Wireshark Assignment 3
Onur Özdemir
2036473

I filtred the packets by using “ICMP” as input.

1) User’s IP Address: 10.10.3.2 **Corresponding Ovs IP**: 10.10.3.1
Attacker’s IP Address: 10.10.2.2 **Corresponding Ovs IP**: 10.10.2.1
Victim’s IP Address: 10.10.1.1 **Corresponding Ovs IP:** 10.10.1.2

2) Because the ICMP protocol runs on network layer. There is no port information on that layer. The port information starts to take role with Transport Layer. The ICMP protocol not designed to communicate between application layer processes.

3)

Request Packet Number	**Corresponding Sequence number**	**Corresponding Reply Packets**
1	In Big Endian: 7 In Little Endian: 1792	No response
2	In Big Endian: 7 In Little Endian: 1792	3
5	In Big Endian: 5 In Little Endian: 1280	6
7	In Big Endian: 8 In Little Endian: 2048	No response
8	In Big Endian: 8 In Little Endian: 2048	9

4) First ping request packet with an existing corresponding reply packet is packet with number 2**.** Reply packet is packet with number: 3

For request packet(Packet with no: 2)
ICMP type is 8 which is Echo (ping) request.
Code number is: 0
Checksum is 2 bytes.
Sequence number is 2 bytes.
Identifier is also 2 bytes.

For response packet(Packet with no: 3)
ICMP type is 0 which is Echo (ping) reply.
Code number is: 0
Checksum is 2 bytes.
Sequence number is 2 bytes.
Identifier is also 2 bytes.

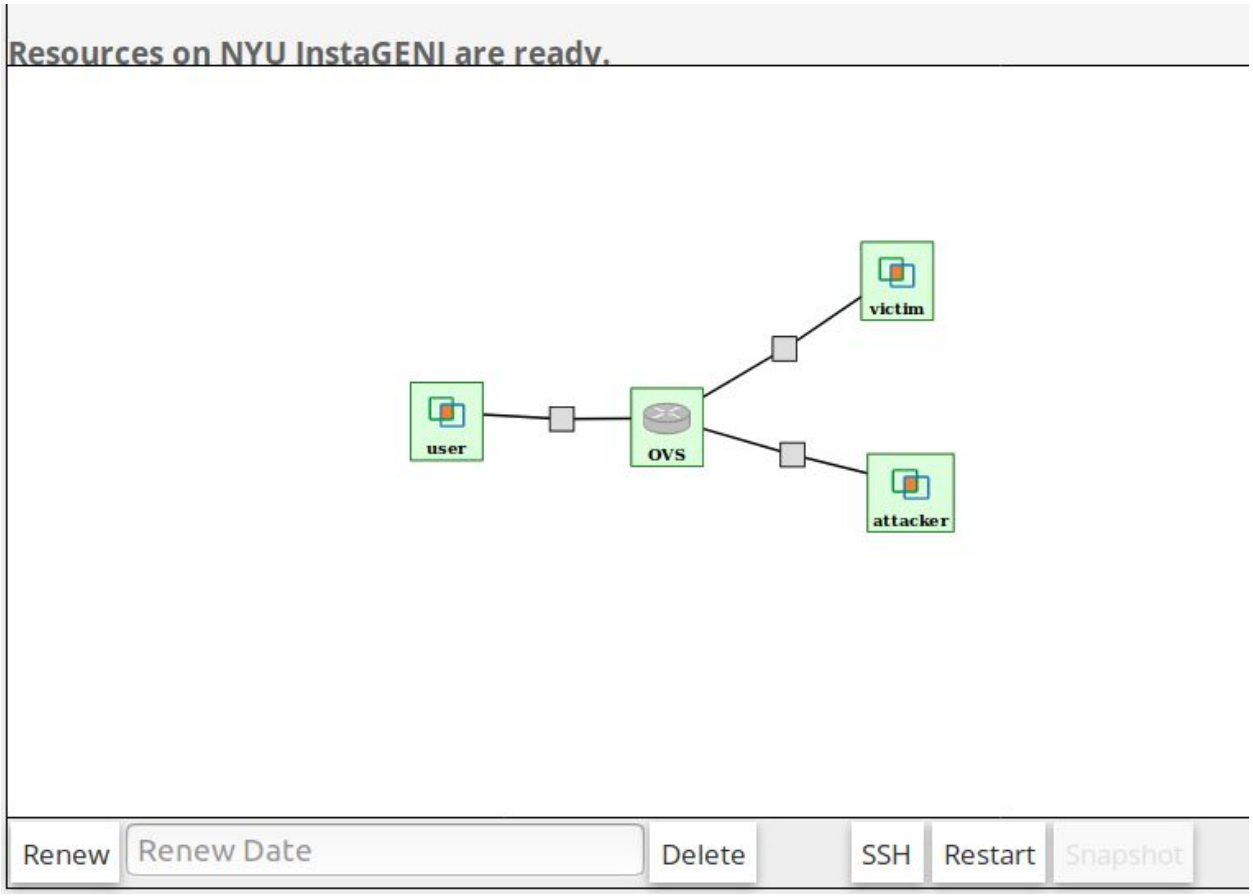
5) TTL is the number of hops that a packet can make after passing through a router. That's why whenever a packet is passed a router the TTL number of that packet is decremented by 1.

For Packets with **Source: 10.10.3.2, Destination: 10.10.3.1 (User is pinging the OVS)...**
Those packets are representing the case where user is pinging the OVS. The packets have TTL value of 64. OVS is working on the router. That's why the ping packets generated by the user is not passing the router (No need to decrement) . The response TTL values are the same as generated TTL values which is 64 with Source: 10.10.3.1, Destination 10.10.3.2 this time.

For Packets with **Source: 10.10.2.2, Destination: 10.10.1.1 (Attacker is pinging the victim)...**
Those packets are representing the case where the attacker is pinging the victim. The packets have TTL value of 64 at the beginning. Victim is otherside of the router. That's why the packets will hop to the otherside. That's also the reason for "no response" is found for those packets. The TTL value should be decremented while transfering the packet to otherside. The packet goes to the victim with the TTL value of 63 from OVS. These packets have source: 10.10.2.2 and destination 10.10.1.1 again. After OVS is decrement the TTL value and transfer the packet to victim, Victim creates a new packet which is a reply packet with TTL: 64 and Source: 10.10.1.1, Destination 10.10.2.2. Same as the first packet, this packet will also hop through the otherside of the router. After the OVS takes the packet the TTL value is decremented by 1 and become 63. Then the packet is transferred to the attacker with TTL value 63, these packets also has Source: 10.10.1.1 and Destination: 10.10.2.2 .

6)

Graphical Illustration:



Continues in next page...

Details Page:

Continues in next page...

Node #2:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	attacker	pc2	2019-01-10T23:36:44.000Z	emulab-xen	attacker.Wireshark-e2036473.ch-geni-net.genirack.nyu.edu
Login	ssh eksert@pc2.genirack.nyu.edu -p 29051 ssh e2036473@pc2.genirack.nyu.edu -p 29051 ssh eronur@pc2.genirack.nyu.edu -p 29051 ssh alperen@pc2.genirack.nyu.edu -p 29051				

Interfaces		MAC	Layer 3
interface-3	pc2:lo0	02b8fa8965e3	ipv4: 10.10.2.2

Node #3:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	user	pc2	2019-01-10T23:36:44.000Z	emulab-xen	user.Wireshark-e2036473.ch-geni-net.genirack.nyu.edu
Login	ssh eksert@pc2.genirack.nyu.edu -p 29052 ssh e2036473@pc2.genirack.nyu.edu -p 29052 ssh eronur@pc2.genirack.nyu.edu -p 29052 ssh alperen@pc2.genirack.nyu.edu -p 29052				

Interfaces		MAC	Layer 3
interface-5	pc2:lo0	02aed00e6e06	ipv4: 10.10.3.2

Node #4:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	OVS	pc2	2019-01-10T23:36:44.000Z	emulab-xen	OVS.Wireshark-e2036473.ch-geni-net.genirack.nyu.edu
Login	ssh eksert@pc2.genirack.nyu.edu -p 29050 ssh e2036473@pc2.genirack.nyu.edu -p 29050 ssh eronur@pc2.genirack.nyu.edu -p 29050 ssh alperen@pc2.genirack.nyu.edu -p 29050				

Interfaces		MAC	Layer 3
interface-1	pc2:lo0	02256d1298df	ipv4: 10.10.1.2
interface-2	pc2:lo0	02afcd2c4b0c	ipv4: 10.10.2.1
interface-4	pc2:lo0	026fc44f629e	ipv4: 10.10.3.1

Link #1:

Client ID	Endpoint #0	Endpoint #1
link-0	interface-0	interface-1

Link #2:

Client ID	Endpoint #0	Endpoint #1
link-1	interface-2	interface-3

Link #3:

Client ID	Endpoint #0	Endpoint #1
link-2	interface-4	interface-5