Module 2

Lab 1: Perform Footprinting Through Search Engines

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks.

Lab Objectives

- Gather information using advanced Google hacking techniques

Overview of Search Engines

Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Task 1: Gather Information using Advanced Google Hacking Techniques

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. This can provide information about websites that are vulnerable to exploitation.

Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. By default, **Windows 11** machine selected, click Ctrl+Alt+Delete and login with **Admin**/**Pa$$w0rd**.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane.

Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.

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

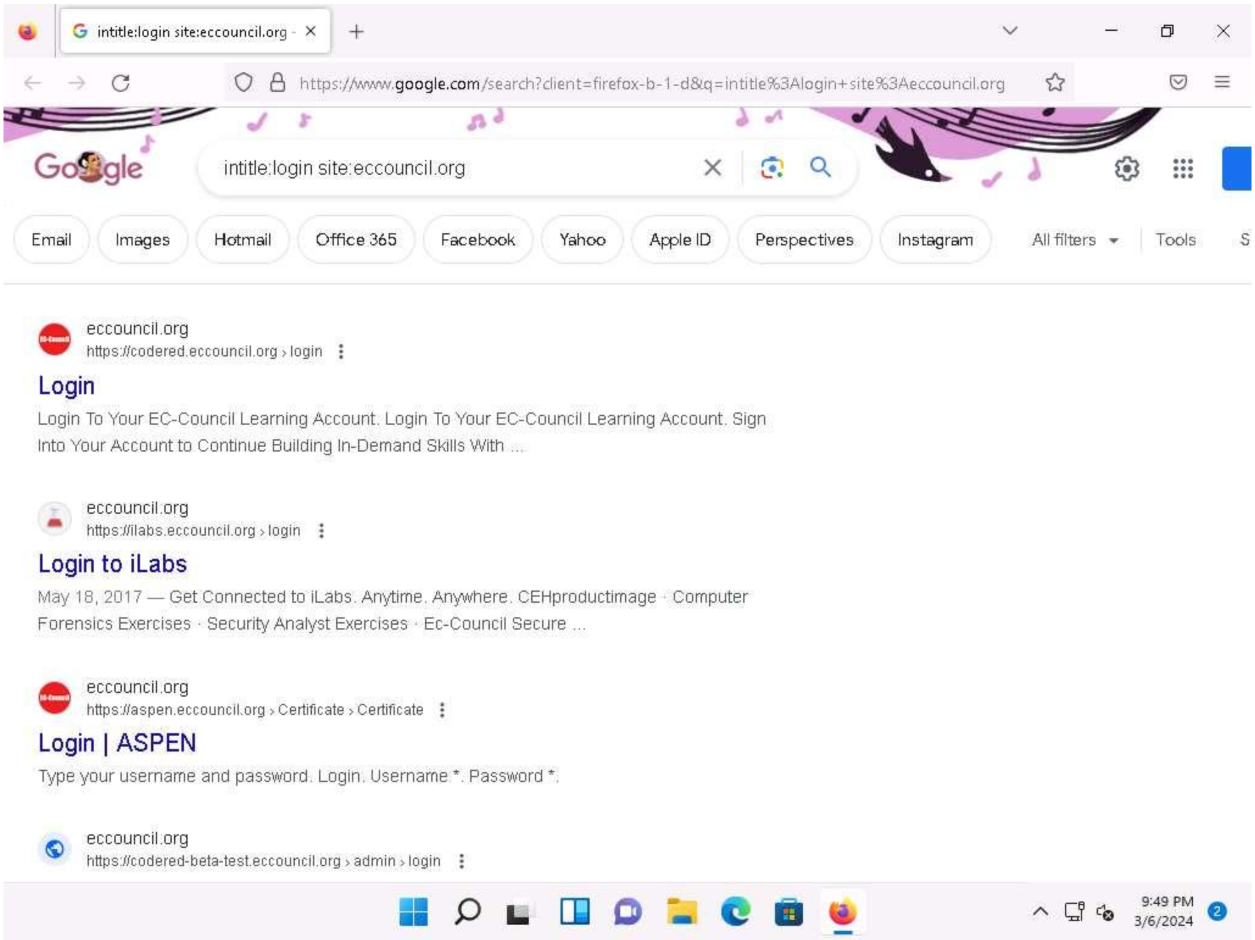
2. Launch any web browser, and go to **https://www.google.com** (here, we are using **Mozilla Firefox**).

If a **Firefox Software Updater** window appears click **No**.

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
- If a notification appears, click **Okay, Got it** to finish viewing the information.

3. In the search bar search for **intitle:login site:eccouncil.org**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **eccouncil.org** website that contain the **login** pages. An example is shown in the screenshot below.

Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential bruteforcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.



https://www.google.com/search?client=firefox-b-1-d&q=intitle%3Alogin+site%3Aeccouncil.org

intitle:login site:eccouncil.org

eccouncil.org
https://codered.eccouncil.org › login

Login

Login To Your EC-Council Learning Account. Login To Your EC-Council Learning Account. Sign Into Your Account to Continue Building In-Demand Skills With ...

eccouncil.org
https://ilabs.eccouncil.org › login

Login to iLabs

May 18, 2017 — Get Connected to iLabs. Anytime. Anywhere. CEHproductimage · Computer Forensics Exercises · Security Analyst Exercises · Ec-Council Secure ...

eccouncil.org
https://aspen.eccouncil.org › Certificate › Certificate

Login | ASPEN

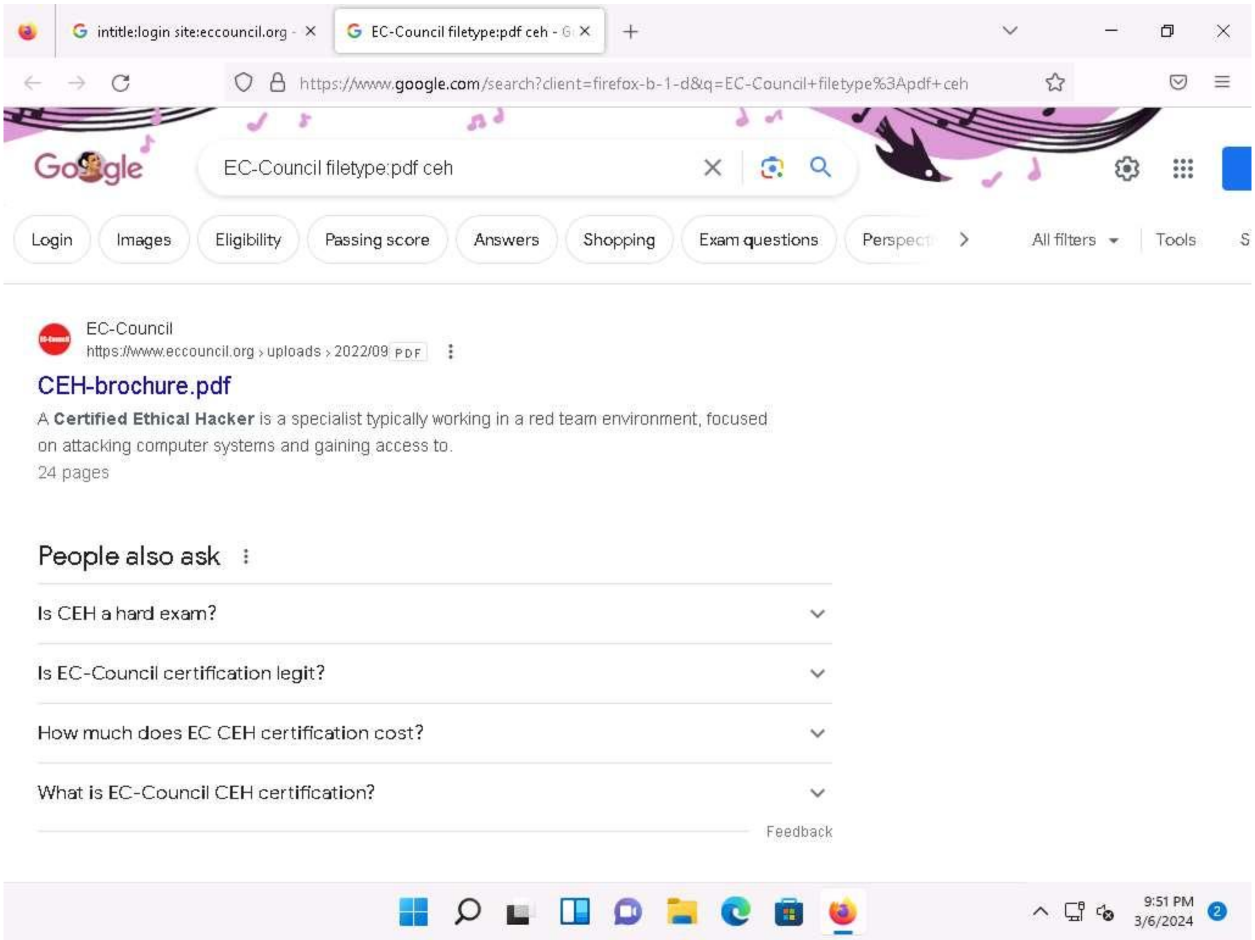
Type your username and password. Login. Username *. Password *.

eccouncil.org
https://codered-beta-test.eccouncil.org › admin › login

4. Similarly, type the command **EC-Council filetype:pdf ceh** in the search bar to search your results based on the file extension and the keyword (here, **ceh**). Click on any link from the results (here, **CEH-brochure.pdf**) to view the pdf file.

Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.

The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target.



intitle:login site:eccouncil.org
EC-Council filetype:pdf ceh - G
https://www.google.com/search?client=firefox-b-1-d&q=EC-Council+filetype%3Apdf+ceh
Google
Login
Images
Eligibility
Passing score
Answers
Shopping
Exam questions
Perspect
All filters
Tools
9:51 PM
3/6/2024

EC-Council filetype:pdf ceh

EC-Council
https://www.eccouncil.org › uploads › 2022/09 PDF

CEH-brochure.pdf

A **Certified Ethical Hacker** is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to.

24 pages

People also ask

Is CEH a hard exam?

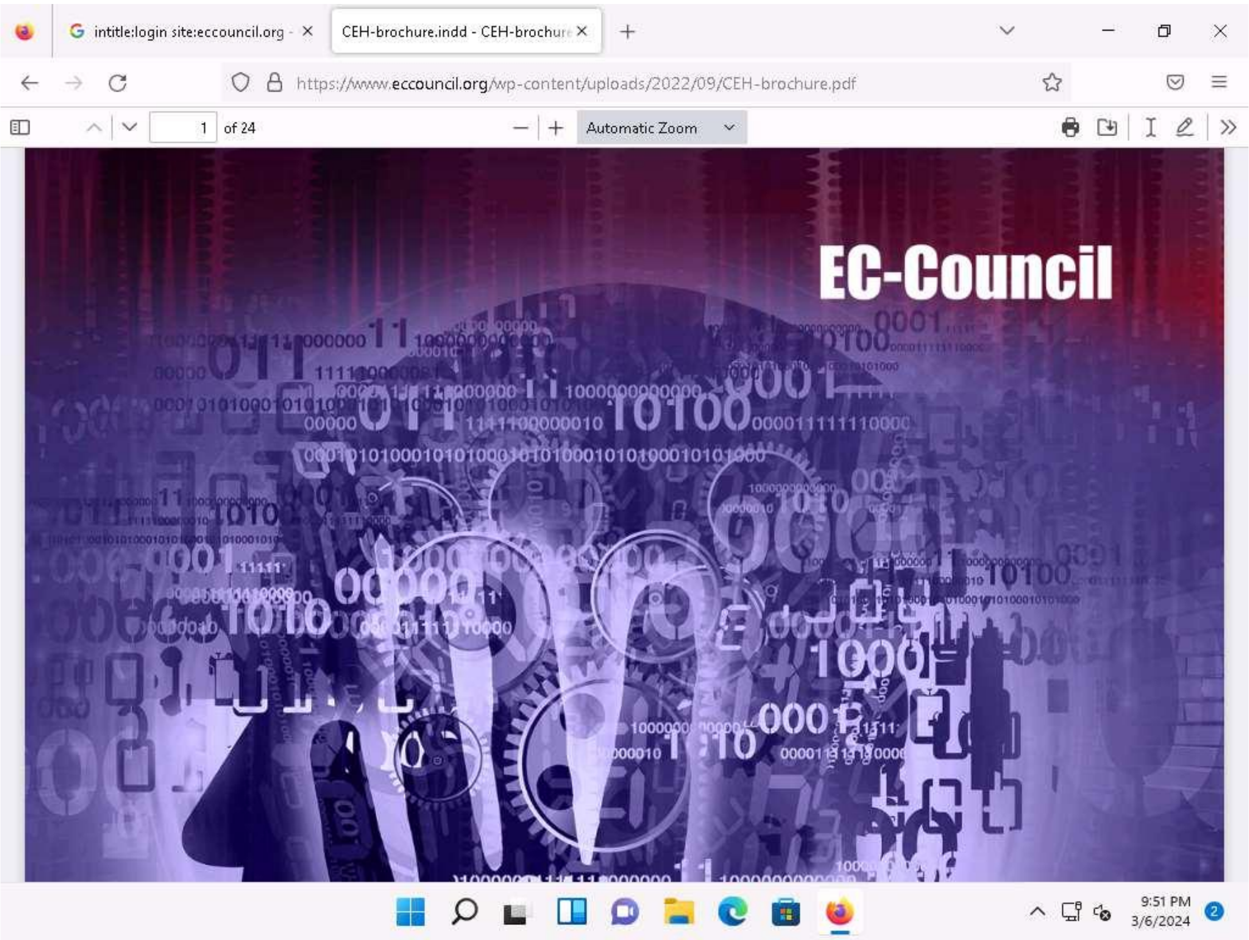
Is EC-Council certification legit?

How much does EC CEH certification cost?

What is EC-Council CEH certification?

Feedback

5. The page appears displaying the PDF file, as shown in the screenshot.


intitle:login site:eccouncil.org
CEH-brochure.indd - CEH-brochure
https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf
1
of 24
Automatic Zoom
EC-Council
9:51 PM
3/6/2024

6. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

    ○ **cache**: This operator allows you to view cached version of the web page. [cache:www.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org

    ○ **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL. [allinurl: EC-Council career]—Query returns only pages containing the words "EC-Council" and "career" in the URL

    ○ **inurl**: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.eccouncil.org]—Query returns only pages in EC-Council site in which the URL has the word "copy"

    ○ **allintitle**: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title

    ○ **inanchor**: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word “Norton” and the page containing the word “Anti-virus”

- **allinanchor**: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words “best,” “cloud,” “service,” and “provider”
- **link**: This operator searches websites or pages that contain links to the specified website or page. [link:www.eccouncil.org]—Finds pages that point to EC-Council’s home page
- **related**: This operator displays websites that are similar or related to the URL specified. [related:www.eccouncil.org]—Query provides the Google search engine results page with websites similar to eccouncil.org
- **info**: This operator finds information for the specified web page. [info:eccouncil.org]—Query provides information about the www.eccouncil.org home page
- **location**: This operator finds information for a specific location. [location: EC-Council]—Query give you results based around the term EC-Council

7. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.

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