

Linux Basics for Hackers - Notes

1) BINARIES

Located in -> /usr/bin and/or /usr/sbin

2) LINUX FILE SYSTEM

'/' -> The actual root system. The top most.

Inside it ->

/boot - Kernel image

/home - user dir

/proc - view of internal kernel data

/dev - special device files

/sbin - binaries

/root - SuperUser's Home Dir (different from '/')

/etc - Sys config

/mnt - GenPurpose Mount point

/sys - Kernel's view of HW

/bin - also binaries

/lib - libraries

/usr -> /sbin, /bin, /lib (more of the same stuff) /media - for eject-able media

3) cd Command

use '\$ > cd ..' to move up 1 level

'\$ > cd' for 2 levels & '\$ > cd' for 3 levels and so on

4) Search-based commands

\$ > locate aircrack-ng -> finds all occurrences.

\$ > whereis aircrack-ng -> finds all BINARIES of the target passed (usually with man pages).

\$ > which aircrack-ng -> finds the binary file located in the PATH variable of the system.

\$ > find -directory -option -targetExp -> finds literally everything.

Eg: \$ > find /etc -type f -name apache2

-- altho apache2.* will find all file extensions but first name as apache2

Lastly, grep to filter

\$ > ps aux | grep apache2 -> will filter from all auxilliary processes containing apache2

5) 'cat' is versatile

\$ > cat file_name -> will spill the file contents.

\$ > cat > file_name -> will let you write in it BUT WILL REPLACE ALL EXISTING DATA.

\$ > cat >> file_name -> will actually let you append the text you enter.

6) Renaming doesn't exist in Linux

So we use

\$ > mv newfile newfile2 -> to essentially rename the file

7) REMOVING A DIRECTORY

Only the directory : \$ > rmdir

When that fails : \$ > rm -r (recursively delete everything in it)

8) TEXT MANIPULATION

'head' and 'tail' :

\$ > head file_name -> first 10 lines

\$ > head -n file_name -> n number of lines from the start

\$ > tail -> for bottom lines (+ specialized with a count)

\$ > nl path_to_file_or_file_name -> will number all the lines.

// 'cat' can & should be clubbed with 'grep' as and when needed.

Eg: \$ > cat snort.conf | grep output

Sed command - for find and replace ->

\$ > sed s/search_term/replace_term/g path_to_filename > newfile_name

-> 's/' will find the term, '/g' is for replacing globally. Rest is elementary.

-> Removing the '/g' will only replace the first occurrence.

Adding a number there can limit the number of occurrences to be changed. '/3' will only replace the first 3.

Eg: sed s/mysql/MySQL/g /etc/snort/snort.conf > snort2.conf

\$ > more file_name -> offers a scroll-able page if the file is too big.

\$ > less file_name -> "less is more" -- offers a filter to search for the term should you need to -- use the '/' key. Still scroll-able but with better functionality.

9) NETWORKING

'loopback' addr -- same as 'localhost' = 127.0.0.1

\$ > iwconfig -> check for wireless adapter info -- good for getting power, the mode [monitor, managed, promiscuous] etc.

Changing IP Addr :

```
$ > ifconfig eth0 192.168.181.155
```

-> modifies what your router sees to redirect packets

Changing Netmask +/ Broadcast :

```
$ > ifconfig eth0 192.168.181.155 netmask 255.255.0.0 broadcast 192.168.1.255
```

-> Netmask is the subnet mask -- determines the portion of the IP Addr to the NW and which refers to the host. Here, first 2 octets (16 bits) represent the network and last 2 show the hosts within that network.

-> Broadcast is the addr used to send packets to all hosts on the same network segment. Default (bcz of subnet) would become 192.168.255.255 but here overridden to 192.168.1.255 -- Basically packets sent to this will be broad-casted on that specific sub-network.

MAC Spoofing :

Take down the interface, change the Addr, restart

```
$ > ifconfig eth0 down > ifconfig eth0 hw ether 00:11:22:33:44:55 > ifconfig eth0 up
```

Assigning new IP via DHCP Server :

Server runs of '*dhcpd*' - the daemon. Requested via '*dhclient*'. Requires a DHCP assigned IP addr. (Note : '*dhclient*' is for Debian, will vary in other distros.)

```
$ > dhclient eth0
```

-> Here, DHCPDISCOVER req is sent by this command and then receives an offer from the DHCP i.e DHCPOFFER. Now, ifconfig will show a diff IP addr as given by the DHCP Server.

Manipulating DNS :

Use 'dig' :

Directly pass-on the domain and add the 'ns' tag to make the domain as the nameserver itself. 'mx' will fetch the mail-exchange server.

```
$ > dig hackerarise.com ns
```

OR

```
$ > dig hackerarise.com mx
```

-- Some Linux servers use BIND (*Berkeley Internet Name Domain*) which is just a fancy name for DNS.

Changing your DNS Server :

Edit a file stored in '/etc/resolv.conf'. There you will see the domain, search & nameserver fields. Swap the values here to switch your DNS server.

Other method to do the same (although this cleanly overwrites the file's content) ->

```
$ > echo "nameserver 8.8.8.8" > /etc/resolv.conf
```

Mapping your own IP Addrs :

'hosts' file located in **/etc/hosts**. Useful for hijacking a TCP connection on your LAN to direct traffic to a malicious webserver by using a tool like '*dnsspoof*'

Usually this file has a mapping for your localhost only BUT you can map any website to any IP Address. Eg : "192.168.181.131 bankofamerica.com". Decent for local network attacks. [although '*dnsspoof*' & '*Ettercap*' can be used]

10) HANDLING SW PACKAGES

Search for package in local repo:

\$ > apt-cache search 'keyword'

-> Eg: \$ > apt-cache search **snort**

Install, Remove, Purge, Update, Upgrade :

\$ > apt-get install --name--

\$ > apt-get remove --name--

\$ > sudo apt-get update

\$ > sudo apt-get upgrade

\$ > apt-get purge --name--

(purge removes the config as well)

or use a package manager like '*synaptic*' or '*gdebi*' like a normie.

Adding Repos to Sources.list file :

\$ > mousepad /etc/apt/sources.list -> will open the list

Categories : main (OSS), universe (community maintained OSS), multiverse (SW restricted by copyright), restricted (proprietary device drivers), backports (packages from later releases)

Format : "deb http:// ----- --package_name-- main non-free contrib" etc.

11) FILE DIRECTORIES & PERMISSION

r,w,x -> read, write and execute

Granting ownership :

\$ > chown *username* *file-path-name* -> Provides the ownership of that file to that user.

\$ > chgrp *group-name* *package-or-module-name* -> Provides a user-group access to that module.

Checking Permissions :

3 Methods

A) \$ > ls -l *file-or-path-to-it* -> will lay down the whole sheet. The type, permission on the file for owner/groups/users, number of links, the owner, size in bytes, creation/mod date & its name.

Eg: "drwxr-xr-x" vs "-rw-r--r--". First letter denotes directory if 'd' or file if empty dash. Followed by the permission values for 3 groups i.e owner then group then other_users. Hence we **observe 3 values at a time**. Dash means no permission ofc.
In '-rw-r--r--' -> File, owner has read/write, group and other users only have read permissions.

B) There is a proper calculation done in Octal terms as well.

```
001 : 1 : --x  
010 : 2 : -w-  
011 : 3 : -wx  
100 : 4 : r--  
101 : 5 : r-x  
110 : 6 : rw-  
111 : 7 : rwx
```

Total RWX is 7. Since we have 3 sets of permissions, giving a full read+write+execute permission to everyone, for example, would look like ->

```
$ > chmod 777 hashcat.hcstat
```

C) UGO Syntax

Here, '-' removes a permission, '+' adds and '=' sets a permission.

Eg: Remove the write (w) permission from user on a file

```
$ > chmod u-w hashcat.hcstat -> Now -rw-r--r-- becomes -r-xr-xr--
```

Or for user and other users at once

```
$ > chmod u+x, o+x hashcat.hcstat
```

Now, you can set execute permission for yourself on a newly downloaded tool/script bcz by default Linux won't set it

```
$ > chmod 766 some_new_tool -> grants us (the owner) all permission including execute -- and everyone else only R/W permissions.
```

Masking can be done :

```
$ > umask 007 -> set it so only the user and members of the user's group have permissions.
```

Special Permissions :

SUID - set user ID & SGID - set group ID

1) Granting Temp Root w/ SUID

/etc/shadow contains all user's password -- requires root privileges to execute. SUID requires an additional bit before the permission bit. So 644 becomes 4644 i.e

```
$ > chmod 4644 file_name
```

2) Granting the Root user's Group permissions SGID

SGID works differently. Someone without execute permission can execute a file if the owner belongs to the group that has the permission to execute that file. When the bit is set on a directory -- **the ownership of new files created in that directory goes to the**

directory's creator's group rather than the file creator's group.

\$ > chmod 2644 *file_name*

[SGID bit is represented by 2 and SUID uses 4]

Privilege Escalation :

One way is by exploiting the **SUID Bit** in the system. Eg: Scripts that need to change the password usually come with the SUID bit set already. Use that to gain temporary root priv - then do something shady like getting the file at /etc/shadow.

To proceed ->

Use commands like 'find' to find the files and see their bit. Example :

\$ > find / -user root -perm -4000

Kali now starts at the top of the filesystem (because of '/') and looks everywhere below this -- the file that are owned by 'root' & specified with 'user root' + have the SUID bit set (-perm -4000).

The above command will give an output like ->

/usr/bin/chsh ; /usr/bin/gpasswd; /usr/bin/pkexec; /usr/bin/sudo; /usr/bin/passwd,... etc.

Navigating to this directory, and observing, let's say "sudo" using ls-alh, you will see ->
-rwsr-xr-x root root 140944 date sudo

Here, the 's' in place of 'x' determines the SUID bit. Logically, anyone who runs the *sudo* file has the priv of a root user -- which becomes an attack vector IF an application -- which needs access to /etc/shadow file to successfully complete their task -- can be hijacked.

12) PROCESS MANAGEMENT

To view - use ->

\$ > ps

Every process ofc has a PID or process ID.

You can use ->

\$ > kill *PID_value* to kill any process.

Issue ? The 'ps' command won't give you much info either ways. We have another command for that ->

\$ > ps aux

It shows the USER, PID, %CPU, VSZ, RSS, TTY, STAT, START, TIME & COMMAND.

Filtering by Process Name

For instance, try running *msfconsole* command to have its process running. Then use *grep* to filter it. This way you can filter all the processes running/attached to it.

\$ > ps aux | grep msfconsole

You might see a few, such as the attached DB running, the ruby script, etc, and finally the program itself.

We also have commands like "**top**" to monitor the processes sorted by their resource usage. It's active i.e refreshes on its own (every 3-4 seconds)

Managing Processes

We can alter the affinity/priority of any process by using the "*nice*" command (by passing a numeric value to its argument '-n'). Kernel always has the final say, we're just suggesting. The value ranges from -20 to +19.

Sadly, **HIGH value means LOW priority and vice versa**. So -20 is most likely to receive priority, 0 is default ofc, and +19 is least likely. Usually, any process inherits the *nice* value of its parent process.

Unsurprisingly, you can alter the priority by using the "*renice*" command.

THERE IS A DIFFERENCE !!

nice is relative. Its adds/subtracts the priority value given what you pass to it. A process with a priority of 15, when asked 'nicely' to be -10 will have a priority of 5 now. OR when asked to be +5, it will now be 20. '*nice*' can use the process via its location as well.

renice is absolute. Requires a fixed value b/w -20 and +19. BUT it sets the process to that level, cuz you've altered the deal and it prays you don't alter it any further. It also requires the PID.

Examples :

\$ > nice -n 10 /bin/some_slow_process [lowers it]

or

\$ > nice -n -9 /bin/some_slow_process [improves it]

and

\$ > renice 20 6996

[6996 is the PID of some_slow_process, and 20 is setting it]

NOTE: 'top' can also be used to alter these values.

Killing Processes

'kill' command is your friend. Just pass the PID and pass the required kill signal. There are 64 of them. Default is SIGTERM (n=15) i.e termination. Ofc they are optional. Use them as a flag arg while using kill command.

\$ > kill -n *PID*

Example :

\$ > kill -9 6887

Signal Interrupts for kill ->

SIGHUP (1) : Hangup - stops and then restarts with the same PID

SIGIN (2) : Interrupt - weak kill signal not guaranteed to work but does work mostly.

SIGQUIT (3) : Quit/Core dump - terminates but saves the process info in memory + inside pwd.

```
SIGKILL (9) : absolute kill signal. Forces the process to stop by sending the process's resources to a special device -- /dev/null
```

Basically : to restart a process : use '-1' ; for zombie/malicious : use '-9'

Running Processes in the Background

Everything runs from within the shell and the shell waits for the task/command to run/finish. It waits for this whole sequence -- hence busy & won't allow any new commands. To prevent this we can essentially detach the process from the shell. Use the '&' right after the task.

```
$ > mousepad someDoc &
```

Moving to foreground

Use the 'fg' command followed by the PID. Fetch the PID if needed.

```
$ > fg 1273
```

Process Scheduling

Either use 'at' or 'crond'.

'at' is useful for scheduling a job to run once at some point in the future -- execute 1 or many commands in the future, passed with time as argument.

Eg: \$ > msfconsole at 7:20PM June 13

OR \$ > msfconsole at now + 20 minutes

// If you just write 'at' followed by a time, then the "at>" console will open asking you to map the file/process path for it.

'crond' is best for scheduling tasks to occur everyday/week/month etc. [SEPARATE CHAPTER LATER]

13) MANAGING USER ENVIRONMENT VARIABLE

Always 2 there are. **Environment** and **Shell** variables.

EnV - always uppercase, system wide, controls the way the system acts/looks/feels + inherited by child shells or processes.

ShV - usually lowercase + valid only in the shell they are set in.

Format ->

KEY=value1

OR

KEY=value1:value2:value3...

To see the Env-V's, use

```
$ > env
```

View All

To see vars of all types (including shell, local + shell functions) use "set" (and

preferably filter it with 'more' to have a scroll-able feed)

```
$ > set | more
```

OUTPUT :

```
BASH=/bin/bash
BASHOPTS=check.....:.....
BASH_ALIASES=()
BASH_ARGC=()
....etc
```

Grep can be used to filter

```
$ > set | grep HISTSIZE
```

HISTSIZE is one such var that contains the maximum number of commands your command history file will store. It does not store the commands themselves just the number of them that can be stored.

Modify these vars

Simply set them like usual. Example:

```
$ > HISTSIZE=0
```

Making Var Changes Permanent

These modifications are not permanent, when done in the terminal this way. We need to 'export' those values from the shell to the system. Since these vars are just strings, you can simply backup the contents in a text file before using the 'export' command.

For a universal backup, use the 'set' command ->

```
$ > set> ~/valueOfAllVarsOn011125.txt
```

For singled out variables ->

```
$ > echo $HISTSIZE> ~/valueOfHISTSIZE.txt
```

then set the new value (histsize default 1000)

```
$ > HISTSIZE=0
```

then export globally

```
$ > export HISTSIZE
```

Changing the Shell Prompt

Might seem like a cool trick but useful if you have multiple shells on different machines.

That var is "PS1". Has 3 flags -> \u for current user's name, \h for hostname and \w for pwd name.

Again, same logic. You can use the 'echo \$PS1' command to fetch the current value and save it somewhere before modifying how your terminal looks. Same logic to modify this var as well and then 'export PS1' it to be seen globally.

Changing your PATH

PATH variable guides the system to look for commands like cd,ls, echo etc. The

directories that has these commands (or even the new ones) must be added to your path else they'll be shown 'not found' even though you have them. Default stuff is mostly in /usr/local/sbin and /usr/local/bin. Each location is separated by ':' respectively.

Pasting my output ->

```
/home/paradoxical/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/paradoxical/.dotnet/tools
```

To add to your PATH variable :

Say a new tool is somewhere on your drive, which is not /bin and /sbin, simply append to the variable itself ->

```
$ > PATH=$PATH:/home/kali/Documents/newHackingTool
```

You can ofc verify by seeing the PATH value and trying to run the command directly on the terminal.

NOTE : Don't add too many directories in this var, it can hog the resources if it needs to locate a lot of directories for one command.

CAUTION : Make sure to APPEND and not OVERWRITE the variable.

Using 'PATH=\$PATH:' and **not** 'PATH=' is super important.

Something like '\$ > PATH=/home/kali/Docs/newHackingTool' will simply overwrite all the contents in this var. Best to save its contents somewhere.

Creating a User-Defined Variable

Simply just name and then value. Test via 'echo' command. Use it in scripts if you want after running 'export' on it. Use 'unset' to empty it.

```
$ > MYVAR="Watch_Dogs"  
$ > export MYVAR  
$ > echo $MYVAR  
$ > unset MYVAR
```

14) BASH SCRIPTING

Very important. Apart from knowing Python/Perl/Ruby.

We run the commands directly here. As in -- more connected to the system than a GUI would let you.

Before that, some more info

/dev/null -> is a black-hole for info in Linux. Dump anything unwanted in it. Good for hiding the on-screen output of any tool/script

2> -> is basically redirecting the error from the preceding command/action. This is the 'stderr' stream. Combining this and dev/null -> \$ > _something_ 2> /dev/null can effectively suppress the errors and send them into the black hole.

Humble Beginnings :

Start with 'shebang' which declares the shell. Comments with '#' and rest are normal commands that you write on the terminal which can be written here.

```
#!/bin/bash
# this is my first bash script
echo "Hello Friend"
```

After making such scripts and saving them, you need to set the execute permission on them.

Do that by either using `$> chmod +x` OR `$> chmod 755` before the script name.

[Difference? `chmod +x` will just add 'x' bit. `chmod 755` will set it specifically for all groups. Meaning, if a group did not have any permission, they won't get it either way if we use '`+x`' but `755` will overwrite their current permission.]

And to run/execute it, simply `$ > ./script_name`

For more functionality, 'echo' can be used like `cout<<` for outputs and 'read' can be used like `cin>>` for inputs. You can directly write the var name for inputs but to use it, you need the '\$' sign. Example :

```
#!/bin/bash
echo "What's your Name?"
read name
echo "Hey" $name "!. Hope you're doing well..."
```

Simple Scanner

First we'll make a basic script that uses 'nmap' with a simple TCP scan mode to scan for ports 3306 i.e MySQL services. We send the on-screen output to `/dev/null` and then outputting the scan results to a file using the `-o` flag but with a 'G' to make it grep-able.

```
#!/bin/bash
# This script is designed to find hosts with MySQL installed on local
network for testing
nmap -sT 192.168.1.0/24 -p 3306 >/dev/null -oG MySQLscan
cat MySQLscan | grep open > MySQLscan2
cat MySQLscan2
```

Self-explanatory code. To improve it, we can use variables to input the first IP Addr, the octet value for range and optionally the port.

Slightly Advanced Scanner

```
#!/bin/bash
echo "Enter the first IP : "
read FirstIP
echo "Enter the last IP (of the octet) : "
read LastIP
echo "Enter the port (3306 for MySQL) : "
read Port
```

```

nmap -sT $FirstIP-$LastIP -p $Port >/dev/null -oG MySQLscan
cat MySQLscan | grep open > MySQLscan2
cat MySQLscan2
[Also self explanatory code]

```

Bash Helpful Commands :

Command	Meaning
:	Returns 0 or true
.	executes a shell script
bg	puts the job in background
break	exits the current loop
cd	change directory
continue	resume the current loop
echo	displays the command arg
eval	evaluate the following expression
exec	execute the command without creating a new process
exit	quits the shell
export	Export a var/fn for all -- globally
fg	brings a job to foreground
getopts	parses args to the shell script
jobs	list jobs in running in bg
pwd	pwd
read	std-input
readonly	var declaration as read-only
set	list all vars (En-V & PATH)
shift	moves the parameters to the left
test	evaluate the args
[conditional test
times	prints the user & system times
trap	traps a signal
type	shows how each arg would be interpreted as a command

Command	Meaning
umask	changes the default permission for a new file
unset	deletes a value from a var or Fn
wait	waits for a bg process to complete

15) COMPRESSING & ARCHIVING

'tar' is your buddy in most cases. **'zip'** is also a tool.
tar is