

Dapoli Education Society's
DAPOLI URBAN BANK OF SENIOR SCIENCE COLLEGE
DAPOLI , Dist. Ratnagiri – 415713
Department of Computer Science

Name : Vivek Avdhesh Sharma

Class :T.Y BSc.CS

Roll No. : 24253026

Expt No. : 1

Date :

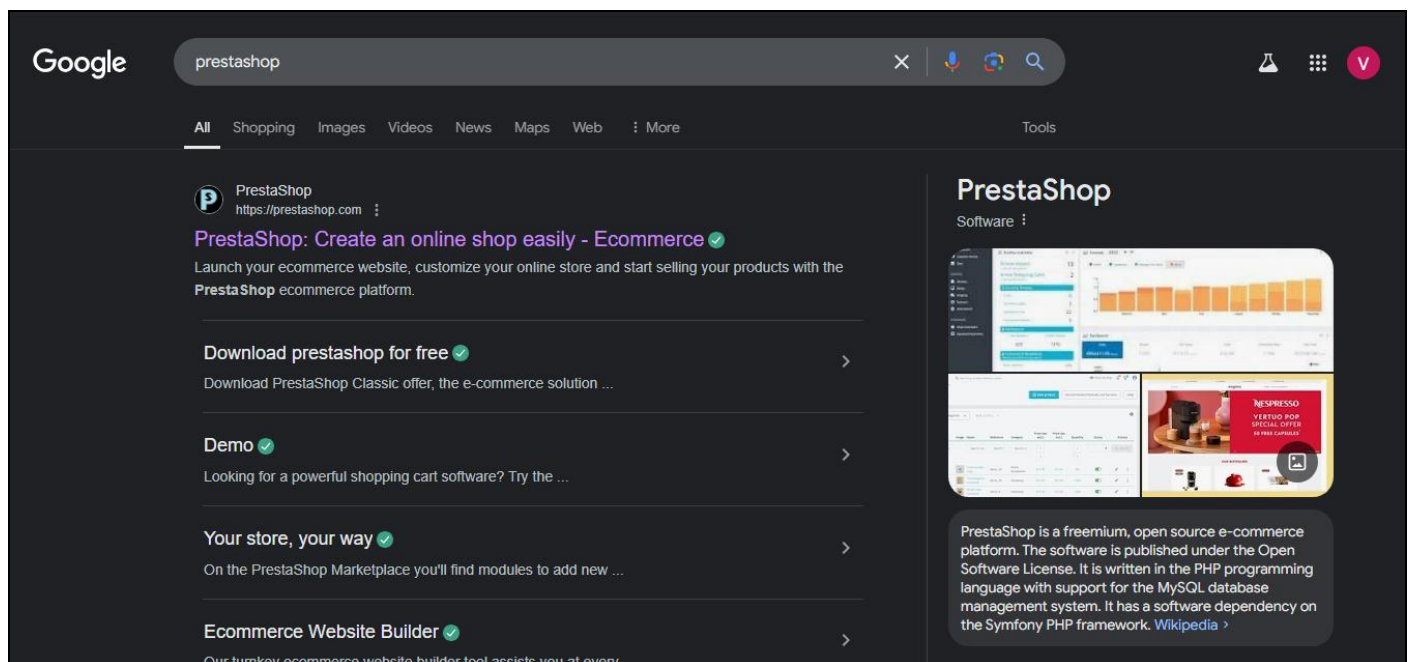
Subject : Ethical Hacking

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.

The screenshot shows the Wikipedia article for PrestaShop. The page has a dark header with the Wikipedia logo and a search bar. The article title "PrestaShop" is prominently displayed. Below the title, there's a "Contents" sidebar on the left and an "Appearance" sidebar on the right. The main content area features a warning box stating that the article has multiple issues, including a need for additional citations and excessive reliance on primary sources. The article text describes PrestaShop as a freemium, open source e-commerce platform published under the Open Software License (OSL), written in PHP, and using MySQL and Symfony. A "Prestashop" infobox on the right lists details: Industry (Internet), Founded (2007; 18 years ago in Paris, France), Founder (Bruno Lévéque, Igor Schlumberger), and Headquarters (Paris, France).

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

The screenshot shows the homepage of the who.is website. The header is dark with links for Premium Domains, Transfer, Features, Login, and Sign Up. The main section features the "who.is" logo and the text "WHOIS Search, Domain Name, Website, and IP Tools". Below this is a search bar with the placeholder text "Domain names or IP addresses..." and a blue search button. A small notification indicates the user's IP address is 72.14.201.138. At the bottom, there's a blue banner with links for "Looking to get a website?", "Web Hosting", "Website Builder", and "SSL Certificates". A large advertisement for name.com is also visible, promoting a 15% discount with the promo code WHOIS.

Step 4: Search for www.prestashop.com

This screenshot shows the same who.is website as the previous one, but with the search bar filled with "www.prestashop.com". The search button is still blue. The notification at the bottom now shows the user's IP address as 60.254.0.97. The rest of the page layout, including the header, logo, and footer, remains the same.

Step 5: Scroll & study the information.

who.is

Premium DomainsTransferFeaturesLoginSign Up

Search domains or IPs

Important Dates

Expires On

2025-04-11

Registered On

2007-04-11

Updated On

2024-02-25

Name Servers

[albert.ns.cloudflare.com](#)

[172.64.33.58](#)

[emily.ns.cloudflare.com](#)

[108.162.192.155](#)

Similar Domains

[prest-on.com](#) | [prest-0.net](#) | [prest-0104.com](#) | [prest-400x285igegroupside.com](#) | [prest-a-connect.com](#) | [prest-a-domicile.com](#) | [prest-a-flate.com](#) | [prest-a-porter.com](#) | [prest-a-pro.fr](#) | [prest-acaoservicos.com.br](#) | [prest-achat.fr](#) | [prest-action.com](#) | [prest-admin.fr](#) | [prest-aerogommage-occitanie.fr](#) | [prest-affair.fr](#) | [prest-agency.com](#) | [prest-agency.es](#) | [prest-agency.eu](#) | [prest-agency.fr](#) | [prest-agency.net](#) |

Registrar Data

We will display stored WHOIS data for up to 30 days.

Make Private Now

Registrant Contact Information:

REDACTED FOR PRIVACY

Build your business from the name up.

Learn more

Save 15% on your first order with promo code: **WHOIS**

Site Status

Status

Active

Server Type

cloudflare

Suggested Domains for prestashop.com

who.is

Premium DomainsTransferFeaturesLoginSign Up

Search domains or IPs

Registrar Data

We will display stored WHOIS data for up to 30 days.

Make Private Now

Registrant Contact Information:

Name:

REDACTED FOR PRIVACY

Organization:

REDACTED FOR PRIVACY

Address Line 1:

REDACTED FOR PRIVACY

Address Line 2:

REDACTED FOR PRIVACY

City:

REDACTED FOR PRIVACY

State/Province:

REDACTED FOR PRIVACY

Postal Code:

REDACTED FOR PRIVACY

Country:

FR

Phone:

REDACTED FOR PRIVACY

Fax:

REDACTED FOR PRIVACY

Email:

info@domain-contact.org

Full Address:

REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, FR

Administrative Contact Information:

Name:

REDACTED FOR PRIVACY

Organization:

REDACTED FOR PRIVACY

Address Line 1:

REDACTED FOR PRIVACY

Address Line 2:

REDACTED FOR PRIVACY

City:

REDACTED FOR PRIVACY

State/Province:

REDACTED FOR PRIVACY

Postal Code:

REDACTED FOR PRIVACY

Country:

REDACTED FOR PRIVACY

Phone:

REDACTED FOR PRIVACY

Fax:

REDACTED FOR PRIVACY

Server Type

cloudflare

Suggested Domains for prestashop.com

☐ p-rest-a-shop.live

\$3.99

☐ prestashops.live

\$3.99

☐ prestastore.live

\$3.99

☐ shopprestashop.live

\$3.99

☐ p-rest-a-shop.com

\$12.99

Purchase Selected Domains

Use promo code **WHOIS** to save 15% on your first [Name.com order.](#)

Find the perfect domain at **name.com**

Step 6: Click on DNS record.

who.is

Premium DomainsTransferFeaturesLoginSign Up

Search domains or IPs

WhoisRDAPDNS RecordsUptimeDiagnostics

DNS Records for prestashop.com

cache expires in 9 minutes and 29 seconds

Hostname	Type	TTL	Priority	Content
prestashop.com	SOA	1800		albert.ns.cloudflare.com dns.cloudflare.com 2362103529 10000 2400 604800 1800
prestashop.com	NS	21600		emily.ns.cloudflare.com
prestashop.com	NS	21600		albert.ns.cloudflare.com
prestashop.com	A	300		104.16.210.130
prestashop.com	A	300		104.16.211.130
prestashop.com	AAAA	300		2606:4700::6810:d282
prestashop.com	AAAA	300		2606:4700::6810:d382
prestashop.com	MX	300	10	aspmx2.googlemail.com
prestashop.com	MX	300	10	aspmx3.googlemail.com
prestashop.com	MX	300	1	aspmx1.google.com
prestashop.com	MX	300	5	alt2.aspmx1.google.com
prestashop.com	MX	300	5	alt1.aspmx1.google.com
www.prestashop.com	A	300		104.16.211.130
www.prestashop.com	A	300		104.16.210.130
www.prestashop.com	AAAA	300		2606:4700::6810:d382
www.prestashop.com	AAAA	300		2606:4700::6810:d282

Step 7: Click on Diagnosis.

The screenshot shows the 'who.is' website with a navigation bar at the top containing 'Premium Domains', 'Transfer', 'Features', 'Login', and 'Sign Up'. A search bar on the right says 'Search domains or IPs'. The main content area is for 'prestashop.com' and includes buttons for 'Whois', 'RDAP', 'DNS Records', and 'Diagnostics'. The 'Diagnostics' section is active, showing 'Ping' and 'Traceroute' results.

Ping

```
PING prestashop.com (104.16.211.130) 56(84) bytes of data:
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=1 ttl=56 time=2.24 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=2 ttl=56 time=1.48 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=3 ttl=56 time=1.45 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=4 ttl=56 time=1.43 ms
64 bytes from 104.16.211.130 (104.16.211.130): icmp_seq=5 ttl=56 time=1.53 ms

--- prestashop.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.426/1.625/2.244/0.311 ms
```

Traceroute

```
traceroute to prestashop.com (104.16.210.130), 30 hops max, 60 byte packets
 1 10.0.0.0-0.119.0.0 (10.0.0.119) 0.243 ms 0.238 ms 0.251 ms
 2 244.5.3.51 (244.5.3.51) 9.095 ms ec2-3-236-62-47.compute-1.amazonaws.com (3.236.62.47) 6.371 ms *
 3 240.3.12.96 (240.3.12.96) 1.253 ms 240.0.56.66 (240.0.56.66) 1.259 ms 240.3.84.65 (240.3.84.65) 1.640 ms
 4 240.3.184.36 (240.3.184.36) 2.460 ms 100.66.29.180 (100.66.29.180) 5.686 ms 240.0.236.1 (240.0.236.1) 1.997 ms
 5 100.66.47.12 (100.66.47.12) 17.114 ms 240.3.180.79 (240.3.180.79) 2.238 ms 241.0.4.214 (241.0.4.214) 1.331 ms
 6 * 99.83.90.51 (99.83.90.51) 10.822 ms 99.83.116.94 (99.83.116.94) 2.182 ms
 7 99.83.116.95 (99.83.116.95) 3.044 ms 240.0.236.1 (240.0.236.1) 1.871 ms 99.83.90.51 (99.83.90.51) 2.943 ms
 8 99.83.93.219 (99.83.93.219) 6.833 ms 173.245.63.119 (173.245.63.119) 3.002 ms 99.83.90.51 (99.83.90.51) 11.074 ms
 9 104.16.210.130 (104.16.210.130) 2.030 ms 2.230 ms 2.516 ms
```

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

The screenshot shows a Google search for 'Codepen'. The search bar at the top contains 'Codepen' and the Google logo. Below the search bar, the 'All' tab is selected, showing search results for 'CodePen'. The first result is 'CodePen: Online Code Editor and Front End Web Developer ...' with a green checkmark. Below this, there are links to 'HTML pen', 'Log In', 'CodePen Free Sign Up', and 'Challenges', each with a green checkmark and a right arrow.

CodePen
https://codepen.io

CodePen: Online Code Editor and Front End Web Developer ... ✓

CodePen doesn't work very well without JavaScript. We're all for progressive enhancement, but CodePen is a bit unique in that it's all about writing and ...

HTML pen ✓ >

About the <head>. In CodePen, whatever you write in the HTML ...

Log In ✓ >

Log In ... If the email address associated with your social ...

CodePen Free Sign Up ✓ >

Free · Include an UPPER and lowercase letter · Include a ...

Challenges ✓ >

CodePen Challenges are purely for fun. It's not a competition.

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

CodePen

8 languages

Contents hide

(Top)
References
External links

Article Talk

Read Edit View history Tools

From Wikipedia, the free encyclopedia



Some of this article's **listed sources may not be reliable**. Please help improve this article by looking for better, more reliable sources. Unreliable citations may be challenged and removed. *(July 2021)* [\(Learn how and when to remove this message\)](#)

CodePen is an [online community](#) for testing and showcasing user-created [HTML](#), [CSS](#) and [JavaScript](#) code snippets. It functions as an online [code editor](#) and [open-source](#) learning environment, where developers can create code snippets, called "pens," and test them. It was founded in 2012 by [full-stack developers](#) Alex Vazquez and Tim Sabat and front-end designer Chris Coyier.^{[1][2]}^{*non-primary source needed*} Its employees work remotely, rarely all meeting together in person. CodePen is a large community for web designers and developers to showcase their coding skills,^[3] with an estimated 330,000^[4] ^{*unreliable source?*} registered users and 14.16 million monthly visitors.^[5] ^{*unreliable source?*}

CodePen

Available in	English
Founder(s)	Alex Vazquez Tim Sabat Chris Coyier
URL	codepen.io
Commercial	Yes
Registration	Optional
Users	339,000
Launched	2012· 13 years ago

Appearance hide

Text

☐ Small
☒ Standard
☐ Large

Width

☒ Standard
☐ Wide

Color (beta)

☐ Automatic
☒ Light
☐ Dark

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

who.is

Premium Domains Transfer Features Login Sign Up

Search domains or IPs

Important Dates

Expires On	2028-02-26
Registered On	2012-02-26
Updated On	2024-11-18

Name Servers

albert.ns.cloudflare.com	172.64.33.58
kristin.ns.cloudflare.com	172.64.32.181

Similar Domains

[codepen-13-cyclotourisme.com](#) | [codepen-buildonbooks.org.uk](#) | [codepen-caluirevernay.fr](#) | [codepen-cyclo79.fr](#) | [codepen-dz.com](#) | [codepen-egypt.com](#) | [codepen-electricite.fr](#) | [codepen-electrodom.com](#) | [codepen-electrodom.fr](#) | [codepen-epgv59.fr](#) | [codepen-epgvnord.fr](#) | [codepen-eure.fr](#) | [codepen-kaolack.com](#) | [codepen-pieces.fr](#) | [codepen-plastiques.fr](#) | [codepen-telecom.com](#) | [codepen.ai](#) | [codepen.cl](#) | [codepen.cn](#) | [codepen.co](#) |

Registrar Data

We will display stored WHOIS data for up to 30 days.

Registrar Contact Information:

Name:	REDACTED FOR PRIVACY
Organization:	CodePen
Address Line 1:	63-65 boulevard Massena
Address Line 2:	
City:	Paris
State/Province:	Paris

Make Private Now

Build your business from the name up.

Learn more

Save 15% on your first order with promo code: **WHOIS**

Site Status

Status	Inactive
Server Type	

Suggested Domains 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.

who.is

Premium DomainsTransferFeaturesLoginSign Up

Search domains or IPs

Q

codepen.io

diagnostic tools

WhoisRDAPDNS RecordsDiagnostics

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