

Baek Seunghyuk

Sbaek44@vt.edu

ECE 5480 Fall 2018

Homework 4

1. How many IP addresses are available under IPv4? How many IP addresses are available under IPv6?

IPv4 has 32 bits so 2^{32}

IPv6 has 128 bits, 3.4×10^{38}

2. What is the difference between a MAC address and an IP address?

MAC address is tied to physical hardware (network card in computer) as a serial number. When a manufacturer produces network card, it assigns MAC address in the product's memory. Therefore, it is very rare to have same MAC address in a same local network. IP address is network address that is assigned by operating system. While MAC address is used to communicate with devices within local network, IP address is better when it is used to communicate via larger network like internet.

3. Explain how to use the three-way TCP handshake protocol to perform a distributed denial-of-service attack, such that the victim is any host computer on the Internet and the sites that are attacking the victim with packets are legitimate (not web servers created by the attacker) web servers.

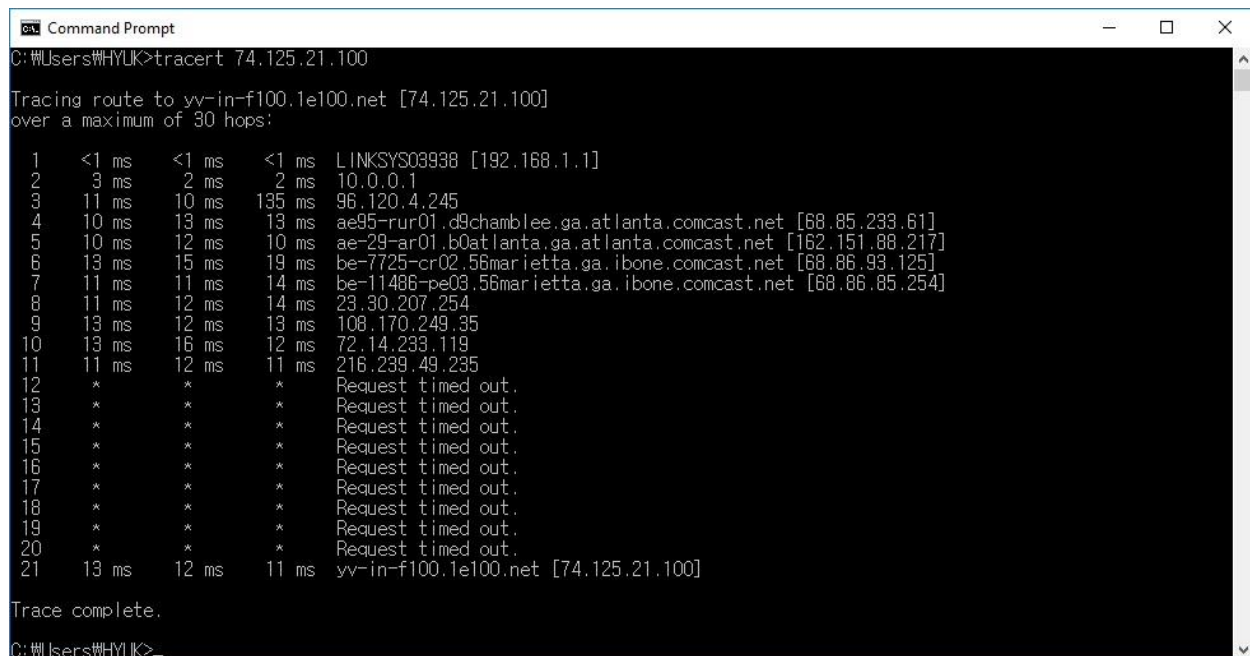
According to 3-way handshake protocol, web-server or service provide receives SYN flagged packet and response with SYN/ACK then receives ACK from the client. This 3-way handshake combined with IP spoofing can launch attack on a victim's computer in following scenario. First, an attacker has many infected IP devices and these infected IP devices are disguised as the victim using IP spoofing. Second, an attacker's botnet sends SYN packet to multiple legitimate web-servers. Because botnet is using the victim's IP address, all SYN/ACK packets are sent to victim's network creating overflow of traffic.

4. Describe the rules to modify a NAT router to prevent packets with spoofed IP addresses from exiting a private network.

NAT device (router) will assign new private IP address whenever new devices are connected to the private network. Then, the router can store all private IP addresses of the network in a look up table.

This table will store the IP address and MAC address so that the router always can locate a particular device within the network. When a packet with spoofed IP address tries to leave a private network, NAT router will match the IP address of the packet with known IP addresses in the table. If the router cannot find the matching IP address, it filters the packet.

5. Run traceroute (traceroute on a UNIX-based machine, tracert on Windows) to 74.125.21.100. Report the result (screenshot or copy/paste your traceroute output) and briefly explain what the values mean, including why there may be “* * *” in the result.



```
Command Prompt
C:\Users\HYUK>tracert 74.125.21.100

Tracing route to yv-in-f100.1e100.net [74.125.21.100]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    LINKSYS03938 [192.168.1.1]
  1  3 ms      2 ms      2 ms      10.0.0.1
  2  11 ms     10 ms     135 ms     96.120.4.245
  3  10 ms     13 ms     13 ms      ae95-rur01.d9chamblee.ga.atlanta.comcast.net [68.85.233.61]
  4  10 ms     12 ms     10 ms      ae-29-ar01.b0atlanta.ga.atlanta.comcast.net [162.151.88.217]
  5  13 ms     15 ms     19 ms      be-7725-cr02.56marietta.ga.ibone.comcast.net [68.86.93.125]
  6  11 ms     11 ms     14 ms      be-11486-pe03.56marietta.ga.ibone.comcast.net [68.86.85.254]
  7  11 ms     12 ms     14 ms      23.30.207.254
  8  13 ms     12 ms     13 ms      108.170.249.35
  9  13 ms     16 ms     12 ms      72.14.233.119
 10  11 ms     12 ms     11 ms      216.239.49.235
 11  *         *         *         Request timed out.
 12  *         *         *         Request timed out.
 13  *         *         *         Request timed out.
 14  *         *         *         Request timed out.
 15  *         *         *         Request timed out.
 16  *         *         *         Request timed out.
 17  *         *         *         Request timed out.
 18  *         *         *         Request timed out.
 19  *         *         *         Request timed out.
 20  *         *         *         Request timed out.
 21  13 ms     12 ms     11 ms      yv-in-f100.1e100.net [74.125.21.100]

Trace complete.
C:\Users\HYUK>
```

Tracert sends ICMP packets to routers between the packet sender and destination of the packet. Tracert sends packets with various TTL values so that returning message can be used in tracing the routers in the path. Very first value of tracert is this TTL value. Above this value is starting from 1 and extends to 21. Next 3 values are response time. Tracert sends 3 packets for each TTL. And the last value is IP address and name of router. If somehow tracert is not able to receive a response signal within certain period, * * * value will appear and 'request timed out' message will be printed. This can happen because of disconnection of the network or setting of the router that is blocked to send response to ICMP packet.

6. You have sniffed the packet below on your network. Assuming the IP header starts with the circled byte, for each field in the IP header and the protocol header that follows the IP header, state the field name, the contents (in hex) of that field, and a brief description of the purpose of that field.

Starting with 45 in circle.

4 – IPv4

5 – Internet header length, $5 \times 32 = 160$ bits long

0 – DSCP: type of service, here it does not used

0 – ECN: congestion notification without dropping packet, here it does not used

00 42 – entire packet size, here is 66 bytes

91 a9 - identifying the group of fragments

00 00 – flag and fragment offset

ff – TTL: maximum number of hops, here is 255

11 – protocol: here is UDP protocol

55 43 - check sum: for error checking

c0 a8 04 06 - source IP address, here is 192.168.4.6

08 08 08 08 - destination IP address: 8. 8. 8. 8

Because this uses UDP protocol, next bytes are UDP header.

e4 b6 – source port: port 58550 of source IP

00 35 – destination port: port 53 of destination IP

00 2e – Length: total bytes of UDP header and data, here is 46 bytes

79 c0 – used for error checking