PolyBandit Command Line Game

Step 1 – Install a Hypervisor on Your Computer

Install a Type-2 Hypervisor on your computer. Report which hypervisor you used. Provide evidence that you installed this as part of your lab report. Make the evidence obviously unique to you, individually so that no one else could copy your lab report by embedded your username in the snapshot image you take.

Don't know what a Hypervisor is and where you can get one? Try some of the hints and pointers below:

The College of IST provides you with VMWare Workstation (for Windows) and VMWare Fusion (for Mac) via the Dreamspark/Imagine License and distribution system. See https://www.up.ist.psu.edu/dreamspark/access.php.

Also, VirtualBox is a free option. Check out https://www.virtualbox.org/

Step 2 – Install a Virtual Machine:

Install Ubuntu Linux Desktop, Version 18.04 LTS as a virtual machine.

Give the virtual machine 2 cores of CPU and 4 GB of Memory

When asked for a Computer Name, name the computer “Ubuntu”

When asked for a User Name, name the user “ubuntu” (note, this is lower-case).

When asked for a password, give it “password” (all lower-case – yes, I know – terrible password)

Step 2a Optional – Get all of the patches and updates to Ubuntu

Step 3 – Open the Terminal application and install components we will need on your system.

Step 3a: Install SSH Daemon (You will need to enter your password of “password” after entering these commands.)

```
sudo apt install ssh
```

Step 3b: Install Git

```
sudo apt install git
```

Step 4 – Establish baseline Snapshot (Optional)

You may wish to revert back to this stage of your implementation. Use your hypervisor to create a snapshot so you can revert back to this stage if things get messed up. See the following instructions:

VMWare Workstation (Windows)
https://docs.vmware.com/en/VMware-Workstation-Pro/14.0/com.vmware.ws.using.doc/GUID-E1002452-383E-4EC1-A9BE-CFC36AFA8631.html

VMWare Fusion (Mac)
https://pubs.vmware.com/fusion-7/index.jsp?topic=%2Fcom.vmware.fusion.help.doc%2FGUID-4C90933D-A31F-4A56-B5CA-58D3AE6E93CF.html

VirtualBox
https://www.techrepublic.com/article/how-to-use-snapshots-in-virtualbox/

Step 5 – Install the PolyBandit Exercise using git

Issue the git command to clone the game's code repository.

```
git clone https://github.com/giacobe/PolyBandit.git
```

Execute the installation script

```
sudo PolyBandit/install.sh
```

Here's what things should look like. Don't put *my* userid in, though. Put yours.:

```
ubuntu@ubuntu:~$ git clone https://github.com/giacobe/PolyBandit.git
Cloning into 'PolyBandit'...
remote: Enumerating objects: 75, done.
remote: Counting objects: 100% (75/75), done.
remote: Compressing objects: 100% (75/75), done.
remote: Total 252 (delta 44), reused 0 (delta 0), pack-reused 177
Receiving objects: 100% (252/252), 106.53 KiB | 1.66 MiB/s, done.
Resolving deltas: 100% (152/152), done.
ubuntu@ubuntu:~$ sudo PolyBandit/install.sh
[sudo] password for ubuntu:
Please enter your PSU ID (abc1234):
nxg13
Setting up the levels of the game... please stand by...
Now starting the game. Please log in with the password 'level0'
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:iHNmmG8K7ouXFZ/H0wKNkLdfXYeiZ+MjWar6oVSDAM0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
level0@localhost's password:
```

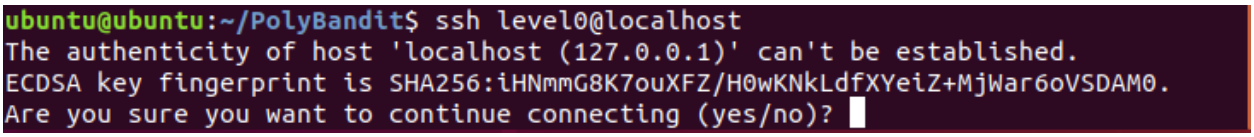
Step 6 – Start Playing the Game

Open the Terminal Application, if it's not open already.

When prompted, enter your PSU username (e.g. xyz1234). Do not enter your full email address.

The game will begin by opening an ssh tunnel back to this machine and will attempt to log in as "level0". The password for level0 is "level0".

For each level, you may get an error-looking message about the key fingerprint for the SSH connection. Bypass the error message by typing “yes” to the message like the one below:



For each level, record exactly what you did to figure out the password to the next level. Report the commands your used to locate the password for the next level. Take screenshots of what the command and the response.

When you find the password for the next level, issue the command to ssh to the next level’s account. Replace the # with the level number.

```
ssh level#@localhost
```

Create a table of all of your passwords. Your passwords will be different than your classmate’s. Don’t copy/paste and cheat. Help each other, but do your own work.

The last password that you find in Level 10 will prove you have completed the exercise. However, I want all of the evidence of **how you completed the exercise** as part of your lab report. Be detailed. Take screen shots.

WARNING

As mentioned before, you may work with each other to figure out how to complete the level, but you must complete the level on your own. You will be reporting each of the passwords and your evidence of how you completed the lab. Failure to report both the passwords AND providing the evidence will result in a significantly lower grade on this lab.

You must complete the exercise and report the passwords that YOU found for YOUR account. If you report someone else’s passwords or use their evidence, I will give you a 0 on this exercise and report the academic integrity incident. Do not cheat. It only cheats yourself and makes me do extra paperwork.

What to turn in

You should turn in a Microsoft Word Document with the following contents:

- Evidence that you installed a hypervisor and got the game set up (Steps 1-5)
- For Step 6, you need to provide:
    - A table listing each level and password
    - A detailed walkthru (written description) of how you solved each level. You should write up, in words, what you did to solve the level.
    - Provide an annotated screen shot of the command(s) you entered and the password that you found.

Note, there are multiple ways to solve these levels. Higher grades on this assignment will be awarded to students who use only Linux command-line tools to solve the level and get the password.

Over-achievers may choose to combine their commands into one string (pipes, redirects, etc). If you do so, you must explain what each part of the string of commands does. Elegant solutions may receive bonus points. Bypassing the intent of the game will result in negative points.