

TABLE OF CONTENTS:

I. Lab 1.2 - ARP, Wireshark, Netsim.....	2
1. ARP.....	2
2. -.....	2
3. ARP (Cloud).....	2
4. Netsim.....	2
II. Lab 1.3 - Cloud Networking.....	3
1. Network Scanning (nmap) #1.....	3
2. Launch targets.....	3
3. Scan targets for services.....	4
4. CIDR and Subnets #2.....	4
5. Navigating Default Networks.....	5
6. Creating Custom Networks.....	6

I. Lab 1.2 - ARP, Wireshark, Netsim

1. ARP

- ada's IP address is `131.252.208.103` and its MAC address is `52:54:00:13:a0:c6`.
- `netstat -rn` tells me that the default router's IP address is `131.252.208.1`.
- `arp` tells me that the router's name is `router.seas.pdx.edu` and its MAC/HW address is `00:00:5e:00:01:01`.
- `arp -a | wc -l` tells me there are 45 entries in the ARP table.

2. -

- `arp -a | sort -k 4 | column -t` tells me that:
`169.254.169.254` and `131.252.208.212` share `30:e4:db:f9:26:37`, and
`131.252.208.15` and `131.252.208.7` share `cc:aa:77:2e:16:a0`.
- Now we're cooking with unix! I love pipes.
`arp -a | sort -k 4 | awk '{print $4}' | uniq | wc -l` tells me that there are 43 unique MAC addresses whereas there are 45 unique ARP table entries (IP addresses), so there are 2 fewer MAC addresses than there are IP addresses.
- `arp -an | awk -F '[]' '{print $2}' > arp_entries` (and then examining the output with `cat`) tells me that most of the IP addresses in Ada's ARP table share the 24-bit prefix `131.252.208`.

3. ARP (Cloud)

- `ip a` tells me the IP address of my cloud VM is `10.138.0.2` and its MAC address is `02:42:5c:60:cb:a9`.
- `netstat -rn` tells me the default router's IP address is `10.138.0.1`.
- `arp` tells me the MAC address of the default router is `42:01:0a:8a:00:01`.

4. Netsim

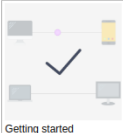
This was really cute and fun. Screenshot overflows to the next page.

Netsim

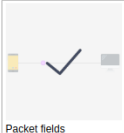
Welcome to Netsim! If this is your first time playing, we recommend you start from the first level below, and work your way forward. [Log out](#)

Please note that this project is still in **beta**. If you find any bugs, you can report them to [@error404](#) or open an issue on [Github](#).


Basics




Getting started




Packet fields



Ping




Routing

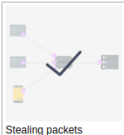


Modems

Spoofs




IP Spoofing




Stealing packets

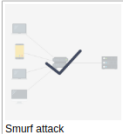
Denial of Service



Basic DoS




Distributed DoS




Smurf attack


Attacks



Man-in-the-middle



Censorship



Traceroute

```
meelzBox:~ > psu
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-75-generic x86_64)

=====
This machine is for the exclusive use of those associated with
the Maseeh College of Engineering and Computer Science.

=====
ALL ACTIVITY MAY BE RECORDED
=====
* CAT Support:   https://cat.pdx.edu/
* Email:        support@cat.pdx.edu
* Phone:        503-725-5420
* Chat:         https://support.cat.pdx.edu
* Location:     FAB 82-01

Last login: Sat Sep 30 10:41:59 2023 from 104.220.249.53
ada:~ > whoami
amminer
ada:~ >
```

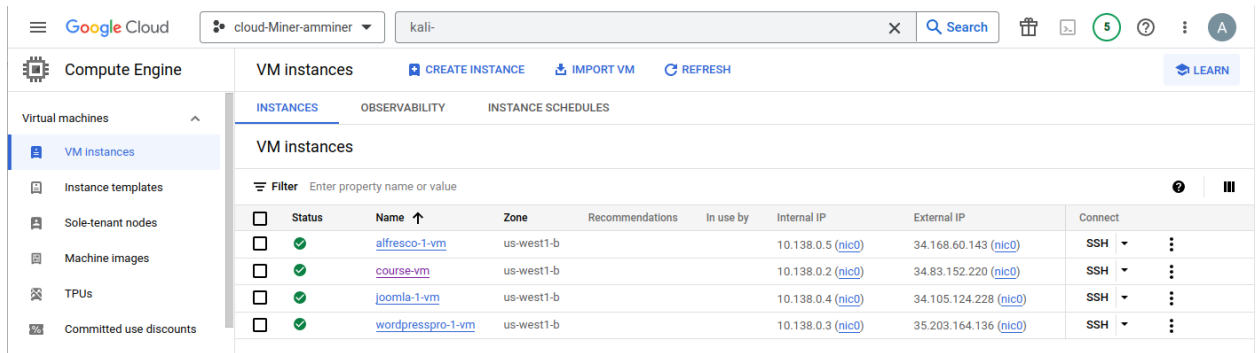
II. Lab 1.3 - Cloud Networking

1. Network Scanning (nmap) #1

- Done.

2. Launch targets

- Done:
(screenshot on next page)

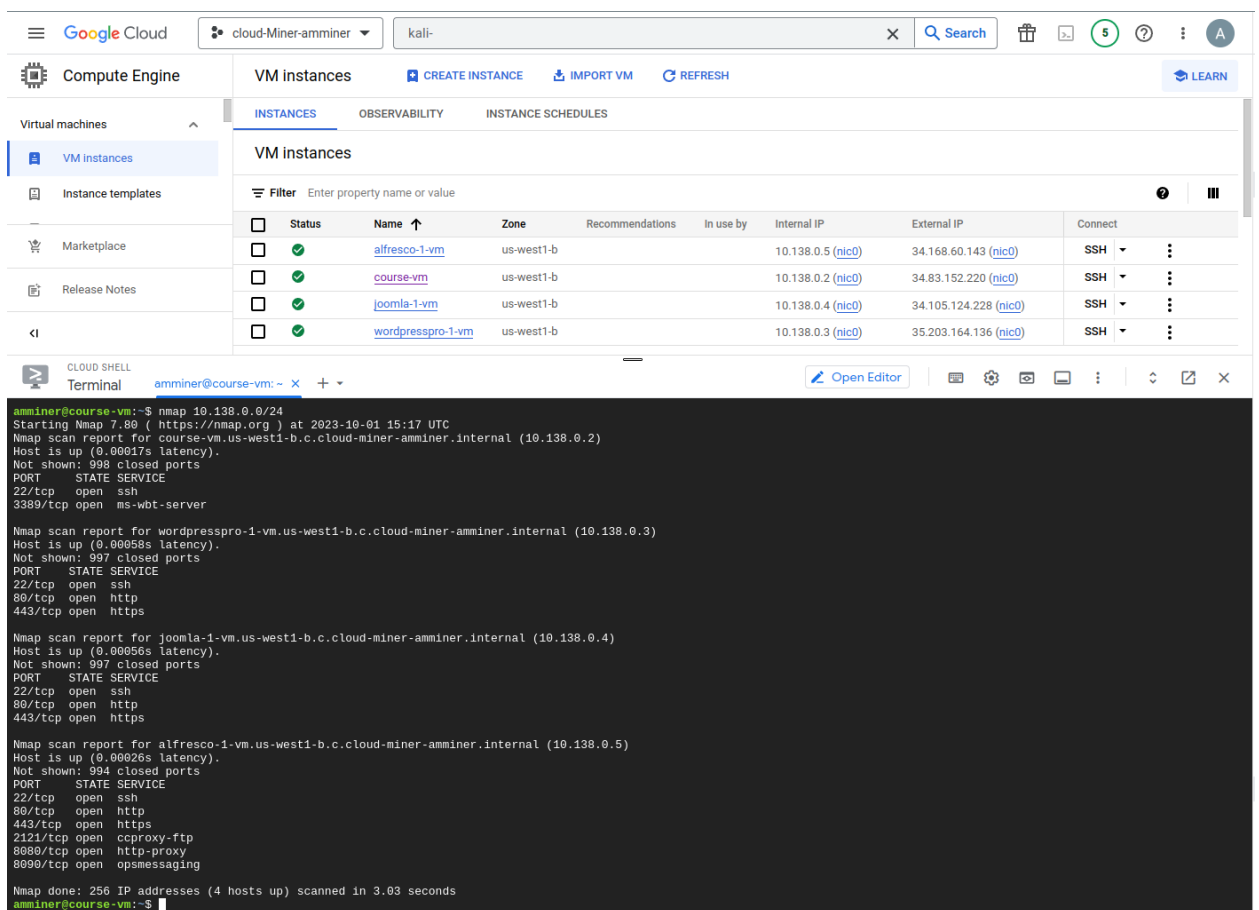


The screenshot shows the Google Cloud console interface for VM instances. The left sidebar lists navigation options: Virtual machines, VM instances (selected), Instance templates, Sole-tenant nodes, Machine images, TPUs, and Committed use discounts. The main panel displays a table of VM instances with columns for Status, Name, Zone, Recommendations, In use by, Internal IP, External IP, and Connect. Four instances are listed: alfresco-1-vm, course-vm, joomla-1-vm, and wordpresspro-1-vm, all in the us-west1-b zone.

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
✓	alfresco-1-vm	us-west1-b			10.138.0.5 (nic0)	34.168.60.143 (nic0)	SSH
✓	course-vm	us-west1-b			10.138.0.2 (nic0)	34.83.152.220 (nic0)	SSH
✓	joomla-1-vm	us-west1-b			10.138.0.4 (nic0)	34.105.124.228 (nic0)	SSH
✓	wordpresspro-1-vm	us-west1-b			10.138.0.3 (nic0)	35.203.164.136 (nic0)	SSH

3. Scan targets for services

- Done:



The screenshot shows the Google Cloud console interface for VM instances, identical to the previous one. Below the table, a terminal window is open, displaying the output of an Nmap scan performed on the four VM instances. The scan results show open ports and services for each host.

```
amminer@course-vm:~$ nmap 10.138.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-01 15:17 UTC
Nmap scan report for course-vm.us-west1-b.c.cloud-miner-amminer.internal (10.138.0.2)
Host is up (0.00017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server

Nmap scan report for wordpresspro-1-vm.us-west1-b.c.cloud-miner-amminer.internal (10.138.0.3)
Host is up (0.00058s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap scan report for joomla-1-vm.us-west1-b.c.cloud-miner-amminer.internal (10.138.0.4)
Host is up (0.00056s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap scan report for alfresco-1-vm.us-west1-b.c.cloud-miner-amminer.internal (10.138.0.5)
Host is up (0.00026s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
2121/tcp  open  ccproxy-ftp
8080/tcp  open  http-proxy
8090/tcp  open  opsmessaging

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.03 seconds
amminer@course-vm:~$
```

4. CIDR and Subnets #2

- Done.

5. Navigating Default Networks

- `gcloud compute networks subnets list | grep "NETWORK: default" | wc -l` tells me there are 40 subnets in the default network.
- `gcloud compute networks subnets list | grep "REGION:" | uniq | wc -l` tells me there are 40 unique regions to which these subnets correspond.
- Every subnet has a CIDR network mask of `/20`, so 20 bits are reserved for the network and 12 remain for hosts. $2^{12} = 4096$. so each subnet has enough address space for 4096 host devices.
- Instances created:

```
amminer@cloudshell:~ (cloud-miner-amminer)$ gcloud compute instances list
NAME: course-vm
ZONE: us-west1-b
MACHINE_TYPE: e2-medium
PREEMPTIBLE:
INTERNAL_IP: 10.138.0.2
EXTERNAL_IP: 34.83.152.220
STATUS: RUNNING

NAME: instance-1
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 34.138.188.25
STATUS: RUNNING

NAME: instance-2
ZONE: us-west3-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.180.0.2
EXTERNAL_IP: 34.106.78.24
STATUS: RUNNING
amminer@cloudshell:~ (cloud-miner-amminer)$
```

- us-east1 has RANGE: `10.142.0.0/20` and us-west3 has RANGE: `10.180.0.0/20`, so the instances are brought up in subnetworks corresponding to their region based on prior commands.
- Pinged instance-2 from instance-1 (screenshot on next page):

```
amminer@cloudshell:~ (cloud-miner-amminer)$ gcloud compute ssh instance-1
Did you mean zone [us-west1-a] for instance: [instance-1] (Y/n)? n

No zone specified. Using zone [us-east1-b] for instance: [instance-1].
Linux instance-1 5.10.0-25-cloud-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct  2 15:14:14 2023 from 35.227.157.249
amminer@instance-1:~$ ping 10.180.0.2
PING 10.180.0.2 (10.180.0.2) 56(84) bytes of data.
64 bytes from 10.180.0.2: icmp_seq=1 ttl=64 time=55.0 ms
64 bytes from 10.180.0.2: icmp_seq=2 ttl=64 time=53.2 ms
64 bytes from 10.180.0.2: icmp_seq=3 ttl=64 time=53.2 ms
^C
--- 10.180.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 53.235/53.822/54.987/0.823 ms
amminer@instance-1:~$
```

- This connection is facilitated by the virtual switch.

6. Creating Custom Networks

- custom-network1 created & listed:

```
amminer@cloudshell:~ (cloud-miner-amminer)$ gcloud compute networks list
NAME: custom-network1
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:

NAME: default
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
amminer@cloudshell:~ (cloud-miner-amminer)$
```

- 192.x.x.x subnets created & listed:

```

amminer@cloudshell:~ (cloud-miner-amminer)$ gcloud compute networks subnets list | grep -e 'us-central1$' -e 'europe-west1$' -C 5
NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

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: 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:
amminer@cloudshell:~ (cloud-miner-amminer)$

```

- Instances created; instance-3 has internal IP 192.168.1.2, instance-4 has 192.168.5.2.
- Pinged the internal addresses of instances 3 and 4 from instance-1; the packets do not reach their destination because these instances are not on the same internal network as instance-1, whereas instance-1 and instance-2 are on different subnets within the same broader network, connected by a virtual switch.
- All 4 instances in the UI with their networks and my ODIN ID:

<input type="checkbox"/>	Status	Name ↓	Zone	Recommendations	Internal IP	External IP	Network
<input type="checkbox"/>	✓	instance-4	europe-west1-d		192.168.5.2 (nic0)	35.233.27.33 (nic0)	custom-network1
<input type="checkbox"/>	✓	instance-3	us-central1-a		192.168.1.2 (nic0)	34.41.183.224 (nic0)	custom-network1
<input type="checkbox"/>	✓	instance-2	us-west3-b		10.180.0.2 (nic0)	34.106.78.24 (nic0)	default
<input type="checkbox"/>	✓	instance-1	us-east1-b		10.142.0.2 (nic0)	34.138.188.25 (nic0)	default

- custom-network1 subnets:

Subnets + ADD SUBNET ≡ FLOW LOGS ▼							
≡ Filter	Enter property name or value						
<input type="checkbox"/>	Name ↑	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway
<input type="checkbox"/>	subnet-europe-west-192	europe-west1	IPv4	192.168.5.0/24	None	None	192.168.5.1
<input type="checkbox"/>	subnet-us-central-192	us-central1	IPv4	192.168.1.0/24	None	None	192.168.1.1

- default network subnets:

← VPC network details EDIT DELETE VPC NETWORK

Subnets ADD SUBNET FLOW LOGS

Filter Enter property name or value

<input type="checkbox"/>	Name	Region ↑	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow logs	
<input type="checkbox"/>	default	asia-east1	IPv4	10.140.0.0/20	None	None	10.140.0.1	Off	Off	
<input type="checkbox"/>	default	asia-east2	IPv4	10.170.0.0/20	None	None	10.170.0.1	Off	Off	
<input type="checkbox"/>	default	asia-northeast1	IPv4	10.146.0.0/20	None	None	10.146.0.1	Off	Off	
<input type="checkbox"/>	default	asia-northeast2	IPv4	10.174.0.0/20	None	None	10.174.0.1	Off	Off	
<input type="checkbox"/>	default	asia-northeast3	IPv4	10.178.0.0/20	None	None	10.178.0.1	Off	Off	
<input type="checkbox"/>	default	asia-south1	IPv4	10.160.0.0/20	None	None	10.160.0.1	Off	Off	
<input type="checkbox"/>	default	asia-south2	IPv4	10.190.0.0/20	None	None	10.190.0.1	Off	Off	
<input type="checkbox"/>	default	asia-southeast1	IPv4	10.148.0.0/20	None	None	10.148.0.1	Off	Off	
<input type="checkbox"/>	default	asia-southeast2	IPv4	10.184.0.0/20	None	None	10.184.0.1	Off	Off	
<input type="checkbox"/>	default	australia-southeast1	IPv4	10.152.0.0/20	None	None	10.152.0.1	Off	Off	
<input type="checkbox"/>	default	australia-southeast2	IPv4	10.192.0.0/20	None	None	10.192.0.1	Off	Off	
<input type="checkbox"/>	default	europa-central2	IPv4	10.186.0.0/20	None	None	10.186.0.1	Off	Off	
<input type="checkbox"/>	default	europa-north1	IPv4	10.166.0.0/20	None	None	10.166.0.1	Off	Off	
<input type="checkbox"/>	default	europa-southwest1	IPv4	10.204.0.0/20	None	None	10.204.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west1	IPv4	10.132.0.0/20	None	None	10.132.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west10	IPv4	10.214.0.0/20	None	None	10.214.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west12	IPv4	10.210.0.0/20	None	None	10.210.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west2	IPv4	10.154.0.0/20	None	None	10.154.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west3	IPv4	10.156.0.0/20	None	None	10.156.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west4	IPv4	10.164.0.0/20	None	None	10.164.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west6	IPv4	10.172.0.0/20	None	None	10.172.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west8	IPv4	10.198.0.0/20	None	None	10.198.0.1	Off	Off	
<input type="checkbox"/>	default	europa-west9	IPv4	10.200.0.0/20	None	None	10.200.0.1	Off	Off	
<input type="checkbox"/>	default	me-central1	IPv4	10.212.0.0/20	None	None	10.212.0.1	Off	Off	
<input type="checkbox"/>	default	me-central2	IPv4	10.216.0.0/20	None	None	10.216.0.1	Off	Off	
<input type="checkbox"/>	default	me-west1	IPv4	10.208.0.0/20	None	None	10.208.0.1	Off	Off	
<input type="checkbox"/>	default	northamerica-northeast1	IPv4	10.162.0.0/20	None	None	10.162.0.1	Off	Off	
<input type="checkbox"/>	default	northamerica-northeast2	IPv4	10.188.0.0/20	None	None	10.188.0.1	Off	Off	
<input type="checkbox"/>	default	southamerica-east1	IPv4	10.158.0.0/20	None	None	10.158.0.1	Off	Off	
<input type="checkbox"/>	default	southamerica-west1	IPv4	10.194.0.0/20	None	None	10.194.0.1	Off	Off	
<input type="checkbox"/>	default	us-central1	IPv4	10.128.0.0/20	None	None	10.128.0.1	Off	Off	
<input type="checkbox"/>	default	us-east1	IPv4	10.142.0.0/20	None	None	10.142.0.1	Off	Off	
<input type="checkbox"/>	default	us-east4	IPv4	10.150.0.0/20	None	None	10.150.0.1	Off	Off	
<input type="checkbox"/>	default	us-east5	IPv4	10.202.0.0/20	None	None	10.202.0.1	Off	Off	
<input type="checkbox"/>	default	us-east7	IPv4	10.196.0.0/20	None	None	10.196.0.1	Off	Off	
<input type="checkbox"/>	default	us-south1	IPv4	10.206.0.0/20	None	None	10.206.0.1	Off	Off	
<input type="checkbox"/>	default	us-west1	IPv4	10.138.0.0/20	None	None	10.138.0.1	Off	Off	
<input type="checkbox"/>	default	us-west2	IPv4	10.168.0.0/20	None	None	10.168.0.1	Off	Off	
<input type="checkbox"/>	default	us-west3	IPv4	10.180.0.0/20	None	None	10.180.0.1	Off	Off	
<input type="checkbox"/>	default	us-west4	IPv4	10.182.0.0/20	None	None	10.182.0.1	Off	Off	

Rows per page: 50 1 - 40 of 40

d-miner-amminer x +

Open Edit

7. Clean Up

- Done!