

Q1. Set up a small network using at least two devices and ping each other. Document the process and explain the results.

```
kali@kali: ~
File Actions Edit View Help
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.238.120 netmask 255.255.255.0 broadcast 192.168.238.255
        inet6 2409:40d4:1018:87f7:2765:fafde:ee18:fbe5 prefixlen 64 scopeid 0x0<global>
            inet6 2409:40d4:12a:89f8:dc7e:382e:7683:16f2 prefixlen 64 scopeid 0<global>
                inet6 fe80::3dbf:5a32:535a:c32d prefixlen 64 scopeid 0x20<link>
                    ether 00:0c:29:c7:d0:ac txqueuelen 1000 (Ethernet)
                    RX packets 27 bytes 4334 (4.2 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 59 bytes 7268 (7.0 KiB)
                    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 8 bytes 480 (480.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 480 (480.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

--(kali㉿kali)-[~]
$
```

```
--(kali㉿kali)-[~]
$ ping 192.168.238.140
PING 192.168.238.140 (192.168.238.140) 56(84) bytes of data.
64 bytes from 192.168.238.140: icmp_seq=1 ttl=64 time=5.15 ms
64 bytes from 192.168.238.140: icmp_seq=2 ttl=64 time=4.73 ms
64 bytes from 192.168.238.140: icmp_seq=3 ttl=64 time=5.24 ms
64 bytes from 192.168.238.140: icmp_seq=4 ttl=64 time=208 ms
64 bytes from 192.168.238.140: icmp_seq=5 ttl=64 time=209 ms
64 bytes from 192.168.238.140: icmp_seq=6 ttl=64 time=5.26 ms
64 bytes from 192.168.238.140: icmp_seq=7 ttl=64 time=3.01 ms
64 bytes from 192.168.238.140: icmp_seq=8 ttl=64 time=5.04 ms
64 bytes from 192.168.238.140: icmp_seq=9 ttl=64 time=3.32 ms
64 bytes from 192.168.238.140: icmp_seq=10 ttl=64 time=210 ms
64 bytes from 192.168.238.140: icmp_seq=11 ttl=64 time=210 ms
64 bytes from 192.168.238.140: icmp_seq=12 ttl=64 time=5.37 ms
64 bytes from 192.168.238.140: icmp_seq=13 ttl=64 time=3.57 ms
```

```
Administrator: C:\Windows\system32\cmd.exe
Link-local IPv6 Address . . . . . : fe80::e412:1ad0:dfed:f9a4%13
IPv4 Address . . . . . : 192.168.238.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::800b:ecff:fe2c:2da1%13
                                                192.168.238.140

Tunnel adapter isatap.{07140AEE-834B-48F7-91FB-231204FD6F63}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : 

C:\Users\IEUser>ping 192.168.238.120

Pinging 192.168.238.120 with 32 bytes of data:
Reply from 192.168.238.120: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.238.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\IEUser>S
```

Explaination:-

- After this, we checked their IP addresses and ping them each other using “ping” command.
- First, we installed two machines(kali & windows) on vmware then set their network type as bridged network.
- Here no packet loss in ping, it means our machines are interconnected to each other.
- Now, Machines (both kali linux and windows) can communicate to each other.

Q2. Use the tracert command on your college website. Explain the steps and the significance of the results obtained.

```
[root@kali]~[/home/kali]
# traceroute aryacollege.in
traceroute to aryacollege.in (104.21.3.178), 30 hops max, 60 byte packets
 1  192.168.238.140 (192.168.238.140)  2.453 ms  2.224 ms  2.479 ms
 2  255.0.0.0 (255.0.0.0)  45.922 ms  49.990 ms  49.863 ms
 3  255.0.0.2 (255.0.0.2)  49.747 ms  49.556 ms  49.415 ms
 4  255.0.0.3 (255.0.0.3)  49.289 ms  54.054 ms  53.939 ms
 5  * * *
 6  255.0.0.5 (255.0.0.5)  52.808 ms  30.547 ms  35.345 ms
 7  192.168.227.98 (192.168.227.98)  39.131 ms  192.168.227.99 (192.168.227.99)
   38.995 ms  42.892 ms
 8  172.25.107.227 (172.25.107.227)  43.215 ms  172.25.107.229 (172.25.107.229)
   43.289 ms  172.25.107.227 (172.25.107.227)  43.102 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  103.198.140.64 (103.198.140.64)  76.920 ms  103.198.140.85 (103.198.140.85)
   186.665 ms  103.198.140.64 (103.198.140.64)  77.885 ms
17  103.198.140.79 (103.198.140.79)  205.503 ms  103.198.140.98 (103.198.140.98)
 )  197.789 ms de-cix-frankfurt.as13335.net (80.81.194.180)  193.084 ms
18  de-cix-frankfurt.as13335.net (80.81.194.180)  201.425 ms  103.198.140.87 (1
03.198.140.87)  197.082 ms de-cix-frankfurt.as13335.net (80.81.194.180)  194.0
96 ms
19  162.158.84.53 (162.158.84.53)  193.245 ms  162.158.84.139 (162.158.84.139)
   193.855 ms  162.158.84.53 (162.158.84.53)  206.986 ms
20  162.158.84.145 (162.158.84.145)  205.923 ms de-cix-frankfurt.as13335.net (
80.81.194.180)  206.764 ms  193.561 ms
21  162.158.84.149 (162.158.84.149)  198.327 ms  104.21.3.178 (104.21.3.178)  1
96.142 ms  189.100 ms
```

```
C:\Administrator:C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>tracert www.aryacollege.in

Tracing route to www.aryacollege.in [2606:4700:3030::6815:3b2]
over a maximum of 30 hops:

 1  10 ms    2 ms    3 ms  2409:40d4:201a:3a78::ea
 2  38 ms    37 ms   45 ms  2405:200:5216:2:3924:110:3:108
 3  34 ms    42 ms   40 ms  2405:200:5216:2:3925::ff22
 4  73 ms    33 ms   39 ms  2405:200:801:2b00::fc
 5  *        *        *      Request timed out.
 6  *        *        *      Request timed out.
 7  *        *        *      Request timed out.
 8  98 ms    202 ms   90 ms  2405:200:80c:760::5
 9  *        *        *      Request timed out.
10  *        *        *      Request timed out.
11  330 ms   205 ms   *      2400:cb00:35:3::a29e:a0de
12  144 ms   119 ms   432 ms  2400:cb00:497:3::
13  138 ms   120 ms   103 ms  2606:4700:3030::6815:3b2

Trace complete.

C:\Users\IEUser>
```

Explaination:-

- We have performed traceroute command in linux and tracert command in windows.
- On every tracert operation maximum 30 hopes are sent to the server (here server named to destination as we took aryacollege.in).
- Hope is refer to the location that the packet stops at, to reach the destination.
- If any packet gets request time out then it will be treate as connection failed.

Q3. Use the netstat command on your system. Document the output and explain its use in network monitoring and troubleshooting.

```
[root@kali ~]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
raw6      0      0 [ ::]:ipv6-icmp          [ ::]:*                7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State     I-Node      Path
unix    3      [ ]      STREAM    CONNECTED  9627      /run/dbus/system_bu
s_socket
unix    2      [ ]      DGRAM     CONNECTED  7328
unix    3      [ ]      STREAM    CONNECTED  9504
unix    3      [ ]      STREAM    CONNECTED  10410
unix    2      [ ]      DGRAM     CONNECTED  5703
unix    3      [ ]      STREAM    CONNECTED  8931
unix    3      [ ]      STREAM    CONNECTED  5941      /run/dbus/system_bu
s_socket
unix    3      [ ]      STREAM    CONNECTED  10614     @/tmp/.X11-unix/X0
unix    3      [ ]      STREAM    CONNECTED  8532      /run/dbus/system_bu
s_socket
unix    3      [ ]      STREAM    CONNECTED  9471
unix    3      [ ]      STREAM    CONNECTED  7877
unix    3      [ ]      STREAM    CONNECTED  8930      /run/user/1000/at-s
pi/bus_0
unix    3      [ ]      STREAM    CONNECTED  7437
unix    3      [ ]      STREAM    CONNECTED  3852      /run/systemd/journa
l/stdout
unix    3      [ ]      STREAM    CONNECTED  8946      /run/user/1000/bus
unix    3      [ ]      STREAM    CONNECTED  10429     /run/user/1000/bus
```

```
C:\Users\lakhan singh>netstat -a
Active Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:445            LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:902            LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:912            LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:5040           LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:7680           LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:49664          LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:49665          LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:49666          LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:49667          LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:49668          LAKHAN-SINGH:0      LISTENING
TCP    0.0.0.0:49670          LAKHAN-SINGH:0      LISTENING
TCP    127.0.0.1:25421         LAKHAN-SINGH:25422   ESTABLISHED
TCP    127.0.0.1:25422         LAKHAN-SINGH:25421   ESTABLISHED
TCP    192.168.140.1:139        LAKHAN-SINGH:0      LISTENING
TCP    192.168.186.1:139        LAKHAN-SINGH:0      LISTENING
TCP    192.168.238.238:139      LAKHAN-SINGH:0      LISTENING
TCP    192.168.238.238:26421    43.134.90.36:mdbs_daemon  ESTABLISHED
TCP    192.168.238.238:26527    49.44.44.33:https   ESTABLISHED
TCP    192.168.238.238:26534    43.154.154.166:9166  SYN_SENT
TCP    192.168.238.238:26537    20.44.239.154:https  TIME_WAIT
TCP    192.168.238.238:49421    20.198.118.190:https ESTABLISHED
TCP    [::]:135                 LAKHAN-SINGH:0      LISTENING
```

Explaination:-

- netstat command is used for network troubleshooting and configuration as well as monitoring.
- Varioud options are used as “netstat -a” , “netstat -n” , “netstat -r” etc.

Network Monitoring

- ***Active Connections:*** *netstat -a*
- ***Listening Ports:*** *netstat -an / find "LISTEN"*
- ***Network Statistics:*** *netstat -s*

Troubleshooting

- ***Open Ports and Services:*** *netstat -tuln (Linux)*
- ***Specific Port:*** *netstat -an / find "PORT_NUMBER"*
- ***Ie:*** *netstat -r or netstat -rn*
- ***Interface Stats:*** *netstat -i (Linux) or netstat -e (Windows)*

**Q4. Research and present a case study of a cyber law incident in India.
Explain the laws involved and the outcome of the case.**

“The 2020 Indian Cyberattack on the Indian Ministry of Defense”

- In 2020, a significant cyberattack targeted the Indian Ministry of Defense. The attack was attributed to a sophisticated group of hackers, potentially state-sponsored, aiming to steal sensitive information related to India's defense infrastructure and military capabilities. This breach raised alarms about the security of national defense information.
- Relevant Laws:-
 - 1. Information Technology Act, 2000 (IT Act)**
 - **Section 66:** Covers hacking and unauthorized access to computer systems.
 - **Section 43:** Addresses illegal access to and downloading of data.
 - **Section 72:** Deals with breaches of confidentiality and privacy.

2. Indian Penal Code (IPC)

- **Section 378:** Encompasses theft of digital data.
- **Section 420:** Pertains to fraud and deceit, including digital fraud.

3. National Cyber Security Policy, 2013

- Provides guidelines and strategies for improving cybersecurity and responding to cyber incidents.

➤ Incident Details:-

- ✓ **Targets:** Indian Ministry of Defense and associated defense-related networks.
- ✓ **Method:** The attackers used advanced phishing techniques and malware to infiltrate the ministry's computer systems and access confidential information.
- ✓ **Impact:** The breach compromised sensitive defense information, potentially impacting national security and military operations.

Legal and Operational Response

- 1. Investigation:** The investigation was led by Indian cybersecurity agencies, including the National Technical Research Organisation (NTRO) and the Computer Emergency Response Team - India (CERT-In). International cybersecurity firms also assisted in identifying and mitigating the threat.
- 2. Legal Actions:** Specific individuals or groups responsible for the attack were not publicly identified. However, the case drew attention to the gaps in India's cyber defenses and the need for stronger legal measures.
- 3. Impact and Reforms:**
 - **Policy Revisions:** The incident accelerated the review and enhancement of India's cybersecurity policies, leading to more stringent measures for protecting sensitive information.
 - **Infrastructure Upgrades:** Increased investment in cybersecurity infrastructure and technologies to safeguard critical data.
 - **Legislative Review:** Ongoing discussions on updating the IT Act and IPC to address emerging cyber threats more effectively

Q5. Use Nmap to perform a network scan. Document the steps, findings, and potential vulnerabilities identified.

```
(root㉿kali)-[~/home/kali]
# nmap 152.58.98.251
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 00:39 EDT
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.90% done; ETC: 00:40 (0:00:15 remaining)
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 70.80% done; ETC: 00:40 (0:00:16 remaining)
Nmap scan report for 152.58.98.251
Host is up (0.037s latency).
All 1000 scanned ports on 152.58.98.251 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 51.88 seconds

Home
(root㉿kali)-[~/home/kali]
# nmap google.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 00:41 EDT
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.45% done; ETC: 00:41 (0:00:02 remaining)
Nmap scan report for google.com (142.250.195.14)
Host is up (0.0073s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:80a::200e
rDNS record for 142.250.195.14: del12s09-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

Explanation:-

- *Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing, helping users to identify active devices, open ports, and services running on a network.*
- *By employing various scanning techniques, such as TCP SYN scans for stealthy port detection, UDP scans for checking open UDP ports, and OS fingerprinting to identify the operating system, Nmap provides detailed insights into network configurations and vulnerabilities.*
- *It supports advanced features like the Nmap Scripting Engine for custom probes and security assessments, and offers multiple output formats including normal, XML, and grepable for flexible data handling.*
- *Nmap's versatility makes it essential for network administrators and security professionals, but it must be used ethically and legally to avoid unauthorized access and potential disruptions.*
- *By using nmap; ports, services, and network traffic can be identified as vulnerability.*

Q6. Use Metasploit to exploit a vulnerability on a Windows 7 machine from a Kali Linux system.
Access the system using Meterpreter and document the process.

```
TX packets 63 bytes 10356 (10.1 KIB)
└── (root㉿kali)-[~/home/kali/assessment]
    └── # python -m simpleHTTPServer 80
/usr/bin/python: No module named simpleHTTPServer
    TX bytes 127.0.0.1 netmask 255.0.0.0
    RX errors 0 dropped 0 overruns 0 frame 0
    └── (root㉿kali)-[~/home/kali/assessment]
        └── # python -m simpleHTTPserver 80 [10<host>]
/usr/bin/python: No module named simpleHTTPserver
    TX bytes 127.0.0.1 netmask 255.0.0.0
    RX errors 0 dropped 0 overruns 0 frame 0
    └── (root㉿kali)-[~/home/kali/assessment]
        └── # python -m SimpleHTTPServer 80
/usr/bin/python: No module named SimpleHTTPServer
    TX bytes 127.0.0.1 netmask 255.0.0.0
    RX errors 0 dropped 0 overruns 0 frame 0
    └── (root㉿kali)-[~/home/kali/assessment]
        └── # python2 -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.238.10 - - [11/Aug/2024 03:56:08] "GET / HTTP/1.1" 200 -
192.168.238.10 - - [11/Aug/2024 03:56:09] code 404, message File not found
192.168.238.10 - - [11/Aug/2024 03:56:09] "GET /favicon.ico HTTP/1.1" 404 -
```

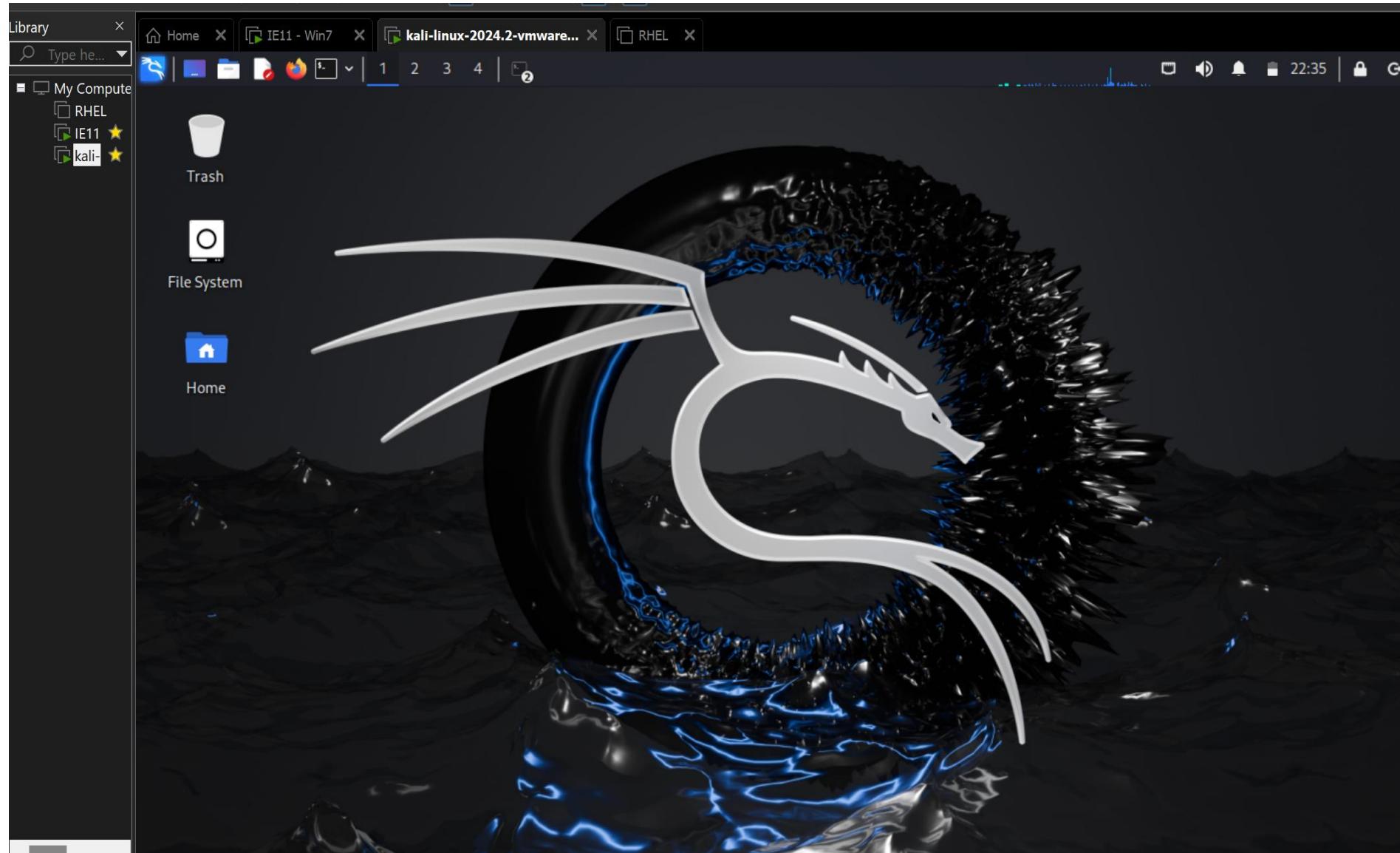
 Directory listing for / - Internet Explorer

   http://192.168.238.204/   

Directory listing for /

- [payload.exe](#)

**Q7. Set up a virtual machine using a hypervisor (e.g., VirtualBox or VMware).
Install a Linux operating system on the VM and optimize its performance. Document the process.**



Procedure:-

- First we downloaded Vmware workstation as hypervisor(vmm).And install it on the system.
- After this, we downloaded ISO image file of kali linux OS.(pre-installed image)
- Now created virtual os of kali linux in vmware by using importing iso image of kali linux.
- We can set configuration files manually or can be setted as auto.
- That's it, our kali linux is ready to use.

Q8. Use search engines and online tools to gather information about a specific target (ensure it is a legal and ethical target). Document the methods used and the information found.

Target:- aryacollege.in

NsLookup.io

aryacollege.in

Fin

DNS records for **aryacollege.in**

Cloudflare Google DNS Authoritative Control D Local DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records during this period; Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 172.67.153.150	5m
> 104.21.3.178	5m

AAAA records

IPv6 address	Revalidate in
> 2606:4700:3030::6815:3b2	5m
> 2606:4700:3036::ac43:9996	5m

(kali㉿kali)-[~]

\$ nmap -sV aryacollege.in

Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-12 22:57 EDT
Nmap scan report for aryacollege.in (104.21.3.178)
Host is up (0.34s latency).

Other addresses for aryacollege.in (not scanned): 2606:4700:3030::6815:3b2
Not shown: 996 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Cloudflare http proxy
443/tcp	open	ssl/http	Cloudflare http proxy
8080/tcp	open	http	Cloudflare http proxy
8443/tcp	open	ssl/http	Cloudflare http proxy

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 71.01 seconds

Contact Us

- 🏡 SP-42, RIICO Industrial Area, Kukas, Delhi Road, Near Hotel Le-Meridian, Jaipur, Rajasthan - 302028
- 📞 91-141-6604555
- 📞 91-141-2621969, 91-141-2621970
- 📞 1800 266 2000 (Toll Free)
- ✉️ info@aryacollege.in

Admission Contact

Dr. Arun Arya (Director, Admissions)

- 📞 +91-9314881683
- 📞 +91-9829158955

Seats & Other Details

B.Tech. Seats (REAP CODE: 14)	
Branch Name	Seats
Artificial Intelligence & Data Science	180
Electronics & Comm. Eng.	120
Computer Science & Engineering	180
Electrical Engineering	60
Mechanical Engineering	60
Information Technology	60

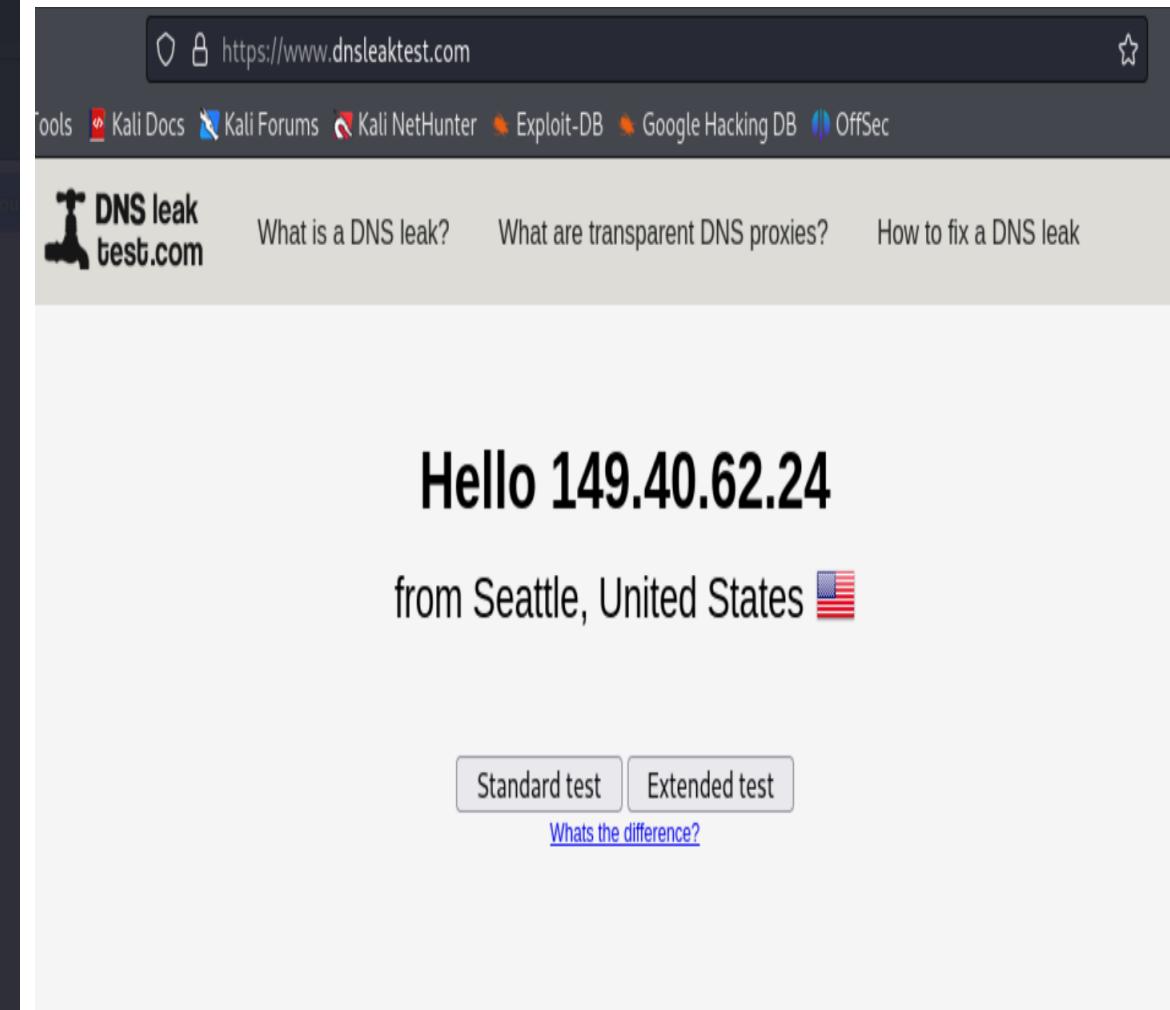
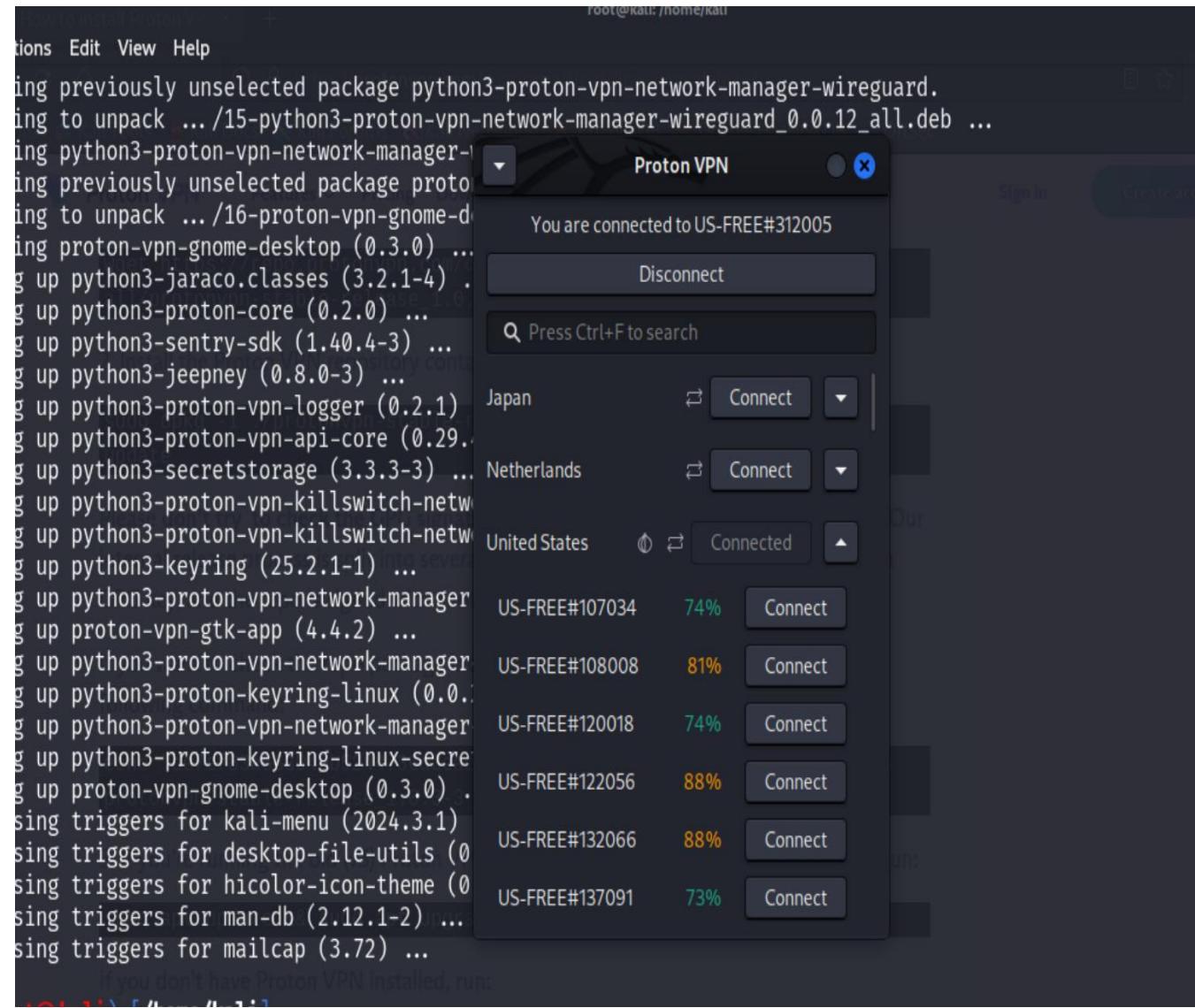
MBA Seats	
Branch Name	Seats
Human Resource & Development	
Information Systems	
Operations & Supply Chain	60
Business Analytics	
Marketing	
Finance	

Hey! I am Dristi...Your Admission Assistant.

**Q9. Perform a WHOIS lookup on a domain name and interpret the results.
Provide details on the domain's ownership, registration, and expiration.**

```
(kali㉿kali)-[~]
$ whois learnandbuild.in
Domain Name: learnandbuild.in
Registry Domain ID: DE5A12D6520D84338875355CDAFF3D365-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2023-10-09T14:18:45Z
Creation Date: 2021-03-17T11:00:43Z
Registry Expiry Date: 2025-03-17T11:00:43Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: LNB Career Pvt. Ltd.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Rajasthan
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
```

Q10. Set up a VPN connection on your system. Document the steps and explain the advantages and disadvantages of using a VPN for secure communication.



Steps:-

- First login into Proton VPN.
- Now perform these commands in kali linux terminal.
 - wget https://repo.protonvpn.com/Debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.3.-3_all.deb
 - sudo dpkg -i https://repo.protonvpn.com/Debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.3.-3_all.deb
 - sudo apt update && sudo apt upgrade
 - sudo apt install proton-vpn-gnome-desktop
 - sudo apt update && sudo apt upgrade
- Now open proton vpn app from app-menu and login and connect to a server.
- That's vpn is connected.
- You can also check dns leak for this vpn.

Advantages:-

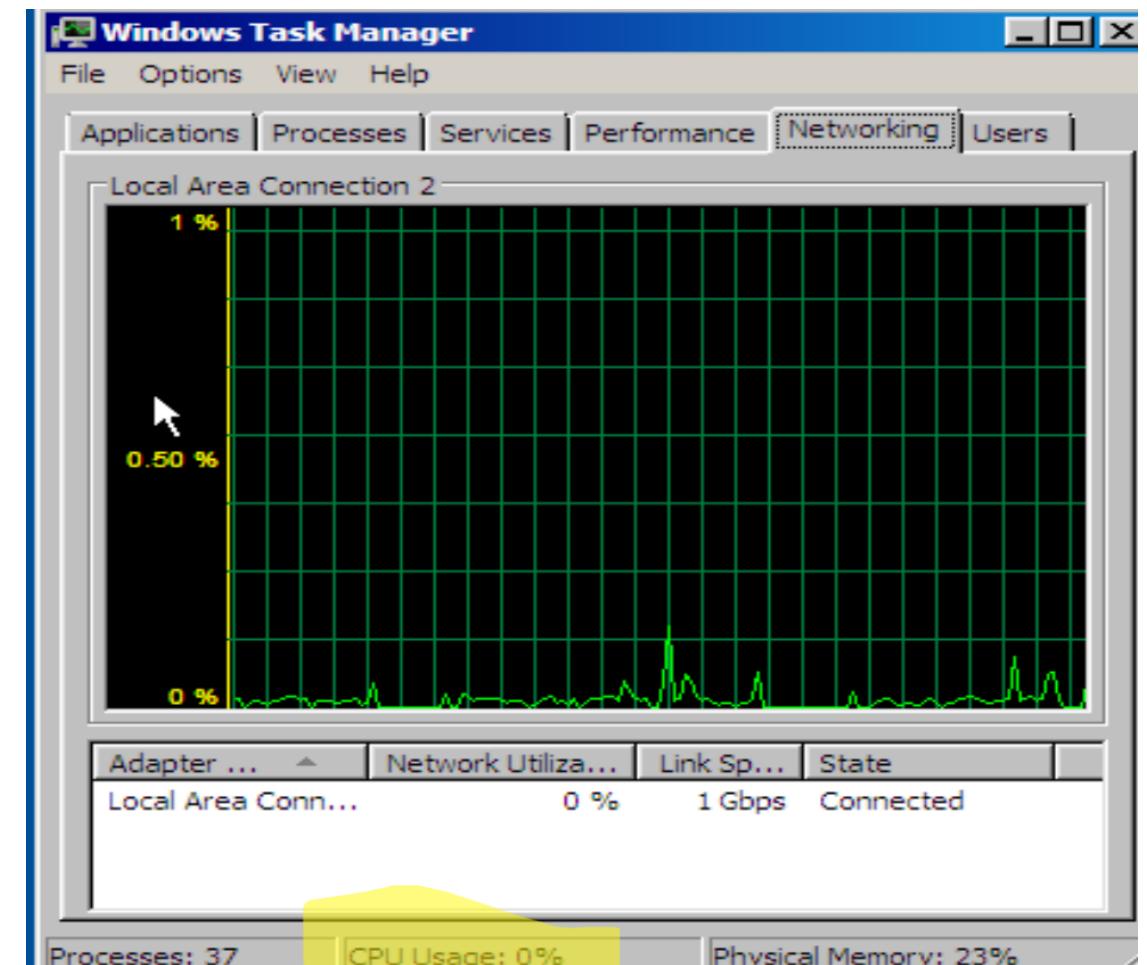
- VPNs improve your privacy
- VPNs can protect you from cyber attacks
- They bypass online censorship
- ISPs can't throttle your bandwidth
- Torrenting is much safer
- VPNs help you save money online
- No more geo-restrictions
- Excellent for businesses

Disadvantages:-

- Your VPN provider can see your data
- Cost
- They can be blocked
- Some smart TVs and game consoles don't support them
- VPNs might slow down your internet connection

Q11. Use hping3 to perform a DoS attack simulation. Document the process, the impact observed, and suggest mitigation strategies.

```
(root㉿kali)-[~/home/kali]
# hping3 --scan 1-65535 192.168.30.10 -S --rand-source
Scanning 192.168.30.10 (192.168.30.10), port 1-65535
65535 ports to scan, use -V to see all the replies
port| serv name | flags | ttl| id | win | len |
+---+-----+-----+---+---+---+---+
 22 ssh      : .S..A... 128 57352 64240 46
 135 epmap    : .S..A... 128 57608 64240 46
 139 netbios-ssn: .S..A... 128 57864 64240 46
 445 microsoft-d: .S..A... 128 58120 64240 46
+9152 game    : .S..A... 128 63241 64240 46
+9155 : .S..A... 128 63497 64240 46
5357 : .S..A... 128 60949 64240 46
+9153 : .S..A... 128 64933 64240 46
+9156 : .S..A... 128 65189 64240 46
+9157 : .S..A... 128 65445 64240 46
All replies received. Done.
Not responding ports: (514 shell) (1220 ) (1222 ) (1225 ) (1254 ) (1255 ) (1256
54 ) (1265 ) (1267 ) (1286 ) (1287 ) (1288 ) (1289 ) (1290 ) (1291 ) (1292 ) (1
1299 ) (1300 ) (1301 ) (1302 ) (1303 ) (1304 ) (1305 ) (1306 ) (1307 ) (1308 )
1314 xtelw) (1315 ) (1316 ) (1317 ) (1318 ) (1319 ) (1320 ) (1321 ) (1322 ) (13
1329 ) (1330 ) (1331 ) (1332 ) (1333 ) (1334 ) (1335 ) (1336 ) (1337 ) (1338 )
) (1345 ) (1346 ) (1347 ) (1348 ) (1349 ) (1350 ) (1351 ) (1352 lotusnote) (135
359 ) (1360 ) (1361 ) (1362 ) (1363 ) (1364 ) (1365 ) (1366 ) (1367 ) (1368 ) (
(1375 ) (1376 ) (1377 ) (1378 ) (1379 ) (1380 ) (1381 ) (1382 ) (1383 ) (1384
) (1391 ) (1392 ) (1393 ) (1394 ) (1395 ) (1396 ) (1397 ) (1398 ) (1399 ) (14
1421 ) (1422 ) (1423 ) (1424 ) (1425 ) (1428 ) (1429 ) (1430 ) (1431 ) (1432 )
) (1437 ) (1438 ) (1439 ) (1440 ) (1441 ) (1442 ) (1443 ) (1444 ) (1445 ) (1446
52 ) (1453 ) (1454 ) (1455 ) (1456 ) (1457 ) (1458 ) (1459 ) (1460 ) (1461 ) (1
1468 ) (1469 ) (1470 ) (1471 ) (1472 ) (1473 ) (1474 ) (1475 ) (1476 ) (1477 )
) (1484 ) (1485 ) (1486 ) (1487 ) (1488 ) (1489 ) (1490 ) (1491 ) (1492 ) (14
99 ) (1500 ) (1501 ) (1502 ) (1503 ) (1504 ) (1505 ) (1506 ) (1507 ) (1508 ) (
1515 ) (1516 ) (1517 ) (1518 ) (1519 ) (1520 ) (1521 ) (1522 ) (1523 ) (1524
```



Mitigation strategies:-

- Network Design and Architecture.
- Traffic Filtering and Analysis.
- Content Delivery Networks.
- Network and Application Monitoring.
- Incident Response Planning.
- IP Blacklisting and Whitelisting.
- Application-Level Protections.
- Infrastructure Scaling.
- Patch Management.

Q12. Perform a vulnerability scan on the WordPress website cybervajra.com using wpScan. Document the process and findings.

```
File Actions Edit View Help
Trash
Wordpress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

[root@kali]-[~/home/kali]
# wpScan --url CyberVajra.com --api-token exvhBlSA5s53ydE5MmG9xFAGYaET3MeVwYCohPPLbXk
```

```
Wordpress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

[root@kali]-[~/home/kali]
#
```

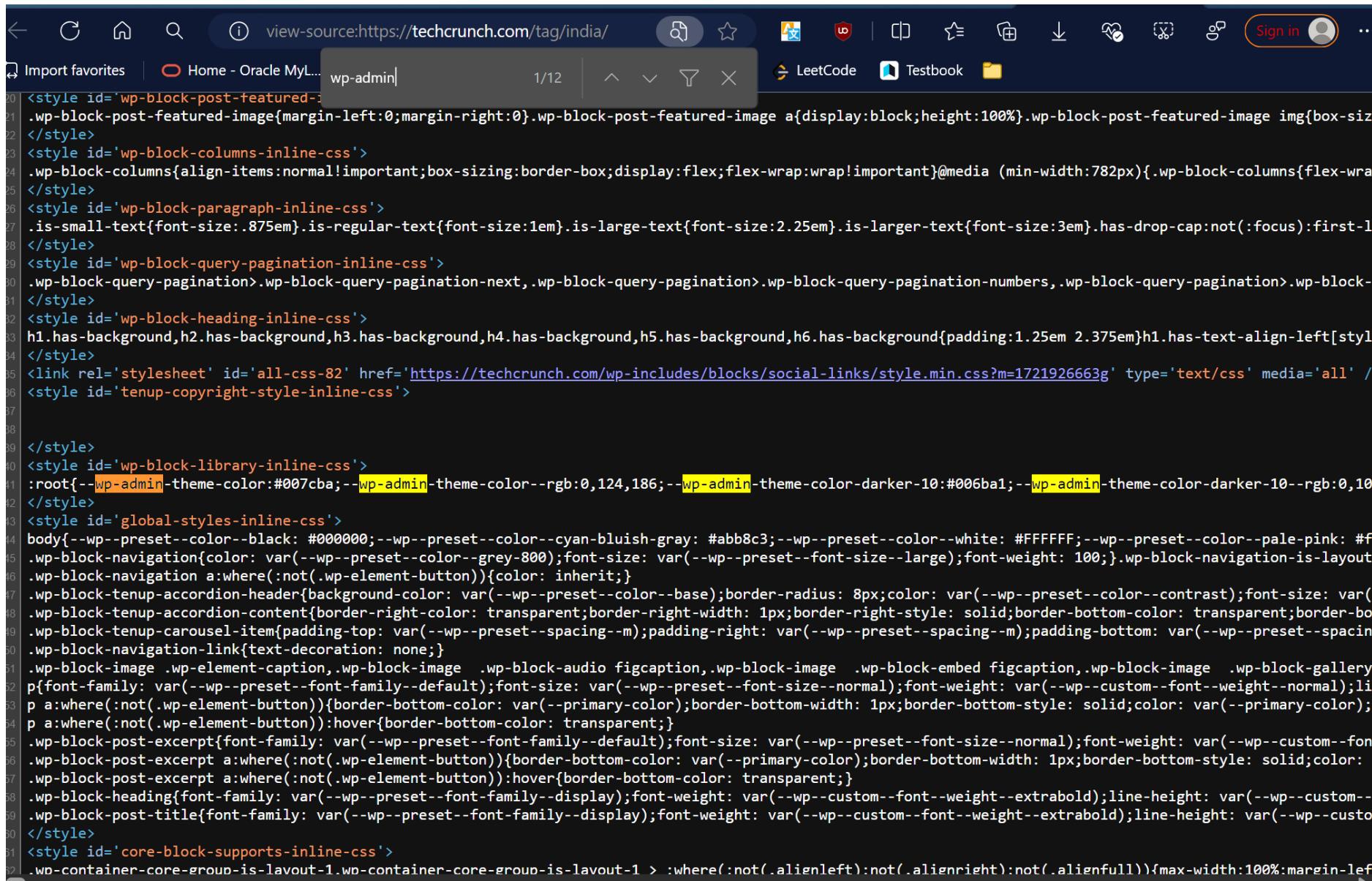
```
(root@kali)-[~/home/kali]
# wpScan --url cybervajra.com

Wordpress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```

Q13. Explain how you would identify if a website is using WordPress.

List the steps and tools used for detection



The screenshot shows a browser window with the address bar set to "view-source:https://techcrunch.com/tag/india/". The main content area displays the raw HTML code of the page. A search bar at the top of the code editor has "wp-admin" typed into it. The code itself is a large block of CSS and HTML, with several lines highlighted in yellow, indicating specific WordPress theme or plugin styles. These highlighted lines include class definitions like ".wp-block-post-featured-image", ".wp-block-columns", and ".wp-block-paragraph", as well as global styles and navigation elements. The overall structure is typical of a WordPress-generated page source code.

```
Import favorites | Home - Oracle My... wp-content 7/380 ^ v < > LeetCode Testbook
200 <script async src="//s.yimg.com/...>
201 <script src="https://use.typekit.net/...>
202 <script id="tc-typekit-fonts-js-aft" Also found: .wp-block-tenup-accordion-content>
203 try{Typekit.load({ async: true });}catch(e){}
204 try{Typekit.load({ async: true });}catch(e){}
205 </script>
206 <script src="https://consent.cmp.oath.com/cmp_js?ver=20240814" id="tc-gdpr-cmp-js"></script>
207 <script src="https://s.yimg.com/cx/acookie/acookie.js?ver=20240814" id="tc-gdpr-acookie-js"></script>
208 <link rel="https://api.w.org/" href="https://techcrunch.com/wp-json/" /><link rel="alternate" type="application/json" href="https://techcrunch.com/wp-json/wp/>
209 <script id="wp-load-polyfill-importmap">
210 ( HTMLScriptElement.supports && HTMLScriptElement.supports("importmap") ) || document.write( '<script src="https://techcrunch.com/wp-includes/js/dist/vendor/w...
211 </script>
212 <script type="importmap" id="wp-importmap">
213 {"imports":{@wordpress\interactivity":"https://techcrunch.com/wp-includes/js/dist/interactivity.min.js?ver=6.5.5"}}
214 </script>
215 <script type="module" src="https://techcrunch.com/wp-includes/blocks/navigation/view.min.js?ver=6.5.5" id="@wordpress/block-library/navigation-js-module"></sc...
216 <link rel="modulepreload" href="https://techcrunch.com/wp-includes/js/dist/interactivity.min.js?ver=6.5.5" id="@wordpress/interactivity-js-modulepreload"> <s...
217 function e(e){var t=!arguments.length>1&&void 0!==arguments[1])|arguments[1],c=document.createElement("script");c.src=e,t?c.type="module":(c.async=!
218 </script>
219 <meta property="mrf:tags" content="Page Type:Archive;Archive Type:Tag" />
220 <script async src="https://s.yimg.com/cx/vzm/cs.js"></script>
221 <link rel="icon" href="https://techcrunch.com/wp-content/uploads/2015/02/cropped-cropped-favicon-gradient.png?w=32" sizes="32x32" />
222 <link rel="icon" href="https://techcrunch.com/wp-content/uploads/2015/02/cropped-cropped-favicon-gradient.png?w=192" sizes="192x192" />
223 <link rel="apple-touch-icon" href="https://techcrunch.com/wp-content/uploads/2015/02/cropped-cropped-favicon-gradient.png?w=180" />
224 <meta name="msapplication-TileImage" content="https://techcrunch.com/wp-content/uploads/2015/02/cropped-cropped-favicon-gradient.png?w=270" />
225 </head>
226
227 <body class="archive tag tag-india tag-3054 wp-embed-responsive">
228
229 <div class="wp-site-blocks">
230 <div class="wp-block-group has-grey-50-background-color has-background is-layout-constrained wp-container-core-group-is-layout-1 wp-block-g...
231 style="border-bottom-color:var(--wp--preset--color--grey-75);border-bottom-width:1px;padding-top:0;padding-bottom:0">
232
233
234 <div class="ad-unit ad-unit--edge-to-edge wp-block-tc-ads-ad-slot">
235 <div class="ad-unit__ad" id="us-tc-ros-dt-top-center" data-unitcode="us_tc_ros_dt_top_center"></div>
236 </div>
237
238
239 <div class="ad-unit ad-unit--edge-to-edge wp-block-tc-ads-ad-slot">
240 <div class="ad-unit__ad" id="us-tc-ros-mw-top-center" data-unitcode="us_tc_ros_mw_top_center"></div>
241 </div>
242
```

Steps:-

- First visit the website.
- Then open the source code of the website using ctrl+u.
- Now search wp-admin & wp-content in source code.
- To launch search bar press ctrl+f.
- If site contains wp-admin & wp-content that means site is using wordpress.
- Else not using wordpress.

**Q14. Create a simple HTML form that saves submitted data to a text file.
Document the steps and the purpose of the form in phishing attacks.**

- "C:\xampp\htdocs\phishing_page.zip"
 - https://drive.google.com/drive/folders/1QHuD_6KyB_Z2fFyWdWc8VXOiatdm_P3t?usp=drive_link
-

Index of /learn_phishing

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 action.php	2024-08-14 11:54	404	
 log.txt	2024-08-14 11:53	93	
 login.php	2024-08-14 11:54	29K	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost Port 80

Q15. Set up a wireless network and attempt to crack its security using tools . Document the process and results, and suggest measures to improve wireless security.



kali@kali:~

File Actions Edit View Help

crunch will now generate the following number of lines: 3917251611

crunch: 2% completed generating output

crunch: 4% completed generating output

crunch: 6% completed generating output

crunch: 8% completed generating output

crunch: 10% completed generating output

hunk1: fprintf failed = 28
the problem is = No space left on device

(kali㉿kali)-[~]

```
$ crunch 8 10 ab -o Pass.txt
crunch will now generate the following amount of data: 18688 bytes
MB
GB
TB
PB
crunch will now generate the following number of lines: 1792
crunch: 100% completed generating output
```

(kali㉿kali)-[~]

Fern WIFI Cracker

wlan0

Monitor Mode Enabled on wlan0mon

Attack Panel

Select Target Access Point

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	10010	10011	10012	10013	10014	10015	10016	10017	10018	10019	10020	10021	10022	10023	10024	10025	10026	10027	10028	10029	10030	10031	10032	10033	10034	10035	10036	10037	10038	10039	10040	10041	10042	10043	10044	10045	10046	10047	10048	10049	10050	10051	10052	10053	10054	10055	10056	10057	10058	10059	10060	10061	10062	10063	10064	10065	10066	10067	10068	10069	10070	10071	10072	10073	10074	10075	10076	10077	10078	10079	10080	10081	10082	10083	10084	10085	10086	10087	10088	10089	10090	10091	10092	10093	10094	10095	10096	10097	10098	10099	100100	100101	100102	100103	100104	100105	100106	100107	100108	100109	100110	100111	100112	100113	100114	100115	100116	100117	100118	100119	100120	100121	100122	100123	100124	100125	100126	100127	100128	100129	100130	100131	100132	100133	100134	100135	100136	100137	100138	100139	100140	100141	100142	100143	100144	100145	100146	100147	100148	100149	100150	100151	100152	100153	100154	100155	100156	100157	100158	100159	100160	100161	100162	100163	100164	100165	100166	100167	100168	100169	100170	100171	100172	100173	100174	100175	100176	100177	100178	100179	100180	100181	100182	100183	100184	100185	100186	100187	100188	100189	100190	100191	100192	100193	100194	100195	100196	100197	100198	100199	100200	100201	100202	100203	100204	100205	100206	100207	100208	100209	100210	100211	100212	100213	100214	100215	100216	100217	100218	100219	100220	100221	100222	100223	100224	100225	100226	100227	100228	100229	100230	100231	100232	100233	100234	100235	100236	100237	100238	100239	100240	100241	100242	100243	100244	100245	100246	100247	100248	100249	100250	100251	100252	100253	100254	100255	100256	100257</th
--	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	------------

kali@kali:~

```
Edit View Help
completed generating output
completed generating output
completed generating output
completed generating output
tf failed = 28
5 = No space left on device
)
l0 ab -o pass.txt
now generate the following amount of data: 18688 bytes

now generate the following number of lines: 1792
completed generating output
)
```

Attack Panel

Select Target Access Point

Redmi Note 7 Vivek's Galaxy A14

Step Automate

Access Point Details

ESSID: Vivek's Galaxy A14 BSSID: E6:FB:CE:07:68:01 Channel: 11 Power: -33 Encryption: wpa Supports WPS

Attack Option

Regular Attack WPS Attack

Probing Access Point

Deauthenticating E6:FB:CE:07:68:01

Handshake Status

Bruteforcing Encryption

Finished

pass.txt Browse

Current Phrase

wlan0

Monitor Mode Enabled on wlan0mon

Stop

None Detected

WEP

WPA

No Key Entries

Key Database

Toolbox

Written by Sevior Emmanuel Siles

Report Bugs at: seviroboys@rocketmail.com



New Volume



OS



Trash



File System



Home

File Actions Edit View Help

kali@kali: ~

```
Crunch can create a wordlist based on criteria you specify. The output from
crunch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crun
ch.

(kali㉿kali)-[~]
$ crunch 8 10 ab -o pass.txt
Crunch will now generate the following amount of data: 18688 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1792
crunch: 100% completed generating output

(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]
$
```

Fern WiFi Cracker

Select Interface

Select an interface card

Scan for Access points

WEP Detection Status

WPA Detection Status

Key Database No Key Entries

ToolBox

Fern WiFi Cracker 3.0

Latest update is already installed

Python Version: 3.11.9 main, Aircrack Version: aircrack-ng 1.7 - (C) 2, Qt Version: 5.15.10

About Fern WiFi Cracker

GUI suite for wireless encryption strength testing of 802.11 wireless encryption standard access points

Written by Sefour Emmanuel Elka Report Bugs at : sefohoya@rocketmail.com

Fern WIFI Cracker

wlan0
Monitor Mode Enabled on wlan0mon

Refresh

Attack Panel

Select Target Access Point

Redmi Note 7

Access Point Details

ESSID: Redmi Note 7 BSSID: E6:3E:E4:A7:22:DE Channel: 1 Power: -52 Encryption: WPA Supports WPS

Attack Option

Regular Attack WPS Attack

Probing Access Point

Deauthentication Status

Handshake Status

Bruteforcing Encryption

Automatically probing and adding clients mac-addresses, please wait...

Current Dictionary File

WPS Attack

Automate

Active

None Detected

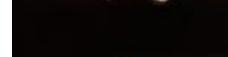
53 Detected

No Key Entries

Key Database

ToolBox

3 4



Recent
Home
Desktop
fern-wifi-cracker
Other Locations

Select Wordlist

Name	Size	Type	Modified
bin			27 May
boot			27 May
dev			20:08
etc			20:10
home			20:08
lib			27 May
lib32			27 May
lib64			27 May
media			27 May
mnt			27 May
opt			27 May
proc			20:08
root			20:25
run			20:10
sbin			27 May
srv			27 May
sys			20:08
tmp			20:26
usr			27 May
var			20:08
initrd.img	92.2 MB	Raw disk image	27 May
vmlinuz	9.3 MB	Program	17 May

The image shows a Kali Linux desktop environment with several open windows and terminal sessions.

Left Panel (File Manager):

- OS
- Trash
- File System

Terminal Session 1 (kali㉿kali: ~):

```
File Actions Edit View Help
crunch: 4% completed generating output
crunch: 6% completed generating output
crunch: 8% completed generating output
crunch: 10% completed generating output
chunk1: fprintf failed = 28
The problem is - No space left on device

(kali㉿kali)-[~]
$ crunch 8 10 ab -o pass.txt
Crunch will now generate the following amount of data: 18688 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1792
crunch: 100% completed generating output

(kali㉿kali)-[~]
$ pwd
/home/kali

(kali㉿kali)-[~]
```

Terminal Session 2 (kali㉿kali: ~):

```
$ airmon-ng start wlan0mon
Monitor Mode Enabled on wlan0mon
[  ] Refresh
```

Attack Panel (Main Window):

The Attack Panel window displays the following information:

- Select Target Access Point:** Shows a list of detected access points, with "Redmi Note 7" selected.
- Access Point Details:** ESSID: Redmi Note 7, BSSID: E6:3E:E4:A7:22:DE, Channel: 1, Power: -52, Encryption: WPA, Supports WPS.
- Attack Option:** Radio buttons for "Regular Attack" (selected) and "WPS Attack".
- Probing Access Point:** A progress bar indicating the status of probing clients.
- Deauthentication Status:** A progress bar indicating the status of deauthenticating clients.
- Handshake Status:** A progress bar indicating the status of capturing handshakes.
- Bruteforce Encryption:** A progress bar indicating the status of bruteforcing encryption keys.
- Finished:** A progress bar indicating the completion of the attack.

Right Side Panel:

- Wi-Fi WEP:** None Detected
- Wi-Fi WPA:** 273 Detected
- Key Database:** No Key Entries
- Toolbox:**

Bottom Status Bar:

Written by Senior Emmanuel Ediba
Report Bugs at: sandboys@rocketmail.com