Colby Heilner

Professor Torres
10/22

IT 120
Lab 9

Part A:

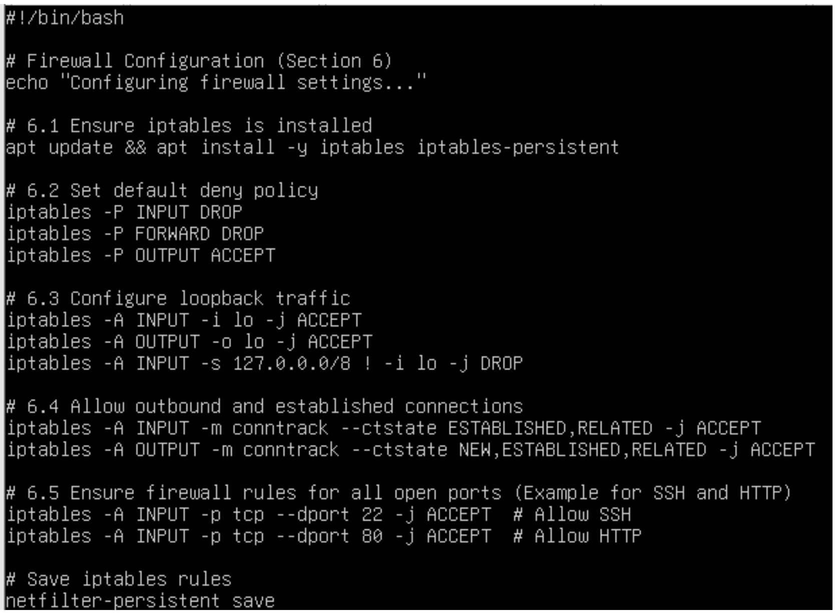
Capture a screenshot of the results of each major command. Log on to Netlab2

Links to an external site. (NISGTC Linux+ Series 2, Lab 01). Configure the below settings on the Ubuntu Workstation

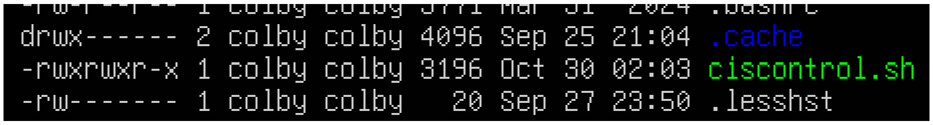
I went onto my vm for ubuntu and copied and pasted a script into it. (it was long)

Here is a snippet of the top and the file name and executability

Snippet of 6.x

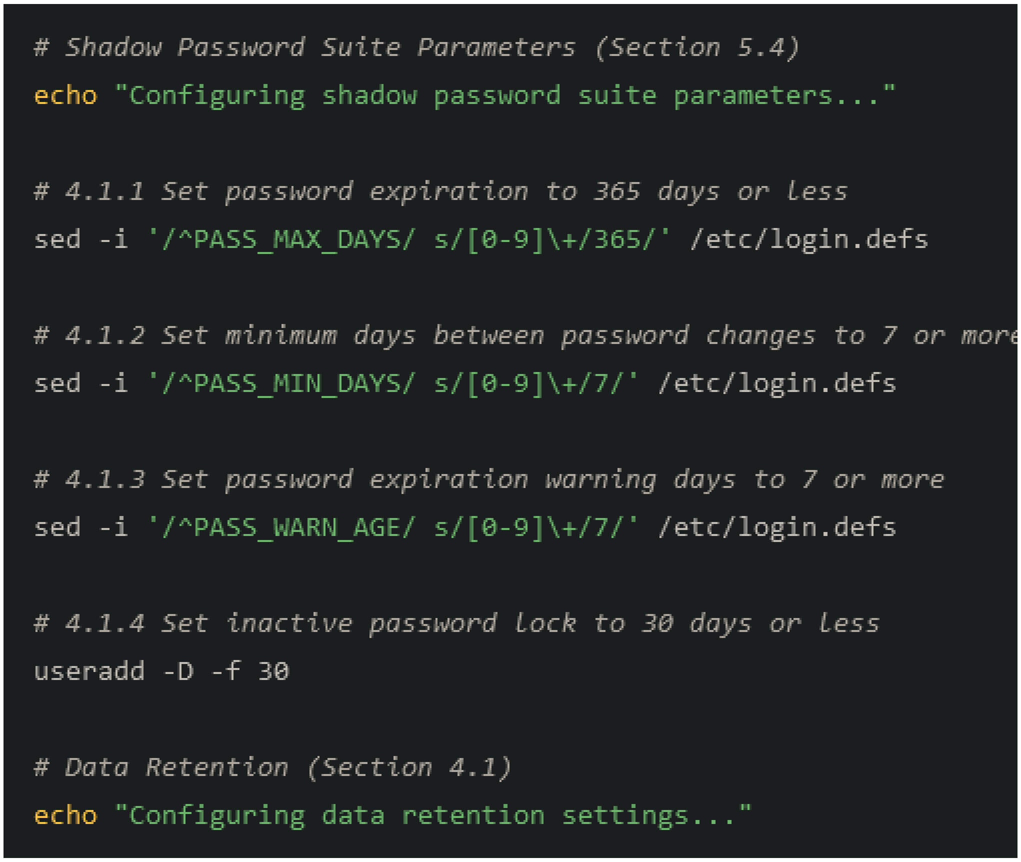


```
#!/bin/bash

# Firewall Configuration (Section 6)
echo "Configuring firewall settings..."

# 6.1 Ensure iptables is installed
apt update && apt install -y iptables iptables-persistent

# 6.2 Set default deny policy
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# 6.3 Configure loopback traffic
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 ! -i lo -j DROP

# 6.4 Allow outbound and established connections
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate NEW,ESTABLISHED,RELATED -j ACCEPT

# 6.5 Ensure firewall rules for all open ports (Example for SSH and HTTP)
iptables -A INPUT -p tcp --dport 22 -j ACCEPT  # Allow SSH
iptables -A INPUT -p tcp --dport 80 -j ACCEPT  # Allow HTTP

# Save iptables rules
netfilter-persistent save
```



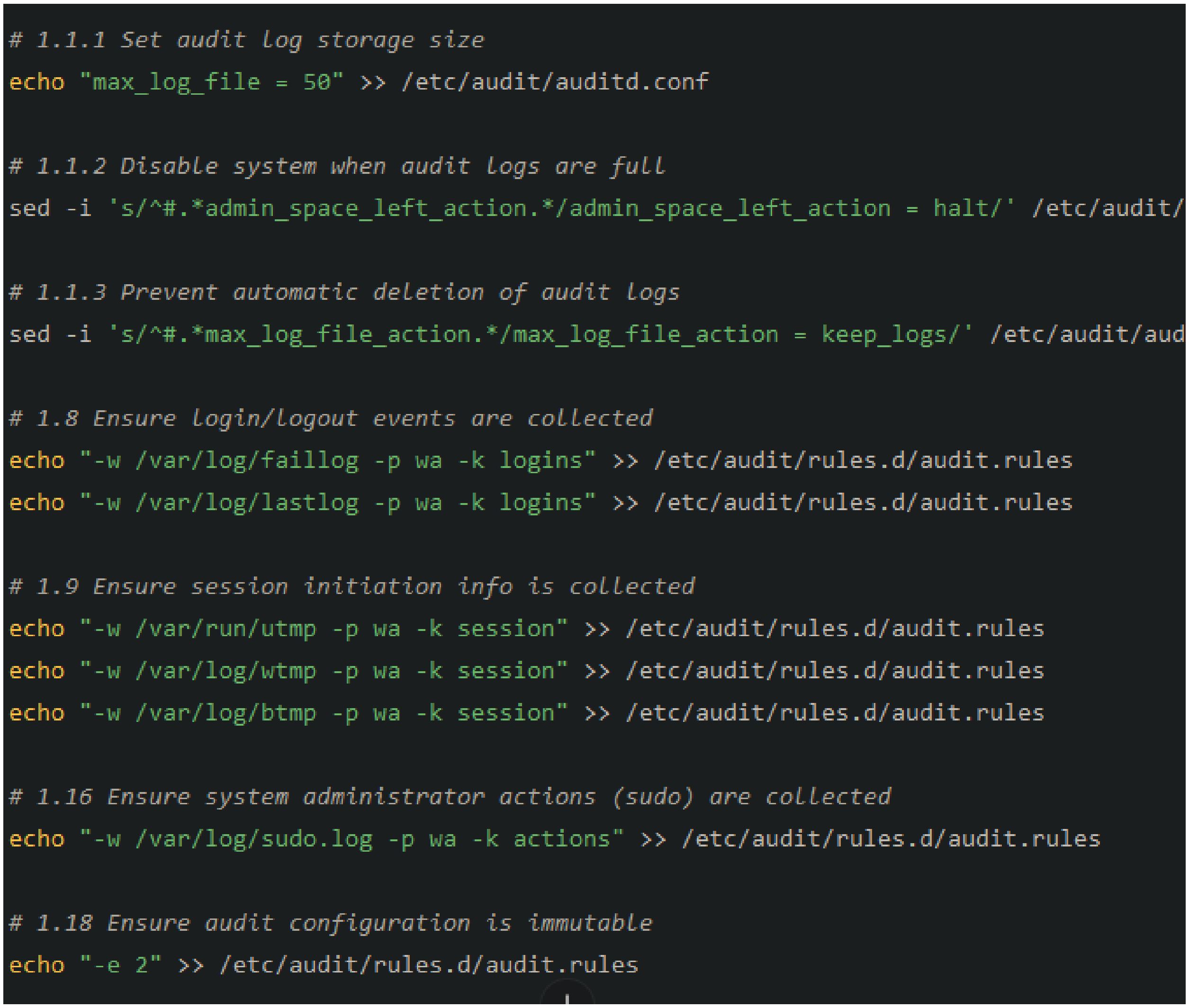
```
-rw-r--r-- 1 colby colby 3771 Mar 31  2024 .bashrc
drwx------ 2 colby colby 4096 Sep 25 21:04 .cache
-rwxrwxr-x 1 colby colby 3196 Oct 30 02:03 ciscontrol.sh
-rw------- 1 colby colby   20 Sep 27 23:50 .lesshst
```

Snippet of 4.x



```
# Shadow Password Suite Parameters (Section 5.4)
echo "Configuring shadow password suite parameters..."

# 4.1.1 Set password expiration to 365 days or less
sed -i '/^PASS_MAX_DAYS/ s/[0-9]\+/365/' /etc/login.defs

# 4.1.2 Set minimum days between password changes to 7 or more
sed -i '/^PASS_MIN_DAYS/ s/[0-9]\+/7/' /etc/login.defs

# 4.1.3 Set password expiration warning days to 7 or more
sed -i '/^PASS_WARN_AGE/ s/[0-9]\+/7/' /etc/login.defs

# 4.1.4 Set inactive password lock to 30 days or less
useradd -D -f 30

# Data Retention (Section 4.1)
echo "Configuring data retention settings..."
```

Snippet of 1.1.x

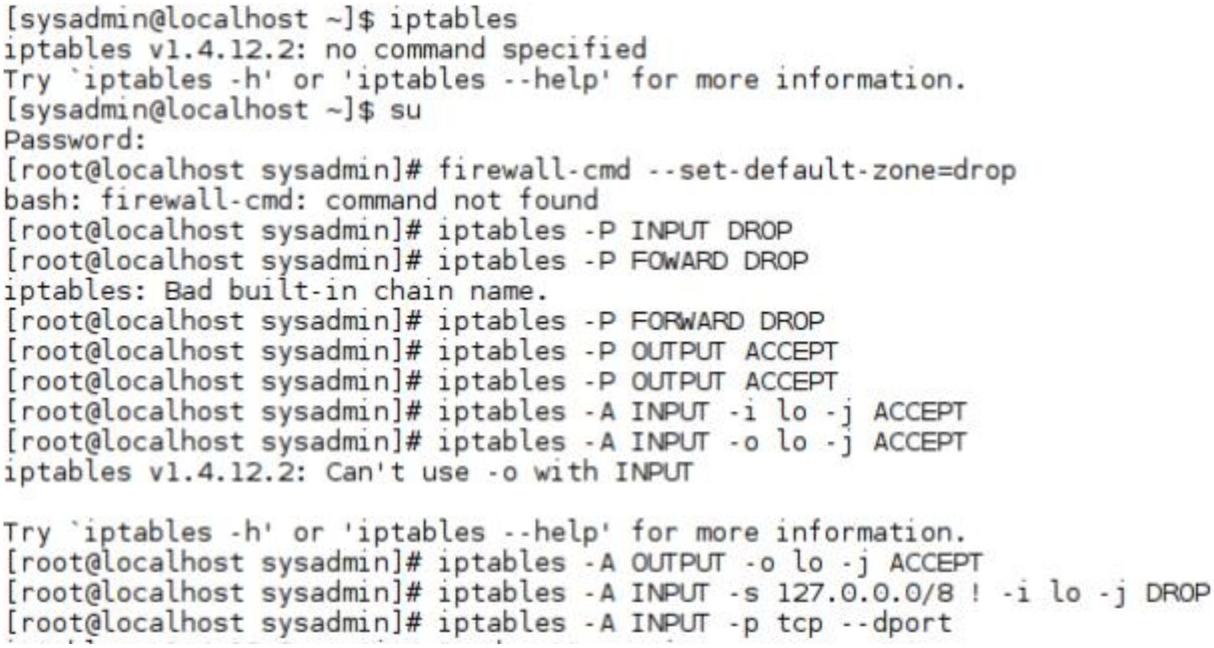


```
# 1.1.1 Set audit log storage size
echo "max_log_file = 50" >> /etc/audit/auditd.conf

# 1.1.2 Disable system when audit logs are full
sed -i 's/^#.*admin_space_left_action.*/admin_space_left_action = halt/' /etc/audit/

# 1.1.3 Prevent automatic deletion of audit logs
sed -i 's/^#.*max_log_file_action.*/max_log_file_action = keep_logs/' /etc/audit/aud

# 1.8 Ensure login/logout events are collected
echo "-w /var/log/faillog -p wa -k logins" >> /etc/audit/rules.d/audit.rules
echo "-w /var/log/lastlog -p wa -k logins" >> /etc/audit/rules.d/audit.rules

# 1.9 Ensure session initiation info is collected
echo "-w /var/run/utmp -p wa -k session" >> /etc/audit/rules.d/audit.rules
echo "-w /var/log/wtmp -p wa -k session" >> /etc/audit/rules.d/audit.rules
echo "-w /var/log/btmp -p wa -k session" >> /etc/audit/rules.d/audit.rules

# 1.16 Ensure system administrator actions (sudo) are collected
echo "-w /var/log/sudo.log -p wa -k actions" >> /etc/audit/rules.d/audit.rules

# 1.18 Ensure audit configuration is immutable
echo "-e 2" >> /etc/audit/rules.d/audit.rules
```

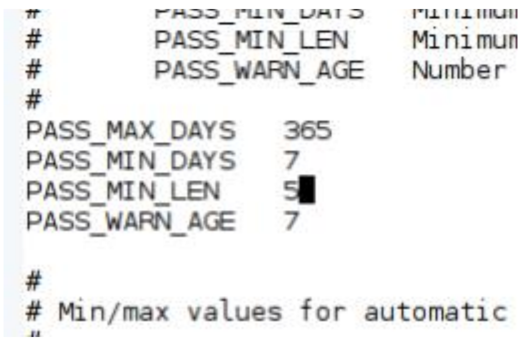
I ran this in my ubuntu but like always had connectivity errors due to the apt updates. With them removed it seems to work. I had to make sure to run it in root.

Part B:

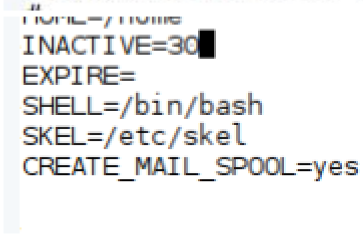
- Capture a screenshot of the results of each major command. Log on to Netlab2 (NISGTC Linux+ Series 2, Lab 01). Configure the below settings on the Fedora Workstation



```
[sysadmin@localhost ~]$ iptables
iptables v1.4.12.2: no command specified
Try `iptables -h' or 'iptables --help' for more information.
[sysadmin@localhost ~]$ su
Password:
[root@localhost sysadmin]# firewall-cmd --set-default-zone=drop
bash: firewall-cmd: command not found
[root@localhost sysadmin]# iptables -P INPUT DROP
[root@localhost sysadmin]# iptables -P FOWARD DROP
iptables: Bad built-in chain name.
[root@localhost sysadmin]# iptables -P FORWARD DROP
[root@localhost sysadmin]# iptables -P OUTPUT ACCEPT
[root@localhost sysadmin]# iptables -P OUTPUT ACCEPT
[root@localhost sysadmin]# iptables -A INPUT -i lo -j ACCEPT
[root@localhost sysadmin]# iptables -A INPUT -o lo -j ACCEPT
iptables v1.4.12.2: Can't use -o with INPUT

Try `iptables -h' or 'iptables --help' for more information.
[root@localhost sysadmin]# iptables -A OUTPUT -o lo -j ACCEPT
[root@localhost sysadmin]# iptables -A INPUT -s 127.0.0.0/8 ! -i lo -j DROP
[root@localhost sysadmin]# iptables -A INPUT -p tcp --dport
```

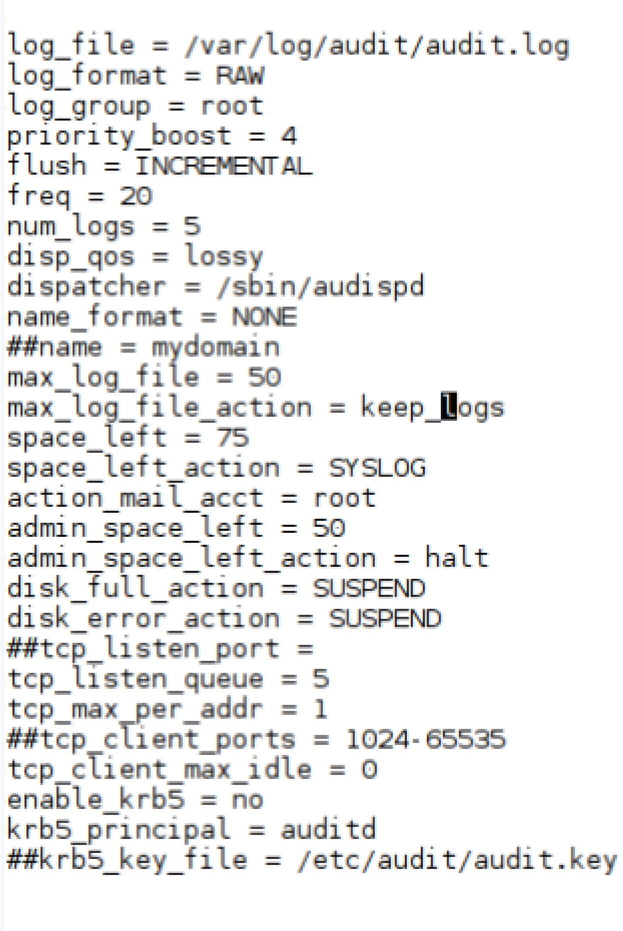


```
#       PASS_MIN_DAYS   Minimum
#       PASS_MIN_LEN    Minimum
#       PASS_WARN_AGE   Number
#
PASS_MAX_DAYS   365
PASS_MIN_DAYS   7
PASS_MIN_LEN    5
PASS_WARN_AGE   7

#
# Min/max values for automatic
```



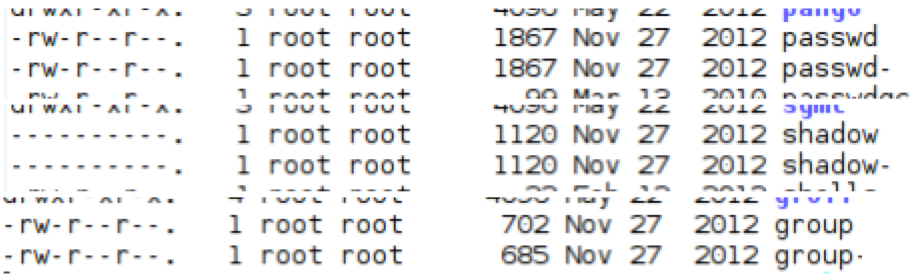
```
HOME=/home
INACTIVE=30
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Made all data retention changes



```
log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 50
max_log_file_action = keep_logs
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = halt
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
```

Ensuring permissions for sensitive file.



```
drwxr-xr-x.   3 root root     4096 May 22  2012 pango
-rw-r--r--.   1 root root     1867 Nov 27  2012 passwd
-rw-r--r--.   1 root root     1867 Nov 27  2012 passwd-
-rw-r--r--.   1 root root       99 Mar 12  2010 passwdqc
drwxr-xr-x.   3 root root     4096 May 22  2012 sgml
----------.   1 root root     1120 Nov 27  2012 shadow
----------.   1 root root     1120 Nov 27  2012 shadow-
drwxr-xr-x.   4 root root     4096 May 22  2012 groff
-rw-r--r--.   1 root root      702 Nov 27  2012 group
-rw-r--r--.   1 root root      685 Nov 27  2012 group-
```

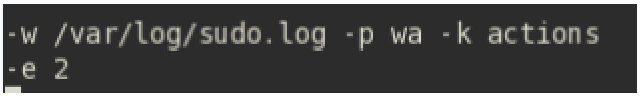
Part C:

- Capture a screenshot of the results of each major command. Log on to Netlab2 (NISGTC Linux+ Series 2, Lab 01). Configure the below settings on the CentOS Server

I will go through and do them on centos as well now. I will try to only post screen shots of commands that might be different from the rest.

Firstly, it uses **yum** as package manger.

I used these to collect login and logout events
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
And these
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
I can also collect sudo logs



```
-w /var/log/sudo.log -p wa -k actions
-e 2
```

All of these are added to /etc/audit/rules.d/audit.rules
These also seem the same between operating systems
sudo chmod 600 /etc/shadow
sudo chown root:shadow /etc/shadow
sudo chmod 644 /etc/passwd
sudo chown root:root /etc/passwd
sudo chmod 644 /etc/group
sudo chown root:root /etc/group

Centos also uses iptables, so commands carry over.

AS A BONUS CentOS 7 and newer comes with **firewalld**

Here is how you could make these changes with FWd instead of iptables

- 6.1 Ensure ~~*iptables*~~ is installed (Scored)
  sudo systemctl enable firewalld --now
- 6.2 Ensure default deny firewall policy (Scored)
  sudo firewall-cmd --set-default-zone=drop
- 6.3 Ensure loopback traffic is configured (Scored)
  sudo firewall-cmd --permanent --zone=trusted --add-interface=lo
- 6.4 Ensure outbound and established connections are configured (Not Scored)
  sudo firewall-cmd --permanent --add-masquerade
  sudo firewall-cmd --permanent --zone=drop --add-rich-rule='rule family="ipv4" source address=127.0.0.1/8 accept'

- 6.5 Ensure firewall rules exist for all open ports (Scored)
  I could find my ports and replace them in <ports>
  sudo firewall-cmd --permanent --add-port=<port>/<protocol>
  Then finally to Save
  sudo firewall-cmd --reload

Extra Credit 5 Points:

- Create and run a bash or python script to configure the above settings on one of the systems

See Ubuntu, first part of my lab.