Cyber Range Lab Assignment 3

Command Line Basics

Jon Mahoney

SRA 440W

# General Context

In this lab assignment, there are four lab activities. The first lab, “Navigation”, has the user iterate on previously established commands like who and ls with different modifiers and techniques. For instance, the lab describes modifiers for the ls command such as -l and -lt. In addition to modifiers, the lab provides techniques such as autocompleting command strings with the tab key. Other commands used in the lab include tty, dir, and who am i. The next lab, “User Accounts and Privileges”, takes a look at password control. It starts out by showing the user the location of the file that contains information on passwords. This information includes personal identifiers, group identifiers, and password settings. Some password settings covered in the lab include -n days before next password change is allowed, -x days before password change warning is issued, and -w for a reset warning to be issued. After establishing information on password settings, the user is directed to create accounts, set passwords, and add them to different groups.

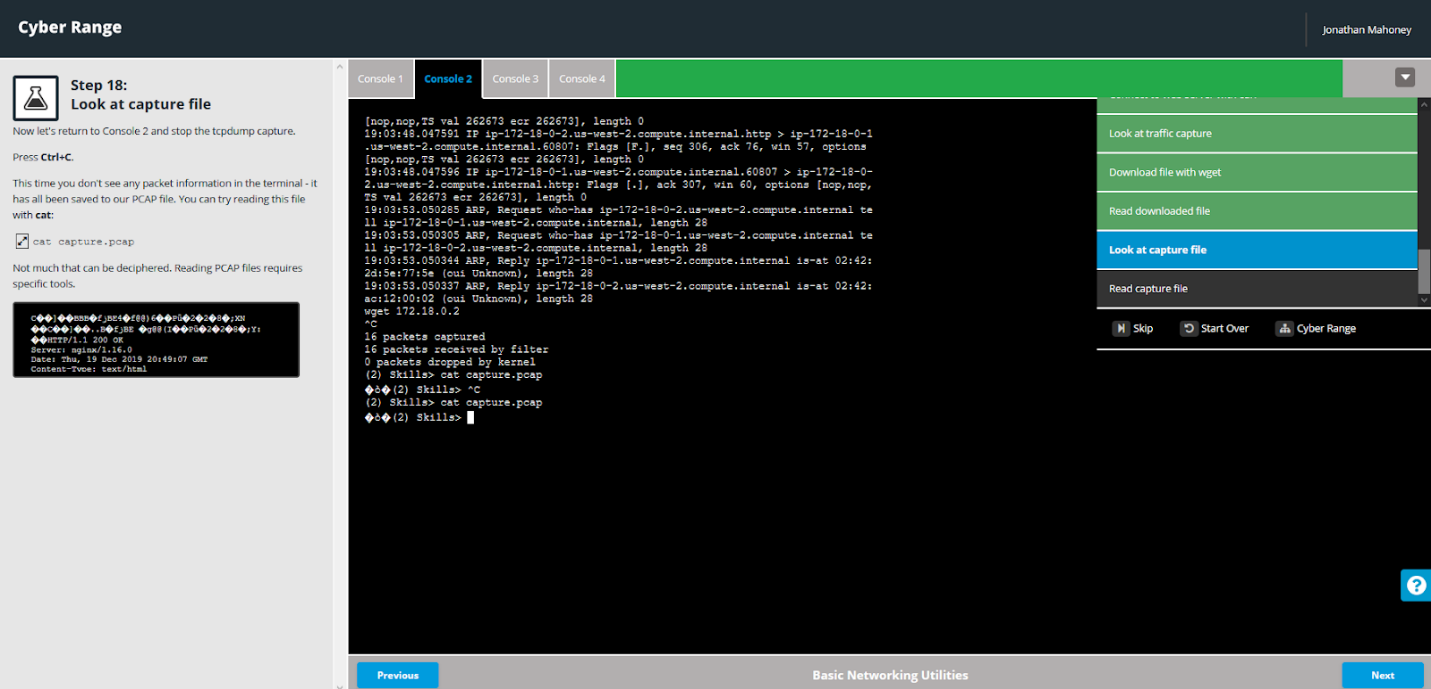
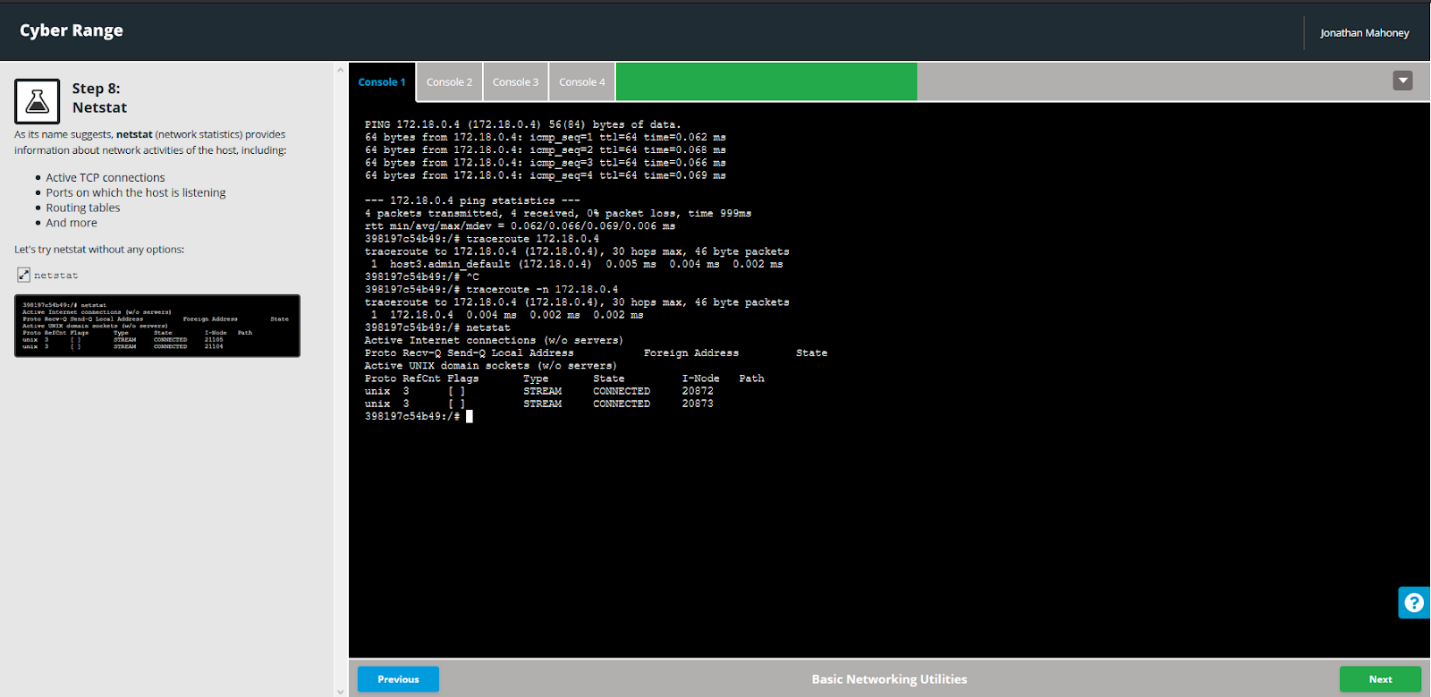
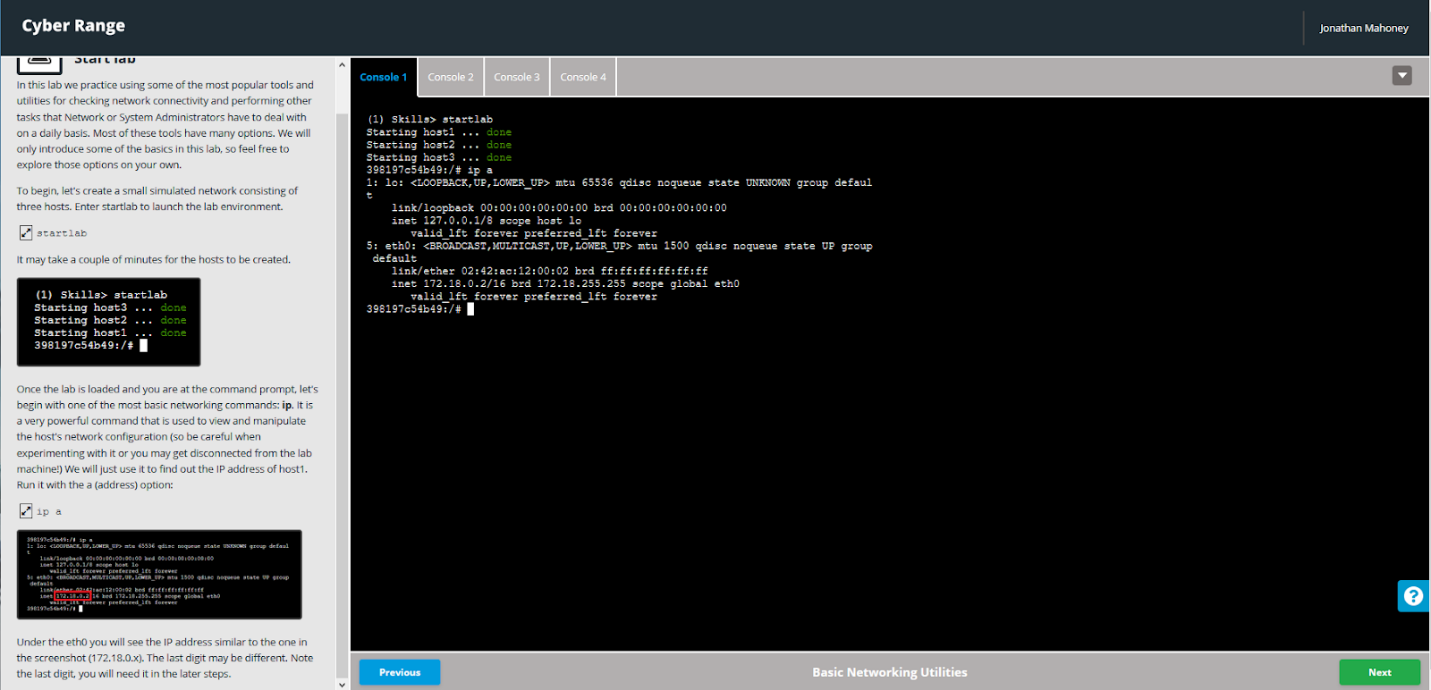
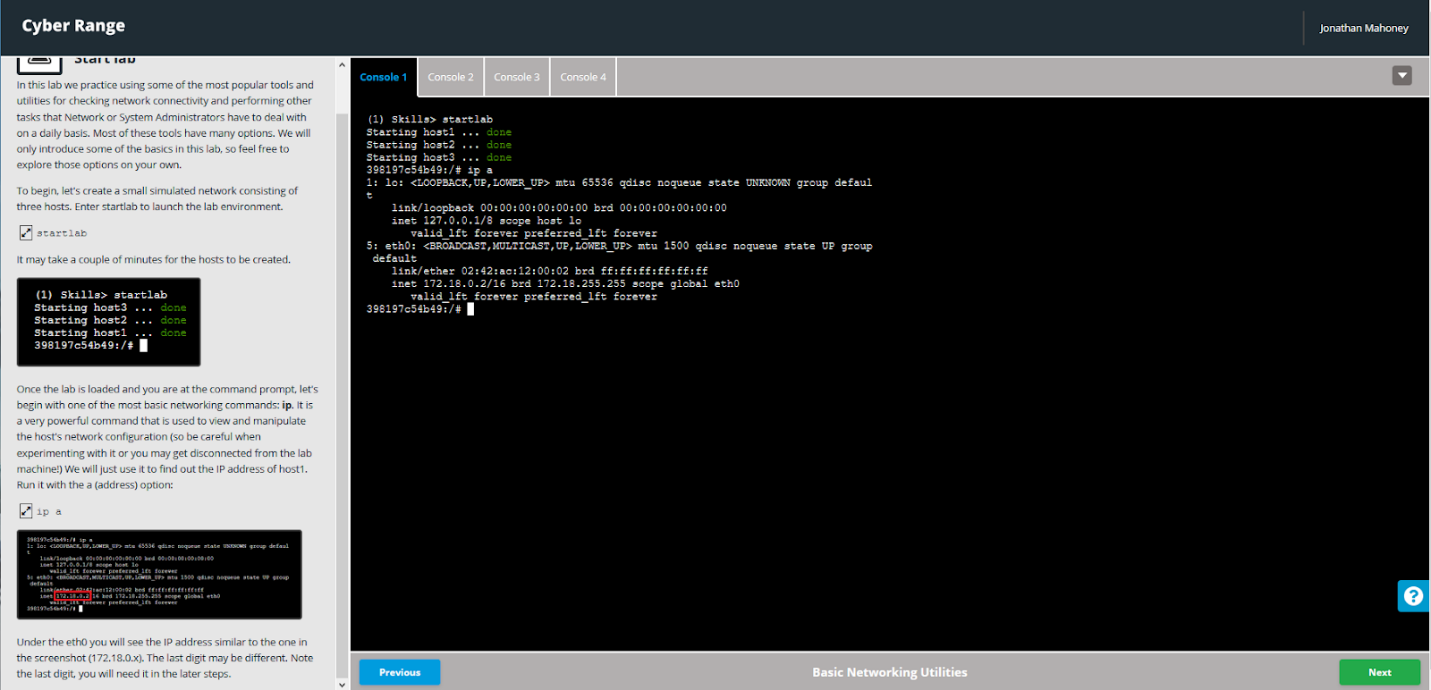
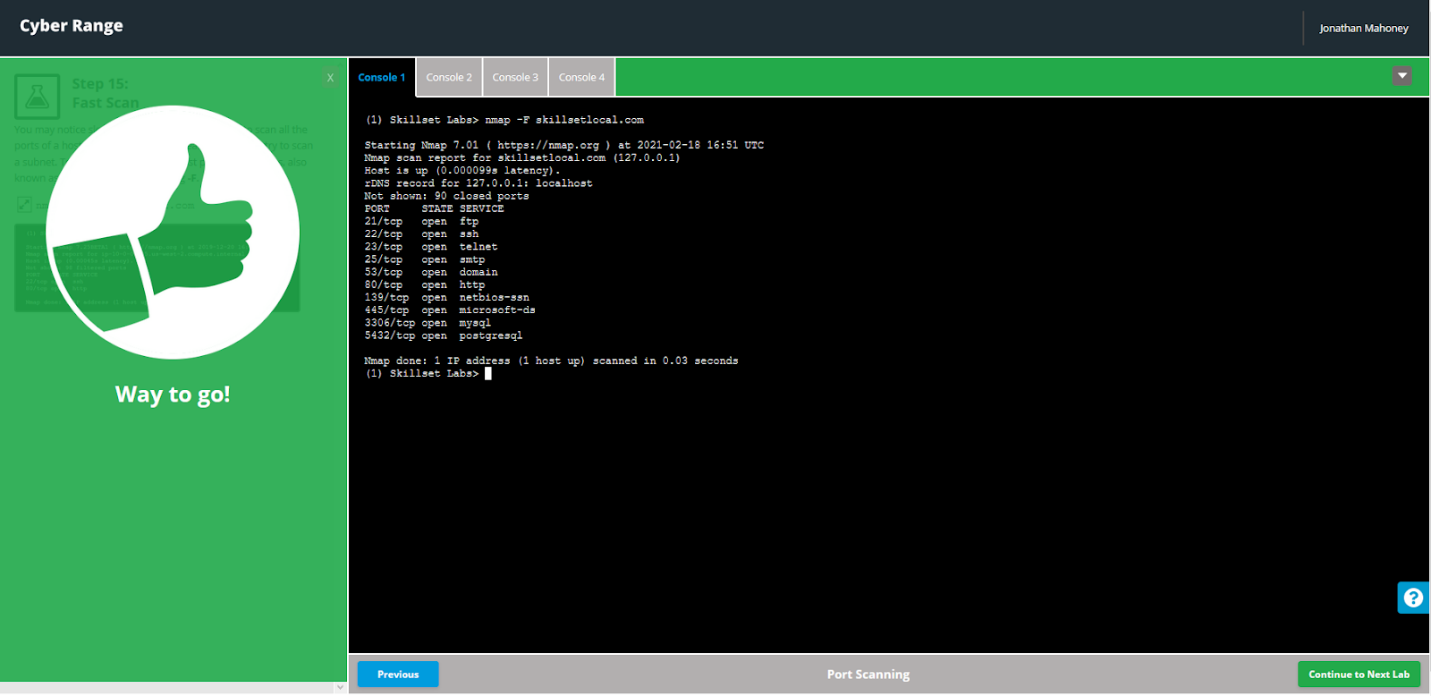
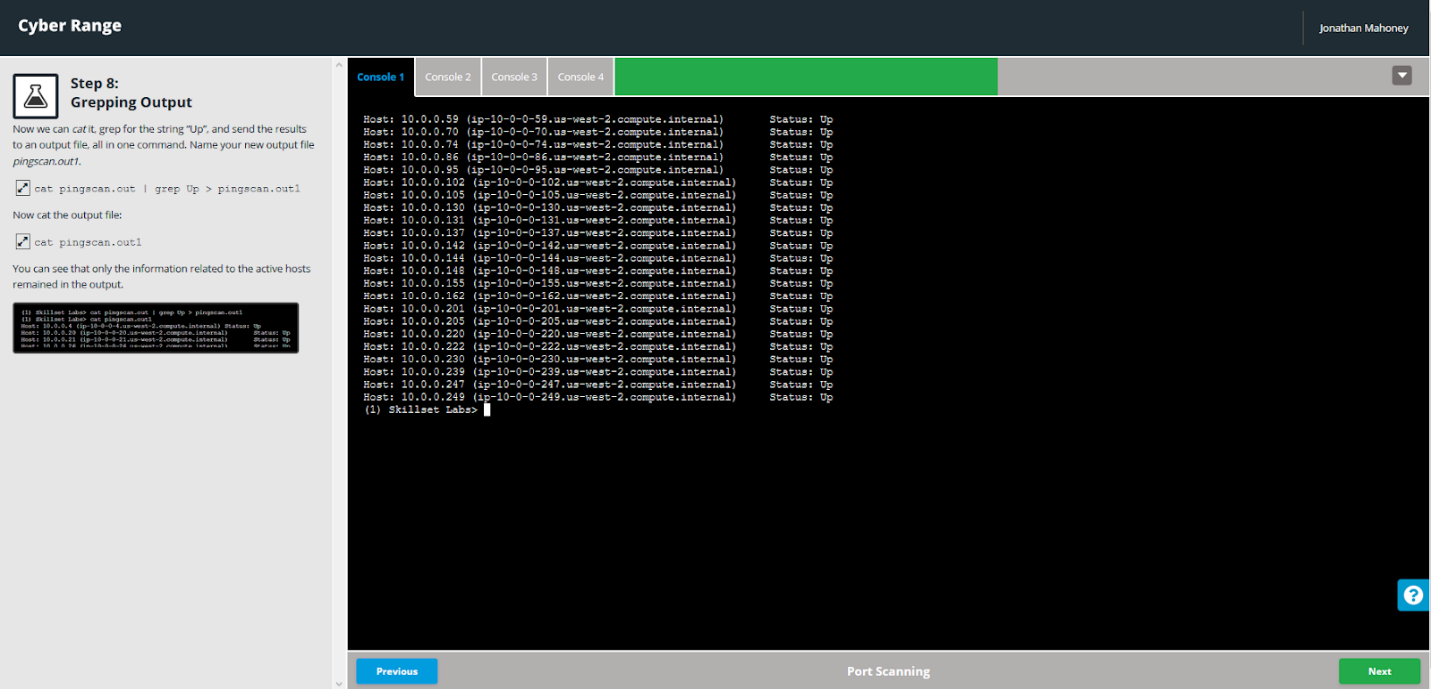
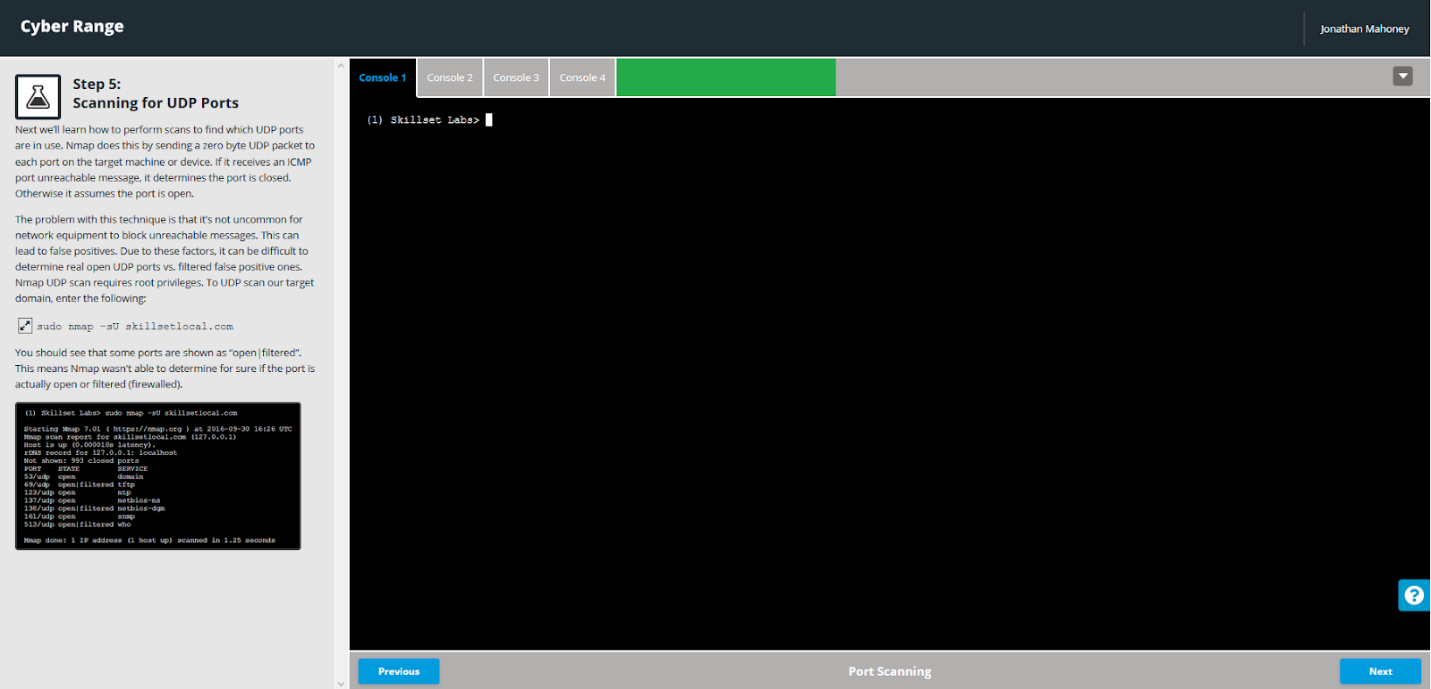
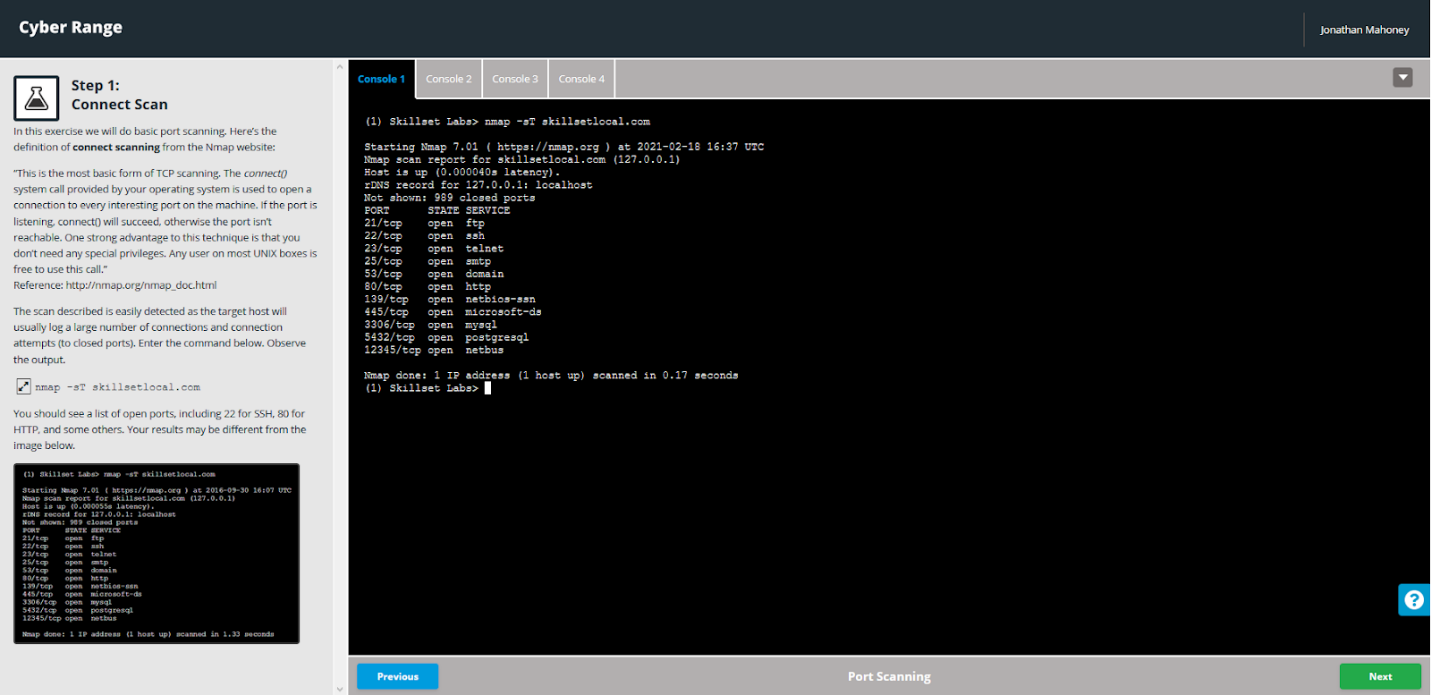
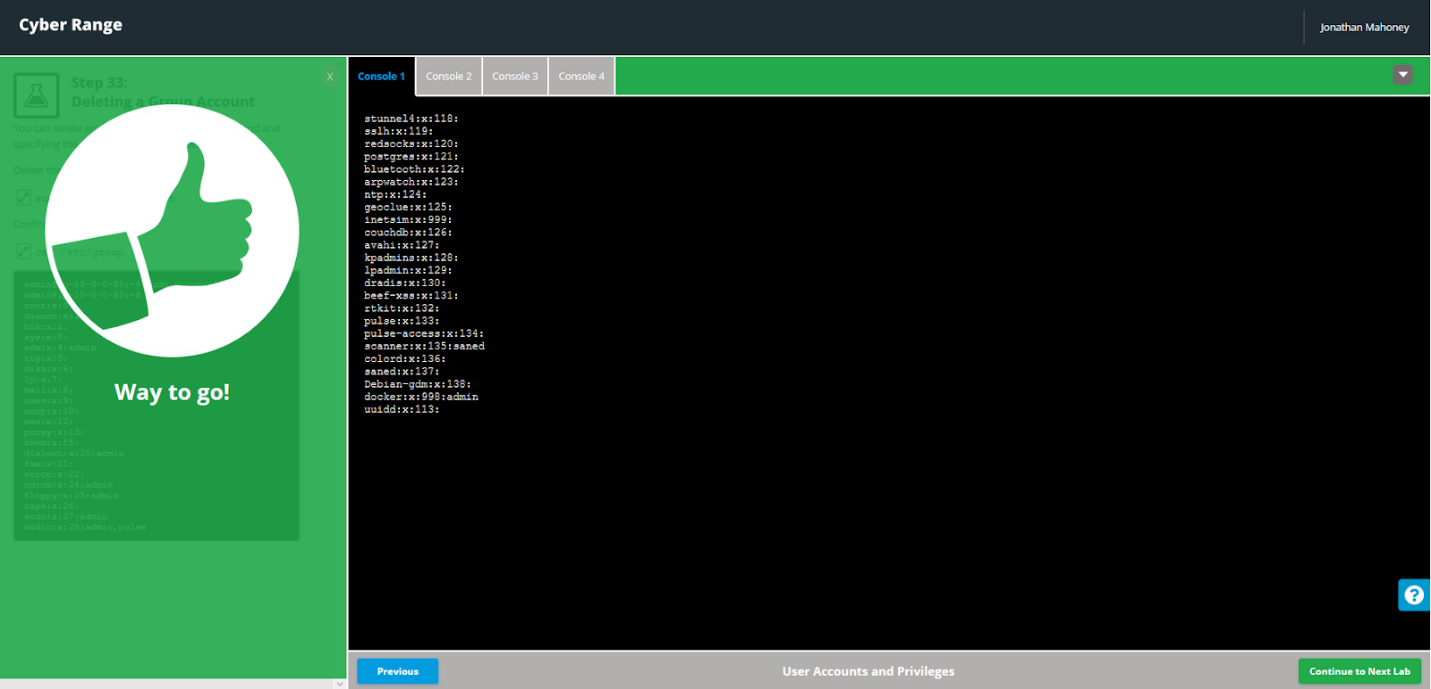
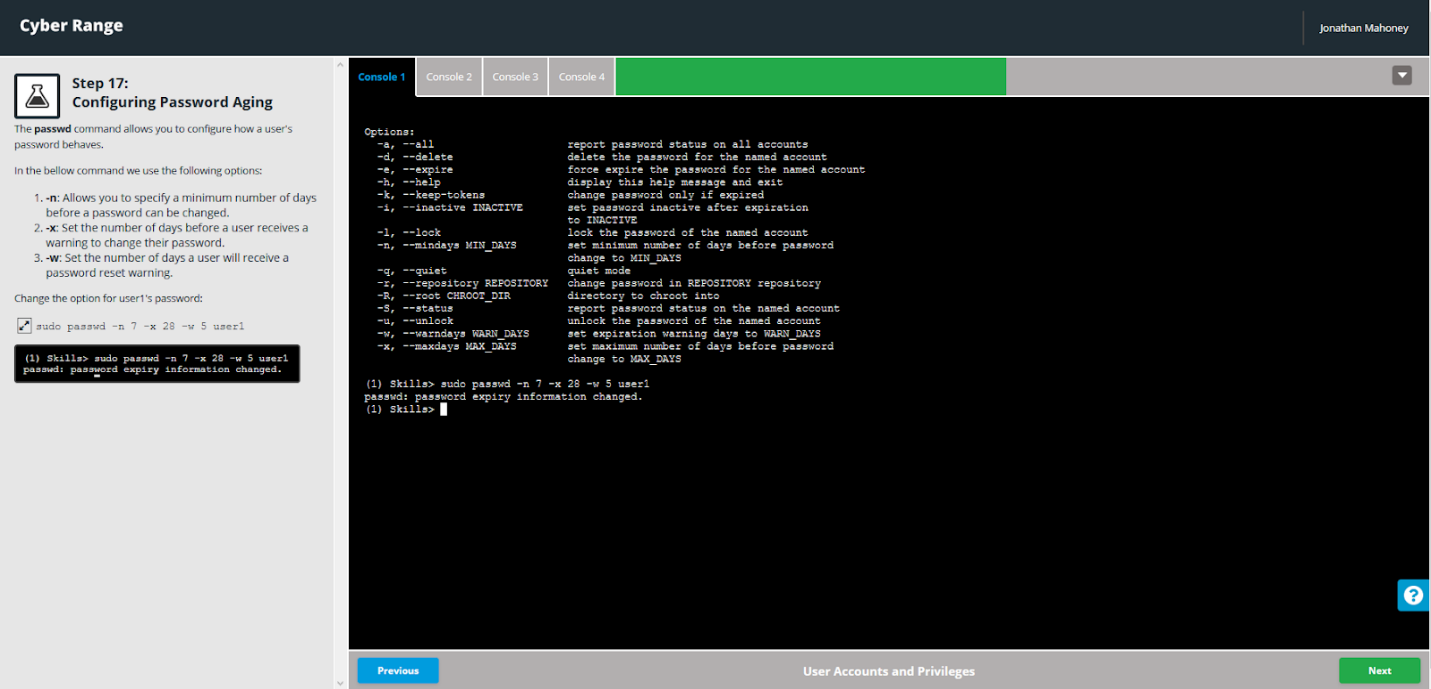
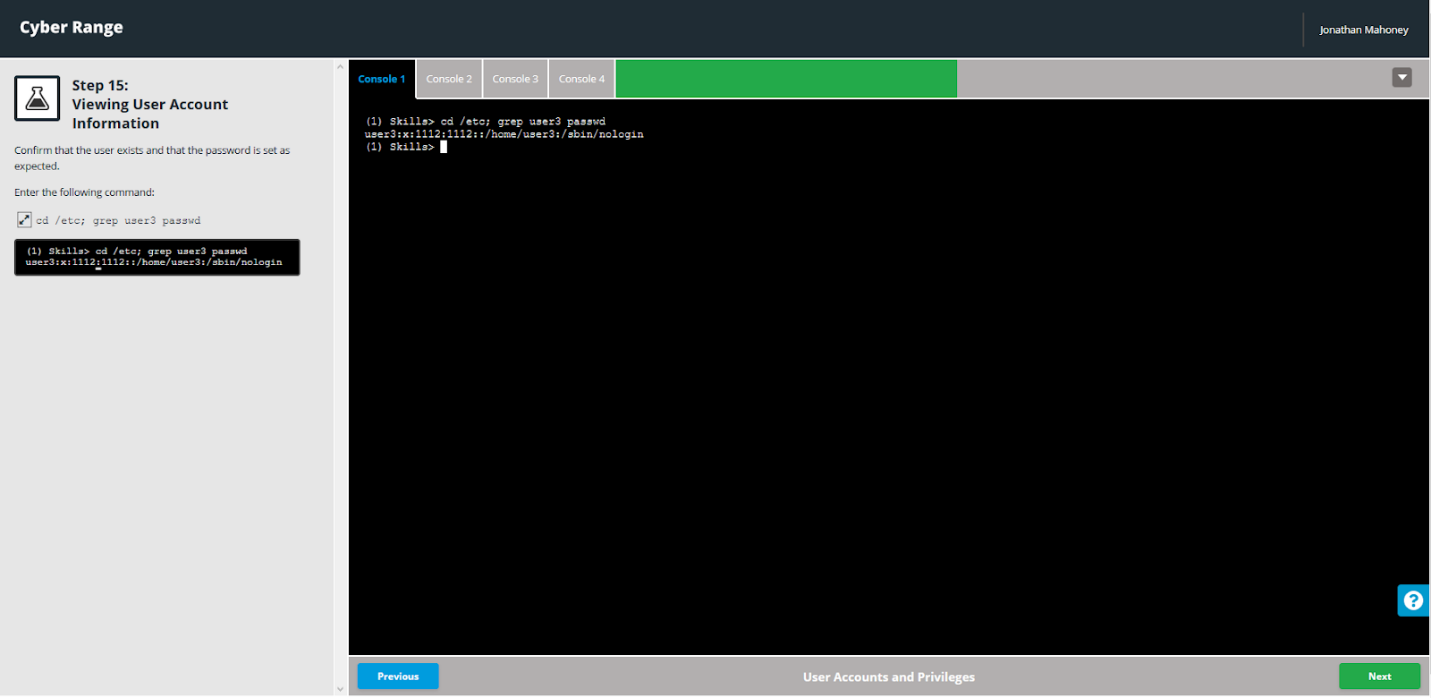
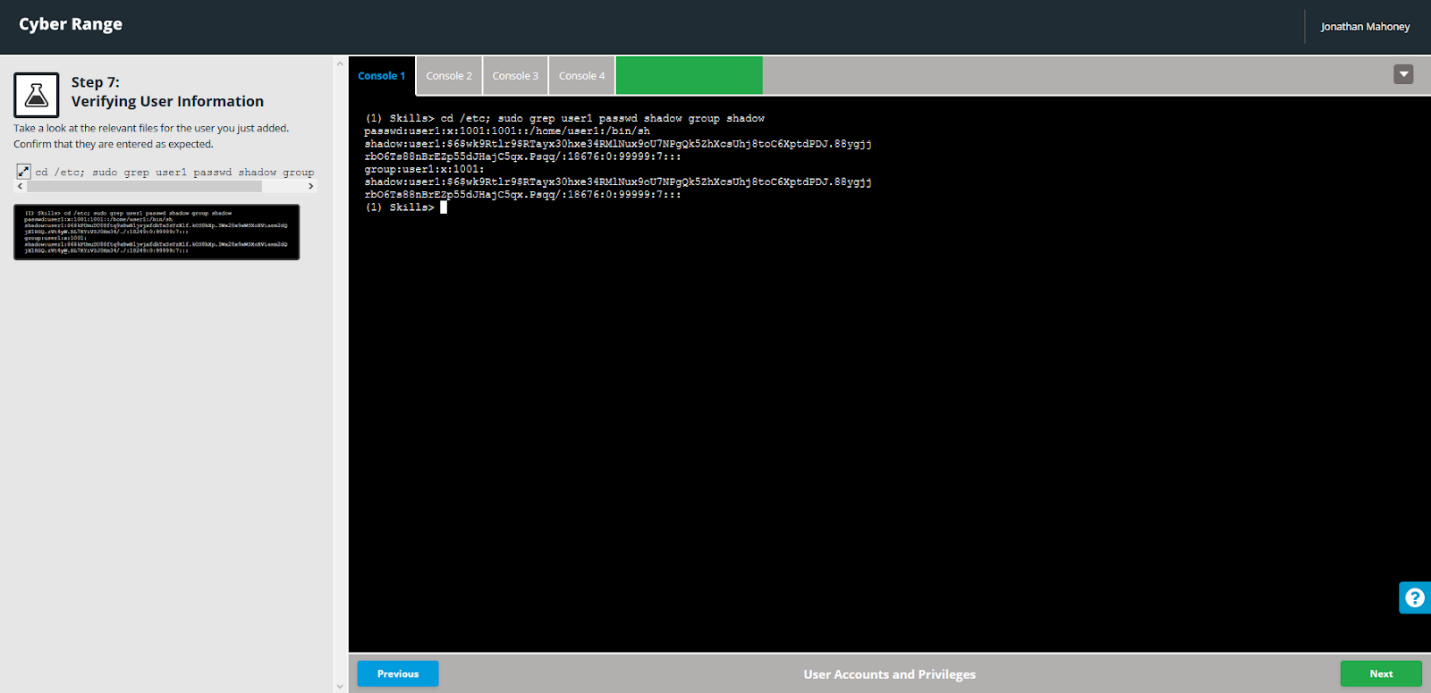
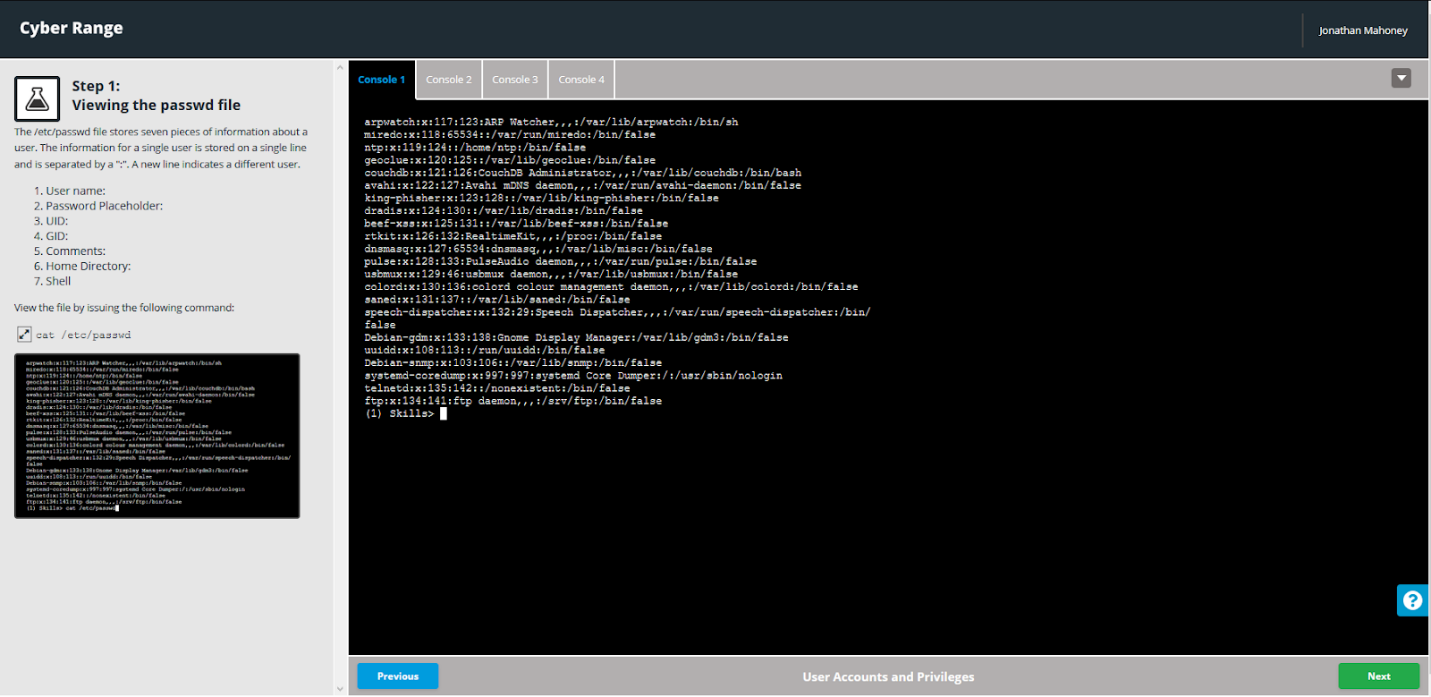
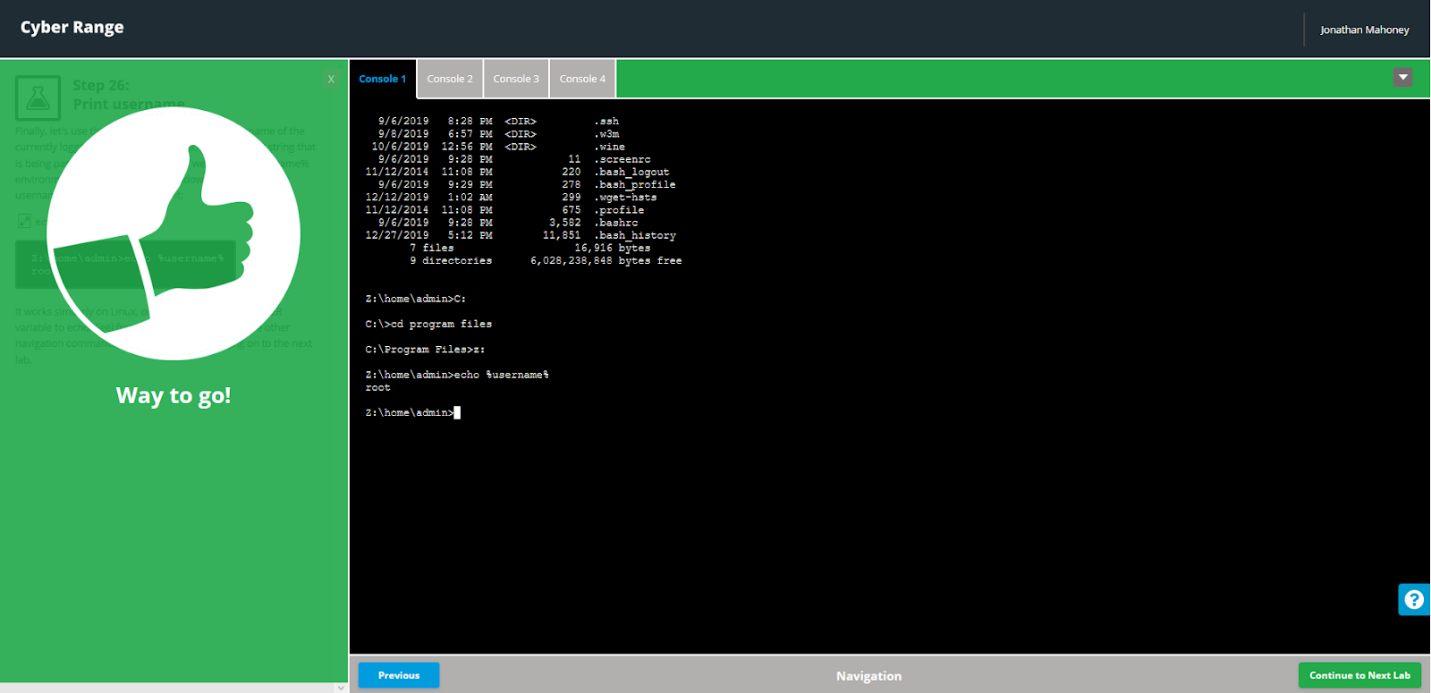
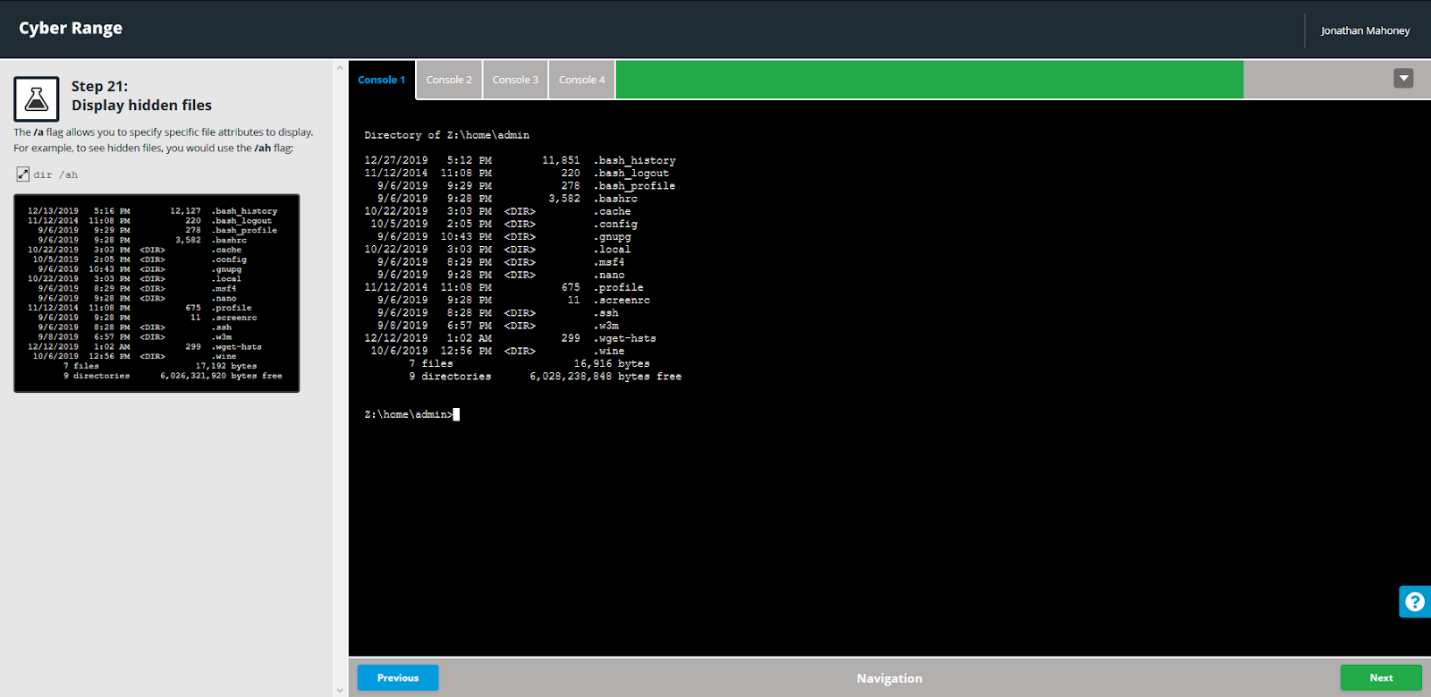
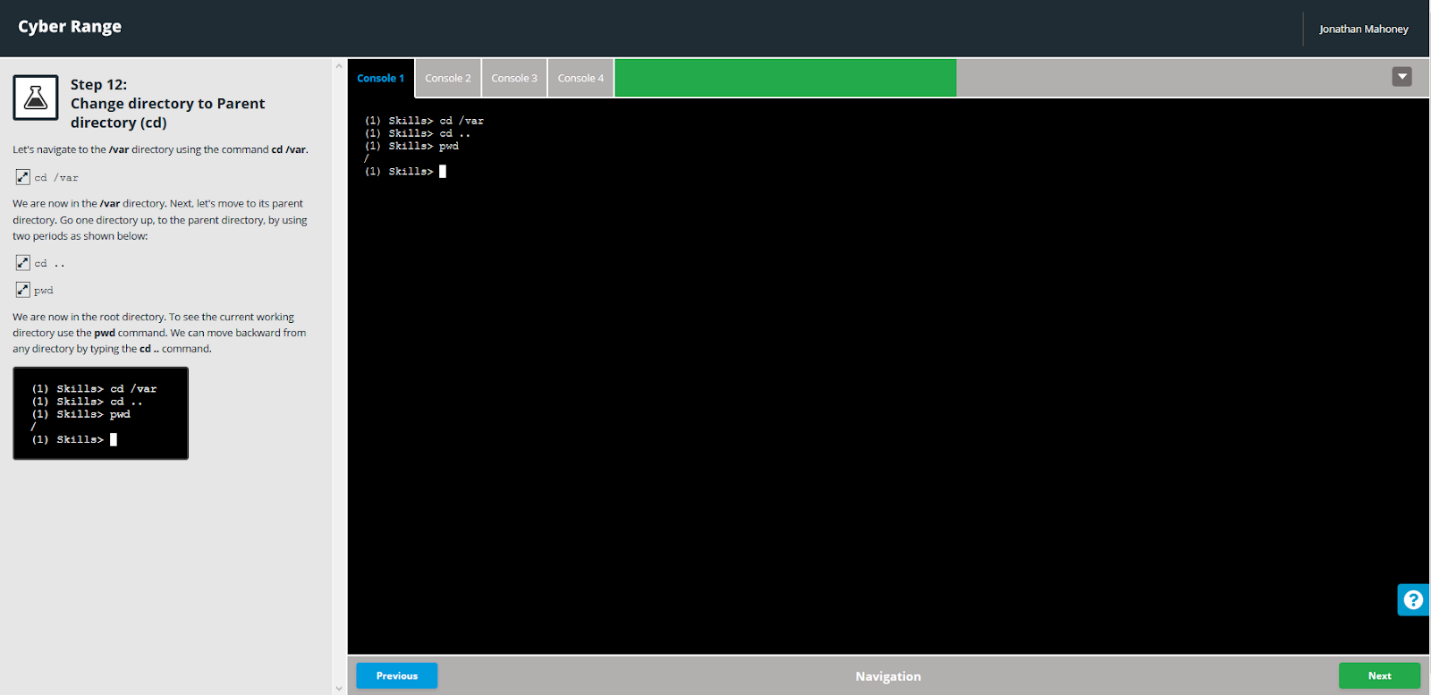
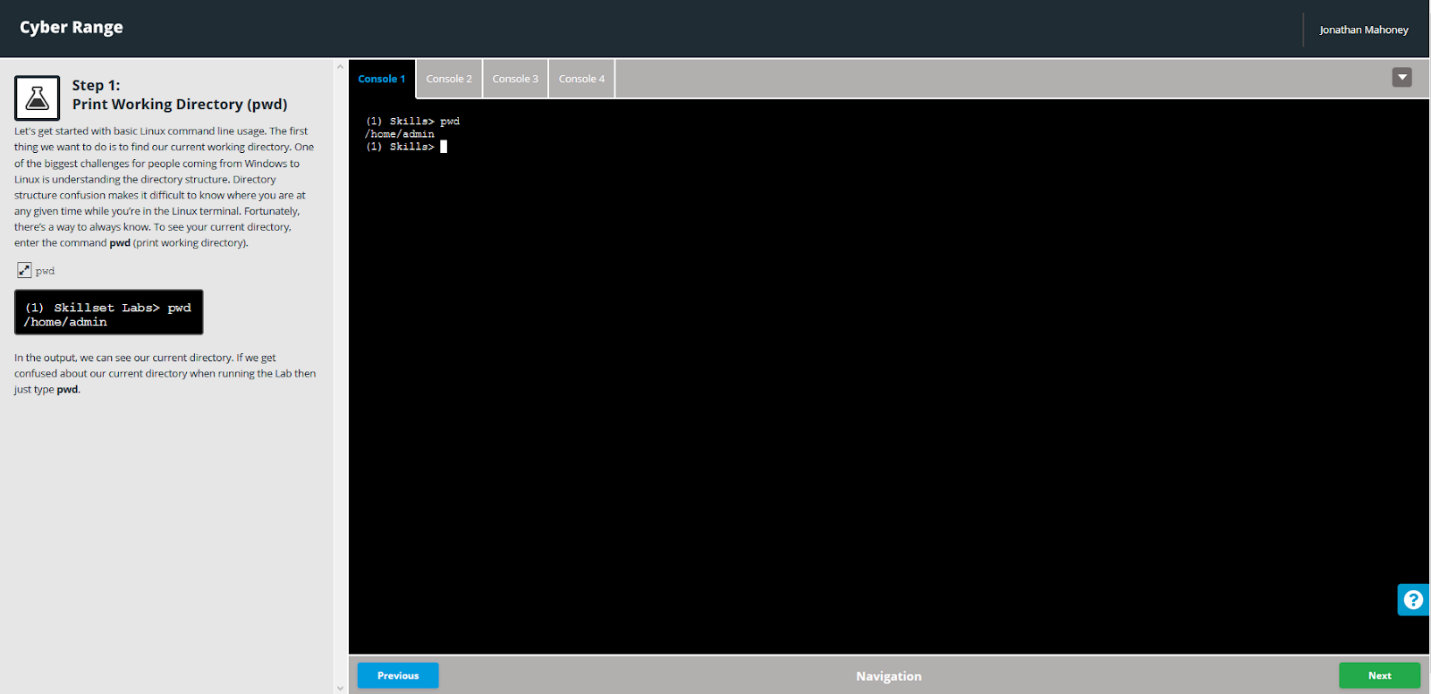
The third lab, “Port Scanning”, describes the process of searching for open networking service endpoints called ports. Port scanning is done using the nmap command which can be pointed at a target host. While port scanning is often a malicious activity, the lab provides information on how to identify when a port scan is occurring by viewing the activity in a separate console. Lastly, the “Basic Networking Utilities” lab involves basic networking commands used in Linux and Windows along with different ways to modify them. These commands are traceroute, netstat, nmap, TCPdump, curl, and wget. Traceroute and netstat are used to track the travel of packets and provide network statistics respectively. Curl and wget are similar as they both allow for transferring data from a server, the only difference is that wget allows for recursive retrieval of the data. TCPdump is used to analyze packets as they are transferred in and out of a network.

# Solution

While working through the lab assignment, I ran into a few issues and I had trouble determining if I was doing something incorrectly or the cyber range was not working properly. For instance, in the networking basics lab, I made it to the last step and input the command as it described but I was stuck. This happened in another lab and when this occurred, I would restart the lab and it often worked. After the lab environment came back online, I was able to finish the networking basics lab by ensuring I entered each command in the correct console. There were two commands which I copied and pasted to be safe as they contained extended strings of letters and numbers to be sure I would not have to do the lab an additional time.

During my time at Penn State, I have become familiar with many of the commands used in these labs in classes like networking and network security as they were frequently used in our exercises. For instance, in my network security class, we had hands on experience with network troubleshooting as we worked on actual networking devices. For that exercise, we used almost all the commands from the cyber range activity. Additionally, classes that are not directly focused on networking often had labs or activities that involved networking commands like the ones we used.

# Screenshots



This is where I got stuck in my first attempt

