

Chapter 1

will get you used to the file system and the terminal, and give you some basic commands.

INTRODUCTORY TERMS AND CONCEPTS:

Binaries: refers to files that can be executed, similar to executables in Windows such as ps, cat, ls, and cd

Case sensitivity: linux is case sensitive that means Desktop is different desktop so if you get the error message "file or directory not found" you probably need to check your case.

Directory: This is the same as a folder in Windows.

Home: Each user has their own /home directory, and this is generally where files you

create will be saved by default. this same as mypc in windows

root: is a superuser who can execute any command and this would include such things as reconfiguring the system, adding users, and changing passwords.

Script: This is a series of commands, Many hacking tools are simply scripts.

Shell : This is an environment and interpreter for running commands in Linux.

The Linux Filesystem

The Linux filesystem structure is somewhat different from that of Windows.

The root (/): of the filesystem is at the top of the tree,

/root : The home directory of root user

/etc: contains configuration files

/home : The user's home directory

/mnt: this content a other filesystems he mont when system restart

/bin :Where application binaries

BASIC COMMANDS IN LINUX:

Pwd:use to get where you are currently.

Whoami:use to get which user you're logged in

cd: To change directories from the terminal

ls: To see the contents of a directory ,you can add some of parmeter to get more information sush as (ls -l)

--help:in linux we can use it to get information about command

man:in addition help , with more information, such as a description and synopsis of the command or application.

Locate: is the quik way ti find the locations file
you can manually update datebase by coomand:
sudo updatedb
locate namelist.txt

whereis: If you're looking for a binary file

find : is the powerfull and flexibleof search

example:

find / -type f -name apache2 (The find command started at the top of the filesystem (/), went through every directory)

-type: Then I specify which type of file to search for, in this case ffor an ordinary file

find pathname expression actions

find -name 'file*'

find Desktop/ -size +10

find Desktop/ -atime +5

find Desktop/ -mtime + - 5 tare7 elt3del
find Desktop/ -user nameof user
find Desktop/ -type d or f file or mogald
find Desktop/ -perm

Cat :display the contents of that file, but to create a file,use > and use >>
twwithout replase

touch: for creating a file in linux

Mkdir : for creating a directory in linux

cp:use to copy file

cp a.txt /home cp a.txt b.txt
-p same as --preserve=mode,ownership,timestamps

mv:use to rename file

rm:use to remove filr

rmdir:use to remove directeroy you can use” rm -r” if the “directory is not
emp

chapter 2

TEXT MANIPULATION

Head: use if you want to view the beginning of a file, he show 10 line but you can use -n to determines the number of line

Example :

head -15 test

head a.txt head -n 5 a.txt

Tail: use if you want to view the last of a file

grep: It lets you filter the content of a file for display.

grep words file

grep -n words file return number the line

grep -c words file return number of line without return value

grep -v words file return the line dont fined the words

grep '^words' file searsh the words begin

grep 'words\$' file searsh the words a7ro word de

grep 'no...y' file search word contet of 6 char start no and a7ro y and between them 3 char

nl: display line numbers.

Less: asmiler of more but we can scrole

Chapter3

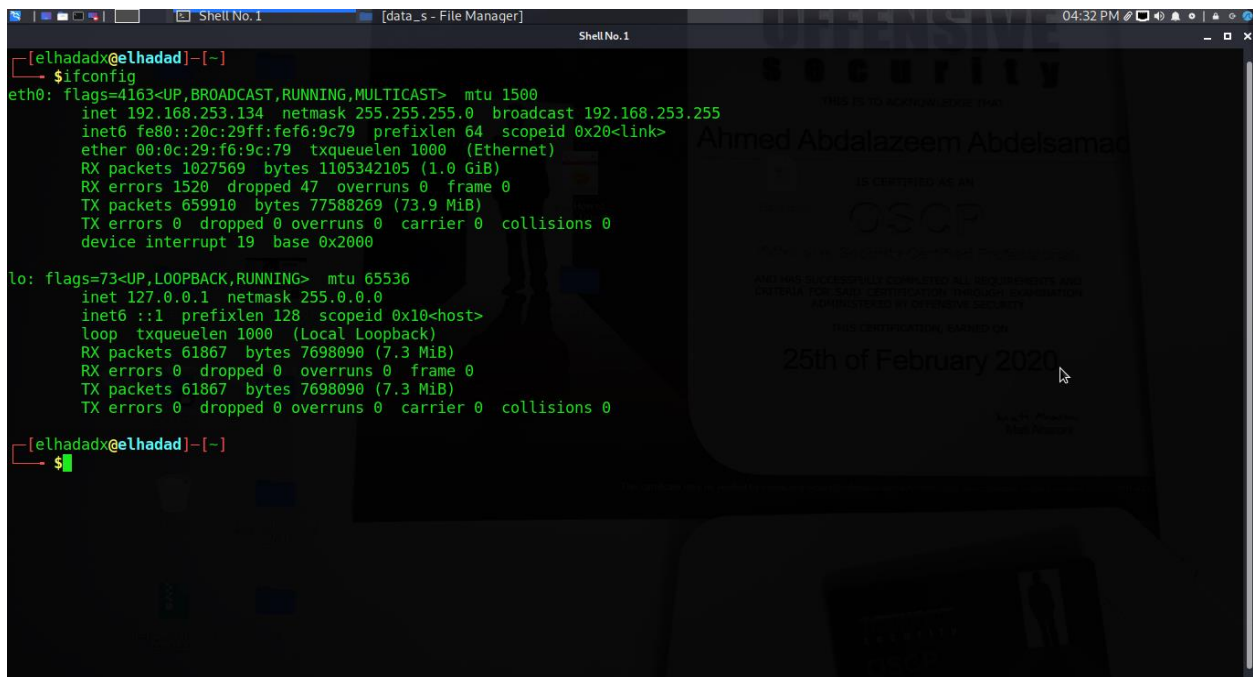
ANALYZING AND MANAGING NETWORKS

Understanding networking is crucial for any security researcher .

You need to know how to connect to and interact with that network

ANALYZING NETWORKS WITH IFCONFIG:

You can use it to query your active network connections by
simply entering ifconfig in the terminal



```
[elhadadx@elhadad]~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.253.134  netmask 255.255.255.0  broadcast 192.168.253.255
    inet6 fe80::20c:29ff:fef6:9c79  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:f6:9c:79  txqueuelen 1000  (Ethernet)
    RX packets 1027569  bytes 1105342105 (1.0 GiB)
    RX errors 1520  dropped 47  overruns 0  frame 0
    TX packets 659910  bytes 77588269 (73.9 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
    device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 61867  bytes 7698090 (7.3 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 61867  bytes 7698090 (7.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

[elhadadx@elhadad]~$
```

Interface eth0 which is short for Ethernet0

Lo:loopback for internal

Changing Your IP Address:

,To change your IP address write > ifconfig eth 0192.168.181.115

Changing Your Network Mask and Broadcast Address

You can also change your network mask and broadcast address

```
>ifconfig eth0 192.168.1.115 netmask 255.255.0.0 broadcast <  
192.168.1.255
```

Spoofing Your MAC Address

You can use ifconfig to change macaddress , then. Changing your MAC address to spoof a different MAC address is

almost trivial and neutralizes those security measures