[!tip] Data Leaks Websites:

- Have I Been Pwned ebrahim hegazy
- Dehashed AI suggestion and the rest also
- Shodan.io ebrahim hegazy
- HackedEMail ebrahim hegazy
- Intelligence X
- Hunter.io
- Snusbase
- WeLeakInfo
- LeakedSource
- LeakCheck

[!note]

- have i been pwned provide details about the breach where and when it happened and the data that was leaked.
- hacked-emails are transferred to something called constella and you have to request a demo to use it.
- shodan provides dbs compormised or protected i still don't know the usage of it.
- for hashed passwords you can use multiple websites to find the original password like hashkiller, crackstation, etc.

linux commands lectures

lec1

[!TIP] lec1

the first thing to do after installing a new linux machine is to update it using the following command:

```
sudo apt update && sudo apt upgrade -y
```

- **man**: command is used to get the manual of a command.
- **apt-cache**: search is used to search for a package.
- **apt-get install**: install is used to install a package.
- **apt-get remove**: remove is used to remove a package.
- **apt-get autoremove**: autoremove is used to remove the package and the dependencies of a package.

[!note]

when there is a question in the terminal giving you options like (Y/n) you can press enter to choose the default option which is the capital letter.

[!question] apt vs apt-get

apt is a newer version of apt-get and it has more features and is more user friendly.

lec2

[!TIP] Commands

- **locate**: is used to search for a file in the system.
- **find**: is used to search for a file in the system.
- **curl**: is used to download a file from the internet.
- **wget**: is used to download a file from the internet.
- **grep**: is used to search for a string in a file.
- **cat**: is used to display the content of a file.
- **touch**: is used to create a file.
- **echo**: is used to display a string in the terminal or to write a string in a file.

[!note]

curl by default make a get request, we can make a post request using the following command:

```
curl -X POST -d "username=admin&password=admin" http://example.com/login
```

[!example]

i downloaded a cat image using the following command:

```
curl -o cat.jpg "https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRXJA32WU4rBpx7ma
xdg-open cat.jpg # to open the image
```

-o is used to save the file with a specific name in this case cat.jpg.

[!note]

if you downloaded a web page with curl it will be displayed in the terminal, to save it in a file you can use the following command:

```
curl -o index.html "http://example.com"
```

or you can use wget to download the page directly to a file.

[!question] locate vs find

- locate is faster than find because it searches in a database that is updated daily and find searches in the system.
- find is more powerful than locate because it can search for a file with a specific size or a specific name (more options).

[!note] echo

echo can be used to write a string in a file using the following command:

```
echo "hello world" > file.txt
```

the above command will create a file called file.txt and write hello world in it, or overwrite the file if it already exists. to append to the file you can use the following command:

```
echo "hello world" >> file.txt
```

the above command will append hello world to the file.txt file.

Lec 3

[!TIP] Commands

- | **(pipe or standard output)**: is used to send the output of a command to another command.
- >: is used to write the output of a command to a file.
- »: is used to append the output of a command to a file.
- **ifconfig**: is used to display the network configuration of the machine (ip address, mac address, etc).
- < **(standard input)**: is used to read the input of a command from a file.
- **2> (standard error)**: is used to write the error of a command to a file.
- **grep -i "word to search for"**: is used to search for a string in a file case insensitive.
- **cut -d "delimiter" -f "field number"**: is used to cut a specific field from a file, it's like split in programming languages, where delimiter is the separator and field number is the index of the field.
- **awk**: is used to manipulate text files, it is a programming language.
- **sed**: is used to manipulate text files, it is a programming language.
- **&**: is used to run a command in the background.
- **;**: is used to run multiple commands in one line.
- **jobs**: is used to display the background processes.
- **head**: is used to display the first 10 lines of a file, you can specify the number of lines using the -n option.
- **tail**: is used to display the last 10 lines of a file, you can specify the number of lines using the -n option.

[!note] & vs ;

- & is used to run a command in the background as follows:

```
sleep 10 &
```

alt text

Figure 1: alt text

the above command will run the sleep command in the background for 10 seconds and you can use the terminal regardless of it's done or not, you can check the background processes using the following command:

```
jobs
```

- ; is used to run multiple commands in one line as follows:

```
echo "hello"; echo "world"
```

in the above example the command using ; will be executed after 10 seconds but the command using & will be executed immediately and the sleep command will be executed in the background. alt text

you can chaeck the background processes using the jobs command as shown in the image above.

[!note] tail

tail also can be used with th logs files to display the last lines of the logs file as follows:

```
tail -f /var/log/apache2/access.log
```

access.log is the logs file of the apache server, **access.log** is the first file checked by the security team to check the logs of the server in case of an attack.

Lec 4

[!TIP] Commands **cat**: is used to display the content of a file.

[!note] grep

- grep can be used with regular expressions to search for a string in a file as follows:

```
grep -i -o "[a-z][0-9a-z_.]*@gmail.com" file.txt
```

the above command will search for emails in the file.txt file and display them in the terminal, -o is used to display only the emails without the line number. then we can sort the distinct emails using the following command:

```
grep -i -o "[a-z][0-9a-z_.]*@gmail.com" file.txt | sort -u | tee emails.txt
```

the above command will sort the emails and save them in a file called emails.txt.

[!note] ps

ps is used to display the processes running on the machine, you can use the following command to display the processes:

```
ps aux
```

aux is used to display all the processes running on the machine, if i write only ps it will display only the processes running in the current terminal.

[!note] kill

kill is used to kill a process, you can use the following command to kill a process:

```
kill -9 PID
```

PID is the process id of the process, while the -9 is to force kill the process. alt text

[!note] top

top is used to display the processes running on the machine and the resources they are using, you can use the following command to display the processes:

```
top
```

[!note] df

df is used to display the disk space of the machine, you can use the following command to display the disk space:

```
df -h
```

-h is used to display the disk space in human readable format.

Lec 5

[!TIP] File Permissions

- **r**: read permission.
- **w**: write permission.
- **x**: execute permission.
- **-**: no permission.
- **d**: directory.
- **l**: link.
- **s**: setuid/setgid.
- **t**: sticky bit.

alt text

Figure 2: alt text

- **rwxrwxrwx**: owner, group, others.
- **chmod**: is used to change the permissions of a file.
- **chown**: is used to change the owner of a file.
- **chgrp**: is used to change the group of a file.
- **ls -l**: is used to display the permissions of a file.
- **ls -ld**: is used to display the permissions of a directory.
- **ls -a**: is used to display the hidden files.
- **ls -lh**: is used to display the permissions of a file in human readable format.
- **ls -lS**: is used to display the files sorted by size.
- **adduser**: is used to add a user.