Jordan Schalter

IT417

ATOMA

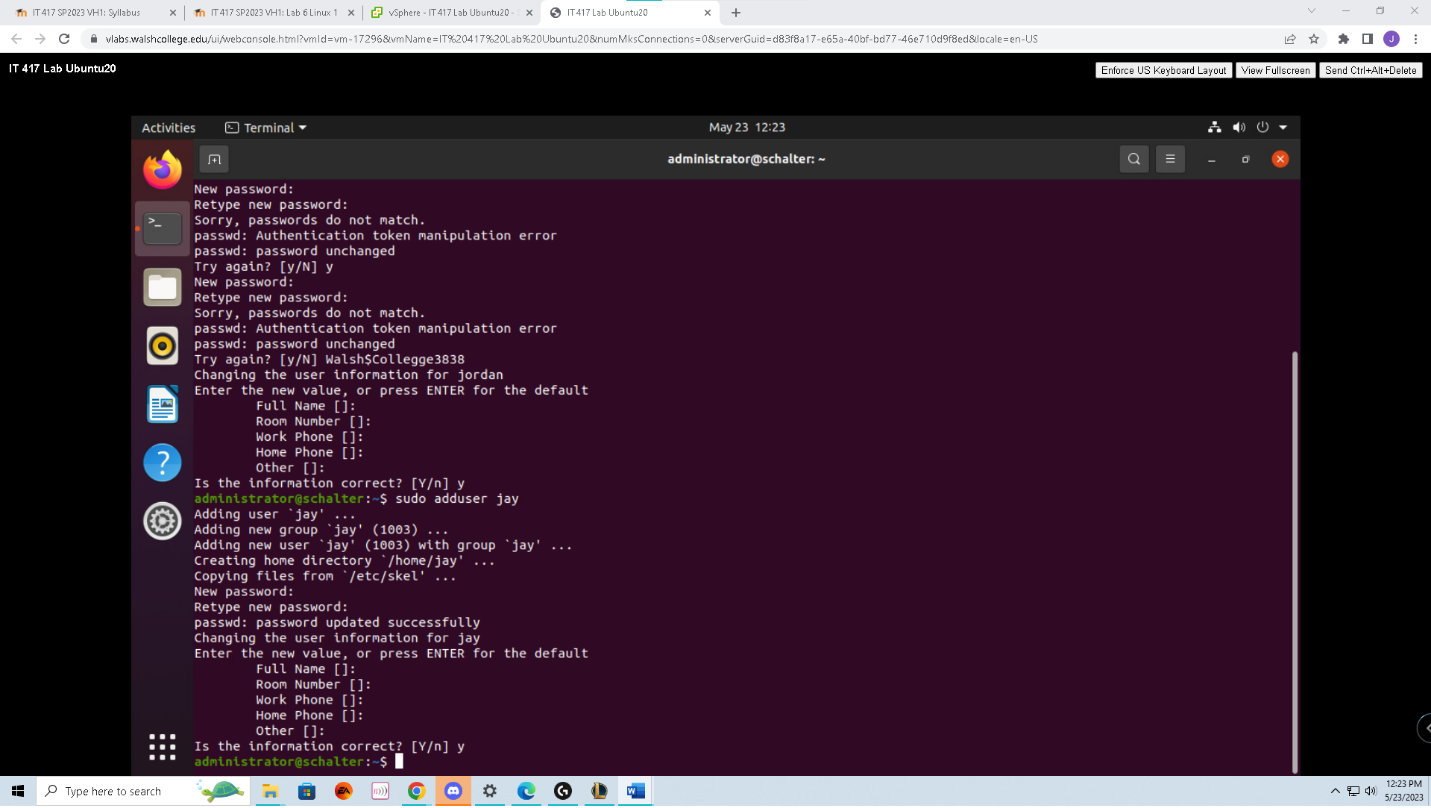
5/23/23

7.

A computer screen shot of a computer

Description automatically generated with low confidence

18.



19.

A screenshot of a computer

Description automatically generated

27c.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

28.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

31.

A screenshot of a computer

Description automatically generated

I double-checked the password and everything to make sure but, the account would still give me this error – this is assuming that the account is locked and it cannot be logged into.

33.

A screenshot of a computer

Description automatically generated

35.

A screenshot of a computer

Description automatically generated

37.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

38 a & b.

A picture containing text, screenshot, software, multimedia software

Description automatically generated

38c.

A screenshot of a computer

Description automatically generated

38d.   
The difference is that an expiry will make it so that the users password expires, and they need to change it. A lock will literally lock the user out from login.

40.

A screenshot of a computer

Description automatically generated

48. The first column shows the user that used the command line, the second is their PID which is the process identifier. Next, is the amount of CPU that the process uses followed by the amount of memory that the process requires.VSZ stands for virtual memory size, and RSS is the resident set size. TTY lets you know if the device has enabled typing. Stat stands for the status of the process, start is when the process started, time is how long the process took, and command shows what the command was intended to do.

A screenshot of a computer

Description automatically generated

55.Answer the following questions about this lab.

* 1. Last | more and hit enter in the terminal. Also, if you are at the computer, you might be able to use whoami.
  2. Ps aux and netstat -antp could show you some more information.
  3. netstat -antp
  4. Let’s say, you find someone logged in and you think its an attacker. You found them with the who command. You need to stop their login session and then lock their account. Provide a list of commands to gather the information, kill their connection, lock their account, and kill all of their running processes.

For the sake of this question, I am going to use the name Orochimaru as the attacker. First, I will use ps aux to figure out that Orochimaru has indeed infiltrated my network. Now, allow me to find the PID he is functioning from with ps -ef | grep. Next, I will change Orochimarus password with sudo passwd -Orochimaru. After changing his password I decided to be extra, we will set his password to expire sudo passwd -e, we will lock his account sudo passwd -l, then kill his tasks/processes sudo pkill -u Orochimaru. Finally, we shut him down with the shutdown command. We also, could delete his account all together with sudo userdel -r Orochimaru but, that was not required. I would also say that order of operations might be better off if he gets locked and killed first.