

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 -nap show listening ports

netstat -nap | 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

ping6 -i eth0 ff02::1:3 use this multicast address for all link-local IPv6 nodes on the same link

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

ping6 -i eth0 ff02::1:2 use this multicast address for all link-local IPv6 nodes on the same link

ip neigh Get arp table / host in same BRD domain

ip route Get GW and routing table

Users and Groups

Users and Groups (cont)

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

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

lists processes in a tree-like format If SSSD or PAM is configured, get hashes for all users, regardless of back-end auth mechanism

Remote information Gathering

services

running

finger @[targetIP]

Get status

of

aprocess ypcat passwd

list all

running

services ypcat group

in systemd

ssh vagrant@192.168.1.25 "id; hostname"

scp root@x.x.x.x:/root/.ssh/id_rsa . (with point at the c)

wget

-nd

-r

-P [directory]

-R/A

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
w	See what they are doing
cat /etc/nsswitch.conf	get config about auth mechanisms

Example1: `wget -nd -r -R htm,html,php,asp,aspx,cgi:main]`

Example1: `wget -nd -r -A pdf,doc,docx,xls,xlsx -P`

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

```
smbclient //IP/share -U "DOMAIN\user"
```

```
smbclient //IP/share -U 'NULL' -N
```



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

Not published yet.
Last updated 24th November, 2022.
Page 1 of 5.

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

Remote information Gathering (cont)

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

Sensitive Locations

/etc/p asswd	user account info
/etc/s hadow	user password info
~/.bas h_h istory	user's history file
~/.ssh directory	SSH keys
~/.mozilla	Firefox profile
/etc/r c.d /rc <x>.d	SystemV runlevels services to run at startup
/etc/s yst emd /sy ste m/< x>.t ar g et.wants	Systemd target 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

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]
less OR more	view large content moving in pages
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 r]	Temporary (Session's life) add directories to your path

Miscellaneous

Miscellaneous (cont)

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

Working with programs/jobs

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

Attack

Port Forwarding

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

Building tools

tar xvf [archi ve.tar]	untar Tape Archive Image file
tar xvfz [archi ve.t ar.gz or archiv e.t gz]	uncompress and untar .tar.gz or tgz file
" ./conf igure make make instal l"	compile and install

<code>grep root *</code>	find files in the current directory that contain theword root
<code>man /info</code>	show detailed usage information for other commands
<code>whatis [command]</code>	Get a hint about What a program does
<code>apropos network</code>	search for topics
<code>man -k network</code>	look up something by keyword,



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

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

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

Setup Services

```
python -m Simple HTTP Server
```

```
python3 -m http.server
```

```
impack et- smb server -comment "Temp Dir" TMP /tmp -username tempuser -p temppass -smb2s up  
ort
```

Change configuration

```
gedit /etc/network/interfaces - set up static or dynamic  
faces network interfaces
```

```
service networking restart pretty much that
```

```
export PATH=/usr/sbin:$PATH To add/usr/sbin to your  
PATH PATH variable
```

Filesystems

```
locate [program name] get location for a file
```

```
find [directory to search] [search criteria]
```

```
find / -name [filename] exhaustively looks for stuff
```

```
find / -name whoami
```

```
updatedb create a locate database
```

```
shred --remove /tmp/sample.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 Serves  
current dir  
as
```

```
iptables -I INPUT 2 -s x.x.x.x -j DROP webcontent  
Serves  
current dir  
as  
webcontent
```

```
iptables -I INPUT 1 -s x.x.x.x -p tcp --dport 4444 -j  
ACCEPT Simple  
SMB  
Service
```

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

```
firewall-cmd --direct --add-rule ipv4 filter INPUT :
```

```
firewall-cmd --direct --remove-rule ipv4 filter INPUT  
:
```

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
```