



AIM: Perform Information Gathering/ Footprinting

Experiment 9

Shraddha She

60004230126

7483th Comp 1

Aim: Perform information gathering / Footprinting

Theory: Information gathering, also known as Reconnaissance, is a crucial initial phase in cybersecurity. It involves collecting as much relevant data as possible about a target system or network to identify potential vulnerabilities and attack vectors.

- 1) Passive Information Gathering - This involves gathering information without directly interacting with the target, which includes searching online public sources such as social media, search engines, forums, etc.
- 2) Active Information Gathering - It involves more direct interaction with the target system. Techniques may include port scanning, network mapping, and service enumeration etc.
- 3) Footprinting - This is the process of collecting information about the target organization's network, systems and infrastructure, involves identifying IP addresses, domain names, network blocks, etc.
- 4) Enumeration - It involves gathering specific information about the target's system, such as user accounts, network shares, installed software and services running on the network.
- 5) Social Engineering - This technique involves manipulating individuals within the target organization to divulge confidential information or perform actions that compromise security.

Scanned with CamScanner

Conclusion: Thus, we have learnt how important Information gathering is in cybersecurity and how to perform it using various tools.

1. Whois

Whois Domain Lookup

Whois search for Domain and IP

Q SEARCH

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

vulnweb.com

Updated 2 hours ago ↻

Domain Information	
Domain:	vulnweb.com
Registrar:	EuroDNS S.A.
Registered On:	2010-06-14
Expires On:	2025-06-13
Updated On:	2023-05-26
Status:	clientTransferProhibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com



Registrant Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator @acunetix.com



Administrative Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator @acunetix.com



Technical Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com

Raw Whois Data

Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: <http://www.eurodns.com>
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: **legalservices@eurodns.com**
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: **administrator@acunetix.com**
Registry Admin ID:
Admin Name: Acunetix Acunetix

Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: **administrator**@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: **administrator**@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of WHOIS database: 2024-02-17T05:16:12Z <<<

2. Tracert

```
C:\Users\SHAUN FERNANDES>tracert google.com

Tracing route to google.com [142.250.192.78]
over a maximum of 30 hops:

 1      1 ms      1 ms      1 ms  192.168.0.1
 2      6 ms      1 ms      1 ms  103.255.115.99
 3      3 ms      3 ms      2 ms  103.255.115.97
 4      9 ms      8 ms      7 ms  202.134.145.222
 5     21 ms      3 ms      2 ms  202.134.145.125
 6      7 ms      3 ms      3 ms  202.134.145.153
 7     10 ms      3 ms      3 ms  202.134.145.121
 8     11 ms      4 ms      3 ms  103.233.140.42
 9      7 ms      3 ms      2 ms  74.125.37.7
10      8 ms      3 ms      7 ms  108.170.226.131
11     10 ms      3 ms      6 ms  bom12s16-in-f14.1e100.net [142.250.192.78]


Trace complete.
```


3. nslookup

```
sf1@DESKTOP-ST93SJ9:~$ nslookup amazon.com
Server:          192.168.240.1
Address:         192.168.240.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 52.94.236.248
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
```

4. Shodan

 SHODAN

Explore

Pricing ↗

hwarkadas

Q

TOTAL RESULTS

1

 View Report

 View on Map

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

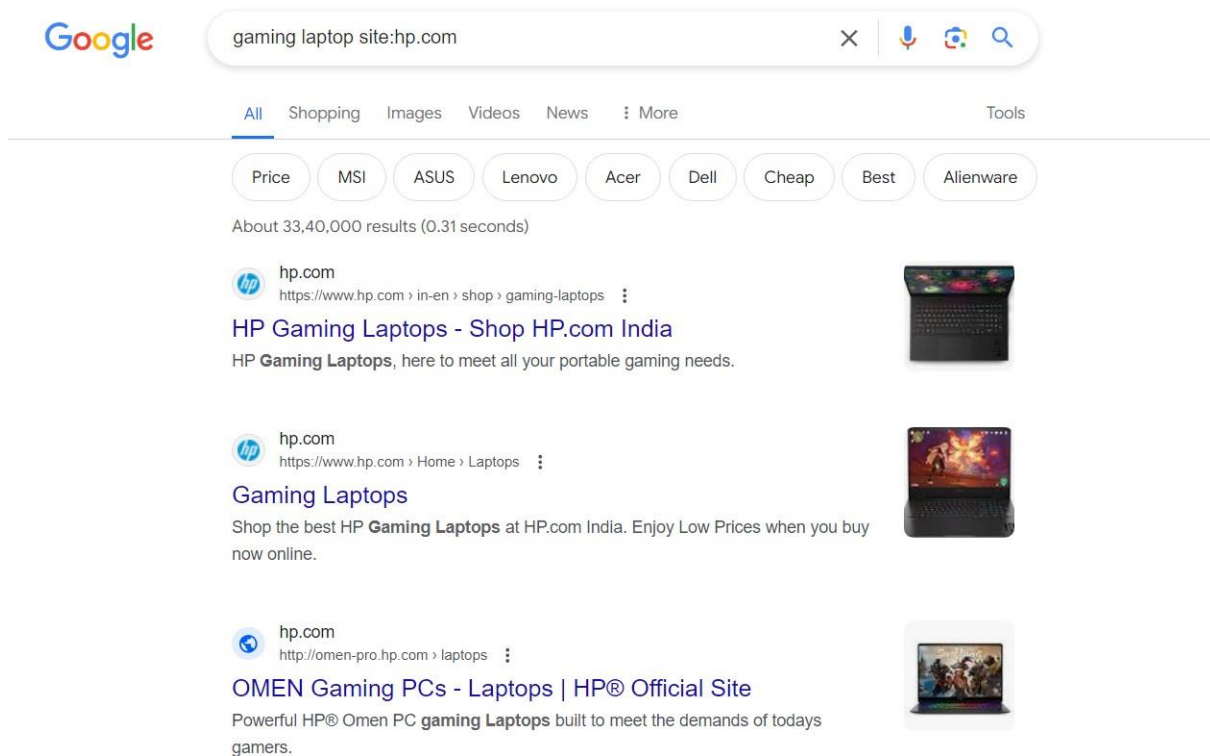
203.192.206.42
dhcp-192-206-42.in2oable.c
om
Indusind Media And
Communication Ltd
India, Mumbai

database

col-product

MS-SQL NTLM Info:
OS: Windows 10 (version 2004)/Windows Server (version 2004)
OS Build: 10.0.19041
Target Name: DWARKADAS-SHAWK
NetBIOS Domain Name: DWARKADAS-SHAWK
NetBIOS Computer Name: DWARKADAS-SHAWK
DNS Domain Name: DWARKADAS-SHAWKUPAR
FQDN: DWARKADAS-SHAWKUPAR

5. Google dork



CONCLUSION :

Thus, we have successfully studied various information gathering tools/ footprint tools and explored how they retrieve information from different sites.