

Module 18: IoT and OT Hacking

Lab 1: Perform Footprinting using Various Footprinting Techniques

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target IoT and OT devices by performing footprinting through search engines, advanced Google hacking, Whois lookup, etc.

The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Lab Objectives

- Gather information using online footprinting tools

Overview of Footprinting Techniques

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

Task 1: Gather Information using Online Footprinting Tools

The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

You can also select a protocol or device of your choice to perform footprinting on it.

1. ☐ By default **Windows 11** machine selected, click [Ctrl+Alt+Delete](#).

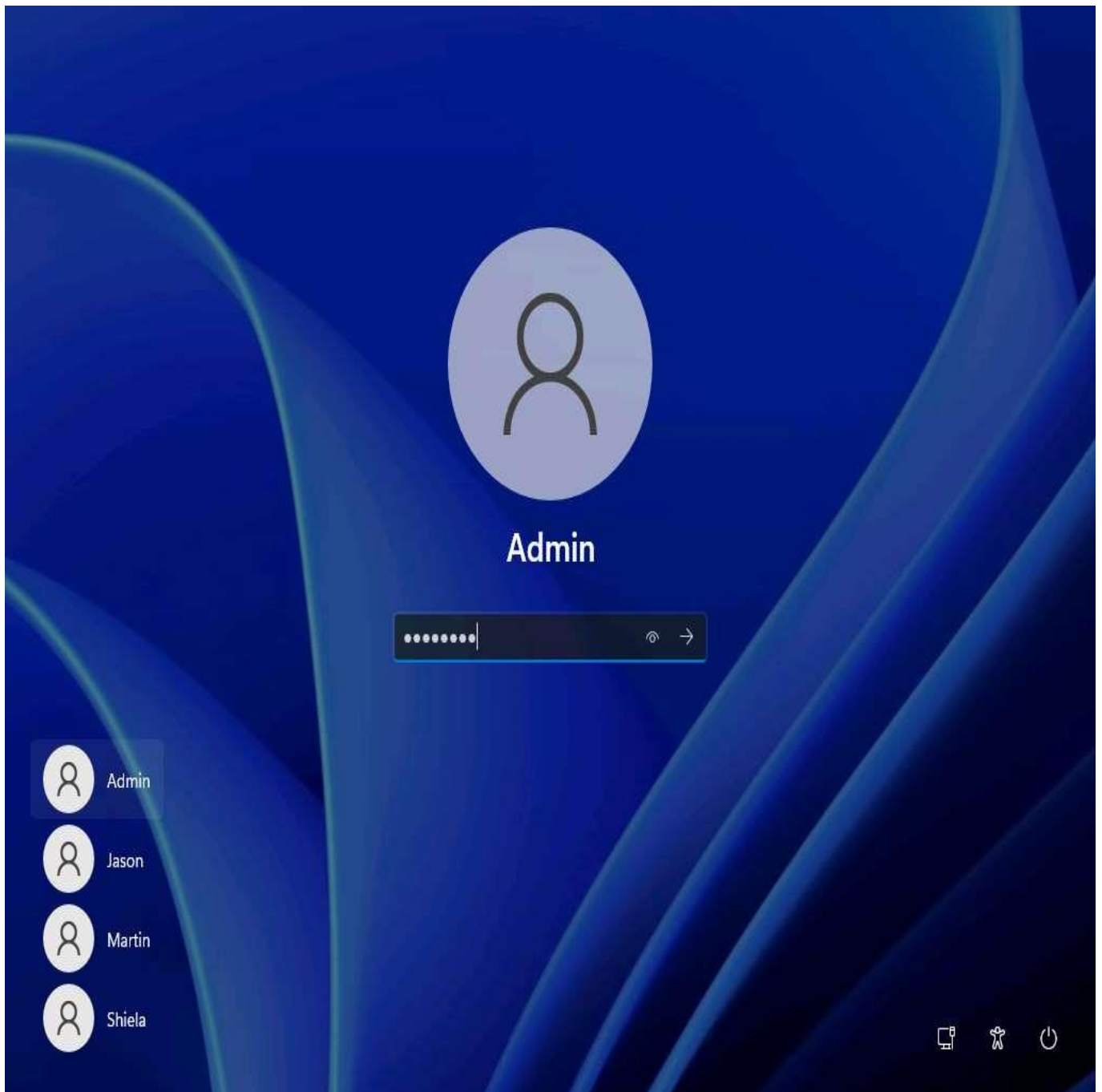
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

2. ☐ By default, **Admin** user profile is selected, click **Pa\$\$w0rd** to paste the password in the **Password** field and press **Enter** to login.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under **Commands** (**thunder** icon) menu.

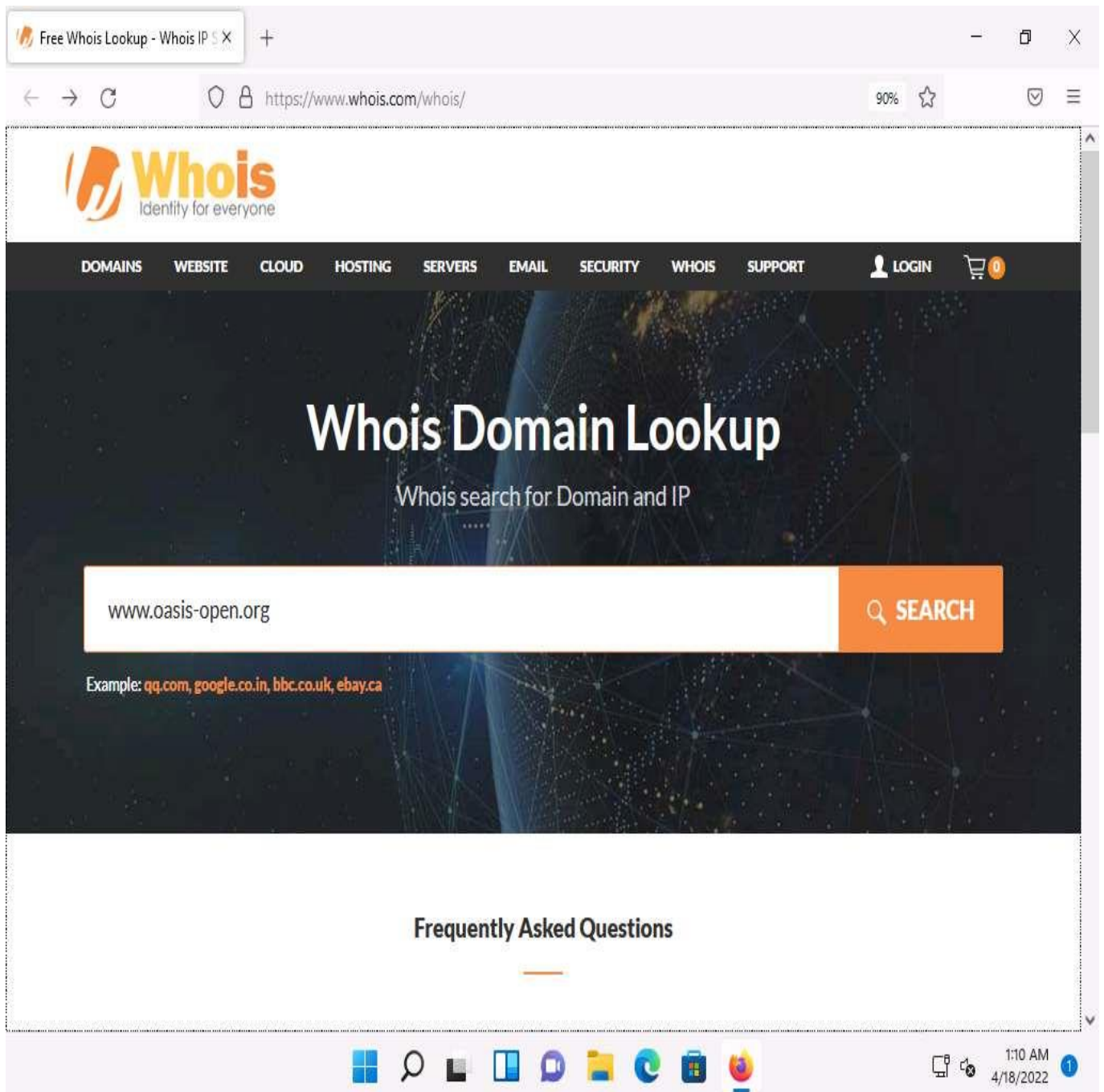
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



3. ☐ Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **<https://www.whois.com/whois/>** and press **Enter**.
4. ☐ The **Whois Domain Lookup** page appears; type **www.oasis-open.org** in the search field and click **SEARCH**.

Oasis is an organization that has published the MQTT v5.0 standard, which represents a significant leap in the refinement and capability of the messaging protocol that already powers IoT.



5. ☐ The result appears, displaying the following information, as shown in the screenshots: Domain Information, Registrant Contact, and Raw Whois Data.

This information is about the organization that has developed the MQTT protocol, and it might help keep track of the modifications and version changes of the target protocol.

Whois oasis-open.org

+

← → ↻


https://www.whois.com/whois/oasis-open.org

90%

☆

🔒

☰

Identity for everyone

Enter Domain or IP

WHOIS

DOMAINSWEBSITECLOUDHOSTINGSERVERSEMAILSECURITYWHOISSUPPORTLOGIN0

oasis-open.org

Updated 6 days ago

Domain Information

Domain:

oasis-open.org

Registrar:

DNC Holdings, Inc.

Registered On:

1998-03-04

Expires On:

2023-03-03

Updated On:

2022-01-17

Status:

clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited

Name Servers:

dns2.stabletransit.com
dns1.stabletransit.com

Registrant Contact

Organization:

OASIS Open

State:

MA

Interested in similar domains?

oasis-open.com

Buy Now

littleoasisopen.com

Buy Now

oasisopenhouse.com

Buy Now

oasisthird.com

Buy Now

oasisdream.net

Buy Now

oasisguest.net

Buy Now

Sale

.space

\$24.88 \$0.88



1:11 AM
4/18/2022

1

Whois oasis-open.org

https://www.whois.com/whois/oasis-open.org

State: MA
Country: US

Raw Whois Data

```
Domain Name: OASIS-OPEN.ORG
Registry Domain ID: D1849375-LROR
Registrar WHOIS Server: whois.directnic.com
Registrar URL: http://www.directnic.com
Updated Date: 2022-01-17T07:40:27Z
Creation Date: 1998-03-04T05:00:00Z
Registry Expiry Date: 2023-03-03T05:00:00Z
Registrar Registration Expiration Date:
Registrar: DNC Holdings, Inc.
Registrar IANA ID: 291
Registrar Abuse Contact Email: abuse@directnic.com
Registrar Abuse Contact Phone: +1.8778569598
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: OASIS Open
Registrant State/Province: MA
Registrant Country: US
Name Server: DNS2.STABLETRANSIT.COM
Name Server: DNS1.STABLETRANSIT.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/whois-inaccuracy-form/
>>> Last update of WHOIS database: 2022-04-11T16:29:49Z <<<

For more information on Whois status codes, please visit https://icann.org/whois-status-codes/

Access to Public Interest Registry WHOIS information is provided to assist you in your research of public interest.

The Registrar of Record identified in this output may have an RDNS server.
```

On Sale!

.TOP

.TOP @ \$1.88 \$9.88

Introducing

WORDPRESS HOSTING

\$3.58 /mo

VIEW MORE

https://shop.whois.com/optimized-wordpress-hosting.php

11:14 AM 4/18/2022

Whois lookup reveals available information on a hostname, IP address, or domain.

6. ☐ Now, open a new tab, and type **https://www.exploit-db.com/google-hacking-database** in the address bar, and press **Enter**.
7. ☐ The **Google Hacking Database** page appears; type **SCADA** in the **Quick Search** field and press **Enter**.
8. ☐ The result appears, which displays the Google dork related to SCADA, as shown in the screenshot.

The screenshot shows the Google Hacking Database (GHD) interface. The search term 'SCADA' is entered in the 'Quick Search' field. The results table shows 6 entries, with the first six rows highlighted by a red box. The table columns are Date Added, Dork, Category, and Author.

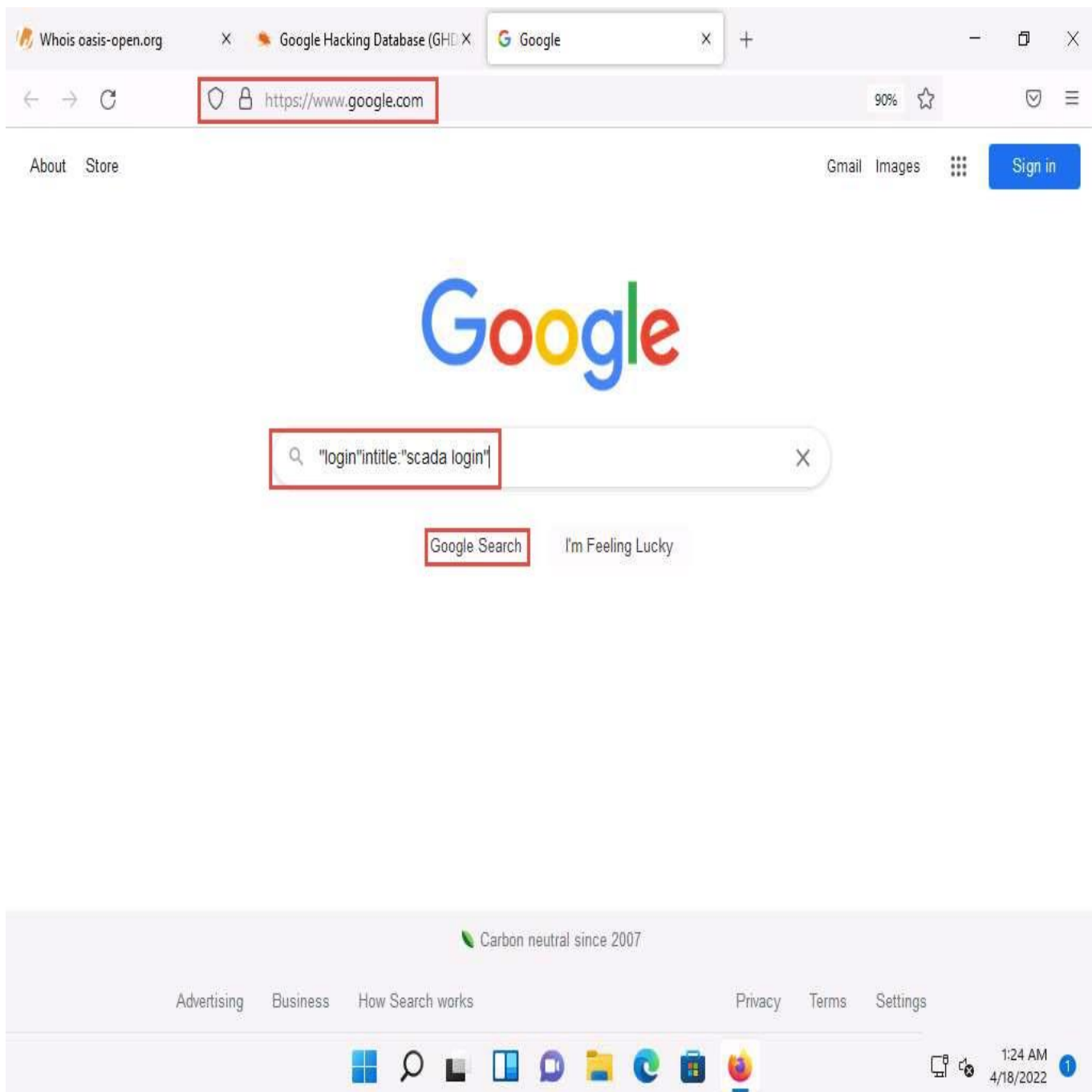
Date Added	Dork	Category	Author
2021-10-04	intitle:"index of SCADA"	Sensitive Directories	Romell Marin Cordoba
2021-09-20	intitle:inurl:"SCADA login"	Pages Containing Login Portals	Cyber Shelby
2021-09-16	intitle:"CirCarLife Scada" inurl:/html/index.html	Various Online Devices	Alexandros Pappas
2020-05-28	"login" intitle:"*scada login"	Pages Containing Login Portals	Alexandros Pappas
2019-04-22	intitle:"index of" scada	Sensitive Directories	Aman Bhardwaj
2018-04-06	"login" intitle:"scada login"	Pages Containing Login Portals	Bruno Schmid

Showing 1 to 6 of 6 entries (filtered from 7,341 total entries)

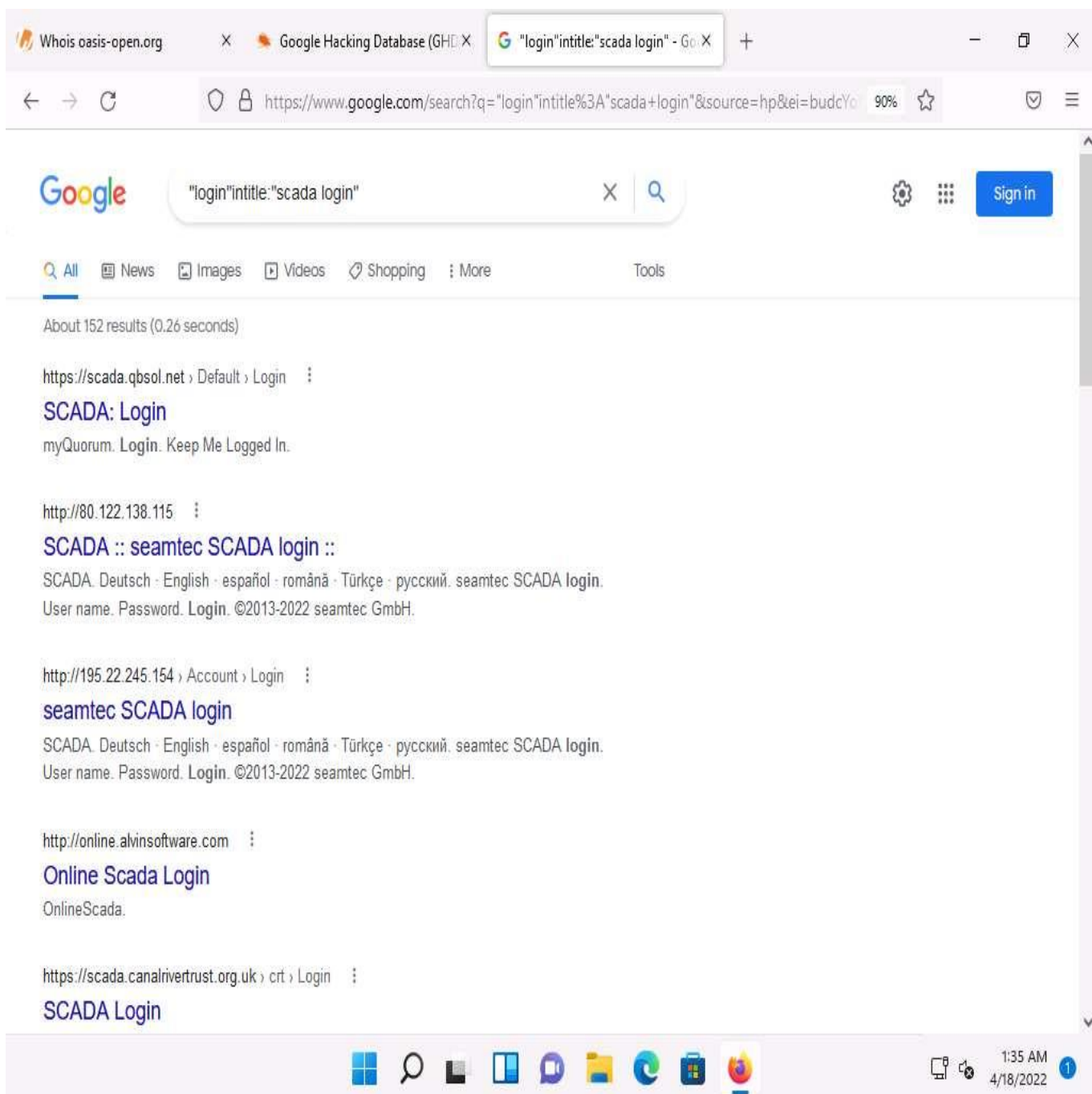
Navigation links: FIRST, PREVIOUS, 1, NEXT, LAST

Footer sections: Downloads (Kali Linux, Kali NetHunter), Certifications (OSCP, OSWP), Training (Penetration Testing with Kali Linux (PWK) (PEN-200), Offensive Security Wireless Attacks (WiFu) (PEN-210)), Professional Services (Penetration Testing, Advanced Attack Simulation).

9. ☐ Now, we will use the dorks obtained in the previous step to query results in Google.
10. ☐ Open a new tab and type **https://www.google.com** in the address bar, and press **Enter**.
11. ☐ In the search field, type **"login" intitle:"scada login"** and click the **Google Search** button.



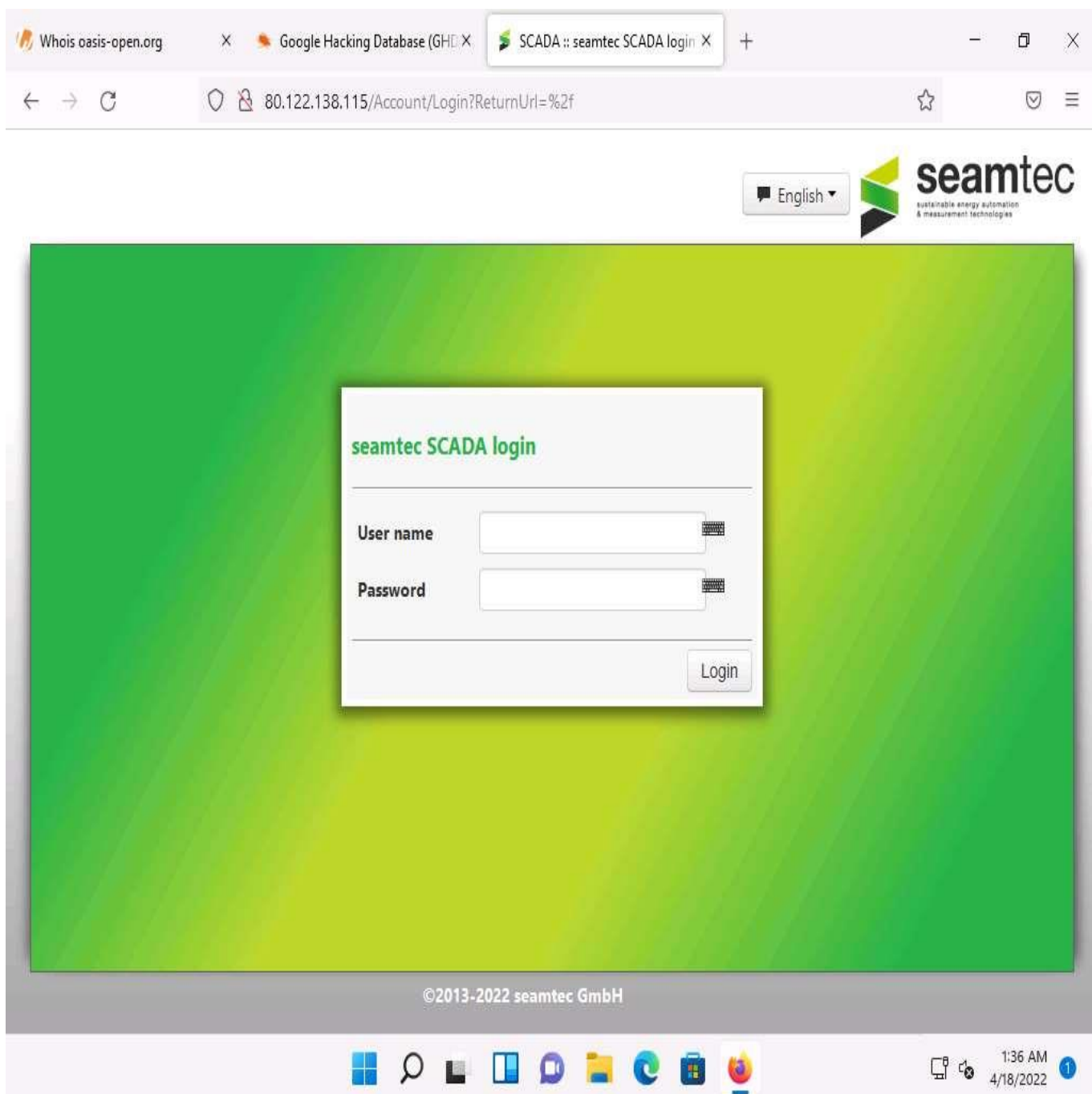
12. ☐ The search result appears; click any link (here, **SCADA :: seamtec SCADA login ::**).



Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results.

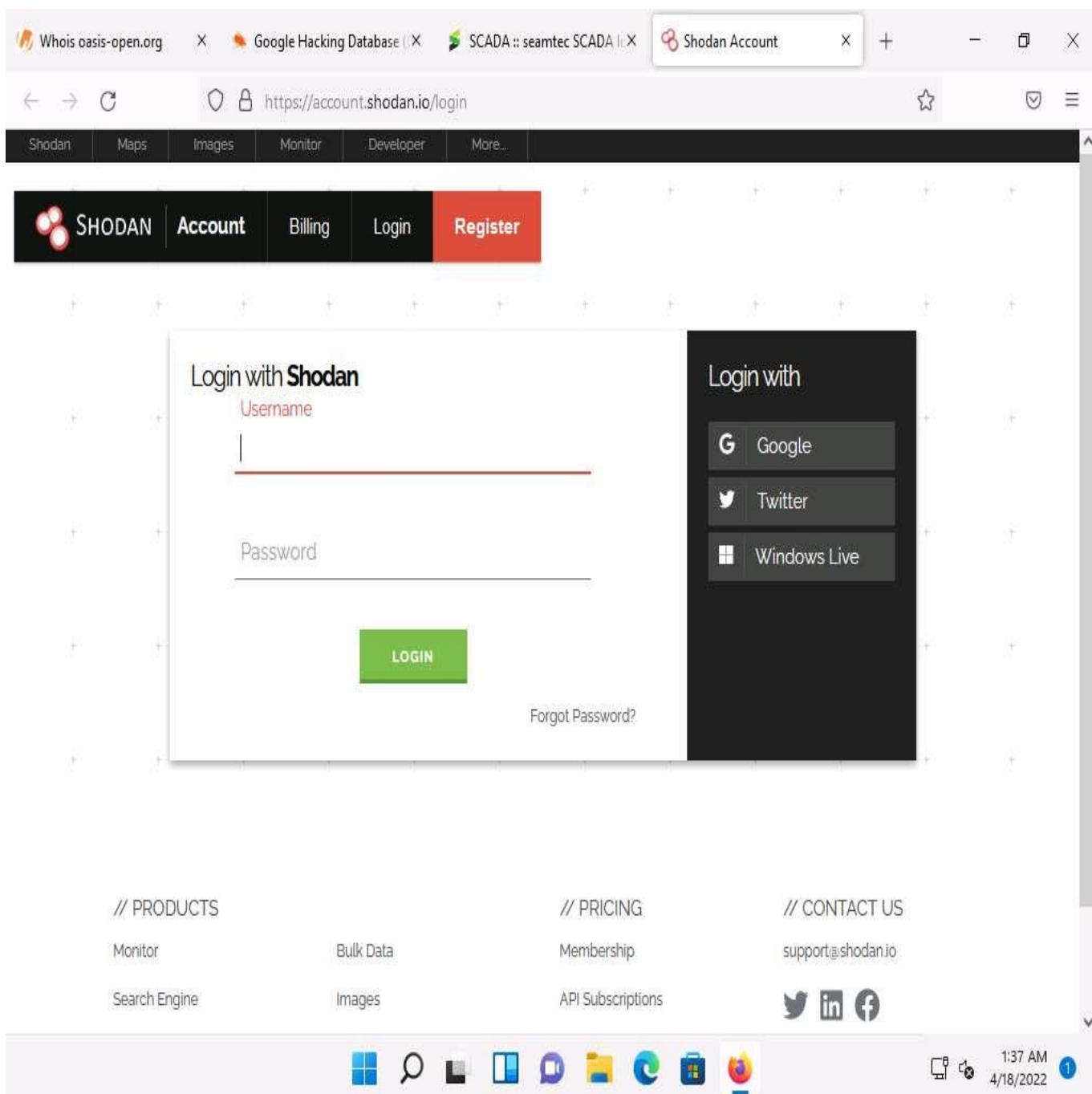
13. ☐ The **seamtec SCADA login** page appears, as shown in the screenshot.

In the login form, you can brute-force the credentials to gain access to the target SCADA system.



14. ☐ Similarly, you can use advanced search operators such as **intitle:"index of" scada** to search sensitive SCADA directories that are exposed on sites.
15. ☐ Now, in the browser window, open a new tab type **https://account.shodan.io/login** in the address bar, and press **Enter**.
16. ☐ The **Login with Shodan** page appears; enter your username and password in the **Username** and **Password** fields, respectively; and click **Login**.

Go to the **Register** option to register yourself if you do not have an existing account.

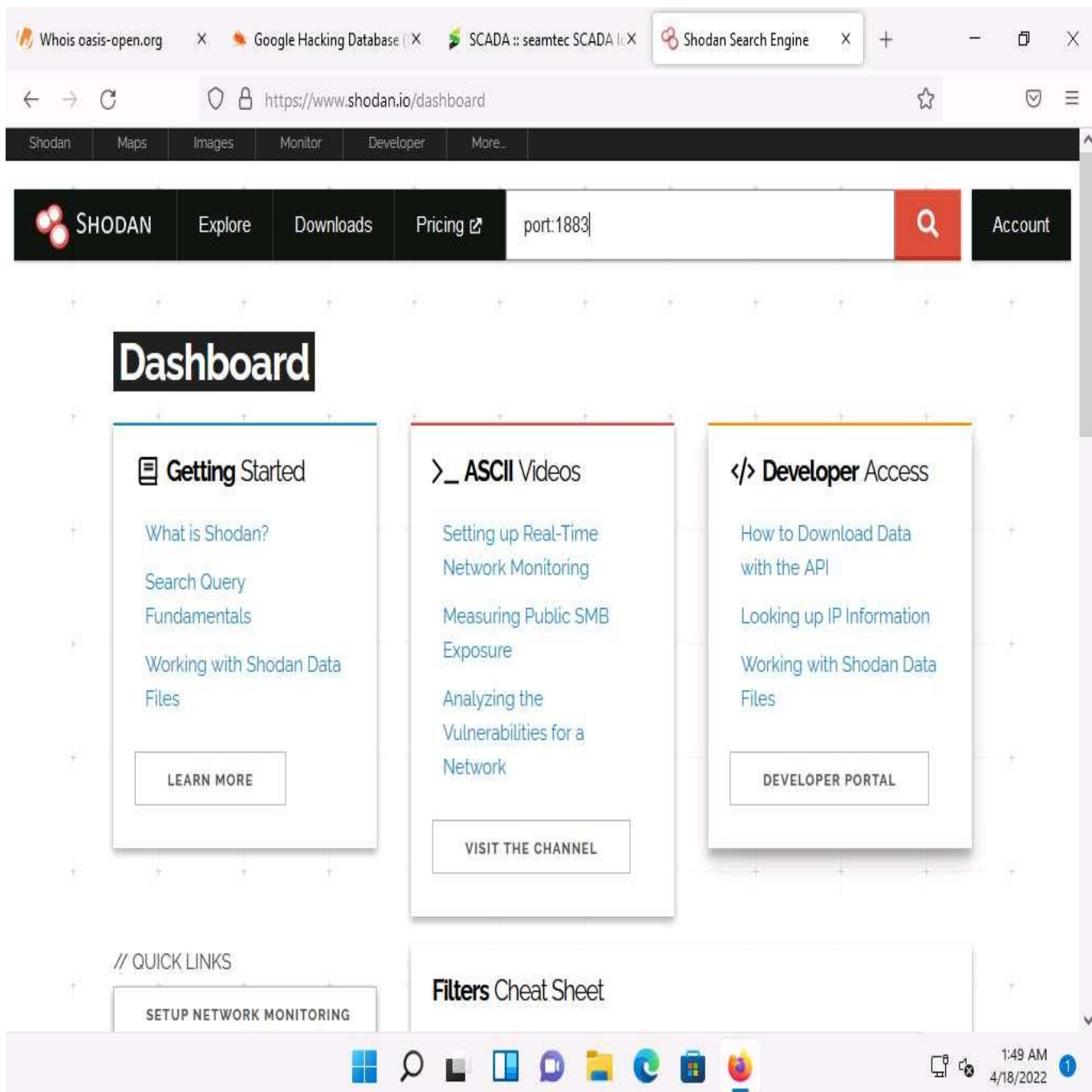


17. ☐ The **Account Overview** page appears, which displays the account-related information.

If the **Would you like Firefox to save this login for shodan.io?** notification appears, click **Don't Save**.

18. ☐ The **Shodan** main page appears; type **port:1883** in the address bar and press **Enter**.

Port 1883 is the default MQTT port; 1883 is defined by IANA as MQTT over TCP.




19. ☐ The result appears, displaying the list of IP addresses having port 1883 enabled, as shown in the screenshot.
20. ☐ Click on any IP address to view its detailed information.

Whois oasis-open.org X Google Hacking Database X SCADA :: seamtec SCADA X port:1883 - Shodan Search X

https://www.shodan.io/search?query=port%3A1883

TOTAL RESULTS
996,760

TOP COUNTRIES



Country	Count
United States	552,702
Korea, Republic of	267,646
China	48,829
Russian Federation	16,658
Japan	15,559

More...

TOP ORGANIZATIONS

Organization	Count
Google LLC	519,142
SK Broadband Co Ltd	259,424
Aliyun Computing Co., LTD	16,150
Open Computer Network	9,264
Amazon Technologies Inc.	7,099

More...

TOP PRODUCTS

Product	Count
MQTT	353,605
Mosquitto	56,818

View Report Browse Images View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

39.121.80.76

SK Broadband Co Ltd

🇰🇷 Korea, Republic of, Daegu

MQTT Connection Code: 0

Topics:

2022-04-18T04:48:41.811959

34.107.253.160

180.253.107.34 bc.go
ogleusercontent.com

Google LLC

🇺🇸 United States, Mountain View

No data returned

2022-04-18T04:48:38.436868

175.125.51.80

SK Broadband Co Ltd

🇰🇷 Korea, Republic of, Seoul

MQTT Connection Code: 0

Topics:

2022-04-18T04:48:38.367617

400 The plain HTTP request was sent to HTTPS port

77.243.119.219

client-119-243-77.irene.ru

Irkutskenergosvyaz

🇷🇺 Russian Federation, Nizhneudinsk

HTTP/1.1 400 Bad Request

Server: nginx

Date: Mon, 18 Apr 2022 04:48:28 GMT

Content-Type: text/html

Content-Length: 650

Connection: close

2022-04-18T04:48:28.905450

218.237.154.2

SK Broadband Co Ltd

🇰🇷 Korea, Republic of, Ansan-si

MQTT Connection Code: 0

Topics:

2022-04-18T04:48:26.678945

21. ☐ Detailed results for the selected IP address appears, displaying information regarding **Ports, Services, Hostnames, ASN**, etc. as shown in the screenshot.

The screenshot shows the Shodan website interface. The browser tabs include 'Whois oasis-open.org', 'Google Hacking Database', and 'SCADA :: seamtec SCADA'. The address bar shows 'https://www.shodan.io/host/34.107.253.160'. The page features a navigation bar with 'SHODAN', 'Explore', 'Downloads', 'Pricing', and a search bar. Below the navigation bar is a map of Mountain View, California. The main content area is divided into two sections: 'General Information' and 'Open Ports'.

General Information

Hostnames	[REDACTED]
Domains	GOOGLEUSERCONTENT.COM
Cloud Provider	Google
Cloud Region	global
Country	United States
City	Mountain View
Organization	Google LLC
ISP	Google LLC
ASN	[REDACTED]

Open Ports

25	43	80	83	84	89	110	143	195
443	485	993	995	1883	1935	3389	5222	5432
5872	5900	5901	6379	8080	8081	8085	8086	8088
8089	8090	8099	9200	9300	11211	20000		

Raw Data

```

// 80 / TCP
623407353 | 2022-04-17T08:41:08.692720

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 277
Date: Sun, 17 Apr 2022 08:41:08 GMT
  
```

22. ☐ Similarly, you can gather additional information on a target device using the following Shodan filters:
- **Search for Modbus-enabled ICS/SCADA systems:**
 - port:502
 - **Search for SCADA systems using PLC name:**
 - "Schneider Electric"
 - **Search for SCADA systems using geolocation:**
 - SCADA Country:"US"
23. ☐ Using Shodan, you can obtain the details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.

24. ☐ This concludes the demonstration of gathering information on a target device using various techniques such as Whois lookup, advanced Google hacking, and Shodan search engine.
25. ☐ Close all open windows and document all the acquired information.