Lab 6: 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

- 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: Perform Network Tracerouting in Windows and Linux Machines

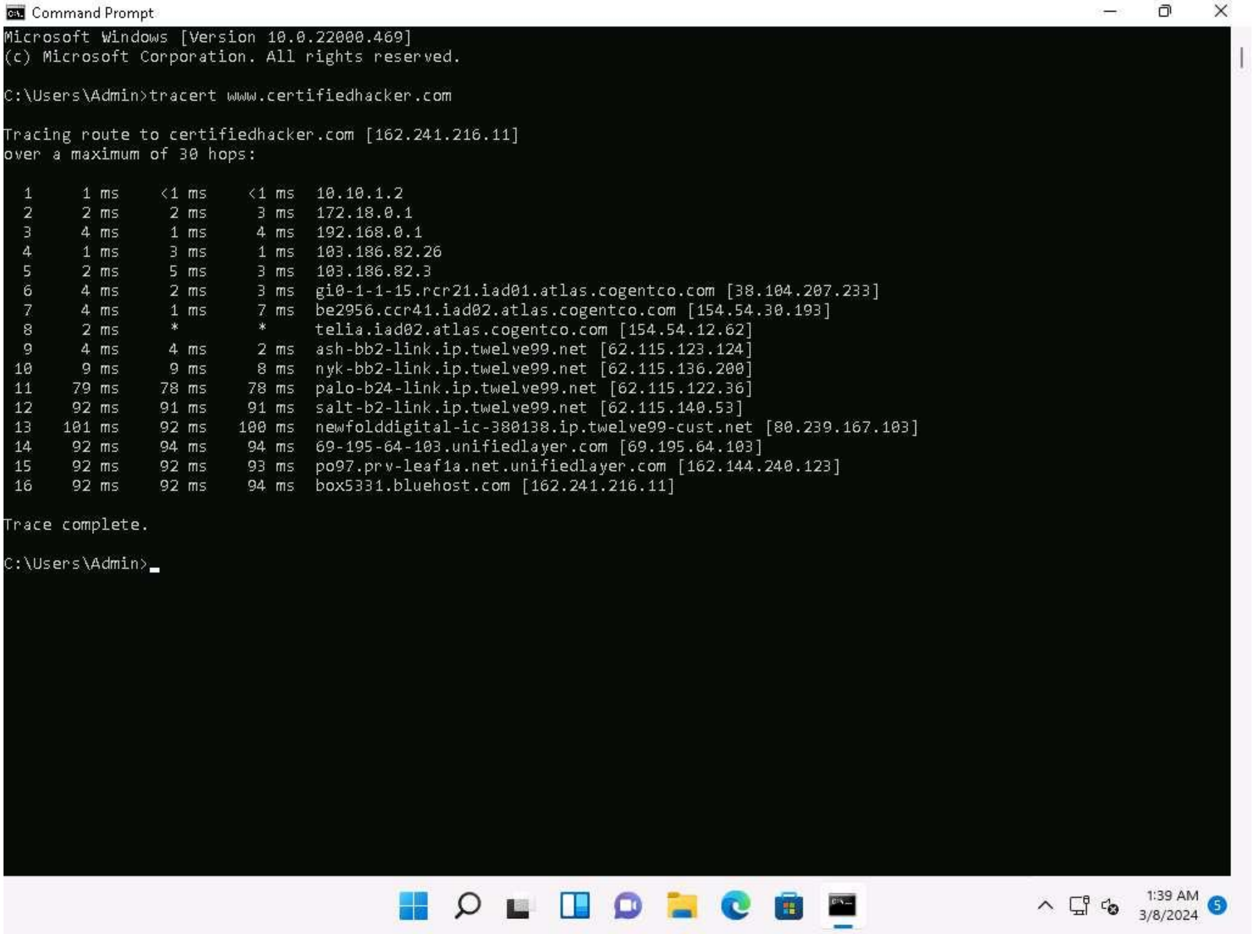
The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between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

Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

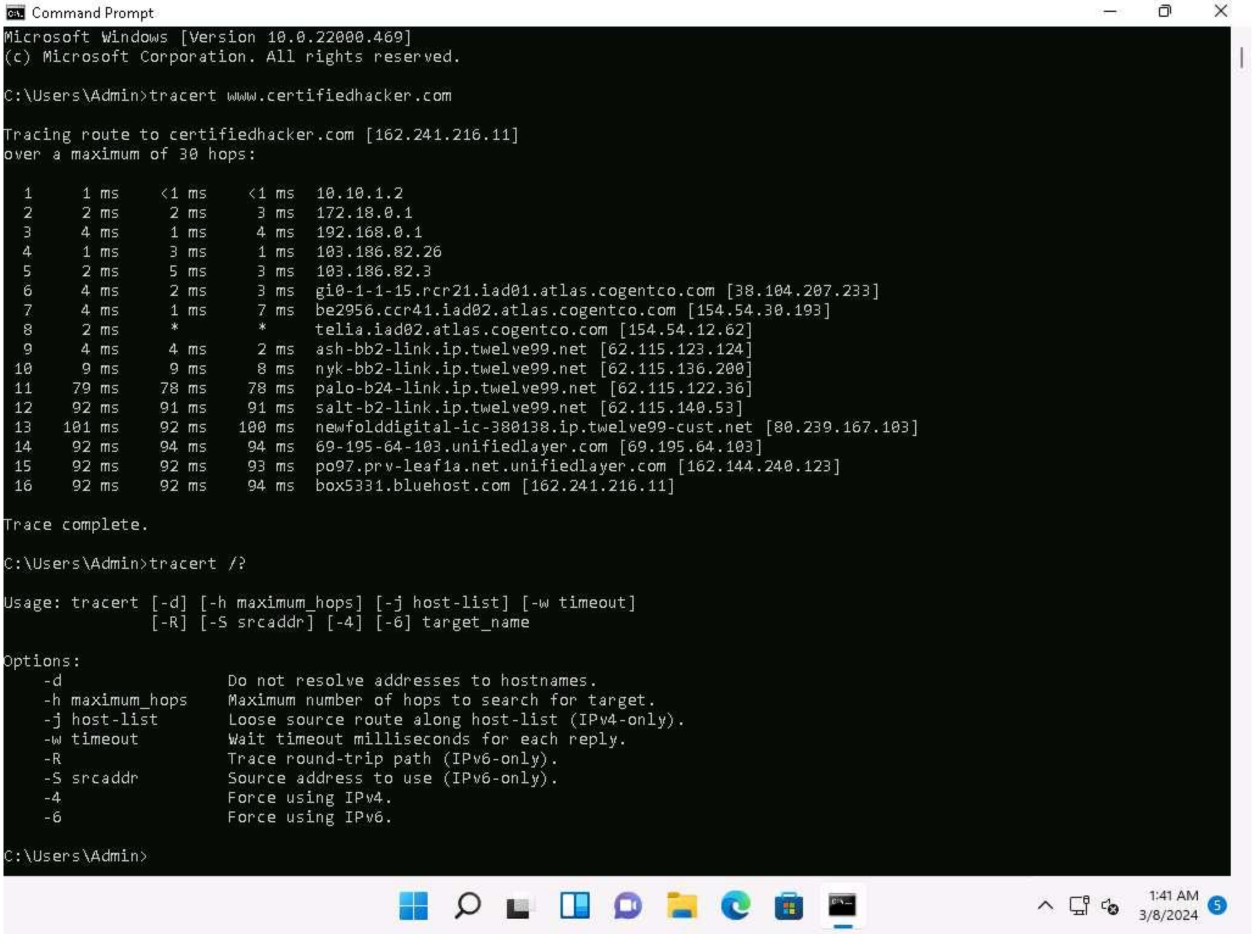
1. In the **Windows 11** machine, open the **Command Prompt** window. Run **tracert www.certifiedhacker.com** command to view the hops that the packets made before reaching the destination.

The results might differ when you perform the lab.



```
Microsoft Windows [Version 10.0.22000.469]
(c) 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     1 ms    <1 ms    <1 ms  10.10.1.2
  2     2 ms     2 ms     3 ms  172.18.0.1
  3     4 ms     1 ms     4 ms  192.168.0.1
  4     1 ms     3 ms     1 ms  103.186.82.26
  5     2 ms     5 ms     3 ms  103.186.82.3
  6     4 ms     2 ms     3 ms  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com [38.104.207.233]
  7     4 ms     1 ms     7 ms  be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193]
  8     2 ms     *        *     telia.iad02.atlas.cogentco.com [154.54.12.62]
  9     4 ms     4 ms     2 ms  ash-bb2-link.ip.twelve99.net [62.115.123.124]
 10     9 ms     9 ms     8 ms  nyk-bb2-link.ip.twelve99.net [62.115.136.200]
 11    79 ms    78 ms    78 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]
 12    92 ms    91 ms    91 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]
 13   101 ms    92 ms   100 ms  newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
 14    92 ms    94 ms    94 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
 15    92 ms    92 ms    93 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]
 16    92 ms    92 ms    94 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>
```

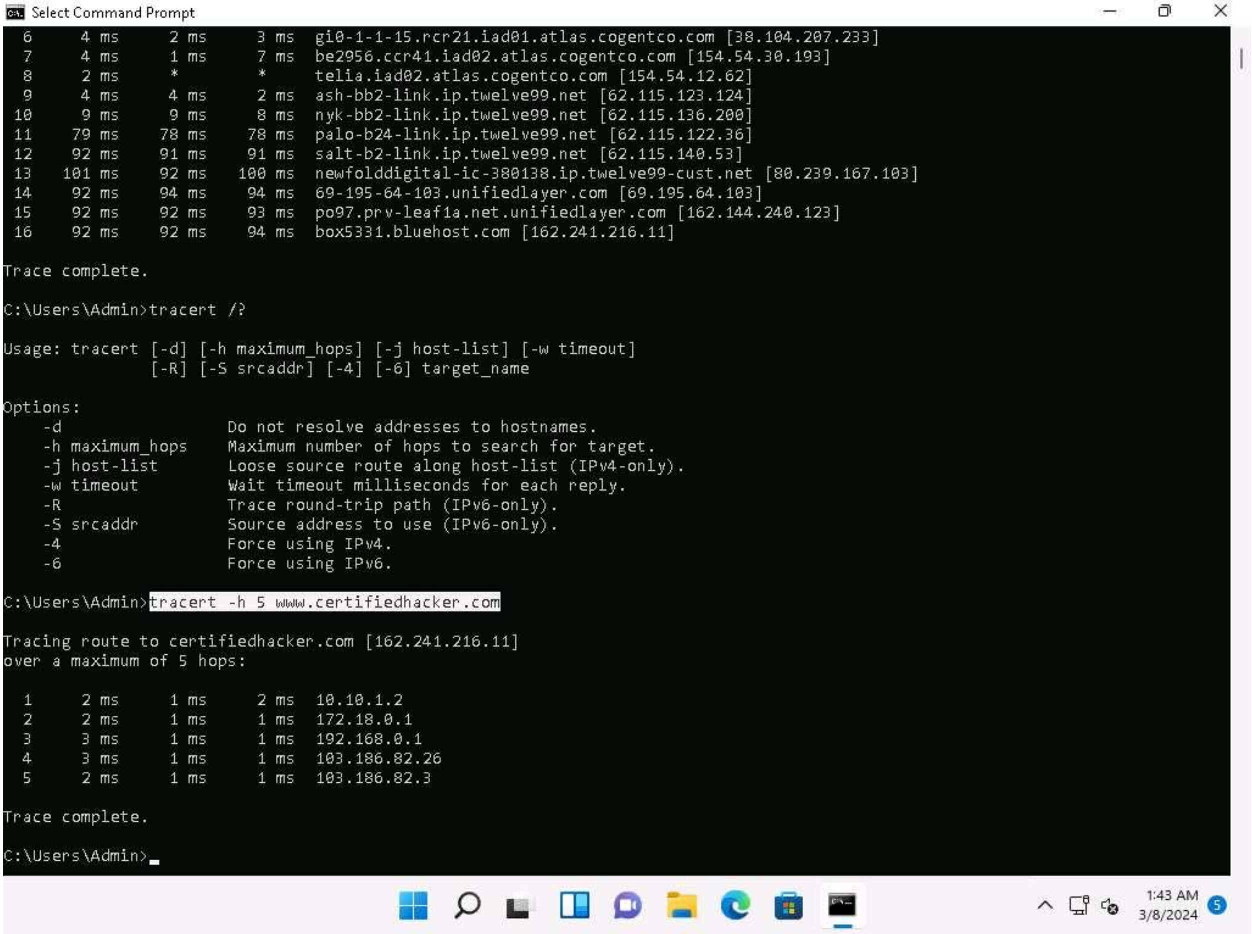
2. Run **tracert /?** command to view the different options for the command, as shown in the screenshot.



```
Microsoft Windows [Version 10.0.22000.469]
(c) 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     1 ms    <1 ms    <1 ms  10.10.1.2
  2     2 ms     2 ms     3 ms  172.18.0.1
  3     4 ms     1 ms     4 ms  192.168.0.1
  4     1 ms     3 ms     1 ms  103.186.82.26
  5     2 ms     5 ms     3 ms  103.186.82.3
  6     4 ms     2 ms     3 ms  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com [38.104.207.233]
  7     4 ms     1 ms     7 ms  be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193]
  8     2 ms     *        *     telia.iad02.atlas.cogentco.com [154.54.12.62]
  9     4 ms     4 ms     2 ms  ash-bb2-link.ip.twelve99.net [62.115.123.124]
 10     9 ms     9 ms     8 ms  nyk-bb2-link.ip.twelve99.net [62.115.136.200]
 11    79 ms    78 ms    78 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]
 12    92 ms    91 ms    91 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]
 13   101 ms    92 ms   100 ms  newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
 14    92 ms    94 ms    94 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
 15    92 ms    92 ms    93 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]
 16    92 ms    92 ms    94 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. Run **tracert -h 5 www.certifiedhacker.com** command to perform the trace, but with only 5 maximum hops allowed.

-h: Number of maximum hops.



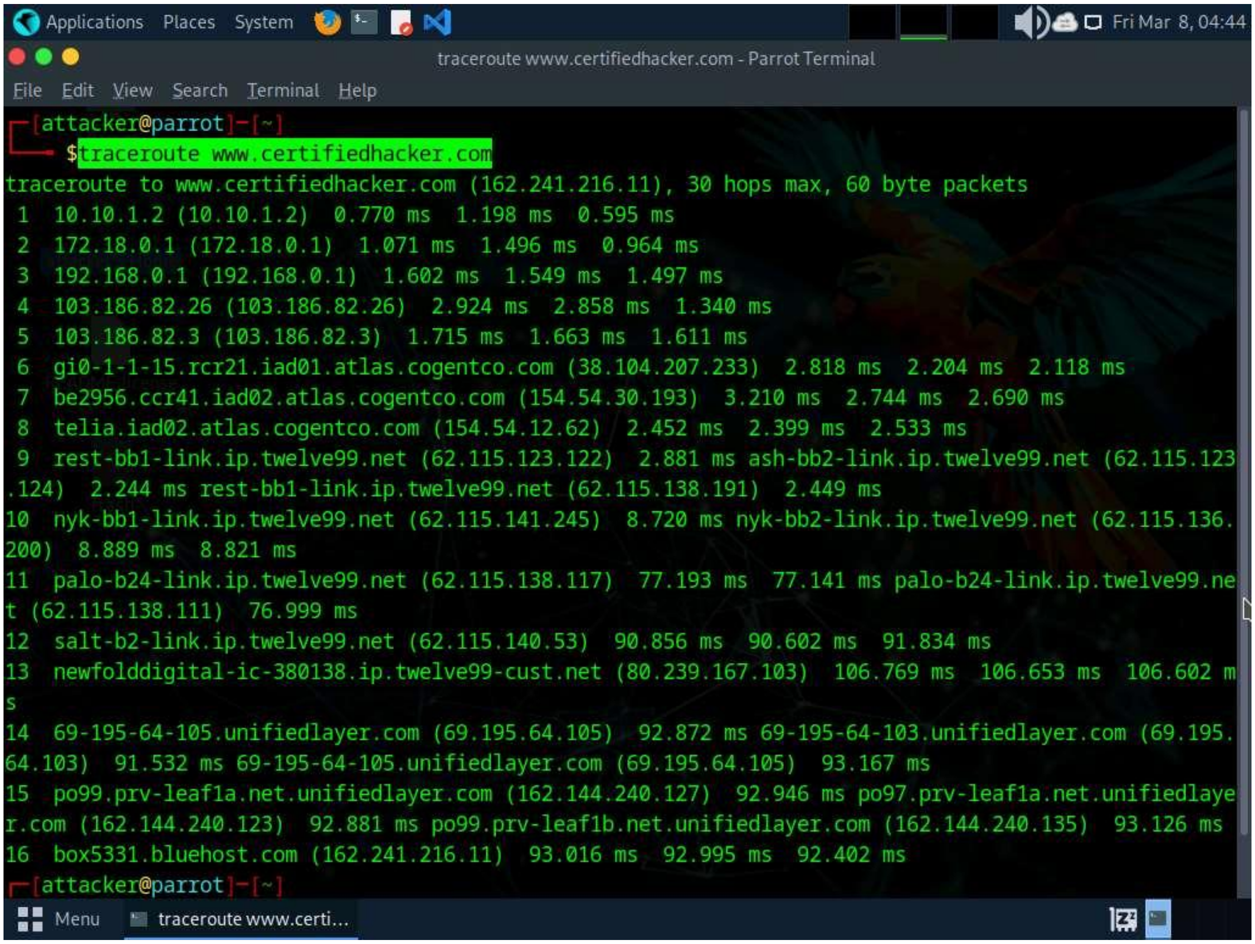
```
  6     4 ms     2 ms     3 ms  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com [38.104.207.233]
  7     4 ms     1 ms     7 ms  be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193]
  8     2 ms     *        *     telia.iad02.atlas.cogentco.com [154.54.12.62]
  9     4 ms     4 ms     2 ms  ash-bb2-link.ip.twelve99.net [62.115.123.124]
 10     9 ms     9 ms     8 ms  nyk-bb2-link.ip.twelve99.net [62.115.136.200]
 11    79 ms    78 ms    78 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]
 12    92 ms    91 ms    91 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]
 13   101 ms    92 ms   100 ms  newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
 14    92 ms    94 ms    94 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
 15    92 ms    92 ms    93 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]
 16    92 ms    92 ms    94 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 www.certifiedhacker.com

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

  1     2 ms     1 ms     2 ms  10.10.1.2
  2     2 ms     1 ms     1 ms  172.18.0.1
  3     3 ms     1 ms     1 ms  192.168.0.1
  4     3 ms     1 ms     1 ms  103.186.82.26
  5     2 ms     1 ms     1 ms  103.186.82.3

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 and open a **Terminal** window.

6. Run **traceroute www.certifiedhacker.com** command 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.



```
┌─[attacker@parrot]─[~]
└──╼ $traceroute www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  0.770 ms  1.198 ms  0.595 ms
 2  172.18.0.1 (172.18.0.1)  1.071 ms  1.496 ms  0.964 ms
 3  192.168.0.1 (192.168.0.1)  1.602 ms  1.549 ms  1.497 ms
 4  103.186.82.26 (103.186.82.26)  2.924 ms  2.858 ms  1.340 ms
 5  103.186.82.3 (103.186.82.3)  1.715 ms  1.663 ms  1.611 ms
 6  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com (38.104.207.233)  2.818 ms  2.204 ms  2.118 ms
 7  be2956.ccr41.iad02.atlas.cogentco.com (154.54.30.193)  3.210 ms  2.744 ms  2.690 ms
 8  telia.iad02.atlas.cogentco.com (154.54.12.62)  2.452 ms  2.399 ms  2.533 ms
 9  rest-bb1-link.ip.twelve99.net (62.115.123.122)  2.881 ms ash-bb2-link.ip.twelve99.net (62.115.123
.124)  2.244 ms rest-bb1-link.ip.twelve99.net (62.115.138.191)  2.449 ms
10  nyk-bb1-link.ip.twelve99.net (62.115.141.245)  8.720 ms nyk-bb2-link.ip.twelve99.net (62.115.136.
200)  8.889 ms  8.821 ms
11  palo-b24-link.ip.twelve99.net (62.115.138.117)  77.193 ms  77.141 ms palo-b24-link.ip.twelve99.ne
t (62.115.138.111)  76.999 ms
12  salt-b2-link.ip.twelve99.net (62.115.140.53)  90.856 ms  90.602 ms  91.834 ms
13  newfolddigital-ic-380138.ip.twelve99-cust.net (80.239.167.103)  106.769 ms  106.653 ms  106.602 m
s
14  69-195-64-105.unifiedlayer.com (69.195.64.105)  92.872 ms 69-195-64-103.unifiedlayer.com (69.195.
64.103)  91.532 ms 69-195-64-105.unifiedlayer.com (69.195.64.105)  93.167 ms
15  po99.prv-leaf1a.net.unifiedlayer.com (162.144.240.127)  92.946 ms po97.prv-leaf1a.net.unifiedlaye
r.com (162.144.240.123)  92.881 ms po99.prv-leaf1b.net.unifiedlayer.com (162.144.240.135)  93.126 ms
16  box5331.bluehost.com (162.241.216.11)  93.016 ms  92.995 ms  92.402 ms
┌─[attacker@parrot]─[~]
```

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

8. You can also use other traceroute tools such as **PingPlotter** (https://www.pingplotter.com/), **Traceroute NG** (https://www.solarwinds.com), etc. to extract additional network information of the target organization.

9. Close all open windows and document all acquired information.