Student Information

Full Name : Yavuz Selim Yesilyurt
Id Number : 2259166

Answer 1

IP numbers of the interfaces of attacker, victim, user to OVS are; 10.10.2.2, 10.10.1.1 and 10.10.3.2 respectively. Ip numbers of the interfaces of OVS machines are; 10.10.3.1 (interface to user), 10.10.1.2 (interface to victim) and 10.10.2.1 (interface to attacker).

Answer 2

Because ICMP is a Network Layer protocol and it is established between host to host; not between process to process. Since it is not established between process to process it doesn't need a port number on either side.

Answer 3

Wireshark sequence numbers of first 5 request packets with their corresponding reply packets are:

$$\begin{gathered}12 -> \text{no reply packet}\\ 13 -> 14 \text{ is the reply packet}\\ 15 -> \text{no reply packet}\\ 16 -> \text{no reply packet}\\ 17 -> 18 \text{ is the reply packet}\end{gathered}$$

Answer 4

First ICMP request packet does not have any response so I decided to examine second ICMP request packet.

Its wireshark sequence number is 13, ICMP type is 8 (Echo (ping) request), code number is 0, checksum field is 2 bytes, sequence number field is 2 bytes, identifier 2 is bytes.

Its reply packet's wireshark sequence number is 14, ICMP type is 0 (Echo (ping) reply), code number is 0, checksum field is 2 bytes, sequence number field is 2 bytes, identifier field is 2 bytes.

Answer 5

Following table shows TTL values of packets by means of source-destination address pairs:

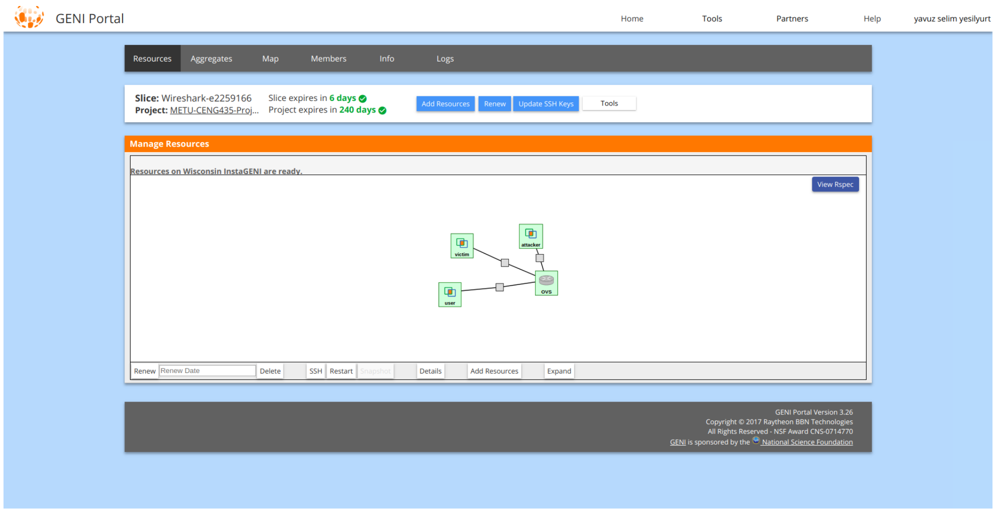
Source - Destination	TTL Value
10.10.2.2 - 10.10.1.1 (1st request-with no reply)	64
10.10.2.2 - 10.10.1.1 (2nd request)	63
10.10.1.1 - 10.10.2.2 (1st reply)	64
10.10.1.1 - 10.10.2.2 (2nd reply-with no request)	63
10.10.3.2 - 10.10.3.1	64
10.10.3.1 - 10.10.3.2	64

There seems a problem on ICMP packets betweeen 10.10.2.2 and 10.10.1.1. For every request/reply cluster, 10.10.2.2 interface of attacker sends a request packet with ttl=64, but it gets no response; so it sends another request packet with ttl=63, then it gets response from victim with ttl=64. Afterwards, victim sends another reply packet(seemingly a reply packet for the first request packet of attacker) with ttl=63 but it does not reply any of the request packets from 10.10.2.2.

For TTL values, we see that ttl value for the first transmitted packet(request or reply does not matter) is 64 and for each retransmitted ICMP packet ttl values gets decremented by one. For instance, as can be seen in above table, ttl values of retransmitted request packet from 10.10.2.2 and retransmitted reply packet from 10.10.1.1 are 63, whereas in their first transmissions they were 64.

Answer 6

Screenshot of graphical illustration of resources:

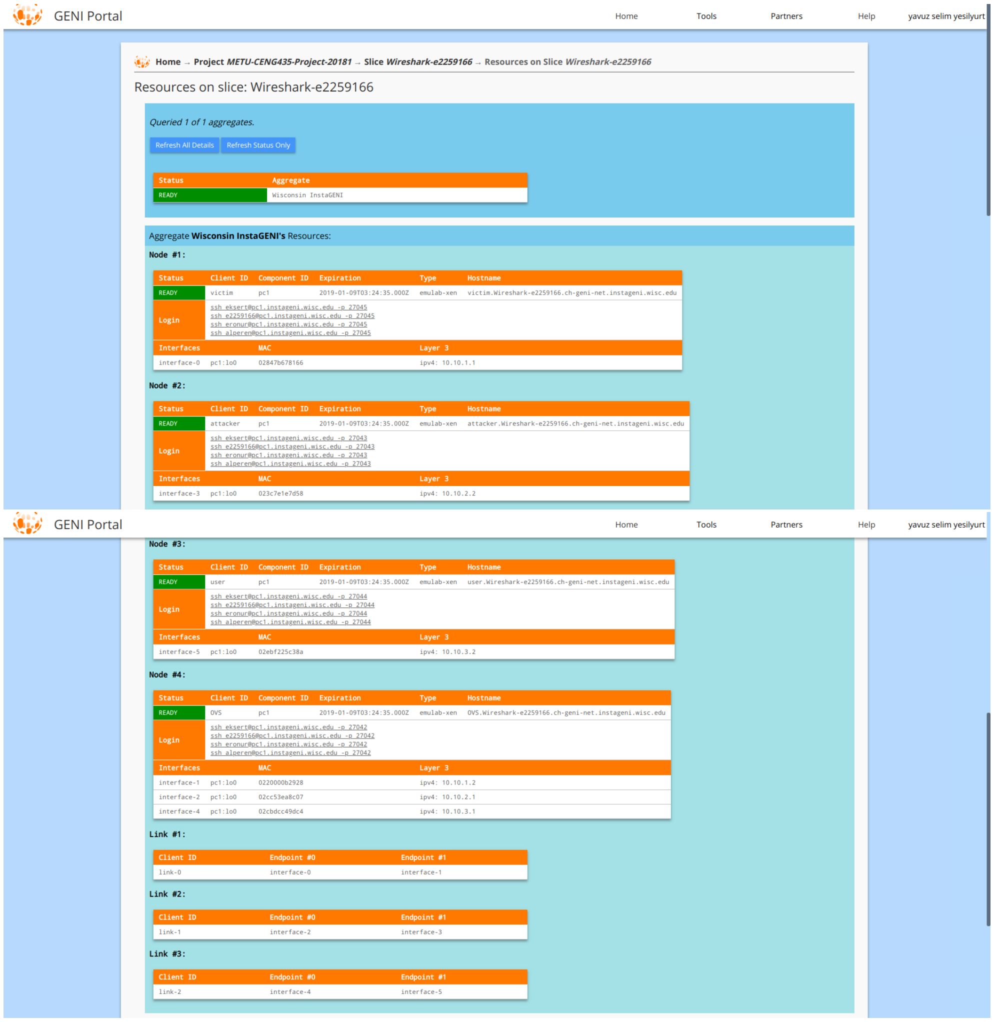


Slice: Wireshark-e2259166 Slice expires in **6 days** ✓
Project: METU-CENG435-Proj... Project expires in **240 days** ✓

Resources on Wisconsin InstaGENI are ready.

GENI Portal Version 3.26
Copyright © 2017 Raytheon BBN Technologies
All Rights Reserved - NSF Award CNS-0714770
GENI is sponsored by the National Science Foundation

Screenshot "details" page:



Home → **Project *METU-CENG435-Project-20181*** → **Slice *Wireshark-e2259166*** → Resources on Slice *Wireshark-e2259166*

Resources on slice: Wireshark-e2259166

Queried 1 of 1 aggregates.

Status	Aggregate
READY	Wisconsin InstaGENI

Aggregate **Wisconsin InstaGENI's** Resources:

Node #1:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	victim	pc1	2019-01-09T03:24:35.000Z	emulab-xen	victim.Wireshark-e2259166.ch-geni-net.instageni.wisc.edu
Login	ssh eksert@pc1.instageni.wisc.edu -p 27045 ssh e2259166@pc1.instageni.wisc.edu -p 27045 ssh eronur@pc1.instageni.wisc.edu -p 27045 ssh alperen@pc1.instageni.wisc.edu -p 27045				
Interfaces		MAC		Layer 3	
interface-0	pc1:lo0	02847b678166		ipv4: 10.10.1.1	

Node #2:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	attacker	pc1	2019-01-09T03:24:35.000Z	emulab-xen	attacker.Wireshark-e2259166.ch-geni-net.instageni.wisc.edu
Login	ssh eksert@pc1.instageni.wisc.edu -p 27043 ssh e2259166@pc1.instageni.wisc.edu -p 27043 ssh eronur@pc1.instageni.wisc.edu -p 27043 ssh alperen@pc1.instageni.wisc.edu -p 27043				
Interfaces		MAC		Layer 3	
interface-3	pc1:lo0	023c7e1e7d58		ipv4: 10.10.2.2	

Node #3:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	user	pc1	2019-01-09T03:24:35.000Z	emulab-xen	user.Wireshark-e2259166.ch-geni-net.instageni.wisc.edu
Login	ssh eksert@pc1.instageni.wisc.edu -p 27044 ssh e2259166@pc1.instageni.wisc.edu -p 27044 ssh eronur@pc1.instageni.wisc.edu -p 27044 ssh alperen@pc1.instageni.wisc.edu -p 27044				
Interfaces		MAC		Layer 3	
interface-5	pc1:lo0	02ebf225c38a		ipv4: 10.10.3.2	

Node #4:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	OVS	pc1	2019-01-09T03:24:35.000Z	emulab-xen	OVS.Wireshark-e2259166.ch-geni-net.instageni.wisc.edu
Login	ssh eksert@pc1.instageni.wisc.edu -p 27042 ssh e2259166@pc1.instageni.wisc.edu -p 27042 ssh eronur@pc1.instageni.wisc.edu -p 27042 ssh alperen@pc1.instageni.wisc.edu -p 27042				
Interfaces		MAC		Layer 3	
interface-1	pc1:lo0	0220000b2928		ipv4: 10.10.1.2	
interface-2	pc1:lo0	02cc53ea8c07		ipv4: 10.10.2.1	
interface-4	pc1:lo0	02cbdcc49dc4		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