IT TechFusion

Cyber Security Summer Internship Progra

Name : Hassnain Safeer

Submitted to : IT TechFusion Team

Email : hassnainsafeer805@gmail.com

Date: 25 April 2025

Weeks 01

Cyber Security Fundamental & Reconnaissance Basic :

1. Introduction to Cyber Security :

Cyber Security :

Cyber Security refers to the practice of protecting system , networks , and data from digital attacks , unauthorized access , damage , or theft .It involves a range of technologies , process , and practice designed to safeguard :

1. *Devices (like computer , smartphones)*
2. *Networks (such as the internet or internal company system)*
3. *Data (personal info , company secrets , etc)*

2. Types of Cyber attacks :

1. **Phishing :**
   - Fake emails or massages trick user int revealing personal info (like password , or credit card numbers)
   - Often disguised as trusted sources like banks or websites .
2. **Malware :**
   - Includes viruses , worms , trojans , ransomware , spyware etc .
   - Infects system to steal ,damage or lock data .
3. **Ransomware :**
   - A type of malware that lock your files and demands payments to unlock them
   - Example : WannaCry attack in 2017
4. **Denial-of-Service (DoS) and Distributed Denial-of-service(DDoS) :**
   - Floods a system or website with traffic to make it unavailable to user
   - DDoS involves multiple System attacking at once
5. **SQL Injection :**
   - Attacker inserts malicious SQL code into a database query.
   - Can expose , delete , or manipulate database contents.

3. The CIA Triad (Confidentially , Integrity , Availability)

The CIA Triad is a foundational model in cybersecurity that represents the three core principles for securing information :

1. **Confidentially :**

   Goal : Keep data private and protected from unauthorized access.

   - Example: Using encryption to protect files.
   - Applying access control (e.g passwords , permissions).
2. **Integrity :**

   Goal : Ensure data is accurate and hasn't been tempered with.

   - Example: Using checksums or hashing to detect unauthorized changes.
   - Audit logs to track who made changes and when.
3. **Availability :**

   Goal : Ensure that data and system are accessible to authorized users when needed.

   - Examples : Redundant systems and backups.
   - DDoS protection.

Linux & Terminal Basic For Security :

- **Installing Kali Linux :**

  This refer to setting up a Linux operating system on a computer or virtual machine. Popular Linux distribution includes Ubuntu , Kali Linux and Debian. Installation involves:

  - Downloading the ISO file
  - Creating on bootable USB
- **Introduction to Terminal Commands :**

  The terminal (shell) is where users can type commands to interact with the Linux System.

  Basic terminal commands

  - Ls
  - cd
  - pwd
- **File System:**

Structure : Linux has a hierarchical file system starting from the root /. Some important directories.

- /home
- /etc
- /bin

4. **Permission:**
   File access is controlled by read (r) , write (w) , and execute (x)

Permission for :

- User
- Group
- Other

5. **Navigation:**
   This involves moving through the linux file system using terminal commands like :
   - cd
   - ls
   - Find or locate
   - Tree

3 Networking Fundamental :

1. **TCP/IP Model and OSI layers:**
   - Application Layers : Handles high-level protocol like HTTP , FTP.
   - Transport Layers: Ensure data delivery (TCP/UDP).
   - Internet Layer : Handle IP addressing and routing.
   - Network Access Layers : Manages physical data transmission (e.g Ethernet)

2. **OSI Model:**
   A 7-layer model that become break down networking into :

- Physical , Data Link , Network , Transport , Session , Presentation , Application Layers.

3. **IP Addressing , ports , protocols :**
   - IP Addressing:

   Unique identifiers for devices on a network

   - IPv4 and IPv6
   - Divided into classes (A,B,C)

   - Port:

   Used to identify specific processes or services.

   Example : port 80 (HTTP) , Port 443 (HTTPS) , Port 22(SSH)

   - Protocols:

   Set of rules for communication.

   Common ones : HTTP , TCP , HTTPS , FTP.

4. **DNS, DHCP, NAT, and Firewalls:**
   - **DNS (Domain Name System):**

     Translate domain name (like google.com) to IP addresses

   - **DHCP (Dynamic Host Configuration Protocol)**

     Automatically assign IP addresses to devices on a network.
   - **NAT (Network Address Translation)**

     Converts private Ips to a public IP to access the internet.
   - **Firewalls:**

     Security systems that monitor and control incoming / outgoing network traffic.

     Can be hardware or software based

4 Ethical Hacking Introduction:

1. **Types of Hackers :**

White Hat Hacker :

Ethical hacker who help improve security.

Black Hat Hacker :

Malicious hacker who exploit vulnerabilities

Grep Hat Hacker :

Fall in between , sometimes violating rules but without harmful intent.

5 Scope and Phases of Penetration Testing:

Penetration testing simulates cyberattacks to find vulnerabilities.

Phases typically include:

- **Planning :** Defining scope and goals.
- **Reconnaissance :** Gathering information.
- **Exploitation:** Attempting to breach system.
- **Post-exploitation :** Assessing Impact and Persistence.
- **Reporting :** Documenting finding and solution

6 Reconnaissance & Information Gathering:

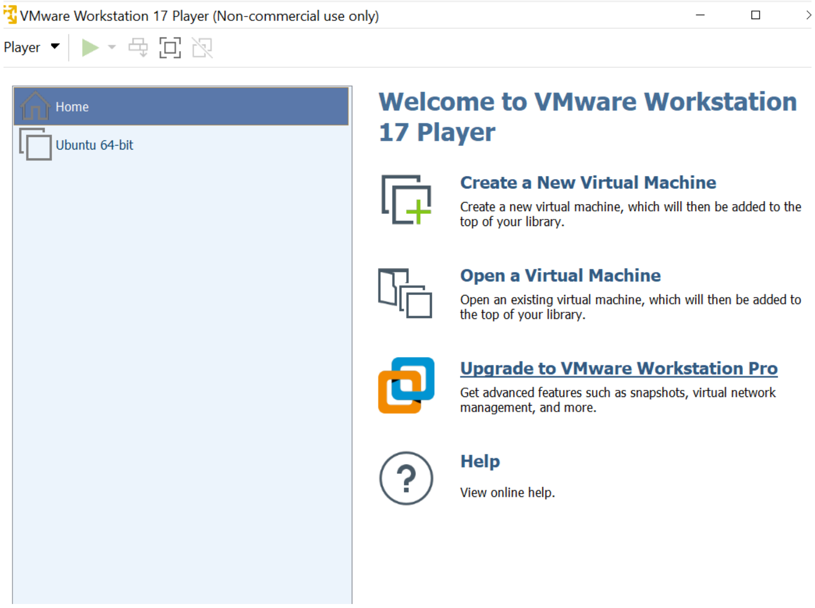
- **Passive:** Gathering data without interacting with the target directly (e.g. Public sources)
- **Active :** Directly engaging with the target system (e.g. port scans)

Tools and Techniques:

- **WHOIS,DNS Lookups :** Gather domain ownership and DNS info.
- **Google Dorking :** Use advanced search queries to find exposed data online.
- **nslookup:** DNS query tools
- **Whois :** Get domain registration details
- **TheHaverester:** Gather emails , subdomains , and more

Practical Tasks:

Setup Kali Linux (or any penetration testing distro):



Welcome to VMware Workstation 17 Player

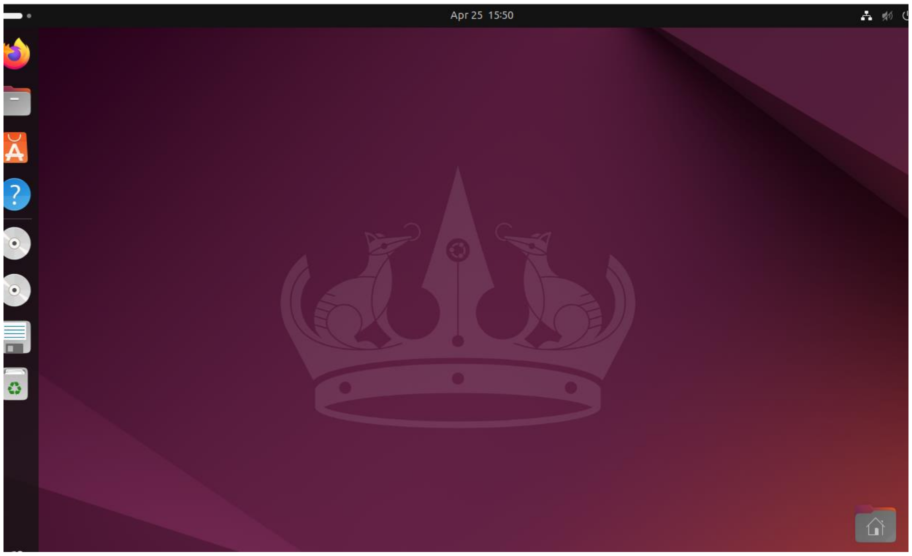
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

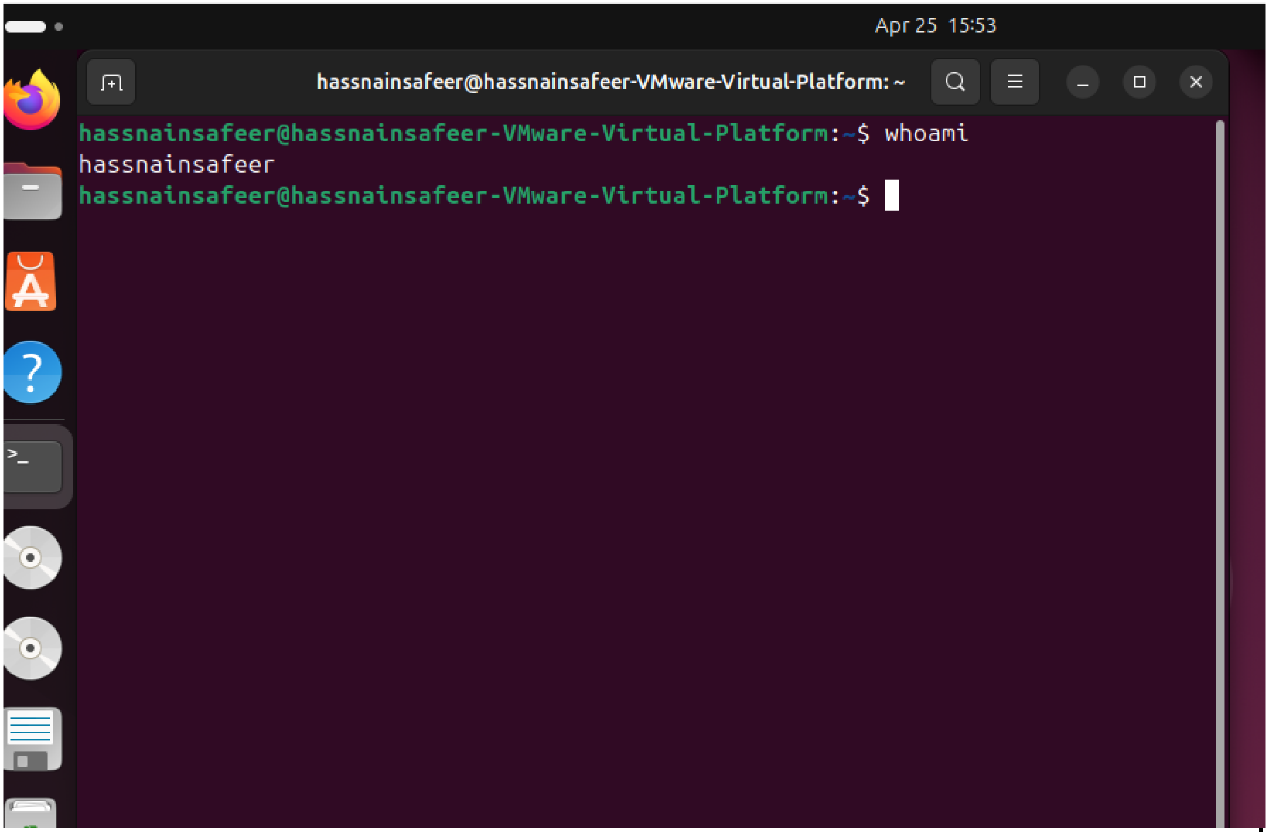
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

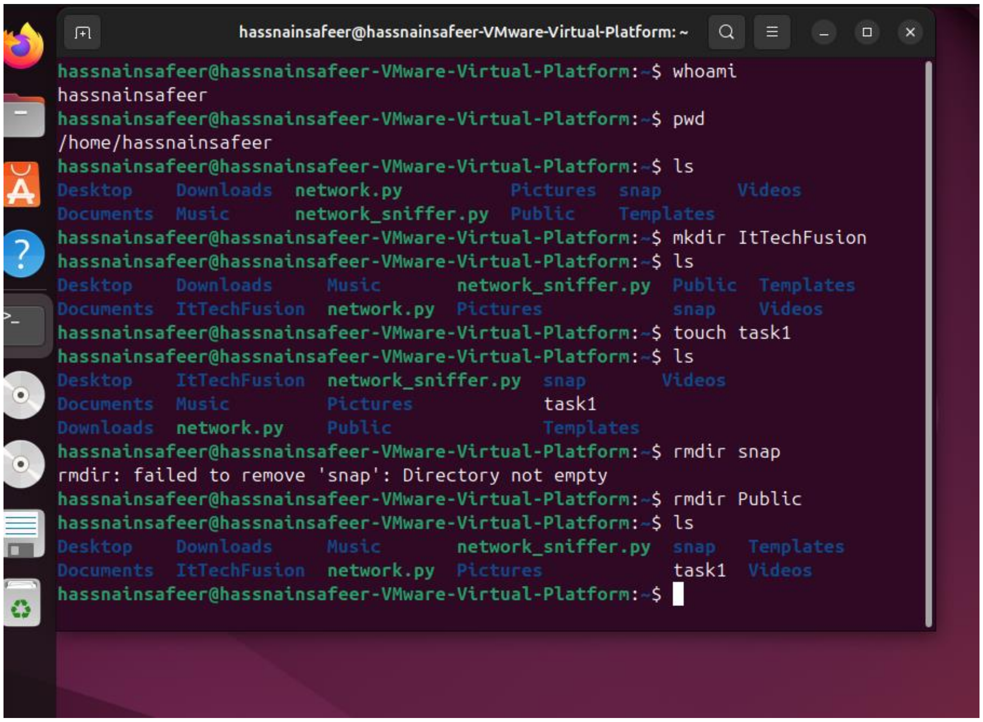
Ubuntu 64 bits operating system:





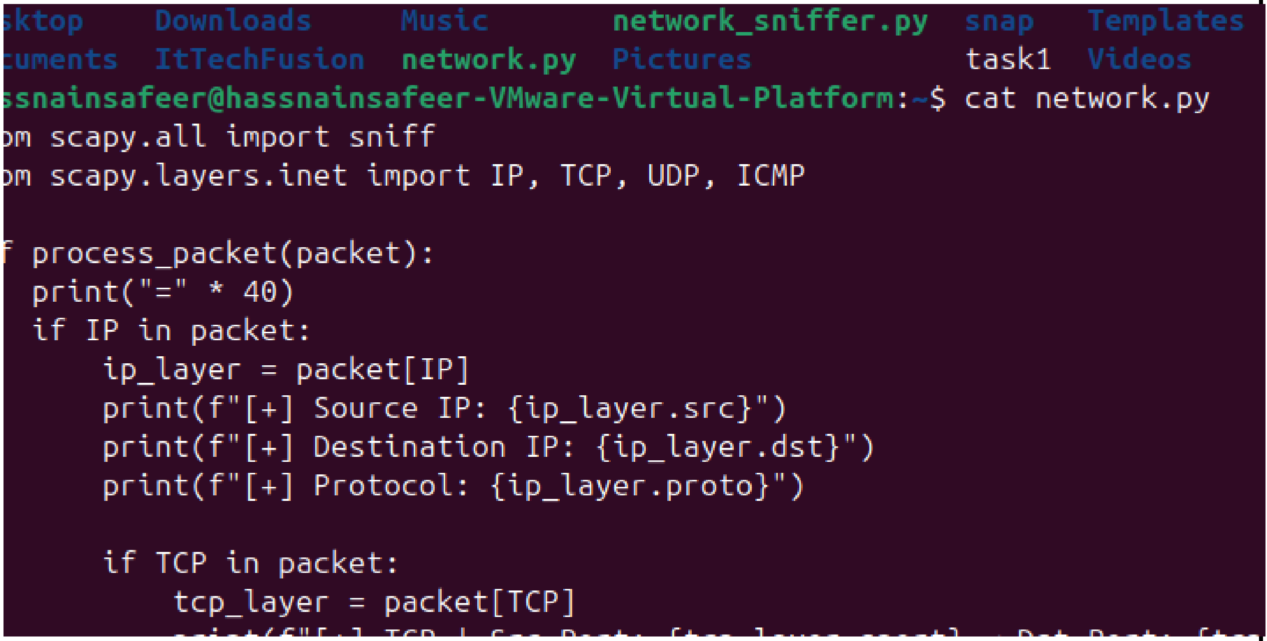
```
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ whoami
hassnainsafeer
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ 
```

HassnainSafeer in terminal .



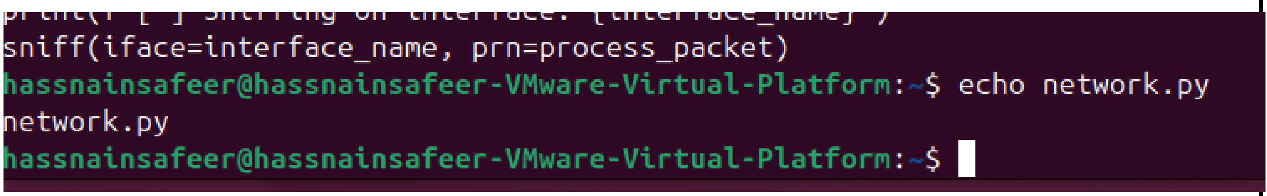
```
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ whoami
hassnainsafeer
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ pwd
/home/hassnainsafeer
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls
Desktop    Downloads  network.py          Pictures  snap       Videos
Documents  Music      network_sniffer.py  Public    Templates
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ mkdir ItTechFusion
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls
Desktop    Downloads     Music       network_sniffer.py  Public  Templates
Documents  ItTechFusion  network.py  Pictures            snap    Videos
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ touch task1
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls
Desktop    ItTechFusion  network_sniffer.py  snap       Videos
Documents  Music         Pictures            task1
Downloads  network.py    Public              Templates
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ rmdir snap
rmdir: failed to remove 'snap': Directory not empty
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ rmdir Public
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls
Desktop    Downloads     Music       network_sniffer.py  snap   Templates
Documents  ItTechFusion  network.py  Pictures            task1  Videos
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ 
```

Here are the First 7 basic command of Linux Operating System and my all commands are working properly.



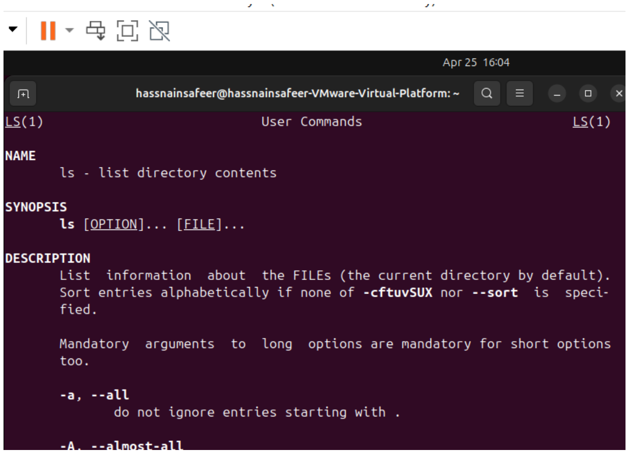
```
sktop     Downloads      Music        network_sniffer.py  snap    Templates
cuments   ItTechFusion   network.py   Pictures            task1   Videos
ssnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ cat network.py
om scapy.all import sniff
om scapy.layers.inet import IP, TCP, UDP, ICMP

f process_packet(packet):
  print("=" * 40)
  if IP in packet:
      ip_layer = packet[IP]
      print(f"[+] Source IP: {ip_layer.src}")
      print(f"[+] Destination IP: {ip_layer.dst}")
      print(f"[+] Protocol: {ip_layer.proto}")

      if TCP in packet:
          tcp_layer = packet[TCP]
          print(f"[+] TCP | Src Port: {tcp_layer.sport} -> Dst Port: {tcp
```

Cat command is working properly.



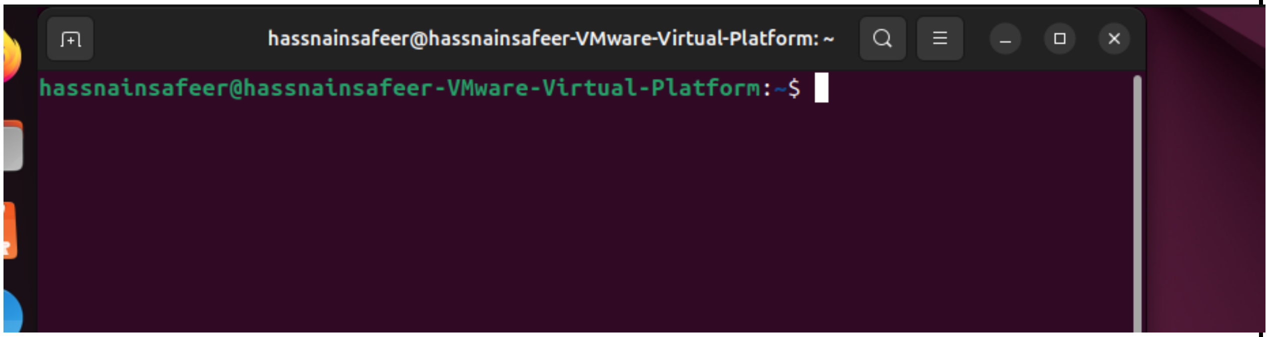
```
print(f"[+] Sniffing on interface: {interface_name}")
sniff(iface=interface_name, prn=process_packet)
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ echo network.py
network.py
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ 
```

Echo command is working properly



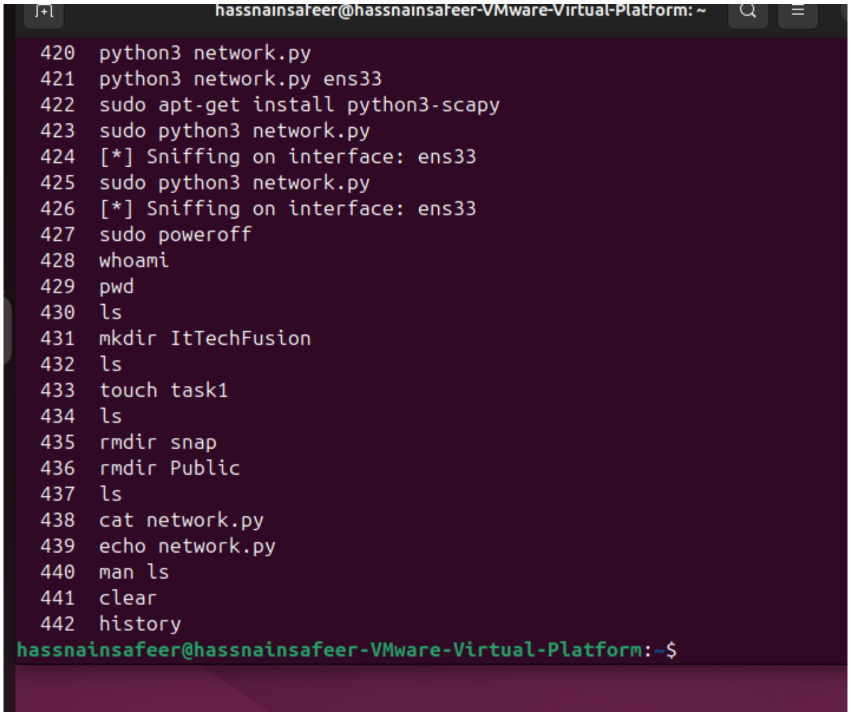
```
LS(1)                          User Commands                          LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about  the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuvSUX nor --sort  is  speci‐
       fied.

       Mandatory  arguments  to  long  options are mandatory for short options
       too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
```

Man command is working properly



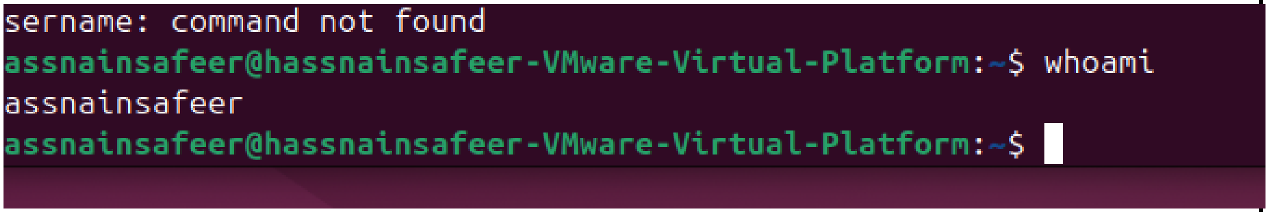
```
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$
```

Clear command is working properly

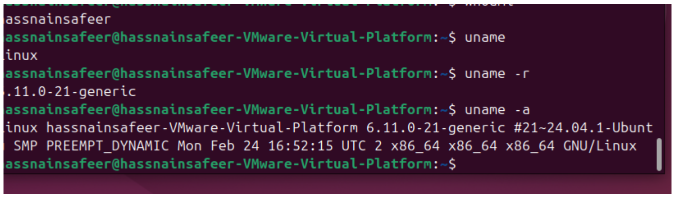


```
  420  python3 network.py
  421  python3 network.py ens33
  422  sudo apt-get install python3-scapy
  423  sudo python3 network.py
  424  [*] Sniffing on interface: ens33
  425  sudo python3 network.py
  426  [*] Sniffing on interface: ens33
  427  sudo poweroff
  428  whoami
  429  pwd
  430  ls
  431  mkdir ItTechFusion
  432  ls
  433  touch task1
  434  ls
  435  rmdir snap
  436  rmdir Public
  437  ls
  438  cat network.py
  439  echo network.py
  440  man ls
  441  clear
  442  history
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$
```

History command is working properly



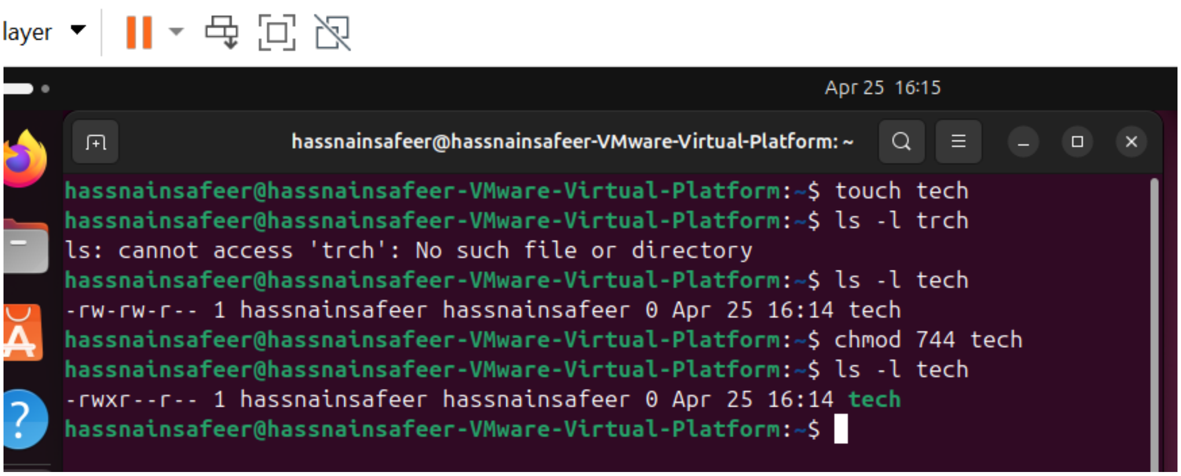
```
sername: command not found
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ whoami
assnainsafeer
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$
```



```
assnainsafeer
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ uname
inux
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ uname -r
.11.0-21-generic
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ uname -a
inux hassnainsafeer-VMware-Virtual-Platform 6.11.0-21-generic #21~24.04.1-Ubunt
 SMP PREEMPT_DYNAMIC Mon Feb 24 16:52:15 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$
```

All 15 basic commands are done.

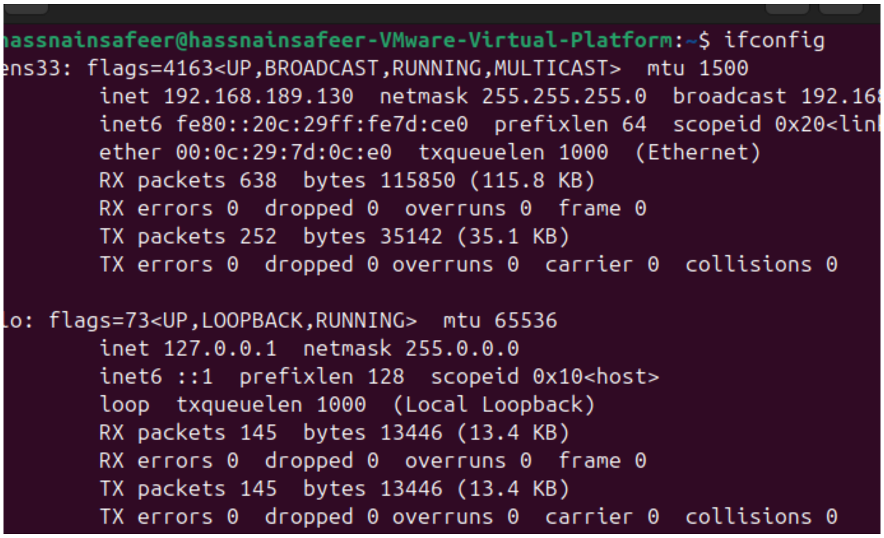
File Permission demo using chmod ls -l :



```
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ touch tech
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls -l trch
ls: cannot access 'trch': No such file or directory
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls -l tech
-rw-rw-r-- 1 hassnainsafeer hassnainsafeer 0 Apr 25 16:14 tech
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ chmod 744 tech
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ls -l tech
-rwxr--r-- 1 hassnainsafeer hassnainsafeer 0 Apr 25 16:14 tech
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$
```

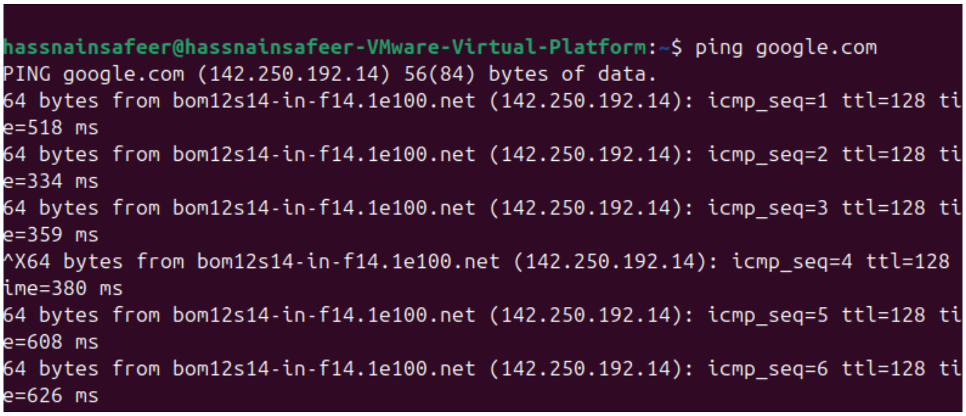
3: Network Analysis :

Using ifconfig command



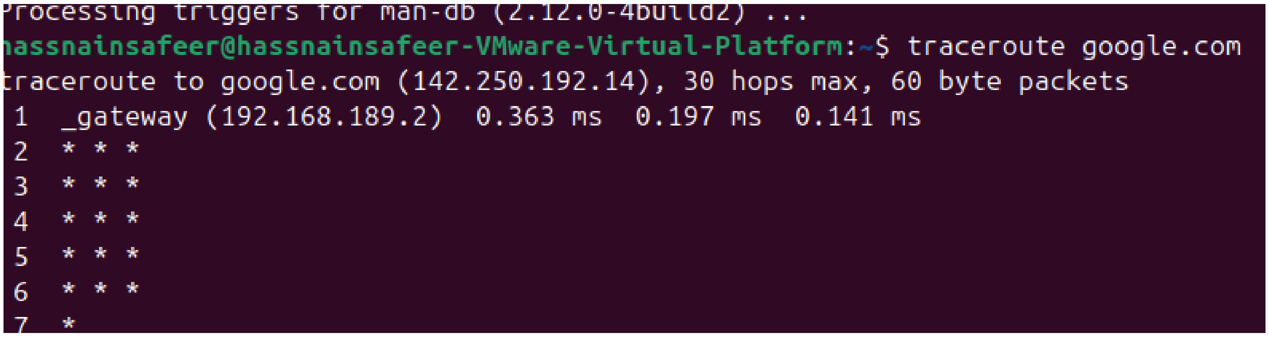
```
assnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.189.130  netmask 255.255.255.0  broadcast 192.16
        inet6 fe80::20c:29ff:fe7d:ce0  prefixlen 64  scopeid 0x20<lin
        ether 00:0c:29:7d:0c:e0  txqueuelen 1000  (Ethernet)
        RX packets 638  bytes 115850 (115.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 252  bytes 35142 (35.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 145  bytes 13446 (13.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 145  bytes 13446 (13.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ping command:



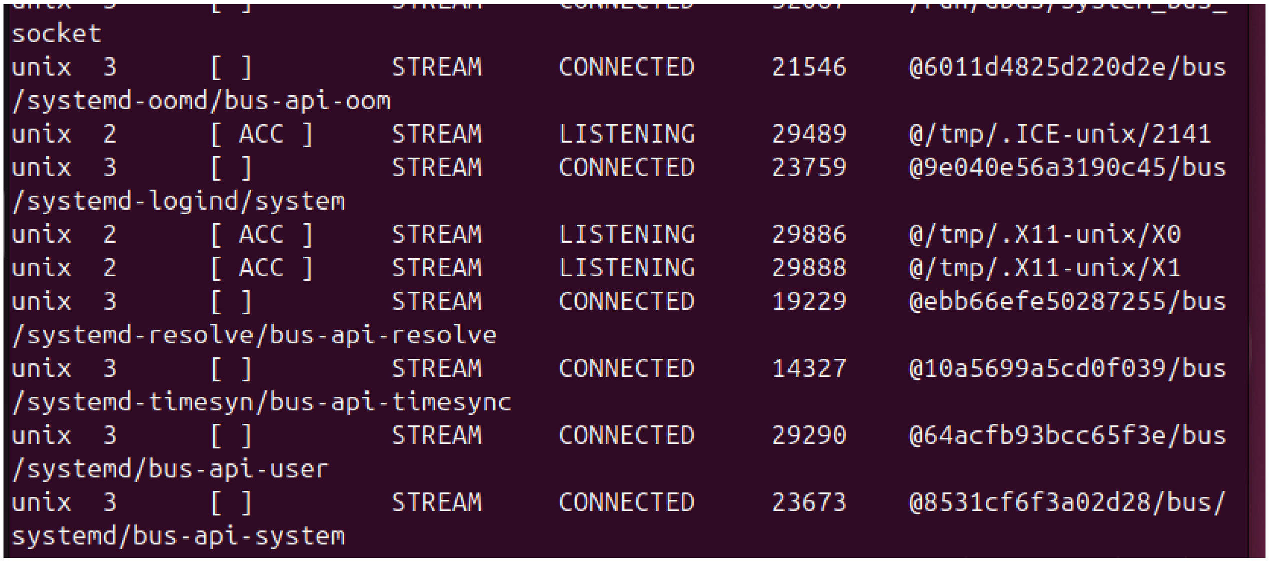
```
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ ping google.com
PING google.com (142.250.192.14) 56(84) bytes of data.
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=1 ttl=128 ti
e=518 ms
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=2 ttl=128 ti
e=334 ms
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=3 ttl=128 ti
e=359 ms
^X64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=4 ttl=128
ime=380 ms
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=5 ttl=128 ti
e=608 ms
64 bytes from bom12s14-in-f14.1e100.net (142.250.192.14): icmp_seq=6 ttl=128 ti
e=626 ms
```

Traceroute command:



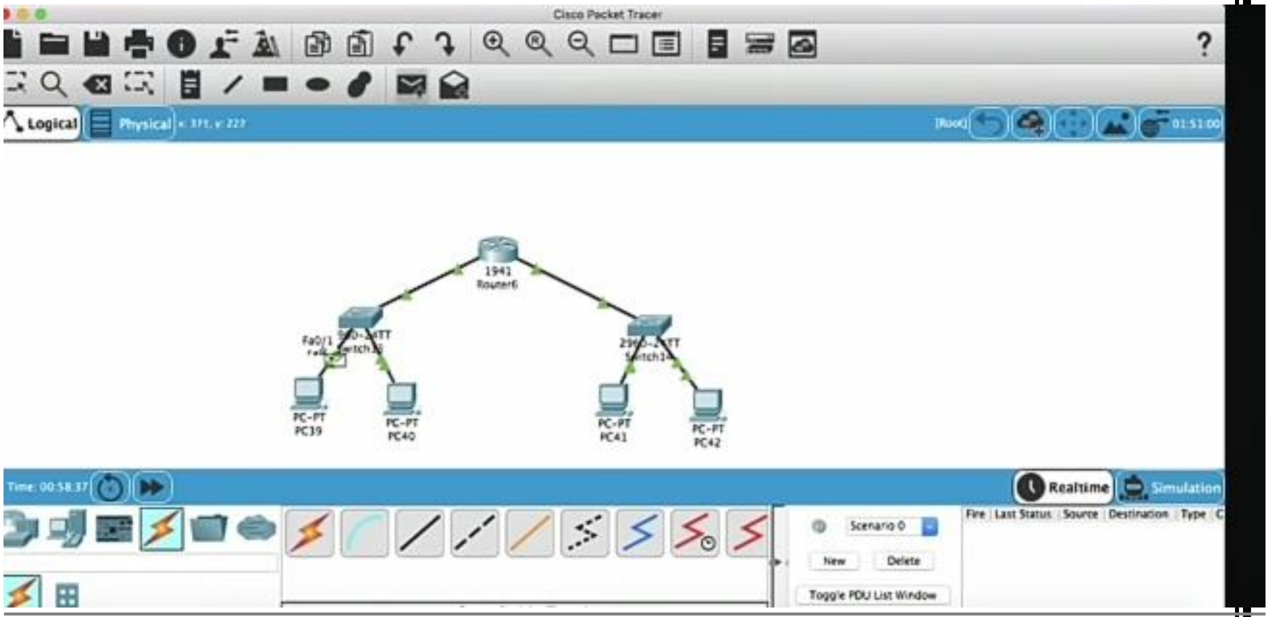
```
rocessing triggers for man-db (2.12.0-4build2) ...
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ traceroute google.com
traceroute to google.com (142.250.192.14), 30 hops max, 60 byte packets
 1  _gateway (192.168.189.2)  0.363 ms  0.197 ms  0.141 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *
```

Netstat command:

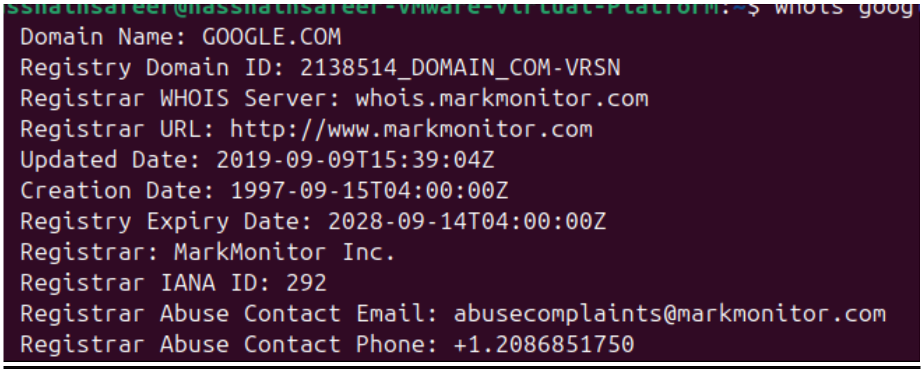


```
unix  3      [ ]         STREAM     CONNECTED     32087    /run/dbus/system_bus_
socket
unix  3      [ ]         STREAM     CONNECTED     21546    @6011d4825d220d2e/bus
/systemd-oomd/bus-api-oom
unix  2      [ ACC ]     STREAM     LISTENING     29489    @/tmp/.ICE-unix/2141
unix  3      [ ]         STREAM     CONNECTED     23759    @9e040e56a3190c45/bus
/systemd-logind/system
unix  2      [ ACC ]     STREAM     LISTENING     29886    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     29888    @/tmp/.X11-unix/X1
unix  3      [ ]         STREAM     CONNECTED     19229    @ebb66efe50287255/bus
/systemd-resolve/bus-api-resolve
unix  3      [ ]         STREAM     CONNECTED     14327    @10a5699a5cd0f039/bus
/systemd-timesyn/bus-api-timesync
unix  3      [ ]         STREAM     CONNECTED     29290    @64acfb93bcc65f3e/bus
/systemd/bus-api-user
unix  3      [ ]         STREAM     CONNECTED     23673    @8531cf6f3a02d28/bus/
systemd/bus-api-system
```

Create the basic network diagram:

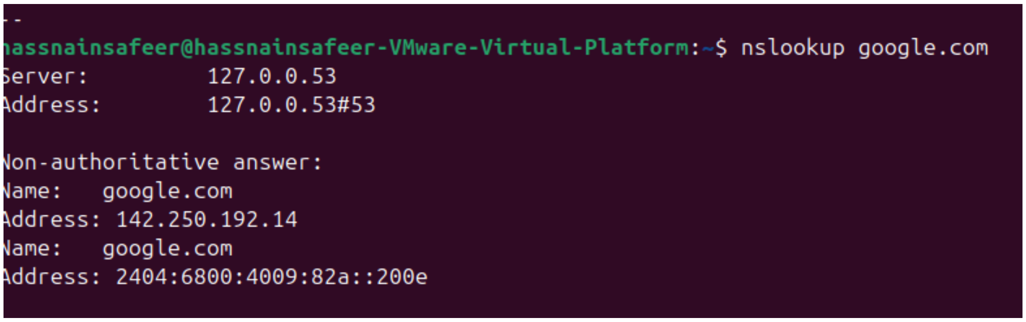


Whois command on google.com:



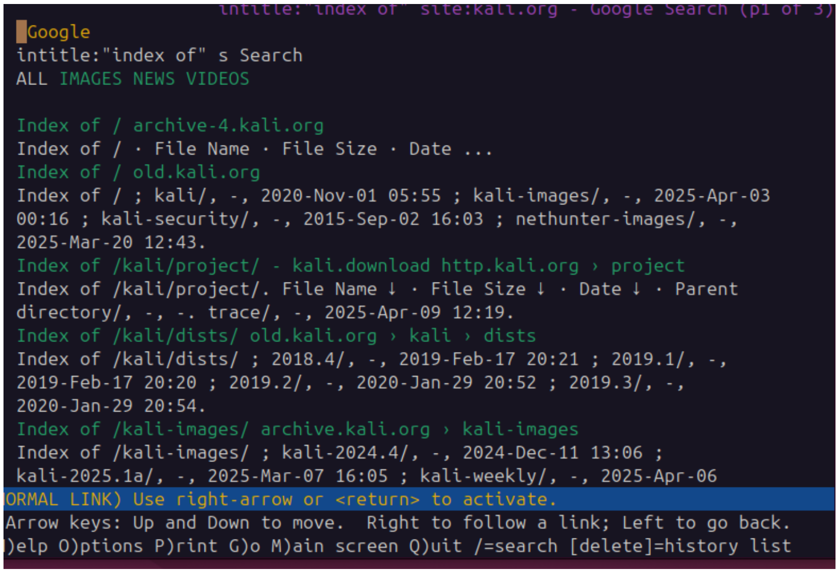
```
ssnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ whois goog
 Domain Name: GOOGLE.COM
 Registry Domain ID: 2138514_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.markmonitor.com
 Registrar URL: http://www.markmonitor.com
 Updated Date: 2019-09-09T15:39:04Z
 Creation Date: 1997-09-15T04:00:00Z
 Registry Expiry Date: 2028-09-14T04:00:00Z
 Registrar: MarkMonitor Inc.
 Registrar IANA ID: 292
 Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
 Registrar Abuse Contact Phone: +1.2086851750
```

Nslookup command on google.com:



```
--
hassnainsafeer@hassnainsafeer-VMware-Virtual-Platform:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.14
Name:   google.com
Address: 2404:6800:4009:82a::200e
```

Google Dorks get information about kali.org :

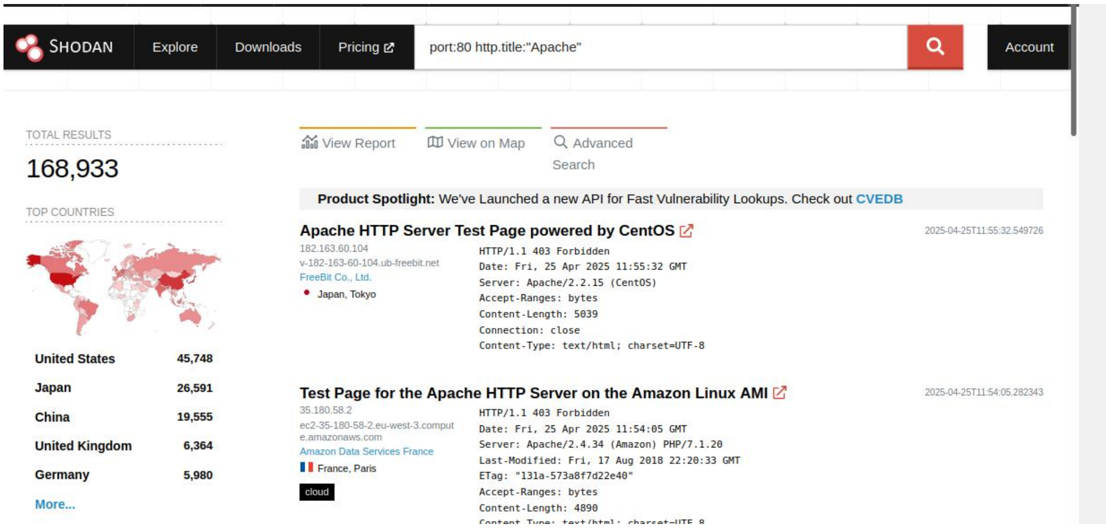


```
                    intitle:"index of" site:kali.org - Google Search (p1 of 3)
Google
intitle:"index of" s Search
ALL IMAGES NEWS VIDEOS

Index of / archive-4.kali.org
Index of / · File Name · File Size · Date ...
Index of / old.kali.org
Index of / ; kali/, -, 2020-Nov-01 05:55 ; kali-images/, -, 2025-Apr-03
00:16 ; kali-security/, -, 2015-Sep-02 16:03 ; nethunter-images/, -,
2025-Mar-20 12:43.
Index of /kali/project/ - kali.download http.kali.org › project
Index of /kali/project/. File Name ↓ · File Size ↓ · Date ↓ · Parent
directory/, -, -. trace/, -, 2025-Apr-09 12:19.
Index of /kali/dists/ old.kali.org › kali › dists
Index of /kali/dists/ ; 2018.4/, -, 2019-Feb-17 20:21 ; 2019.1/, -,
2019-Feb-17 20:20 ; 2019.2/, -, 2020-Jan-29 20:52 ; 2019.3/, -,
2020-Jan-29 20:54.
Index of /kali-images/ archive.kali.org › kali-images
Index of /kali-images/ ; kali-2024.4/, -, 2024-Dec-11 13:06 ;
kali-2025.1a/, -, 2025-Mar-07 16:05 ; kali-weekly/, -, 2025-Apr-06
ORMAL LINK) Use right-arrow or <return> to activate.
Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

5 Tool Demo:

Now I am using Shodan.io on a Target domain

I am using the port 80 of the Apache:



port:80 http.title:"Apache"

TOTAL RESULTS

168,933

TOP COUNTRIES

United States	45,748
Japan	26,591
China	19,555
United Kingdom	6,364
Germany	5,980

More...

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

Apache HTTP Server Test Page powered by CentOS 2025-04-25T11:55:32.549726

182.163.60.104
v-182-163-60-104.ub-freebit.net
FreeBit Co., Ltd.
Japan, Tokyo

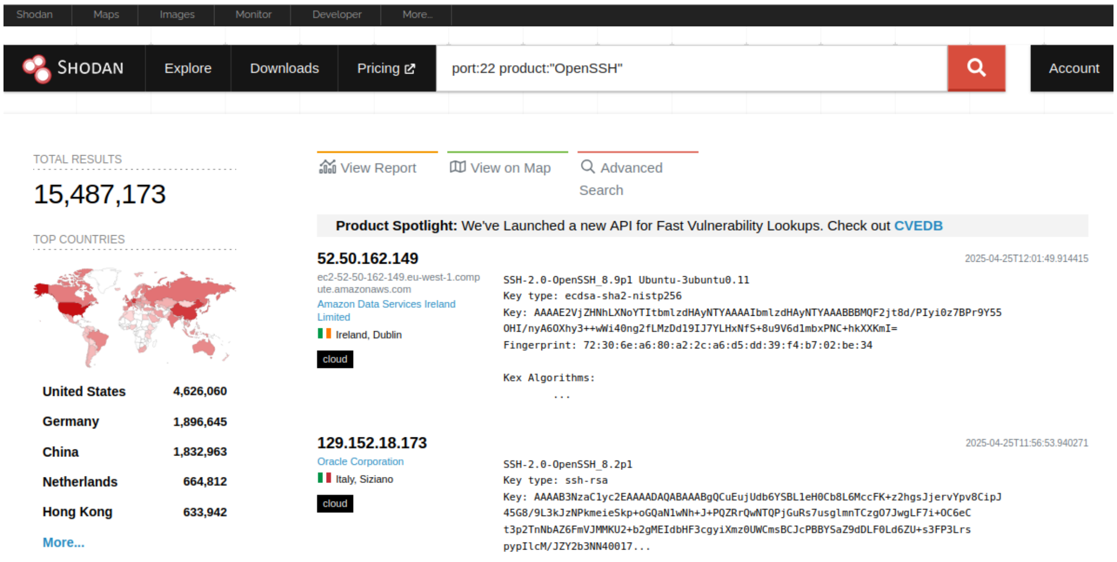
```
HTTP/1.1 403 Forbidden
Date: Fri, 25 Apr 2025 11:55:32 GMT
Server: Apache/2.2.15 (CentOS)
Accept-Ranges: bytes
Content-Length: 5039
Connection: close
Content-Type: text/html; charset=UTF-8
```

Test Page for the Apache HTTP Server on the Amazon Linux AMI 2025-04-25T11:54:05.282343

35.180.58.2
ec2-35-180-58-2.eu-west-3.compute.amazonaws.com
Amazon Data Services France
France, Paris

```
HTTP/1.1 403 Forbidden
Date: Fri, 25 Apr 2025 11:54:05 GMT
Server: Apache/2.4.34 (Amazon) PHP/7.1.20
Last-Modified: Fri, 17 Aug 2018 22:20:33 GMT
ETag: "131a-573a8f7d22e40"
Accept-Ranges: bytes
Content-Length: 4890
Content-Type: text/html; charset=UTF-8
```

Now I am check the port 22 for brute-force attack



port:22 product:"OpenSSH"

TOTAL RESULTS

15,487,173

TOP COUNTRIES

United States	4,626,060
Germany	1,896,645
China	1,832,963
Netherlands	664,812
Hong Kong	633,942

More...

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

52.50.162.149

ec2-52-50-162-149.eu-west-1.compute.amazonaws.com
Amazon Data Services Ireland Limited
Ireland, Dublin
cloud

2025-04-25T12:01:49.914415

```
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMQF2jt8d/PIyi0z7BPr9Y55
OHI/nyA6OXhy3++wWi40ng2fLMzDd19IJ7YLHxNfS+8u9V6d1mbxPNC+hkXXKmI=
Fingerprint: 72:30:6e:a6:80:a2:2c:a6:d5:dd:39:f4:b7:02:be:34

Kex Algorithms:
        ...
```

129.152.18.173

Oracle Corporation
Italy, Siziano
cloud

2025-04-25T11:56:53.940271

```
SSH-2.0-OpenSSH_8.2p1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCuEujUdb6YSBL1eH0Cb8L6MccFK+z2hgsJjervYpv8CipJ
45G8/9L3kJzNPkmeieSkp+oGQaN1wNh+J+PQZRrQwNTQPjGuRs7usglmnTCzgO7JwgLF7i+OC6eC
t3p2TnNbAZ6FmVJMMKU2+b2gMEIdbHF3cgyiXmz0UWCmsBCJcPBBYSaZ9dDLF0Ld6ZU+s3FP3Lrs
pypIlcM/JZY2b3NN40017...
```

THE END