**Task 1: Finding Vulnerabilities**

Let us start our exercise by performing an advanced search. The following command is proposed:

*intitle:"index of" /etc/shadow*

1. Explain in detail what is the objective of this search. What does the operator do? What is the purpose of the string “index of”? Why is the objective of the parameter etc/shadow? Is there any malicious purpose by executing this dork?

Basically, the objective of this search is to find exposed shadow files on the internet. The keyword “intitle” searches for the user given string in HTML page titles, while the string “index of” is a common string shown by http servers when listing files.

*/etc/shadow* → File that stores linux system user passwords (hashed).

For obvious reasons, shadow files are a clear objective because they store user password hashes, which can later be used to gain unauthorized access to a system. This google dork has indeed a malicious purpose.

1. Run the command in Google Search bar, and take a look to the search results. Explain what you can see.

We can see a huge number of domains that have an exposed /etc/shadow file, containing real password hashes.

1. Let us focus on the url <https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org>

List the files you can see and describe the type of contents that you can find in “passwd” and “shadow” files

# **Index of /etc/shrishikshayatancollege.org**

|  | [**Name**](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/?C=N;O=D) | [**Last modified**](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/?C=M;O=A) | [**Size**](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/?C=S;O=A) | [**Description**](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/?C=D;O=A) |
| --- | --- | --- | --- | --- |
|  | | | | |
|  | [Parent Directory](https://shrishikshayatancollege.org/etc/) |  | - |  |
|  | [@pwcache/](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/@pwcache/) | 2017-08-28 14:07 | - |  |
|  | [\_privs.json](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/_privs.json) | 2017-07-25 11:15 | 14 |  |
|  | [passwd](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/passwd) | 2018-02-22 17:23 | 956 |  |
|  | [placementcell/](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/placementcell/) | 2017-08-25 15:17 | - |  |
|  | [quota](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/quota) | 2018-02-22 17:23 | 15 |  |
|  | [shadow](https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org/shadow) | 2018-02-22 17:23 | 1.1K |  |
|  | | | | |

In the passwd file we can find user account information. Each line in the file represents a user, with fields separated by **(:)**.

The different fields are:

* Username: user’s login name
* Password: ‘x’ indicates that the password is in /etc/shadow encrypted.
* User ID: unique number that identifies the user.
* Group ID: the identifier of the group the user belongs to.
* User info: here we can find information like user’s name, phone number …
* Home directory: the path to the user’s home directory.
* Shell: the default shell for the user

In the shadow file we can find encrypted password information and other security-related details for each user. It is only accessible by the root user.   
  
The fields are:

* Username: user’s login name.
* Encrypted password: hashed password.
* Last password change: the number of days since the password was last changed.
* Minimum password age: the minimum number of days that must pass before the user can change the password again.
* Maximum password age: the maximum number of days a password can be used before it must be changed.
* Password warning period: the number of days before the password expires that the user will start receiving warnings.
* Password inactivity period: the number of days after the password has expired that the account becomes disabled.
* Account expiration date: the number of days when the account will be disabled.

1. Let us get some additional information about the main site <https://shrishikshayatancollege.org>

Using the aforementioned tools, provide the following information:

* 1. Registrant contact information → *$ whois shrishikshayatancollege.org*

Organization: Shri Shikshayatan College

State: West Bengal

Country: IN

* 1. IP address of the domain → *$ nslookup shrishikshayatancollege.org*

Name: shrishikshayatancollege.org

IPv4: 178.79.159.193

IPv6: 2a01:7e00::f03c:91ff:fe2f:736e

* 1. Internet service provider → *From shodan.io*

Akamai Connected Cloud

* 1. Cloud service provider → *From shodan.io*

Linode

* 1. Open ports → *From shodan.io*

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 21 | tcp | ftp - Pure-FTPd |
| 22 | tcp | ssh - OpenSSH |
| 53 | tcp / udp | (?) dns |
| 80 | tcp | httpd - Apache |
| 110 | tcp | (?) imap - Dovecot |
| 143 | tcp | (?) imapv4 - Dovecot |
| 443 | tcp | httpd - Apache |
| 465 | tcp | smtpd - Exim |
| 587 | tcp | smtpd - Exim |
| 993 | tcp | (?) imapv4 - Dovecot |
| 995 | tcp | (?) imap - Dovecot |
| 2077 | tcp | (?) |
| 2082 | tcp | (?) |
| 2083 | tcp | (?) |
| 2086 | tcp | (?) |
| 2087 | tcp | (?) |
| 2096 | tcp | (?) |

* 1. Web Technologies → *From shodan.io and Wappalyzer extension*

As seen in the previous table, the server is running multiple services, such as FTP, SSH, some mail services and the HTTP server running Apache. The main web technologies used are WordPress, PHP, jQuery javascript libraries and a MySQL database.

| **Blogs** | WordPress |
| --- | --- |
| **CMS** | WordPress |
| **Databases** | MySQL |
| **Ecommerce** | Abicart |
| **Form builders** | Contact Form 7 |
| **JavaScript libraries** | jQuery, jQuery Migrate 1.4.1, prettyPhoto |
| **Photo galleries** | Slider Revolution 5.2.6 |
| **Programming languages** | PHP |
| **Widgets** | Slider Revolution 5.2.6 |
| **WordPress plugins** | Contact Form 7 |
| **WordPress themes** | BeTheme 15.5 |

1. Now, think as a black hat, and describe (not perform):
   1. A vulnerability/weakness you detected

CVE-2023-51385, a vulnerability in OpenSSH versions prior to 9.6 that relates to OS command injection. (extracted from shodan.io).

A different one, is the public shadow file that they have.

* 1. Potential actions to exploit such vulnerability. You can propose using additional tools and making assumptions for those aspects that you cannot know with the obtained information.

In OpenSSH, usernames can be referenced in command-line operations. If a username or hostname includes shell metacharacters (;, &, |, >, <,...), these characters can be used to manipulate the shell command that gets executed. A Git repository could have a submodule with a username that includes special characters. For instance, a username like rm -rf / is a problem for the institution. This vulnerability has a 6.5 score out of 10 (explanation of this score explained in task 2).

For the second one, as we have seen in this session, we can log in to an open ssh port with the password that is in the shadow file of Index of /etc/shrishikshayatancollege.org.

1. Come back to point 2), and select another different domain. Repeat points 4) and 5); if possible, select a different vulnerability and/or potential actions to perform.

Searching Index of etc/shadow in google, we find that the website https://hksargegu.org.hk/ has the shadow file public, so let’s focus on that one.

6.4)

* 1. Registrant contact information → *$ whois hksargegu.org.hk*

Company name: HKSAR GOVERNMENT EMPLOYEES GENERAL UNION

Address: 5/F, CHEUNG SHING BUILDING, 1 CHEUNG SHA WAN ROAD KOWLOON

Country: Hong Kong (HK)

* 1. IP address of the domain → *$ nslookup hksargegu.org.hk*

Name: hksargegu.org.hk

IPv4: 103.38.163.22

* 1. Internet service provider → *From shodan.io*

Speedy Group Cloud Limited

* 1. Cloud service provider

Not shown on shodan.io.

* 1. Open ports → *From shodan.io*

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 21 | tcp | ftp - Pure-FTPd |
| 25 | tcp | smtpd - Exim |
| 53 | tcp / udp | (?) dns |
| 80 | tcp | httpd - Apache |
| 110 | tcp | (?) |
| 143 | tcp | (?) imapv4 - Dovecot |
| 443 | tcp | httpd - Apache |
| 465 | tcp | smtpd - Exim |
| 587 | tcp | smtpd - Exim |
| 993 | tcp | (?) imapv4 |
| 995 | tcp | (?) imap - Dovecot |
| 1025 | tcp | smtpd - Exim |
| 2082 | tcp | (?) |
| 2083 | tcp | (?) |
| 4949 | (?) | (?) |

* 1. Web Technologies → *From shodan.io*

| **JavaScript Libraries** | jQuery (18.3), jQuery UI |
| --- | --- |
| **UI Frameworks** | Bootstrap |

6.5)

1. A vulnerability/weakness you detected

The same as in the previous point, the public shadow file.

We also are looking for another one, which will be the CVE-2024-4577 vulnerability, taken from shodan.io.

1. Potential actions to exploit such vulnerability. You can propose using additional tools and making assumptions for those aspects that you cannot know with the obtained information.

Focusing on CVE-2024-4577, in some PHP versions, Windows may replace characters given to certain API. PHP may misinterpret those characters as PHP functions, so malicious code could be executed. This vulnerability has a 9.8 score (we will see below that is a critical vulnerability).

Task 2

Task 2: Exploiting a CVE

For this task we focus on a CVE clearly identified (CVE-2021-42013):

<https://nvd.nist.gov/vuln/detail/CVE-2021-42013>

1. Explain in your words, your understanding on this vulnerability.

An update made it possible for attackers to map files with urls, and since the files had permissions allowed, they could be accessed easily, as well as execute code remotely.

1. The vulnerability has a CVSS Score of 9.8. Explain what this value means and decode the CVSS Vector associated.

A vulnerability of 9.8 indicates that it has a large security breach. The score ranges from 0 (low) to 10 (very high), with 9.8 being a high value that tells us that the breach is easy to break and that we are exposed to data stealing. The CVSS vector is CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, which means:

**CVSS:3.1**- CVSS version.

**AV (Attack Vector): N (Network)**- the attack can be done through the network, not mandatory to be physically in the place.

**AC (Attack Complexity): L (Low)**- the attack is easy to execute.

**PR (Privileges Required): N (None)**- no privileges are required.

**UI (User Interaction): N (None)**- no interactions are needed, so the attack can be done automatically (without anyone clicking a link, for example).

**S (Scope): U (Unchanged)**- it only attacks the system that has that vulnerability.

**C (Confidentiality): H (High)**- the attack exposes a lot of confidential data.

**I (Integrity): H (High)**- the integrity of the system is also very exposed, meaning that the attacker can erase information.

**A (Availability): H (High)**- the availability of the system is exposed, meaning that the system can be shut down easily.

1. Search in exploit-db one identified exploit of this vulnerability. Briefly explain how the exploit works (do not execute any code)

We have found this exploit: Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE).  
  
The exploit works by taking advantage of a path traversal and remote code execution vulnerability in Apache HTTP Server 2.4.50. It allows the attacker to bypass security restrictions and have access to files outside the web root directory or execute commands on the server.

This is possible because of the improper URL validation, which lets the attacker use encoded sequences to navigate through the directory structure. The script sends a specially crafted HTTP request with these encoded characters, gaining access to sensitive files like /etc/passwd explained previously or allowing to execute system commands. This could give the attacker the possibility to control the server or to expose important information.

1. Which tool will you use (and how) to list the servers that are affected by this vulnerability? Write the results

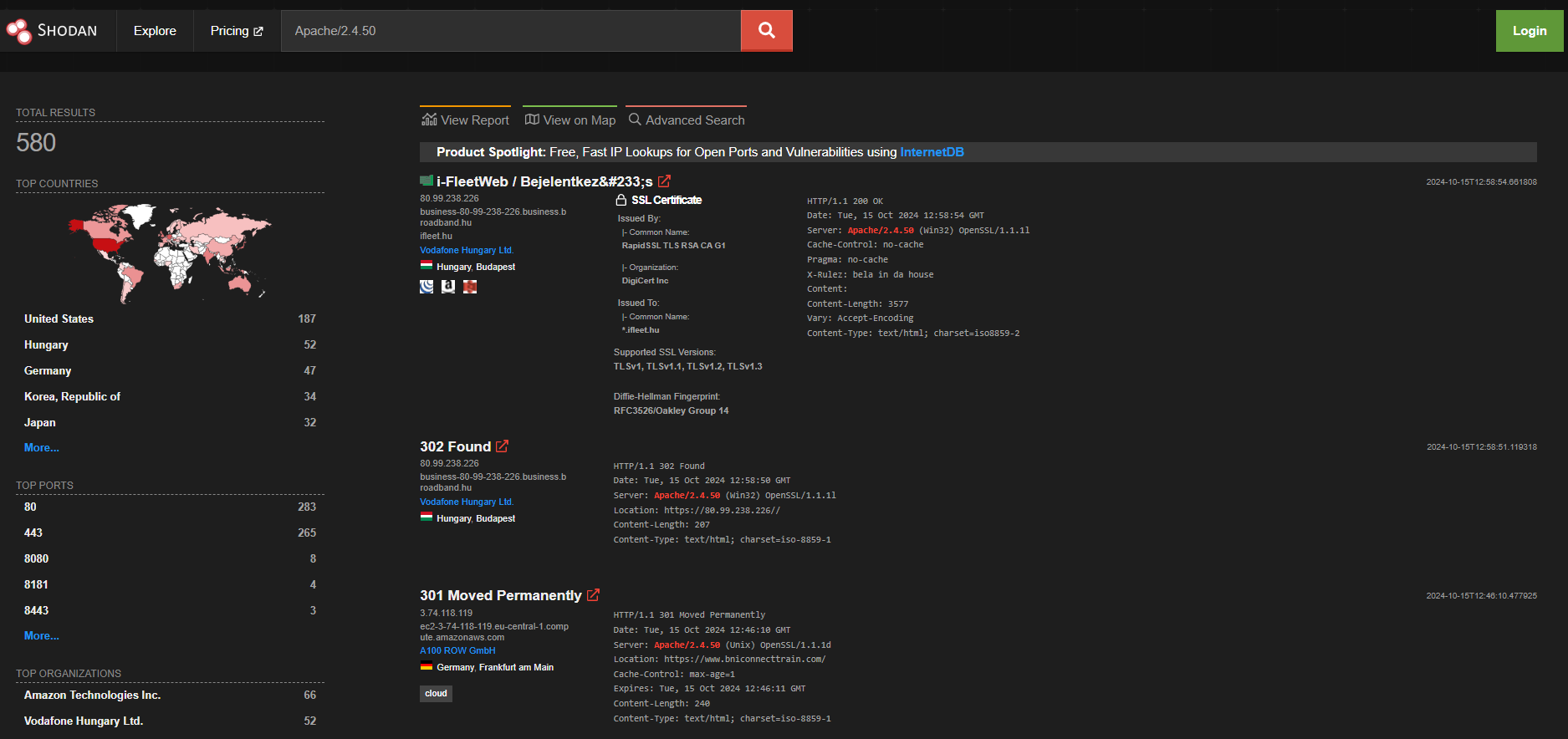
We could use a google dork to find the servers affected by this vulnerability.   
  
If we search: *"Index of" "Apache/2.4.50*(or 49)*"* we can find all the servers that use this affected version of Apache.  
Then, we select some examples and translate the addresses in nslookup. Some servers affected:  
  
128.97.102.135 - physics.ucla.edu

62.68.75.83 - noobzcheatz.de

134.157.176.20 - distrib-coffee

We can also see the servers affected by this vulnerability through **shodan.io.**

On Shodan.io, not only we can search by IP addresses but also by specific text, like software versions, open ports, or other details. For example, if we want to find the servers running Apache version 2.4.50/49 (the ones affected by the vulnerability), we could search: Apache/2.4.50 and obtain the following info:



80.99.238.226 - i-FleetWeb

3.74.118.119

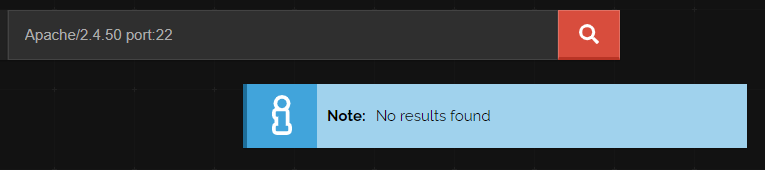
3.124.101.245

35.76.234.47 - SBI Africa

18.168.232.3 - SnapDBA

1. Is there any public site affected by the vulnerability that is exposing port 22 (ssh)?

To find out, we need to create a Shodan account. This will allow us to add filters to our searches. In this case, we would add port:22.



We can see that there are no servers exposing port 22. (Also for Apache/2.4.49).

1. Is it good practice to include the web server product and version within the Header “Server” in our server responses? Justify your answer.

It’s not a good practice to include the web server product and version within the Server header of server responses. The reason for this is that revealing this information can make it easier for attackers to identify specific vulnerabilities that affect that version of the software. A good example is what we’ve seen in this report.

By hiding this information, we reduce the risk of targeted attacks based on known specific vulnerabilities

Task 3

For this task we will give information about WHOIS and Reverse WHOIS.

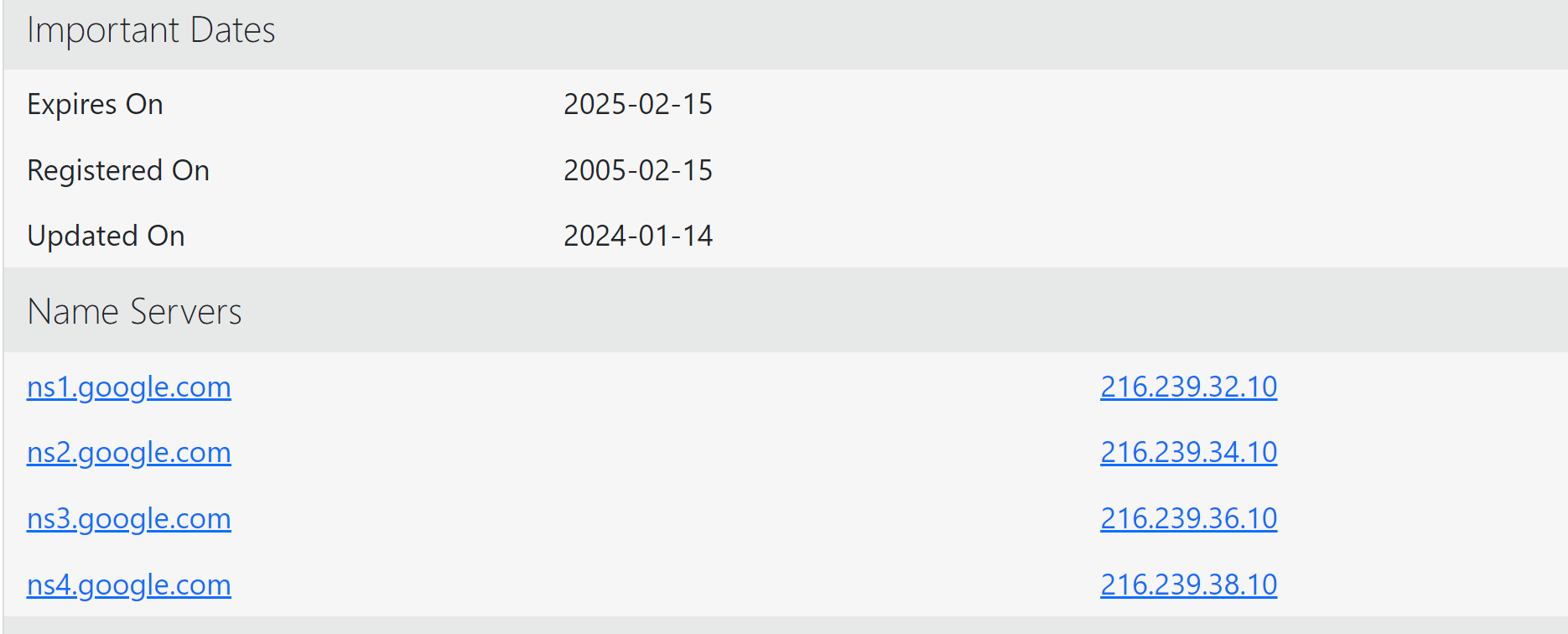
1. What does the tool do, how does it work and some examples:

**WHOIS** is a protocol used to look up information about a domain name or IP address. It helps in identifying domain ownership, facilitating contact, supporting cybersecurity, and handling legal disputes.

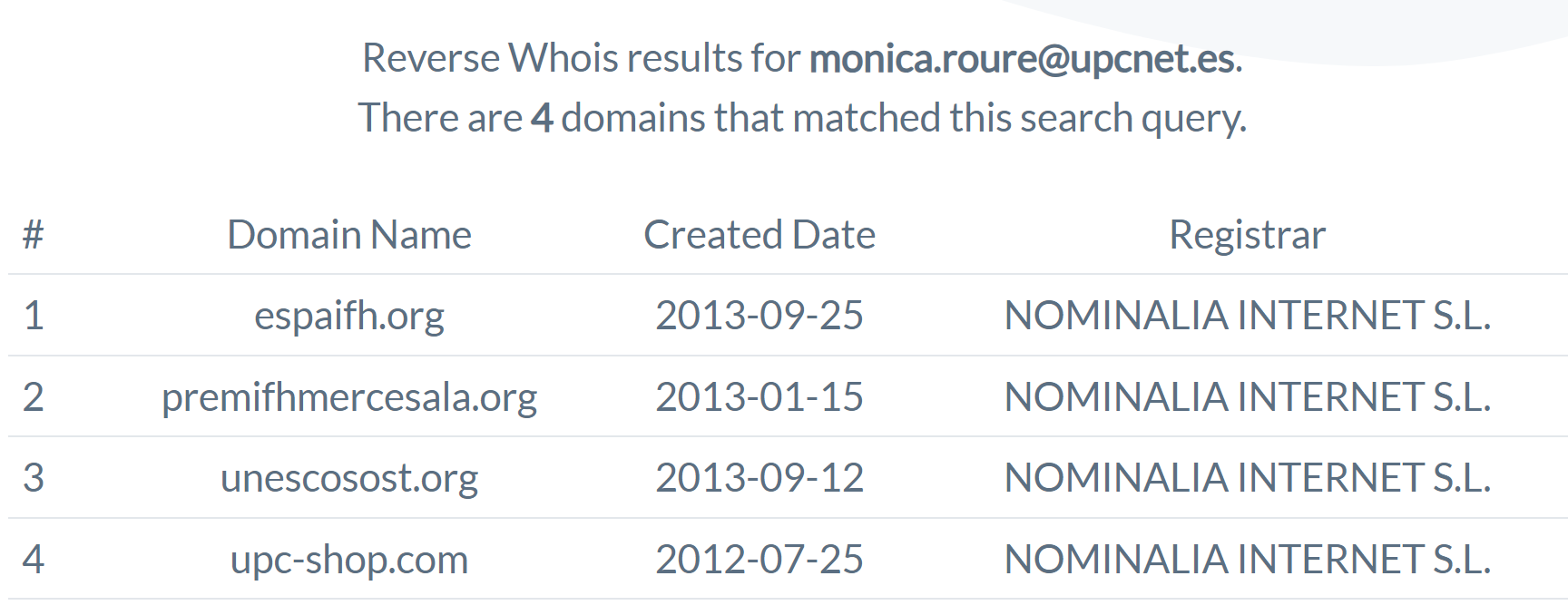
WHOIS data is often accessible via web-based tools or command-line queries, though privacy laws and services may obscure some details.

Information about domain upc.edu domain

Information about youtube.com



**Reverse WHOIS** allows users to search for all domains associated with specific registrant details (like an email or name)



1. Benefits the tool has for a white hat:

Threat detection: The tool can help in detecting threats such as malicious domains linked to phishing, social engineering or other cyberattacks by revealing the domain’s registrant details.

Tracking cybercriminals: WHOIS can be used to trace the origin of an attack.

Vulnerability analysis: Checking the registration and expiration dates of domains helps ensure that critical domains are not left vulnerable

Identification of domain Networks: Reverse WHOIS can uncover all domains

associated with a particular registrant, helping white hats track down a network of malicious domains operated by a threat actor.

Tracking domain movements: Reverse WHOIS allows white hats to monitor when cybercriminals shift their operations to new domains, enabling proactive defenses against emerging threats.

1. Can a black hat take advantage of the tool?

Yes, they can take advantage of the tool in different ways:

Gathering personal information and launching phishing attacks: Black hats can use WHOIS to obtain sensitive details about domain owners, such as names, email addresses, phone numbers, and physical addresses. This can aid in social engineering attacks, phishing, or identity theft.

FInding vulnerable domains: Black hats can look for domains that are about to expire or have outdated contact information, potentially exploiting them for takeovers or using them as a part of spam or malware campaigns.

Finding associated domains to one owner: By identifying multiple domains owned by a single entity, attackers can target less-secure domains in a company's portfolio to gain a foothold in their infrastructure or impersonate the brand for malicious purposes.

1. Which features and functionalities of the tool have we explored during the task?

We’ve used the tool to gather information about <https://shrishikshayatancollege.org/> such as the Registrant contact information.

