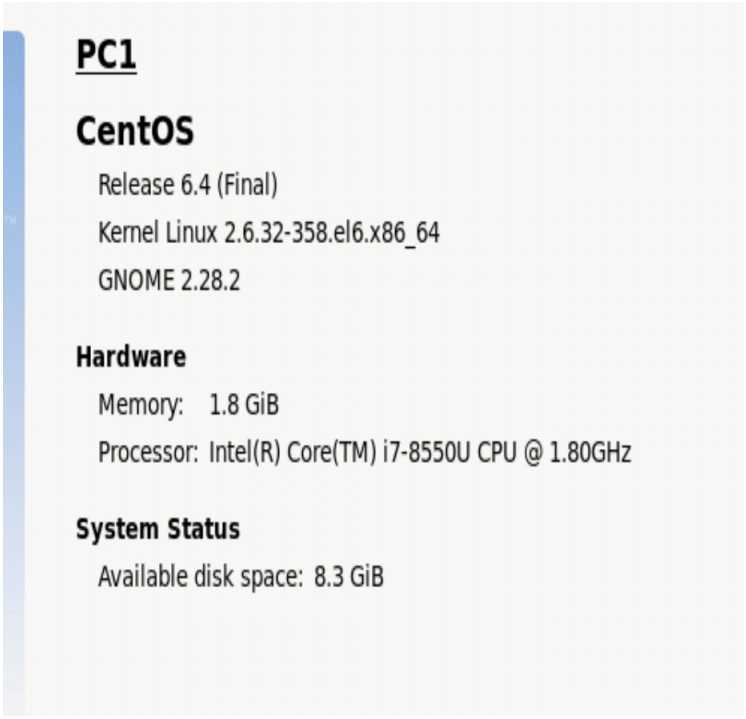
1) What OS version is being used for the CEO's computer?

A good way to examine the operating system in the linux terminal is to type:

lsb_release -a

```
[user@PC1 ~]$ lsb_release -a
LSB Version:    :base-4.0-amd64:base-4.0-noarch:core-4.0-amd64:core-4.0-noarch:g
raphics-4.0-amd64:graphics-4.0-noarch:printing-4.0-amd64:printing-4.0-noarch
Distributor ID: CentOS
Description:    CentOS release 6.4 (Final)
Release:        6.4
Codename:       Final
```

You can also see the operating system details in the menu under "System" \ "About This Computer" \ Which brings up the System Monitor Console:



2) Explain the purpose of the DMZ?

The purpose of the DMZ is to provide internet access to the webserver. This will enable customers to access the webpage designed to sell/inform/whatever else without putting the internal VLAN at risk

The DMZ is the only partially trusted VLAN that people on the internet with any IP address can talk to. Because anyone can talk to these nodes on the network. Customers, hackers and attackers can all access it. These nodes must be in a place where a firewall is in place to protect administrators.

Everything in the DMZ should be hardened because it can be exposed to attack. Bastion the nodes. Since any box in the DMZ can potentially be taken over by an attacker, no money, no privacy, no critical data.

3) How many different operating systems are being utilized in the project

scenario?

There are two: Linux and Windows operating systems.

4) Why would you conduct a scan from different points of the network?

To assess vulnerabilities within a subnet and prevent the necessity of analyzing packets through a firewall or router or switch that may have filters on. Generally if you're scanning a network from within the subnet you can see more information than from outside of the VLAN.

5) What ports are open on the firewall?

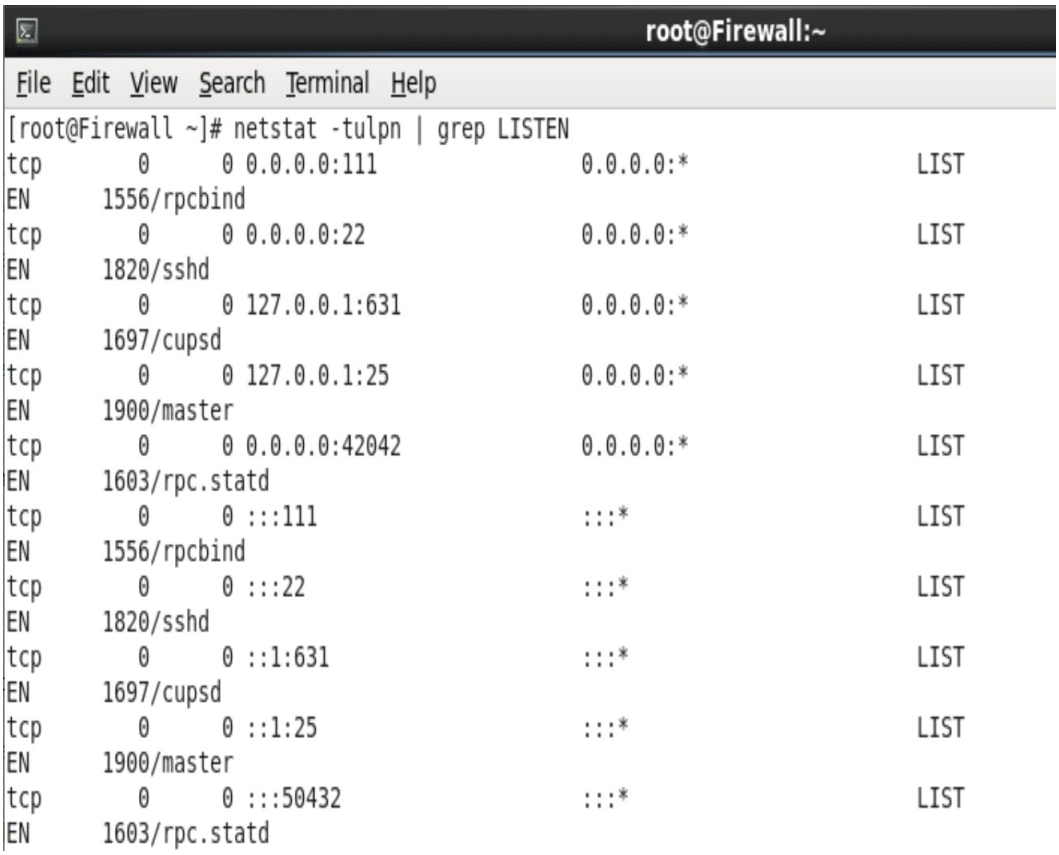
In order to see the ports that allow traffic through the firewall. The firewall application is

system-config-firewall

There are no special rules or other allowances. The only checkbox in the firewall config is SSH on port 22 which is a trusted service.

A good way to see what ports are open in linux is by using the following command in the terminal: sudo netstat -tulpn | grep LISTEN

When I input the command in the firewall the following is printed:



According to my understanding these are the ports that are in use or connections have been established.

6) What type of Linux system is being utilized for the CEO's computer?

Red-Hat Linux is the distribution used on the CEO's computer.

7) What users are on the Kali Linux device?

Root is the only user created on the Kali Linux device - the root user has superuser permissions

8) What users are located on the CEO's computer?

There are two - User and CEO, the password for CEO is unknown. While logged in as user we can create a group of commands to see permissions:

/etc/sudoers

ALL=/sbin/service, /sbin/chkconfig

This will produce a list of commands that "user" is allowed to run.

```
[user@PC1 ~]$ # /etc/sudoers
[user@PC1 ~]$ ALL=/sbin/service, /sbin/chkconfig
NetworkManager  0:off   1:off   2:on    3:on    4:on    5:on    6:off
abrt-ccpp       0:off   1:off   2:off   3:on    4:off   5:on    6:off
abrtd           0:off   1:off   2:off   3:on    4:off   5:on    6:off
acpid           0:off   1:off   2:on    3:on    4:on    5:on    6:off
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
autofs          0:off   1:off   2:off   3:on    4:on    5:on    6:off
blk-availability        0:off   1:on    2:on    3:on    4:on    5:on    6:off
bluetooth       0:off   1:off   2:off   3:on    4:on    5:on    6:off
certmonger      0:off   1:off   2:off   3:on    4:on    5:on    6:off
cpuspeed        0:off   1:on    2:on    3:on    4:on    5:on    6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
cups            0:off   1:off   2:on    3:on    4:on    5:on    6:off
dnsmasq         0:off   1:off   2:off   3:off   4:off   5:off   6:off
firstboot       0:off   1:off   2:off   3:off   4:off   5:off   6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
htcacheclean    0:off   1:off   2:off   3:off   4:off   5:off   6:off
httpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
ip6tables       0:off   1:off   2:on    3:on    4:on    5:on    6:off
ipsec           0:off   1:off   2:off   3:off   4:off   5:off   6:off
iptables        0:off   1:off   2:off   3:off   4:off   5:off   6:off
irqbalance      0:off   1:off   2:off   3:on    4:on    5:on    6:off
kdump           0:off   1:off   2:off   3:off   4:off   5:off   6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mdmonitor       0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:on    3:on    4:on    5:on    6:off
mip6d           0:off   1:off   2:off   3:off   4:off   5:off   6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
nfs             0:off   1:off   2:off   3:off   4:off   5:off   6:off
nfslock         0:off   1:off   2:off   3:on    4:on    5:on    6:off
ntpd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
ntpdate         0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

9) What users are located on Web Server?

There are two users on the Web Server. Root user with all permissions and Admin. When I use the same group of commands to list permissions, I receive an error that there is no such file or directory "chkconfig"

10) What type of web traffic does Wireshark capture when someone navigates

to the webserver from the CEO's computer?

After enabling promiscuous mode on the NICs within virtualbox I was able to see the traffic from all sides. Most of the traffic that went through was TCP (color coded green) with some HTTP as well (also green). There were several DNS queries going on at the same time but most of those failed as the network is not connected to the internet but self-contained within the host. Wireshark in both subnets (INTnet and DMZnet) showed the same traffic