

## Module 02: Ethical Hacking Fundamentals

### Scenario

Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security. It focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system's security. Ethical hackers perform security assessments for an organization with the permission of concerned authorities.

The labs in this module will give you real-time experience in understanding different phases of hacking cycle.

### Objective

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- **Organization Information** Employee details, partner details, weblinks, web technologies, patents, trademarks, etc.
- **Network Information** Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information
- **System Information** Operating systems, web server OSES, user accounts and passwords, etc.

### Overview of Ethical Hacking

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities.

White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking.

Nowadays, most organizations (such as private companies, universities, and government organizations) are hiring White Hats to assist them in enhancing their cybersecurity. They perform hacking in ethical ways, with the permission of the network or system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system.

### Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

1. Perform passive footprinting to gather information about a target
  - Gather information using advanced google hacking techniques
  - Extract a company's data using Web Data Extractor
  - Perform whois lookup using DomainTools
2. Perform network scanning to identify live hosts, open ports and services and target OS in the network
  - Perform network tracerouting in Windows and Linux machines
  - Perform host discovery using Nmap
  - Perform port and service discovery using MegaPing
  - Perform OS discovery using Unicornscan
3. Perform enumeration on a system or network to extract usernames, machine names, network resources, shares, etc.
  - Perform NetBIOS enumeration using Windows Command-Line utilities
  - Perform NetBIOS enumeration using NetBIOS Enumerator

#### Lab 1: Perform Passive Footprinting to Gather Information About a Target

##### **Lab Scenario**

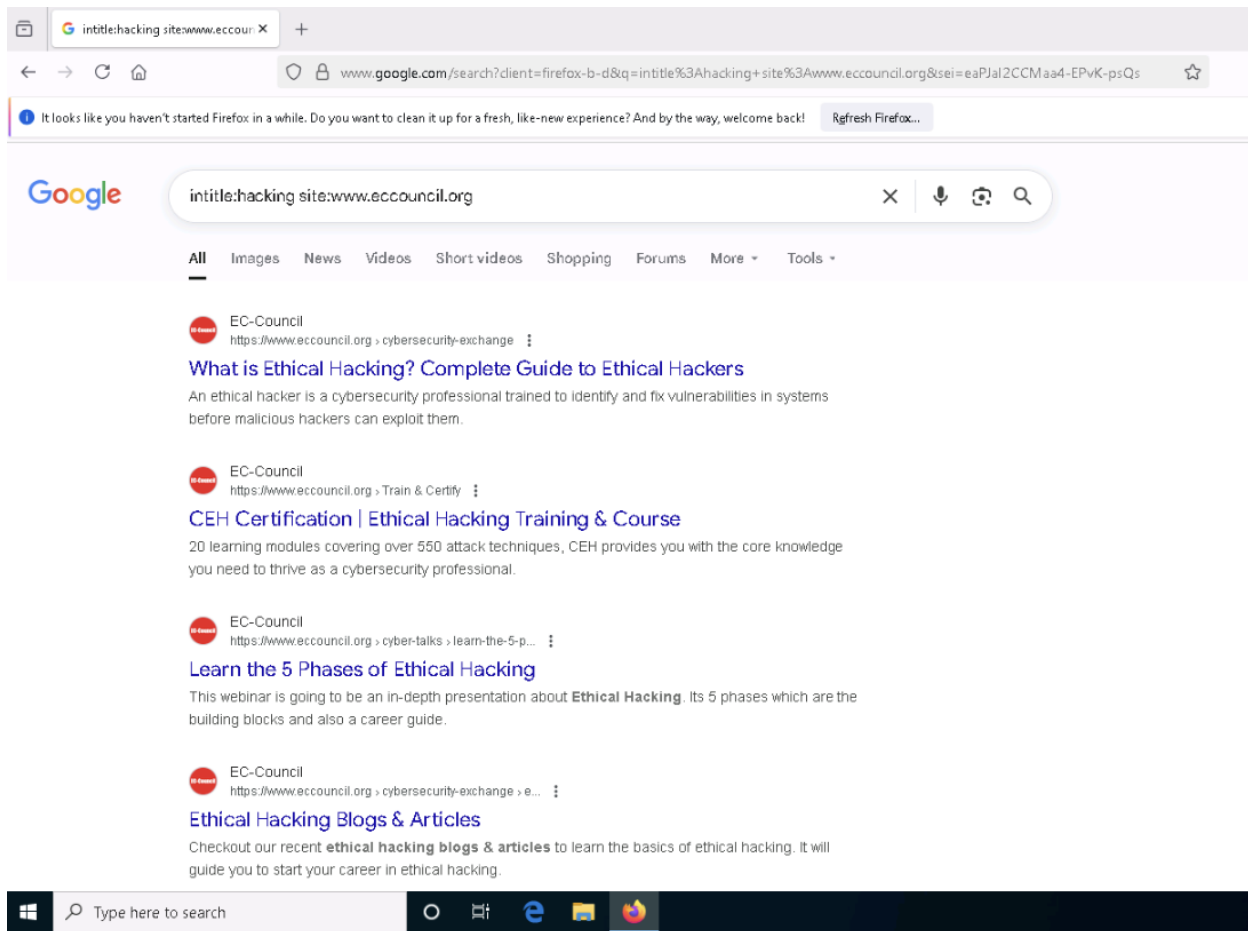
Passive footprinting involves gathering information about the target without direct interaction. It is mainly useful when the information gathering activities are not to be detected by the target. Performing passive footprinting is technically difficult, as active traffic is not sent to the target organization from a host or anonymous hosts or services over the Internet. We can only collect archived and stored information about the target using search engines, social networking sites, and so on.

##### **Lab Objectives**

- Gather Information using Advanced Google Hacking Techniques
- Extract a Company's Data using Web Data Extractor
- Perform Whois Lookup using DomainTools

## 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. Note: Here, we will consider EC-Council as a target organization.



Ec-Council filetype:pdf - Google

← → ↺ 🏠

🔒 www.google.com/search?q=Ec-Council+filetype%3Apdf&client=firefox-b-d&sa\_esv=4e89ca1d2fd0e141&ei=3KPJaPibFuGjuMPgve: ⭐

🔍

🔔 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...](#)

Ec-Council filetype:pdf

✕ 🔊 🔄 🔍

All Images News Videos Shopping Short videos Maps More Tools

EC-Council  
https://www.eccouncil.org › uploads › 2023/02 PDF

**Cyber-Handbook-Enterprise-2.pdf**  
EC-Council creates content (course materials and exams) and certification delivered through our channel of authorized training centers which.

People also ask

What is the EC-Council?

Is EC-Council certification good?

What is the EC-Council scandal?

Is EC-Council better than CompTIA?

[Feedback](#)

EC-Council  
https://www.eccouncil.org › uploads › 2025/07 PDF

**Certified Ethical Hacker Hall of Fame 2025 Industry Report**  
EC-Council is the creator of the Certified Ethical Hacker (CEH) program and a leader in cybersecurity education. Founded in 2001, EC-Council's mission is to ...

🪟 🔍 Type here to search

allinurl: ethical hacking - Google

← → ↻ 🏠

www.google.com/search?q=allinurl%3A+ethical+hacking&scas\_esv=4e89ca1d2fd0e141&source=hp&ei=t6PJaJu-KJyb4-EPzZeaoA8&...

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...

Google

allinurl: ethical hacking

×

🔍

All

Images

Videos

Short videos


News

Shopping

Forums


More

Tools




EC-Council  
<https://www.eccouncil.org/cybersecurity-exchange>

**What is Ethical Hacking? Complete Guide to Ethical Hackers**  
Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an ...




IBM  
<https://www.ibm.com/think/topics/ethical-hacking>

**What is Ethical Hacking? | IBM**  
Ethical hacking is the **use of hacking techniques by friendly parties** in an attempt to uncover, understand and fix security vulnerabilities in a network or ...



Online Courses Australia  
<https://www.onlinecoursesaustralia.edu.au/the-phases-...>


**The 5 Phases of Ethical Hacking Explained**  
Ethical hacking involves **legally assessing the security of computer systems, networks, and applications** to identify vulnerabilities that could be exploited by ...



Imperva  
<https://www.imperva.com/Home/AppSec>

**What is Ethical (White Hat) Hacking | CEH Certification**  
An ethical hacker ("white hat hacker") is an **information security professional who has the same skills** and uses the same technologies as a malicious hacker.

**Certified ethical hacker**



**Certified Ethical Hacker**  
Council and obtained by assessing the security of vulnerabilities in target s

Source: [Wikipedia](#)

**Focus:** Ethical hacking

**Issuing Organization:**

Turn On Wi  
Automatica  
Documents  
OneDrive sc  
protected a  
OneDrive

Remind me again in:  
1 Week  
Let's get started

related:www.eccouncil.org - Google

← → ↻ 🏠

🔒 www.google.com/search?q=related%3Awww.eccouncil.org&scas\_esv=4e89ca1d2fd0e141&source=hp&ei=t6PJaJu-KJyb4-EPzZeaoAB: ⭐


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...

Google

related:www.eccouncil.org

✕ 🔊 📷 🔍

All Images News Short videos Videos Shopping Forums More ▾ Tools ▾

 EC-Council  
https://www.eccouncil.org

**EC-Council: Best Cyber Security Courses Online | Cybersecurity ...**  
Enroll in the best cyber security courses online by **EC-Council**. Boost your career with one of the top cybersecurity training program. Get certified now!

Login

Get started with a free account and gain immediate access to 20+ ...

➤

Free Cybersecurity Courses

EC-Council offers a free cyber security course online for ...

➤

Cybersecurity Certification

Explore EC-Council Cybersecurity Certifications - Top Cyber ...

➤

Certified Ethical Hacker v13

Earn your ethical hacking certification with EC-Council's ...

➤

View Our Courses


EC-Council iLearn provides advanced Cyber Security ...

➤

More results from eccouncil.org »

Windows taskbar

Type here to search 🔍

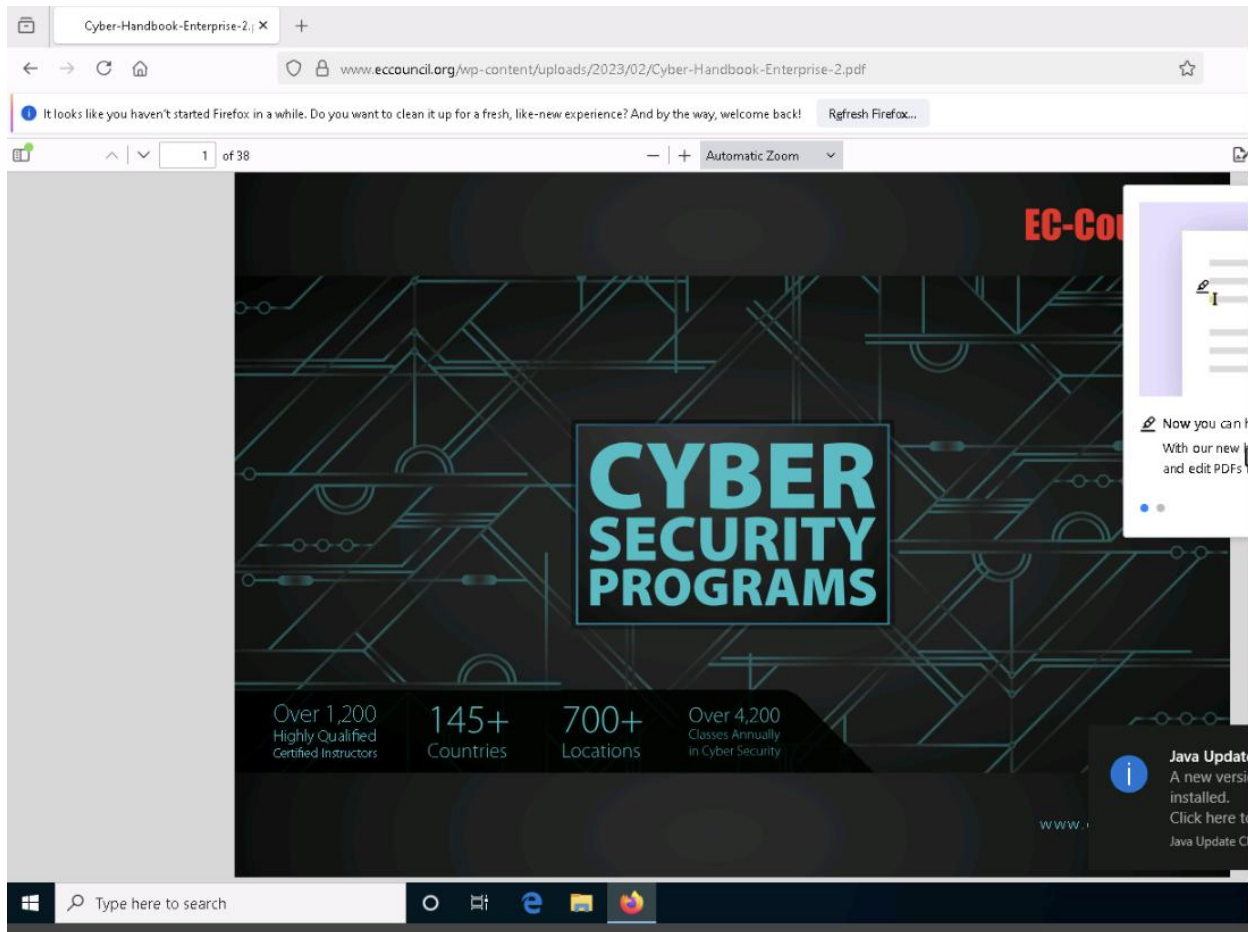


Turn On Windows Security

Automatic updates  
Documents  
OneDrive sync  
protected app  
OneDrive

Remind me again in:  
1 Week

Let's get started

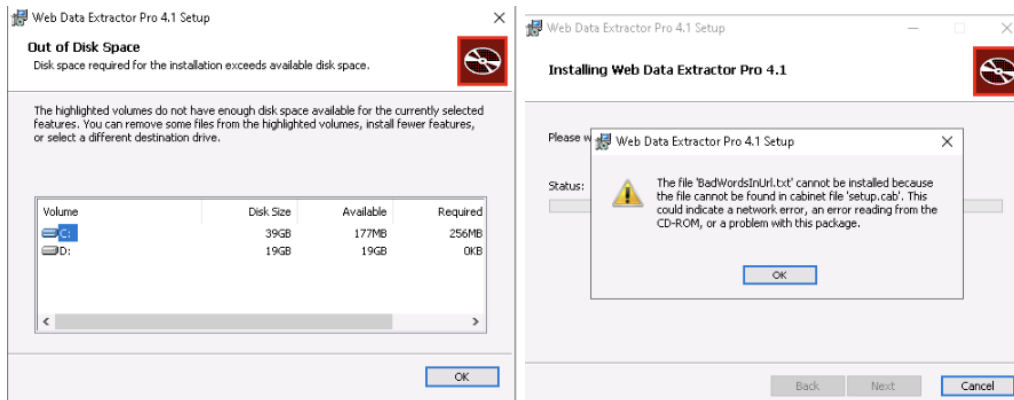


## Task 2: Extract a Company's Data using Web Data Extractor

Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion, directories, web research, etc. are important sources of information for an ethical hacker. Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

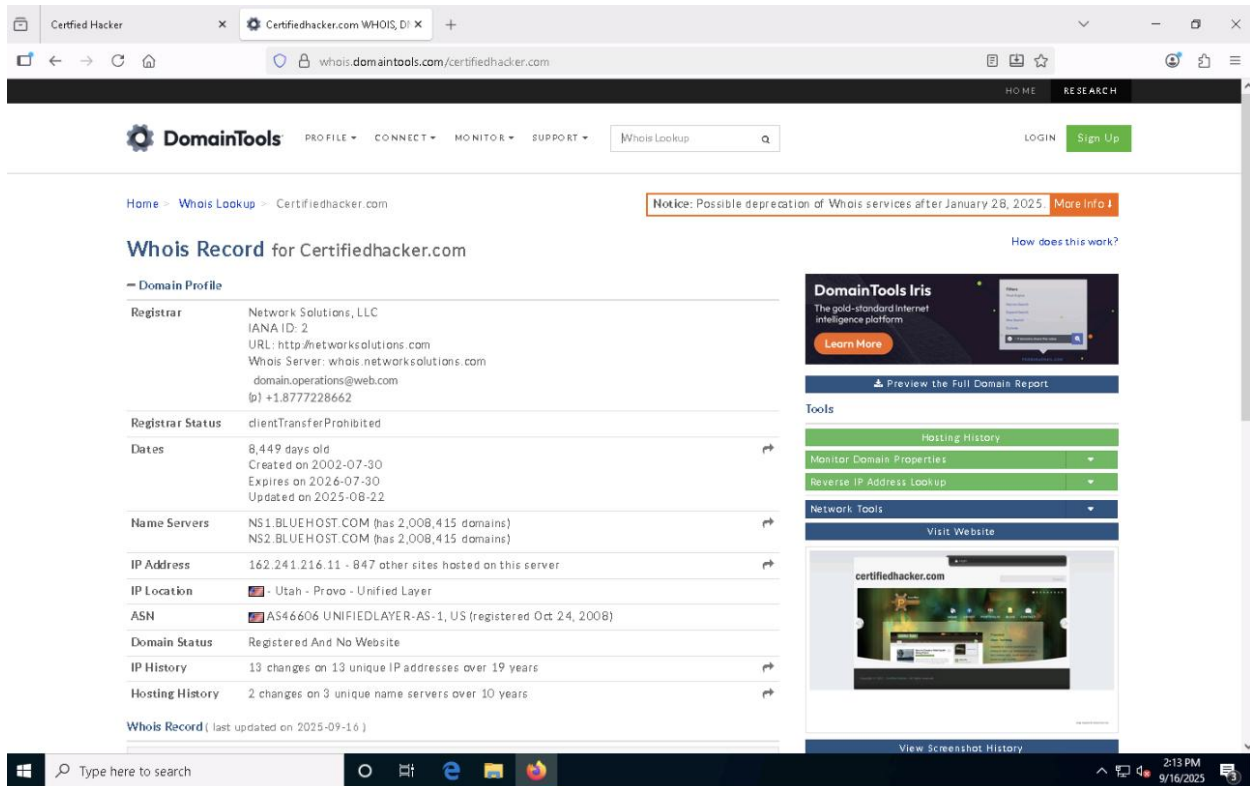
Here, we will gather the target company's data using the Web Data Extractor tool.

Could not use Web Data Extractor tool (see below screenshots).



### Task 3: Perform Whois Lookup using DomainTools

Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates). Here, we will gather target information by performing Whois lookup using DomainTools.





## Lab 2: Perform Network Scanning to Identify Live Hosts, Open Ports and Services and Target OS in the Network

### Lab Scenario

Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine. It is one of the most important phases of intelligence gathering for an attacker, which enables him/her to create a profile of the target organization. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

### Lab Objectives

- Perform Network Tracerouting in Windows and Linux Machines
- Perform Host Discovery using Nmap
- Perform Port and Service Discovery using MegaPing
- Perform OS Discovery using Unicornscan

### Task 1: Perform Network Tracerouting in Windows and Linux Machines

The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

Here, we will perform network tracerouting using both Windows and Linux machines.

```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1  3 ms  1 ms  1 ms  10.10.1.1
  2  10 ms  9 ms  10 ms  172.18.0.1
  3  7 ms  11 ms  10 ms  192.168.0.29
  4  27 ms  26 ms  25 ms  103.18.87.33
  5  6 ms  10 ms  *  63.222.112.64
  6  *  *  *  Request timed out.
  7  3 ms  3 ms  3 ms  63.216-144-10.static.as3491.net [63.216.144.10]
  8  3 ms  *  3 ms  ae-2.r24.sngps107.sg.bb.gln.ntt.net [129.250.6.62]
  9  *  *  *  Request timed out.
 10 172 ms 172 ms 172 ms ae-1.r26.lsanca07.us.bb.gln.ntt.net [129.250.2.176]
 11 104 ms 102 ms 103 ms ae-2.a03.lsanca07.us.bb.gln.ntt.net [129.250.3.91]
 12 179 ms 180 ms 179 ms ce-3-0-1.a03.lsanca07.us.ce.gln.ntt.net [168.143.228.173]
 13 188 ms 187 ms 188 ms 162-215-195-144.unifiedlayer.com [162.215.195.144]
 14 192 ms 192 ms 192 ms 69-195-64-113.unifiedlayer.com [69.195.64.113]
 15 193 ms 193 ms 194 ms po99.prv-leafib.net.unifiedlayer.com [162.144.240.135]
 16 198 ms 197 ms 197 ms box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>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:\Users\Admin>
```

```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1  1 ms  <1 ms  <1 ms  10.10.1.1
  2  1 ms  1 ms  1 ms  172.18.0.1
  3  2 ms  1 ms  3 ms  192.168.0.29
  4  3 ms  3 ms  2 ms  103.18.87.33
  5  3 ms  3 ms  3 ms  63.222.112.64

Trace complete.

C:\Users\Admin>tracert -w 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1  1 ms  1 ms  1 ms  10.10.1.1
  2  1 ms  1 ms  1 ms  172.18.0.1
  3  2 ms  1 ms  1 ms  192.168.0.29
  4  3 ms  3 ms  2 ms  103.18.87.33
  5  3 ms  3 ms  3 ms  63.222.112.64
  6  *  3 ms  4 ms  Hu-0-0-0-2.br07.sin02.as3491.net [63.218.164.102]
  7  3 ms  3 ms  2 ms  63.216-144-10.static.as3491.net [63.216.144.10]
  8  3 ms  3 ms  3 ms  ae-2.r24.sngps107.sg.bb.gln.ntt.net [129.250.6.62]
  9  *  *  *  Request timed out.
 10 172 ms 172 ms *  ae-1.r26.lsanca07.us.bb.gln.ntt.net [129.250.2.176]
 11 192 ms 192 ms *  ae-2.a03.lsanca07.us.bb.gln.ntt.net [129.250.3.91]
 12 198 ms 179 ms *  ce-3-0-1.a03.lsanca07.us.ce.gln.ntt.net [168.143.228.173]
 13 187 ms 187 ms *  162-215-195-144.unifiedlayer.com [162.215.195.144]
 14 192 ms 192 ms *  69-195-64-113.unifiedlayer.com [69.195.64.113]
 15 193 ms 193 ms *  po99.prv-leafib.net.unifiedlayer.com [162.144.240.135]
 16 198 ms 197 ms *  box5331.bluehost.com [162.241.216.11]
 17 197 ms 197 ms *  box5331.bluehost.com [162.241.216.11]
 18 197 ms 199 ms *  box5331.bluehost.com [162.241.216.11]
 19 197 ms 197 ms *  box5331.bluehost.com [162.241.216.11]
 20 197 ms 198 ms *  box5331.bluehost.com [162.241.216.11]
 21 197 ms 198 ms *  box5331.bluehost.com [162.241.216.11]
 22 199 ms 197 ms *  box5331.bluehost.com [162.241.216.11]
 23 198 ms 197 ms *  box5331.bluehost.com [162.241.216.11]
 24 197 ms 198 ms *  box5331.bluehost.com [162.241.216.11]
 25 199 ms 200 ms *  box5331.bluehost.com [162.241.216.11]
 26 197 ms 197 ms *  box5331.bluehost.com [162.241.216.11]
 27 199 ms 199 ms *  box5331.bluehost.com [162.241.216.11]
 28 198 ms 207 ms *  box5331.bluehost.com [162.241.216.11]
 29 210 ms 199 ms *  box5331.bluehost.com [162.241.216.11]
 30 197 ms 207 ms *  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>
```

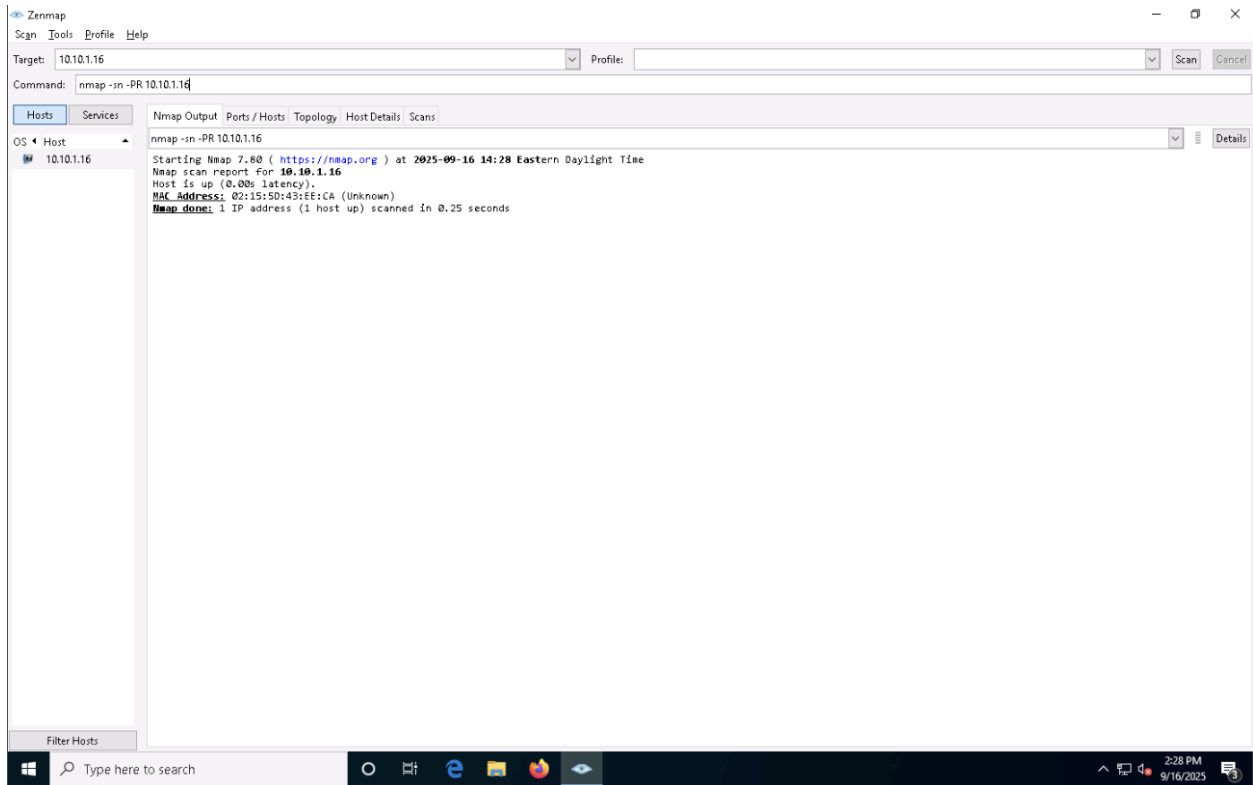
```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ traceroute www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1 10.10.1.1 (10.10.1.1) 1.908 ms 1.838 ms 1.790 ms
 2 172.18.0.1 (172.18.0.1) 2.605 ms 2.548 ms 2.503 ms
 3 192.168.0.29 (192.168.0.29) 2.482 ms 2.438 ms 2.392 ms
 4 103.18.87.33 (103.18.87.33) 18.605 ms 5.073 ms 5.021 ms
 5 63.222.112.64 (63.222.112.64) 13.091 ms 13.047 ms 3.894 ms
 6 * Hu-0-0-0-2.br07.sin02.as3491.net (63.218.164.102) 3.206 ms *
 7 63-216-144-10.static.as3491.net (63.216.144.10) 14.116 ms 17.242 ms 3.200 ms
 8 * ae-2.r24.sngpsi07.sg.bb.gin.ntt.net (129.250.6.62) 3.210 ms 9.736 ms
 9 ae-0.r25.sngpsi07.sg.bb.gin.ntt.net (129.250.6.61) 3.003 ms *
10 ae-1.r26.lsanca07.us.bb.gin.ntt.net (129.250.2.176) 168.857 ms 186.978 ms *
11 ae-2.a03.lsanca07.us.bb.gin.ntt.net (129.250.3.91) 193.134 ms 197.918 ms 212.447 ms
12 ce-3-0-1.a03.lsanca07.us.ce.gin.ntt.net (168.143.228.173) 186.719 ms 178.542 ms ae-3.a03.lsanca
07.us.bb.gin.ntt.net (129.250.3.245) 187.263 ms
13 162-215-195-144.unifiedlayer.com (162.215.195.144) 198.318 ms 208.077 ms ce-3-0-1.a03.lsanca07.
us.ce.gin.ntt.net (168.143.228.173) 179.153 ms
14 69-195-64-113.unifiedlayer.com (69.195.64.113) 207.839 ms 162-215-195-144.unifiedlayer.com (162.
215.195.144) 199.716 ms 69-195-64-111.unifiedlayer.com (69.195.64.111) 202.197 ms
15 69-195-64-113.unifiedlayer.com (69.195.64.113) 186.860 ms 186.814 ms po99.prv-leaf1b.net.unifie
dlayer.com (162.144.240.135) 211.598 ms
16 box5331.bluehost.com (162.241.216.11) 222.492 ms 195.880 ms po99.prv-leaf1b.net.unifiedlayer.co
m (162.144.240.135) 186.999 ms
[attacker@parrot]~$
```

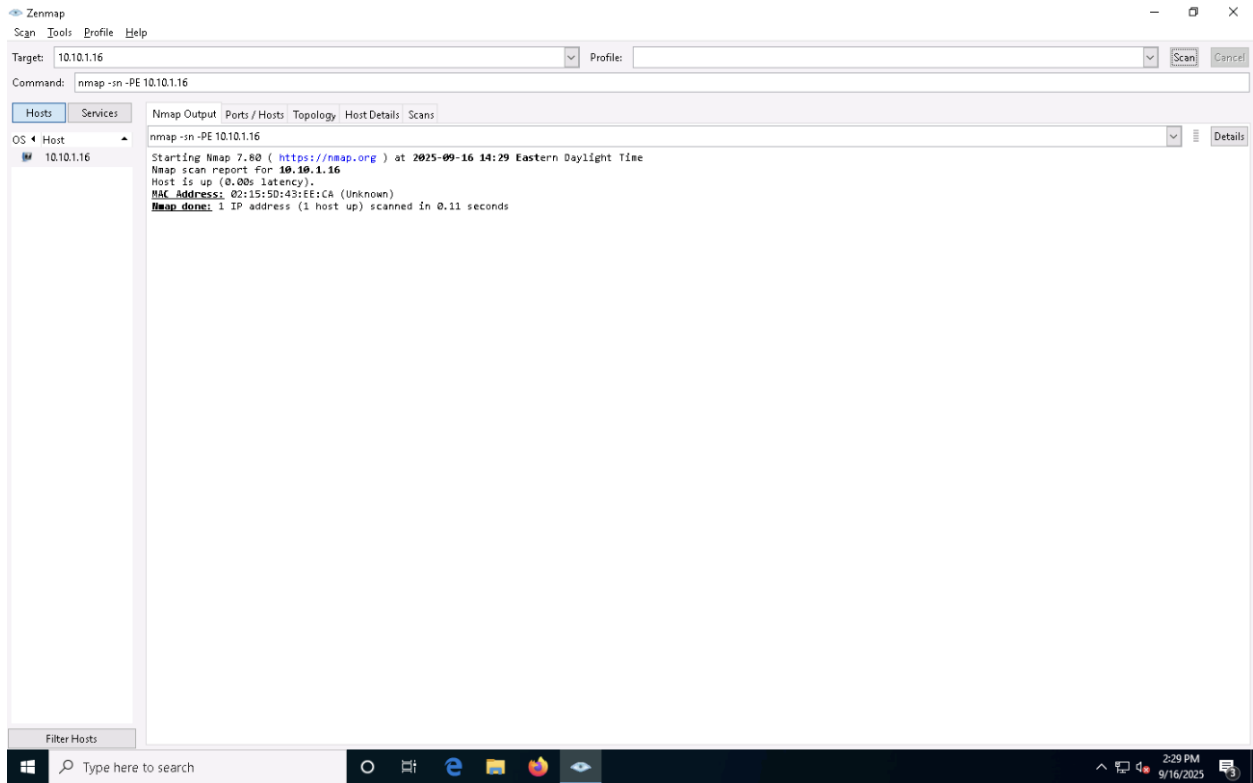
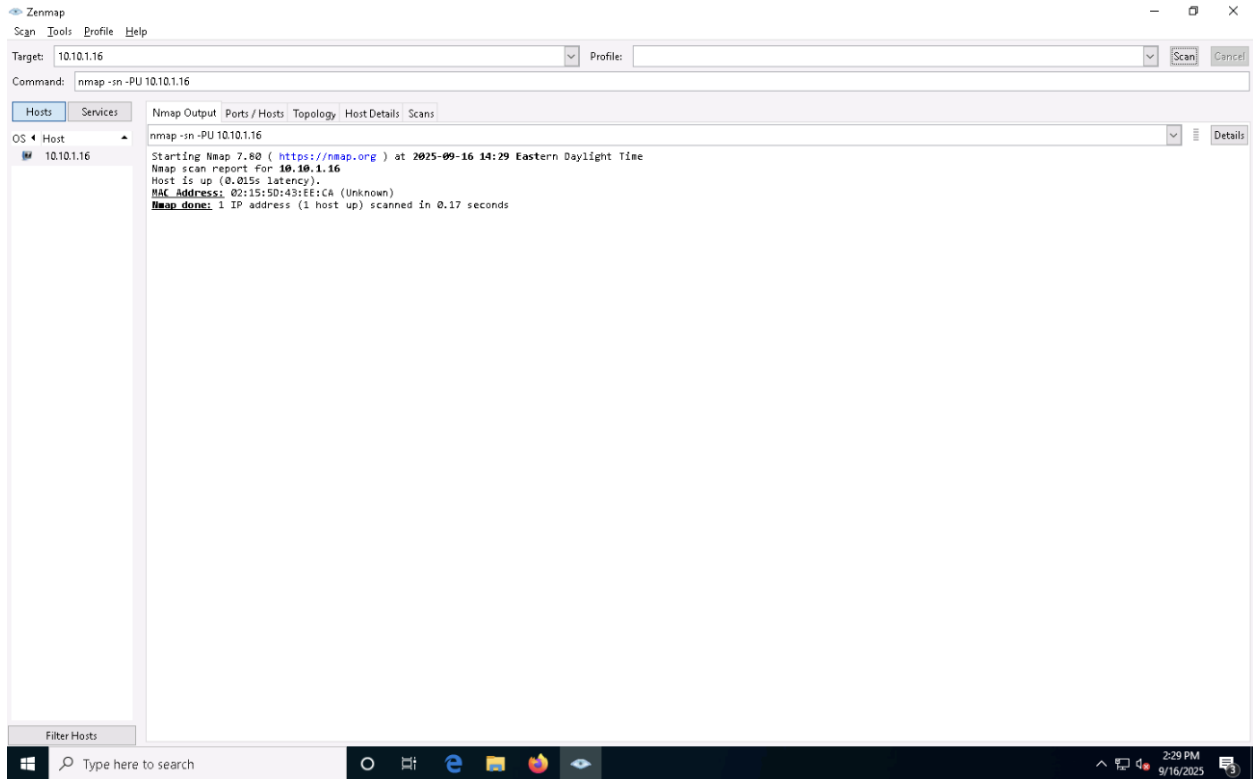
```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
5 63.222.112.64 (63.222.112.64) 13.091 ms 13.047 ms 3.894 ms
6 * Hu-0-0-0-2.br07.sin02.as3491.net (63.218.164.102) 3.206 ms *
7 63-216-144-10.static.as3491.net (63.216.144.10) 14.116 ms 17.242 ms 3.200 ms
8 * ae-2.r24.sngpsi07.sg.bb.gin.ntt.net (129.250.6.62) 3.210 ms 9.736 ms
9 ae-0.r25.sngpsi07.sg.bb.gin.ntt.net (129.250.6.61) 3.003 ms *
10 ae-1.r26.lsanca07.us.bb.gin.ntt.net (129.250.2.176) 168.857 ms 186.978 ms *
11 ae-2.a03.lsanca07.us.bb.gin.ntt.net (129.250.3.91) 193.134 ms 197.918 ms 212.447 ms
12 ce-3-0-1.a03.lsanca07.us.ce.gin.ntt.net (168.143.228.173) 186.719 ms 178.542 ms ae-3.a03.lsanca
07.us.bb.gin.ntt.net (129.250.3.245) 187.263 ms
13 162-215-195-144.unifiedlayer.com (162.215.195.144) 198.318 ms 208.077 ms ce-3-0-1.a03.lsanca07.
us.ce.gin.ntt.net (168.143.228.173) 179.153 ms
14 69-195-64-113.unifiedlayer.com (69.195.64.113) 207.839 ms 162-215-195-144.unifiedlayer.com (162.
215.195.144) 199.716 ms 69-195-64-111.unifiedlayer.com (69.195.64.111) 202.197 ms
15 69-195-64-113.unifiedlayer.com (69.195.64.113) 186.860 ms 186.814 ms po99.prv-leaf1b.net.unifie
dlayer.com (162.144.240.135) 211.598 ms
16 box5331.bluehost.com (162.241.216.11) 222.492 ms 195.880 ms po99.prv-leaf1b.net.unifiedlayer.co
m (162.144.240.135) 186.999 ms
[attacker@parrot]~$
[attacker@parrot]~$ traceroute -, 5 www.certifiedhacker.com
Bad option '-', (argc 1)
[attacker@parrot]~$
[attacker@parrot]~$ traceroute -m 5 www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 5 hops max, 60 byte packets
 1 10.10.1.1 (10.10.1.1) 1.515 ms 1.420 ms 1.359 ms
 2 172.18.0.1 (172.18.0.1) 1.844 ms 1.796 ms *
 3 192.168.0.29 (192.168.0.29) 1.761 ms 1.715 ms 1.668 ms
 4 103.18.87.33 (103.18.87.33) 39.935 ms 25.632 ms 39.843 ms
 5 63.222.112.64 (63.222.112.64) 3.497 ms 3.451 ms *
[attacker@parrot]~$
```

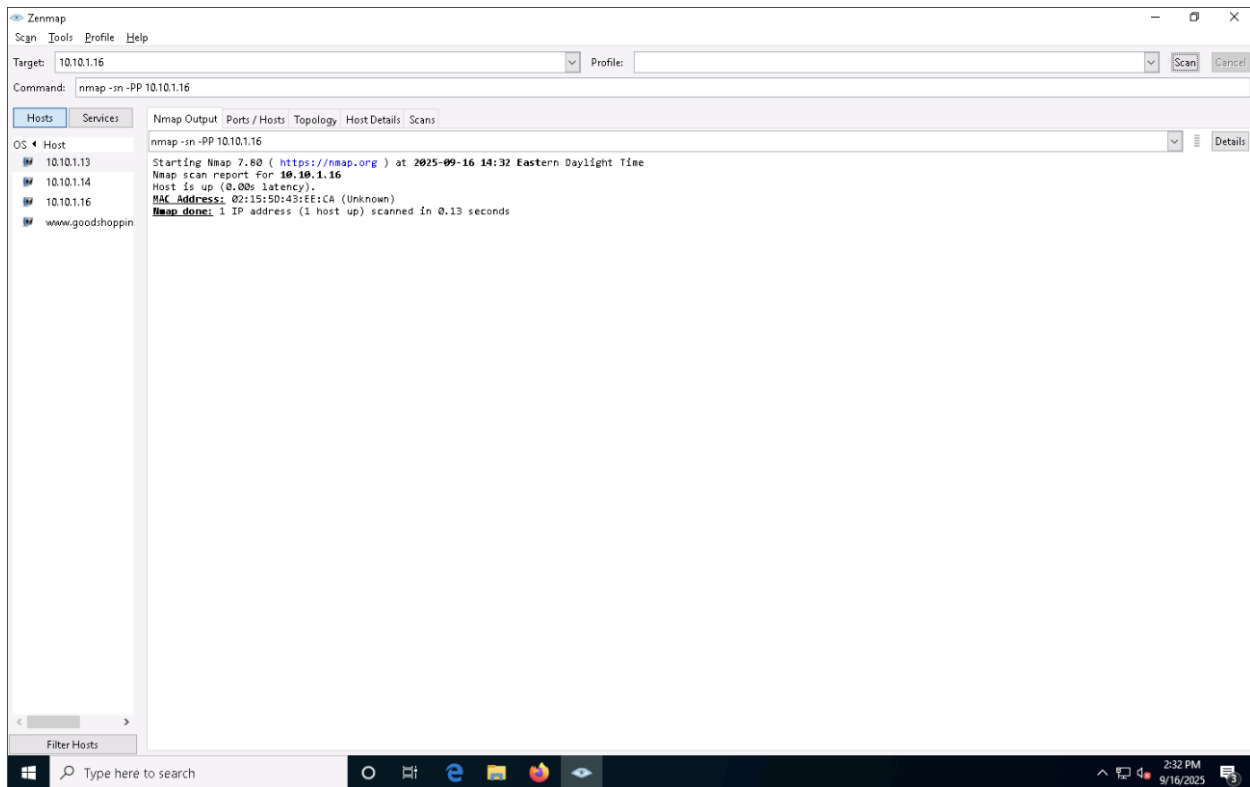
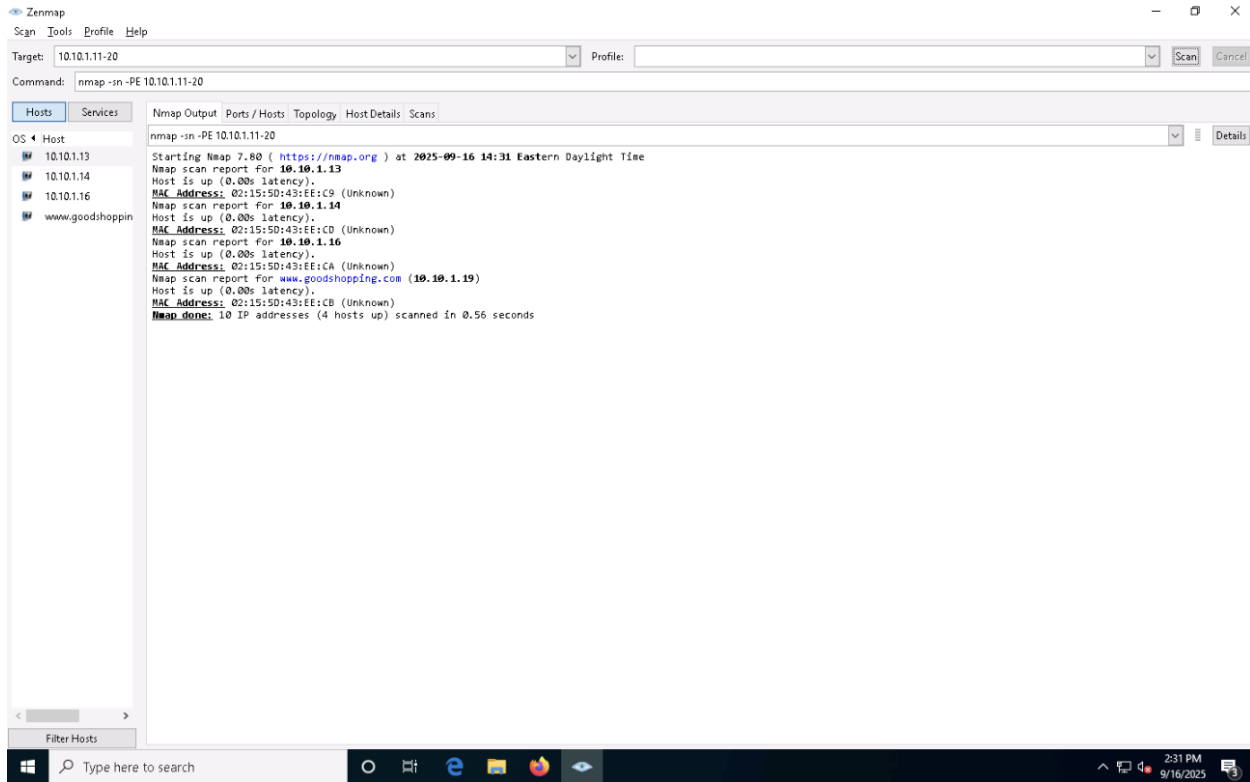
Task 2: Perform Host Discovery using Nmap

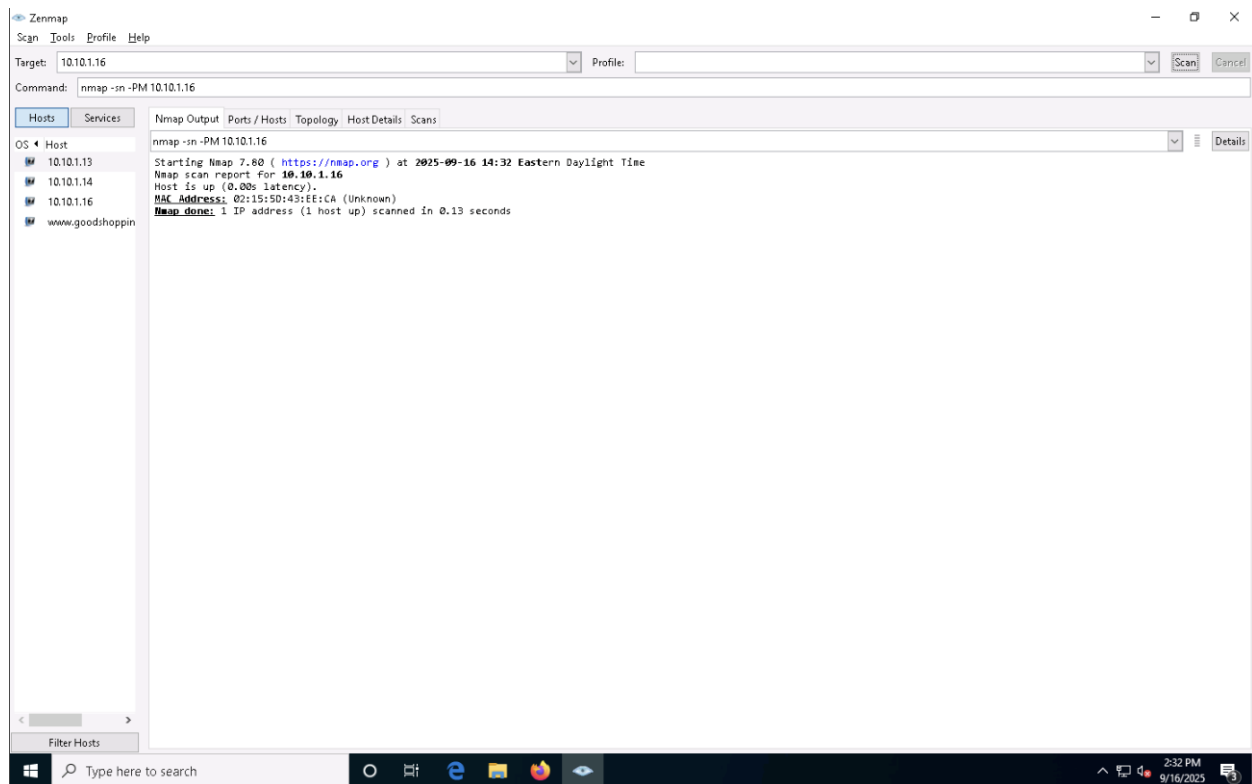
Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.





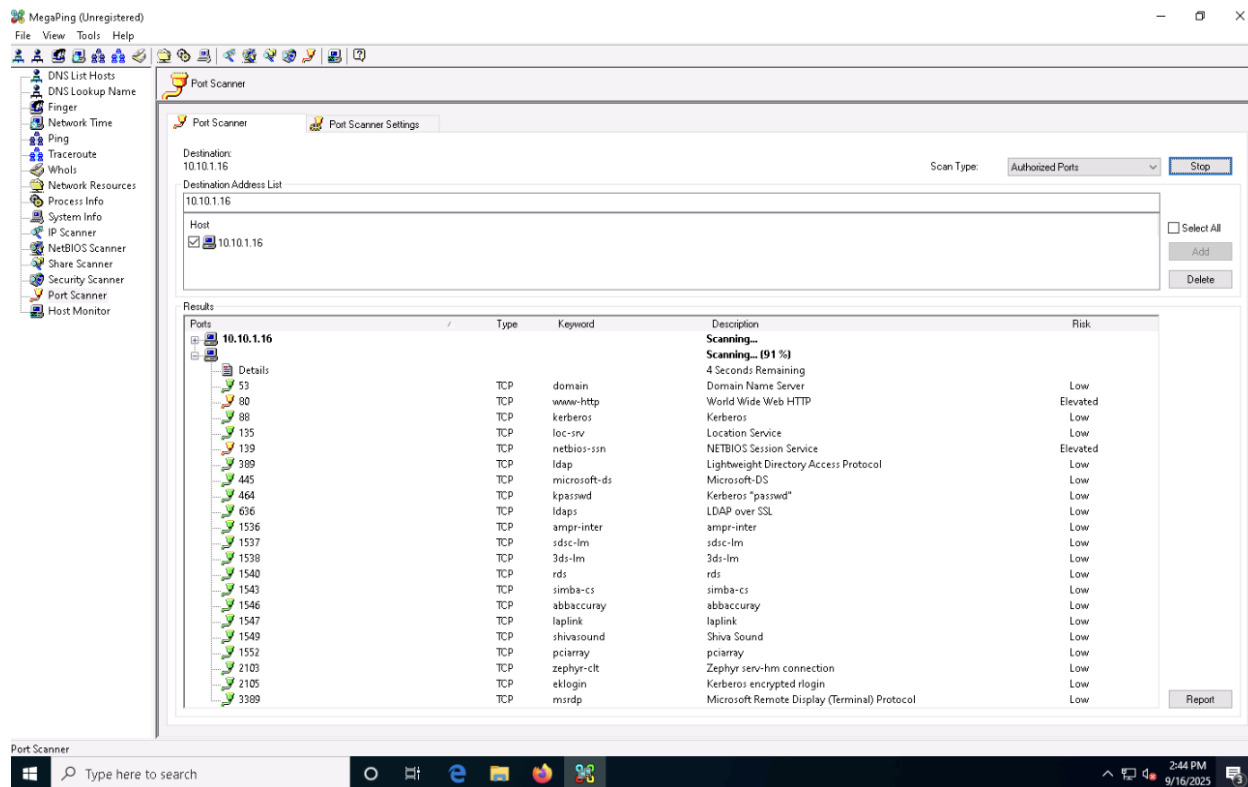
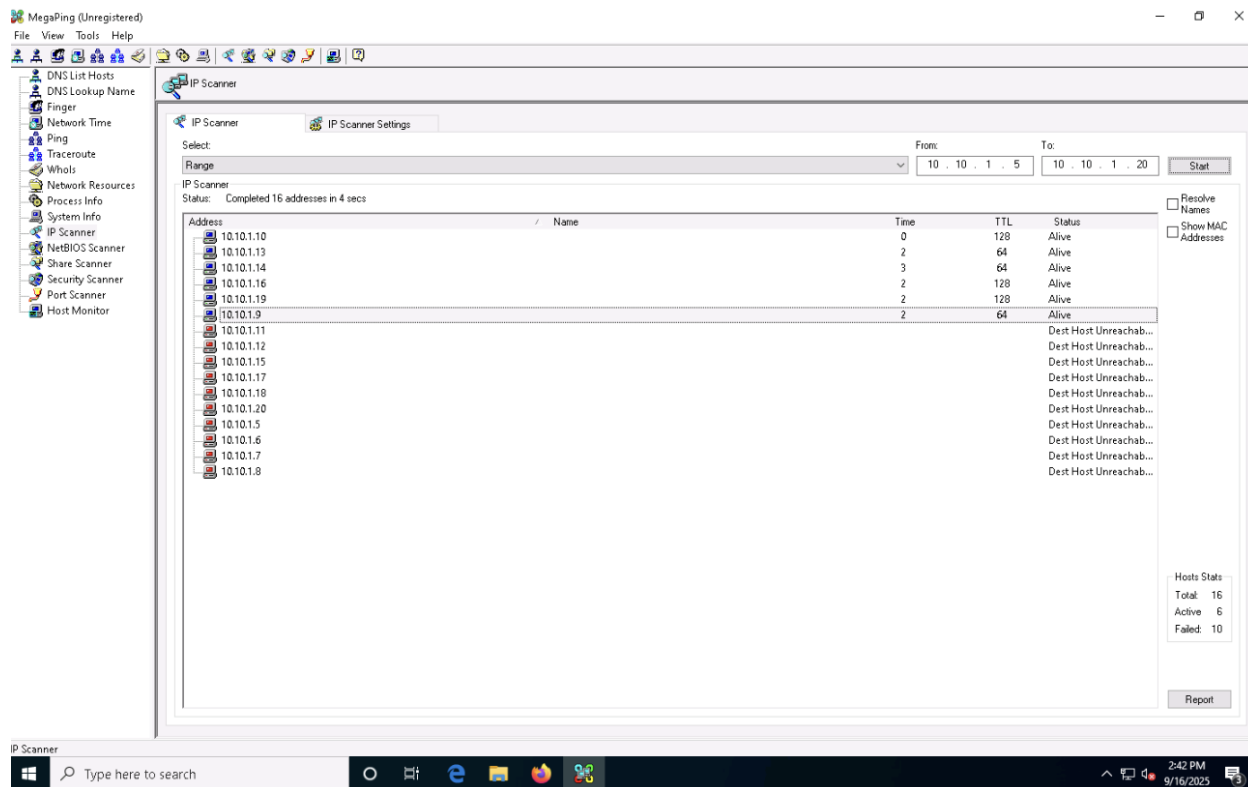




### Task 3: Perform Port and Service Discovery using MegaPing

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

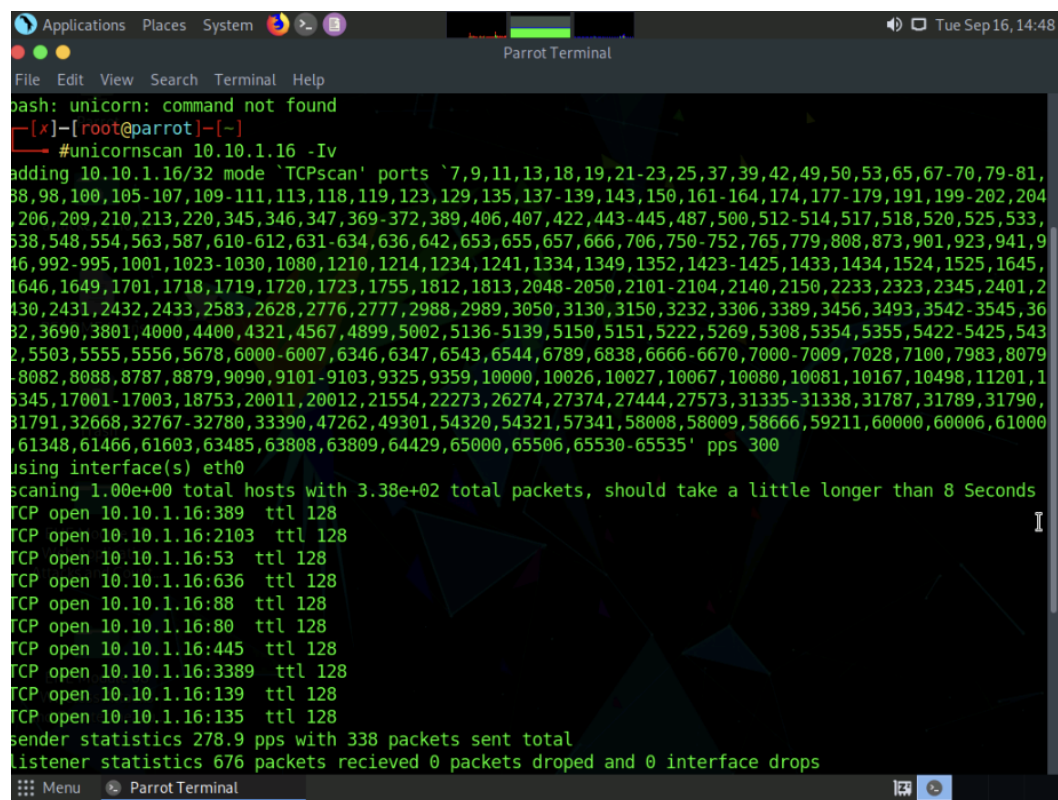




#### Task 4: Perform OS Discovery using Unicornscan

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

Here, we will use the Unicornscan tool to perform OS discovery on the target system.



```
bash: unicorn: command not found
[*]-[root@parrot]-[-]
#unicornscan 10.10.1.16 -Iv
adding 10.10.1.16/32 mode 'TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,
38,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164,174,177-179,191,199-202,204
,206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,
538,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,9
46,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,
1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2
430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,36
32,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,543
2,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079
-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,1
5345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,
31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000
,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer than 8 Seconds
TCP open 10.10.1.16:389 ttl 128
TCP open 10.10.1.16:2103 ttl 128
TCP open 10.10.1.16:53 ttl 128
TCP open 10.10.1.16:636 ttl 128
TCP open 10.10.1.16:88 ttl 128
TCP open 10.10.1.16:80 ttl 128
TCP open 10.10.1.16:445 ttl 128
TCP open 10.10.1.16:3389 ttl 128
TCP open 10.10.1.16:139 ttl 128
TCP open 10.10.1.16:135 ttl 128
sender statistics 278.9 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets dropped and 0 interface drops
```



Net use connects a computer to, or disconnects it from a shared resource. It also displays information about computer connections.

Here, we will use the Nbtstat and Net use Windows command-line utilities to perform NetBIOS enumeration on the target network.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.10

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                Type             Status
    -----
    WINDOWS10           <00>             UNIQUE          Registered
    WORKGROUP            <00>             GROUP           Registered
    WINDOWS10           <20>             UNIQUE          Registered
    WORKGROUP            <1E>             GROUP           Registered
    WORKGROUP            <1D>             UNIQUE          Registered
    *MSBROWSE*          <01>             GROUP           Registered

    MAC Address = 00-15-5D-01-80-01

C:\Users\Administrator>
```

```

Administrator Command Prompt

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Machine Name Table

    Name                           Type                  Status
-----
WINDOWS10                         <00>   UNIQUE           Registered
WORKGROUP                          <00>   GROUP             Registered
WINDOWS10                         <20>   UNIQUE           Registered
WORKGROUP                          <1E>   GROUP             Registered
WORKGROUP                          <1D>   UNIQUE           Registered
00_00_MSBRWSE_00<01>              GROUP             Registered

MAC Address = 00-15-5D-01-B0-01

C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Cache Name Table

    Name                           Type          Host Address      Life [sec]
-----
WINDOWS10                         <20>   UNIQUE           10.10.1.10        488

C:\Users\Administrator>
```

```

C:\> Administrator: Command Prompt

WORKGROUP          <1E>   GROUP          Registered
WORKGROUP          <1D>   UNIQUE         Registered
00-__MSBROWSE__-0<01> GROUP          Registered

MAC Address = 00-15-5D-01-80-01

C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

NetBIOS Remote Cache Name Table

    Name                Type                Host Address        Life [sec]
    -----
WINDOWS10              <20>   UNIQUE             10.10.1.10          488

C:\Users\Administrator>net use
New connections will be remembered.

Status      Local      Remote      Network
-----
OK           Z:         \\WINDOWS10\EHE-Tools  Microsoft Windows Network
The command completed successfully.

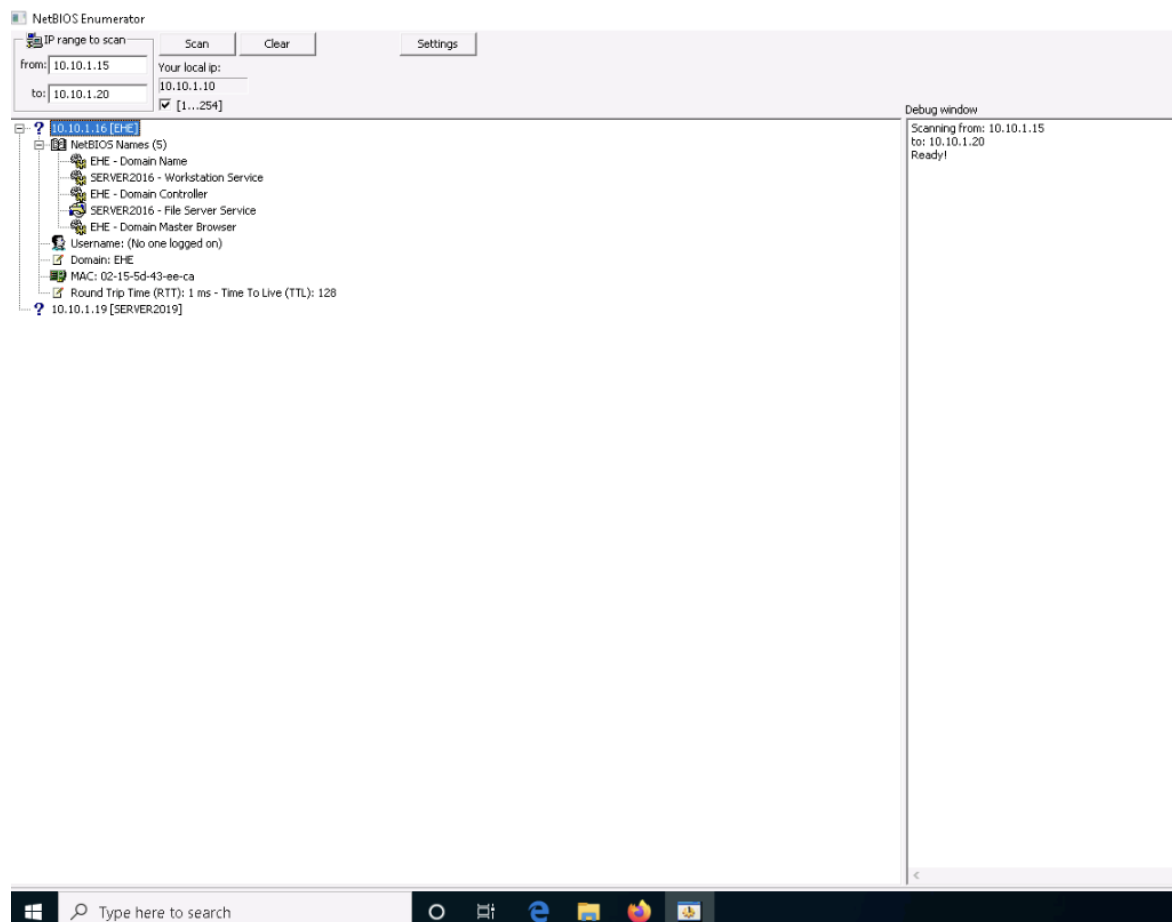
C:\Users\Administrator>_

```

## Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.



## Module 02: Ethical Hacking Fundamentals – Lab Summary

The labs in this module introduced the fundamental phases of the hacking cycle through practical exercises.

In Lab 1 (Passive Footprinting), I used advanced Google search operators, attempted data extraction with web crawling tools, and performed Whois lookups to gather organization details without direct interaction.

In Lab 2 (Network Scanning), I practiced tracerouting, host discovery with Nmap, port and service scanning with MegaPing, and OS identification using Unicornscan to profile network systems.

In Lab 3 (Enumeration), I conducted NetBIOS enumeration with Windows command-line utilities and NetBIOS Enumerator to extract usernames, machine names, and shared resources.

These labs reinforced core skills in reconnaissance, scanning, and enumeration, which are essential for ethical hackers to identify vulnerabilities and strengthen organizational defenses.

