Name : Vivek Avdhesh Sharma   **Class :T.Y BSc.CS**

Roll No. : 24253026

**Expt No. : 1**

Date :

Subject : Ethical Hacking

Title of Experiment : Google and Who is Reconnaissance

Aim: Google and Who is Reconnaissance

   a) Use Google search techniques to gather information about a specific target or organisation
   b) Utilize advanced search operators to refine search results and access hidden information.
   c) Performs Who is lookups to retrieve domain registration information and gather details about the target's infrastructures.

Step 1: Search Prestashop on google and take a screenshot of the result displayed**.**
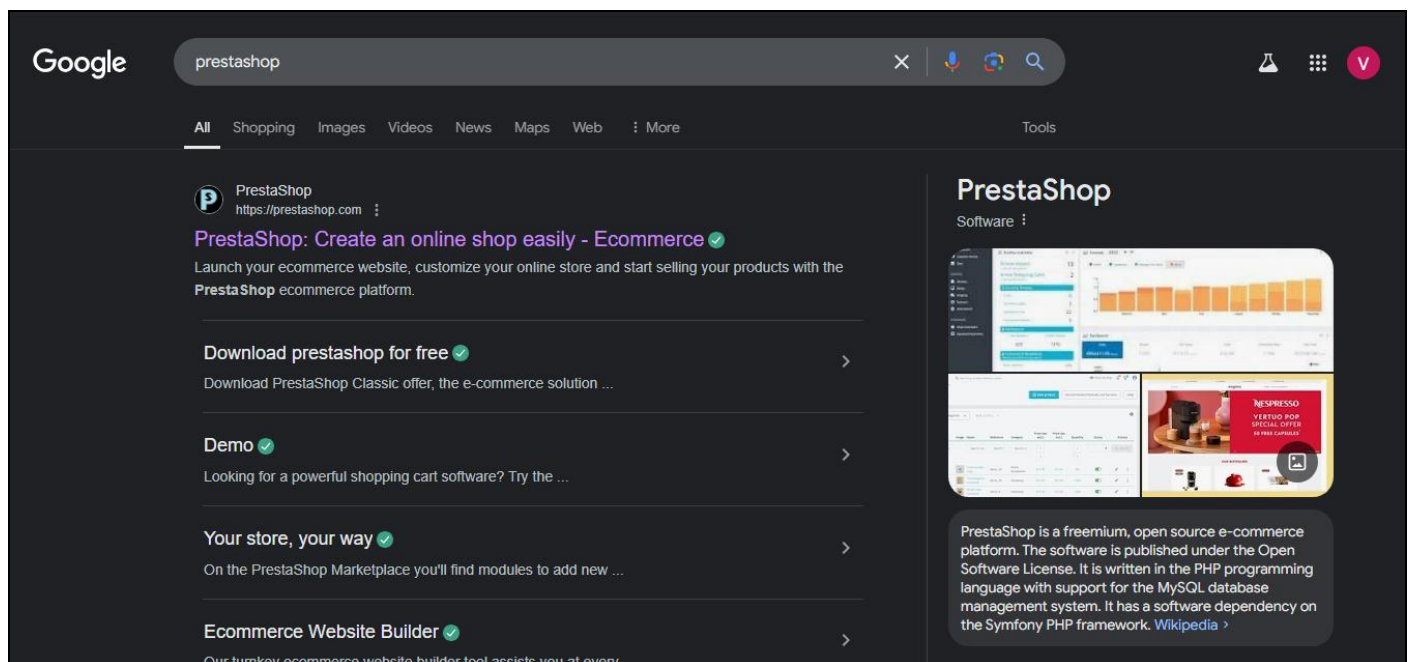
Remark :

Signature :

Step 2: Take screenshot of the slide panel containing prestaShop information.

Step 3: Go to browser and search for https://who.is/

Step 4: Search for www.prestashop.com

Step 5: Scroll & study the information.

Step 6: Click on DNS record.

Step 7: Click on Diagnosis.

Step 8: Search Codepen.io on Google & take screenshot of the result displayed.

Step 9: take screenshot of the side panel containing codepen.io information.

Step 10: Go to who.is and Now, search for codepen.io

Step 11: Click on DNS Record.

DNS Records for codepen.io

cache expires in 8 minutes and 34 seconds

Hostname	Type	TTL	Priority	Content
codepen.io	SOA	1800		albert.ns.cloudflare.com dns@cloudflare.com 2361068376 10000 2400 604800 1800
codepen.io	NS	21600		albert.ns.cloudflare.com
codepen.io	NS	21600		kristin.ns.cloudflare.com
codepen.io	A	300		104.16.32.228
codepen.io	A	300		104.18.111.164
codepen.io	AAAA	300		2606:4700::6812:6fa4
codepen.io	AAAA	300		2606:4700::6810:20e4
codepen.io	MX	300	5	alt2.aspmx.l.google.com
codepen.io	MX	300	10	aspmx3.googlemail.com
codepen.io	MX	300	5	alt1.aspmx.l.google.com
codepen.io	MX	300	10	aspmx2.googlemail.com
codepen.io	MX	300	1	aspmx.l.google.com
www.codepen.io	A	300		104.18.111.164

Step 12 : Click on Diagnosis.

codepen.io
diagnostic tools

[Whois] [RDAP] [DNS Records] [**Diagnostics**]

Ping

```
PING codepen.io (104.16.32.228) 56(84) bytes of data.
64 bytes from 104.16.32.228 (104.16.32.228): icmp_seq=1 ttl=56 time=2.86 ms
64 bytes from 104.16.32.228 (104.16.32.228): icmp_seq=2 ttl=56 time=2.03 ms
64 bytes from 104.16.32.228 (104.16.32.228): icmp_seq=3 ttl=56 time=2.03 ms
64 bytes from 104.16.32.228 (104.16.32.228): icmp_seq=4 ttl=56 time=2.10 ms
64 bytes from 104.16.32.228 (104.16.32.228): icmp_seq=5 ttl=56 time=2.09 ms

--- codepen.io ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.026/2.221/2.857/0.319 ms
```

Traceroute

```
traceroute to codepen.io (104.18.111.164), 30 hops max, 60 byte packets
 1  ip-10-0-0-119.ec2.internal (10.0.0.119)  18.330 ms  18.300 ms  18.269 ms
 2  216.182.239.59 (216.182.239.59)  45.879 ms 244.5.3.7 (244.5.3.7)  18.240 ms 216.182.231.86 (216.182.231.86)  19.453 ms
 3  240.3.84.69 (240.3.84.69)  18.147 ms 240.0.56.99 (240.0.56.99)  18.127 ms 240.0.56.67 (240.0.56.67)  18.108 ms
 4  240.3.180.78 (240.3.180.78)  18.097 ms 100.66.29.196 (100.66.29.196)  18.076 ms 240.3.180.79 (240.3.180.79)  18.046 ms
 5  240.3.180.82 (240.3.180.82)  18.025 ms 100.66.27.190 (100.66.27.190)  18.008 ms 241.0.4.197 (241.0.4.197)  17.958 ms
 6  99.83.116.94 (99.83.116.94)  17.959 ms *  2.341 ms
 7  * * 240.3.180.84 (240.3.180.84)  2.219 ms
 8  173.245.63.121 (173.245.63.121)  2.471 ms 173.245.63.97 (173.245.63.97)  2.880 ms 173.245.63.149 (173.245.63.149)  2.794 ms
 9  104.18.111.164 (104.18.111.164)  2.212 ms  2.179 ms  2.039 ms
```