

# Lab 8: Perform Network Footprinting

---

## Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, as a professional ethical hacker, your next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack.

## Lab Objectives

- Locate the network range
- Perform network tracerouting in Windows and Linux Machines

## Overview of Network Footprinting

Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

## Task 1: Locate the Network Range

Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating system used in the target network.

Here, we will locate the network range using the ARIN Whois database search tool.

1. ☐ Click [Windows 10](#) to switch to the **Windows 10** machine.
2. ☐ Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and click <https://www.arin.net/about/welcome/region> and press **Enter**.

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

3. ☐ 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.

The screenshot shows the ARIN website's 'Our Region' page. The browser's address bar displays 'https://www.arin.net/about/welcome/region/'. The page header includes the ARIN logo and a search bar containing the IP address '162.241.216.11'. Below the header, the page title 'Our Region' is displayed. The main content area features a section titled 'ARIN's Region' with a description of its geographical service area. Below this, there is a section titled 'Complete List of Countries in the ARIN Region' with a table showing the 'Canada Sector' and 'Caribbean and North Atlantic Islands Sector'. The table for the Canada Sector has columns for 'Country', 'A 2', and 'A 3', with the entry 'CANADA', 'CA', and 'CAN' respectively. The table for the Caribbean and North Atlantic Islands Sector is partially visible. On the right side, there is a sidebar with links to 'Welcome to ARIN', 'Organization Structure & Staff', 'Our Region', 'ARIN Board of Trustees', 'Advisory Council', 'NRO Number Council', 'Careers', and 'Related' links to 'All', 'AFRINIC', 'APNIC', and 'LACNIC'. The Windows taskbar at the bottom shows the time as 12:56 AM on 5/21/2020.

Your IPv4 address is 199.101.110.10

Log in

ARIN  
American Registry for Internet Numbers

162.241.216.11

Search

all requests subject to terms of use

IP Addresses & ASNs Policy & Participation Reference & Tools About

Pay Now Feedback

Home > About > Welcome to ARIN > Our Region

## Our Region

On this page

- » **ARIN's Region**
  - o Complete List of Countries in the ARIN Region
- » **Regional Internet Registry Regions**

### ARIN's Region

ARIN's geographical service area includes all of the countries in the list below. The links on the right provide a list of the countries within each Regional Internet Registry's region, and a map is available below showing all regions.

### Complete List of Countries in the ARIN Region

by sector

#### Canada Sector

Country	A 2	A 3
CANADA	CA	CAN

#### Caribbean and North Atlantic Islands Sector

Country	A 2	A 3
---------	-----	-----

#### Welcome to ARIN

- Organization Structure & Staff
- Our Region
- ARIN Board of Trustees
- Advisory Council
- NRO Number Council
- Careers

#### Related

- All
- AFRINIC
- APNIC
- LACNIC

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

The screenshot shows a web browser window with the ARIN Whois/RDAP search interface. The search bar contains the IP address 162.241.216.11, and the search filter is set to 'Automatic'. The results show the network range 162.240.0.0 - 162.241.255.255, which is highlighted in blue. The network is identified as NET-162-240-0-0-1, a direct allocation from AS46606. The registration and last changed dates are both from August 22, 2013. The 'Self' link points to the RDAP record, and the 'Alternate' link points to the Whois record. The 'Port 43 Whois' link points to the whois.arin.net service. The 'Related Entities' section shows 1 entity.

ARIN Whois/RDAP - American

https://search.arin.net/rdap/?query=162.241.216.11

Your IPv4 address is 199.101.110.10 Log in

# ARIN Whois/RDAP

162.241.216.11 Search

» Search www.arin.net instead Search Filter: Automatic all requests subject to terms of use

"162.241.216.11"

## Network: NET-162-240-0-0-1

Source Registry	ARIN
Net Range	162.240.0.0 - 162.241.255.255
CIDR	162.240.0.0/15
Name	UNIFIEDLAYER-NETWORK-16
Handle	NET-162-240-0-0-1
Parent	NET-162-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS46606
Registration	Thu, 22 Aug 2013 17:57:53 GMT (Thu Aug 22 2013 local time)
Last Changed	Thu, 22 Aug 2013 17:57:54 GMT (Thu Aug 22 2013 local time)
Self	<a href="https://rdap.arin.net/registry/ip/162.240.0.0">https://rdap.arin.net/registry/ip/162.240.0.0</a>
Alternate	<a href="https://whois.arin.net/rest/net/NET-162-240-0-0-1">https://whois.arin.net/rest/net/NET-162-240-0-0-1</a>
Port 43 Whois	whois.arin.net

Related Entities 1 Entity

Report Whois Inaccuracy  
Whois/RDAP Documentation  
ARIN Technical Discussion Mailing List  
FAQs

Type here to search 12:57 AM 5/21/2020

5. ☐ This concludes the demonstration of locating network range using the ARIN Whois database search tool.
  6. ☐ Close all open windows and document all the acquired information.
- 

## Task 2: 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.

1. ☐ Click [Windows 10](#) to switch to the **Windows 10** machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

```
Command Prompt
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:

  0  1 ms    1 ms    1 ms    10.10.10.1
  1  2 ms    1 ms    1 ms    172.18.0.1
  2  2 ms    2 ms    2 ms    192.168.100.6
  3  4 ms    2 ms    3 ms    72.15.250.219
  4  9 ms    5 ms    3 ms    te0-0-1-1.edge02.tpa.peak10.net [66.129.96.185]
  5  9 ms    10 ms   9 ms    te0-0-0-0.edge01.tpa.peak10.net [66.129.65.157]
  6  9 ms    9 ms    9 ms    be31.bbrt01.tpa01.flexential.net [148.66.237.130]
  7  9 ms    9 ms    9 ms    be120.bbrt01.mia10.flexential.net [148.66.238.58]
  8  10 ms   8 ms    9 ms    be23.brdr11.mia10.flexential.net [148.66.237.153]
  9  9 ms    10 ms   8 ms    mai-b1-link.telial.net [62.115.181.148]
 10 18 ms    20 ms   19 ms   atl-b24-link.telial.net [62.115.113.48]
 11 41 ms    41 ms   46 ms   hou-b1-link.telial.net [62.115.116.46]
 12 40 ms    40 ms   41 ms   cyrusone-svc067800-lag002969.c.telial.net [62.115.184.145]
 13 40 ms    41 ms   40 ms   72-250-192-6.cyrusone.com [72.250.192.6]
 14 41 ms    41 ms   41 ms   po101.router2a.hou1.net.unifiedlayer.com [162.241.0.7]
 15 42 ms    42 ms   41 ms   108-167-150-118.unifiedlayer.com [108.167.150.118]
 16 41 ms    40 ms   41 ms   box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>
```

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

```
Command Prompt
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:

  0  1 ms    1 ms    1 ms  10.10.10.1
  1  2 ms    1 ms    1 ms  172.18.0.1
  2  2 ms    2 ms    2 ms  192.168.100.6
  3  4 ms    2 ms    3 ms  72.15.250.219
  4  9 ms    5 ms    3 ms  te0-0-1-1.edge02.tpa.peak10.net [66.129.96.185]
  5  9 ms    10 ms   9 ms  te0-0-0-0.edge01.tpa.peak10.net [66.129.65.157]
  6  9 ms    9 ms    9 ms  be31.bbrt01.tpa01.flexential.net [148.66.237.130]
  7  9 ms    9 ms    9 ms  be120.bbrt01.mia10.flexential.net [148.66.238.58]
  8  10 ms   8 ms    9 ms  be23.bdr11.mia10.flexential.net [148.66.237.153]
  9  9 ms    10 ms   8 ms  mai-b1-link.telial.net [62.115.181.148]
 10 18 ms    20 ms   19 ms  atl-b24-link.telial.net [62.115.113.48]
 11 41 ms    41 ms   46 ms  hou-b1-link.telial.net [62.115.116.46]
 12 40 ms    40 ms   41 ms  cyrusone-svc067800-lag002969.c.telial.net [62.115.184.145]
 13 40 ms    41 ms   40 ms  72-250-192-6.cyrusone.com [72.250.192.6]
 14 41 ms    41 ms   41 ms  po101.router2a.hou1.net.unifiedlayer.com [162.241.0.7]
 15 42 ms    42 ms   41 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
 16 41 ms    40 ms   41 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>
```

3. ☐ Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

```
Command Prompt
over a maximum of 30 hops:
 1  1 ms  1 ms  1 ms  10.10.10.1
 2  2 ms  1 ms  1 ms  172.18.0.1
 3  2 ms  2 ms  2 ms  192.168.100.6
 4  4 ms  2 ms  3 ms  72.15.250.219
 5  9 ms  5 ms  3 ms  te0-0-1-1.edge02.tpa.peak10.net [66.129.96.185]
 6  9 ms  10 ms  9 ms  te0-0-0-0.edge01.tpa.peak10.net [66.129.65.157]
 7  9 ms  9 ms  9 ms  be31.bbrt01.tpa01.flexential.net [148.66.237.130]
 8  9 ms  9 ms  9 ms  be120.bbrt01.mia10.flexential.net [148.66.238.58]
 9  10 ms  8 ms  9 ms  be23.brdr11.mia10.flexential.net [148.66.237.153]
10  9 ms  10 ms  8 ms  mai-b1-link.telial.net [62.115.181.148]
11  18 ms  20 ms  19 ms  atl-b24-link.telial.net [62.115.113.48]
12  41 ms  41 ms  46 ms  hou-b1-link.telial.net [62.115.116.46]
13  40 ms  40 ms  41 ms  cyrusone-svc067800-lag002069.c.telial.net [62.115.184.145]
14  40 ms  41 ms  40 ms  72-250-192-6.cyrusone.com [72.250.192.6]
15  41 ms  41 ms  41 ms  po101.router2a.hou1.net.unifiedlayer.com [162.241.0.7]
16  42 ms  42 ms  41 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
17  41 ms  40 ms  41 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>tracert -h 5 lolwut.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:
 1  1 ms  <1 ms  1 ms  10.10.10.1
 2  2 ms  2 ms  2 ms  172.18.0.1
 3  2 ms  1 ms  2 ms  192.168.100.6
 4  3 ms  2 ms  3 ms  72.15.250.219
 5  2 ms  2 ms  2 ms  te0-0-1-1.edge02.tpa.peak10.net [66.129.96.185]

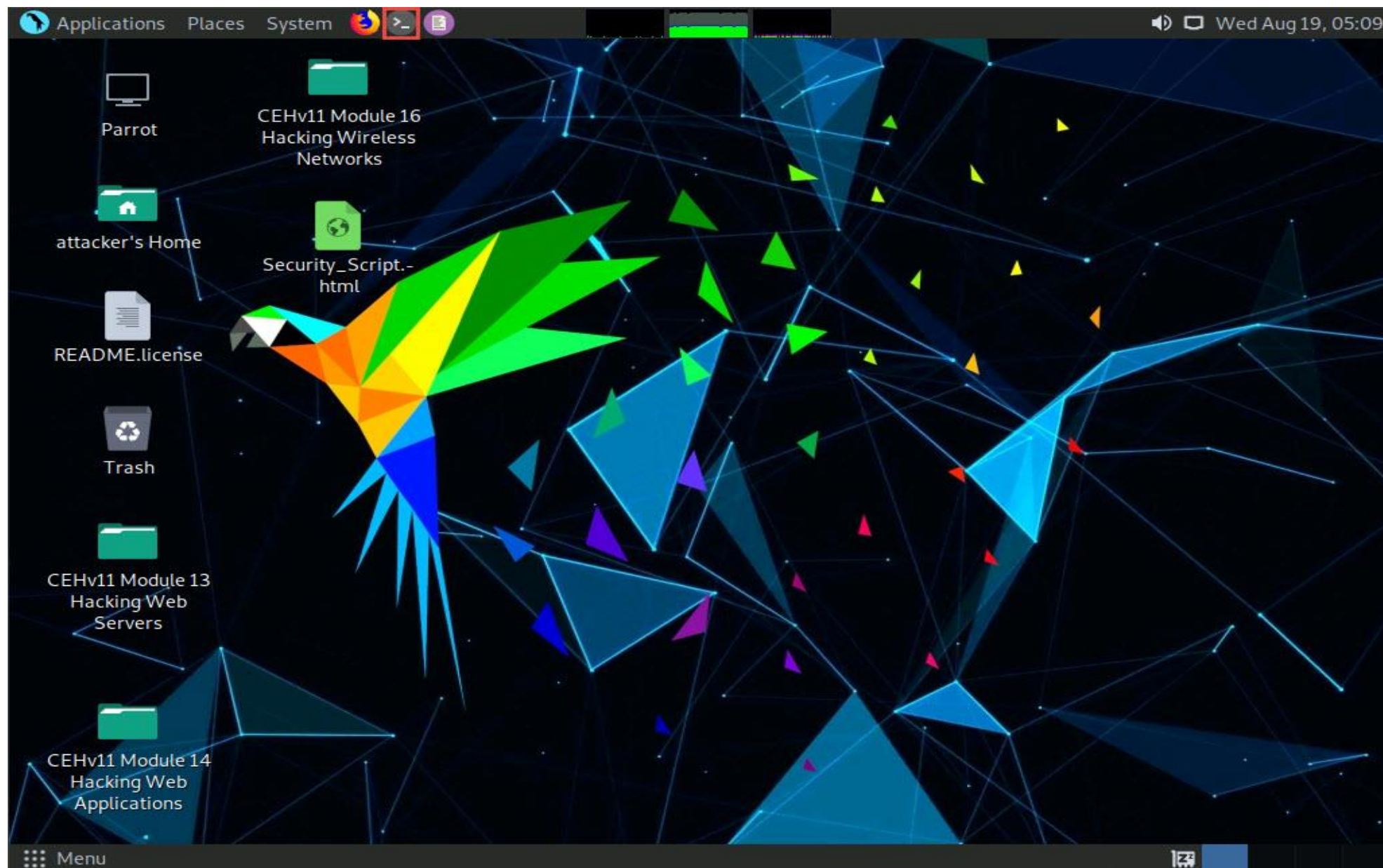
Trace complete.

C:\Users\Admin>
```

4. ☐ After viewing the result, close the command prompt window.
5. ☐ Now, click [Parrot Security](#) to switch to the **Parrot Security** machine.



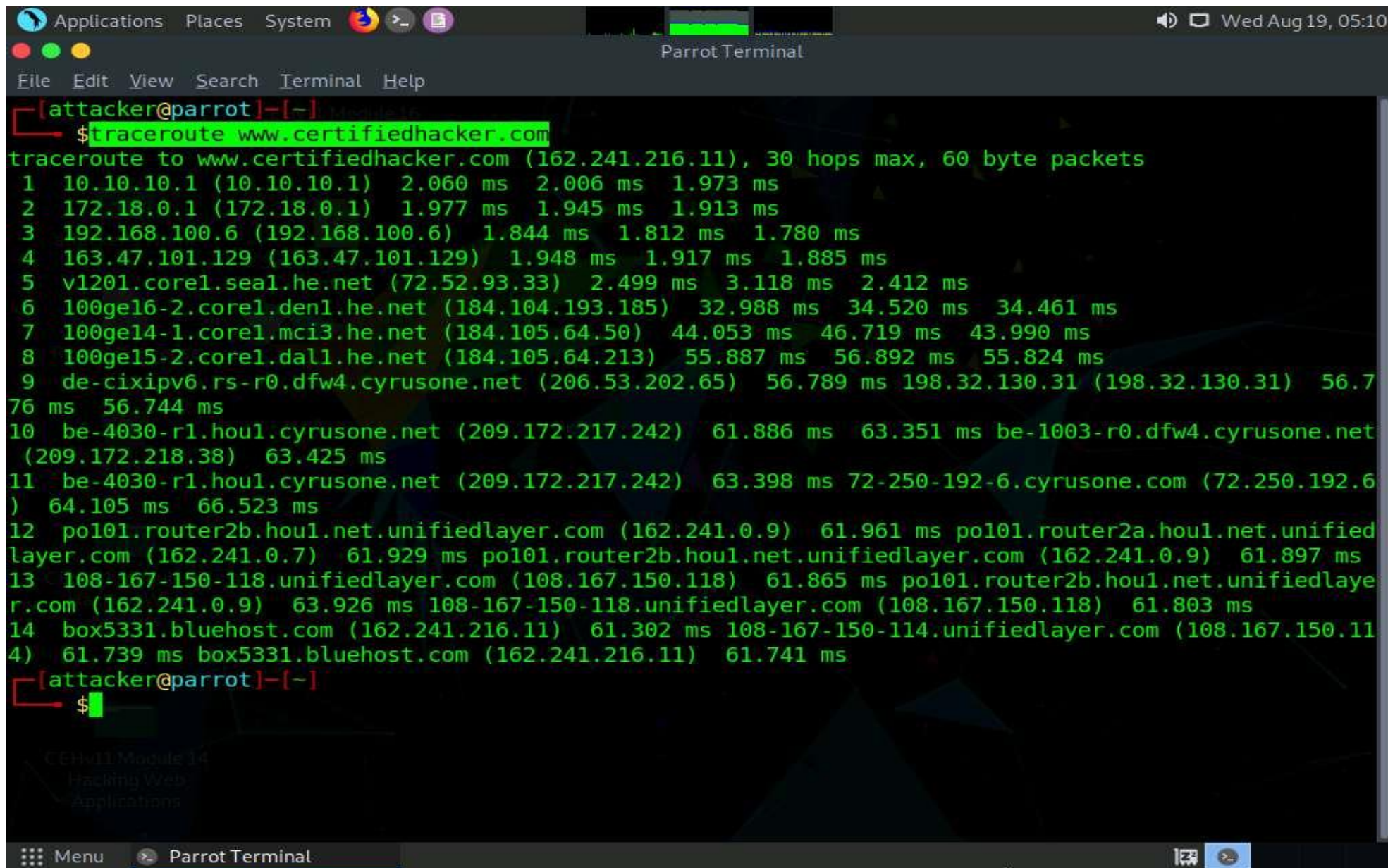
6. ☐ Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.





7. ☐ A **Parrot Terminal** window appears. In the terminal window, type **tracert** [www.certifiedhacker.com](http://www.certifiedhacker.com) and press **Enter** to view the hops that the packets made before reaching the destination.

Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.



The screenshot shows a Parrot Terminal window with a dark theme. The title bar at the top includes 'Applications', 'Places', 'System', and a date/time indicator 'Wed Aug 19, 05:10'. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt is '[attacker@parrot]-[~]'. The command '\$tracert www.certifiedhacker.com' is entered and executed. The output shows a series of hops from the local machine to the destination IP 162.241.216.11. The hops are numbered 1 through 14, with some hops showing multiple paths or repeated IP addresses. The final hop is box5331.bluehost.com (162.241.216.11) with a latency of 61.741 ms. The terminal window also shows a sidebar on the left with 'CEHv11 Module 14', 'Hacking Web', and 'Applications'. The bottom status bar shows 'Menu' and 'Parrot Terminal'.

```
[attacker@parrot]-[~]
$tracert www.certifiedhacker.com
tracert to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.10.1 (10.10.10.1)  2.060 ms  2.006 ms  1.973 ms
 2  172.18.0.1 (172.18.0.1)  1.977 ms  1.945 ms  1.913 ms
 3  192.168.100.6 (192.168.100.6)  1.844 ms  1.812 ms  1.780 ms
 4  163.47.101.129 (163.47.101.129)  1.948 ms  1.917 ms  1.885 ms
 5  v1201.core1.sea1.he.net (72.52.93.33)  2.499 ms  3.118 ms  2.412 ms
 6  100ge16-2.core1.den1.he.net (184.104.193.185)  32.988 ms  34.520 ms  34.461 ms
 7  100ge14-1.core1.mci3.he.net (184.105.64.50)  44.053 ms  46.719 ms  43.990 ms
 8  100ge15-2.core1.dal1.he.net (184.105.64.213)  55.887 ms  56.892 ms  55.824 ms
 9  de-cixipv6.rs-r0.dfw4.cyrusone.net (206.53.202.65)  56.789 ms 198.32.130.31 (198.32.130.31)  56.7
76 ms  56.744 ms
10  be-4030-r1.hou1.cyrusone.net (209.172.217.242)  61.886 ms  63.351 ms be-1003-r0.dfw4.cyrusone.net
(209.172.218.38)  63.425 ms
11  be-4030-r1.hou1.cyrusone.net (209.172.217.242)  63.398 ms 72-250-192-6.cyrusone.com (72.250.192.6
)  64.105 ms  66.523 ms
12  po101.router2b.hou1.net.unifiedlayer.com (162.241.0.9)  61.961 ms po101.router2a.hou1.net.unified
layer.com (162.241.0.7)  61.929 ms po101.router2b.hou1.net.unifiedlayer.com (162.241.0.9)  61.897 ms
13  108-167-150-118.unifiedlayer.com (108.167.150.118)  61.865 ms po101.router2b.hou1.net.unifiedlaye
r.com (162.241.0.9)  63.926 ms 108-167-150-118.unifiedlayer.com (108.167.150.118)  61.803 ms
14  box5331.bluehost.com (162.241.216.11)  61.302 ms 108-167-150-114.unifiedlayer.com (108.167.150.11
4)  61.739 ms box5331.bluehost.com (162.241.216.11)  61.741 ms
[attacker@parrot]-[~]
$
```

8. ☐ This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

9. ☐ You can also use other traceroute tools such as **VisualRoute** (<http://www.visualroute.com>), **Traceroute NG** (<https://www.solarwinds.com>), etc. to extract additional network information of the target organization.
10. ☐ Close all open windows and document all acquired information.