

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.

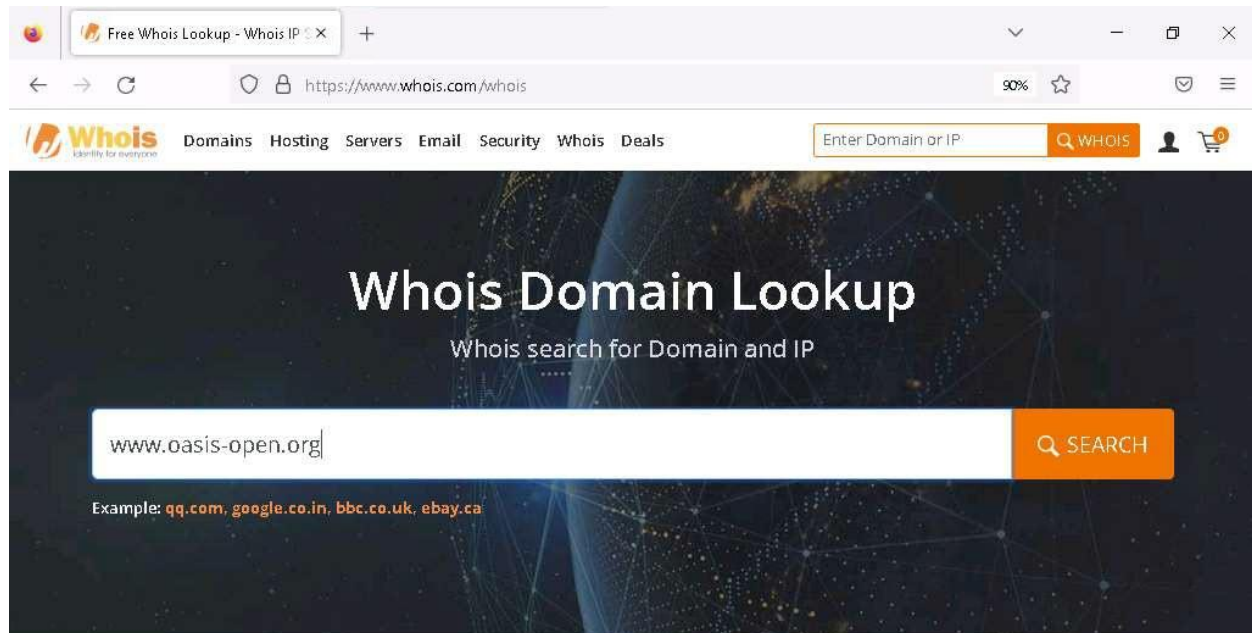
You can also select a protocol or device of your choice to perform footprinting on it.

1. By default **Windows 11** machine selected, click [Ctrl+Alt+Delete](#). Login with **Admin/Pa\$\$w0rd**.

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

2. Launch any web browser, go to <https://www.whois.com/whois> (here, we are using **Mozilla Firefox**).
3. 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.



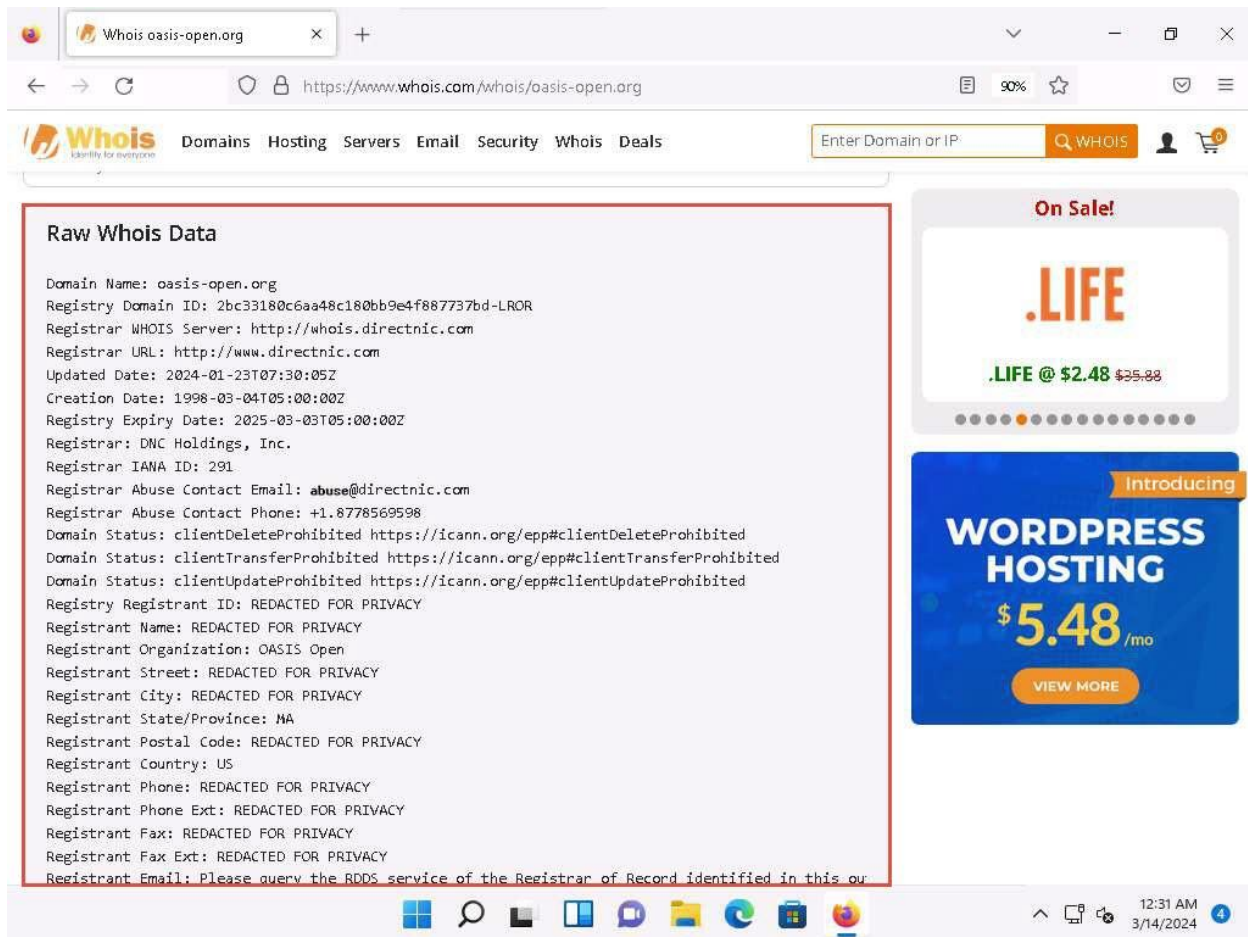
Frequently Asked Questions

+ What is a Whois domain lookup?

File Explorer

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

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

Exploit Database

Google Hacking Database

Filters Reset All

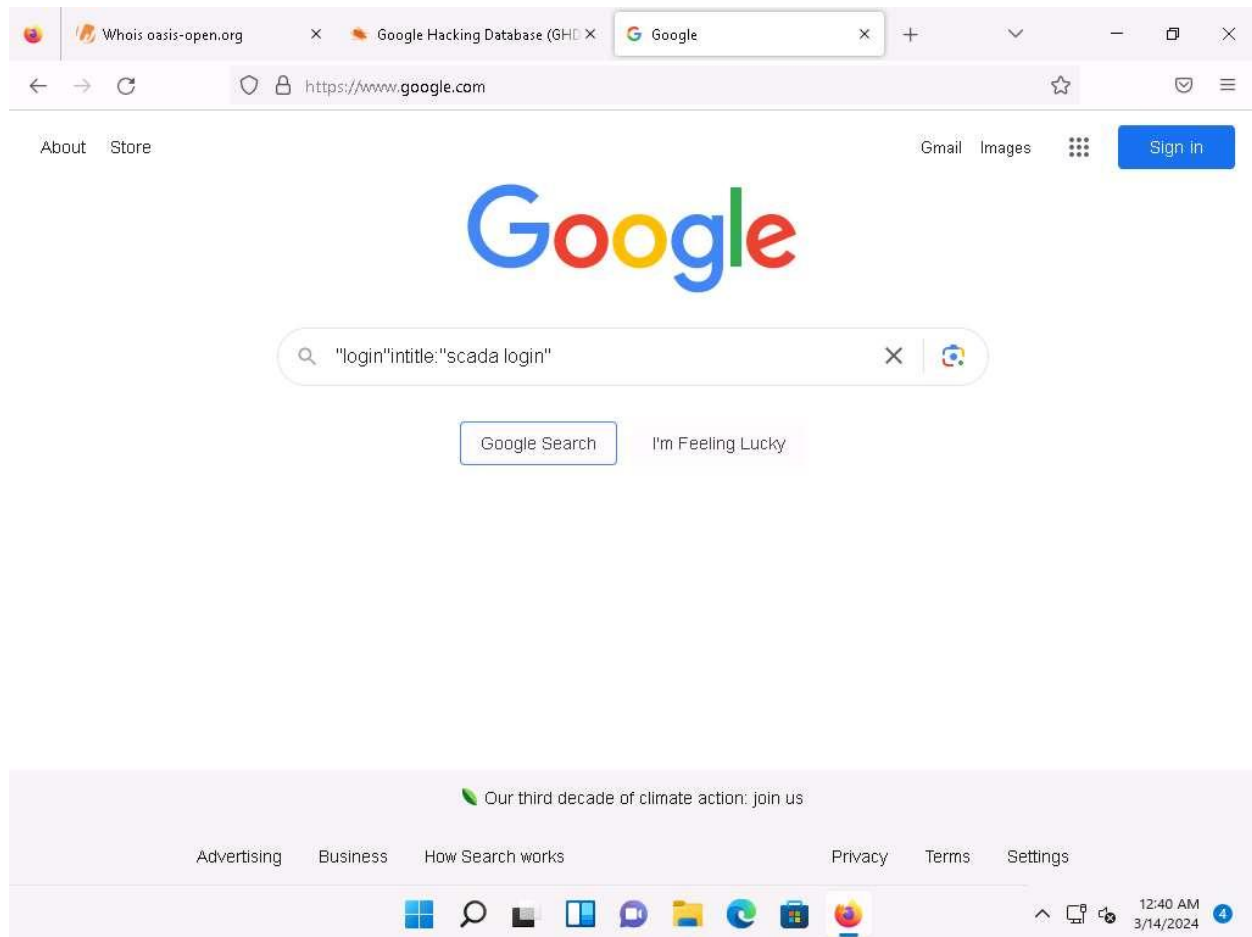
Show 15 Quick Search SCADA

Date Added	Dork	Category	Author
2023-04-06	inurl:"/scada-vis"	Files Containing Juicy Info	Parsa Rezaie Khiabanloo
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

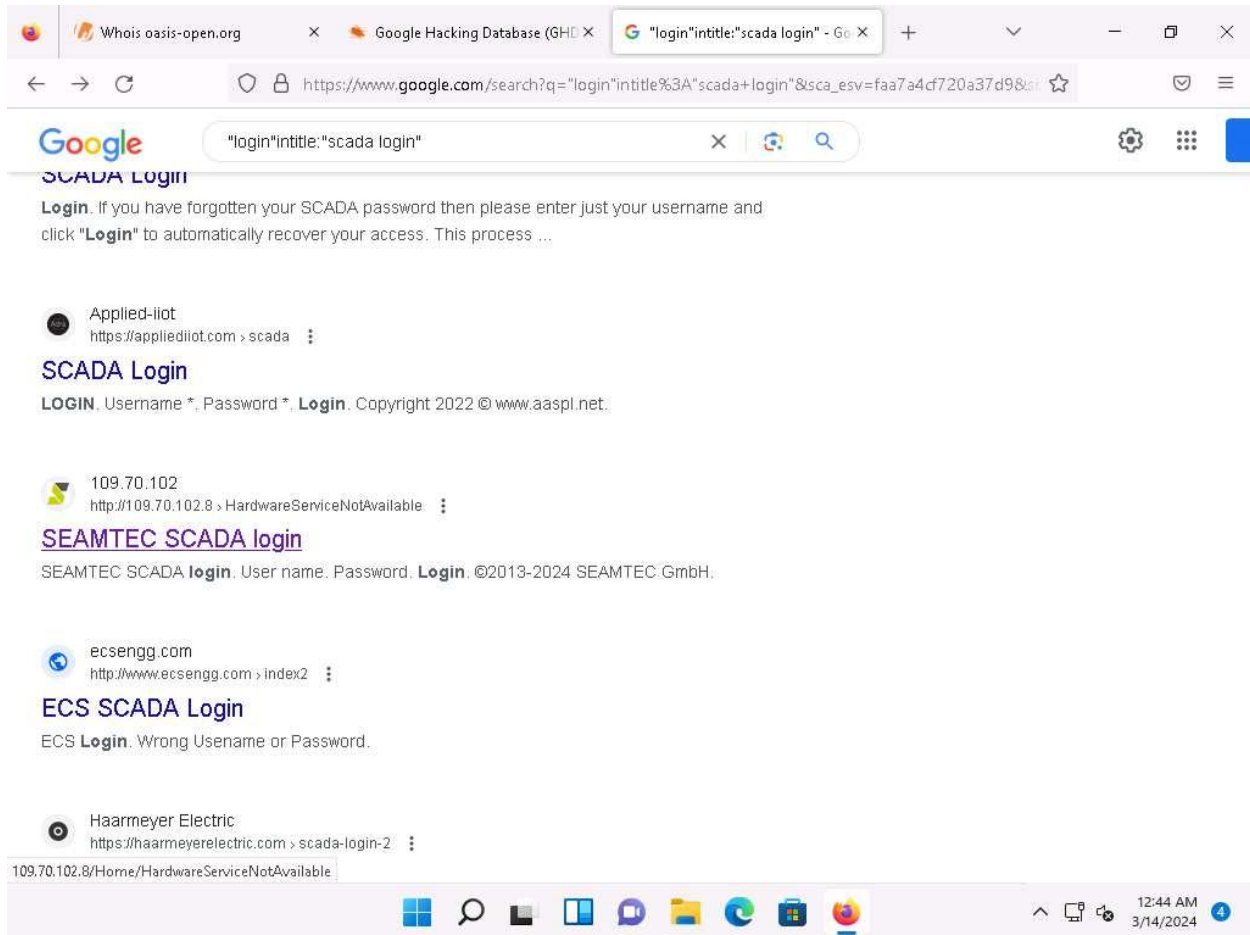
Showing 1 to 7 of 7 entries (filtered from 7,915 total entries)

FIRST PREVIOUS 1 NEXT LAST

8. Now, we will use the dorks obtained in the previous step to query results in Google.
9. Open a new tab and go to <https://www.google.com>. In the search field, enter **"login" intitle:"scada login"**.



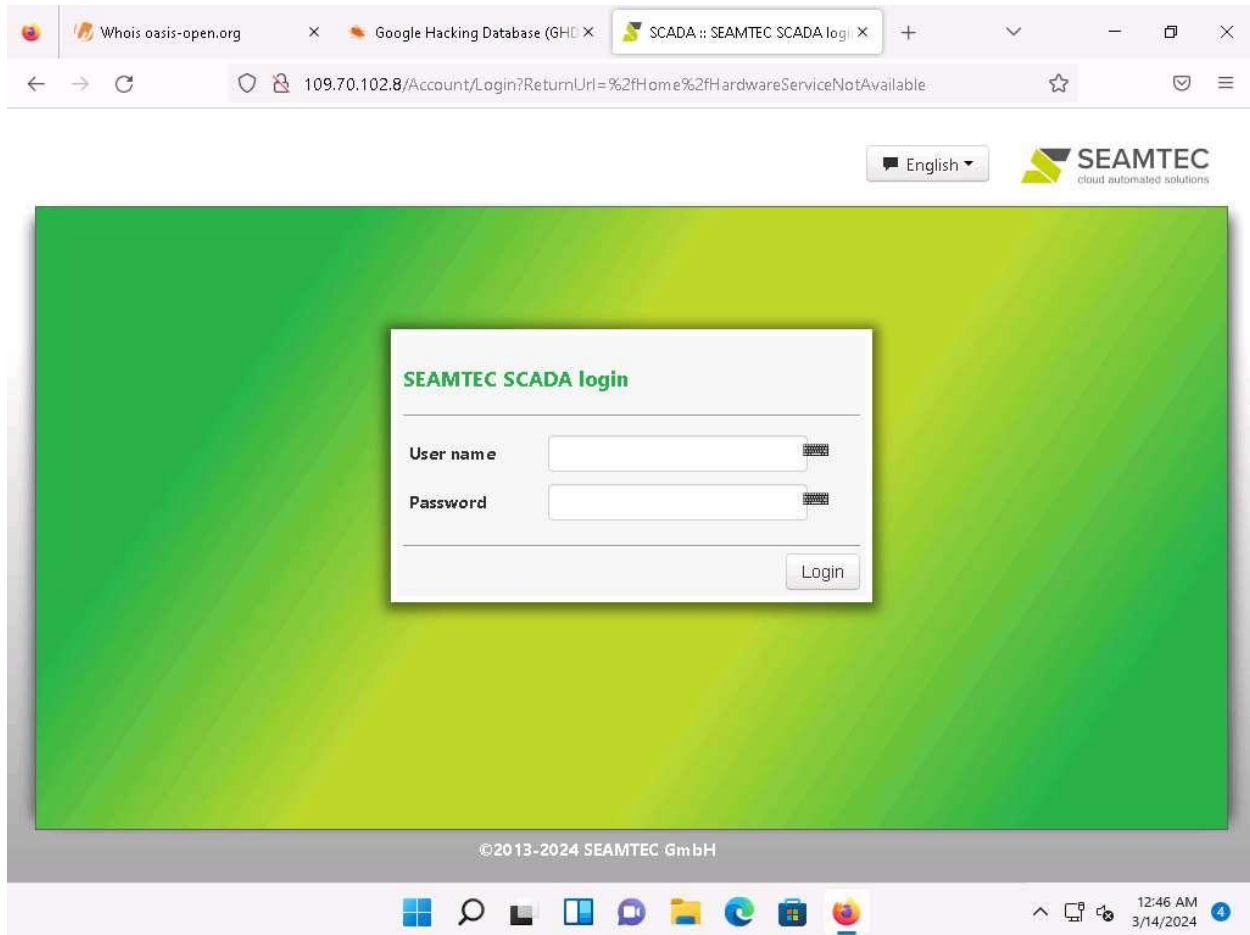
10. The search result appears; click any link (here, **SEAMTEC SCADA login**).



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.

11. 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.

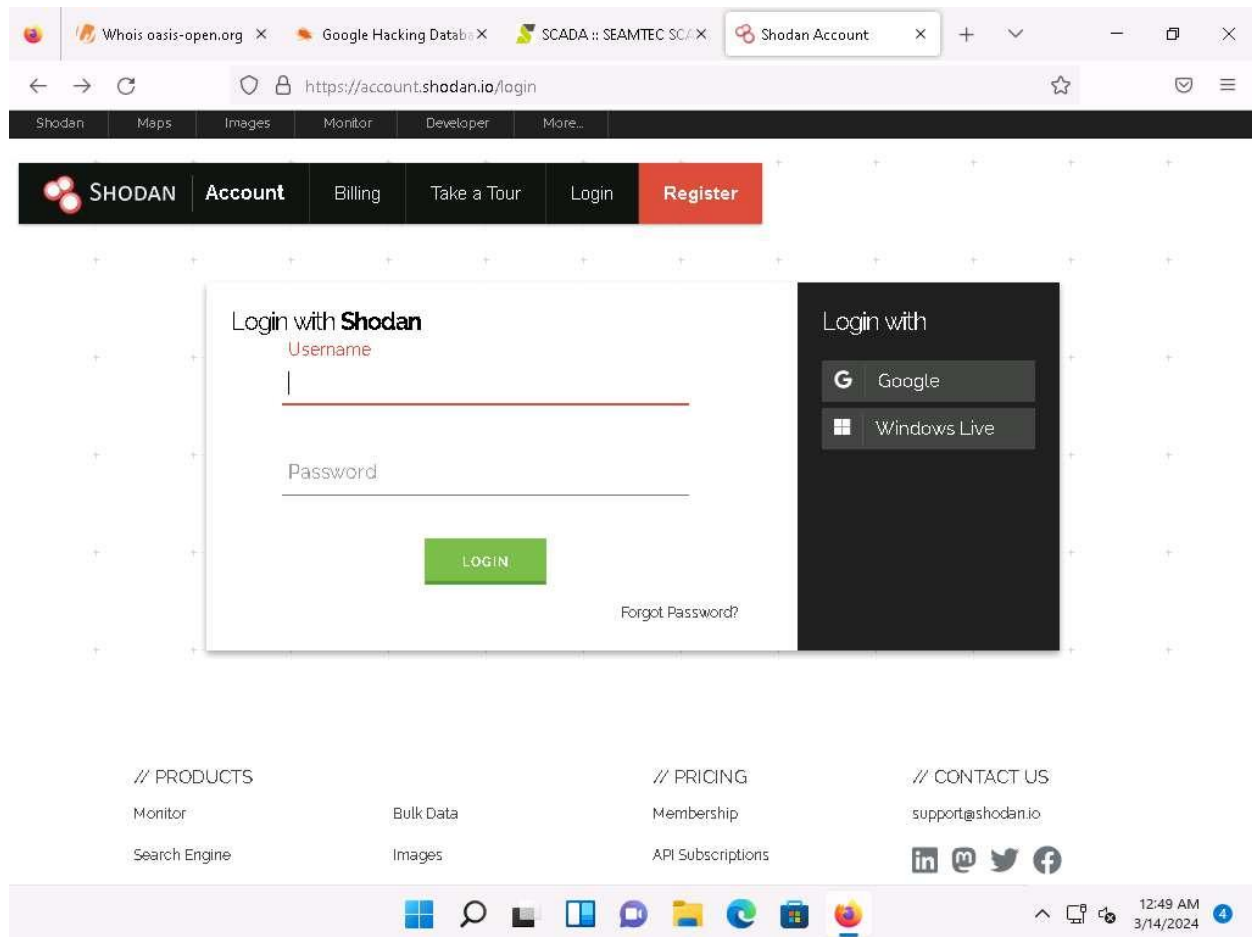


12. Similarly, you can use advanced search operators such as **intitle:"index of" scada** to search sensitive SCADA directories that are exposed on sites.

13. Now, in the browser window, open a new tab and go to **<https://account.shodan.io/login>**.

14. The **Login with Shodan** page appears; enter your username and password in the **Username** and **Password** fields, respectively; and click **Login**.

If you do not have an existing account, then go to the **Register** option to register yourself .

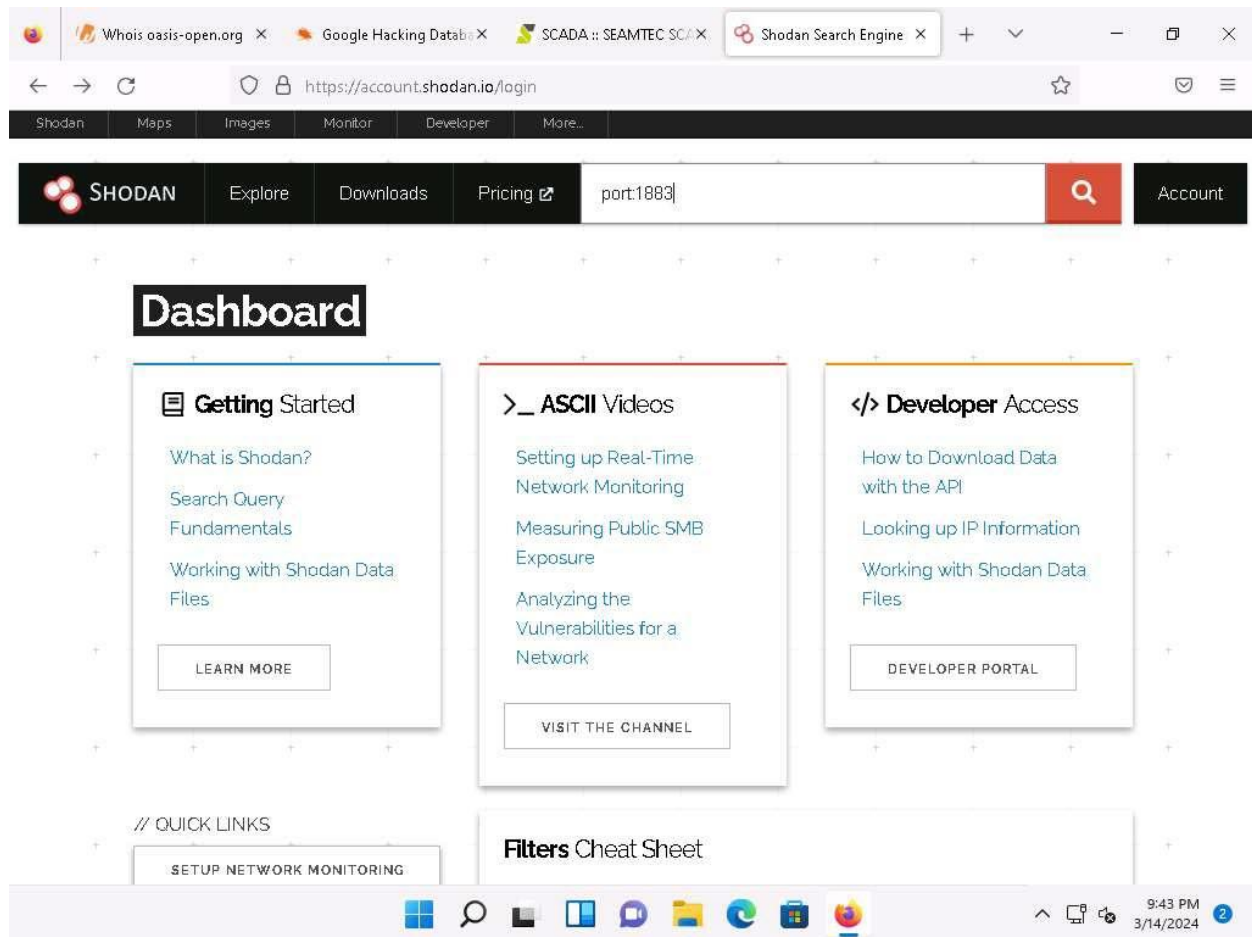


15. The **Account Overview** page appears, which displays the account-related information. Click on **Shodan** on top-left corner of the window to go to the main page of **Shodan**.

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

16. 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.



17. The result appears, displaying the list of IP addresses having port 1883 enabled.


18. Click on any IP address to view its detailed information.

Whois oasis-open.org X Google Hacking Datab X SCADA :: SEAMTEC SCA X port:1883 - Shodan Search X

https://account.shodan.io/login

TOTAL RESULTS
1,018,738

TOP COUNTRIES



United States	418,011
Korea, Republic of	363,848
China	105,214
Japan	18,113
Germany	13,585

[More...](#)

TOP ORGANIZATIONS

SK Broadband Co ...	357,215
Google LLC	355,579
Allyun Computing C...	40,166
Flyio, Inc.	22,508
Huawei Public Clou...	10,559

[More...](#)

TOP PRODUCTS

View Report Browse Images View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

34.49.29.35 2024-03-15T04:43:20.440441

35.29.49.34.bc.googleusercontent.com
Google LLC
United States, Kansas City
cloud

130.211.8.229 2024-03-15T04:43:13.001874

229.8.211.130.bc.googleusercontent.com
Google LLC
United States, Kansas City
cloud

213.188.219.148 2024-03-15T04:43:00.028015

Flyio, Inc.
United States, Chicago

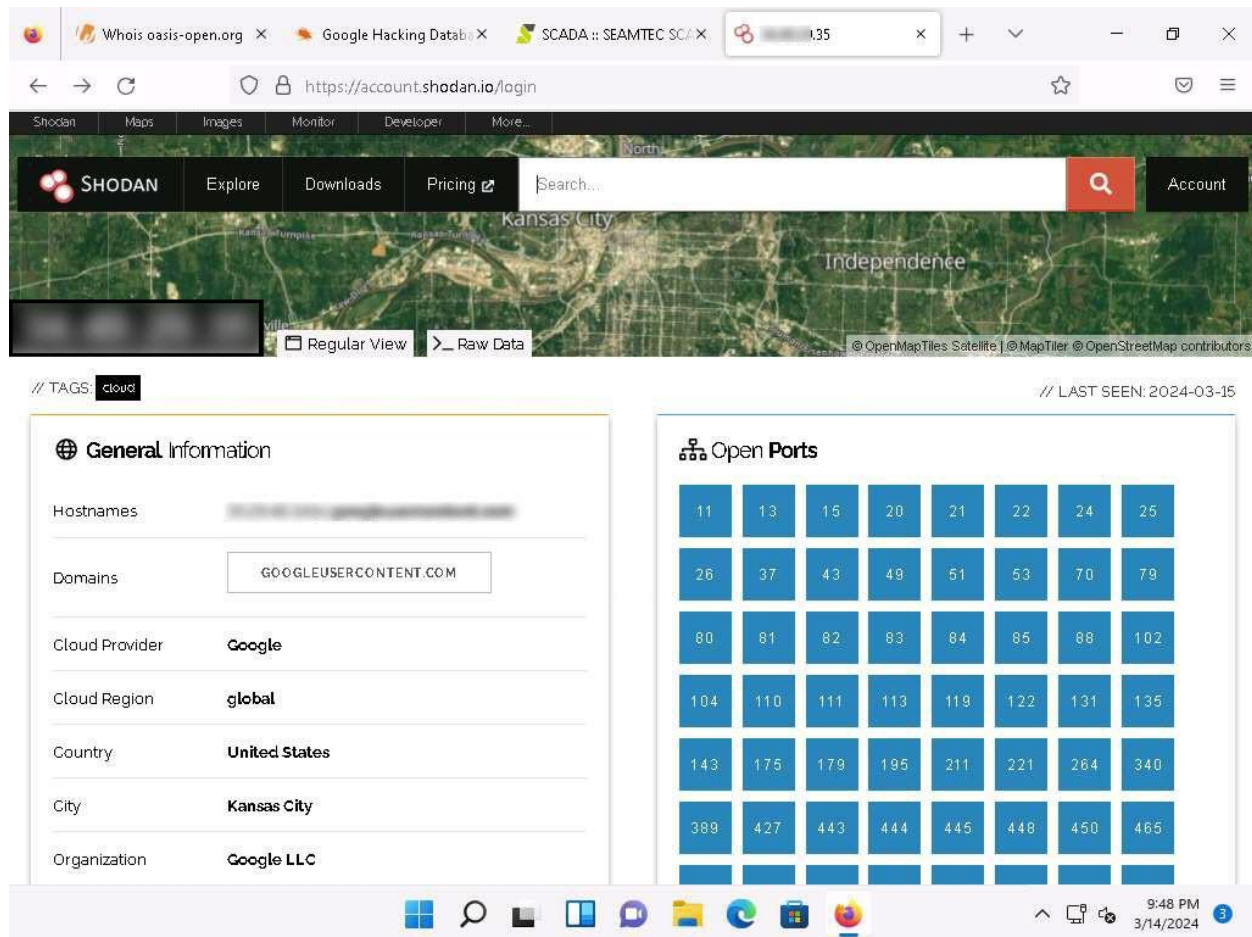
39.125.233.41 2024-03-15T04:42:48.171868

SK Broadband Co Ltd
Korea, Republic of, Yeosu
MQTT Connection Code: 0
Topics:

58.236.75.116 2024-03-15T04:42:46.756183

Windows taskbar: 9:44 PM 3/14/2024

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



20. 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"

21. 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.

22. 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.

23. Close all open windows and document all the acquired information.

Question 18.1.1.1

Use the Shodan search engine to collect the IP addresses with MQTT enabled. Perform a search using the MQTT port number. Which port number will you enter in the search field to obtain the desired result?