Docker Home lab – Cyber Security Home lab

u- steve (and or kevin)

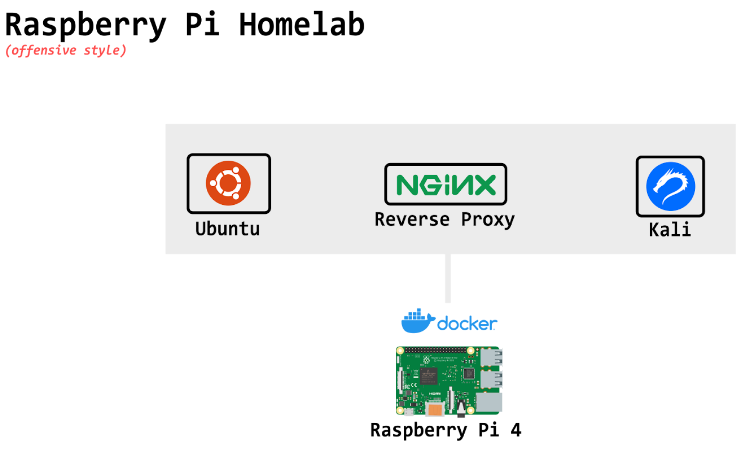
p- towson2025

192.168.3.94 (Or your RaspberryPi’s static IP address)

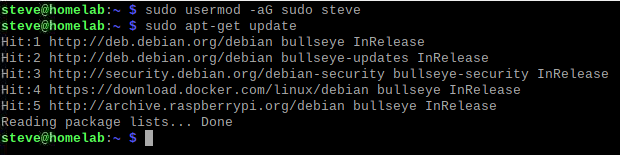
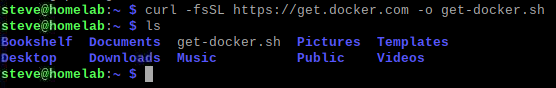
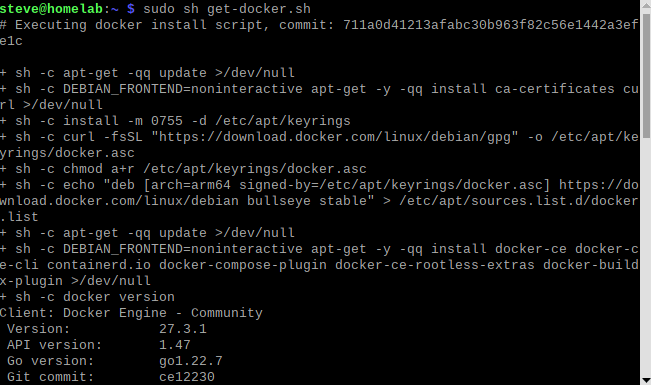
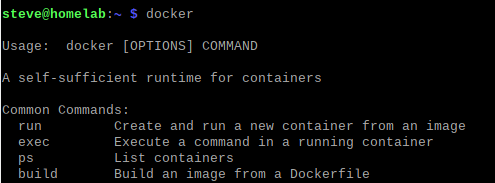
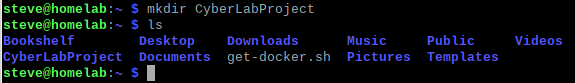
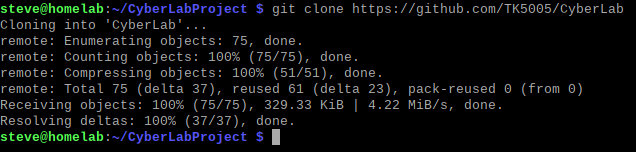
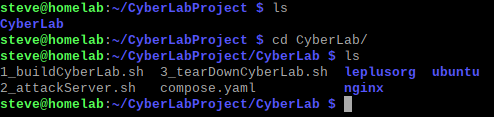
ssh steve@”your Pi’s static ip address” -p 22

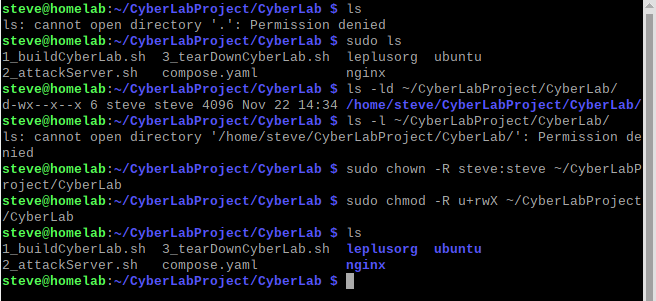
Raspberry Pi 4 Model B Rev 1.1

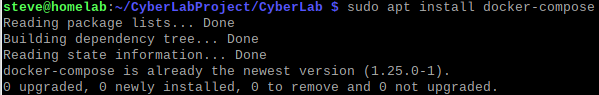
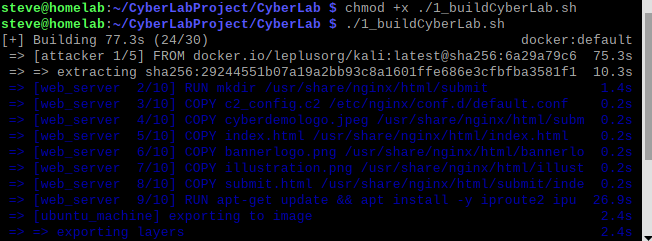
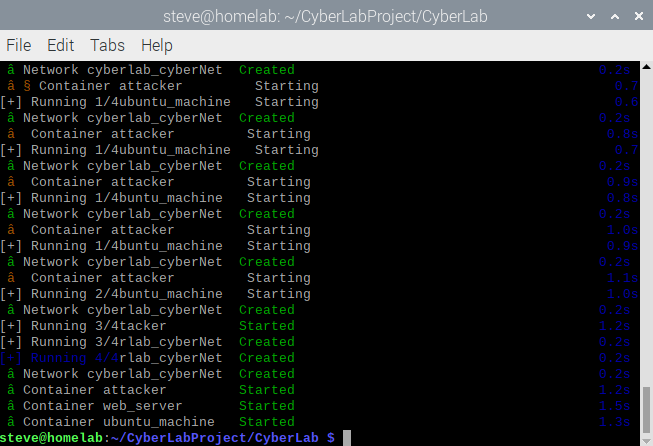
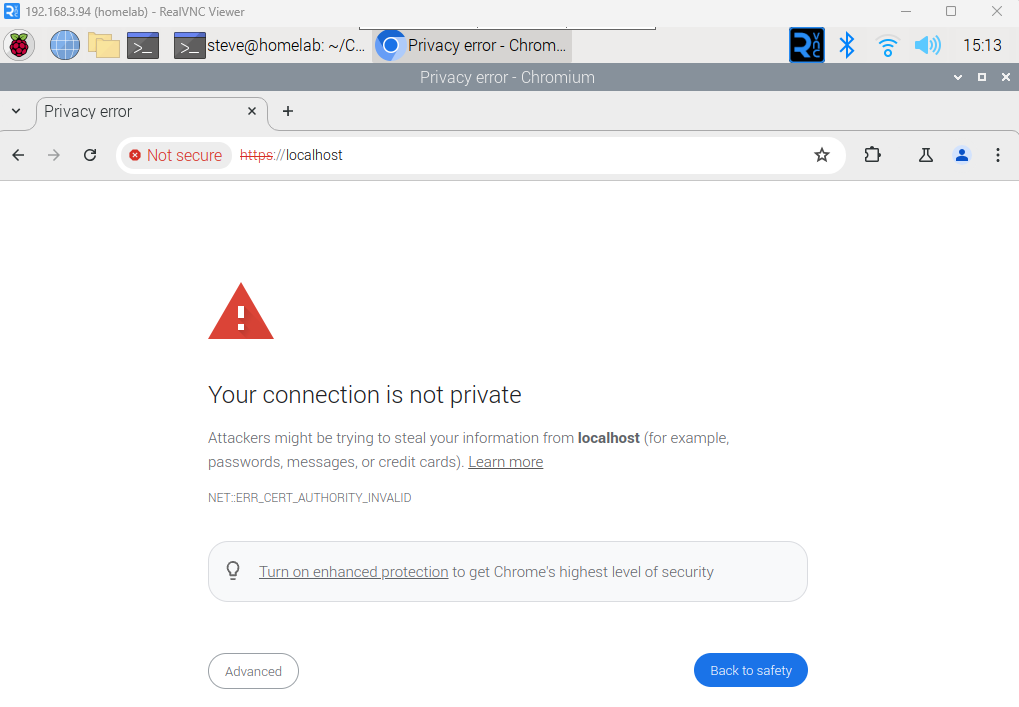
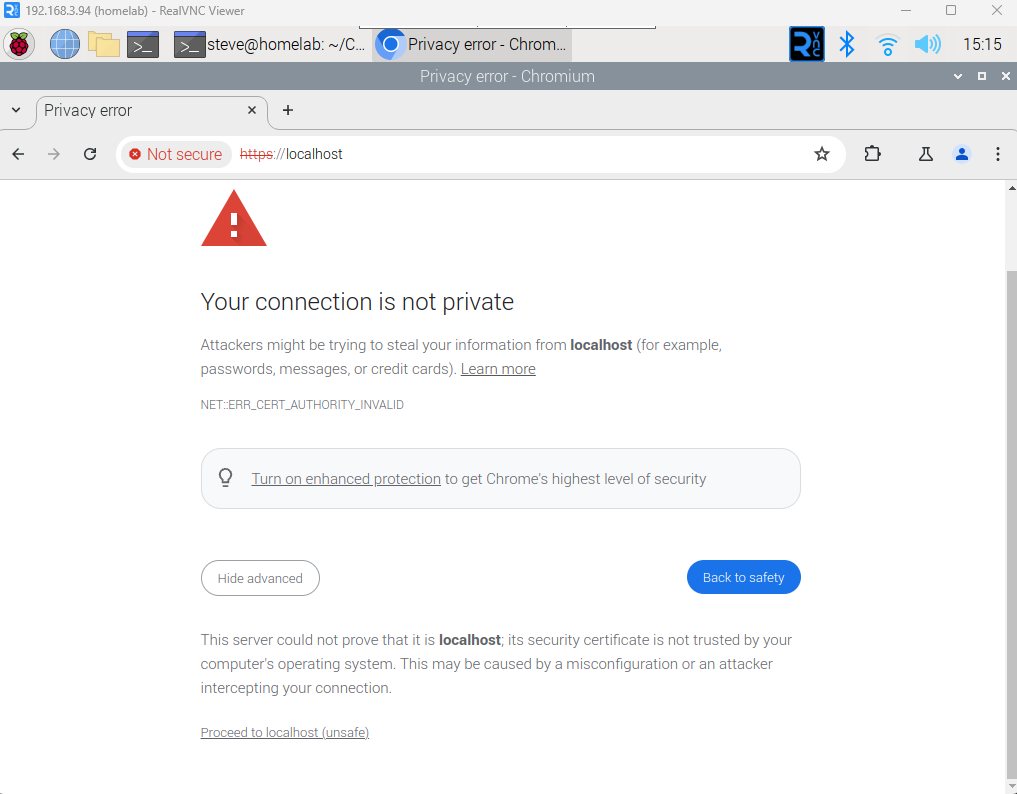
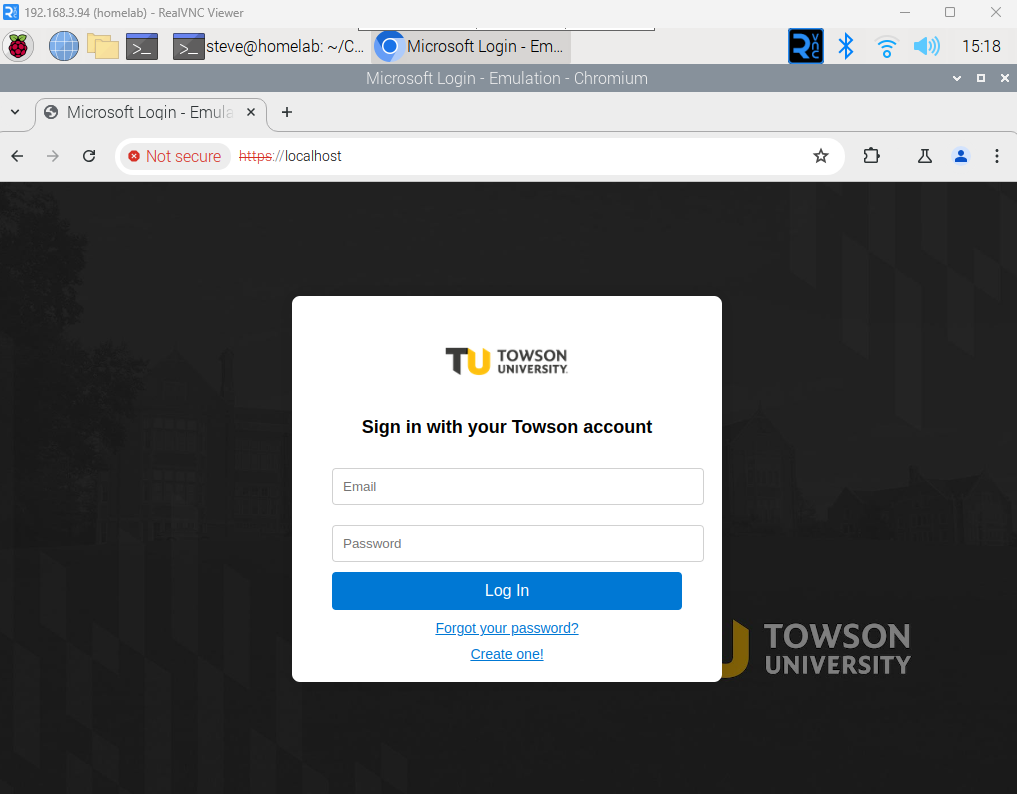
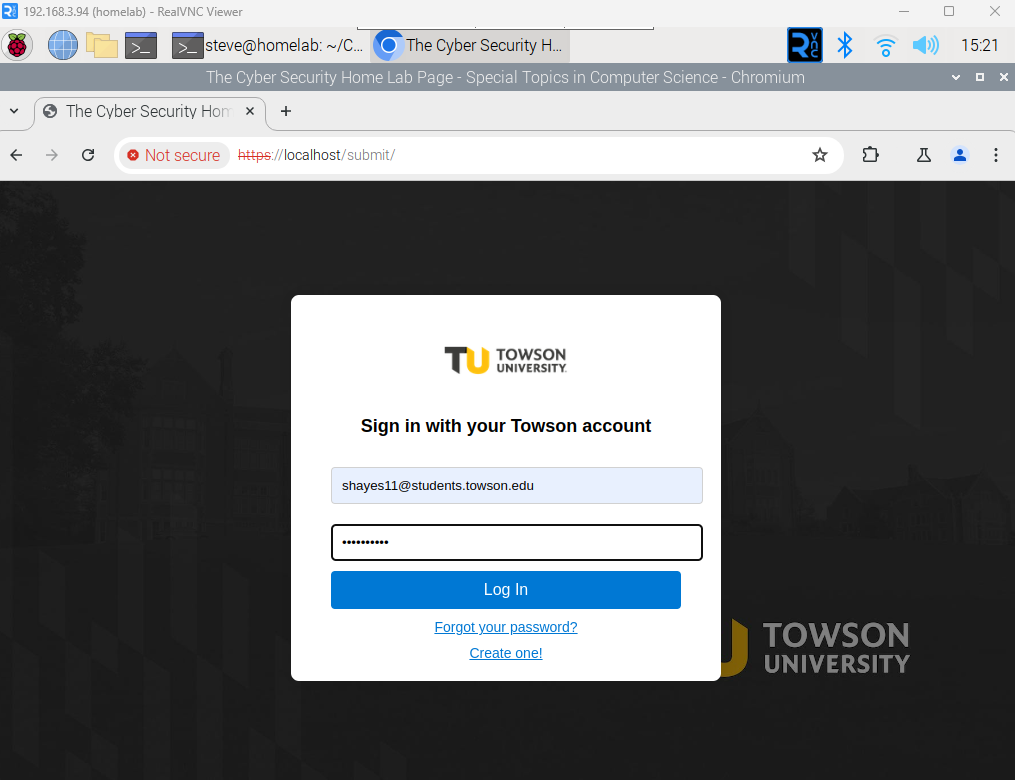
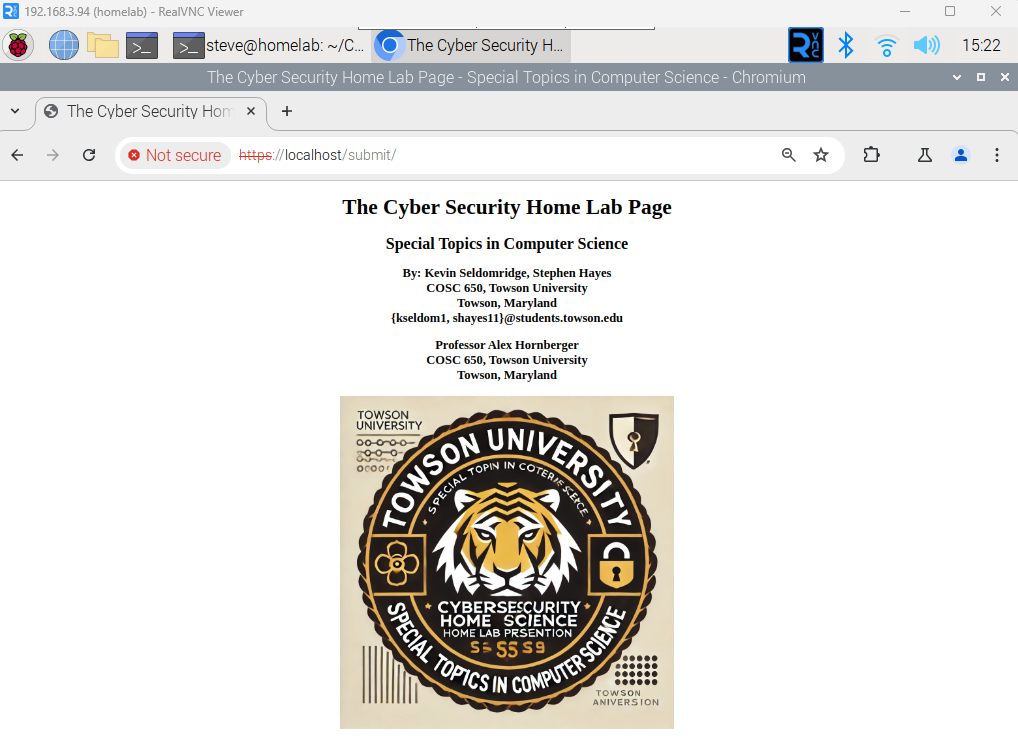
Recommended to add your user name to the Sudoers group or the Pi using:  
 ‘sudo usermod -aG sudo steve’



Version: 20231012~bullseye

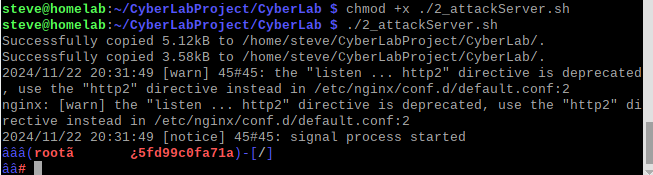
1. Open Terminal and Update the Pi: sudo apt-get update  
   
2. Install docker from convenience script: curl -fsSL <https://get.docker.com> -o get-docker.sh
3. Type: ls  
   
4. Type: sudo sh get-docker.sh  
   
5. Type: docker <- This will verify that docker is successfully installed.   
   
6. Create a project folder on your desktop: mkdir CyberLabProject
7. Type: ls <- To confirm the folder was created.  
   
8. Change the directory to the project folder you just created: cd CyberLabProject/  
   
9. Do a pull of the CyberLab software from github.com: <https://github.com/TK5005/CyberLab>  
   
10. Type: ls <- To verify the download.
11. Type: cd CyberLab <- Changes the working directory to the CyberLab folder we just downloaded.
12. Type ls: <- to verify the files have been downloaded.  
    
13. If you get an error after typing ‘ls’, see if you can run ls as sudo ‘sudo ls’. If you can, you will need to change the permissions of the newly downloaded “CyberLab’ folder by running the following commands: ls -ld ~/CyberLabProject/CyberLab and ls -l ~/CyberLabProject/CyberLab
14. Then change Ownership of the folder: sudo chown -R steve:steve ~/CyberLabProject/CyberLab
15. Then modify permissions of the folder: sudo chmod -R u+rwX ~/CyberLabProject/CyberLab

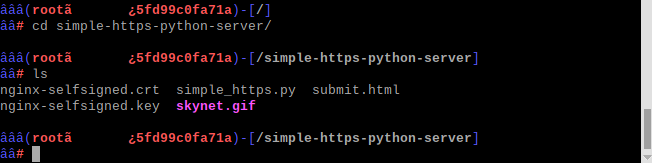
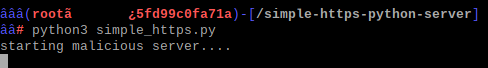
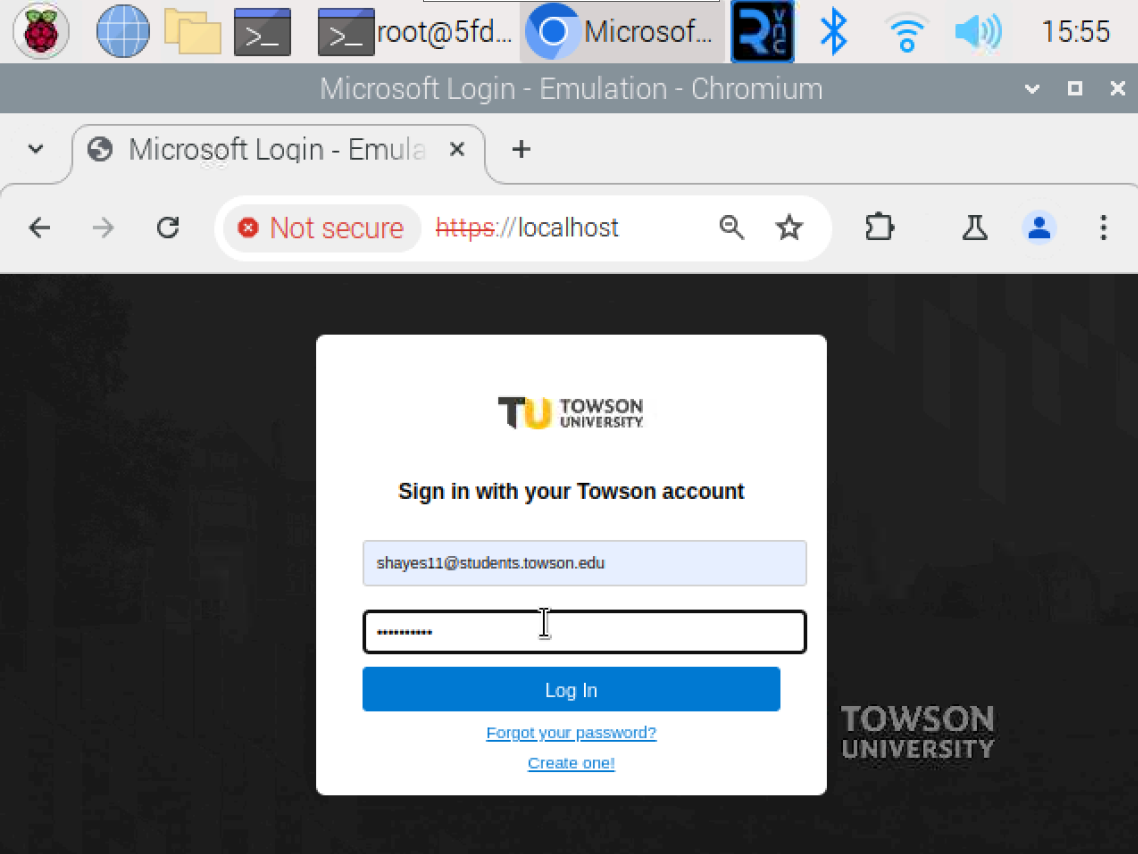
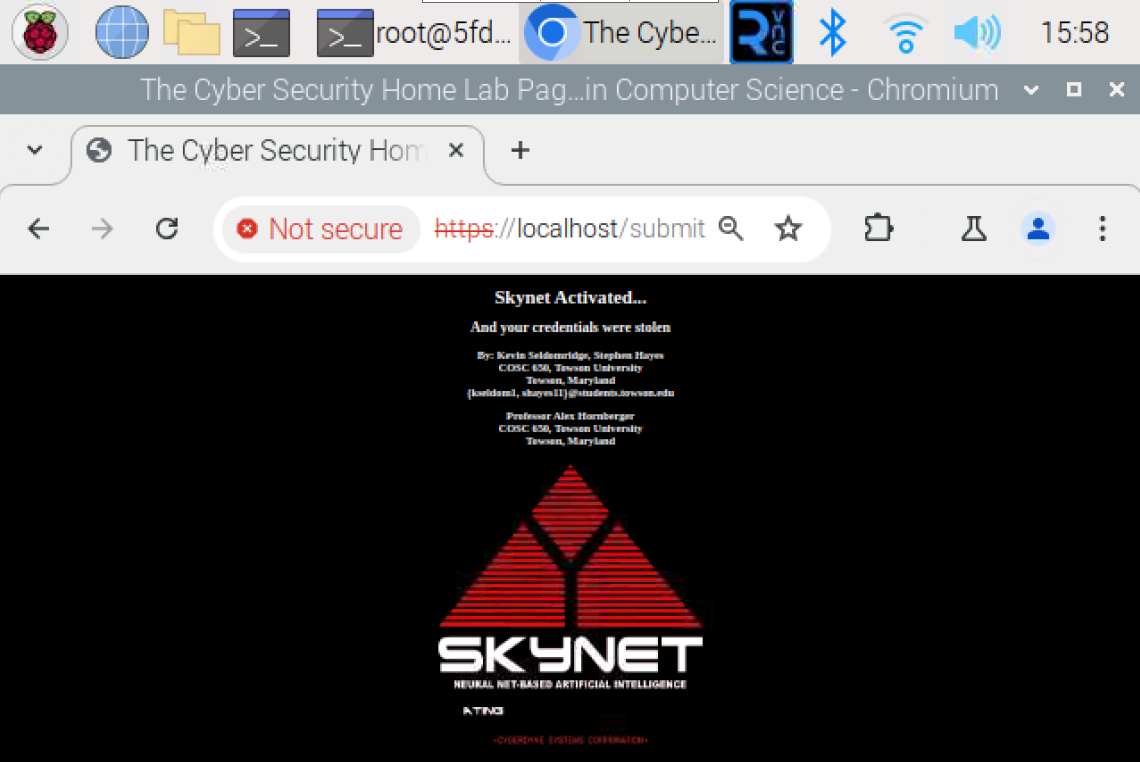
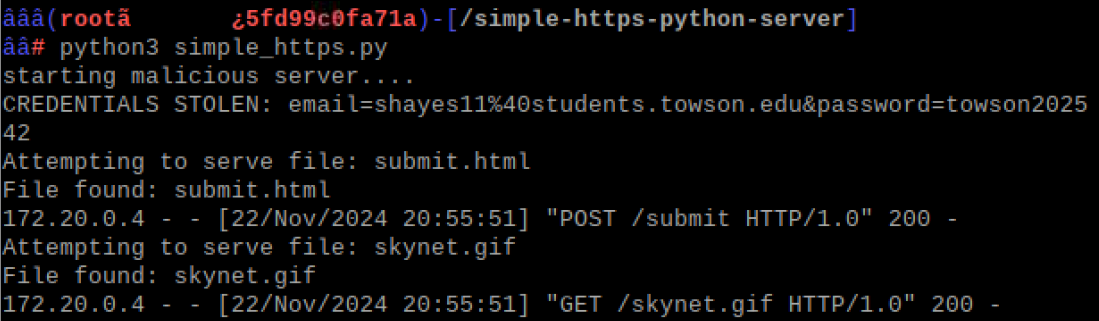
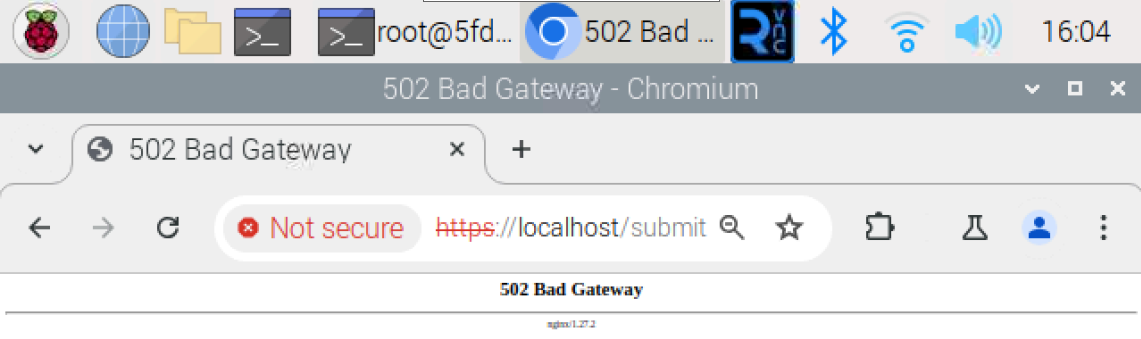
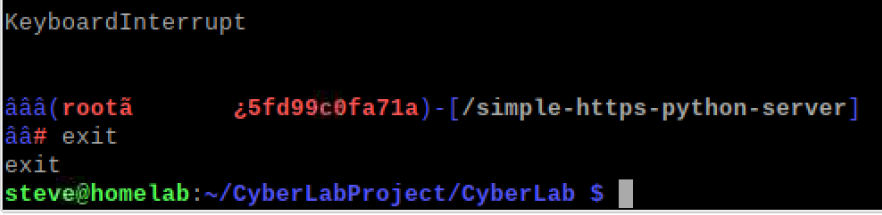
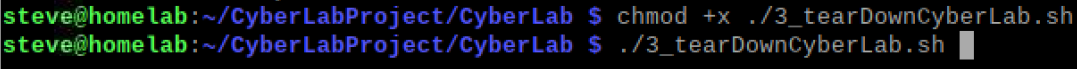


1. You should now be able to ‘ls’ with no errors.
2. Install docker-compose: sudo apt install docker-compose  
   
3. Make the script executable: chmod +x ./1\_buildCyberLab.sh
4. Build the CyberLab by running script #1. Type: ./1\_buildCyberLab.sh  
   
5. After 3-5 minutes, the download of the docker images and associated files will now be complete.  
   
6. Once the script has completed, open your web browser and visit: <https://localhost>  
   
7. Click on ‘Advanced’ in the bottom left of the screen.
8. Click on ‘Proceed to localhost (unsafe)’  
   
9. Welcome to the Towson University Blackboard Login Page:  
   
10. Login with your email and password: [shayes11@students.towson.edu](mailto:shayes11@students.towson.edu) & towson2025  
    
11. Welcome to “The Cyber Security Home Lab Page”  
    

Everything looks great and feels safe…… Now lets run the hack and steal some credentials.

1. Back in the terminal, run the 2nd script after making it executable:  
   chmod +x ./2\_attackServer.sh

./2\_attackServer.sh  


1. Type ‘ls’ to verify the AttackServer is live and then Change the Directory to the ‘simple-https-python-server’ and Type ‘ls’ again to verify the contents of the new directory.  
   
2. Type: python3 simple\_https.py to activate the attacker server.  
   
3. The Malicious Server is now running. Go back to the web browser, and revisit the “<https://localhost>” website and login again.  
   
4. Congratulations. You have successfully activated SkyNet and your login credentials have been stolen.  
   
5. Go back to the terminal, and you will see that the Attack Server has captured your Credentials.  
   
6. To stop the Attack Server, Type Ctrl + C.
7. This command will issue a Keyboard Interrupt to the Attack Server, and it will stop running.   
   
8. When finished grabbing the users credentials, exit out of the attacker server. Type: exit  
   
9. Now that the fun is over, lets clean up the lab.
10. Run the third script after making it executable: chmod +x ./3\_tearDownCyberLab.sh  
    ./3\_tearDownCyberLab.sh  
    
11. With the teardown complete. This concludes the Lab/Demo. Thank you!!  
    