A summary of the first 3 chapters from Linux Basics for Hackers

root : Like nearly every operating system, Linux has an administrator like Windows Can do anything in the system would include such things as reconfiguring the system, adding users, and
changing passwords

Script : commands run in an interpretive environment that converts each line to source code such as Python, Perl, or Ruby

Terminal : This is a command line interface

Linux Filesystem : Linux doesn't have a physical drive (such as the C: drive) at the base of the filesystem but uses a logical filesystem instead. At the very top of the filesystem structure is /, which is often referred to as the root of the filesystem

Important subdirectories to know

root/ : The home directory of the all-powerful root user
etc/ : Generally contains the Linux configuration files—files that control when and how programs start up
home/ : The user's home directory

BASIC COMMANDS IN LINUX

pwd : will return that directory name instead.

```
kali >pwd
/root
```

whoami : to see which user you're logged in

```
kali >whoami
```

```
root
```

cd : To change directories from the terminal

```
kali >cd/etc
root@kali:/etc#
```

cd .. : To go back

```
root@kali:/etc# pwd
/etc

root@kali:/etc# cd..
root@kali:/# pwd
/
root@kali:/#
```

ls : To see the contents of a directory

```
kali >ls
bin initrd.img media run var
boot initrd.img.old mnt sbin vmlinuz
dev lib opt srv vmlinuz.old
etc lib64 proc tmp
home lost+found root usr
```

ls-l : provides us with significantly more information, such as whether an object is a file or directory, the number of links, the owner, the group, its size, when it was created or modified, and its name

```
kali >ls-la
```

“name of tool” --help or -h : to get help with this tool or this command

```
kali >aircrack-ng--help
kali >nmap-h
```

whereis : This command returns not only the location of the binary but also its source and man page if they are available

```
kali >whereisaircrack-ng
aircarckng: /usr/bin/aircarckng /usr/share/man/man1/aircarckng.1.gz
```

find : to search for a file with the name

```
kali >find /-typef-nameapache2
/usr/lib/apache2/mpmitk/apache2
/usr/lib/apache2/mpmevent/apache2
/usr/lib/apache2/mpmworker/apache2
/usr/lib/apache2/mpmprefork/apache2
/etc/cron.daily/apache2

/etc/logrotate.d/apache2
/etc/init.d/apache2
/etc/default/apache2
```

mkdir : command for creating a directory in Linux

```
kali >mkdirnewdirectory
```

cp : command to copy files

```
kali >cp oldfile /root/newdirectory/newfile
```

mv : command can be used to move a file or directory to a new location

```
kali >mvnewfilenewfile2
kali >ls
oldfile newfile2
```

rm : command to remove a file

```
kali >rmnewfile2
```

rmdir : The command for removing a directory is similar to the “rm” command for removing files
but with “dir”

```
kali >rmdirnewdirectory
rmdir:failed to remove 'newdirectory': Directory not empty
```

head : this command displays the first 10 lines of a file

```
kali >head/etc/snort/snort.conf
#
# VRT Rules Packages Snort.conf
#
# For more information visit us at:

snip
```

you can use -20 to make it 20 you can change it as you like

```
kali >head-20/etc/snort/snort.conf

#
#VRT Rule Packages Snort.conf
#
#For more information visit us at:
#.
#.
#.
#Options : enablegre enablempls enabletargetbased
enableppm enableperfprofiling enablezlib enableact
liveresponse enablenormalizer enablereload enablereact
```

tail : it’s used to view the last lines of a file

```
kali >tail/etc/snort/snort.conf
#include $SO_RULE_PATH/smtp.rules
#include $SO_RULE_PATH/specificthreats.rules
```

```
#include $SO_RULE_PATH/webactivex.rules
#include $SO_RULE_PATH/webclient.rules
#include $SO_RULE_PATH/webiis.rules
#include $SO_RULE_PATH/webmiscp.rules


#Event thresholding and suppression commands. See threshold.conf
```

you can use -20 to make it 20 you can change it as you like

```
kali >tail-20/etc/snort/snort.conf
#include $SO_RULE_PATH/chat.rules

#include $SO_RULE_PATH/chat.rules
#include $SO_RULE_PATH/chat.rules
snip
#Event thresholding or suppression commands. See theshold.conf
```

ANALYZING NETWORKS WITH IFCONFIG

ifconfig : You can use it to query your active network connections

```
kali >ifconfig
❶eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f
❷inet addr:192.168.181.131 ❸Bcast:192.168.181.255
❹Mask:255.255.255.0

snip

❺lo Linkencap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
snip
❻wlan0 Link encap:EthernetHWaddr 00:c0:ca:3f:ee:02
```

As you can see, the command ifconfigshows some useful information about the active network interfaces on the system. At the top of the output is the name of the first detected interface, eth0❶, which is short for Ethernet0 (Linux starts counting at 0 rather than 1). This is the first wired network connection. If there were more wired Ethernet interfaces, they would show up in the output using the same format (eth1, eth2, and so on).

The type of network being used (Ethernet) is listed next, followed by HWaddrand an address; this is the globally unique address stamped on every piece of network hardware—in this case, the network interface card (NIC), usually referred to as the media access control (MAC) address.

The second line contains information on the IP address currently assigned to that network interface (in this case, 192.168.181.131 ❷); the Bcast❸, or broadcast address, which is the address used to send out information to all IPs on the subnet; and finally the network mask (Mask❹), which is used to determine what part of the IP address is connected to the local network. You'll also find more technical info in this section of the output, but it's beyond the scope of this Linux networking basics chapter.

The next section of the output shows another network connection called lo❺, which is short for loopback address and is sometimes called localhost. This is a special software address that connects you to your own system. Software and services not running on your system can't use it. You would use loto test something on your system, such as your own web server. The localhost is generally represented with the IP address 127.0.0.1.

The third connection is the interface wlan0❻. This appears only if you have a wireless interface or adapter, as I do here. Note that it also displays the MAC address of that device (HWaddr).

This information from ifconfigenables you to connect to and manipulate your local area network (LAN) settings, an essential skill for hacking.

iwconfig : command to gather crucial information for wireless hacking such as the adapter’s IP address

```
kali >iwconfig
wlan0 IEEE 802.11bg ESSID:off/any
Mode:Managed Access Point: Not Associated TxPower=20 dBm
snip
lo no wireless extensions

eth0 no wireless extensions
```

To change your IP address, enter “ifconfig” followed by the interface you want to reassign (eth0) and the new IP address you want assigned to that interface.

```
kali >ifconfigeth0192.168.181.115
```

You can also change your network mask (netmask) and broadcast address with the “ifconfig” command.

```
kali >ifconfigeth0192.168.181.115netmask255.255.0.0broadcast
192.168.1.255
```

DNS:

(Domain Name System) The Internet's system for converting alphabetic names into numeric IP addresses. For example, when a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name. In this made-up example, the DNS converts the URL www.ibrahim.com into the IP address x.x.x.x Without DNS, you would have to type the series of four numbers and dots into your browser to retrieve the website

dig ** ns : to get information on a domain nameserver

```
kali >dighackers-arise.comns
snip
;; QUESTION SECTION:
;hackersarise.com. IN NS

;; ANSWER SECTION:
hackersarise.com. 5 IN NS ns7.wixdns.net.

hackersarise.com. 5 IN NS ns6.wixdns.net.

;; ADDITIONAL SECTION:
ns6.wixdns.net. 5 IN A 216.239.32.100
snip
```

Mail Exchange Server :

Exchange server, being a product of Microsoft, is a mail server and calendar server, that helps small and medium scale companies to achieve better reliability and improved performance.

It runs only on Windows Server Operating systems.

dig ** mx : to get information on a domain mail exchange server

```
kali >dighackers-arise.commx
snip
;; QUESTION SECTION:
;hackersarise.com. IN MX

;; AUTHORITY SECTION:
hackersarise.com. 5 IN SOA ns6.wixdns.net. support.wix.com
2016052216 10800
3600 604 800 3600
snip
```

Changing Your DNS Server :

```
kali >leafpad/etc/resolv.conf
```

“note : Leafpad is an open source text editor for Linux”

As you can see on line 3, my nameserver is set to a local DNS server at 192.168.181.2.
That works fine, but if I want to add or replace that DNS server with, say, Google’s
public DNS server at 8.8.8.8, I’d add the following line in the /etc/resolv.conf file to
specify the nameserver:

```
nameserver 8.8.8.8
```

change dns from here