MITM Route Table Modification

Alex Hendren

Nova Scotia Community College

ISEC2025

Assignment 1 Part 2

January 31st, 2025

Table of Contents

For this scenario:

The Kali Machine: 192.168.179.128

The Server: 192.168.179.130

The Host: 192.168.179.131

Task 1. Modify the route table of the Windows host

initialstate - Notepad

File Edit Format View Help

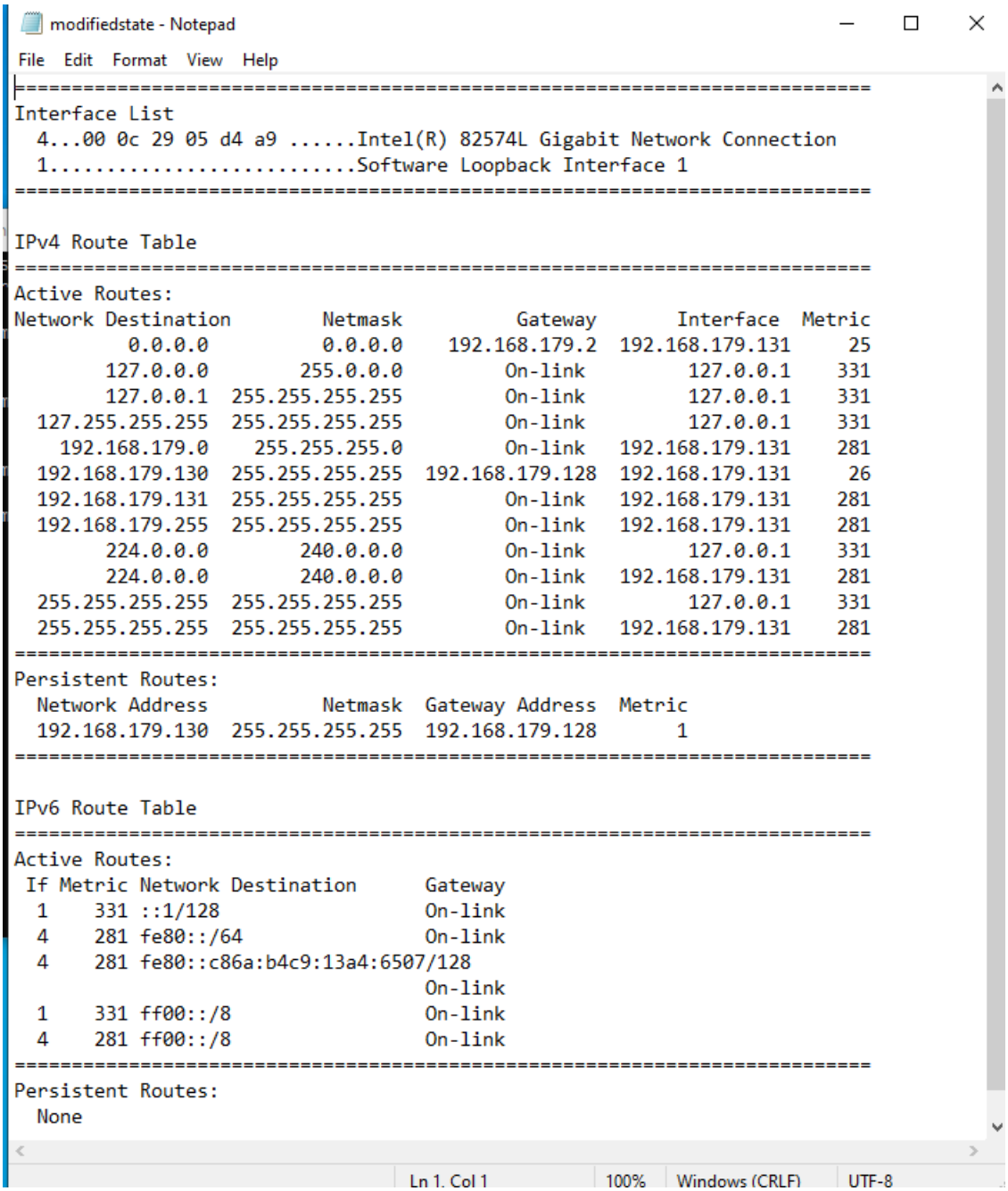
```
===========================================================================
Interface List
  4...00 0c 29 05 d4 a9 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.179.2  192.168.179.131     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.179.0    255.255.255.0         On-link   192.168.179.131    281
  192.168.179.131  255.255.255.255         On-link   192.168.179.131    281
  192.168.179.255  255.255.255.255         On-link   192.168.179.131    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.179.131    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.179.131    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  4    281 fe80::/64                On-link
  4    281 fe80::c86a:b4c9:13a4:6507/128
                                    On-link
  1    331 ff00::/8                 On-link
  4    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Figure 1. Screenshot of initial Route Table.

The command used to alter the Routing Table:

Route add 192.168.179.130 mask 255.255.255.255 192.168.179.128 metric 1 -p



```
modifiedstate - Notepad
File  Edit  Format  View  Help
===========================================================================
Interface List
  4...00 0c 29 05 d4 a9 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.179.2  192.168.179.131     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.179.0    255.255.255.0         On-link   192.168.179.131    281
  192.168.179.130  255.255.255.255  192.168.179.128  192.168.179.131     26
  192.168.179.131  255.255.255.255         On-link   192.168.179.131    281
  192.168.179.255  255.255.255.255         On-link   192.168.179.131    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.179.131    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.179.131    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
  192.168.179.130  255.255.255.255  192.168.179.128       1
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  4    281 fe80::/64                On-link
  4    281 fe80::c86a:b4c9:13a4:6507/128
                                    On-link
  1    331 ff00::/8                 On-link
  4    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
Ln 1, Col 1   100%   Windows (CRLF)   UTF-8
```

Figure 2. Screenshot showing the modified routing table showing the Kali machine is the gateway.

Task 2. Configure your kali host to forward routed packets.

To configure the kali host to forward routed packets we use the command route add -net 192.168.179.130 netmask 255.255.255.255 gw 192.168.179.130. This adds a route to the server from the kali machine. Then we enable the NAT module in iptables using the command modprobe iptable_nat. We then temporarily enable ip forwarding using echo 1>/proc/sys/net/ipv4/ip_forward. We then use the iptables postrouting rule.

Question 1. Explain in your own words what the *iptables -t nat -A POSTROUTING -o [interface] -j MASQUERAD* command does

The *iptables -t nat -A POSTROUTING -o [interface] -j MASQUERAD* command enables masquerading on whatever interface you specify. Masquerading makes the server send its responses to the kali where they are then sent to the victim. Masquerading works by changing the IP address of packets from the host to use the Kali's IP address.

Question 2.

Case 1.

The command would not be needed because we can already see the traffic from the victim to the server because we added our kali IP as a route in the victims route table. We only enable masquerading to intercept the servers response back to the host.

Case 2.

Yes, because if we were not using masquerading the server would send replies directly to the host, not the kali. If that was happening, we would only be seeing outbound traffic from the host because we wouldn't be able to see the servers reply. When we use masquerading, when the server replies to the host, it actually replies to the Kali. The Kali then forwards to the victim, letting us see both inbound and outbound traffic.

Task 3. Test that the Windows Host now routes its packets through the kali machine

routingresult - Notepad

File Edit Format View Help

```
Tracing route to DESKTOP-Q4MUI94 [192.168.179.130]
over a maximum of 30 hops:

  1     *       <1 ms    <1 ms  192.168.179.128
  2    <1 ms    <1 ms    <1 ms  DESKTOP-Q4MUI94 [192.168.179.130]

Trace complete.
```

Figure 3. Screenshot of tracert on server host IP.