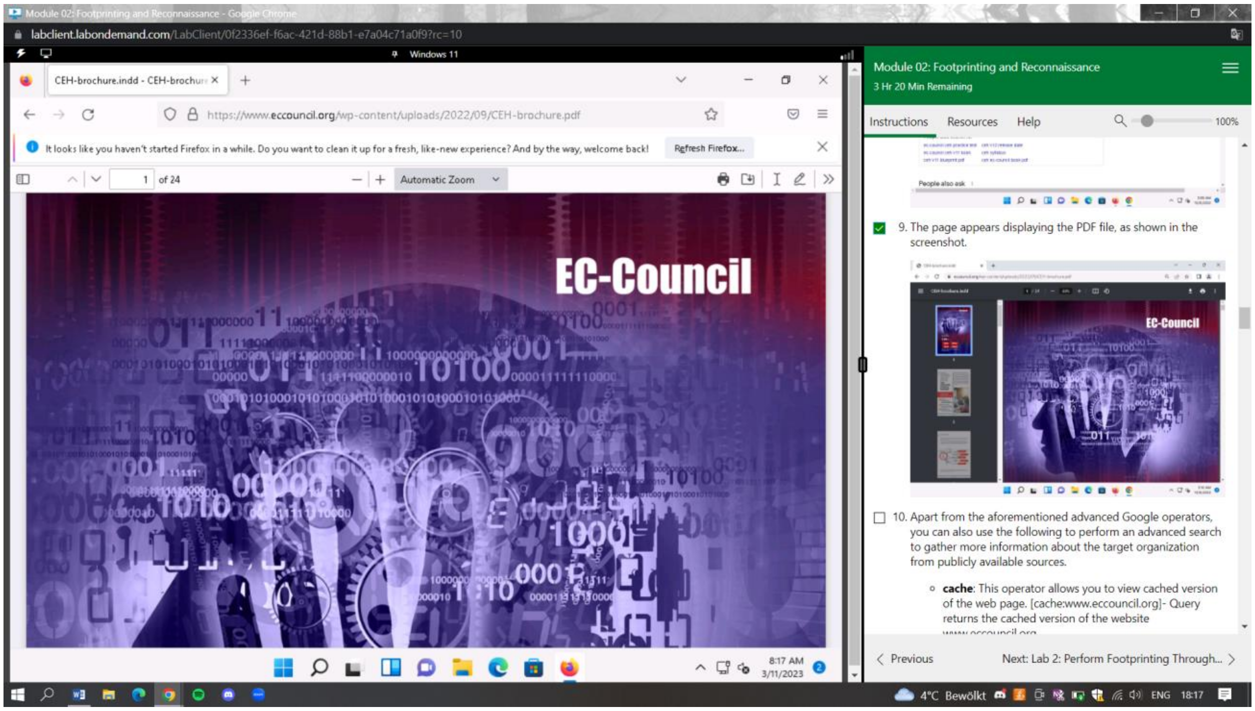
CEH Lab 1 - Footprinting

13.03.2023
Grigoraş Ana-Maria
Application Security and Pentesting ILV mcr22
Dr. Gerald Emerick

LAB1:



Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Windows 11
CEH-brochure.indd - CEH-brochure
https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
1 of 24
Automatic Zoom
EC-Council
8:17 AM
3/11/2023
Instructions
Resources
Help
100%
People also ask
Previous
Next: Lab 2: Perform Footprinting Through...
4°C Bewölkt
ENG
18:17

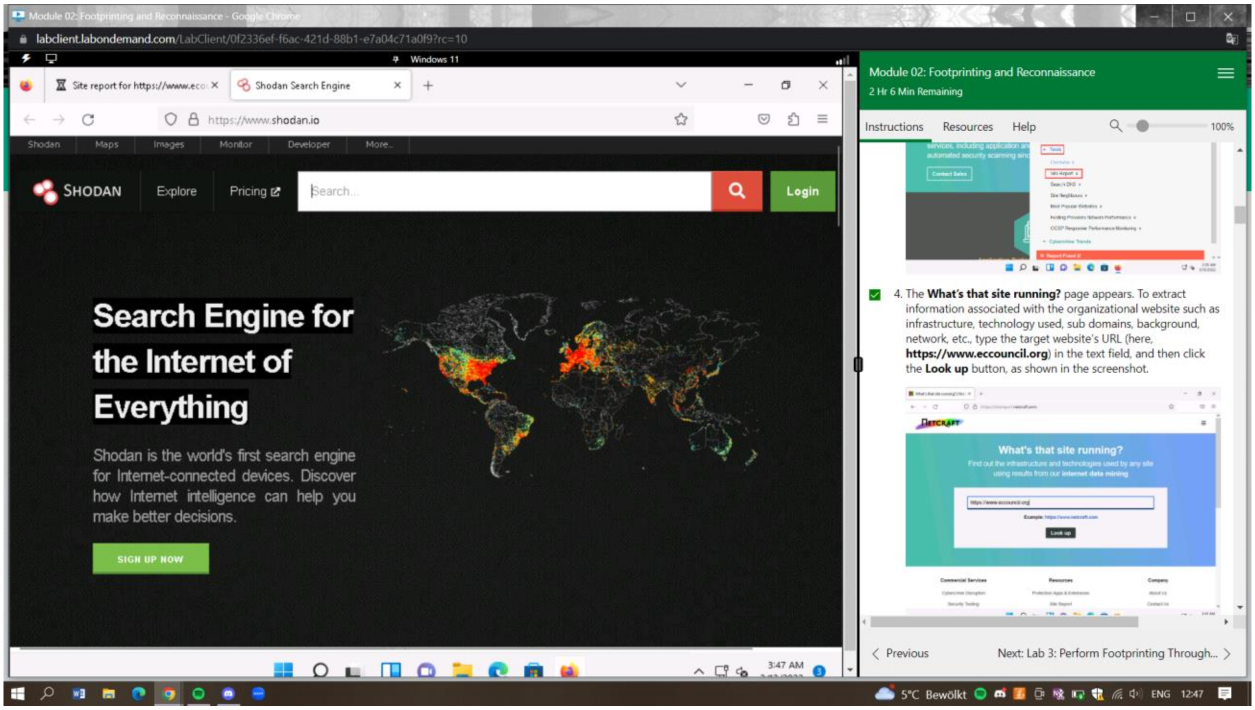
Module 02: Footprinting and Reconnaissance

3 Hr 20 Min Remaining

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

□ 10. 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

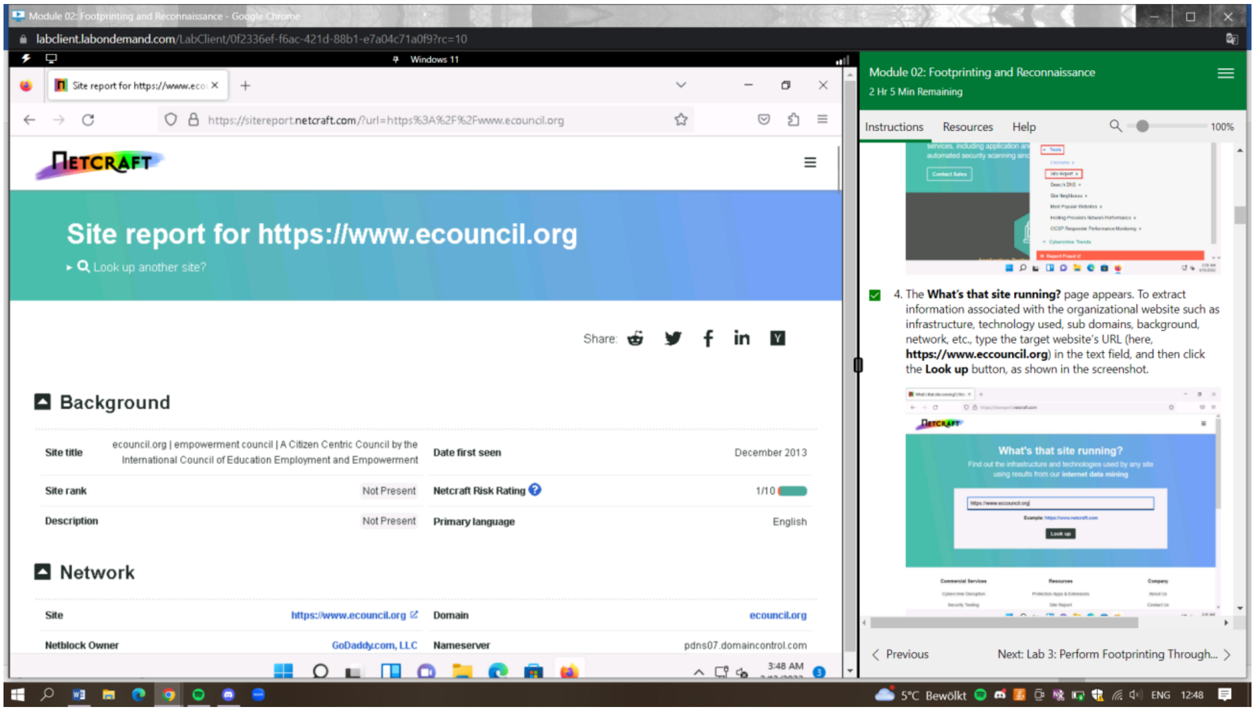

Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Windows 11
Site report for https://www.eco
Shodan Search Engine
https://www.shodan.io
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Pricing
Search...
Login
SIGN UP NOW
3:47 AM
Module 02: Footprinting and Reconnaissance
2 Hr 6 Min Remaining
Instructions
Resources
Help
100%
Previous
Next: Lab 3: Perform Footprinting Through...
5°C Bewölkt
ENG
12:47

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

☑ 4. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the **Look up** button, as shown in the screenshot.

LAB2:


Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Windows 11
Site report for https://www.eco
https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.ecouncil.org
NETCRAFT
Share:
3:48 AM
Module 02: Footprinting and Reconnaissance
2 Hr 5 Min Remaining
Instructions
Resources
Help
100%
Previous
Next: Lab 3: Perform Footprinting Through...
5°C Bewölkt
ENG
12:48

Site report for https://www.ecouncil.org

▸ Look up another site?

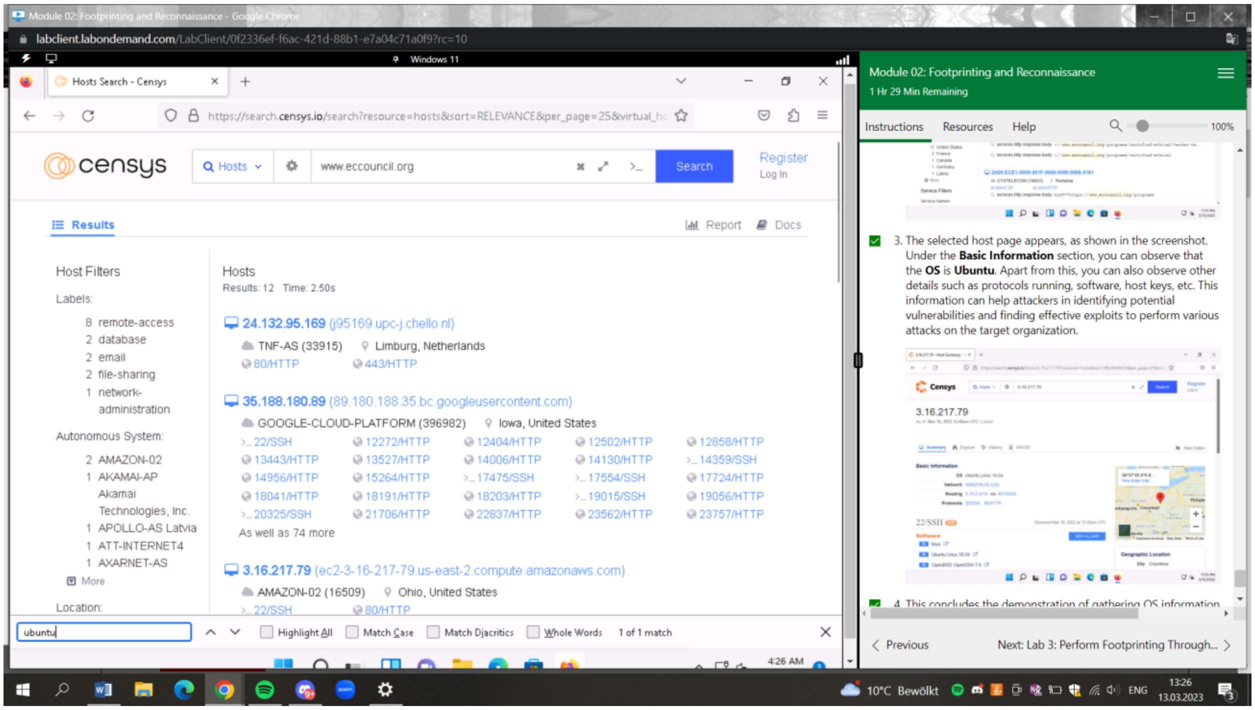
Background

Site title	ecouncil.org | empowerment council | A Citizen Centric Council by the International Council of Education Employment and Empowerment	Date first seen	December 2013
Site rank	Not Present	Netcraft Risk Rating	1/10
Description	Not Present	Primary language	English

Network

Site	https://www.ecouncil.org	Domain	ecouncil.org
Netblock Owner	GoDaddy.com, LLC	Nameserver	pdns07.domaincontrol.com

☑ 4. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the **Look up** button, as shown in the screenshot.



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

Hosts Search - Censys

https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_ho

censys — Hosts — www.eccouncil.org — Search

Results

Host Filters

Labels:
8 remote-access
2 database
2 email
2 file-sharing
1 network-administration

Autonomous System:
2 AMAZON-02
1 AKAMAI-AP Akamai Technologies, Inc.
1 APOLLO-AS Latvia
1 ATT-INTERNET4
1 AXARNET-AS
More

Location:

Hosts
Results: 12 Time: 2.50s

24.132.95.169 (j95169.upc-j.chello.nl)
TNF-AS (33915) Limburg, Netherlands
80/HTTP 443/HTTP

35.188.180.89 (89.180.188.35.bc.googleusercontent.com)
GOOGLE-CLOUD-PLATFORM (396982) Iowa, United States
22/SSH 12272/HTTP 12404/HTTP 12502/HTTP 12858/HTTP 13443/HTTP 13527/HTTP 14006/HTTP 14130/HTTP 14359/SSH 14956/HTTP 15264/HTTP 17475/SSH 17554/SSH 17724/HTTP 18041/HTTP 18191/HTTP 18203/HTTP 19015/SSH 19056/HTTP 20325/SSH 21706/HTTP 22837/HTTP 23562/HTTP 23757/HTTP
As well as 74 more

3.16.217.79 (ec2-3-16-217-79.us-east-2.compute.amazonaws.com)
AMAZON-02 (16509) Ohio, United States
22/SSH 80/HTTP

ubuntu — Highlight All — Match Case — Match Diacritics — Whole Words — 1 of 1 match

Module 02: Footprinting and Reconnaissance
1 Hr 29 Min Remaining

Instructions Resources Help 100%

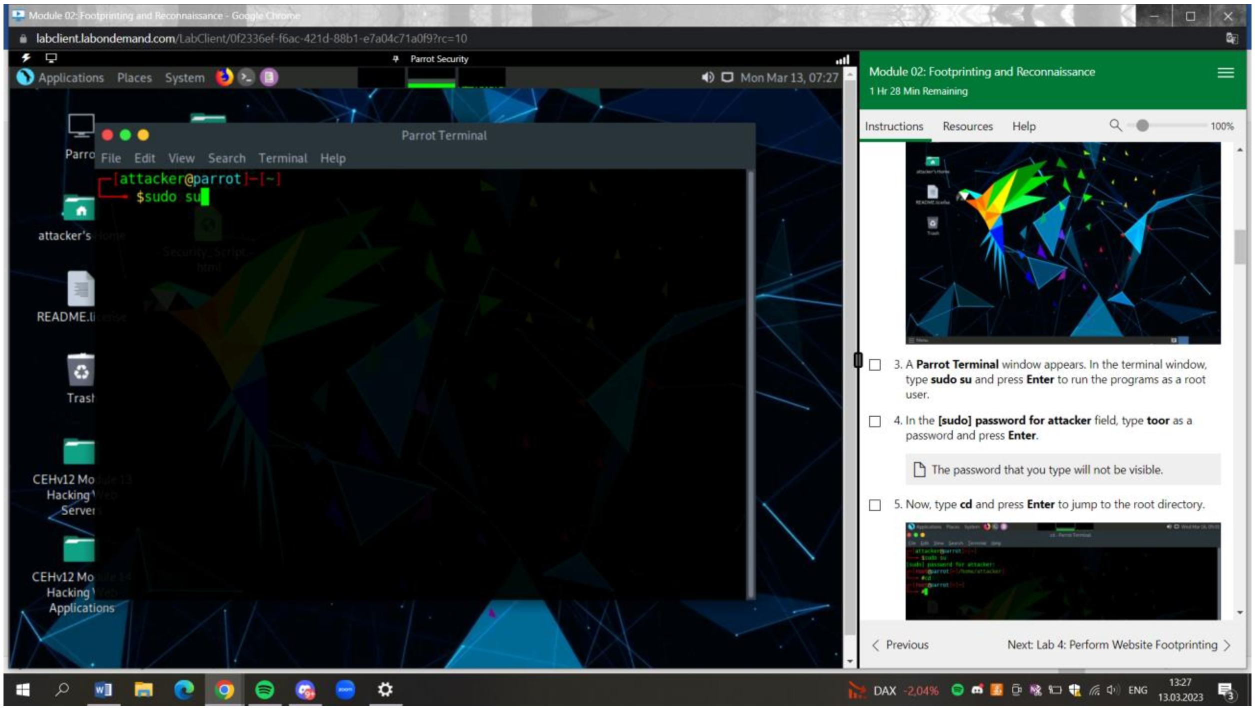
☑ 3. The selected host page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Ubuntu**. Apart from this, you can also observe other details such as protocols running, software, host keys, etc. This information can help attackers in identifying potential vulnerabilities and finding effective exploits to perform various attacks on the target organization.

☑ 4. This concludes the demonstration of gathering OS information

Previous — Next: Lab 3: Perform Footprinting Through...

10°C Bewölkt ENG 13:26 13.03.2023

LAB3:



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

Parrot Security

Applications Places System Mon Mar 13, 07:27

Parrot Terminal

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
```

Module 02: Footprinting and Reconnaissance
1 Hr 28 Min Remaining

Instructions Resources Help 100%

□ 3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

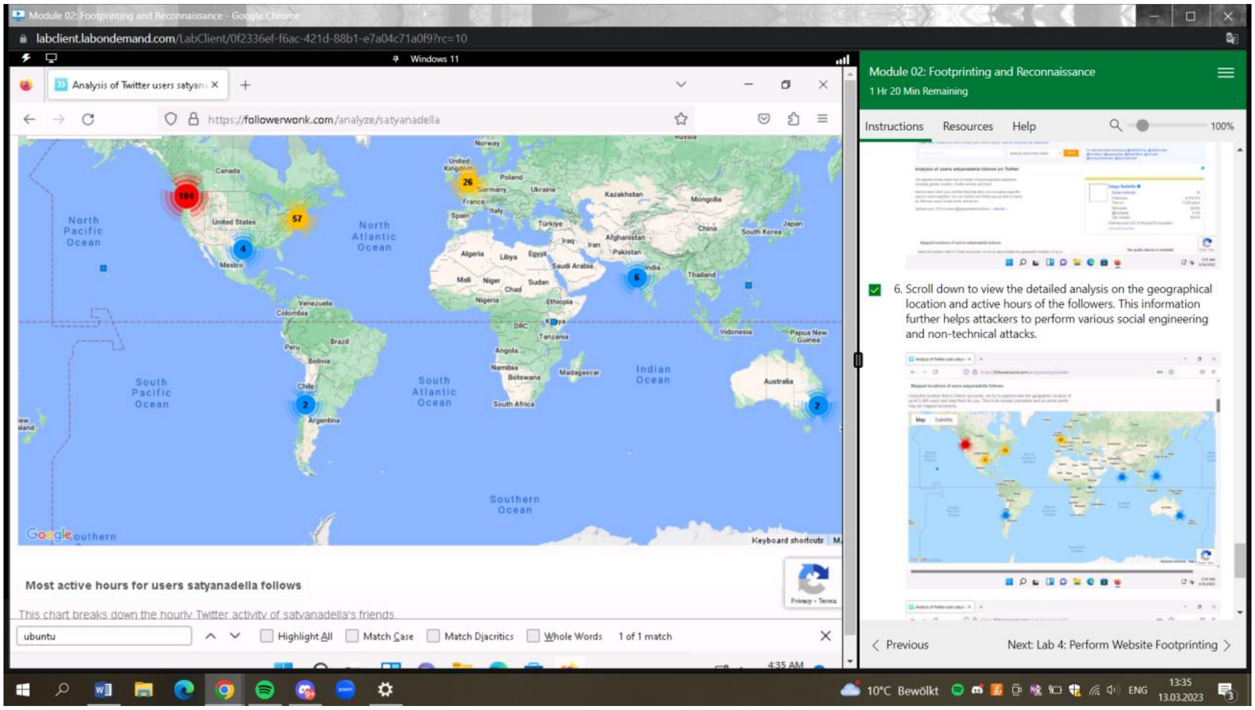
□ 4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

□ 5. Now, type **cd** and press **Enter** to jump to the root directory.

Previous — Next: Lab 4: Perform Website Footprinting

DAX -2,04% ENG 13:27 13.03.2023



Most active hours for users satyanadella follows

This chart breaks down the hourly Twitter activity of satyanadella's friends.

Module 02: Footprinting and Reconnaissance

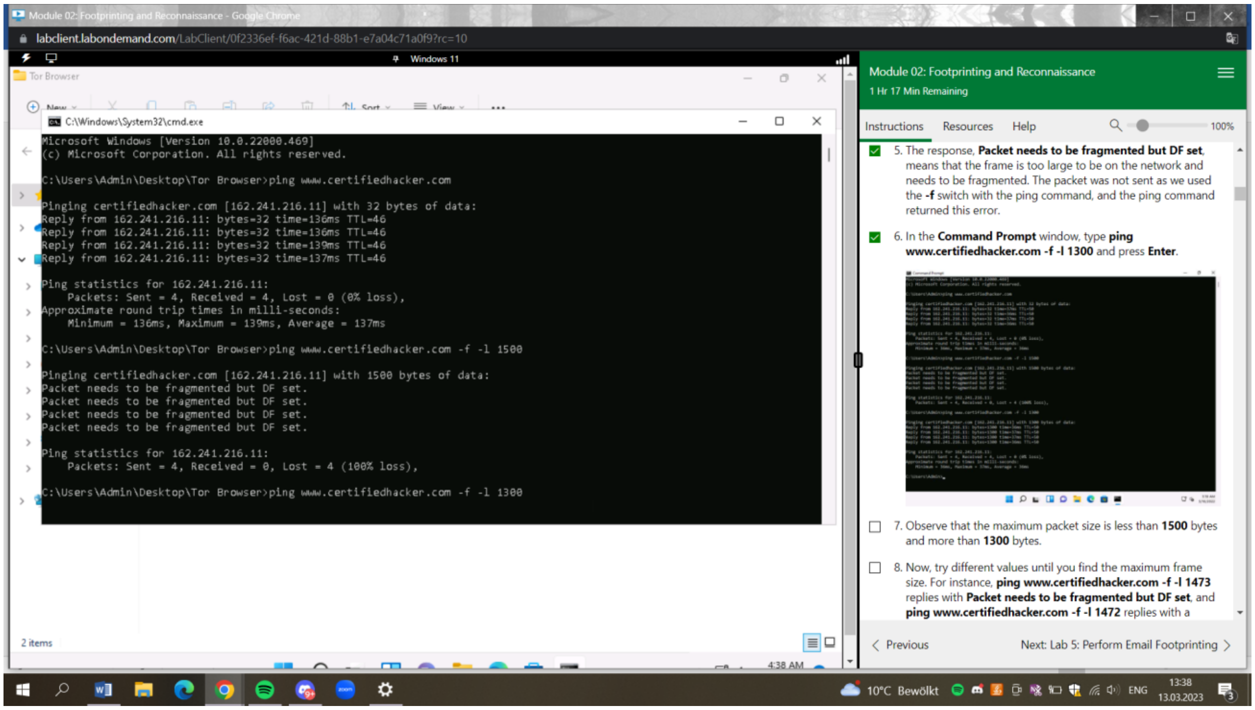
1 Hr 20 Min Remaining

Instructions Resources Help 100%

☑ 6. Scroll down to view the detailed analysis on the geographical location and active hours of the followers. This information further helps attackers to perform various social engineering and non-technical attacks.

< Previous Next: Lab 4: Perform Website Footprinting >

LAB4:



Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Windows 11
Tor Browser
New
Sort
View
C:\Windows\System32\cmd.exe
2 items
4:38 AM
10°C Bewölkt
ENG
13:38
13.03.2023

```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Desktop\Tor Browser>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=136ms TTL=46
Reply from 162.241.216.11: bytes=32 time=136ms TTL=46
Reply from 162.241.216.11: bytes=32 time=139ms TTL=46
Reply from 162.241.216.11: bytes=32 time=137ms TTL=46

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 139ms, Average = 137ms

C:\Users\Admin\Desktop\Tor Browser>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin\Desktop\Tor Browser>ping www.certifiedhacker.com -f -l 1300
```

Module 02: Footprinting and Reconnaissance

1 Hr 17 Min Remaining

Instructions Resources Help 100%

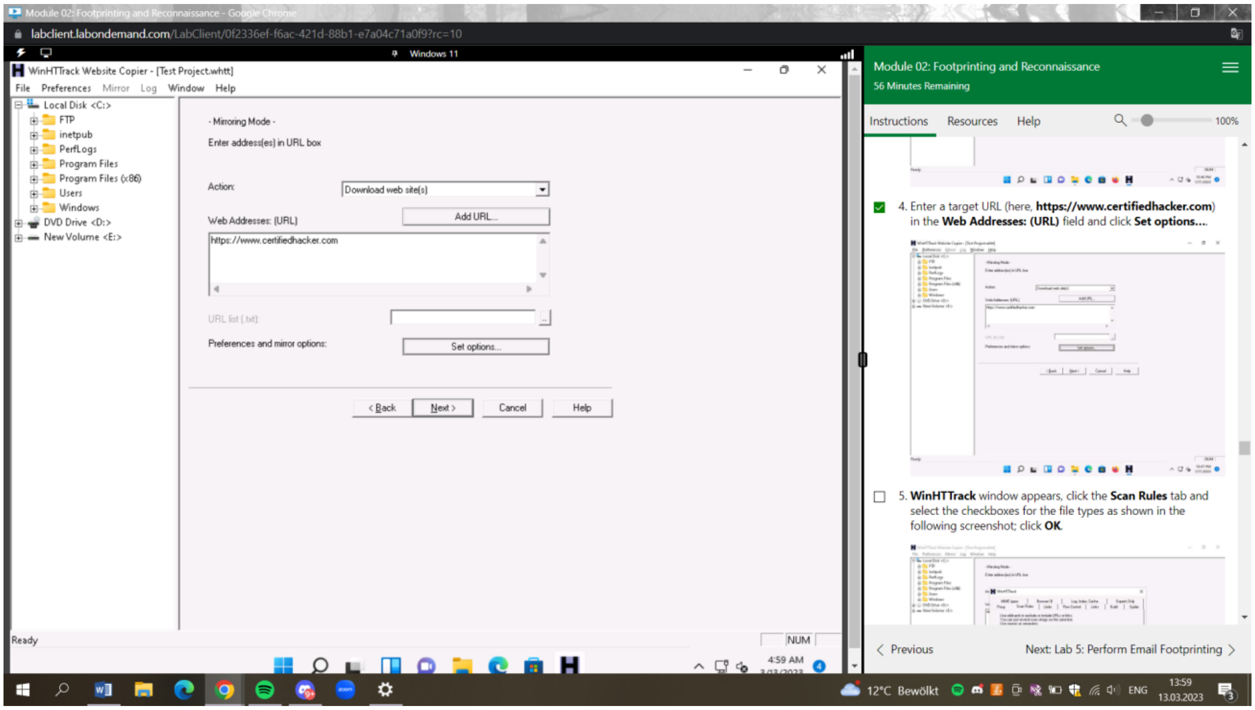
☑ 5. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the **-f** switch with the ping command, and the ping command returned this error.

☑ 6. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.

☐ 7. Observe that the maximum packet size is less than **1500** bytes and more than **1300** bytes.

☐ 8. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set**, and **ping www.certifiedhacker.com -f -l 1472** replies with a

< Previous Next: Lab 5: Perform Email Footprinting >



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

WinHTTrack Website Copier - [Test Project.whtt]

- Mirroring Mode -

Enter address(es) in URL box

Action: Download web site(s)

Web Addresses: (URL)

https://www.certifiedhacker.com

URL list (.txt):

Preferences and mirror options:

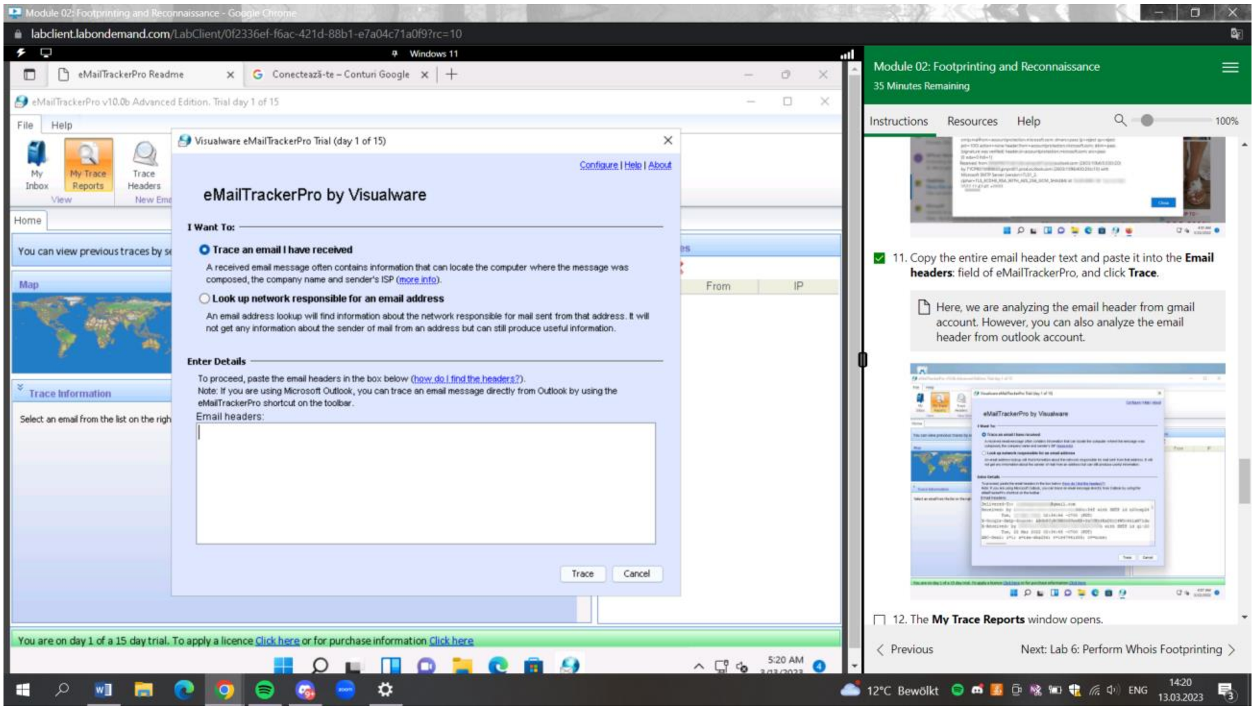
Module 02: Footprinting and Reconnaissance

56 Minutes Remaining

☑ 4. Enter a target URL (here, **https://www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options...**.

□ 5. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.

Lab5:



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

Visualware eMailTrackerPro Trial (day 1 of 15)

eMailTrackerPro by Visualware

I Want To:

● **Trace an email I have received**

A received email message often contains information that can locate the computer where the message was composed, the company name and sender's ISP (more info).

○ **Look up network responsible for an email address**

An email address lookup will find information about the network responsible for mail sent from that address. It will not get any information about the sender of mail from an address but can still produce useful information.

Enter Details

To proceed, paste the email headers in the box below (how do I find the headers?).
Note: If you are using Microsoft Outlook, you can trace an email message directly from Outlook by using the eMailTrackerPro shortcut on the toolbar.

Email headers:

You can view previous traces by se

Select an email from the list on the righ

You are on day 1 of a 15 day trial. To apply a licence Click here or for purchase information Click here

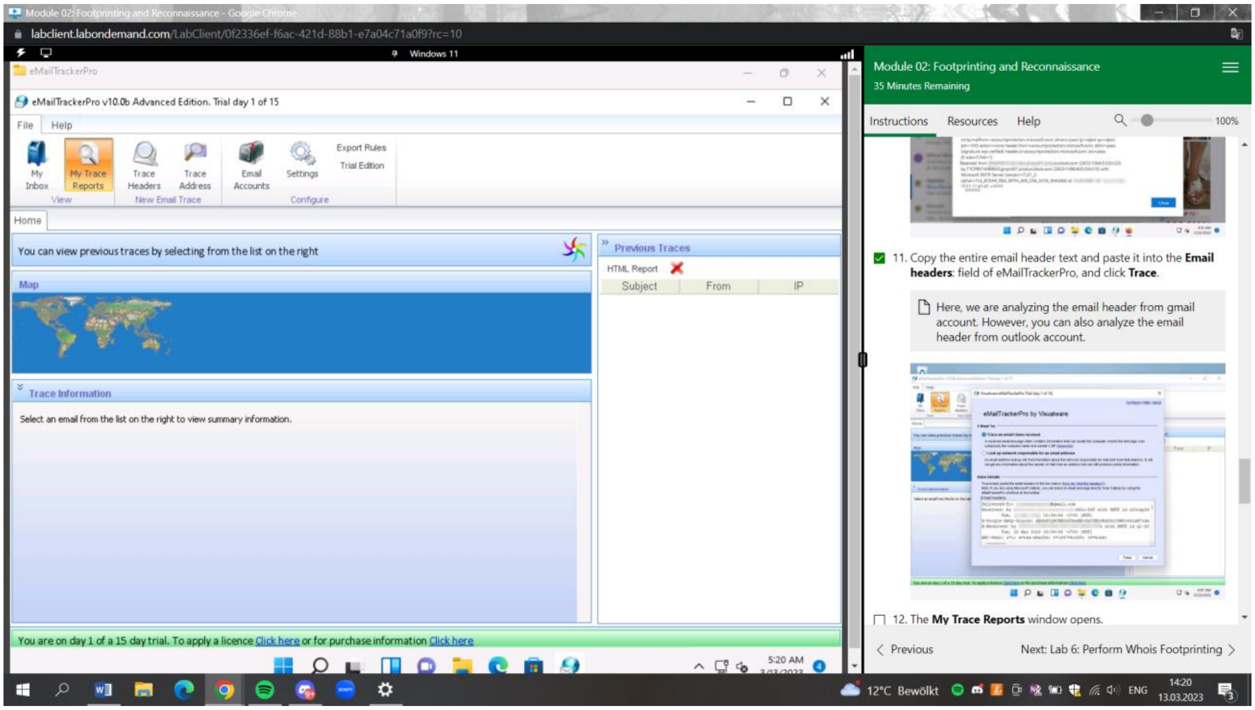
Module 02: Footprinting and Reconnaissance

35 Minutes Remaining

☑ 11. Copy the entire email header text and paste it into the **Email headers**: field of eMailTrackerPro, and click **Trace**.

Here, we are analyzing the email header from gmail account. However, you can also analyze the email header from outlook account.

□ 12. The **My Trace Reports** window opens.



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

You can view previous traces by selecting from the list on the right

Select an email from the list on the right to view summary information.

You are on day 1 of a 15 day trial. To apply a licence Click here or for purchase information Click here

Module 02: Footprinting and Reconnaissance

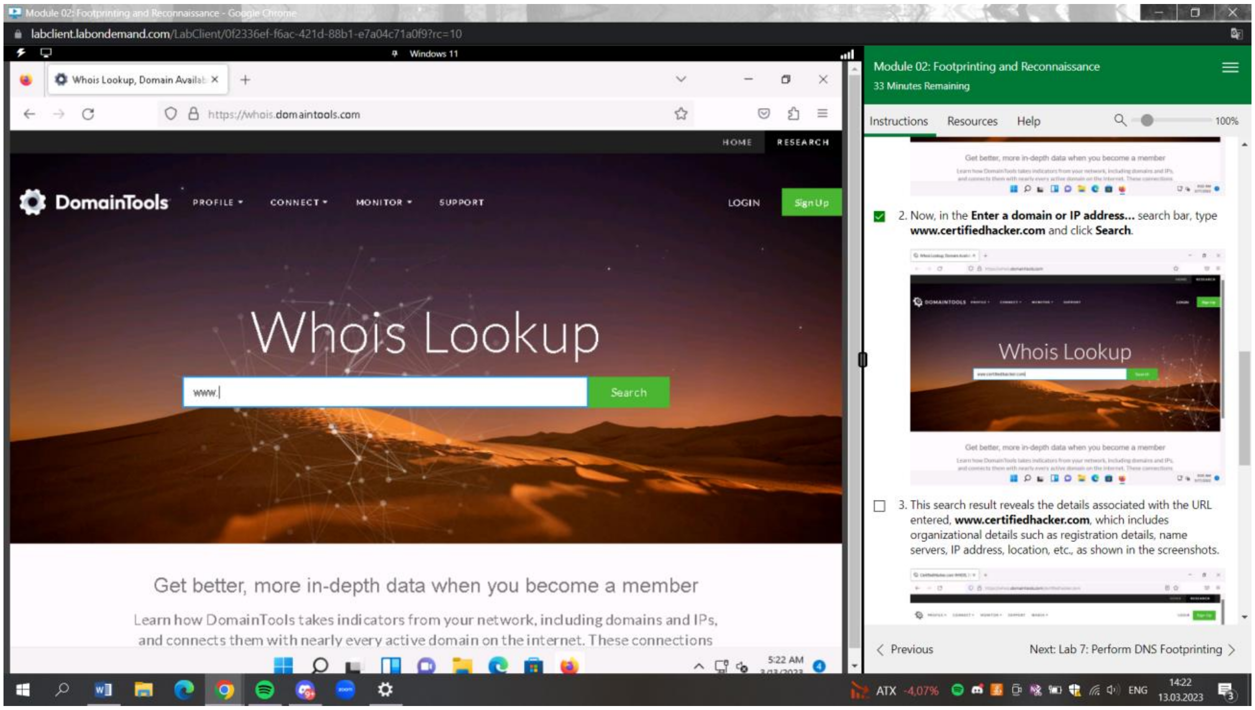
35 Minutes Remaining

☑ 11. Copy the entire email header text and paste it into the **Email headers:** field of eMailTrackerPro, and click **Trace**.

Here, we are analyzing the email header from gmail account. However, you can also analyze the email header from outlook account.

□ 12. The **My Trace Reports** window opens.

Lab6:



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

Whois Lookup, Domain Availab

https://whois.domaintools.com

Get better, more in-depth data when you become a member

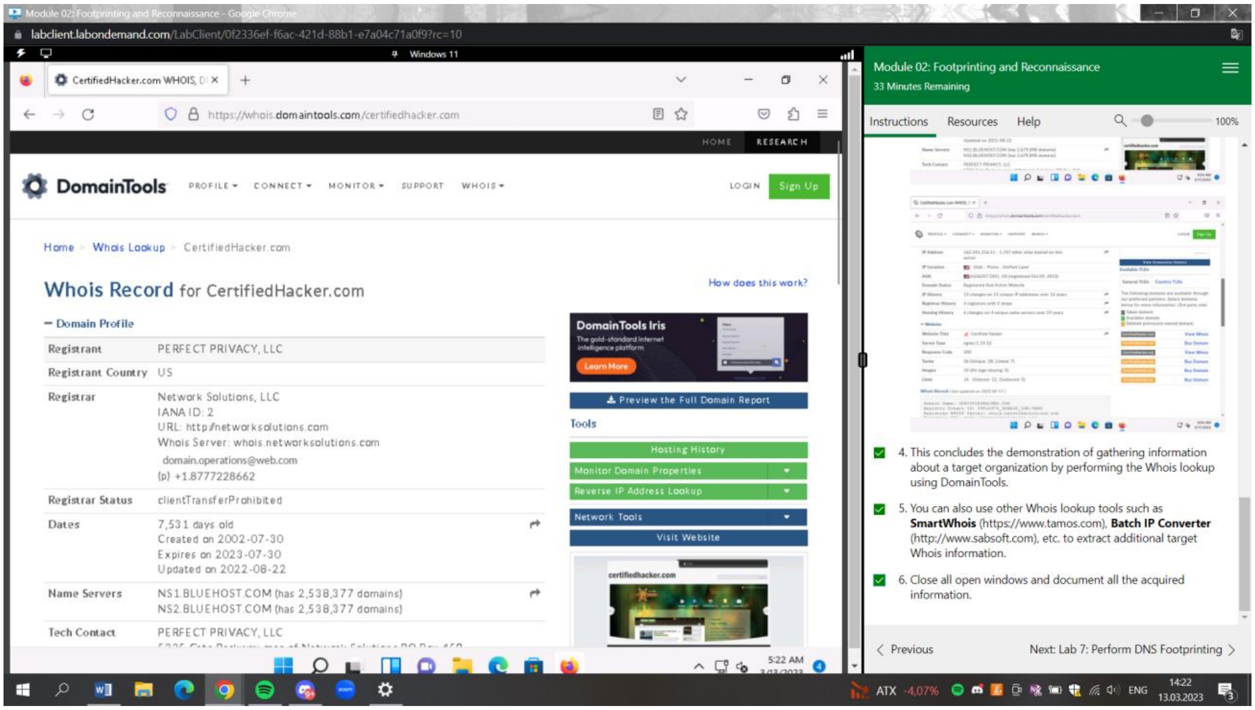
Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections

Module 02: Footprinting and Reconnaissance

33 Minutes Remaining

☑ 2. Now, in the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.

□ 3. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.


Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Windows 11
CertifiedHacker.com WHOIS, D
https://whois.domaintools.com/certifiedhacker.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
WHOIS
LOGIN
Sign Up
Home
Whois Lookup
CertifiedHacker.com
How does this work?
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website
certifiedhacker.com
5:22 AM
Module 02: Footprinting and Reconnaissance
33 Minutes Remaining
Instructions
Resources
Help
100%
ATX -4,07%
ENG
14:22
13.03.2023

Whois Record for CertifiedHacker.com

– Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	US
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	7,531 days old Created on 2002-07-30 Expires on 2023-07-30 Updated on 2022-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,538,377 domains) NS2.BLUEHOST.COM (has 2,538,377 domains)
Tech Contact	PERFECT PRIVACY, LLC

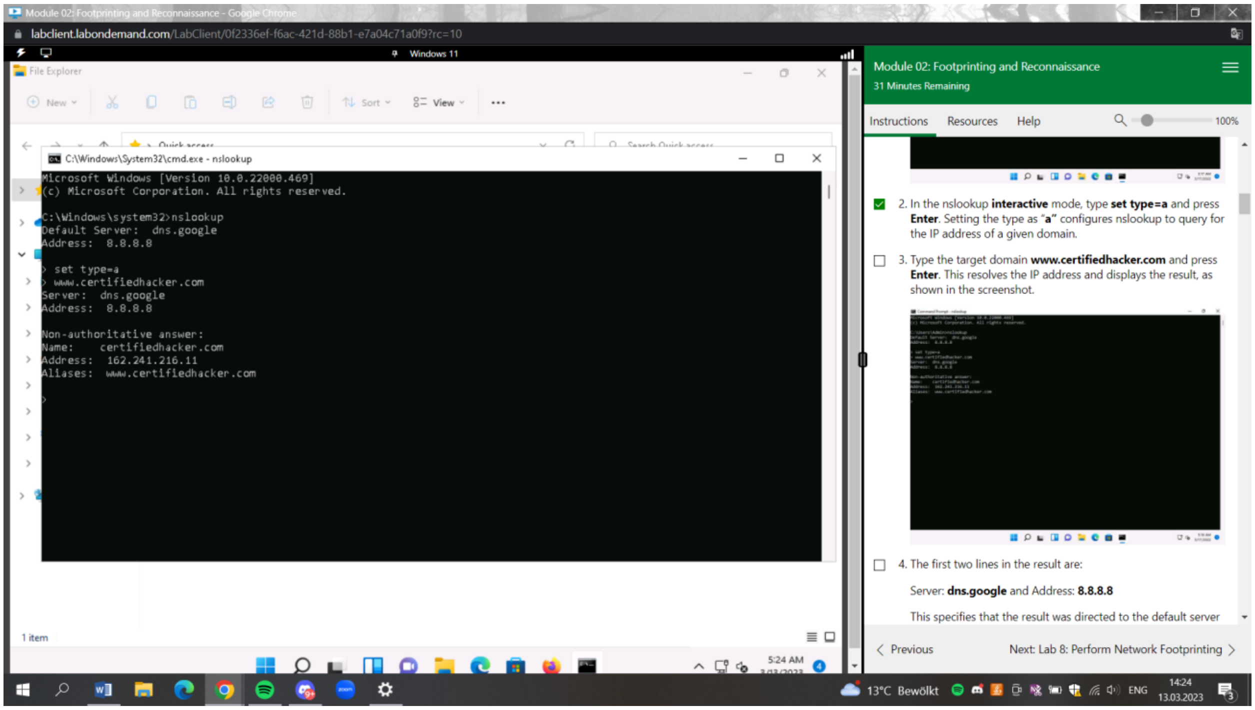
☑ 4. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.

☑ 5. You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.

☑ 6. Close all open windows and document all the acquired information.

< Previous   Next: Lab 7: Perform DNS Footprinting >

Lab7:


Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Windows 11
File Explorer
New
Sort
View
Quick access
Search Quick access
1 item
C:\Windows\System32\cmd.exe - nslookup
5:24 AM
Module 02: Footprinting and Reconnaissance
31 Minutes Remaining
Instructions
Resources
Help
100%
13°C Bewölkt
ENG
14:24
13.03.2023

```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com

>
```

☑ 2. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as "**a**" configures nslookup to query for the IP address of a given domain.

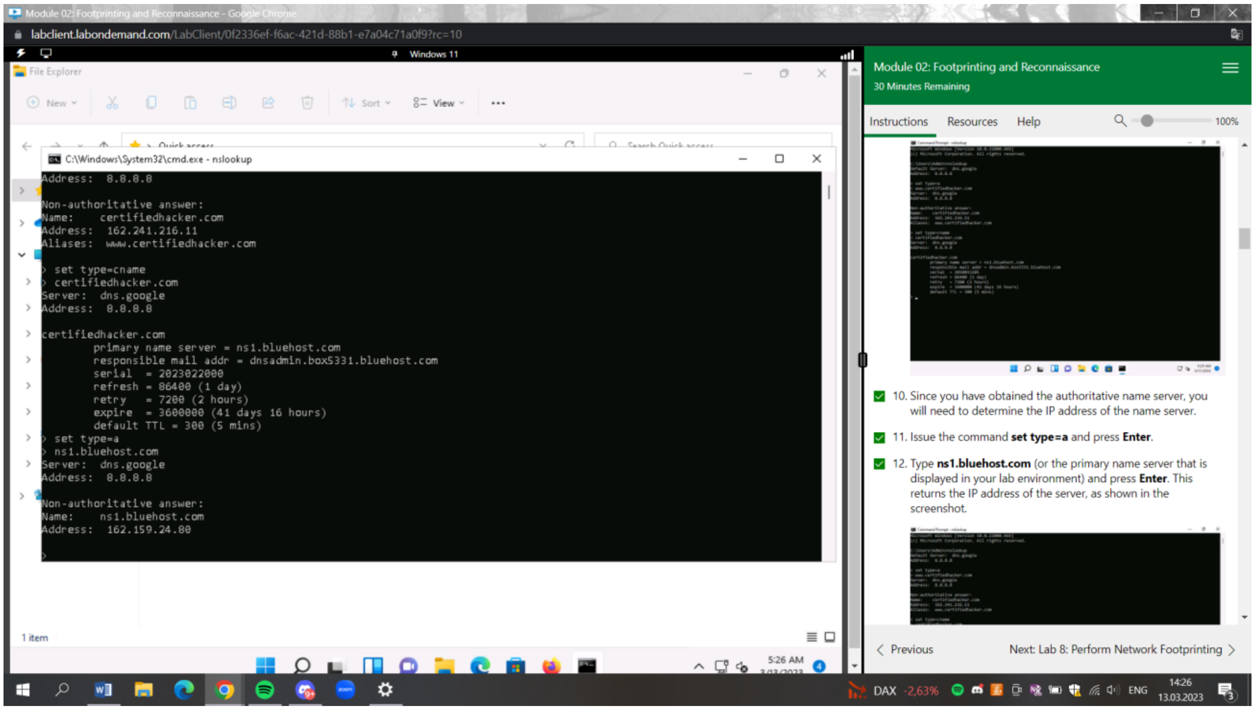
□ 3. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.

□ 4. The first two lines in the result are:

Server: **dns.google** and Address: **8.8.8.8**

This specifies that the result was directed to the default server

< Previous   Next: Lab 8: Perform Network Footprinting >



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

C:\Windows\System32\cmd.exe - nslookup

```
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2023022000
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> set type=a
> ns1.bluehost.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    ns1.bluehost.com
Address:  162.159.24.80

>
```

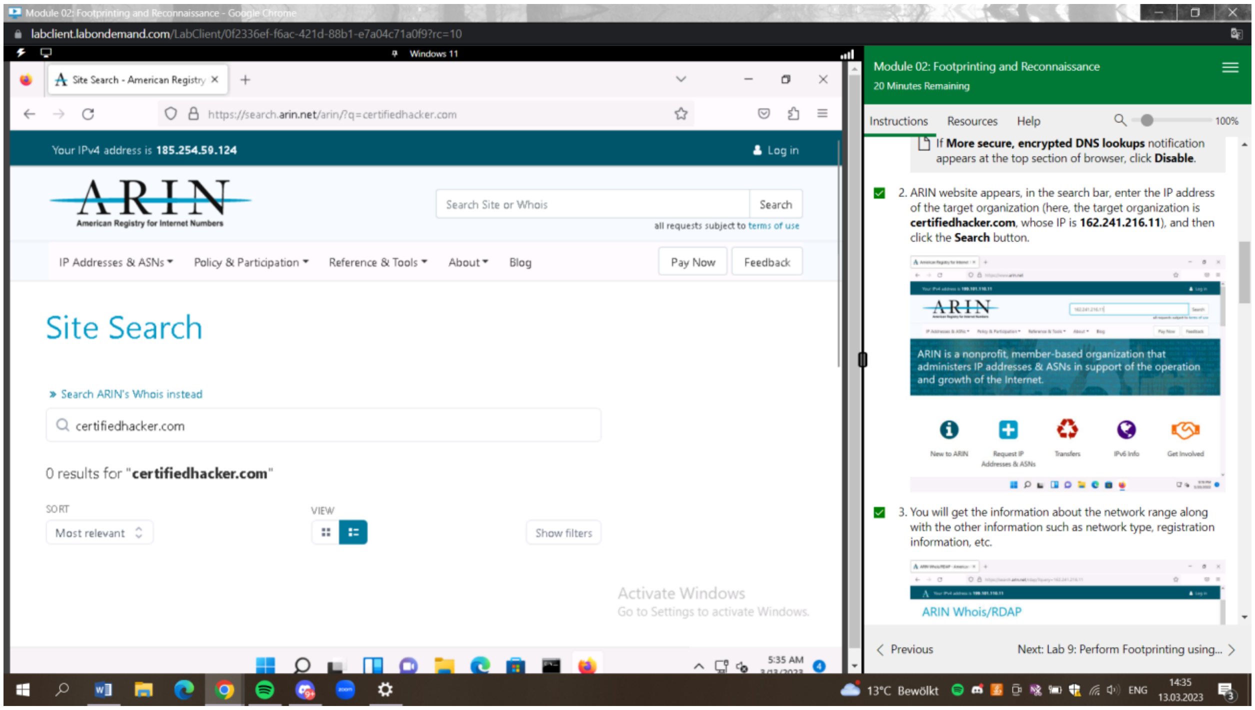
Module 02: Footprinting and Reconnaissance
30 Minutes Remaining

☑ 10. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

☑ 11. Issue the command **set type=a** and press **Enter**.

☑ 12. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.

Lab8:



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

https://search.arin.net/arin/?q=certifiedhacker.com

Your IPv4 address is **185.254.59.124**

Site Search

» Search ARIN's Whois instead

certifiedhacker.com

0 results for "**certifiedhacker.com**"

SORT: Most relevant

Module 02: Footprinting and Reconnaissance
20 Minutes Remaining

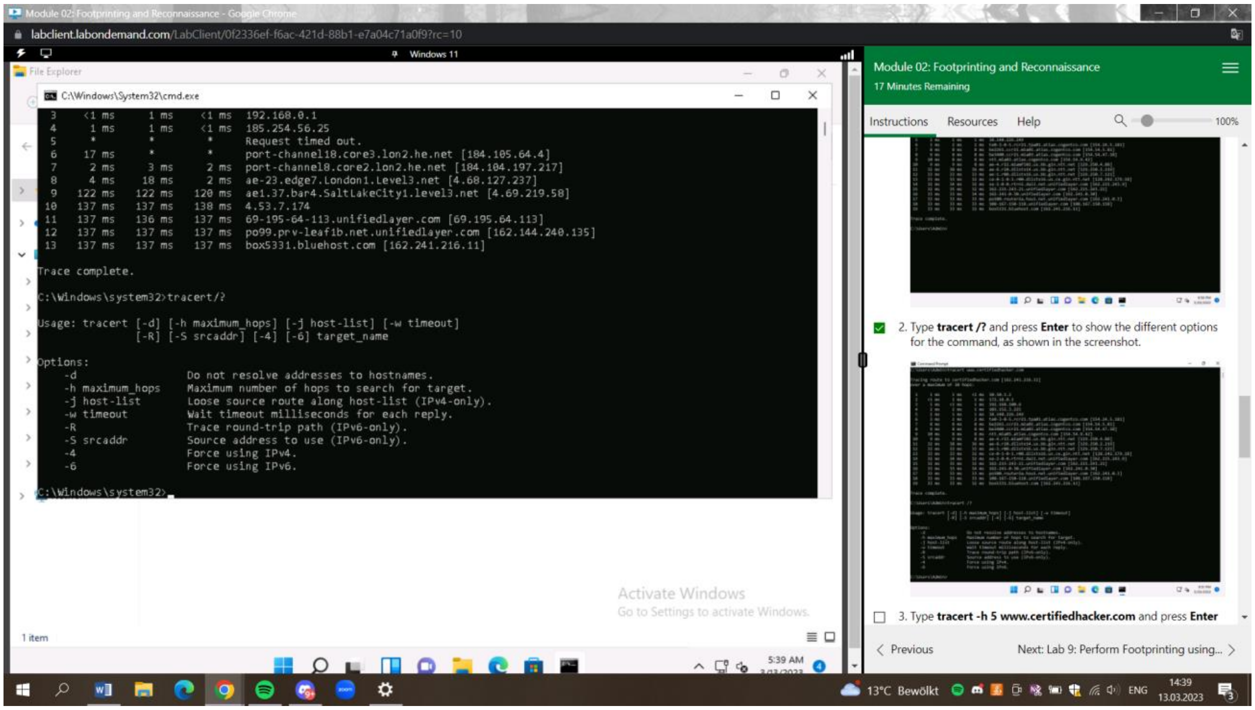
If **More secure, encrypted DNS lookups** notification appears at the top section of browser, click **Disable**.

☑ 2. ARIN website appears, in the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet.

☑ 3. You will get the information about the network range along with the other information such as network type, registration information, etc.

ARIN Whois/RDAP



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

C:\Windows\System32\cmd.exe

```
  3    <1 ms     1 ms    <1 ms  192.168.0.1
  4     1 ms     1 ms    <1 ms  185.254.56.25
  5     *        *        *     Request timed out.
  6    17 ms     *        *     port-channel18.core3.lon2.he.net [184.105.64.4]
  7     2 ms     3 ms     2 ms  port-channel8.core2.lon2.he.net [184.104.197.217]
  8     4 ms    18 ms     2 ms  ae-23.edge7.London1.Level3.net [4.68.127.237]
  9   122 ms   122 ms   120 ms  ae1.37.bar4.SaltLakeCity1.level3.net [4.69.219.58]
 10   137 ms   137 ms   138 ms  4.53.7.174
 11   137 ms   136 ms   137 ms  69-195-64-113.unifiedlayer.com [69.195.64.113]
 12   137 ms   137 ms   137 ms  po99.prv-leaf1b.net.unifiedlayer.com [162.144.240.135]
 13   137 ms   137 ms   137 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Windows\system32>tracert/?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Windows\system32>
```

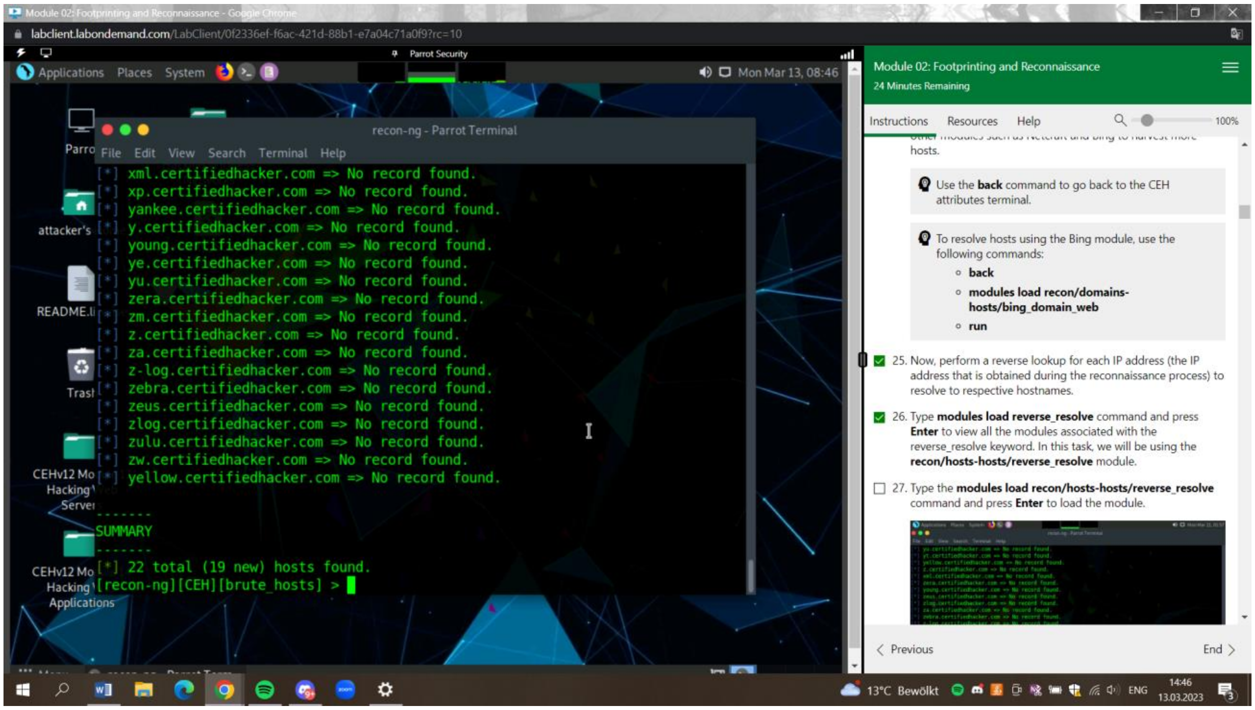
Module 02: Footprinting and Reconnaissance

17 Minutes Remaining

☑ 2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

□ 3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter**

Lab9:



Module 02: Footprinting and Reconnaissance - Google Chrome

labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10

recon-ng - Parrot Terminal

```
[*] xml.certifiedhacker.com => No record found.
[*] xp.certifiedhacker.com => No record found.
[*] yankee.certifiedhacker.com => No record found.
[*] y.certifiedhacker.com => No record found.
[*] young.certifiedhacker.com => No record found.
[*] ye.certifiedhacker.com => No record found.
[*] yu.certifiedhacker.com => No record found.
[*] zera.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.
[*] z.certifiedhacker.com => No record found.
[*] za.certifiedhacker.com => No record found.
[*] z-log.certifiedhacker.com => No record found.
[*] zebra.certifiedhacker.com => No record found.
[*] zeus.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] zulu.certifiedhacker.com => No record found.
[*] zw.certifiedhacker.com => No record found.
[*] yellow.certifiedhacker.com => No record found.

-------
SUMMARY
-------
[*] 22 total (19 new) hosts found.
[recon-ng][CEH][brute_hosts] >
```

Module 02: Footprinting and Reconnaissance

24 Minutes Remaining

other modules such as Netcraft and Bing to harvest more hosts.

Use the **back** command to go back to the CEH attributes terminal.

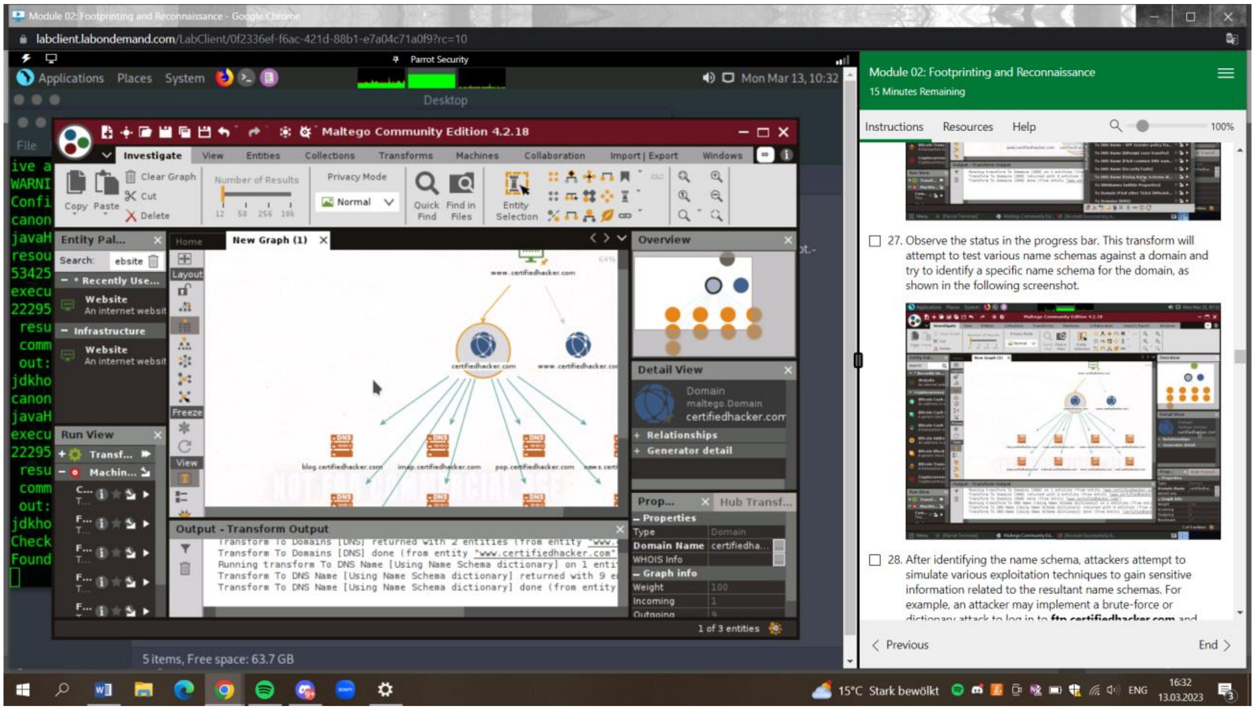
To resolve hosts using the Bing module, use the following commands:

- **back**
- **modules load recon/domains-hosts/bing_domain_web**
- **run**

☑ 25. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

☑ 26. Type **modules load reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse_resolve** module.

□ 27. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.


Module 02: Footprinting and Reconnaissance - Google Chrome
labclient.labondemand.com/LabClient/0f2336ef-f6ac-421d-88b1-e7a04c71a0f9?rc=10
Parrot Security
Applications Places System
Mon Mar 13, 10:32
Maltego Community Edition 4.2.18
Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows
Entity Palette
Run View
New Graph (1)
Overview
Detail View
www.certifiedhacker.com
certifiedhacker.com
blog.certifiedhacker.com
imap.certifiedhacker.com
pop.certifiedhacker.com
Domain Name certifiedha...
1 of 3 entities
5 items, Free space: 63.7 GB
Module 02: Footprinting and Reconnaissance
15 Minutes Remaining
Instructions Resources Help
100%
Previous
End
15°C Stark bewölkt
ENG
16:32
13.03.2023

```
Output - Transform Output
Transform To Domains [DNS] returned with 2 entities (from entity "www.
Transform To Domains [DNS] done (from entity "www.certifiedhacker.com"
Running transform To DNS Name [Using Name Schema dictionary] on 1 enti
Transform To DNS Name [Using Name Schema dictionary] returned with 9 e
Transform To DNS Name [Using Name Schema dictionary] done (from entity
```

□ 27. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.

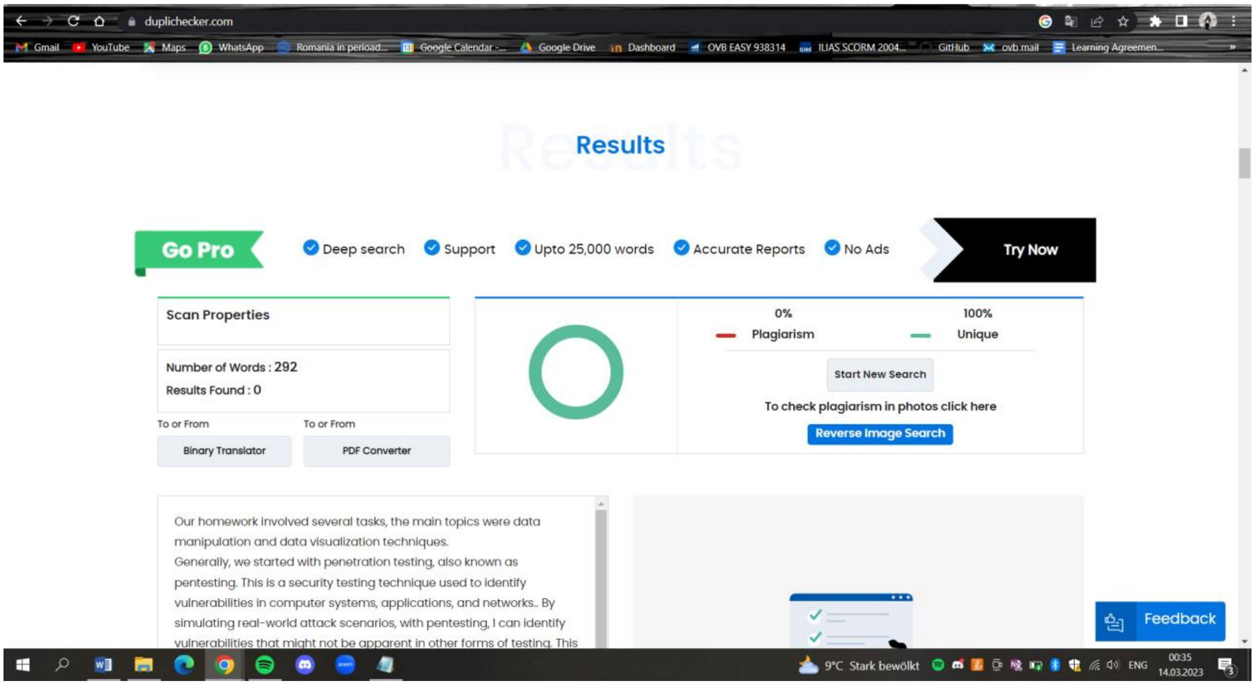
□ 28. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and

Our homework involved several tasks, the main topics were data manipulation and data visualization techniques.

Generally, we started with penetration testing, also known as pentesting. This is a security testing technique used to identify vulnerabilities in computer systems, applications, and networks. By simulating real-world attack scenarios, with pentesting, I can identify vulnerabilities that might not be apparent in other forms of testing. This makes it an important tool for enhancing the security of websites and software applications. For example, we used Parrot Security OS. This is a popular Linux distribution used by security professionals and hackers for penetration testing, digital forensics, and other security-related tasks. The Parrot Security OS command prompt provides users with a wide range of tools and utilities that can be used to perform a variety of tasks. Our iLab assignment introduced us to Footprinting and Google Hacking by helping us gather information about users, shares, and passwords all across the world, also taught us how to exploit Metadata and gain access to some target systems. It developed our practical experience with Google Hacking by using some ethical hacking techniques and tools and taught me how to identify and prevent some potential risks.

Ethically, the goal of it is to legitimately identify security weaknesses and vulnerabilities that could be exploited by attackers to gain unauthorized access, steal data, or cause other types of damage. Pen testing can be conducted on websites, software applications, and computer networks to identify potential security risks and recommend remedial actions.

Honestly, I was not familiar with all those information and tools we used, all were a bit new for me, but I enjoyed doing the iLab and I would like to learn more about this subject. It took me almost four hours, but I liked working on it and it surprised me how well it was structured.

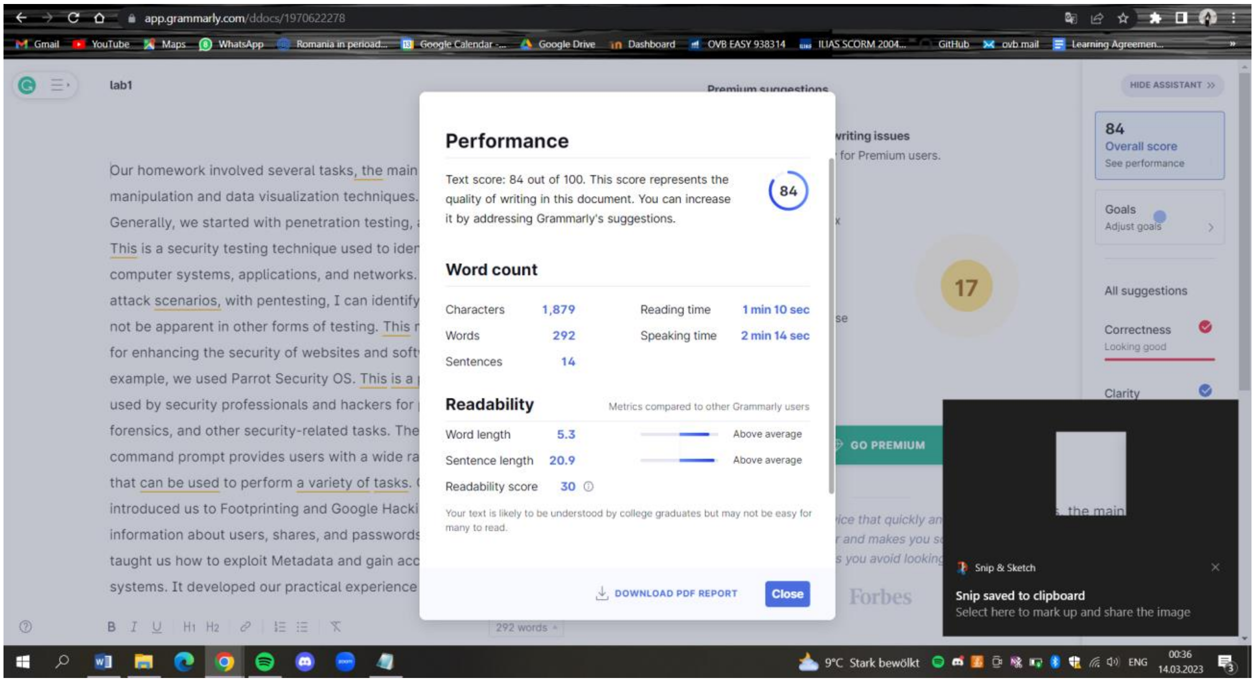


Scan Properties

Number of Words : 292
Results Found : 0

0% Plagiarism
100% Unique

Our homework involved several tasks, the main topics were data manipulation and data visualization techniques.
Generally, we started with penetration testing, also known as pentesting. This is a security testing technique used to identify vulnerabilities in computer systems, applications, and networks.. By simulating real-world attack scenarios, with pentesting, I can identify vulnerabilities that might not be apparent in other forms of testing. This



Our homework involved several tasks, the main
manipulation and data visualization techniques.
Generally, we started with penetration testing,
This is a security testing technique used to iden
computer systems, applications, and networks.
attack scenarios, with pentesting, I can identify
not be apparent in other forms of testing. This r
for enhancing the security of websites and soft
example, we used Parrot Security OS. This is a
used by security professionals and hackers for
forensics, and other security-related tasks. The
command prompt provides users with a wide ra
that can be used to perform a variety of tasks.
introduced us to Footprinting and Google Hacki
information about users, shares, and passwords
taught us how to exploit Metadata and gain acc
systems. It developed our practical experience

Performance

Text score: 84 out of 100. This score represents the quality of writing in this document. You can increase it by addressing Grammarly's suggestions.

84

Word count

Characters	1,879	Reading time	1 min 10 sec
Words	292	Speaking time	2 min 14 sec
Sentences	14		

Readability

Metrics compared to other Grammarly users

Word length	5.3	Above average
Sentence length	20.9	Above average
Readability score	30	

Your text is likely to be understood by college graduates but may not be easy for many to read.

DOWNLOAD PDF REPORT

Close