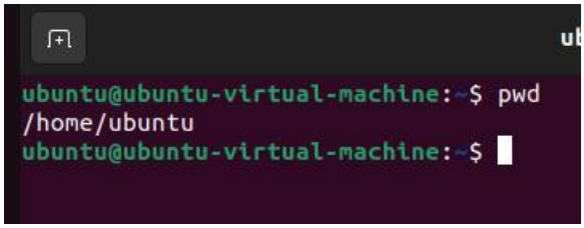
BASH CHALLENGES

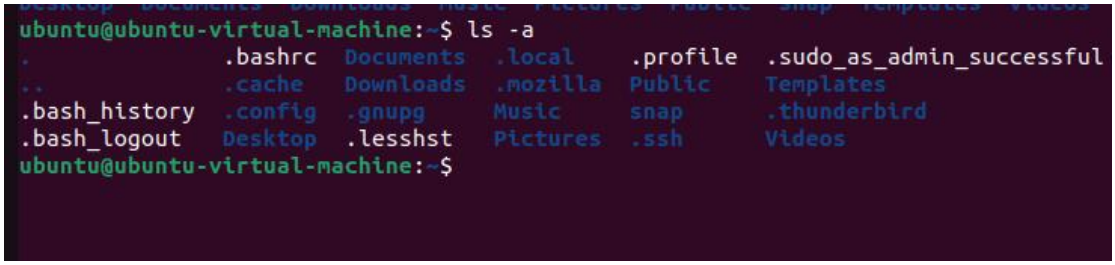
QN1.

(a) Display the path of your current directory



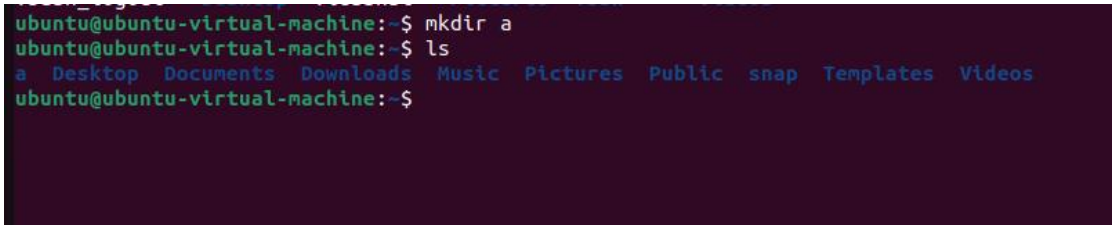
(b.) List out the contents of your current directory

(c.) List out the contents of your current directory including hidden files

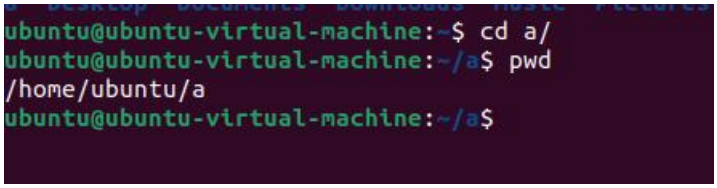


QN2.

(a.) Create a new directory named a



(b.) Move to the newly created directory a



(c.) Create a blank file named “file1”

```
ubuntu@ubuntu-virtual-machine:~/a$ touch file1
ubuntu@ubuntu-virtual-machine:~/a$ ls
file1
```

(d.) Display the file type of “file1”

```
ubuntu@ubuntu-virtual-machine:~/a$ file file1
file1: empty
ubuntu@ubuntu-virtual-machine:~/a$
```

(e.) Add the line “Hello World” to “file1” using the command echo

```
ubuntu@ubuntu-virtual-machine:~/a$ echo "hello world">file1
ubuntu@ubuntu-virtual-machine:~/a$ cat file1
hello world
```

(f.) Display the contents of “file1”

```
ubuntu@ubuntu-virtual-machine:~/a$ echo "hello world">file1
ubuntu@ubuntu-virtual-machine:~/a$ cat file1
hello world
```

(g.) Display the file type of “file1” again

```
ubuntu@ubuntu-virtual-machine:~/a$ file file1
file1: ASCII text
ubuntu@ubuntu-virtual-machine:~/a$
```

QN3.

(a.) Stay in directory a. Create a file “file2” and add the contents below using the command cat

First Line Second Line Third Line

```
ubuntu@ubuntu-virtual-machine:~/a$ touch file2
ubuntu@ubuntu-virtual-machine:~/a$ cat > file2
First line
Second Line
Third Line
```

(b.) Display the contents of “file2”

```
ubuntu@ubuntu-virtual-machine:~/a$ cat file2
First line
Second Line
Third Line
```

(c.) Display the contents of “file2” with the lines reversed

```
ubuntu@ubuntu-virtual-machine:~/a$ tac -r file2
Third Line
Second Line
First line
```

QN4.

(a.) Stay in directory a. Concatenate the contents of “file1” and “file2” and save them into a new file “file3”

```
ubuntu@ubuntu-virtual-machine:~/a$ cat file1 file2 >file3
```

(b.) Display the contents of “file3”

```
ubuntu@ubuntu-virtual-machine:~/a$ cat file3
hello world
First line
Second Line
Third Line
```

QN5.

(a.) Stay in directory a. Create 2 directories b/c with a single command

```
ubuntu@ubuntu-virtual-machine:~/a$ mkdir -p b/c
```

(b.) Create a new directory d

```
ubuntu@ubuntu-virtual-machine:~/a$ mkdir d
```

(c.) Copy the directory d to directory c using a single command

```
ubuntu@ubuntu-virtual-machine:~/a$ cp -r d b/c
ubuntu@ubuntu-virtual-machine:~/a$ ls -R b
b:
c

b/c:
d

b/c/d:
```

(d.) Delete the directory d in the current directory a

```
ubuntu@ubuntu-virtual-machine:~/a$ rmdir d
```

(e.) Copy “file3” to the directory d with a single command

```
ubuntu@ubuntu-virtual-machine:~/a$ cp file3 b/c/d/
ubuntu@ubuntu-virtual-machine:~/a$ ls b
c
ubuntu@ubuntu-virtual-machine:~/a$ ls -R b
b:
c

b/c:
d

b/c/d:
file3
```

QN6.

(a.) Go to directory d and rename “file3” to “file0”

```
ubuntu@ubuntu-virtual-machine:~/a$ cd b/c/d/
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$ ls
file3
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$ mv file3 file0
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$ ls
file0
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$
```

(b.) Stay in the same directory and move “file0” to directory a

```
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$ mv file0 ~/a
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$ ls ~/a
b  file0  file1  file2  file3
ubuntu@ubuntu-virtual-machine:~/a/b/c/d$
```

QN7.

(a.) Go to your home directory

```
ubuntu@ubuntu-virtual-machine:~$ cd
ubuntu@ubuntu-virtual-machine:~$ pwd
/home/ubuntu
ubuntu@ubuntu-virtual-machine:~$
```

(b.) Create a file named “test” in the directory a/b/c/d

```
ubuntu@ubuntu-virtual-machine:~$ touch a/b/c/d/test
ubuntu@ubuntu-virtual-machine:~$ ls -R a/
b/     file0  file1  file2  file3
ubuntu@ubuntu-virtual-machine:~$ ls -R a
a:
b  file0  file1  file2  file3

a/b:
c

a/b/c:
d

a/b/c/d:
test
```

(c.) Stay in the home directory. Find and display the path of “test”

```
ubuntu@ubuntu-virtual-machine:~$ find ~/ -name test
/home/ubuntu/Downloads/Malware_Detection_Linux/ELF_dataset/benignware/test
/home/ubuntu/a/b/c/d/test
```

QN8.

(a.) Go to directory a. Get the man page of grep and save its contents to a file named “grepman.txt”

```
ubuntu@ubuntu-virtual-machine:~$ cd a
ubuntu@ubuntu-virtual-machine:~/a$ pwd
/home/ubuntu/a
ubuntu@ubuntu-virtual-machine:~/a$ man grep > grepman.txt
ubuntu@ubuntu-virtual-machine:~/a$ ls
b  file0  file1  file2  file3  grepman.txt
```

(b.) Print the lines containing the word “FILE” (Case sensitive) in the file “grepman.txt”

```
ubuntu@ubuntu-virtual-machine:~/a$ grep "FILE" grepman.txt
       grep [OPTION...] PATTERNS [FILE...]
       grep [OPTION...] -e PATTERNS ... [FILE...]
       grep [OPTION...] -f PATTERN_FILE ... [FILE...]
       grep  searches  for  PATTERNS  in  each  FILE.  PATTERNS is one or more
       A FILE of "-"  stands  for  standard  input.   If  no  FILE  is  given,
       -f FILE, --file=FILE
              Obtain patterns from FILE, one per line.  If this option is used
       --exclude-from=FILE
              read  from  FILE  (using  wildcard  matching  as described under
```

QN9.

(a.) Go to directory a and remove the directory b with a single command

```
ubuntu@ubuntu-virtual-machine:~/a$ rm -r b
ubuntu@ubuntu-virtual-machine:~/a$ ls -R
.:
file0  file1  file2  file3  grepman.txt
```

(b.) Remove the files starting with the word “file” with a single

Command

```
ubuntu@ubuntu-virtual-machine:~/a$ rm file*
ubuntu@ubuntu-virtual-machine:~/a$ ls
grepman.txt
```

QN10.

(a.) Go to https://blog.bi0s.in/ and download the logo.png image using wget

```
ubuntu@ubuntu-virtual-machine:~/a$ wget http://blog.bi0s.in/assets/logo.png
--2024-01-02 20:05:23--  http://blog.bi0s.in/assets/logo.png
Resolving blog.bi0s.in (blog.bi0s.in)... 104.21.80.254, 172.67.155.165, 2606:470
0:3033::ac43:9ba5, ...
Connecting to blog.bi0s.in (blog.bi0s.in)|104.21.80.254|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22693 (22K) [image/png]
Saving to: ‘logo.png’

logo.png            100%[===================>]  22.16K  --.-KB/s    in 0s

2024-01-02 20:05:24 (140 MB/s) - ‘logo.png’ saved [22693/22693]
```

(b.) Do the same with python script (Hint : request library)

```
ubuntu@ubuntu-virtual-machine:~/a$ cat > logo.py
import requests

url="https://blog.bi0s.in/assets/logo.png"

response = requests.get(url)

with open("logo.png","wb") as fw:
        fw.write(response.content)
ubuntu@ubuntu-virtual-machine:~/a$ python3 -m logo
ubuntu@ubuntu-virtual-machine:~/a$ ls
grepman.txt  logo.png  logo.py  metadata.txt  __pycache__
```

(c.) Also, display the metadata of the png.

```
ubuntu@ubuntu-virtual-machine:~/a$ identify -verbose logo.png > metadata.txt
ubuntu@ubuntu-virtual-machine:~/a$ gedit metadata.txt
```

Used identify command from imagemagick

QN11.

(a.) Use **traceroute** on google.com and find list of the IP addresses and hostnames between you and google.com

```
ubuntu@ubuntu-virtual-machine:~/a$ traceroute google.com
traceroute to google.com (142.250.182.78), 64 hops max
  1   192.168.18.1  2.644ms  2.482ms  2.487ms
  2   100.82.0.1  8.768ms  7.403ms  8.623ms
  3   103.153.93.61  6.211ms  8.031ms  5.459ms
  4   10.1.6.14  21.296ms  22.031ms  30.794ms
  5   72.14.205.178  20.821ms  20.357ms  20.606ms
  6   *  *  *
  7   142.250.224.6  22.285ms  19.326ms  18.664ms
  8   142.251.55.247  22.268ms  20.662ms  21.286ms
  9   142.250.182.78  21.992ms  22.376ms  21.436ms
```

(b.) Find Subdomains,ip addresses of google.com (Tool i will add if you want me to)

```
ubuntu@ubuntu-virtual-machine:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.78
Name:   google.com
Address: 2404:6800:4007:81b::200e

ubuntu@ubuntu-virtual-machine:~$ nslookup -type=NS google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns4.google.com  has AAAA address 2001:4860:4802:38::a
```

QN12.

(a) Start a web server on port 8080 with python command

(In any directory and access the files in web browser)

```
ubuntu@ubuntu-virtual-machine:~$ cd a
ubuntu@ubuntu-virtual-machine:~/a$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
127.0.0.1 - - [04/Jan/2024 15:35:11] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [04/Jan/2024 15:35:11] code 404, message File not found
127.0.0.1 - - [04/Jan/2024 15:35:11] "GET /favicon.ico HTTP/1.1" 404 -
```

QN13.

(a.) Learn about nmap and use that scanner to scan your own machine

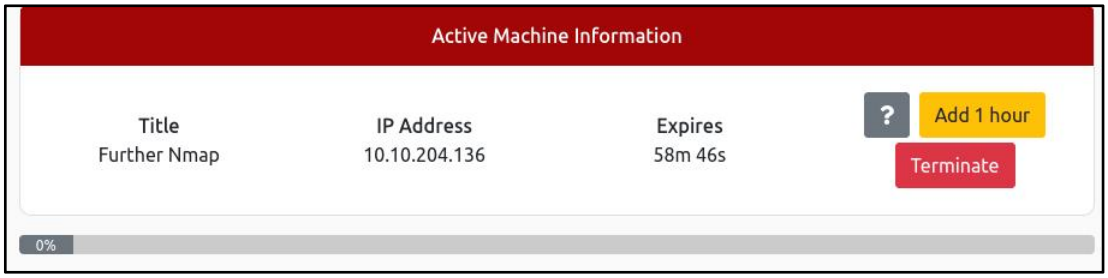
```
ubuntu@ubuntu-virtual-machine:~/a$ nmap -A localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-06 23:15 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000051s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.5 (Ubuntu Linux; protocol 2.
0)
631/tcp open  ipp     CUPS 2.4
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/2.4 IPP/2.1
|_http-title: Home - CUPS 2.4.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.56 seconds
```

(b.) Go to https://tryhackme.com/room/furthernmap and get ip address and

Scan the ip address with (-sS,-sV,-A) in your terminal include all ports

(Hint : start machine)




```
ubuntu@ubuntu-virtual-machine:~/a$ sudo nmap -sV -sS -A 10.10.204.136
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-07 00:02 IST
Nmap scan report for 10.10.204.136
Host is up (0.00090s latency).
All 1000 scanned ports on 10.10.204.136 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   ... 30

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.69 seconds
ubuntu@ubuntu-virtual-machine:~/a$
```

QN14.

(a.) Create a chat application using nc on your local machine with one terminal as server and other as the client

```
ubuntu@ubuntu-virtual-machine:~/a$ sudo bash
[sudo] password for ubuntu:
root@ubuntu-virtual-machine:/home/ubuntu/a# nc -nvlp 601
Listening on 0.0.0.0 601
Connection received on 127.0.0.1 38620
Server:Hey
Client:Hey
```

```
root@ubuntu-virtual-machine:/home/ubuntu# nc -nv 0.0.0.0 601
Connection to 0.0.0.0 601 port [tcp/*] succeeded!
Server:Hey
Client:Hey
```

(b.) Transfer a file from server to client (save that file with another name) and display the file.