Francisco Laureano
CIS245

Ubuntu Networking

1. Document network setup. Your setup should include how to find all the networking information, as well as the basics on how your server does networking by default. This should include locations of any files you've created or need to reference. You should include any programs you've installed or updated as well, with dates of when you've done those things. Include a short document including how you did any of the installs or updates.

1a.

Tools and Updates

- The server was last updated on 10/11/24 using sudo apt update and sudo apt upgrade

- Installed network tool openssh on 9/7/24

Openssh allows for ssh connections on the ubuntu server, in turn allowing me to connect with my preferred ssh tool putty.

- Installed network tool fail2ban on 10/10/24

Fail2ban is a critical tool that enhances the security of the server by banning malicious connections that attempt to brute force their way into the server over the network.

Commands and their function

Now, to quickly find a comprehensive list of networking information on the server setup you can use the following command:

- sudo netplan status

When inputted, you will see that your DNS information, interface connections and their mac addresses, ip addresses of interfaces, and the route information. This is a great way to generally see some of the most important network information about a server. Netplan as a whole is how ubuntu manages the configuration of its network.

Francisco Laureano
CIS245

```
flaureano@cis245-ubuntu:~$ sudo netplan  status
     Online state: online
    DNS Addresses: 127.0.0.53 (stub)
       DNS Search: localdomain

●  1: lo ethernet UNKNOWN/UP (unmanaged)
      MAC Address: 00:00:00:00:00:00
        Addresses: 127.0.0.1/8
                   ::1/128

●  2: ens33 ethernet UP (networkd: ens33)
      MAC Address: 00:0c:29:8b:29:cd (Intel Corporation)
        Addresses: 192.168.186.130/24 (dhcp)
                   fe80::20c:29ff:fe8b:29cd/64 (link)
    DNS Addresses: 192.168.186.2
       DNS Search: localdomain
           Routes: default via 192.168.186.2 from 192.168.186.130 metric 100 (dhcp)
                   192.168.186.0/24 from 192.168.186.130 metric 100 (link)
                   192.168.186.2 from 192.168.186.130 metric 100 (dhcp, link)
                   fe80::/64 metric 256
```

Additionally, you can dive deeper into the network configuration by running a few other commands:

- ip a

Ip will show more in depth information about the network interfaces that are connected to the server.

```
flaureano@cis245-ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:8b:29:cd brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.186.130/24 metric 100 brd 192.168.186.255 scope global dynamic ens33
       valid_lft 1645sec preferred_lft 1645sec
    inet6 fe80::20c:29ff:fe8b:29cd/64 scope link
       valid_lft forever preferred_lft forever
```

- route -n

route -n will show a routing table of your network without resolving the addreses. If you want to see a routing table with resolved addresses, you can simply type route

```
flaureano@cis245-ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.186.2   0.0.0.0         UG    100    0        0 ens33
192.168.186.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
192.168.186.2   0.0.0.0         255.255.255.255 UH    100    0        0 ens33
flaureano@cis245-ubuntu:~$
```

- sudo ss

sudo ss will show socket information and the port they're listing on which can be useful for troubleshooting network issues. However this list can be extremely long so if you want to see a summary you can add the -s switch (ss -s)

Francisco Laureano
CIS245

```
flaureano@cis245-ubuntu:~$ sudo ss -s
Total: 178
TCP:   4 (estab 1, closed 0, orphaned 0, timewait 0)

Transport Total     IP        IPv6
RAW       1         0         1
UDP       3         3         0
TCP       4         2         2
INET      8         5         3
FRAG      0         0         0

flaureano@cis245-ubuntu:~$
```

- cat /etc/resolv.conf

This command will display the dns information of your server and if you would like to change it from the default, you can edit the resolv.conf file to add in your new dns server(s) but this is not recommended unless you are entire 100% sure of what youre doing.

```
flaureano@cis245-ubuntu:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search localdomain
flaureano@cis245-ubuntu:~$
```

Netplan and how it works with Ubuntu

As my server is based on Ubuntu, all the networking is handled through Netplan which houses the network configuration. Netplan can be found in /etc/netplan/ and in these settings, configuration for network interfaces or dns resolution is housed and any changes regarding those settings would need to take place in there. As the server is hosted on a VM, the network traffic gets routed from the VM onto my computer and from there it routes out to the internet. This setup is standard as I have not made any changes with dns or the routing table.