

Gather info

Processes

ps faux

ps -ef

systemctl status <service>

systemctl list-units --type=service --state=active

Network

ifconfig -a Get IP address for all net interfaces

netstat -a Get connections info

netstat -anp show listening ports

netstat -anp | less Look for "LISTENING" and "ESTABLISHED"

lsof -i | less List and read open connections by processes

netstat -plnt ports/process in LISTEN state

netstat -rn OR route -v Get GW and routing table

arp -a Get arp table

ip addr Get IP address for all net interfaces

ss -a Get connections info

ss -plnt ports/process in LISTEN state

ping6 -i eth0 ff02::1 use this multicast address for all link-local IPv6 nodes

ping6 -i eth0 ff02::2 use this multicast address for all link-local IPv6 routers

ip neigh Get arp table / host in same BRD domain

Network (cont)

ip route Get GW and routing table

Users and Groups

cat /etc/passwd Get local user info

cat /etc/shadow Get user hashes

cat /etc/group Get all local groups

finger OR who See who is currently logged in

services See what they are doing

cat /etc/nsswitch.conf Get config about auth mechanisms

getent passwd Get user accounts, regardless of back-end auth mechanism

getent group Get groups, regardless of back-end auth mechanism

getent shadow If SSSD or PAM is configured, get hashes for all users, regardless of back-end auth mechanism

Remote information Gathering

finger @[targetIP] See who is currently logged in

ypcat passwd If NIS is in use, get users

ypcat group If NIS is in use, get groups and memberships

ssh vagrant@192.168.1.25 "id; hostname" runs id and hostname on the dest host

scp root@x.x.x.x:/root/.ssh/id_rsa . copy remote file to current location (with point at the end)

wget

-nd No directories, puts all files in one directory

Remote information Gathering (cont)

```
-r

-P [direc tory]
```

```
-R/A
```

Example1: `wget -nd -r -R htm,ht ml, php,asp ,aspx,cgi -P /home /560 /Cours eFiles/ 560met ada ta ex [tgt_d c`
`cat [filename]` get content from a file

Example1: `wget -nd -r -A pdf, doc, docx,x ls,xlsx -P /home /560 Course Files/ 560met ada ta ex [tgt_d c`
`cat [filename]` get content from a file

```
smbclient --list=IP --no-pass
```

```
smbclient //IP/s haredF -U " DOM AIN \us er"
```

```
smbclient //IP/s haredF -U 'NULL' -N
```

```
sudo mount //IP/s haredF /mount /point -o rw,guest
```

Sensitive Locations (cont)

```
/etc/s yst emd /sy ste m/< x>.t ar g Systemd target
et.wants directory

/etc/n ssw itc h.conf determine which
authentication
back-end a Linux
system is
configured to
use

/etc/s udo ers.d/ sudoers file

grep -iHR passw * get files with "-
passw" in them
```

Read & execute

```
-P /home /560 /Cours eFiles/ 560met ada ta ex [tgt_d c
cat [filename] get content from a file

head -n 20 [filename] get first 20 lines of [filename]

tail -n 2 [filename] get last 2 lines of [filename]

ls /dev | less putting command output as
input to less

which ls see Where your commands are
run from

./prog ram _name run a program located in the
current directory

PATH=$PATH /[anot her _di Temporary (Session's life) add
r] directories to your path
```

Miscellaneous

```
grep root * find files in the current directory that contain
theword root

man /info show detailed usage information for other
commands

whatis [command] Get a hint about What a program does

apropos network search for topics

man -k network look up something by keyword,
```

Sensitive Locations

/etc/passwd	user account info
/etc/shadow	user password info
~/.bash_history	user's history file
~/.ssh directory	SSH keys
~/.mozilla	Firefox profile
/etc/rc.d/rc <x>.d	SystemV runlevels services to run at startup



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

Not published yet.
Last updated 24th November, 2022.
Page 2 of 5.

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

Miscellaneous (cont)

<code>unset HISTFILE</code>	Disable command history/logging
<code>watch 'ls -al file.zip'</code>	monitor when a file will appear
<code>env</code>	Listing environment variables
<code>echo \$PATH</code>	View your path env variable
<code>wc -l /path/ file.txt</code>	WordCount -l count the number of lines

Working with programs/jobs

<code>[command] &</code>	run command in background as a job
<code>CTRL+Z</code>	if a program/command is running, it'll pause the job letting the process in the background paused
<code>jobs</code>	list background/pauses jobs
<code>bg %[job_number]</code>	resume program in background
<code>fg %[job_number]</code>	resume program in foreground, back to actual screen

Attack

Port Forwarding

<code>ssh -L 8888:victimIP:victimPORT usr@PIVOT-PC</code>	LOCAL - forward traffic from local port 8888 to DSThostIP:80
<code>"ssh usr@PIVOT-PC ssh root@192.168.1.119 -R 9999:192.168.1.25:80"</code>	REMOTE - forwarding traffic through the SSH connection, but your SSH connection this time will be "outbound."
<code>ssh usr@PIVOT-PC -D 9050</code>	Dynamic Port forwarding OR SOCKS proxy

Building tools

<code>tar xvf [archive.tar]</code>	untar Tape Archive Image file
<code>tar xvfz [archive.tar.gz or archive.tgz]</code>	uncompress and untar .tar.gz or tgz file
<code>" ./configure make make install"</code>	compile and install

Setup Services

`python -m SimpleHTTPServer`

`python3 -m http.server`

`impacket-smbserver -comment "Temp Dir" TMP /tmp -u user -p password`

Change configuration

<code>gedit /etc/network/interfaces</code>	set up static or dynamic network interfaces
<code>service networking restart</code>	pretty much that
<code>export PATH=/usr/sbin:\$PATH</code>	To add/usr/sbin to your PATH variable

Filesystems

<code>locate [program name]</code>	get location for a file
<code>find [directory to search] [search criteria]</code>	
<code>find / -name [filename]</code>	exhaustively looks for stuff
<code>find / -name whoami</code>	
<code>updatedb</code>	create a locate database



Filesystems (cont)

`shred --remove /tmp/s am.txt` Shred overwrites the file with alternating zeros and ones three times so that they cannot be recovered.

Accounts

`useradd -d [home dir] [username]` create a user login

`passwd` change actual user password

`passwd [username]` change other user's password

`sudo su` becomes root

`whoami` shows which account you are using

`id` get more details about your user and privs

`userdel [username]` Delete user

Firewall / IPTables

`iptables -D INPUT 2` Delete INPUT rule ID 2

`iptables -I INPUT 2 -s x.x.x.x -j DROP` fw INPUT rule ID 2, action DROP traffic from X.X.X.X

`iptables -I INPUT 1 -s x.x.x.x -p tcp --dport 4444 -j ACCEPT` allow inbound port 4444

`firewall-cmd --direct --add-rule ipv4 filter INPUT 1 -m tcp -p tcp --dport 8443 -j ACCEPT` add fw rule to allow incoming traffic

`firewall-cmd --direct --remove-rule ipv4 filter INPUT 1 -m tcp -p tcp --dport 8443 -j ACCEPT` remove fw rule to allow incoming traffic

Authentication

`ssh-keygen -t rsa -b 2048` generate a new identity file

Priv elevation

`%admins ALL=(root) NOPASSWD: /bin/bar` Let admins Group run command as root