Week1

Lab1

Armant Touche

Class/Instructor: CS430P/ Dr. Wu-Chang
Date: 9/30/22

Table of Contents

Homework #1 (Link)

1. Linux VM setup
    - [ ] Download Ubuntu 20.04 VM
        i. Link: https://releases.ubuntu.com/20.04/
    - [ ] VirtualBox (VB)
        i. Install
            1. Link: https://www.virtualbox.org/wiki/Downloads
2. Slack Account
    - [ ] Join
3. GitLab Account
    - [ ] Signup
    - [ ] Add `id_rsa.pub` key in Preferences -> SSH Keys
4. GitLab repo
    - [ ] Create Project
    - [ ] Invite Instructor and TA
    - [ ] Setup local git in VB, clone, and add README
5. Git
    - [ ] Init notebook
6. Docker Hub account
    - [ ] Add `dockerhub.txt` after signing up with @pdx.edu email
7. Google Cloud Platform account
    - [ ] Get Coupon
    - [ ] Create Project
8. AWS Academy
    - [ ] Wait for Canvas invite (NOTE: did not receive yet)
9. AWS via Vora
10. AWS CLI
    - [ ] Using Option **(1)**

ARP, Wireshark, Netsim (Link)

1. ARP #1
    - [ ] Install Wireshark
    - [ ] Perform tasks
        i. Use `ip` cmd to find virtual `lo` interface address

```
atouche@atouche:~$ ip -br addr show
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             10.0.2.15/24 fe80::a4f3:d7aa:92d9:2e89/64
docker0          DOWN           172.17.0.1/16
```

1. enp0s3: 10.0.2.15

ii. Perform `netstat -rn` d to find default router's IP address

```
atouche@atouche:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 enp0s3
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
```

1. gateway: 10.0.2.2

iii. `ping` default and use `arp` to find it's hardware address (`MAC`)

```
atouche@atouche:~$ ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.133 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.241 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1050ms
rtt min/avg/max/mdev = 0.133/0.187/0.241/0.054 ms
atouche@atouche:~$ arp -a 10.0.2.2
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
atouche@atouche:~$
```

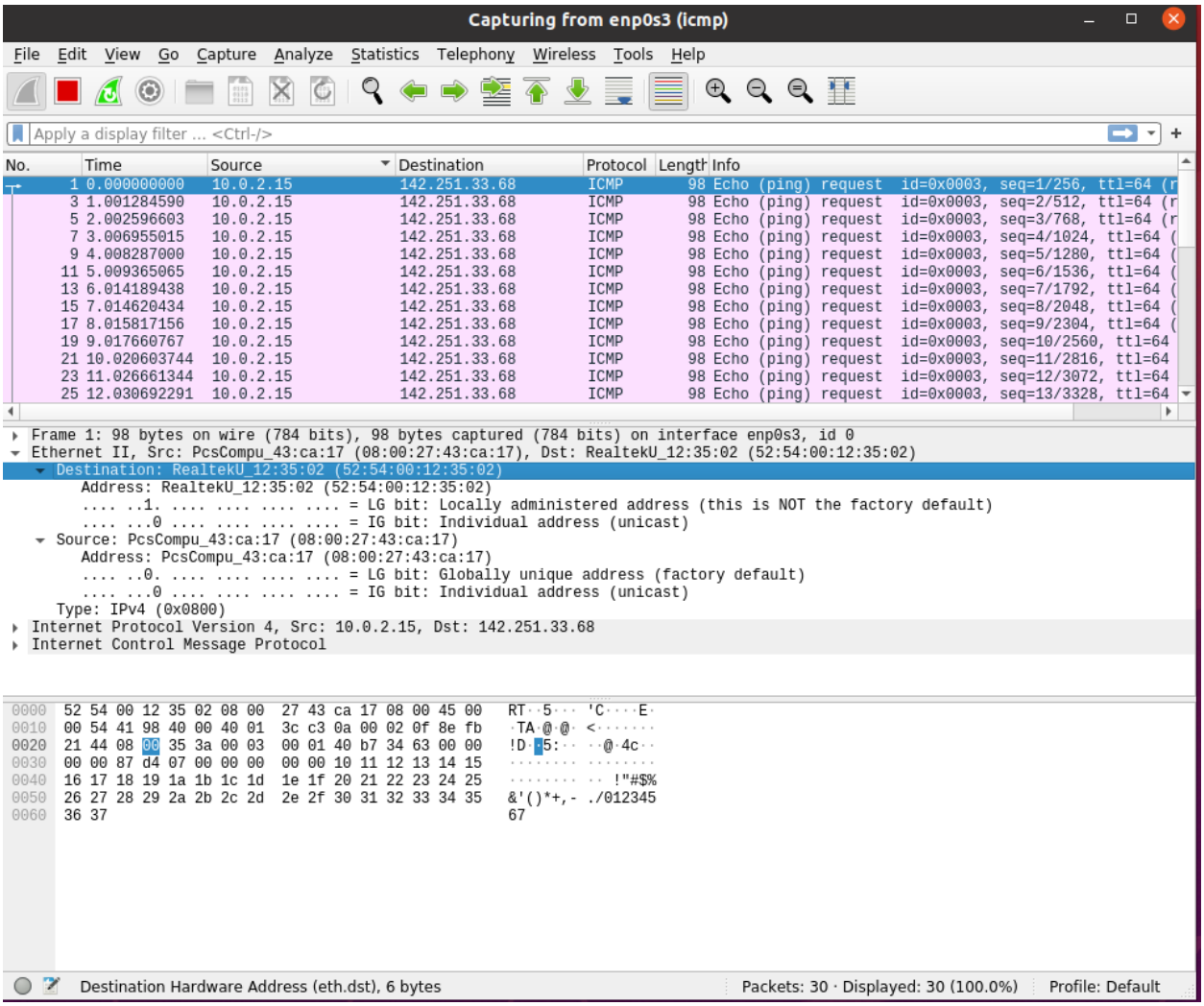
1. MAC: 52:54:00:12:35:02

iv. Wireshark

1. Add `icmp` and ping `www.google.com`
2. Answer following questions for `request`:
    a. **Which hardware manufacturer does the destination hardware address of the packet indicate?**

In the data-link layer (L2) packet or frame, the MAC address for destination is 52:54:00:12:35:02 which is the MAC address of the default gateway (10.0.0.2). L2 frame indicates source device is the VM and destination is the router/default gateway.

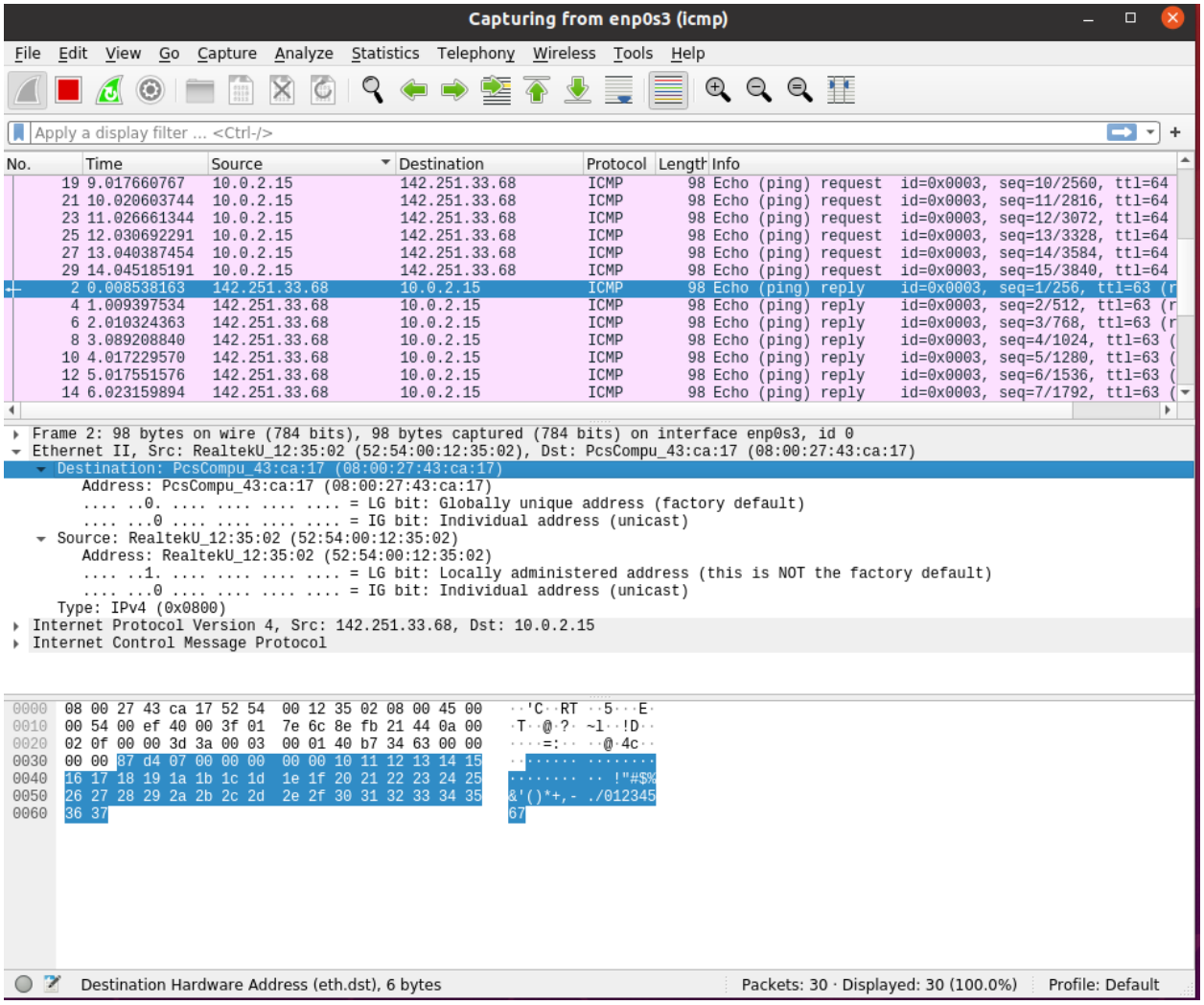
    b. **Take a screenshot of the bytes in the packet dump window as shown below**



3. Answer following questions for `reply`:
    a. **Which hardware manufacturer does the destination hardware address of the packet indicate?**

        In the data-link layer (L2) packet or frame, the MAC address for destination is 08:00:27:43:ca:17 which is the MAC address of Google's servers (142.251.33.68). L2 frame indicates source device is the default gateway and destination is Google's server.

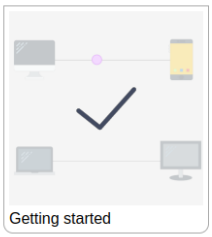
    b. **Take a screenshot of the bytes in the packet dump window as shown below**

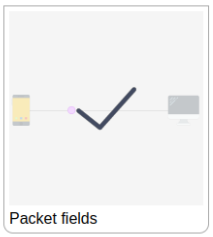


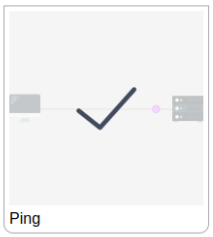
2. Netsim #2

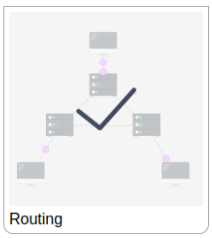
- [ ] Complete all levels

Basics


Getting started

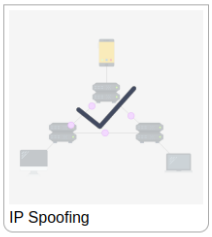

Packet fields


Ping


Routing

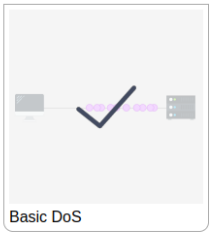

Modems

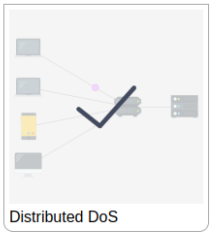
Spoofs

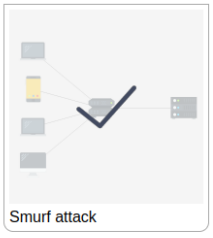

IP Spoofing


Stealing packets

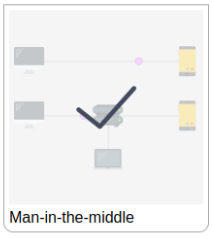
Denial of Service

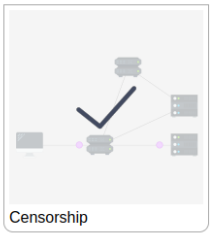

Basic DoS


Distributed DoS


Smurf attack

Attacks


Man-in-the-middle


Censorship


Traceroute

Cloud Networking

1. Network scanning (`nmap`) #1
    - ☐ Create VM
    - ☐ Install nmap
2. Launch targets
3. Scan targets for services

```
atouche@atouche:~$ nmap 10.138.0.2/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-30 03:45 UTC
Nmap scan report for atouche.c.cloud-touche-atouche.internal (10.138.0.2)
Host is up (0.00020s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for target-1-vm.c.cloud-touche-atouche.internal (10.138.0.3)
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 target-2-vm.c.cloud-touche-atouche.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 target-3-vm.c.cloud-touche-atouche.internal (10.138.0.5)
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: 256 IP addresses (4 hosts up) scanned in 3.08 seconds
```

4. CIDR and subnets #2

5. Navigating default network
   - ☐ Answer following questions:
     i. **How many subnetworks are created initially on the `default` network? How many regions does this correspond to? (Use a pipe to pass output to `grep` in order to return specific lines of output and then another to pass output to `wc` to count them: `| grep default | wc -l`)**

        72 subnetworks are created initially with default.

     ii. **Given the CIDR prefix associated with each subnetwork, how many hosts does each subnetwork support?**

        $2^{(32-20)}$-2 = 4094 host(s) / subnetwork

     iii. **Which CIDR subnetworks are these instances brought up in? Do they correspond to the appropriate region based on the prior commands?**

        In 10.150.0.0/instance-1 and 10.182.0.0/instance-2. Yes

```
atouche@instance-1:~$ ping 10.182.0.2
PING 10.182.0.2 (10.182.0.2) 56(84) bytes of data.
```

     iv. **From the figure in the previous step. What facilitates this connectivity: the virtual switch or the VPN Gateway?**

        Virtual switch

6. Creating custom networks
    - [ ] custom-network1

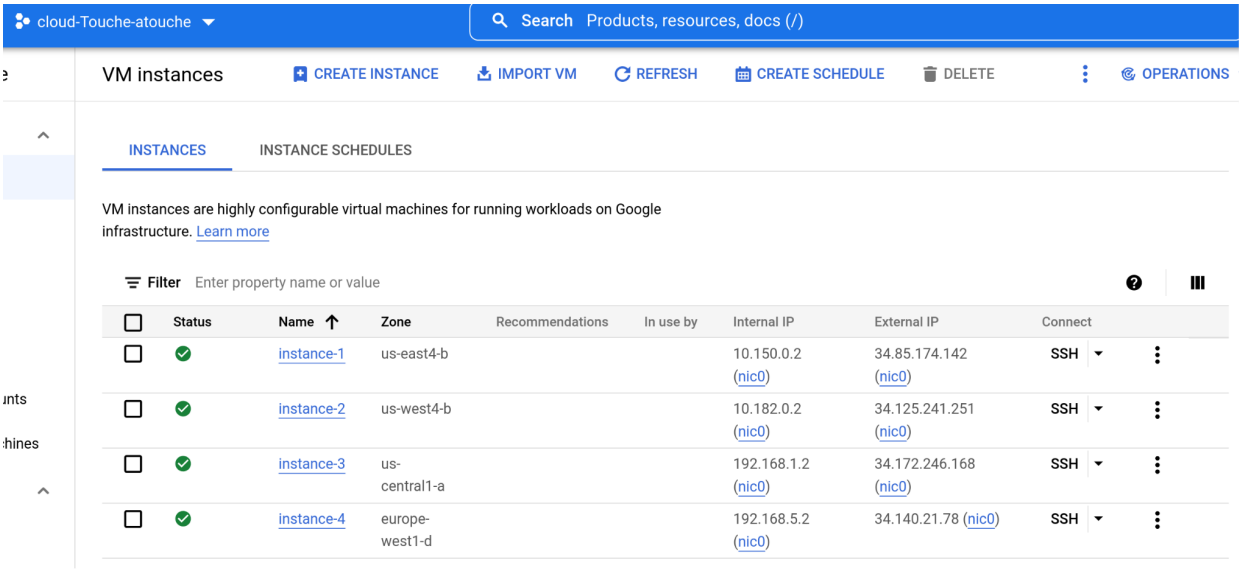
```
NAME: subnet-us-central-192
REGION: us-central1
NETWORK: custom-network1
RANGE: 192.168.1.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:

NAME: 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:
```

    - [ ] Ping instance-3&4 from instance-1
        i. Cannot ping outside of region since they are not on the same subnet and do not share the same virtual network switch like instance1&2 does.

- [ ] Take screenshot of all instances



- [ ] Then visit VPC Network

Name	Region	Subnets	MTU	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Firewall Rules	Global dynamic routing	Flow
custom-network1		2	1460	Custom	None				0	Off	
	us-central1	subnet-us-central-192			192.168.1.0/24	None	None	192.168.1.1			Off
	europe-west1	subnet-europe-west-192			192.168.5.0/24	None	None	192.168.5.1			Off
default		36	1460	Auto	None				4	Off	
	us-central1	default			10.128.0.0/20	None	None	10.128.0.1			Off
	europe-west1	default			10.132.0.0/20	None	None	10.132.0.1			Off
	us-west1	default			10.138.0.0/20	None	None	10.138.0.1			Off
	asia-east1	default			10.140.0.0/20	None	None	10.140.0.1			Off

7. Clean up