

Late Labs - marvleon

Lab 1.2 ARP Wireshark Netsim	1
1.2.1 ARP (linux.cs.pdx.edu)	1
1.2.2 -	1
1.2.3 ARP (Cloud)	2
1.2.4 NetSim Cloud	3
Lab 1.3 Cloud Networking	4
1.3.3 Scan targets for services	4
1.3.5 Navigating Default Networks	4
1.3.6 Creating custom networks	5

Lab 1.2 ARP Wireshark Netsim

1.2.1 ARP (linux.cs.pdx.edu)

IPv4 address (ens): 131.252.208.103
Hardware address: 52:54:00:13:a0:c6
Default router's IP address: 131.252.208.1
Default router name: router.seas.pdx.edu
Default router hardware address: 00:00:5e:00:01:01
50 entries in the ARP table

1.2.2 -

List any IP addresses share the same hardware address

(30:e4:db:f9:26:37) 131.252.208.212, 169.254.169.254
(52:54:00:5f:45:5f) 131.252.208.121, 131.252.208.20

How many less hardware addresses are there than IP addresses in the ARP table?

```
arp -a | sort -k 4 | awk '{print $4}' | uniq | wc -l
```

(2)

Use a single command-line to create a file that contains each IP address that appears in the machine's arp table and places the results in a file called arp_entries.

```
arp -an | awk -F '[]' '{print $2}' > arp_entries
```

What network prefix do most of the IP addresses in the ARP table share?

131.252.208

1.2.3 ARP (Cloud)

IPv4 address of ens4: 10.138.0.2

Hardware address: 42:01:0a:8a:00:02

Default Router IP address: 10.138.0.1

Default Router Hardware address: 42:01:0a:8a:00:01

1.2.4 NetSim Cloud

Inbox (247) - marvleon@pdx.edu x CS4G Network Simulator x +

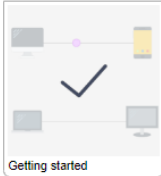
netsim.erinn.io

Netsim

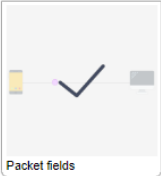
Welcome to Netsim! If this is your first time playing, we recommend you start from the first level below, and work your way forward. [Log out](#)

Please note that this project is still in beta. If you find any bugs, you can report them to [@errorin](#) or open an issue on [Github](#).

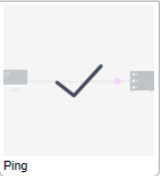
Basics



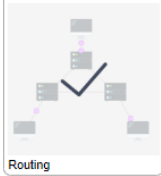
Getting started




Packet fields



Ping

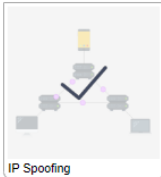


Routing

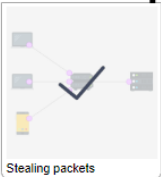


Modems

Spoofs

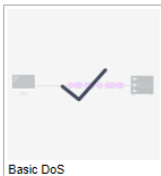


IP Spoofing

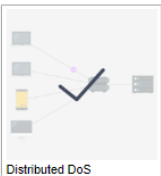


Stealing packets

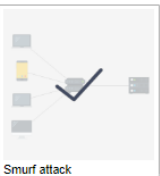
Denial of Service



Basic DoS

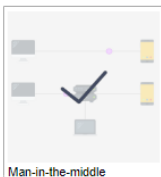


Distributed DoS




Smurf attack


Attacks



Man-in-the-middle



Censorship



Traceroute

marvleon

Lab 1.3 Cloud Networking

1.3.3 Scan targets for services

```
marvleon@course-vm:~$ nmap 10.138.0.29
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-09 09:19 UTC
Nmap scan report for multi-tier-wordpress-1-node-0.c.cloud-leon-marvleon.internal (10.138.0.29)
Host is up (0.00022s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
marvleon@course-vm:~$ nmap 10.138.0.31
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-09 09:19 UTC
Nmap scan report for tomcat-1-vm.c.cloud-leon-marvleon.internal (10.138.0.31)
Host is up (0.00021s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
marvleon@course-vm:~$ nmap 10.138.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-09 09:19 UTC
Nmap scan report for wordpress-1-vm.c.cloud-leon-marvleon.internal (10.138.0.30)
Host is up (0.00027s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
marvleon@course-vm:~$
```

1.3.5 Navigating Default Networks

```
marvleon@cloudshell:~ (cloud-leon-marvleon)$ gcloud compute networks subnets list | grep default | wc -l
84
marvleon@cloudshell:~ (cloud-leon-marvleon)$ gcloud compute networks subnets list | grep REGION | awk '{print $2}' | sort | uniq | wc -l
42
marvleon@cloudshell:~ (cloud-leon-marvleon)$
```

- Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?
 - 4094
- Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands?
 - US-WEST-1-b is brought up in 10.138.0.0/20
 - US-EAST-1-b is brought up in 10.142.0.0/20
 - Yes they correspond to the appropriate region
- What facilitates this connectivity: the virtual switch or the VPN Gateway?
 - Virtual Switch

1.3.6 Creating custom networks

```
marvleon@cloudshell:~ (cloud-leon-marvleon) $ gcloud compute networks subnets list --network custom-network1
NAME: subnet-us-central-192
REGION: us-central1
NETWORK: custom-network1
RANGE: 192.168.1.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: subnet-europe-west-192
REGION: europe-west1
NETWORK: custom-network1
RANGE: 192.168.5.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
marvleon@cloudshell:~ (cloud-leon-marvleon) $ gcloud compute networks subnets list --regions=europe-west1
NAME: default
REGION: europe-west1
NETWORK: default
RANGE: 10.132.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: subnet-europe-west-192
REGION: europe-west1
NETWORK: custom-network1
RANGE: 192.168.5.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

- Explain why the result of this ping is different from when you performed the ping to instance-2
 - It's different because its on a different subnet!

cloud-Leon-marvleon		Search (/) for resources, docs, products, and more			Search			7
VM instances		CREATE INSTANCE	IMPORT VM	REFRESH				
<input type="checkbox"/>	✓	instance-1	us-west1-b	10.138.0.32	35.197.73.116 (nic0)	default	SSH	
<input type="checkbox"/>	✓	instance-2	us-east1-b	10.142.0.3 (nic0)	35.231.174.63 (nic0)	default	SSH	
<input type="checkbox"/>	✓	instance-3	us-central1-a	192.168.1.2 (nic0)	35.232.241.17 (nic0)	custom-network1	SSH	
<input type="checkbox"/>	✓	instance-4	europe-west1-d	192.168.5.2 (nic0)	34.79.118.202 (nic0)	custom-network1	SSH	

cloud-Leon-marvleon

vpc net

←

VPC network details

DELETE VPC NETWORK

custom-network1

<

OVERVIEW

SUBNETS

STATIC INTERNAL IP ADDRESSES

FIREWALLS

FIREWALL ENDPOINTS

ROU

Subnets

+ ADD SUBNET

≡ FLOW LOGS

Filter

Enter property name or value

<input type="checkbox"/>	Name ↑	Region	Stack Type	Internal IP ranges	Gateway	Private Google Acces
<input type="checkbox"/>	subnet-europe-west-192	europe-west1	IPv4	192.168.5.0/24	192.168.5.1	Off
<input type="checkbox"/>	subnet-us-central-192	us-central1	IPv4	192.168.1.0/24	192.168.1.1	Off