**Linux Security Exercise**

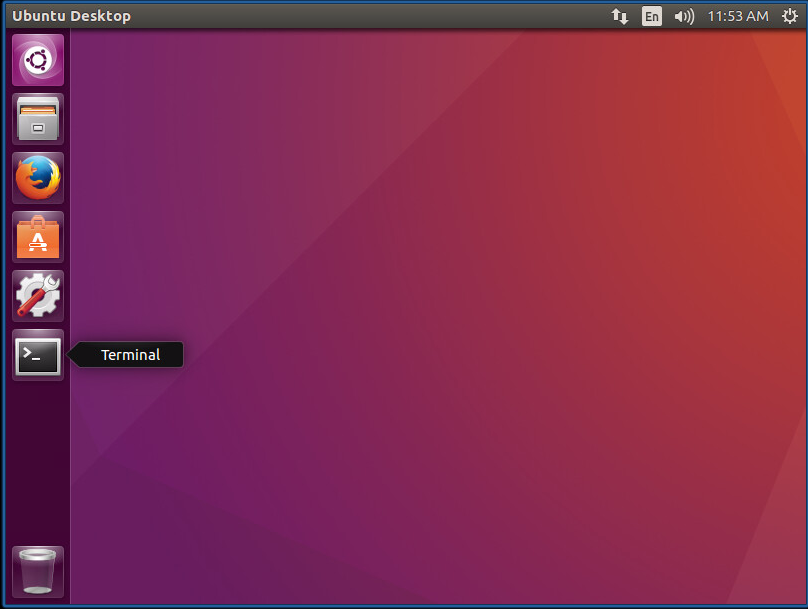
1. **Introduction**

Linux is a free, open-source operating system. While not as popular as Windows, Linux is widely used on servers and some desktop machines. OSX and iOS, Apple’s desktop and mobile operating systems, respectively, are offshoots of Linux. Hardening Linux VMs is also part of the CyberPatriot competition.

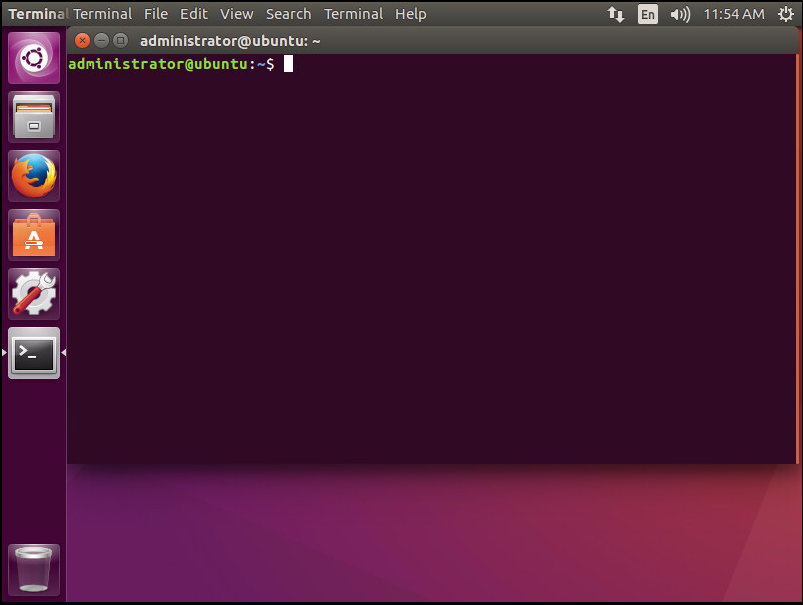
To get started with this exercise, select you “Ubuntu” VM and revert to the “Linux Security Exercise” snapshot. Power on the VM and open the console window. Click on the “administrator” user and enter the password “password”. Once logged in, you will notice that Ubuntu has a full GUI like Windows, however, in this exercise we will use the GUI very sparingly. Although almost everything you will do in this exercise can be done via the GUI, it is not uncommon for a Linux server to have no GUI. On servers, the GUI is unnecessary and an additional source of potential vulnerabilities so it is often disabled. In this exercise we will be using the Linux command line to enter commands. It is important to be able to utilize the command line on a Linux host in case the GUI is either disabled or not working properly.

1. **The Terminal**

In order to enter commands you will need to open a terminal window. Click on the “Terminal” icon on the left side of the screen:



A terminal window will open as shown below:



1. **The Command Prompt**

Once the terminal window opens you will see a prompt. In this case the prompt is “administrator@ubuntu:~$”. Let’s examine what that prompt is telling you. The first part, “administrator”, is your user name. The “@” character separates your username from the next field – the hostname. The name of your machine is “ubuntu” – you can verify this by typing the command “hostname”. The colon separates the hostname from the next field which is the current directory. The “~” character always refers to a user’s home directory, so you are in the administrator user’s home directory. The last character in the prompt, “$”, tells you that you are executing commands as a regular (unprivileged user). If you were a privileged user it would be a pound sign (#) instead of a dollar sign ($).

Since you are in the administrator user’s home directory, enter the command “ls” to see what is in that directory. You will see a number of items. If you enter the command “cd Documents” you will enter the Documents subdirectory. Note how the prompt has changed to “administrator@ubuntu:~/Documents$” to reflect that you are no longer in the administrator user’s home directory, but are now in the Documents subdirectory within the administrator user’s home directory. If you do another “ls” command, you will see that there are no files or directories in the Documents subdirectory. You can go to the parent directory above Documents with the command “cd ..”. You are now back in the administrator user’s home directory and the prompt should read: “administrator@ubuntu:~$”. You can always use the “pwd” command to see the directory that you are currently in on the filesystem. Enter the command “pwd” now and you should see “/home/administrator”. So you are in the “administrator” subdirectory of the “/home” directory.

Use the “cd ..” and then “ls” commands to go up one level and see what else is in the “/home” directory. Note that your prompt changes to “administrator@ubuntu:/home$”. There are directories for administrator, curly, elvis, larry, and moe. Can you get into larry’s directory with the command “cd larry”? Try it, and you will see that you get a permission denied error. If you know his password, you can switch to the larry user. Do this with the command “su larry”. When prompted for a password, enter “password”. Note how the prompt has changed to “larry@ubuntu:/home$”. You are now entering commands as larry. Try going into administrator’ home directory with the command “cd administrator”. Again, permission denied – larry does not have access to administrator’ home directory just as administrator did not have access to larry’s home directory. Now try the command “cd larry” note that your prompt changes to “larry@ubuntu:~$”. Type the command “ls” to see what is in larry’s home directory. Then use the “cd ..” command to return to the “/home” directory. We are now done executing commands as larry so type the command “exit” and you should be back to the administrator user. Note the prompt now identifies the user as “administrator”.

1. **Change Default Administrator Password**

The first, and most important thing to do is to change all passwords from their default values. An attacker will likely know any default passwords that are used by a system, and if they are not changed the attacker will easily be able to log in cause damage. First, let’s take care of the administrator user who is the administrator of the machine. Enter the command “passwd administrator”. When asked for the current password type “password”. You will then be asked to type a new password twice. If you do this correctly you will see that the password was updated successfully.

1. **Set Password Policies for your Users**

Let’s return to the user larry. To enter commands as larry you must first enter the command “su larry” and type larry’s password: “password”. Now let’s change larry’s password from the default. Enter the command “passwd larry”. Enter larry’s password and for his new password enter “larry123” twice. You have now changed larry’s password, but it is not a very good password since it can be quite easily guessed. Type the command “exit” to go back to entering commands as the administrator user. You will now install the cracklib package which will force users to choose harder-to-guess passwords. Enter the command “sudo apt-get install libpam-cracklib”. The sudo at the beginning of this command tells the system that you would like to perform a privileged action. If you are one of the user’s authorized to perform privileged actions (as the administrator is on this system), you will need to enter the administrator’s password.

Now that cracklib is installed, go back to the larry user with the command “su larry”. Enter larry’s password: “larry123”. Type the command “passwd larry” to change his password. Enter his old password “larry123” and then try entering “larry321” for his new password. That password is not allowed since it is based on his user name. Try entering “password” as the new password. That password is not allowed because it is based on a dictionary word that attackers often guess. Try entering “abc” as the new password. That password is not allowed because it is way too short. Enter the “passwd larry” command again and choose a good password for larry. Type “exit” to return to using the administrator’s account. Then change the passwords for all the other users with the commands:

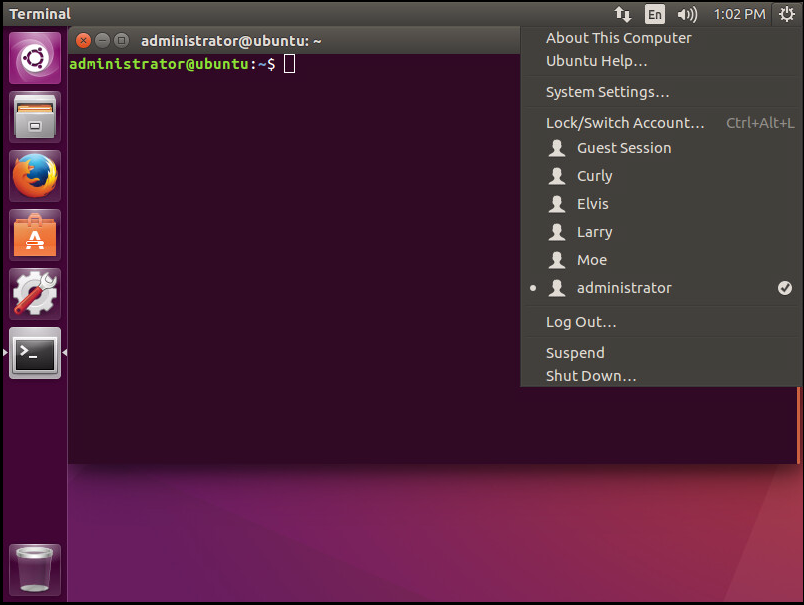
sudo passwd curly

sudo passwd elvis

sudo passwd moe

1. **Set Failed Login Attempt Limit**

Attackers can use an automated tool that will repeatedly try guessing passwords for an account until it succeeds. To stop this attack we need the system to temporarily lock an account if too many incorrect login attempts are made. Click on the icon in the upper right corner and choose “Log Out…”:



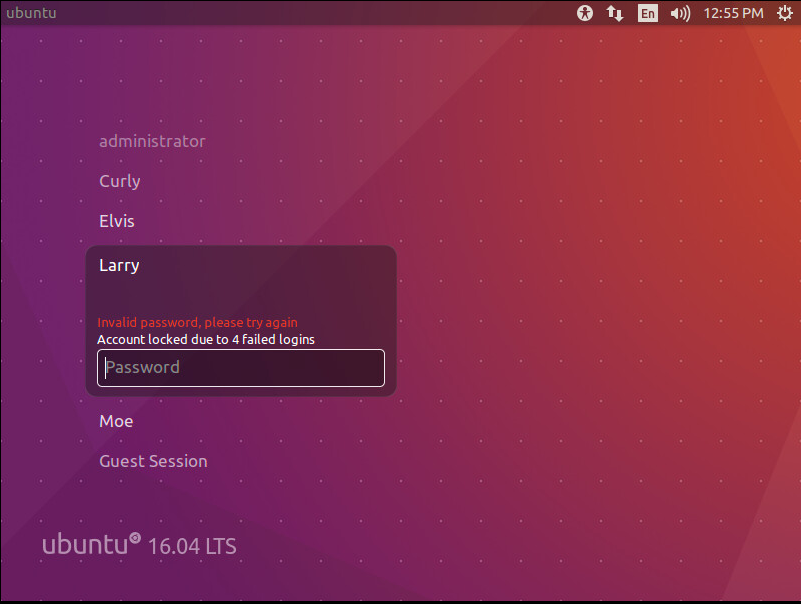
Then click on the “Log Out” button.

On the logon screen, click on the account for larry and try entering a password that is not larry’s about five or six times. Notice how the system just keeps asking you to try again. Enter larry’s correct password and you are successfully logged in. Log out of larry’s account and log into the administrator’s. Open the terminal and enter the

command “sudo gedit /etc/pam.d/common-auth”. You will be prompted for the administrator’s password and then an editor will appear. Add the following line at the top of the file:

auth required pam\_tally2.so deny=3 unlock\_time=20

This line tells the system to lock an account after three unsuccessful login attempts and to unlock the account after 20 seconds have passed with no unsuccessful login attempts. Click the “Save” button in the upper right and then the “x” in the upper left to close the editor. Log out of the administrator’s account and click on the larry account on the logon screen. Enter incorrect passwords until you see that the account has been locked:



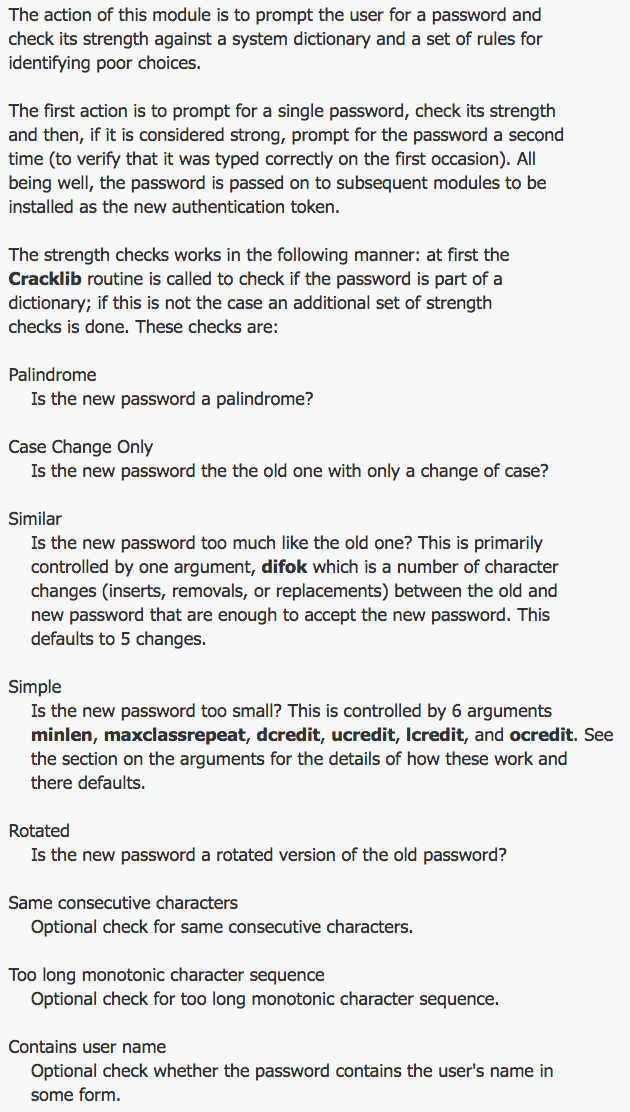
Enter larry’s correct password and you still will not be able to log in. Wait 20 seconds and enter larry’s correct password and you should be able to log in. Log back out of larry’s account and into the administrator’s.

1. **Other Account Settings**

Once logged into the administrator’s account, open a terminal and enter the command: “sudo gedit /etc/pam.d/common-auth”. Add a new line below the one you already added:

password requisite pam\_cracklib.so retry=3 minlen=8 difok=3 reject\_username minclass=3 maxrepeat=2 dcredit=1 ucredit=1 lcredit=1 ocredit=1

This line specifies some parameters about how cracklib should determine what types of passwords are allowed:



For the full manual page on cracklib see:

<http://manpages.ubuntu.com/manpages/trusty/man8/pam_cracklib.8.html>

Add another line that says:

password requisite pam\_pwhistory.so use\_authtok remember=24

This enables the system to remember the last 24 passwords that a user has used and will not allow him/her to reuse one of those passwords.

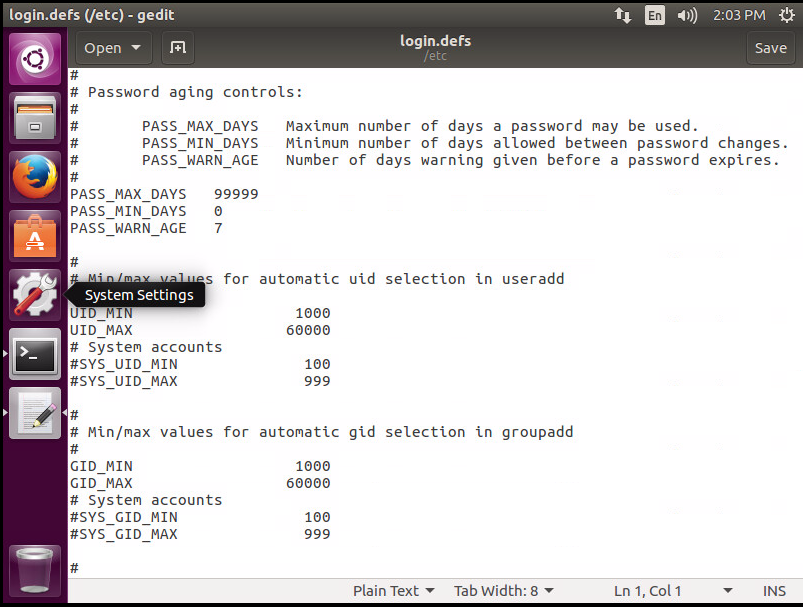
Finally, add another line that says:

password [success=1 default=ignore] pam\_unix.so obscure use\_authtok sha512 shadow

This tells the system to use the newer, stronger SHA512 algorithm to store password hashes rather than the older, weaker MD5 algorithm. Click the “Save” button in the upper right and then the “x” in the upper left to close the editor.

1. **Password Policies**

Now enter the command “sudo gedit /etc/login.defs”. Scroll down to the part of the file that deals with password aging controls:



Change the value for PASS\_MAX\_DAYS to 90, the value for PASS\_MIN\_DAYS to 7, and the value for PASS\_WARN\_AGE to 14. This will only allow a user to change his/her password once every 7 days, require a user to change his/her password every 90 days, and start warning the user that his/her password is expiring 14 days in advance. Click the “Save” button in the upper right and then the “x” in the upper left to close the editor. Of course, these policies do not apply to users who already exist on the system. To implement these settings for them use the following commands:

sudo chage –m 7 –M 90 –W 14 administrator

sudo chage –m 7 –M 90 –W 14 curly

sudo chage –m 7 –M 90 –W 14 elvis

sudo chage –m 7 –M 90 –W 14 larry

sudo chage –m 7 –M 90 –W 14 moe

1. **Delete Unneeded Users**

Larry, Moe, and Curly have proven to be unreliable employees and have been fired. Let’s lock their accounts so that they can no longer log into the system. Use the commands:

sudo passwd –l larry

sudo passwd –l moe

sudo passwd –l curly

Also, the administrator account is the only one who should be able to use sudo to execute privileged actions. Use the command “sudo gedit /etc/group” to open the editor. Delete the user elvis from the “sudo” group. Click the “Save” button in the upper right and then the “x” in the upper left to close the editor.

1. **System Patching**

Another very important task is to make sure our system is running the most up-to-date version of its software. Older software often has vulnerabilities that are fixed in updated versions. We do not want to be running an old, vulnerable piece of software if a new, fixed one is available as this would make the system more susceptible to attacks. Update the system software using the commands:

sudo apt-get update

sudo apt-get upgrade

The second step might take several minutes to download and install all the newest versions of software on the system.

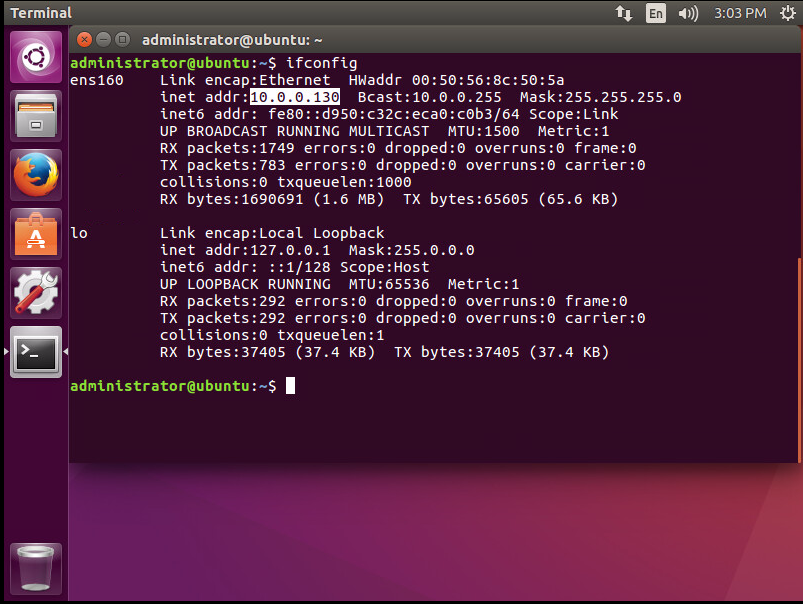
1. **Services**

Even if all of the system’s software is up-to-date, running services that are not needed unnecessarily exposes the system to extra risks. Use the command “service –status-all” to see all the services currently running on the system. Many of these services are needed, but some are not. The “cups” service, for example, is a printing service. Since we do not plan to do any printing from this VM, the cups service is not needed. First, stop the service using the command “service cups stop”. Next, use the command “sudo update-rc.d –f cups remove” to disable and remove the cups service so that it does not start back up when the system reboots. You can use the “service –status-all” and “service cups status” commands to verify that the service is disabled.

1. **Firewall**

The built-in Ubuntu firewall is called the Uncomplicated FireWall (ufw). Running a host-based firewall can help limit the risks of attackers connecting to unauthorized ports on your system. Use the command “sudo ufw status” to view the current state of the firewall on your VM. You will notice that it is inactive. Enable the firewall with the command “sudo ufw enable”. It is also a good idea to enable logging by your firewall so that you have a record of what types of traffic are being blocked by it. Use the command “sudo ufw logging on”. Because we have not specified any exceptions, the firewall is now blocking all incoming network traffic to our VM. However, we might have legitimate services that we want external users to be able to access over the network (our SSH server, for instance). Use the command “sudo ufw allow 22/tcp” to allow traffic through the firewall to TCP port 22 (which is where the SSH server listens). A final “sudo ufw status” command shows that our firewall is running and blocking all traffic except to TCP port 22 for the SSH server.

Let’s add a new service and allow traffic to it through the firewall. Install the Apache web server using the command “sudo apt-get install apache2”. Now the web server is running on our VM, but our firewall will block all incoming network traffic to it. Type the command “ifconfig” and note your VM’s IP address. In the figure below it is 10.0.0.130:



Ask your neighbor to open the Firefox web browser on his/her VM and try to connect to your web server with the URL: http://*<your IP address>* and verify that they get no response. However, if you open the Firefox web browser in your VM you should be able to use the same URL and get the default web page.Now*,* let’s add a firewall exception that allows traffic through your firewall to the web server: “sudo ufw allow 80/tcp”. Ask your neighbor to re-try a connection to your web server and it should now work.

1. **Conclusion**

Linux (especially the command line) can be a bit intimidating at first, but there are a few simple commands that you need to know to get started hardening a Linux machine. In addition to online guides that can help you, each Linux system has a built-in manual system that explains commands, their arguments, and usage to you. Just put the word “man” in front of any command and you will see the command’s manual page (e.g. *man passwd* or *man ufw*). If you don’t know the name of a command that does something you will have to Google it, but once you know the name you should be able to use the man page to understand what the command does and how to use it.