# KEY

# Network Security, test 1

1. What is the command you use to display running processes?  
     
   ps aux  
     
   It usually contains a lot of output. What can you do to just show lines that contain a word you are interested in?

ps aux | grep thewordIwant

1. What is the difference between User Mode and Kernel Mode?

Kernel mode has complete access to the OS kernel and hardware. User mode has limited access.

1. How would you redirect output from some command (say, cat) to a file without overwriting it?

cat somefile >> otherfile appends

cat somefile > otherfile will overwrite otherfile

1. What is the PATH variable used for?

The OS looks in each directory listed in PATH when it is trying to find the command you entered

1. What would this command do: chmod 741 svgsfile

It would set the rights of the file, svgsfile, to rwxr----x. Not practical, but I needed a test question.

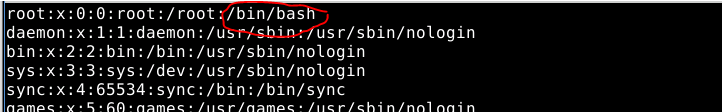
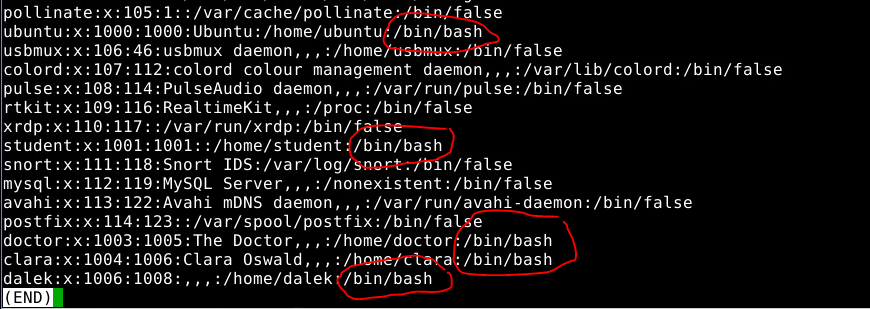
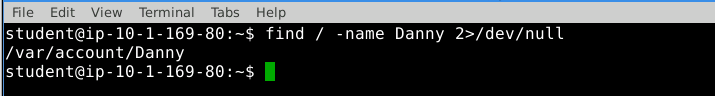
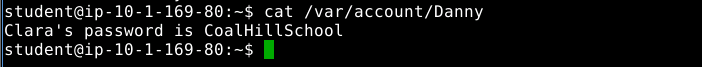
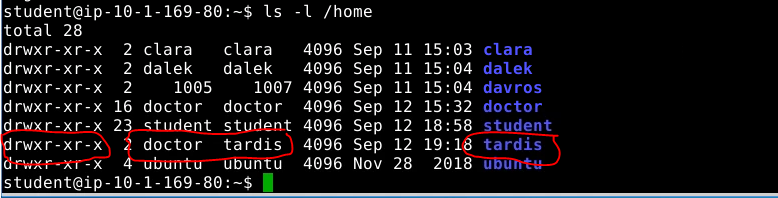
# Open Book, Open Internet

This VM quest is based on the Dr. Who television series. This scenario works for the 12th Doctor (Peter Capaldi). So that Whovians don’t get an advantage, here is the cast of characters. All you need to know is who is good and who is evil.

* Dr. Who, or the Doctor. The hero.
* Clara Oswald. The Doctor’s traveling companion and co-hero.
* Tardis. The Doctor’s time and space travel ship.
* Davros. Evil mad scientist who created the Dalek race of cyborgs.
* Dalek. Evil cyborgs.
* Skaros. Home planet of the Daleks.

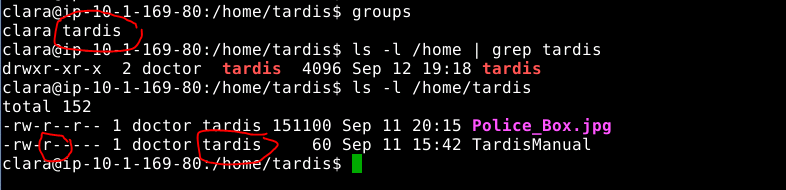
Passwords  
root Exterminate!  
doctor Gallifrey  
clara CoalHillSchool  
davros Exterminate!

The VM you need on the Virginia Cyber Range and is named “Linux Dr Who Adventure.” Log into the VM as student (user name is student and password is student )

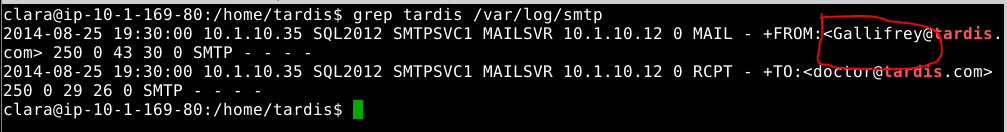
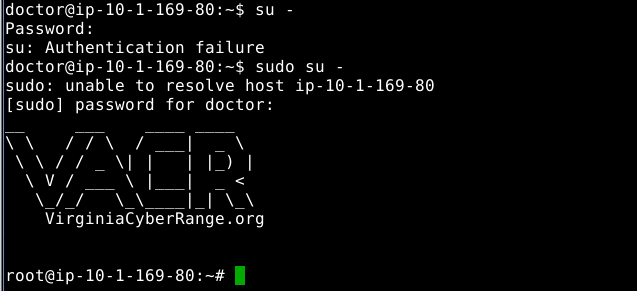
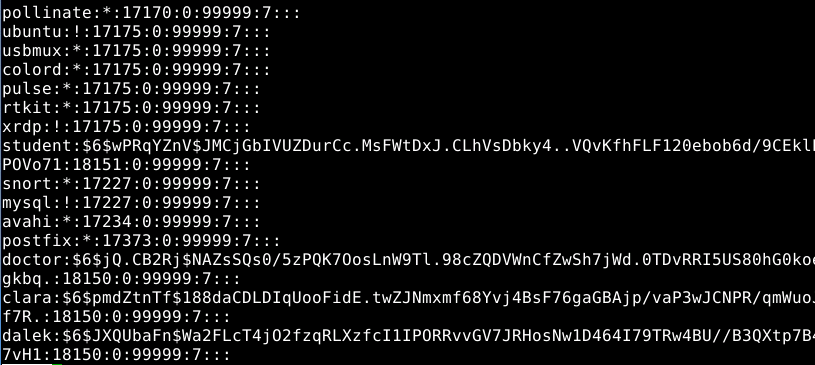
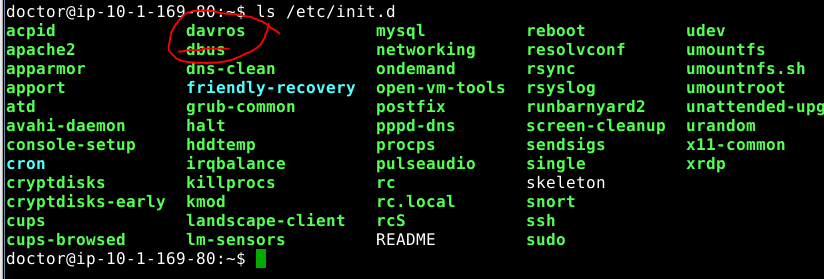
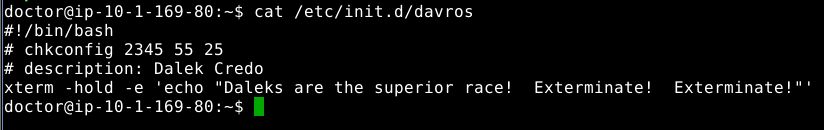
1. What users can run a terminal in the VM? (Hint: There’s a standard file in Linux that lists all the users; it also lists the user’s terminal. If the terminal is listed as “nologin”, “sync”, “false”, or “halt”, that user can’t run a terminal.)   
   less /etc/passwd  
     
   <snip>  
     
   The users root, ubuntu, student, doctor, clara, and dalek can run /bin/bash. The user dalek certainly looks suspicious.
2. Clara always forgets her password, so she had the Doctor save it in a file called Danny (her boyfriend’s name is Danny Pink.) She forgot where the file is, so you’ll have to find it for her. (Hint: the find command will help.) What is Clara’s password? (Hint: if the command gives so many errors that you can’t find the file, you can: pipe the output to less; or use the technique in the files lesson to redirect the errors to a place where they won’t bother you; or pipe the output to something that searches for Danny.)  
   find / -name Danny 2>/dev/null  
     
   cat /var/account/Danny  
     
   Clara’s password is CoalHillSchool.
3. The Doctor created a directory /home/tardis.
   1. Who is the owner and what is the group for that directory? What permissions are assigned?  
      ls -l /home  
        
      The owner of /home/tardis is doctor, and the group is tardis. The owner (doctor) has rwx, the group (tardis) has r-x and other has r-x.
   2. Log in as, or switch user to clara. Can she read the Tardis Manual in /home/tardis? Can she write to files in /home/tardis? (Hint: if clara can read files try to create a file in that directory to see if she has write privileges.)  
      su - clara (password is CoalHillSchool)  
        
      Clara can read files  
      

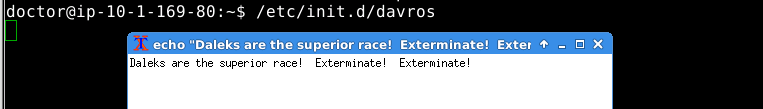
Clara cannot write files

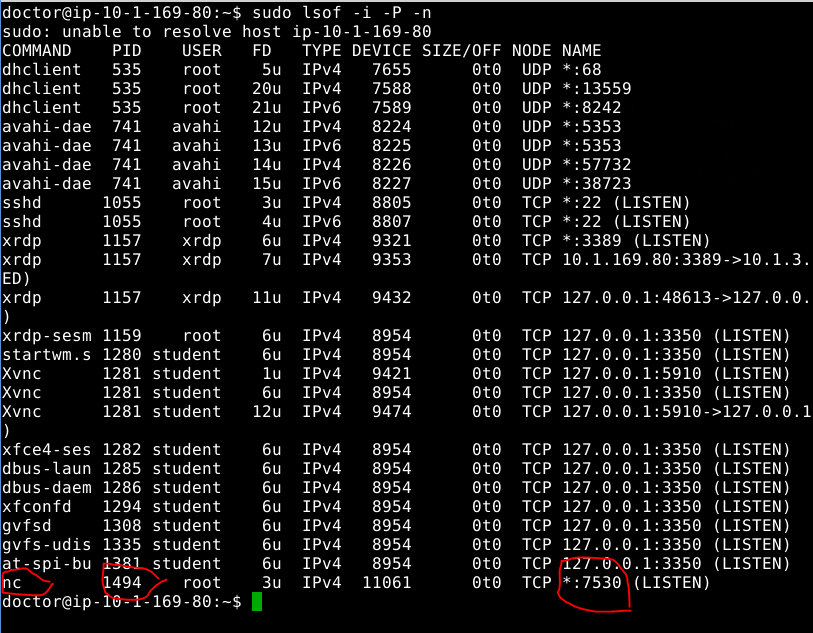
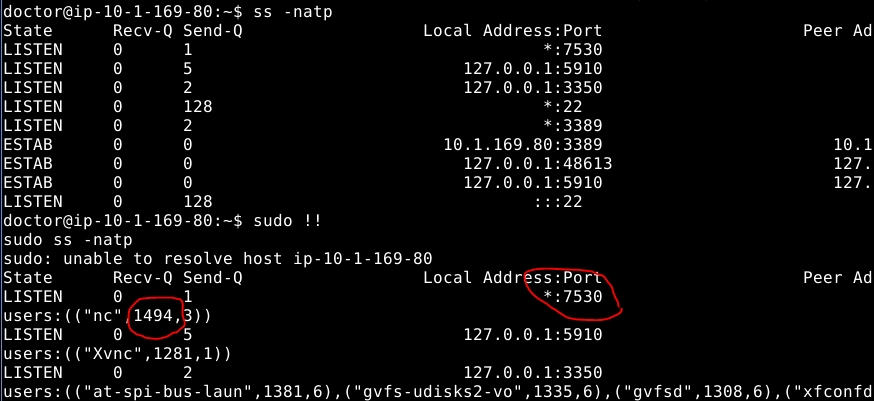
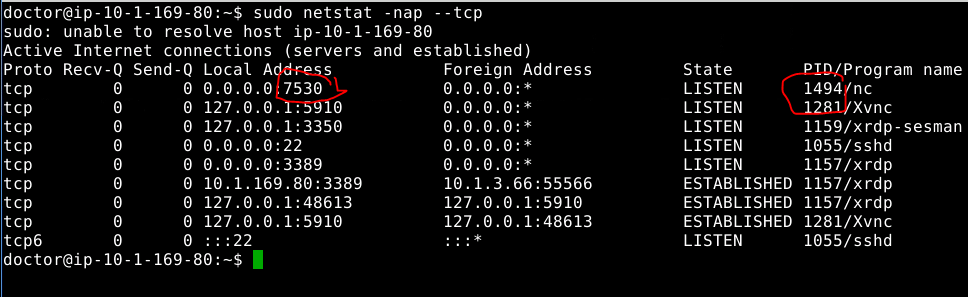
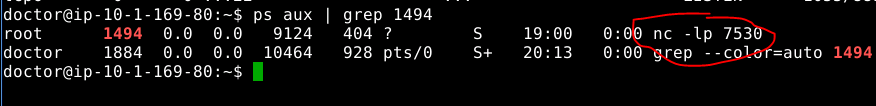
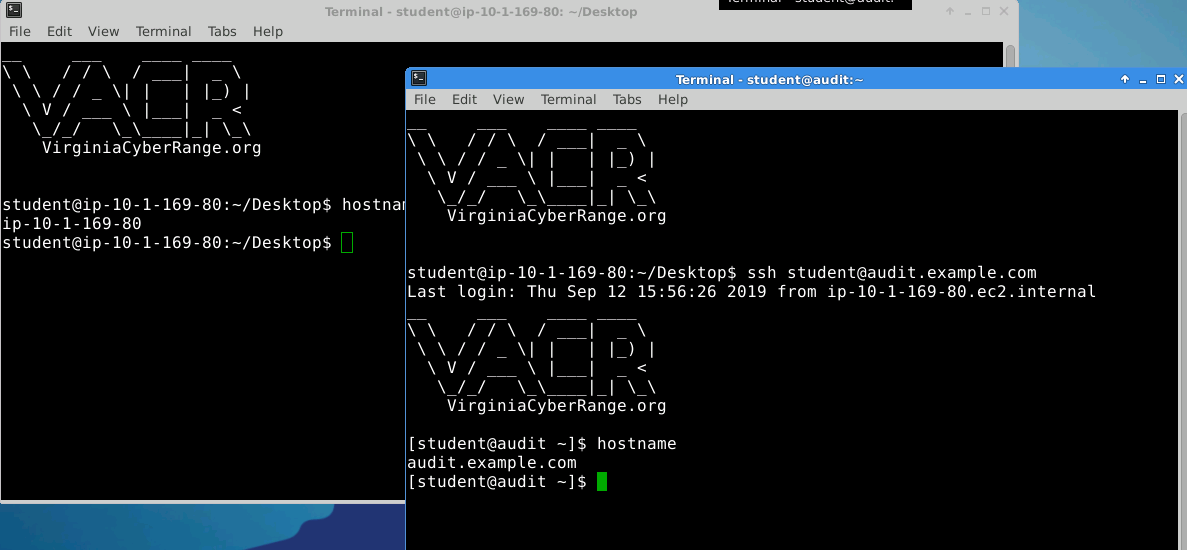
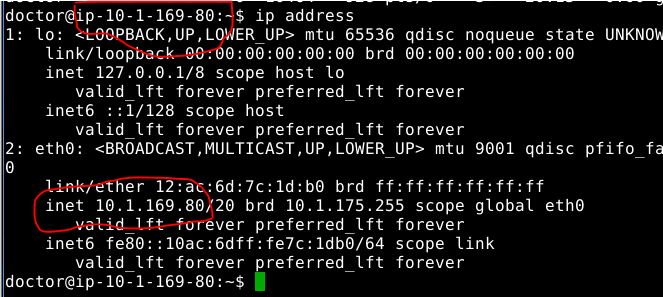
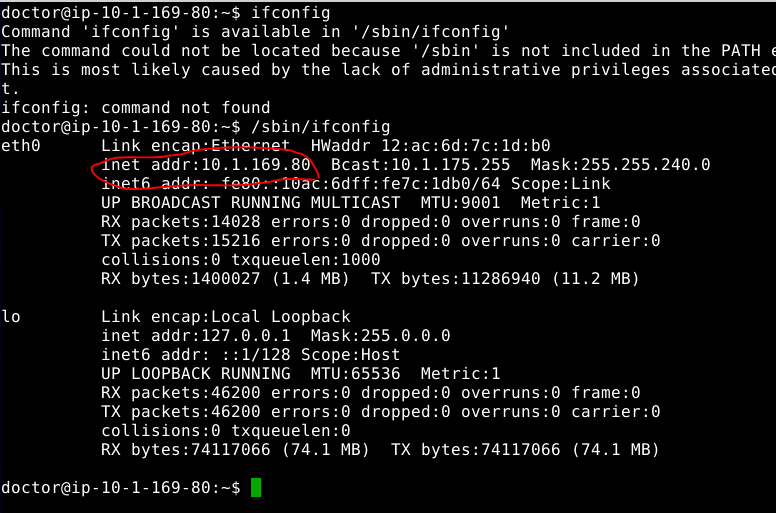
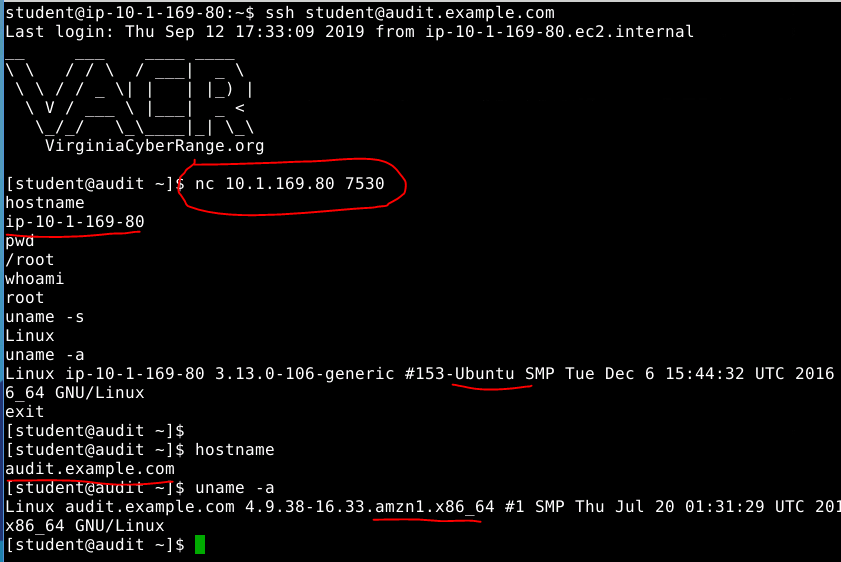
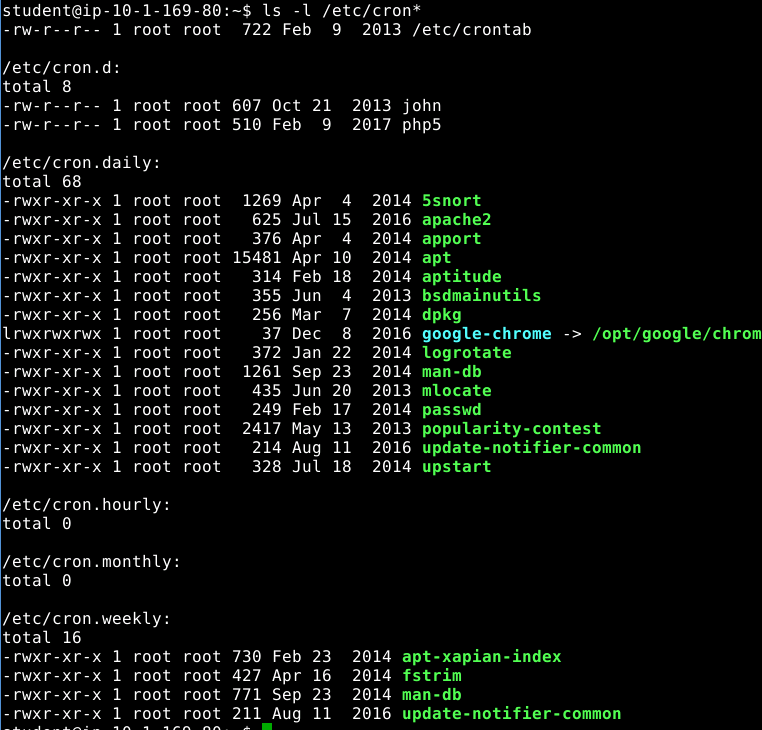
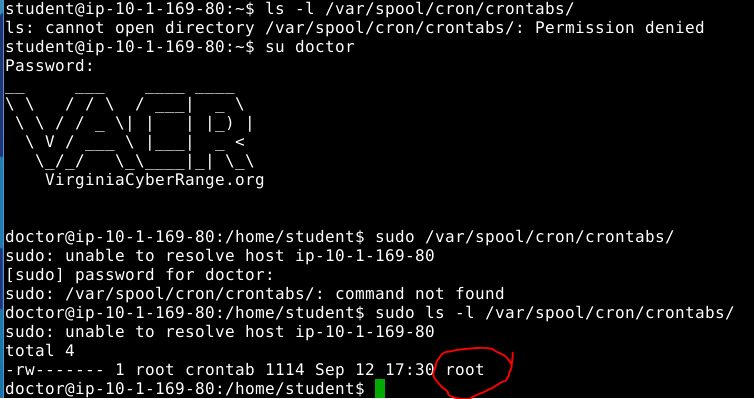
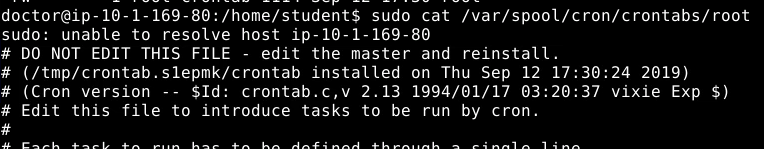
* 1. Why does clara have the rights she does?

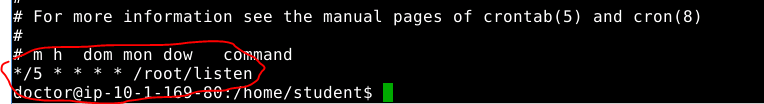
groups or cat /etc/group | grep clara or grep clara /etc/group  
ls -l /home  
  
clara has read permissions to the Tardis Manual because she is in the tardis group

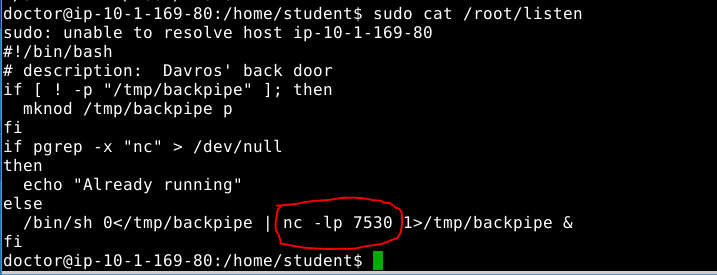
* 1. Using the clara user, read the Tardis manual. How do you make the Tardis take off?  
     Trick question! The Doctor threw the manual away.

1. The Doctor can’t remember passwords either. He is in the habit of emailing his password to himself so he can find it later. He thinks it is clever to use the password as the From: address. Usually it looks like From:<password>@tardis.com and To:doctor@tardis.com. There is a large SMTP log file in /var/log/smtp. It would take a long time to page through the entire file, but you should be able to find the password with one simple command. (Don’t let it bother you that the SMTP log file is from a Windows server, but is stored on an Ubuntu machine. Weird things happen when the Doctor is involved.)
   1. What is the Doctor’s password?  
        
      grep tardis /var/log/smtp  
      The doctor’s password is Gallifrey.
2. Since the Doctor is the hero, he should have root access. Log in as doctor and see if he does. How does the Doctor access his privileges? (Hint: remember there are two ways, and both start with “su”. Try both and see if they work.)  
   su - doctor (password is Gallifrey)  
     
     
   su - with the doctor’s password doesn’t work. It looks like someone changed the password on the root account. However, sudo does work, either sudo su -, or sudo -i will do the trick.
3. Now that you have root access using the Doctor’s account, let’s go back and look at the users again. Examine /etc/shadow, and determine which of the users you found in step 1) can actually log in. (Hint: they need a valid hash. An ‘!’ in the position for the hash means the account is disabled, and an ‘\*’ means no password has ever been set for that account. Valid hashes are usually long.)  
     
   <snip>  
     
   <snip>  
     
   root, student, doctor, clara, and dalek have passwords set. Ubuntu is locked, so can’t log in.
4. Davros tried to create a service that runs when the machine changes run levels. He used the old sysV method for creating services. Can you find it? (Hint: Where are scripts for services put in SysV?) What is the full path to the file he made, and what does it do when executed? (The answer to this question is a strong hint for the next question.)  
   Scripts for SysV services are kept in /etc/init.d  
   ls /etc/init.d  
     
   Hmmm, davros looks suspicious. What’s in it, I wonder.  
   

Looks bad. (Normally you would only execute malware in a restricted sandbox, but since this is an adventure…  


1. The Doctor says the root password should be the same as his password, but it’s not. It appears Davros has changed it. Can you guess the root password? What is it? (Hint: see the answer for question 7.)  
   If you try the words in the Dalek Credo, you will find that Exterminate! is the root password.  
   su - (use Exterminate! as the password)  
   
2. Davros was successful in installing a back door that is listening to the network. Use the techniques you learned in the lab on unnecessary services to find it. Note: the open TCP port 3389 is what VA Cyber Range uses to allow you to get a GUI connection to your VM. Don’t mess with it. There are two other open TCP ports; one is normal, one is not and could be a back door.
   1. Is there a suspicious port open?  
      ss -nat (netstat -na --tcp also works)  
        
      (right-most column clipped in screenshot)  
      The listening ports are 22, 3389, and 7530. Port 22 is ssh, may be legit, port 3389 is used by VA Cyber Range, and port 7530 bears further investigation.
   2. What is the process ID (PID)?  
      sudo lsof -I -P -n or  
      sudo ss -natp or  
      netstat -nap --tcp will work.  
        
        
        
      The PID is 1494. Yours will be different since PIDs are dynamically assigned.
   3. What file or command opened the suspicious port?  
      ps aux | grep 1494  
        
      The command was nc -lp 7530
3. For fun, let’s be Davros and use his back door. There is a second VM in this environment used for auditing, or checking, the main VM. To access the second VM, open a second terminal as student (su to student if you logged in with the doctor or clara accounts.) Execute this command:  
   ssh [student@audit.example.com](mailto:student@audit.example.com)  
   This will establish a Secure Shell (SSH) connection to the audit VM, and log you in with the student account on the audit server. (You don’t need a password because your account on the main VM has a private key that is allowed to log in--it’s in ~/.ssh)  
     
   The image above shows a terminal in the main VM (background, grey title bar). The hostname command outputs ip-10-1-169-80, which is the name of the main VM. The foreground terminal (blue title bar) shows the ssh command (ssh [student@audit.example.com](mailto:student@audit.example.com)) and the output of hostname shows audit.example.com. That means the foreground terminal is remotely commanding the audit VM.  
   We want to use the audit VM to connect to Davros’ backdoor on the main VM. To do that we will use nc (netcat), but first we will need to know:
   1. The IP address of the main VM. (You can look up the command to use to determine this, but there is an obvious give-away on this particular VM. Hint: If you are choosing between addresses, it is not 127.0.0.1; that’s the loopback address.)  
      ip address or the older ifconfig will work  
        
        
      The IP address of my VM is 10.1.169.80. Yours may be different. Note that the host name for this VM is the IP address.
   2. The port that Davros’ back door listens on. (You should have found that in step 9.)  
      7530  
        
      Once you have the information, enter this command on the audit VM. The audit VM is the one with the blue title bar in the picture above. The output of its hostname command was audit.example.com.  
      nc [ip address of main VM] [port that the back door listens on]  
      Here’s an example, but with the wrong IP (10.0.0.1) and port (1234)  
      nc 10.0.0.1 1234  
        
      If the command gives no output, don’t panic! Davros’ back door is a shell, not a terminal. It does not give you a prompt (ex. student@ip-10-1-169-80:~$). However, if you type a command, you should get a response. In the image below, I typed hostname, and the backdoor responded with ip-10-1-169-80.  
        
      Try other commands for basic exploration, like  
      pwd (show the current directory, or print working directory)  
      whoami (show the user I’m logged in as)  
      uname -a (show all the info about the Unix version)  
      ls  
      You can also mess around with changing directories, executing programs, or whatever you want. GUI programs and nano will not work, though.  
        
      When you are finished, you can type exit or hit control-C to get your prompt back on the audit VM.  
        
      The answer to this question is a screenshot of the audit VM terminal with the response to the hostname command from Davros’ back door, just like the image above (without the whiteout, though :-)  
        
      Note that after I exit the back door and return to the audit VM, the answers are different.
4. (Extra Credit) If you kill the process, you should find that it will restart within 5 minutes. Can you (and your friend Google) find something that would cause that to happen?  
   The big hint is “will restart within 5 minutes.” The cron program starts jobs at specific time intervals.  
     
   System cron files are found in /etc  
     
   Let’s search them to see if any contain part of the command we saw before, nc -lp 7530  
     
   Nothing.  
   User cron files are found in /var/spool/cron/crontabs/  
     
   There is a file, /var/spool/cron/crontabs/root. Wonder what’s in it…  
     
   <snip>



AHA!! Every 5 minutes, it runs /root/listen   
  
  
There’s a bunch of BASH gobbledegook there, but the command we saw in ps is there. Case solved.