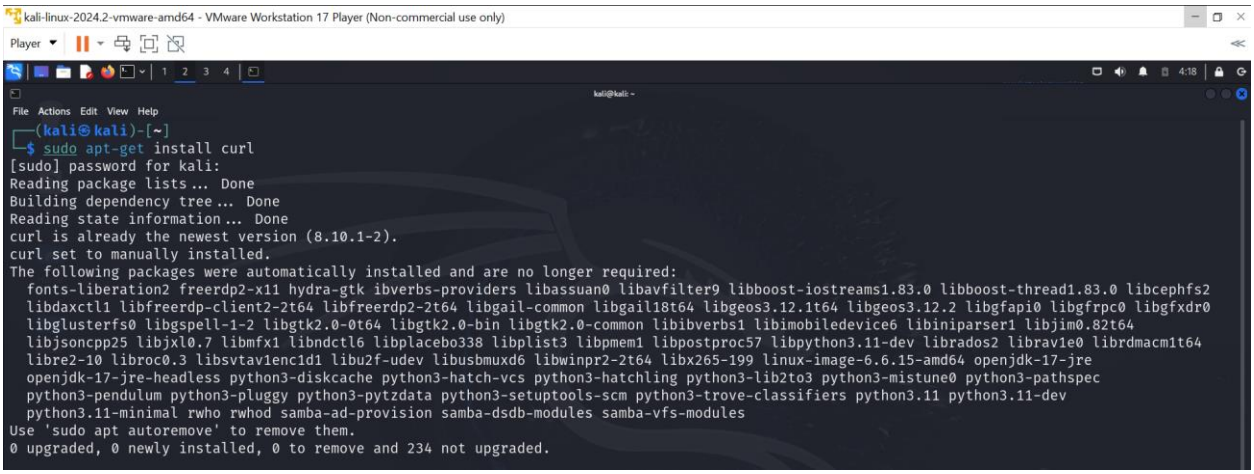
MANUAL INFORMATION GATHERING

TOOL: CURL TOOL

The curl tool is a command-line utility used to transfer data to or from a server using various protocols, including HTTP, HTTPS, FTP, and others. It's widely used for making web requests, testing APIs, downloading files, and more.

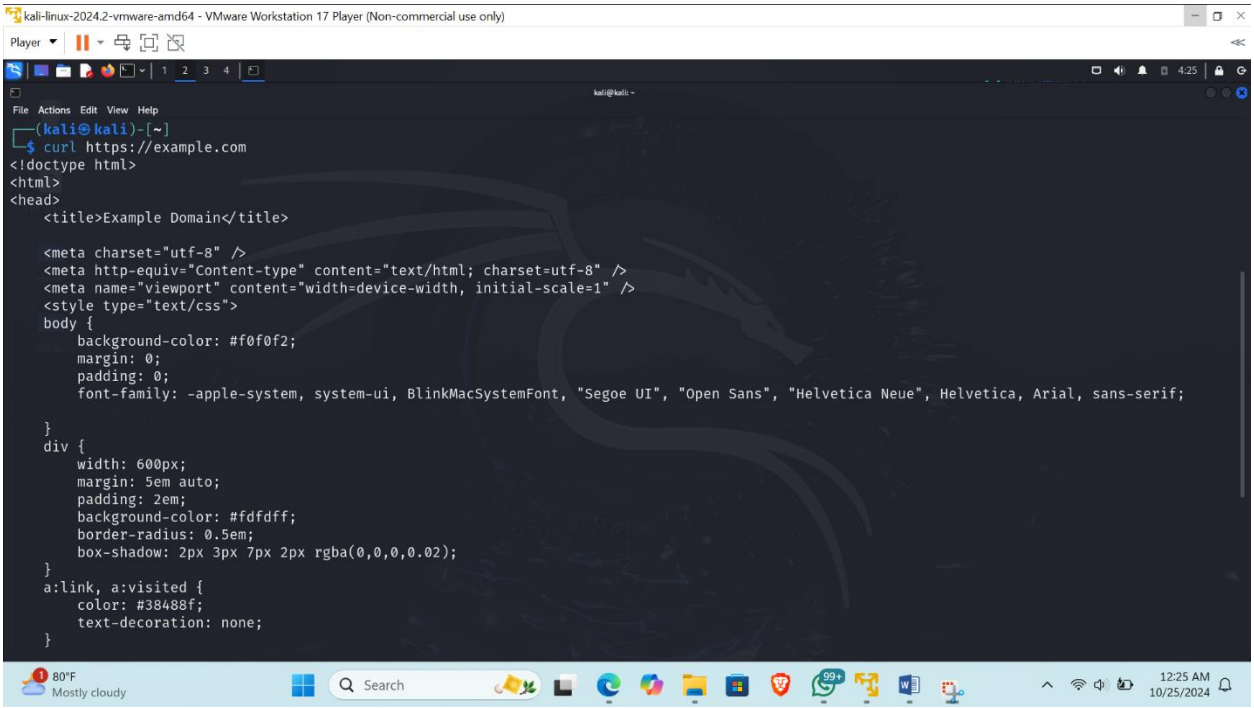
TASK 1

Installation of **"curl"** in Linux using this command: **sudo apt-get install curl**



TASK 2

We are getting the source code of a site by typing **"curl https://example.com"**



This are the brief statistic data on this output after typing “curl -o output.txt https://example.com” to save your output below

```
┌──(kali㉿kali)-[~]
└─$ curl -o output.txt https://example.com


  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1256  100  1256    0     0   1201      0  0:00:01  0:00:01 --:--:--  1201
```

TASK 3

Curl also provides you with the ability to download multiple files at once. To do this, use multiple -O options, followed by the URL of the file you want to download. For example:

curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O

```
┌──(kali㉿kali)-[~]
└─$ curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O https://arxiv.org/pdf/2103.08624.pdf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  846k  100  846k    0     0   538k      0  0:00:01  0:00:01 --:--:--  538k
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   249  100   249    0     0    903      0 --:--:-- --:--:-- --:--:--   905
```

TASK 4

When you want to resume download, you will make use of this command: **“curl -C- -O https://arxiv.org/pdf/2103.08624.pdf”**

```
┌──(kali㉿kali)-[~]
└─$ curl -C- -O https://arxiv.org/pdf/2103.08624.pdf
** Resuming transfer from byte position 249
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0   249    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

When testing a site, **curl** is useful for downloading HTTP header by typing this **“curl -I https://example.com”**

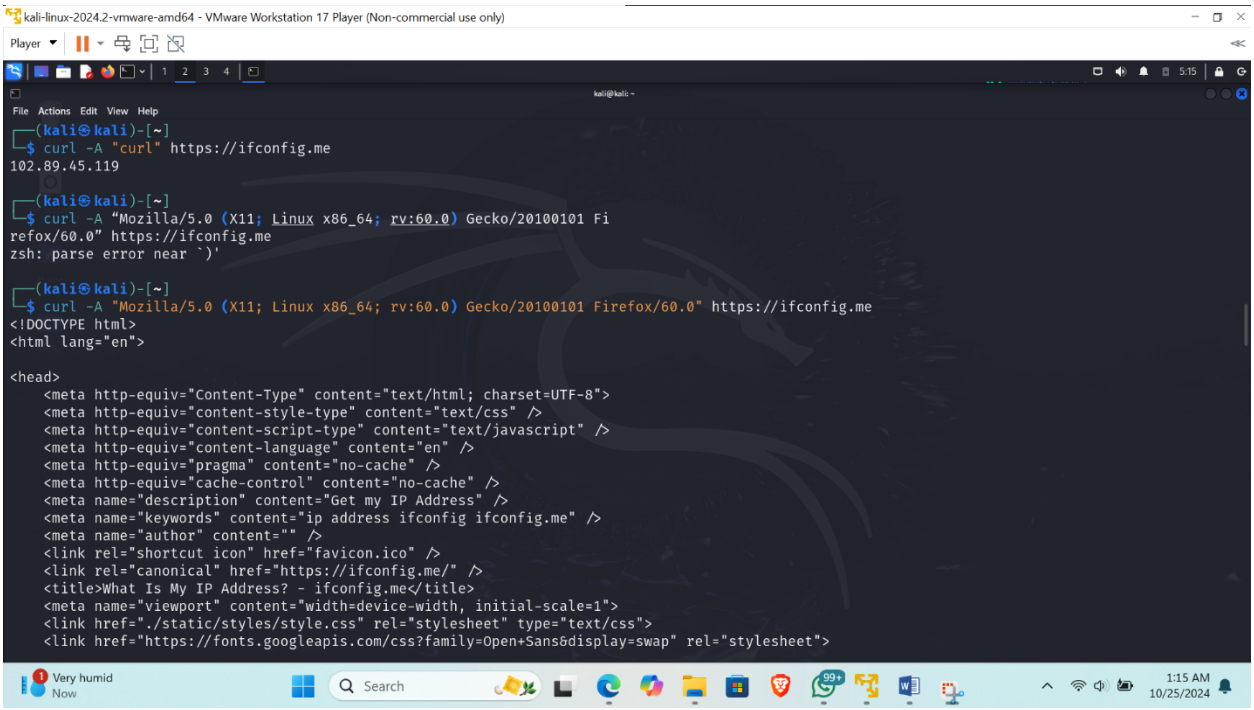
This will display many useful pieces of information, such as server info, content type, and content encoding.

```
┌──(kali㉿kali)-[~]
└─$ curl -I https://example.com
HTTP/2 200
content-encoding: gzip
accept-ranges: bytes
age: 17845
cache-control: max-age=604800
content-type: text/html; charset=UTF-8
date: Thu, 24 Oct 2024 23:56:08 GMT
etag: "3147526947+gzip"
expires: Thu, 31 Oct 2024 23:56:08 GMT
last-modified: Thu, 17 Oct 2019 07:18:26 GMT
server: ECAcc (dcd/7D82)
x-cache: HIT
content-length: 648
```

TASK 5

When attempting to download a file or gather other information using curl, you may discover that the target site may be designed to block curl. In this case, it is useful to emulate a browser, such as Firefox, to return the information you are looking for. To do this, use the following command:

curl -A “Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0” https://ifconfig.me



In this example, remote site https://ifconfig.me answers with different messages according to clients’ user-agent strings.

TASK 6

To access a protected FTP server, use the -u option to specify the username and password:

curl -u “username:pwd” ftp://mirrors.sonic.net/knoppix/live.iso

```
┌──(kali㉿kali)-[~]
└─$ curl -u “username:pwd” “ftp://mirrors.sonic.net/knoppix/live.iso”
Warning: The argument '“username:pwd”' starts with a Unicode quote where maybe an ASCII " was intended?
Warning: The argument '“ftp://mirrors.sonic.net/knoppix/live.iso”' starts with a Unicode quote where maybe an ASCII " was intended?
curl: (3) URL rejected: Port number was not a decimal number between 0 and 65535
```

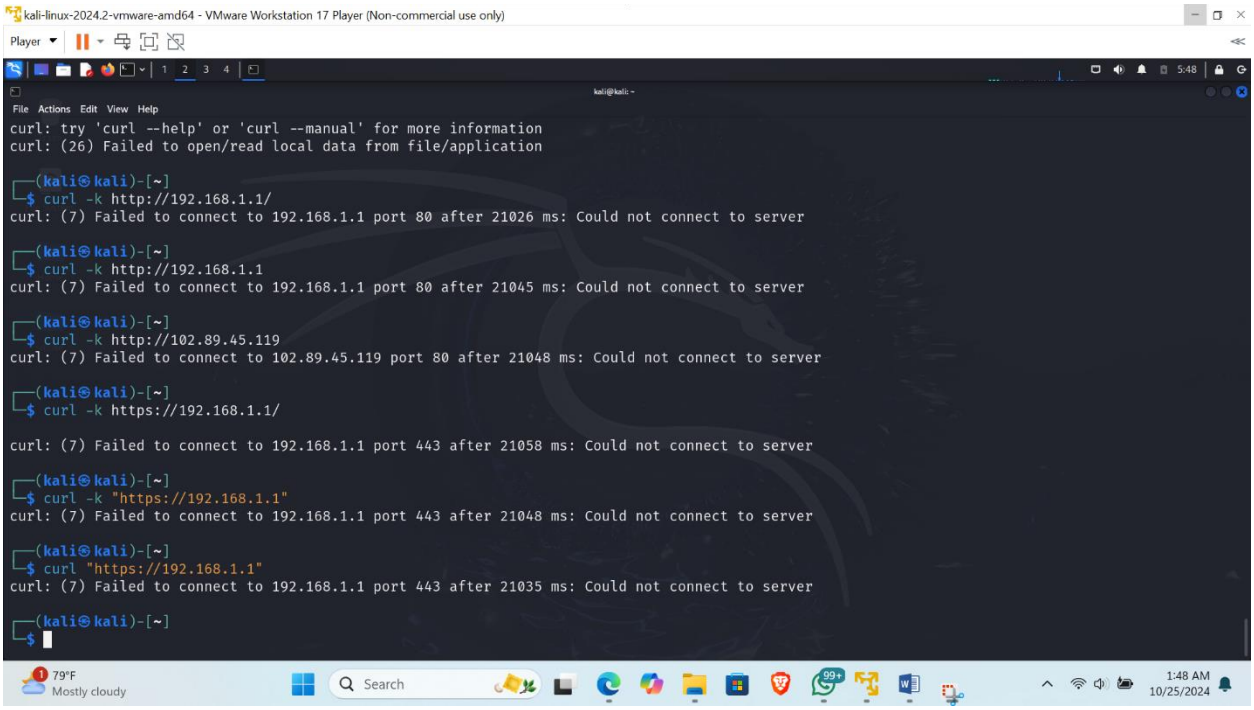
To upload a file to the server, we can use the -T option:

curl -T file.zip -u “username:password” ftp://mirrors.sonic.net/

```
┌──(kali㉿kali)-[~]
└─$ curl -T file.zip -u “username:password” ftp://mirrors.sonic.net/
Warning: The argument '“username:password”' starts with a Unicode quote where maybe an ASCII " was intended?
curl: cannot open 'file.zip'
curl: try 'curl --help' or 'curl --manual' for more information
curl: (26) Failed to open/read local data from file/application
```

TASK 7

curl -k http://192.168.1.1



TASK 8

Curl can also be configured to use a proxy. To do this, use the -x option followed by the proxy URL. For example:

curl -x 192.168.0.1:8080 http://example.com/