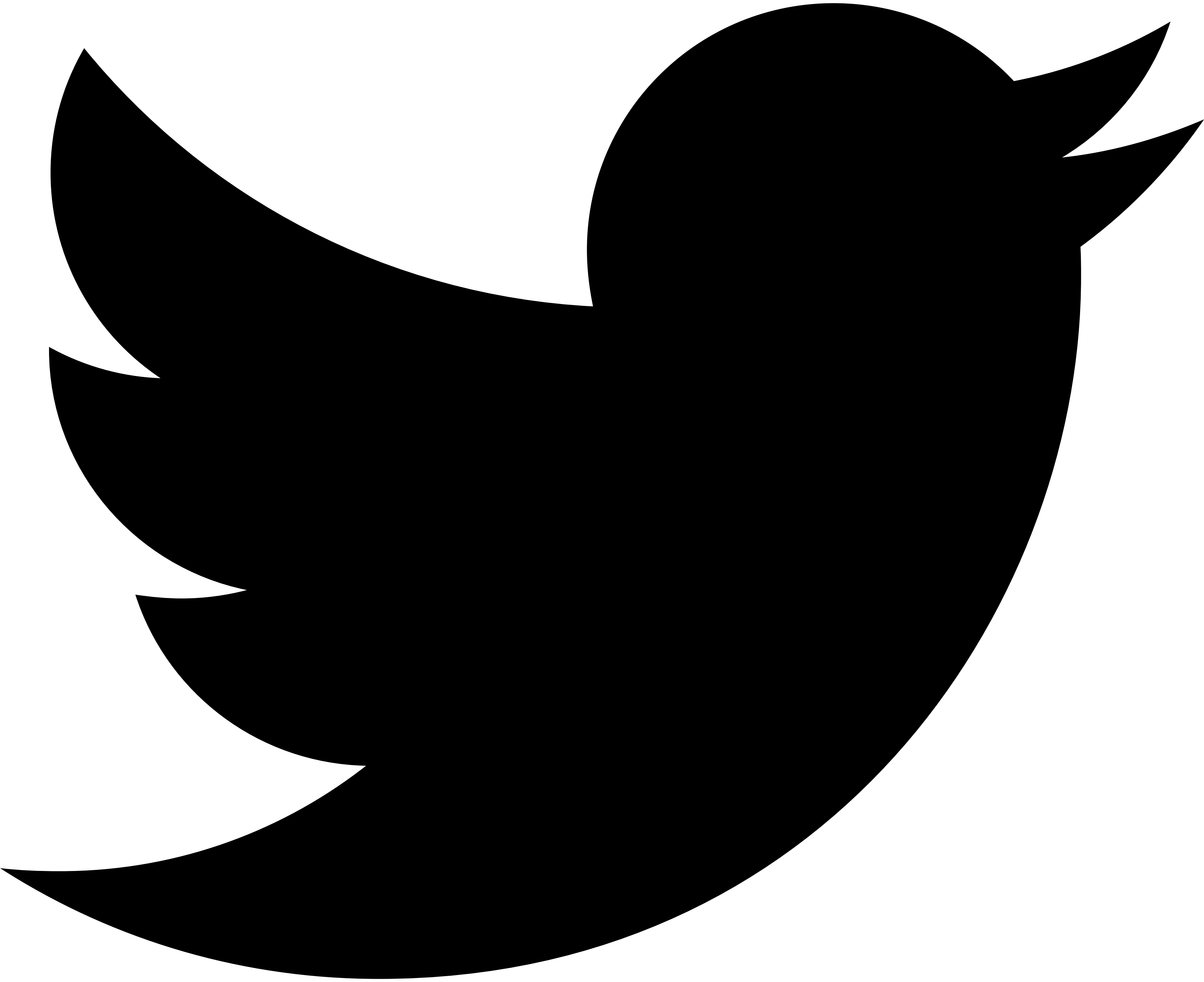
Metasploit Cheat Sheet: A Quick Guide to Master the Modules

February 9, 2023 / By Nathan House



Listen to the article

Hello hacker! We're going to take your pentesting skills to the next level with Metasploit. This powerful framework is a must-have in any ethical hacker's toolkit, so we better get you up to speed quickly.

Whether you're a seasoned red teamer or just starting out, this cheat sheet will put all the essential commands and modules right at your fingertips. We aim to give you a solid understanding of how the Metasploit Framework works and **how to use it effectively**.

Download a PDF version of the Metasploit cheat sheet **here** to keep on your desk. If you're ready to get hacking, read on!

Search cheats here

What Is Metasploit?

Metasploit is a popular open-source framework for creating, testing, and deploying exploits. It is used by hackers (ethical and otherwise) and security researchers to test the security of machines, networks, and infrastructure.

Metasploit's collection of exploits, payloads, and tools to conduct penetration testing can speed up the testing process and take on much of the heavy lifting.

Most of the available tools and exploits only require filling in some basic information, such as the target ip address and port number and possibly operating system or software version of the target. Very little modification is required of the user.

It also has the ability to easily upload files to and download files from a target system, perform network scanning, routing network traffic, and manage multiple sessions at once.

Whether you're a security professional or a student learning about cybersecurity, Metasploit is a valuable tool to have in your arsenal.

Networking Commands

These will allow you to view and manipulate network information and data transmission on a target network.

ipconfig:	Show network interface configuration
portfwd:	Forward packets
route:	View / edit network routing table

Meterpreter Commands

These commands can be used in an existing meterpreter session to enumerate and manipulate you target.

BASIC AND FILE HANDLING COMMANDS

sysinfo	Display system in formation
ps	List and display running processes
kill (PID)	Terminate a running process
getuid	Display user ID
upload or download	Upload / download a file
pwd or lpwd	Print working directory (local / remote)
cd or lcd	Change directory (local or remote)
cat	Display file content
bglist	show background running scripts
bgrun	make a script run in the background
bgkill	terminate a background process
background	Move active session to background
edit <FILE Name>	Edit a file in vi editor
shell	Access shell on the target machine
migrate <PID>	Switch to another process
idletime	Display idle time of user
screenshot	Take a screenshot
clearev	Clear the system logs
? or Help	Help showing all the commands
exit / quit :	Exit the Meterpreter session

BASIC AND FILE HANDLING COMMANDS	
shutdown / reboot	Restart the system
use	Extension load
channel	Show active channels

Process Handling Commands

Gather information on running software and processes on the target machine with these commands.

COMMAND	DESCRIPTION
getpid:	Display the process ID
getuid:	Display the user ID
ps:	Display running process
Kill:	Stop and terminate a process
getprivs	Shows multiple privileges as possible
reg	Access target machine registry
Shell	Access target machine shell
execute:	Run a specified
migrate:	Move to a given destination process ID

Interface / Output Commands

View the target desktop and capture keystrokes with these commands.

enumdesktops	Show all available desktops
Getdesktop	Display current desktop
keyscan_ start	Start keylogger in target macahine
Keyscan_ stop	Stop keylogger in target machine
set _desktop	Configure desktop
keyscan_dump	Dump keylogger content

Password Management Commands

Steal user and system passwords.

hashdump	Access content of password file – Hash file

MSF Venom Command Options

Use these flags to generate reverse shell payloads.

SWITCH	SYNTAX	DESCRIPTION
-p	– p (Payload option)	Display payload standard options
– l	– l (list type)	List module type i .e payload, encoders
– f	– f (format)	output format
– e	-e (encoder)	Define which encoder to use
-a	– a (Architecture or platform	Define which platform to use
-s	-s (Space)	Define maximum payload capacity
-b	-b (characters)	Define set of characters not to use
– i	– i (Number of times)	Define number of times to use encoder
-x	-x (File name)	Define a custom file to use as template
– o	-o (output)	Save a payload
– h	-h	Help

Conclusion

Metasploit can speed up your pentesting, help organize multiple sessions, and make you a more efficient hacker. By automating many simple but time consuming tasks, you can spend more time focused on enumerating your targets and planning your next attack steps.

You can master Metasploit with our **collection of Ethical Hacking and Penetration Testing courses** available in our member's section.

Frequently Asked Questions

⊖ What are the types of payloads?

Payloads come in either **staged** or **stageless** formats.

A **staged** payload is sent in parts. The first part is the loader which, when successfully executed, will call back to the attacker system for the remainder of the reverse shell payload. This makes the size of the packets being sent smaller and, since the system does not view the entire payload in one go, makes it more likely to evade detection from antivirus and intrusion detection systems.

A **stageless** payload is one sent entirely in one shot. It contains all the information required to initiate a reverse shell. As a result, it is a larger file and more easily detected.

⊕ What are the different types of modules in Metasploit?

⊕ Which programming language is used in Metasploit?

⊕ What is better than Metasploit?

⊕ How can I use Metasploit to hack a computer?

⊕ Can Metasploit crack passwords?

⊕ How do I update Metasploit?

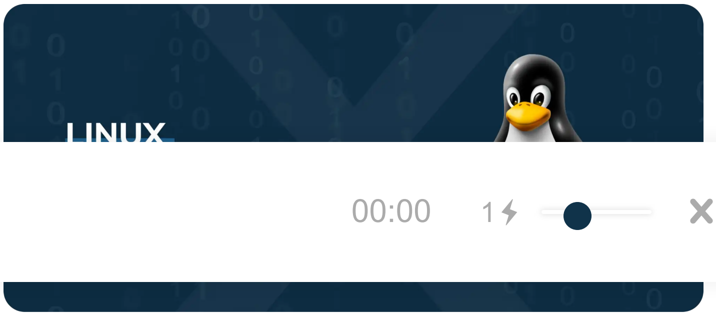
FIND OUT MORE

CATEGORIES CHEAT SHEETS HACKING

Nathan House

Nathan House is the founder and CEO of StationX. He has over 25 years of experience in cyber security, where he has advised some of the largest companies in the world. Nathan is the author of the popular "The Complete Cyber Security Course", which has been taken by over half a million students in 195 countries. He is the winner of the AI "Cyber Security Educator of the Year 2020" award and finalist for Influencer of the year 2022.

Related Articles



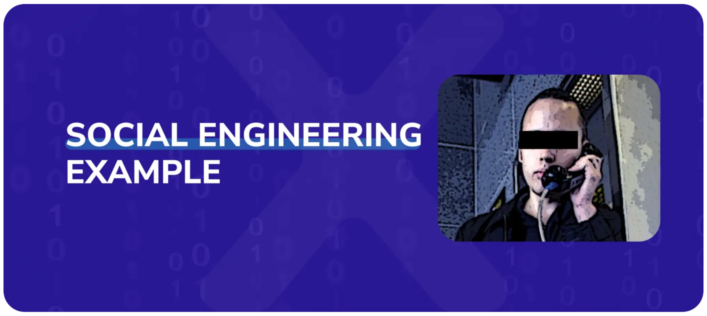
00:00 00:00 1

Nmap Cheat Sheet 2023: All the Commands, Flags & Switches

Read More »

Linux Command Line Cheat Sheet: All the Commands You Need

Read More »



Social Engineering Example

Read More »

Movies for Hackers to Watch

Read More »

INFO

Affiliates

Legal Notices

Privacy Policy

Site Map

SECURITY ASSESSMENT

Penetration Testing

Vulnerability

Source Code Review

Social Engineering

CONSULTING

Audit & Compliance

Incident Response

Risk Assessment

Security Training

00:00 00:00 1

00:00 00:00 1