Q1/

Bipin created a fake e-commerce website to lure people into entering their credit card information so that he could steal their money. While a security expert was using that website, he noticed something wrong and got to know that it is a fake website. Now that the expert can do a Whois lookup on the website, and get the details of the owner, can Bipin be tracked?

| | |
|---|---|
| A | Yes |
| B | No ✓ |

Well done. Correct Answer.

**Explanation:**
Whois information is in most cases not cross checked and the registrant can enter any information in the whois details while registering a domain/IP. Hence it cannot be used as a proof of ownership.

Q2/

While we are busy surfing the internet on a daily basis, we leave some traces of information that can be used to trace us. What term is commonly used to refer to these traces of information left by us on the internet?

| | |
|---|---|
| A | Breadcrumbs |
| B | Personal information |
| C | Digital footprints ✓ |

Well done. Correct Answer.

**Explanation:**
Digital Footprint is the trail of information a specific person leaves on the internet while he/she browses through the Internet.

Q3/

White box testing requires more information gathering than black box testing.

| | |
|---|---|
| A | True |
| B | False ✓ |

Well done. Correct Answer.

**Explanation:**
In white box testing, most of the information is provided by the client itself and although information assessment is still required, it is lesser as compared to that required during a black box test

Nalin did a Whois lookup for myntra.com and found some information about the domain owner. Which of these pieces of information is he unlikely to find?

A Full name

B Email address

C House address

D Office address

E None of the above

Q5/

Which of these services is used to get a list of all the domains hosted on a single IP address?

| | |
|---|---|
| A | WhoIs |
| B | Reverse registrant check |
| C | Hosting history |
| D | Reverse IP check ✓ |

Well done. Correct Answer.

**Explanation:**

Whois shows registration details of a domain. Reverse registrant check shows all domains registered by a single registrant. Hosting history shows whois information of a domain over time. Reverse IP check is used to see all other domains resolving to the same IP as the IP of a given domain.

Now that we have come to the end of this topic, you should be able to:

1. Explain the concept of digital footprinting
2. Gather Whois information of any website and analyse it
3. Find out other websites running on the shared server of a website

If you have doubts regarding any of the above mentioned points, please go through the relevant videos and text chapters again.

**Here are some key pieces of information that a security expert usually gathers about a website:**

1. Related domains and subdomains

2. Technology and programming languages being used

3. Cached pages

4. Website history

5. Publically indexed files on search engines

6. Default pages and login forms

7. Related IP addresses

8. Other services running on those IP addresses

9. Version of the services/softwares being used

10. Publicly disclosed vulnerabilities in the softwares being used

11. Default users

12. Default passwords

13. Valid email address and usernames

## Gathering targeted information about people

### 1. Name-How to find out full names and their related information:

Social media platforms

Professional platforms

### 2. Email- How to find out the name behind an email address:

Forgot password

Services linked to that email

Google search

### 3. Mobile numbers- How to find out the name behind a phone numbers:

Login and forgot password pages

Google search

## Gathering targeted information about organisations

### 1. How to find information about an organisation:

Social media platforms

Company review services

Webserver: To see the server software being used

**2. Going through the history of a website**

To see how the website looked in the past, its features, additions and deletions that have been made over time:

web.archive.org

Important sections:

Go to the year you want to see

Check out screenshots taken on any day, and also see the website as it was on that day

**3. Finding out sub domains related to a domain**

www.dnsdumpster.com

Important sections:

Host Records (A): To see a list of all the sub domains of any given domain.

Q1/6

Web archive can be used to interact with an older version of any recorded website and its servers.

A True

B False

Well done. Correct Answer.

**Explanation:**
Archives only takes snapshots - i.e only the front-end part of the website is recorded. So we can see how the website looked, previous images, files, designs, etc. Interaction with an older version of the website is not possible via Web Archives.

Q2/6

DNSdumpster.com can be used for which of the following?

| | | |
|---|---|---|
| A | Finding other subdomains of a domain | ✓ |

Well done. Correct Answer.

**Explanation:**
DNS Dumpster has a lot of features but finding other domains (not subdomains) related/similar to the domain is not one of them nor is providing whois information.

*69% students get this answer correct at their first attempt*

| | |
|---|---|
| B | Finding other domains related to a domain |
| C | Finding whois details of a domain |

Q3/6

Professional platforms can be used for gathering information about which of the following?

A People

B Organisations

C Websites

D All of the Above

Well done. Correct Answer.

**Explanation:**
Both people and organisations have professional profiles. Organisations also enlist their websites on such networks. Hence, professional social networks are extremely beneficial to information gatherers.

*64% students get this answer correct at their*

Q4/6

Which of the following websites can be used to identify the plugins being used by a domain?

| | |
|---|---|
| A | Crunchbase |
| B | Builtwith ✓ |

Well done. Correct Answer.

**Explanation:**
-Crunchbase is useful for looking at the financial and funding records of an organisation. -Glassdoor is for Company Review. -WhoIs is used for getting Whois information. -BuiltWith can be used to get a lot of information about the website running on a domain like the programming languages used, server softwares used, plugins used (like facebook plugin, tweet plugin, etc.) and much more.

*68% students get this answer correct at their*

Q6/6

Searching for subdomains is helpful to malicious hackers as server admins don’t pay attention to sub domain logs. Is it true or false?

A True

B False

Well done. Correct Answer.

**Explanation:**
All domains are equally monitored. It’s just that developers sometimes assume that if they don’t talk about it on the main website, they don’t need to put too much security on it as no one will visit it. Moreover, it increases the scope for hackers and gives them a new endpoint to break in from.

Now that we have come to the end of this topic, you should be able to:

1. Gather targeted information about an organisation or a person using the basic information acquired earlier
2. Use social media, yellow pages and other listing services to gather detailed information about the target

If you have doubts regarding any of the above mentioned points, please go through the relevant videos and text chapters again.