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

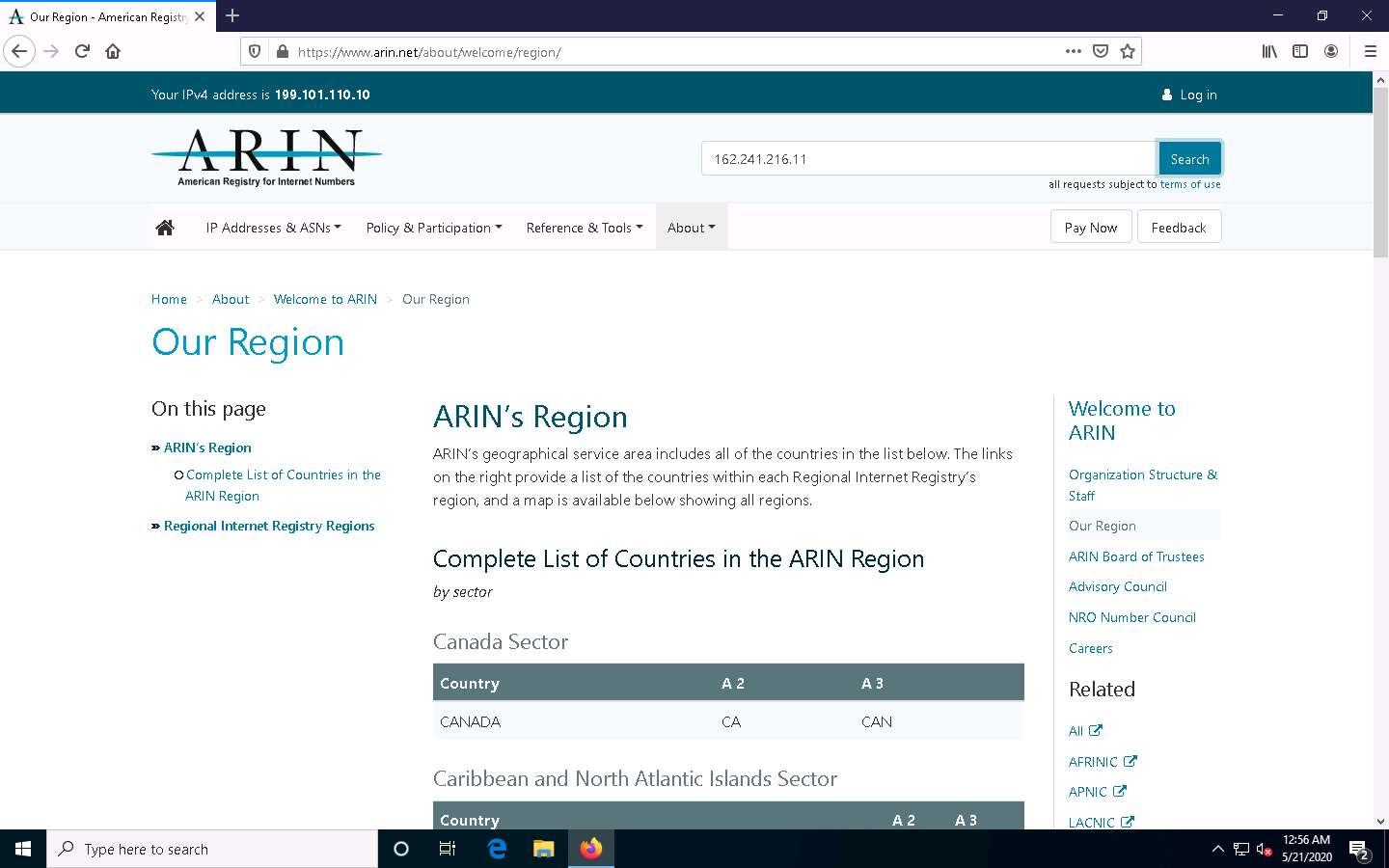
Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating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

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

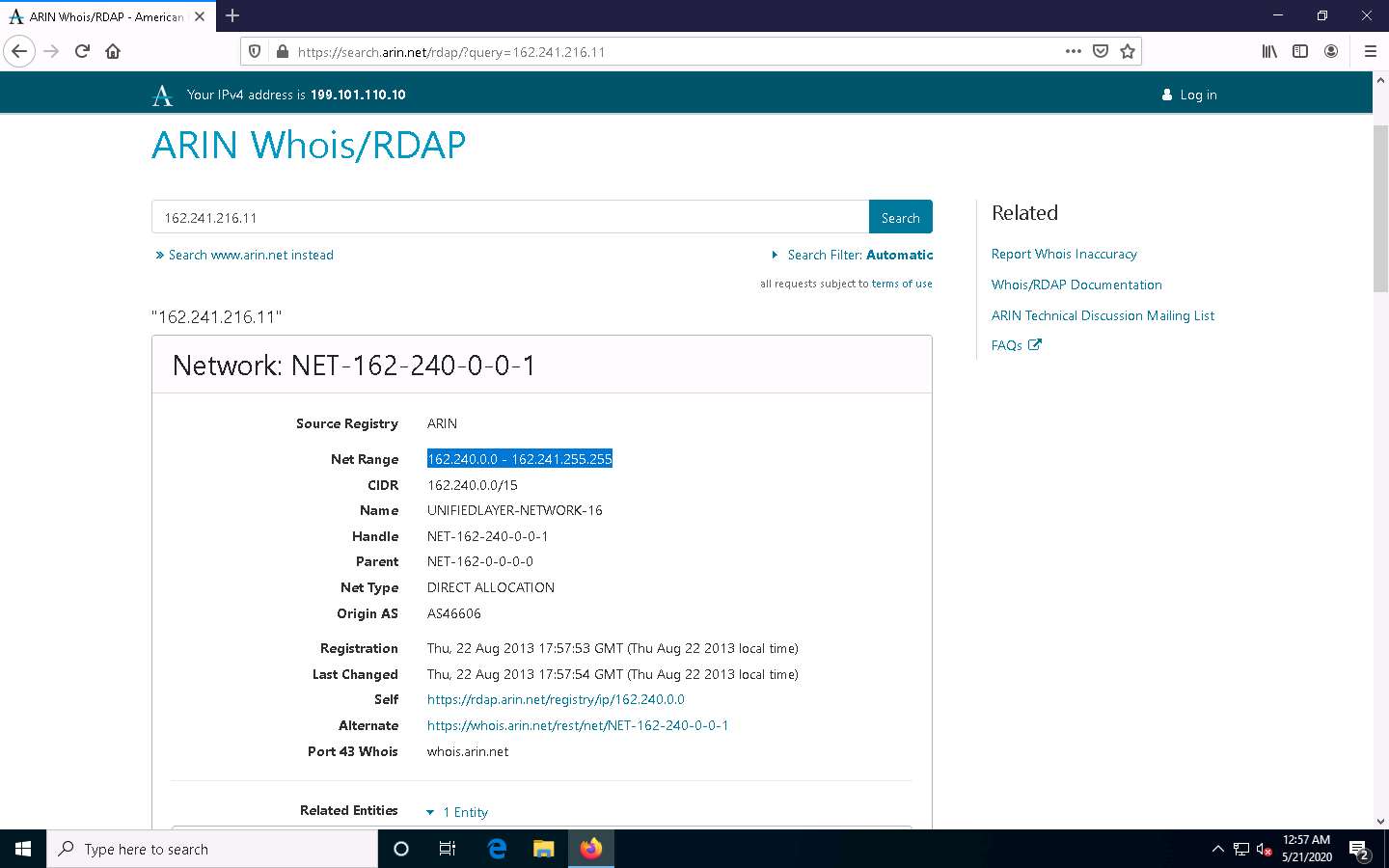
1. Click [Windows 10](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10) to switch to the **Windows 10** machine.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and click https://www.arin.net/about/welcome/region and press **Enter**.

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

1. 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.



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



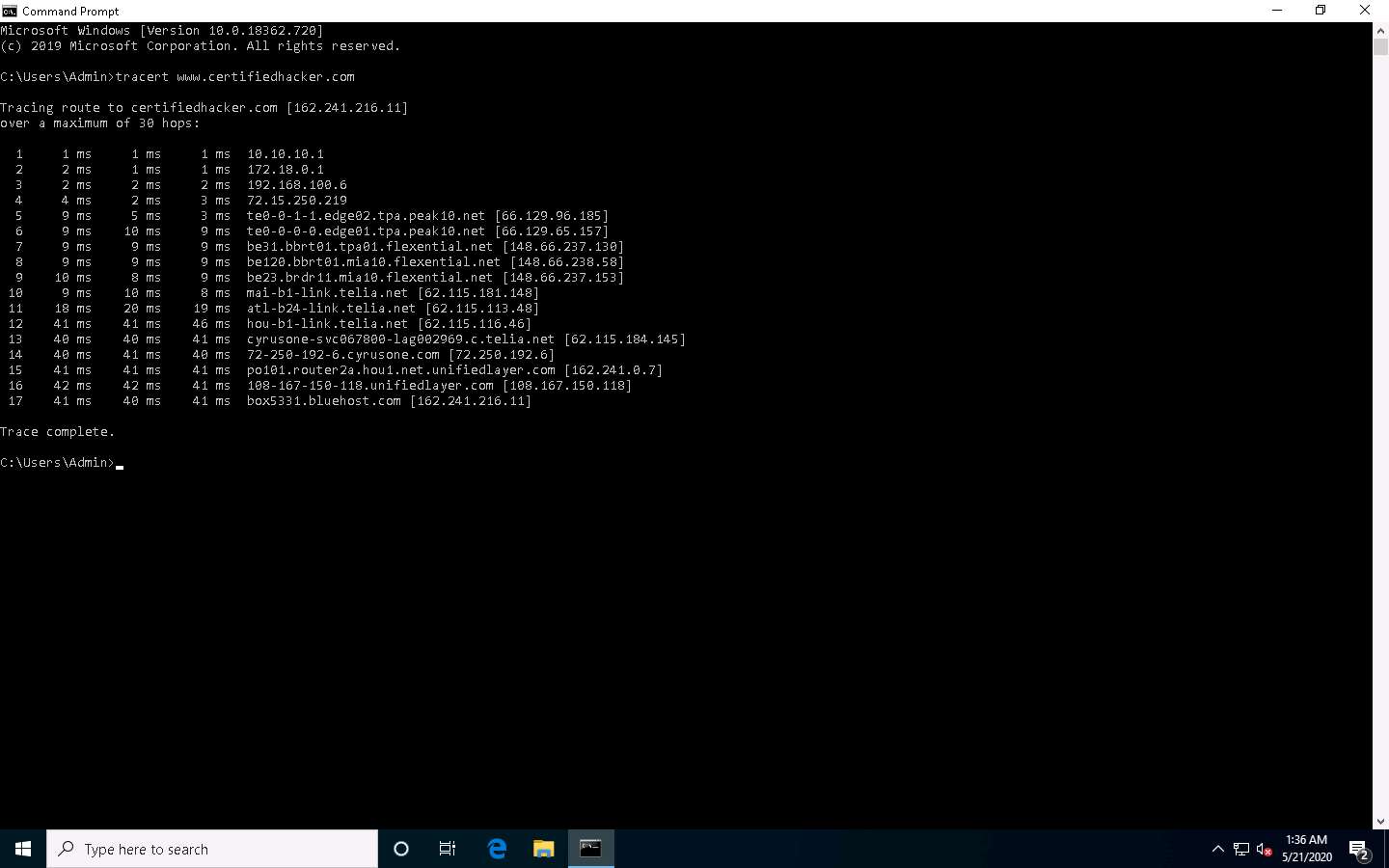
1. This concludes the demonstration of locating network range using the ARIN Whois database search tool.
2. Close all open windows and document all the acquired information.

Task 2: Perform Network Tracerouting in Windows and Linux Machines

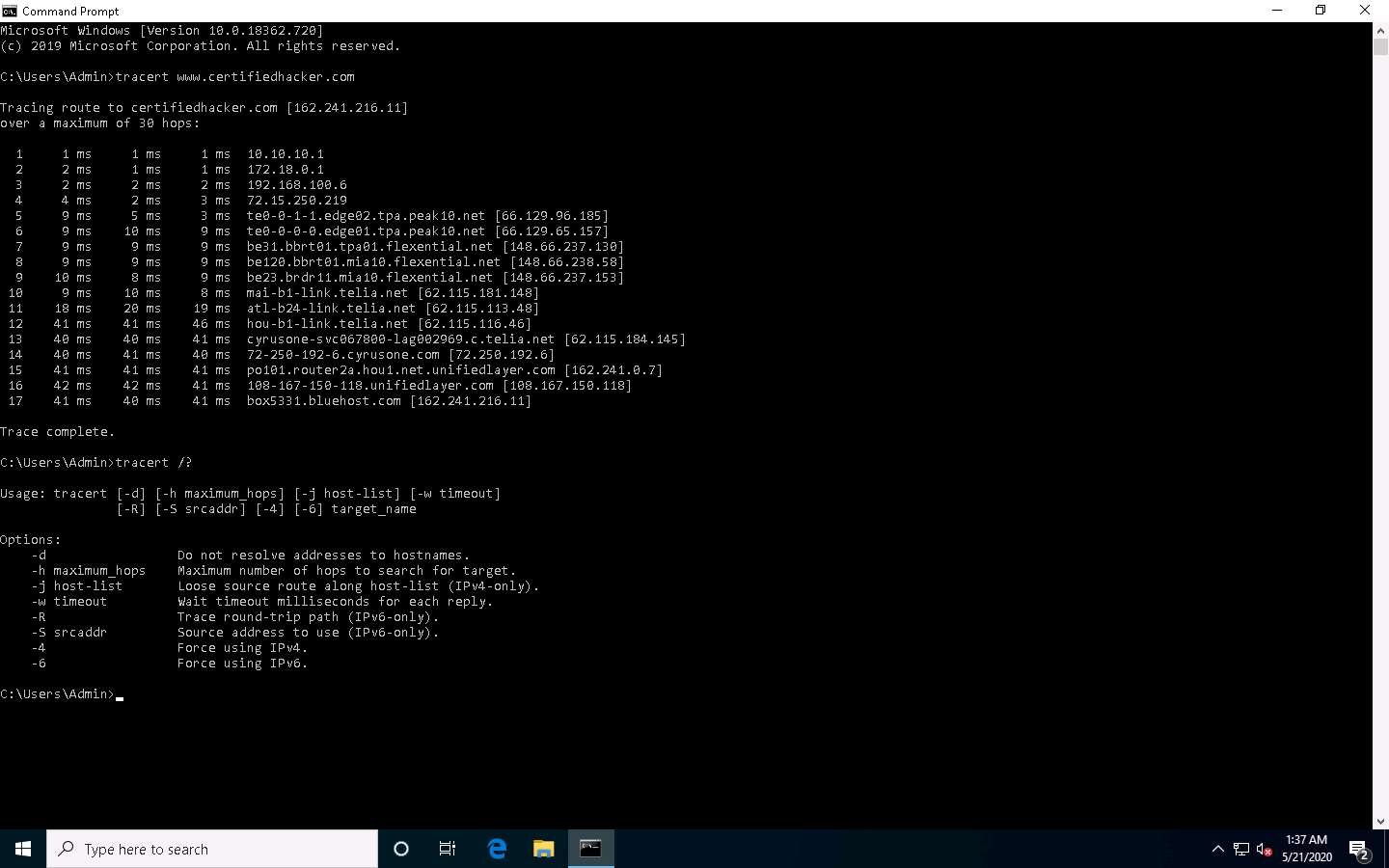
The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between 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.

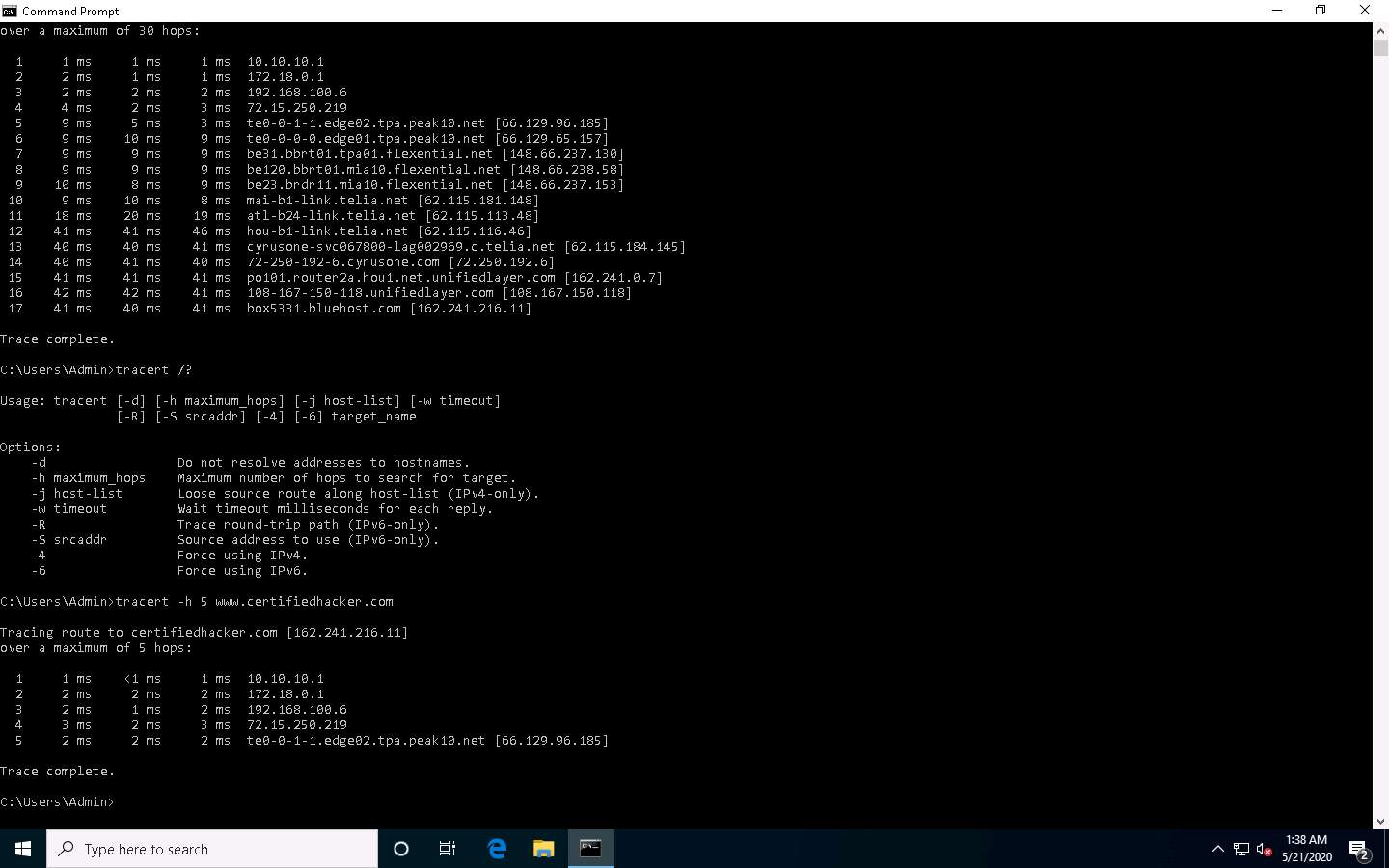
1. Click [Windows 10](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10) to switch to the **Windows 10** machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.



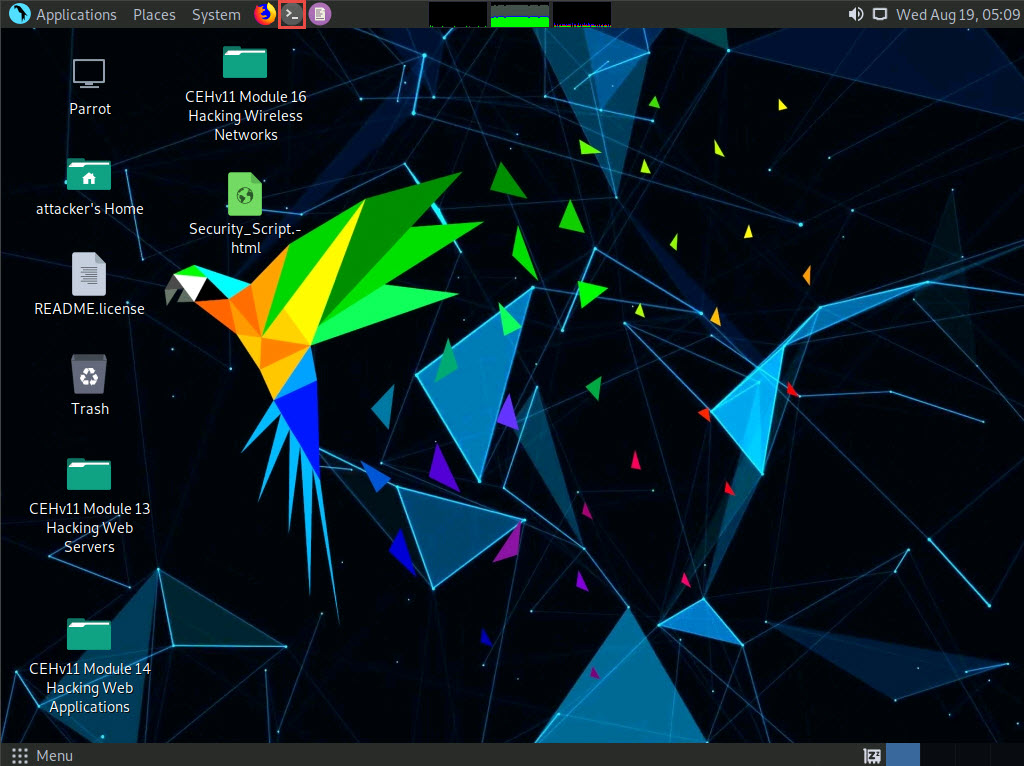
1. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.



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

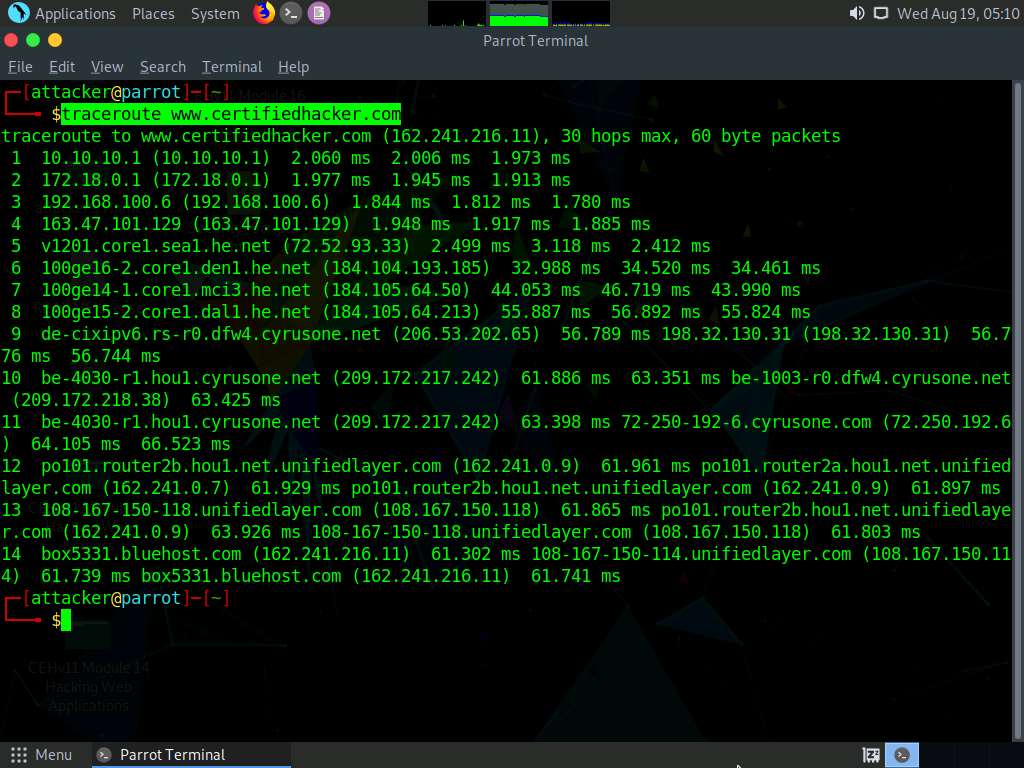


1. After viewing the result, close the command prompt window.
2. Now, click [Parrot Security](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10) to switch to the **Parrot Security** machine.
3. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.



1. A **Parrot Terminal** window appears. In the terminal window, type **traceroute 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.



1. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
2. 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.
3. Close all open windows and document all acquired information.