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
th0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.238.120  netmask 255.255.255.0  broadcast 192.168.238.25

        inet6 2409:40d4:1018:87f7:2765:fafd:ee18:fbe5  prefixlen 64  scopeid
×0<global>
        inet6 2409:40d4:12a:89f8:dc7e:382e:7683:16f2  prefixlen 64  scopeid 0
0<global>
        inet6 fe80::3dbf:5a32:535a:c32d  prefixlen 64  scopeid 0×20<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

o: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<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
Reply from 192.168.238.120: bytes=32 time<1ms TTL=64
Reply from 192.168.238.120: bytes=32 time<1ms TTL=64
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
```

```
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)-[/home/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"*
- ***le****: 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

┌──(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:-

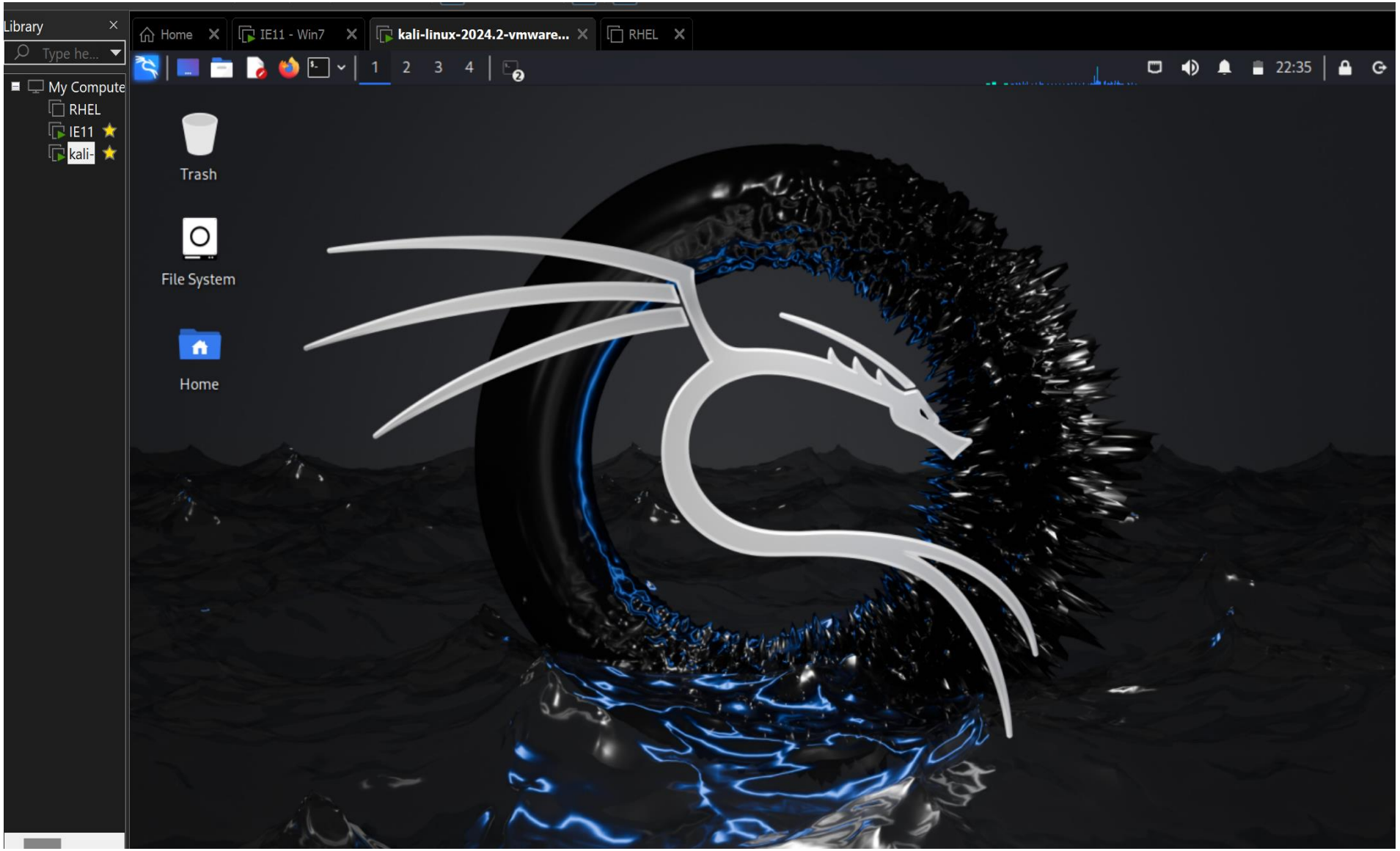
- *Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing, helping users to identify active devices, open ports, and services running on a network.*
- *By employing various scanning techniques, such as TCP SYN scans for stealthy port detection, UDP scans 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.

```
┌──(root㉿kali)-[/home/kali/assessment]
└─# python -m simpleHTTPServer 80
/usr/bin/python: No module named simpleHTTPServer

┌──(root㉿kali)-[/home/kali/assessment]
└─# python -m simpleHTTPserver 80
/usr/bin/python: No module named simpleHTTPserver

┌──(root㉿kali)-[/home/kali/assessment]
└─# python -m SimpleHTTPServer 80
/usr/bin/python: No module named SimpleHTTPServer

┌──(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 record 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::6
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

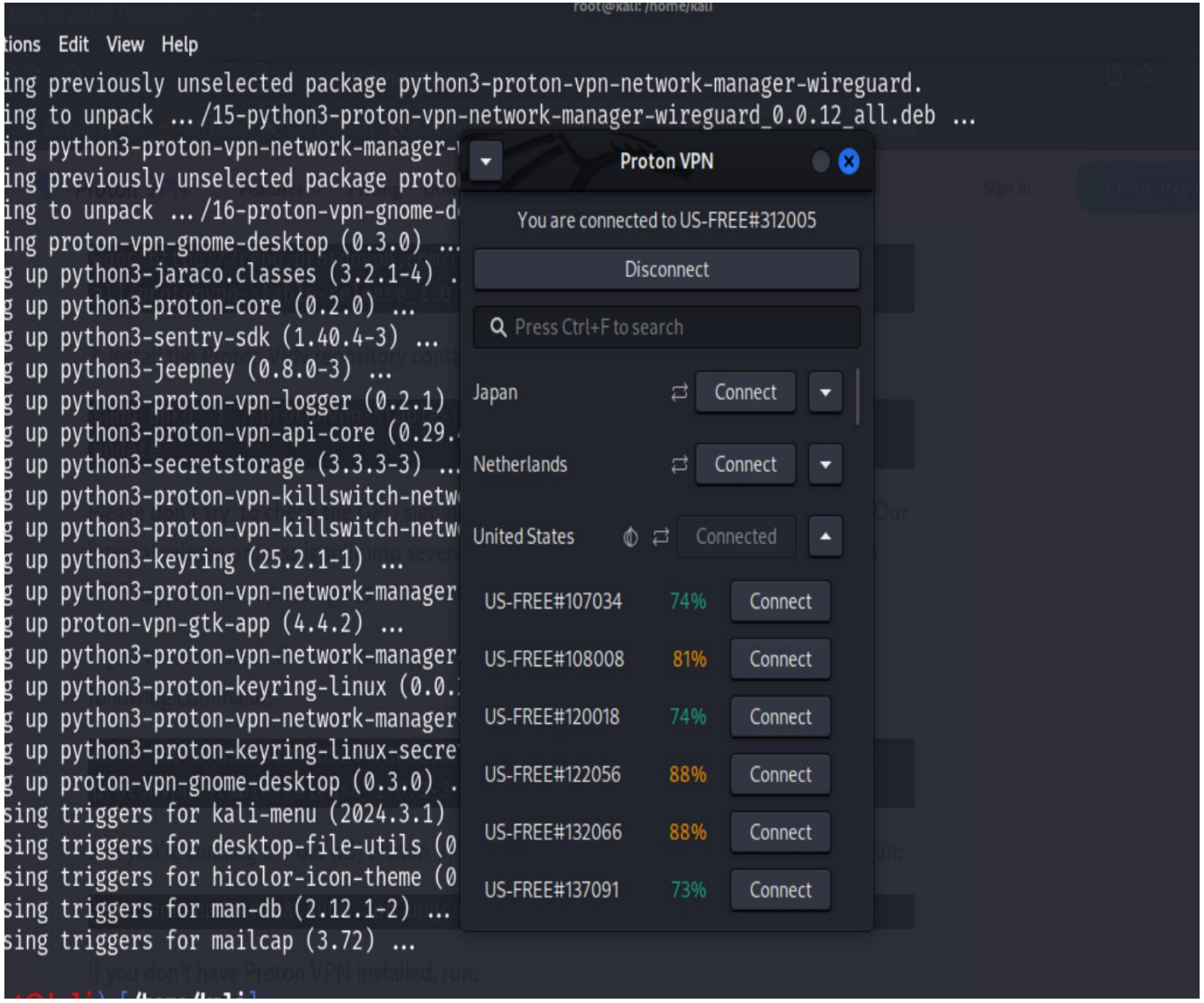
B.Tech. Seats (REAP CODE: 14)	
Branch Name	Seats
Artificial Intelligence & Data Science	180
Electronics & Comm. Eng.	120
Computer Science & Engineering	180
Electrical Engineering	60
Mechanical Engineering	60
Information Technology	60

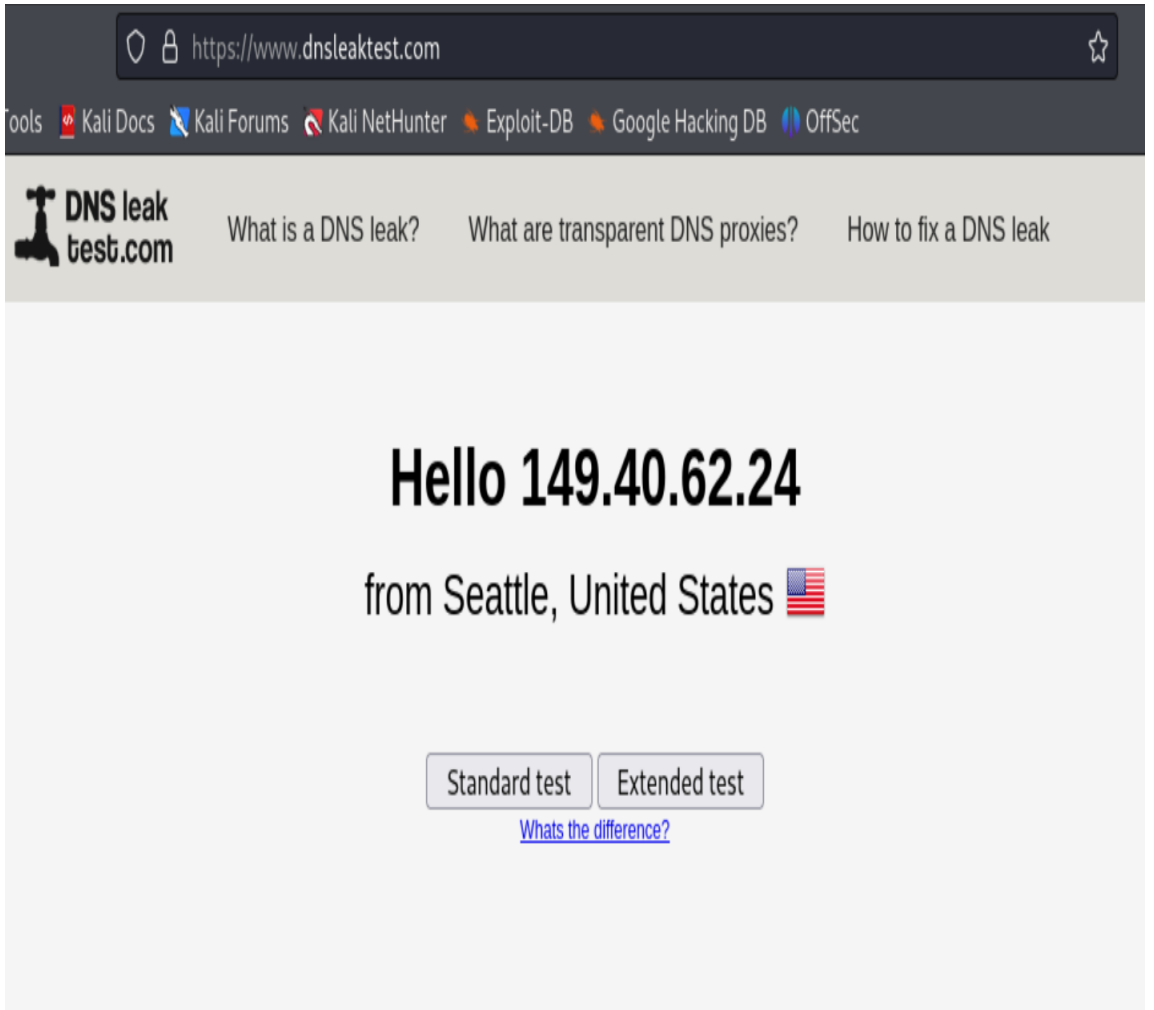
MBA Seats	
Branch Name	Seats
Human Resource & Development	60
Information Systems	
Operations & Supply Chain	
Business Analytics	
Marketing	
Finance	

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:-

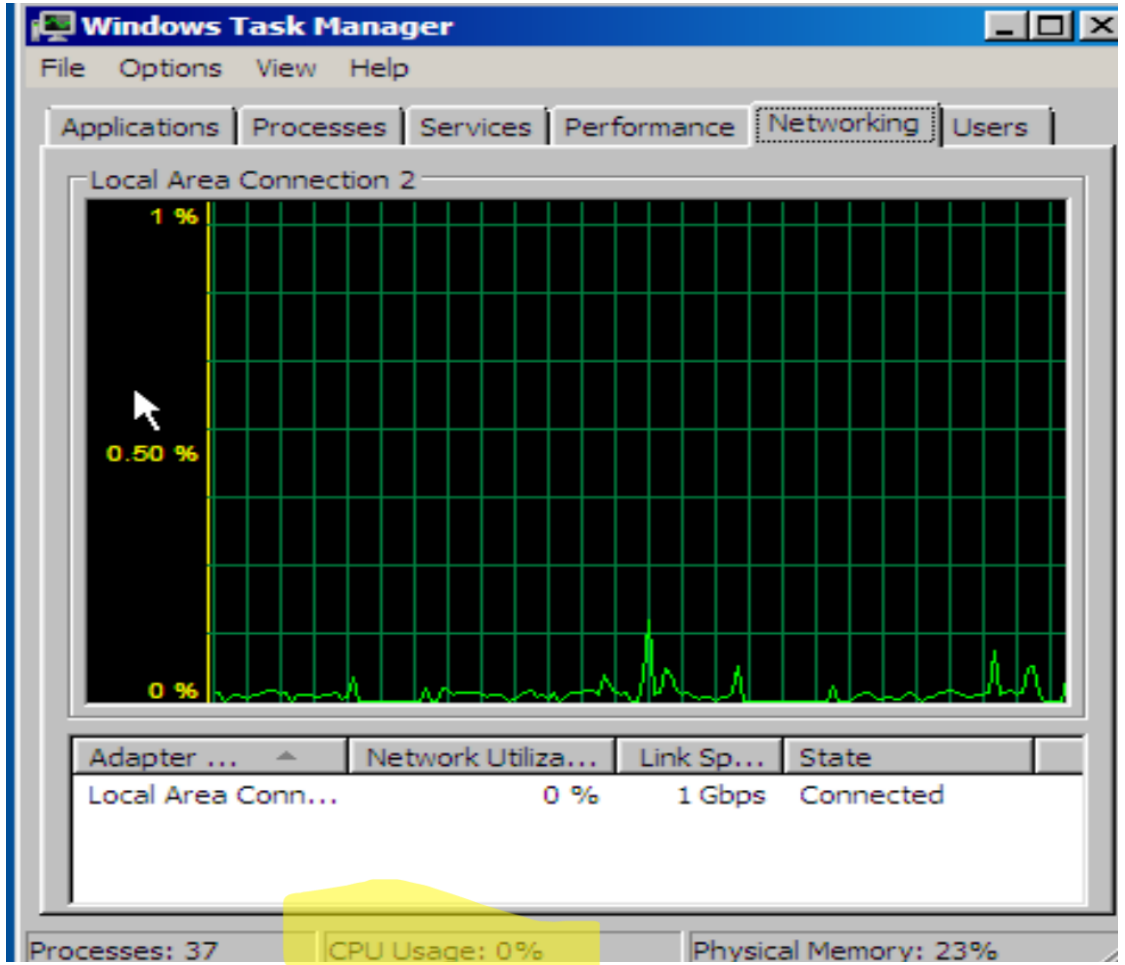
- VPNs improve your privacy
- VPNs can protect you from cyber attacks
- They bypass online censorship
- ISPs can’t throttle your bandwidth
- Torrenting is much safer
- VPNs help you save money online
- No more geo-restrictions
- Excellent for businesses

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
 49152            : .S..A... 128 63241 64240    46
 49155            : .S..A... 128 63497 64240    46
  5357            : .S..A... 128 60949 64240    46
 49153            : .S..A... 128 64933 64240    46
 49156            : .S..A... 128 65189 64240    46
 49157            : .S..A... 128 65445 64240    46
All replies received. Done.
Not responding ports: (514 shell) (1220 ) (1222 ) (1225 ) (1254 ) (1255 ) (1256
64 ) (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 ) (149
499 ) (1500 ) (1501 ) (1502 ) (1503 ) (1504 ) (1505 ) (1506 ) (1507 ) (1508 ) (
(1515 ) (1516 ) (1517 ) (1518 ) (1519 ) (1520 ) (1521 ) (1522 ) (1523 ) (1524
```

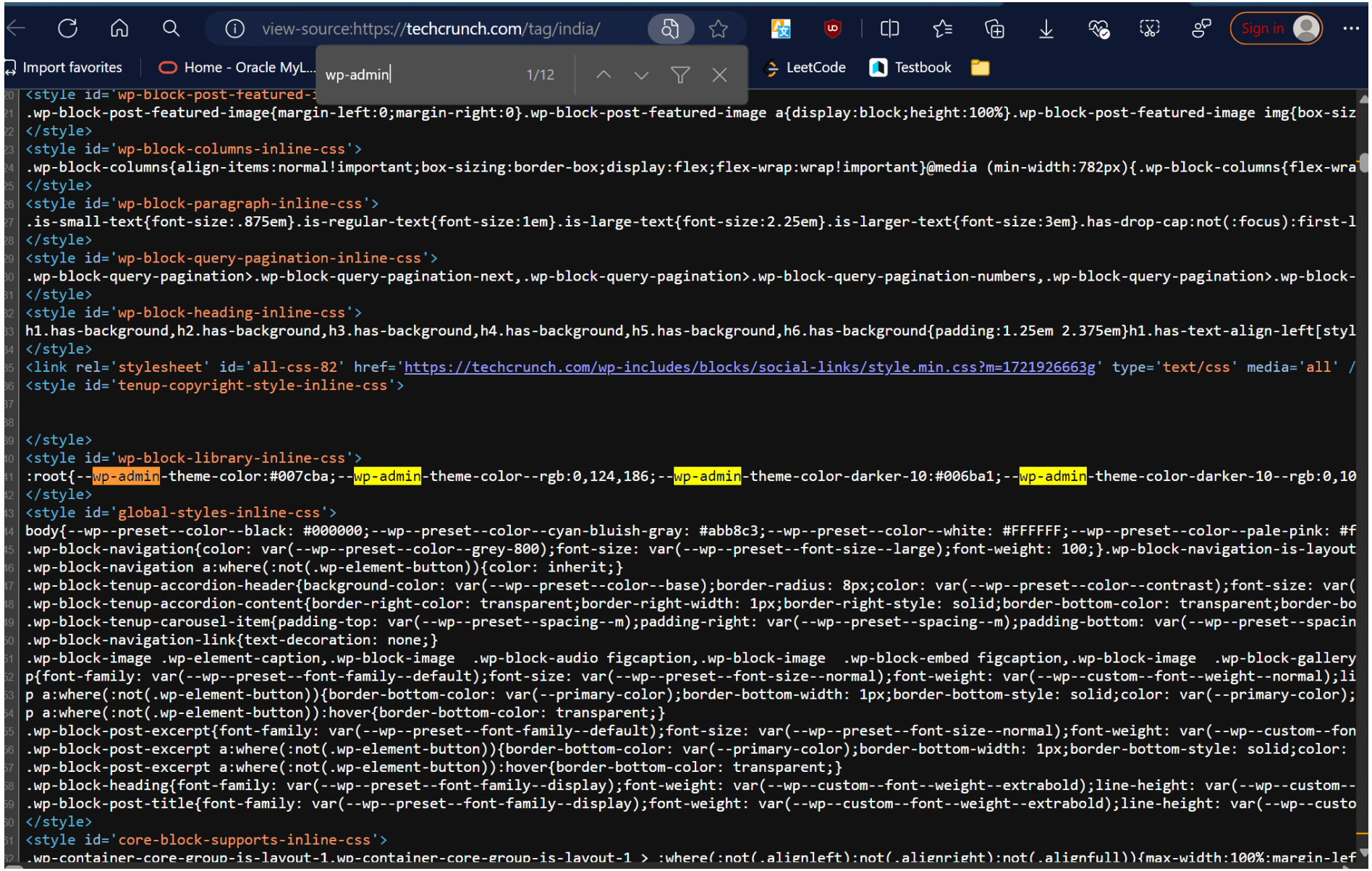


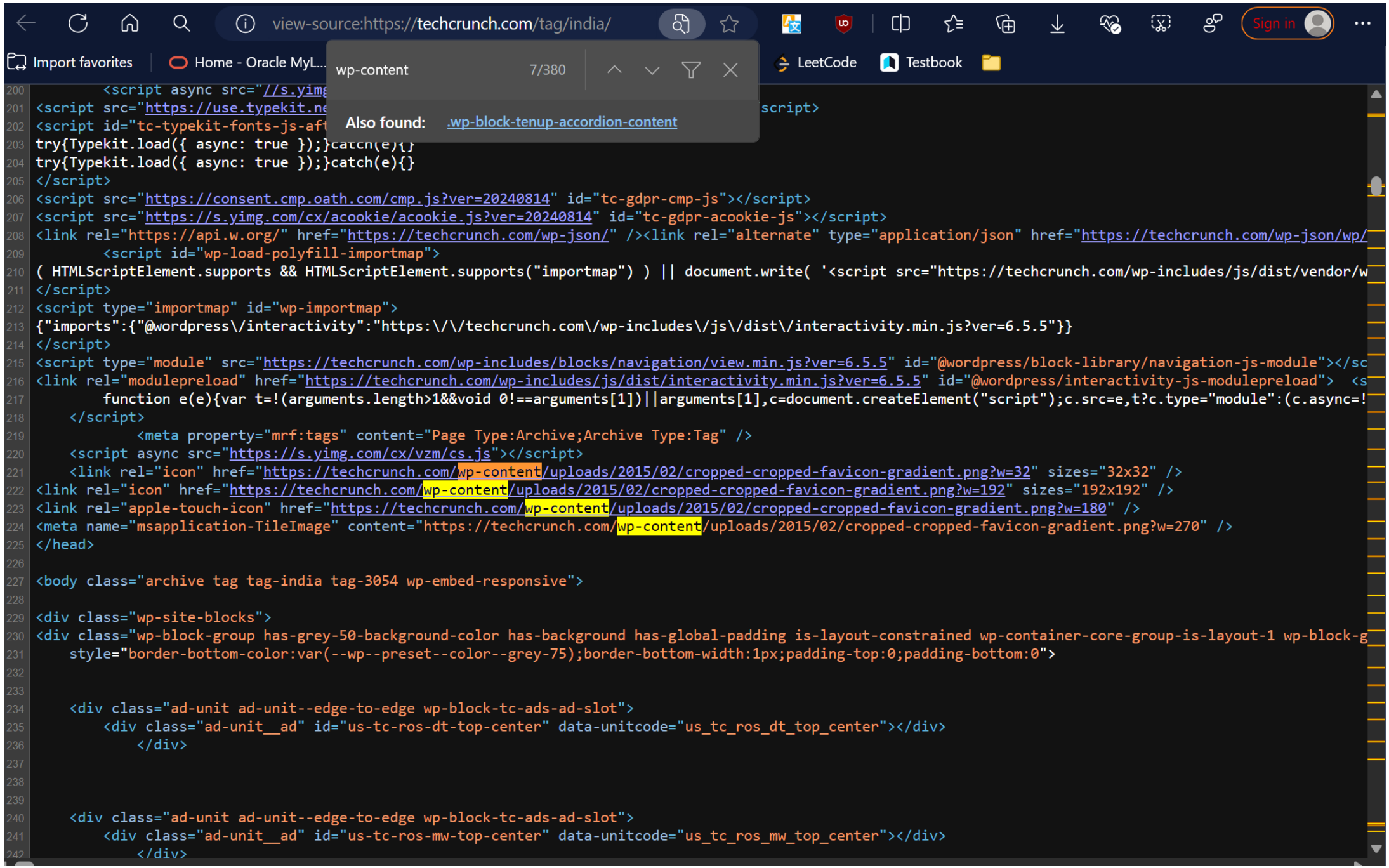
Mitigation strategies:-

- ❑ 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.

Q13. Explain how you would identify if a website is using WordPress. List the steps and tools used for detection




view-source:https://techcrunch.com/tag/india/
Sign in
Import favorites
Home - Oracle MyL...
LeetCode
Testbook
wp-content
7/380
Also found:
.wp-block-tenup-accordion-content

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.

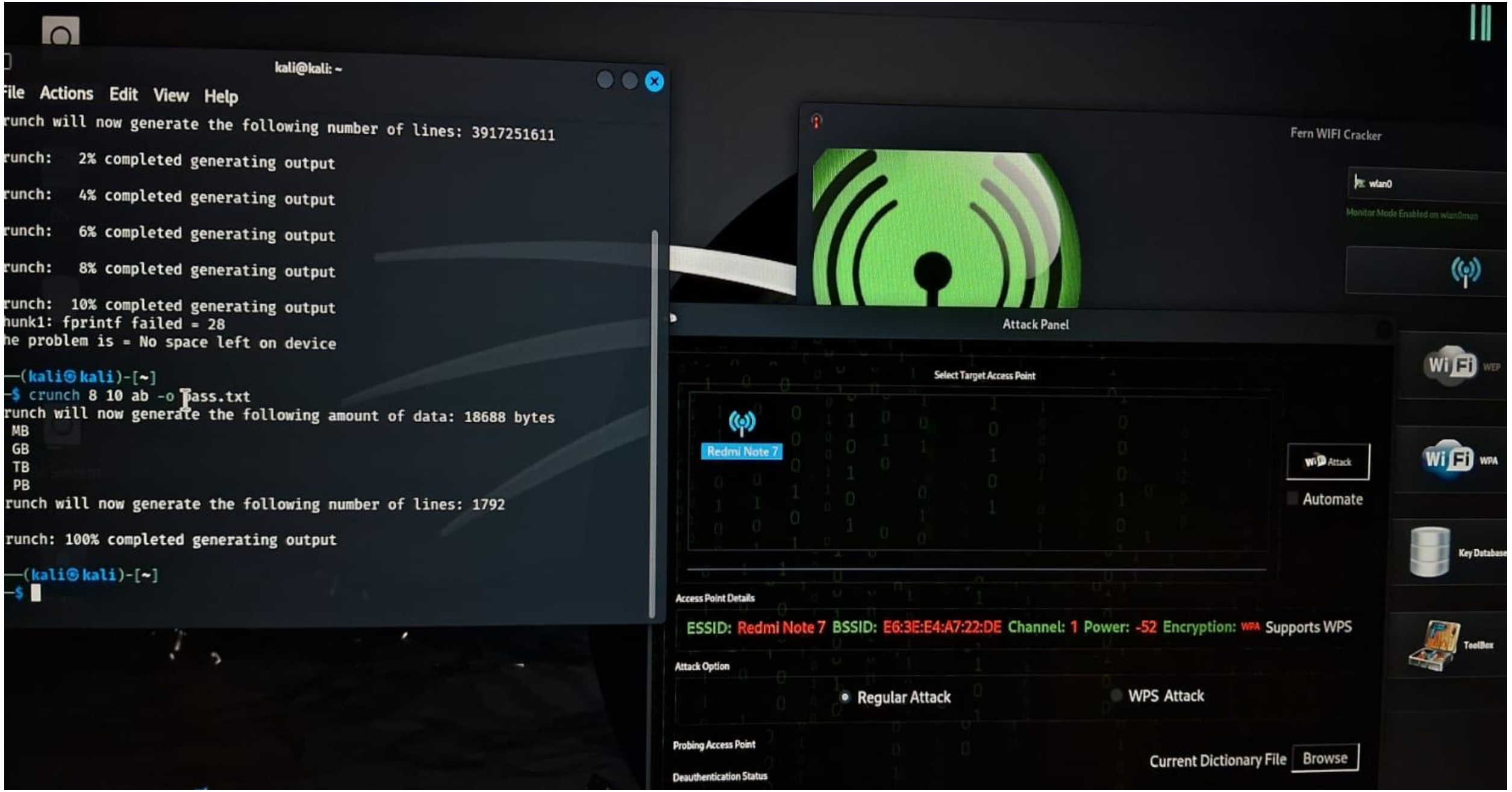
- "C:\xampp\htdocs\phishing_page.zip“
- https://drive.google.com/drive/folders/1QHuD_6KyB_Z2fFyWdWc8VXOiatdm_P3t?usp=drive_link

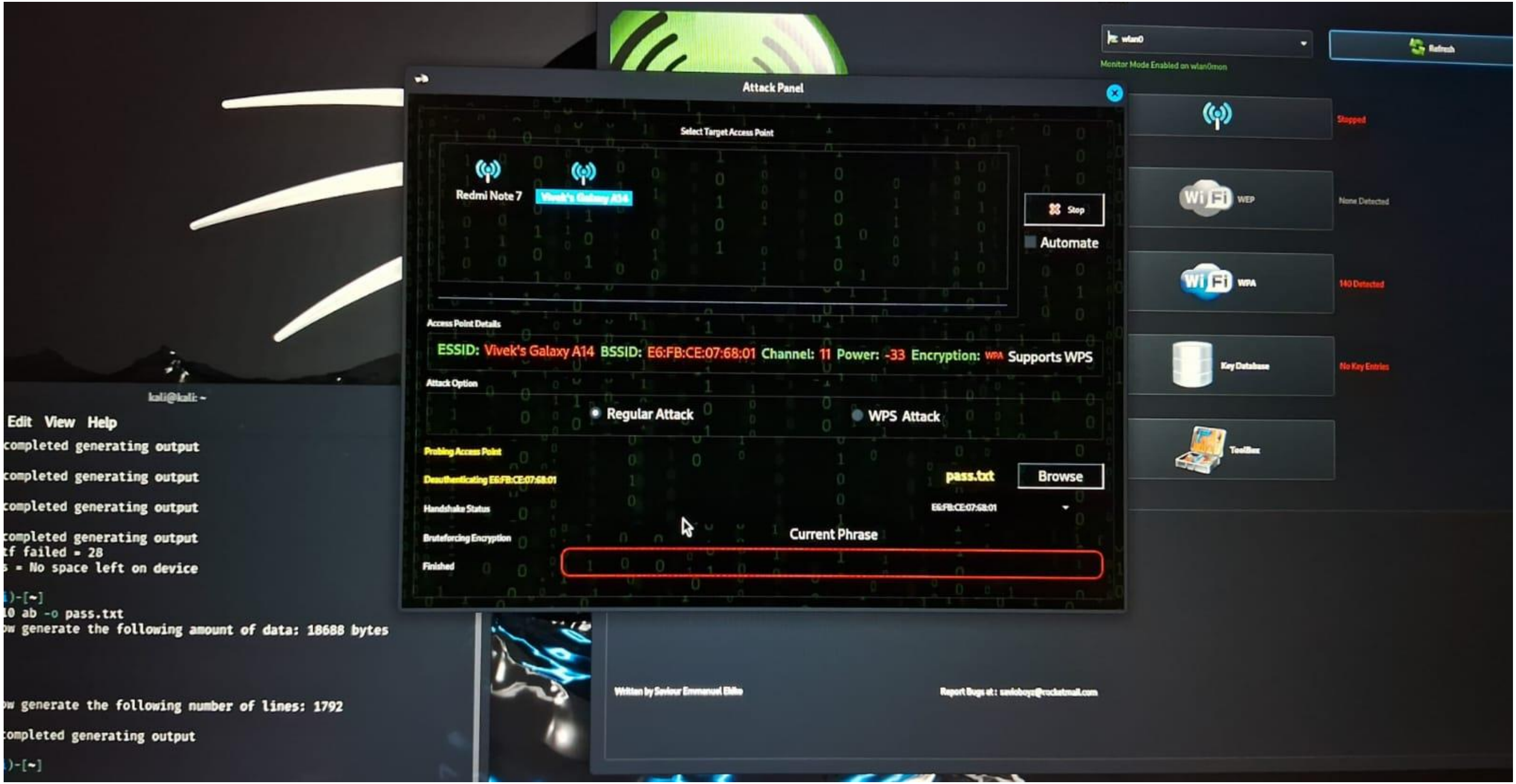
Index of /learn_phishing

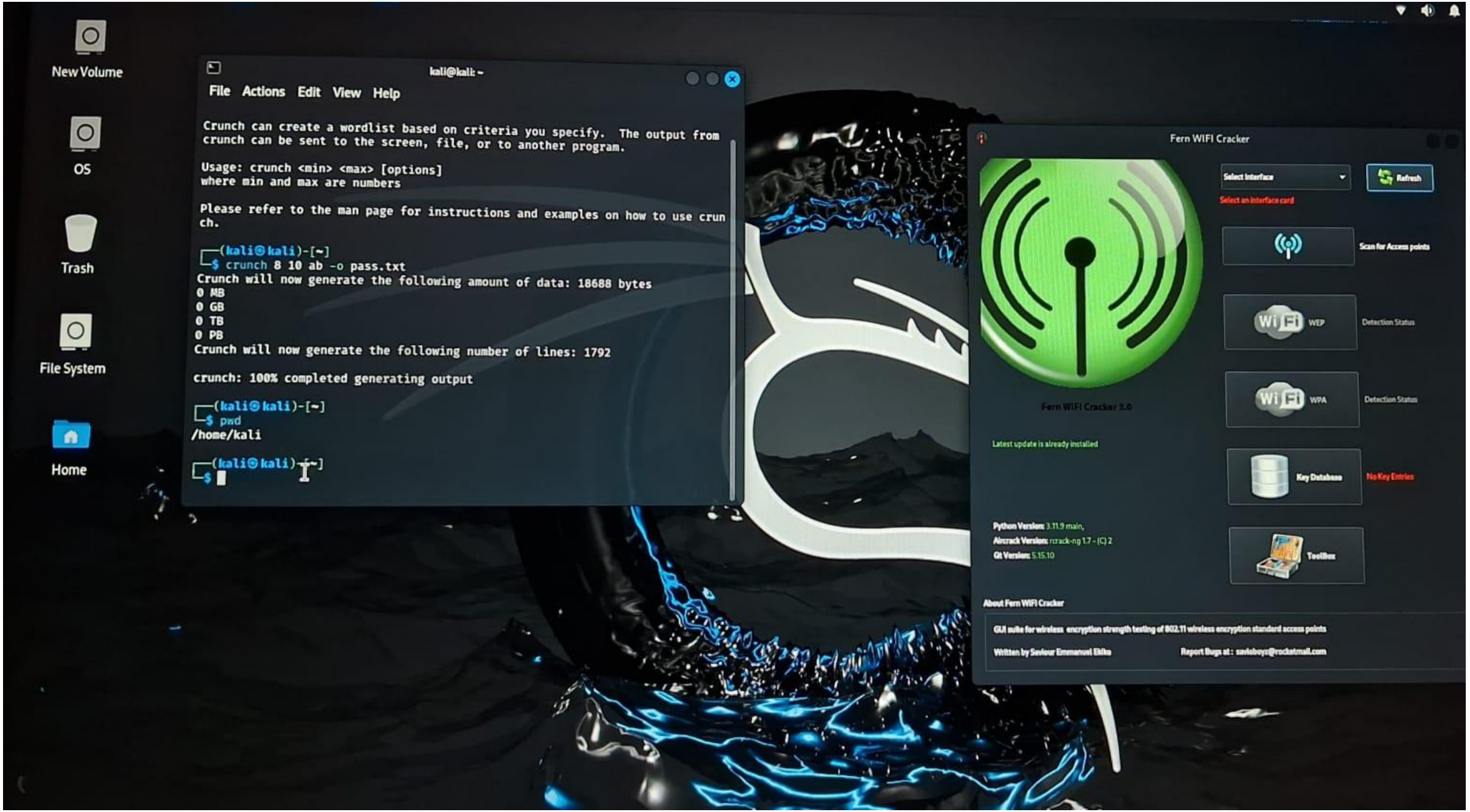
Name	Last modified	Size	Description
Parent Directory		-	
action.php	2024-08-14 11:54	404	
log.txt	2024-08-14 11:53	93	
login.php	2024-08-14 11:54	29K	

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

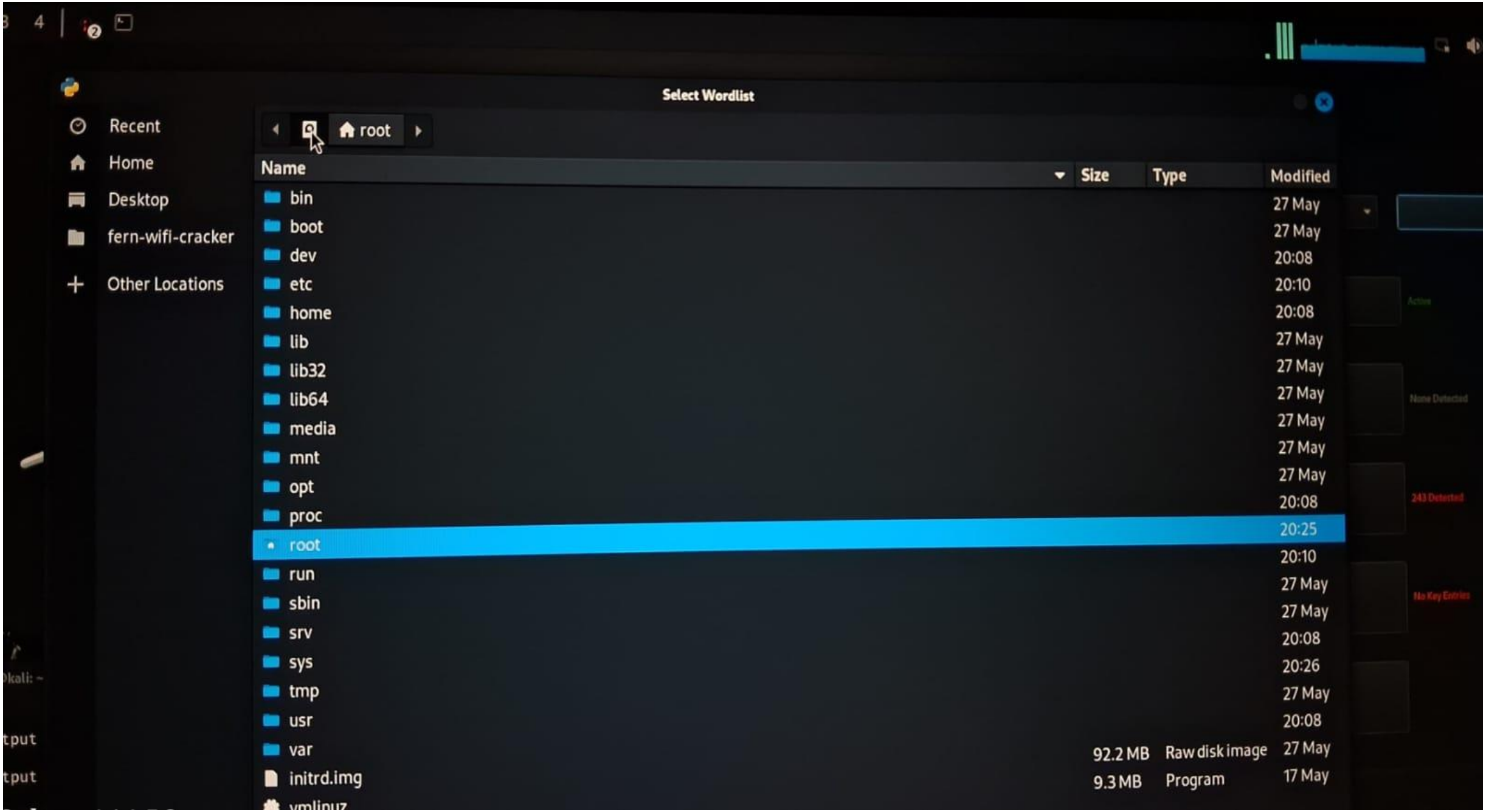
Q15. Set up a wireless network and attempt to crack its security using tools .
Document the process and results, and suggest measures to improve wireless security.

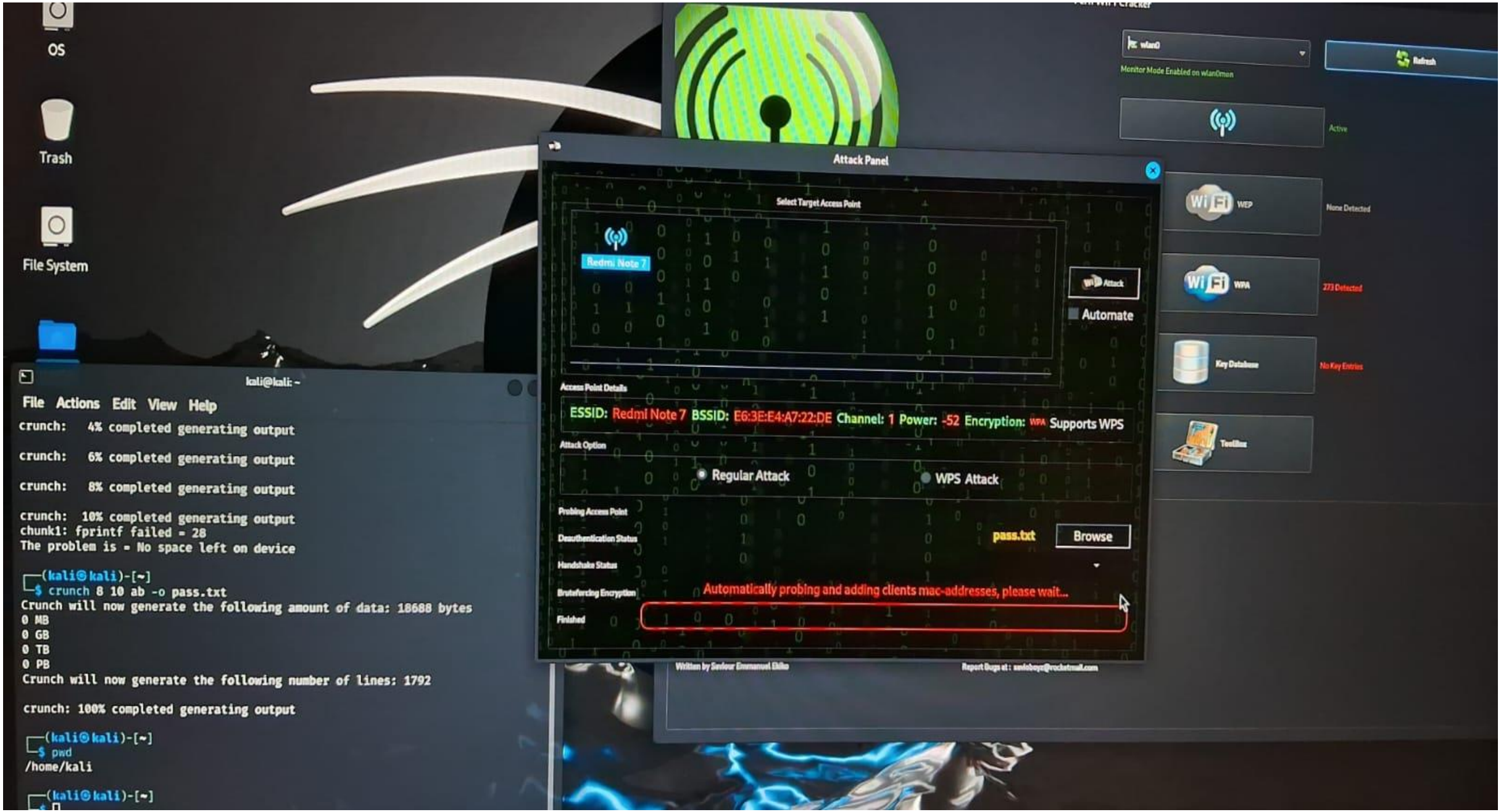

kali@kali: ~
File Actions Edit View Help
runch will now generate the following number of lines: 3917251611
runch: 2% completed generating output
runch: 4% completed generating output
runch: 6% completed generating output
runch: 8% completed generating output
runch: 10% completed generating output
hunk1: fprintf failed = 28
he problem is = No space left on device
(kali㉿kali)-[~]
$ crunch 8 10 ab -o pass.txt
runch will now generate the following amount of data: 18688 bytes
MB
GB
TB
PB
runch will now generate the following number of lines: 1792
runch: 100% completed generating output
(kali㉿kali)-[~]
$
Fern WIFI Cracker
wlan0
Monitor Mode Enabled on wlan0mon
Attack Panel
Select Target Access Point
Redmi Note 7
Attack
Automate
WEP
WPA
Key Database
ToolBox
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
Current Dictionary File
Browse


Attack Panel
Select Target Access Point
Redmi Note 7
Vivek's Galaxy A14
Stop
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
E6:FB:CE:07:68:01
Current Phrase
wlan0
Monitor Mode Enabled on wlan0mon
Refresh
Stopped
WEP
None Detected
WPA
140 Detected
Key Database
No Key Entries
Toolbox
Written by Saviour Emmanuel Ekiko
Report Bugs at : sanlobuys@rocketmail.com
kali@kali: ~
Edit View Help
completed generating output
completed generating output
completed generating output
completed generating output
f failed = 28
= No space left on device
)-[~]
0 ab -o pass.txt
w generate the following amount of data: 18688 bytes
w generate the following number of lines: 1792
completed generating output
)-[~]


New Volume
OS
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
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 crunch.
(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
Refresh
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: rcrack-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 Saviour Emmanuel Ekiko
Report Bugs at : saviaboyz@rocketmail.com


Fern WIFI Cracker
wlan0
Refresh
Monitor Mode Enabled on wlan0mon
Active
WEP
None Detected
WPA
53 Detected
Key Database
No Key Entries
ToolBox
Attack Panel
Select Target Access Point
Redmi Note 7
Attack
Automate
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
Finished
Current Dictionary File
Browse
Automatically probing and adding clients mac-addresses, please wait...


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


OS
Trash
File System
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)-[~]
Attack Panel
Select Target Access Point
Redmi Note 7
Attack
Automate
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
Finished
pass.txt
Browse
Automatically probing and adding clients mac-addresses, please wait...
Written by Saviour Emmanuel Ekiko
Report Bugs at : xeroboyz@rocketmail.com
wlan0
Monitor Mode Enabled on wlan0mon
Refresh
Active
WEP
None Detected
WPA
273 Detected
Key Database
No Key Entries
Toolbox