ISIN 335 –Penetration Testing Project 1
Instructor: Gerald Emerick

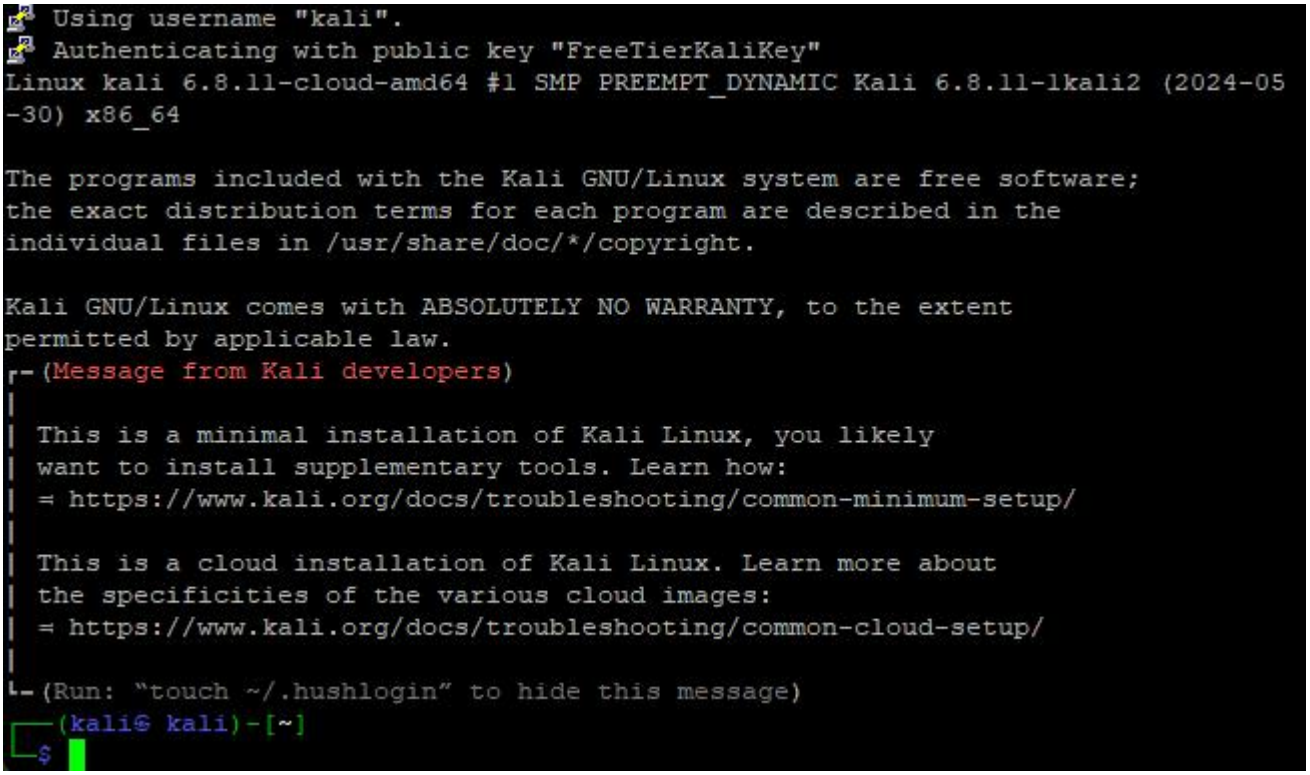
Penetration Testing Project 1

Use your AWS Free Tier account for this assignment. In this assignment you will create a small pen testing lab environment with your AWS Free Tier.

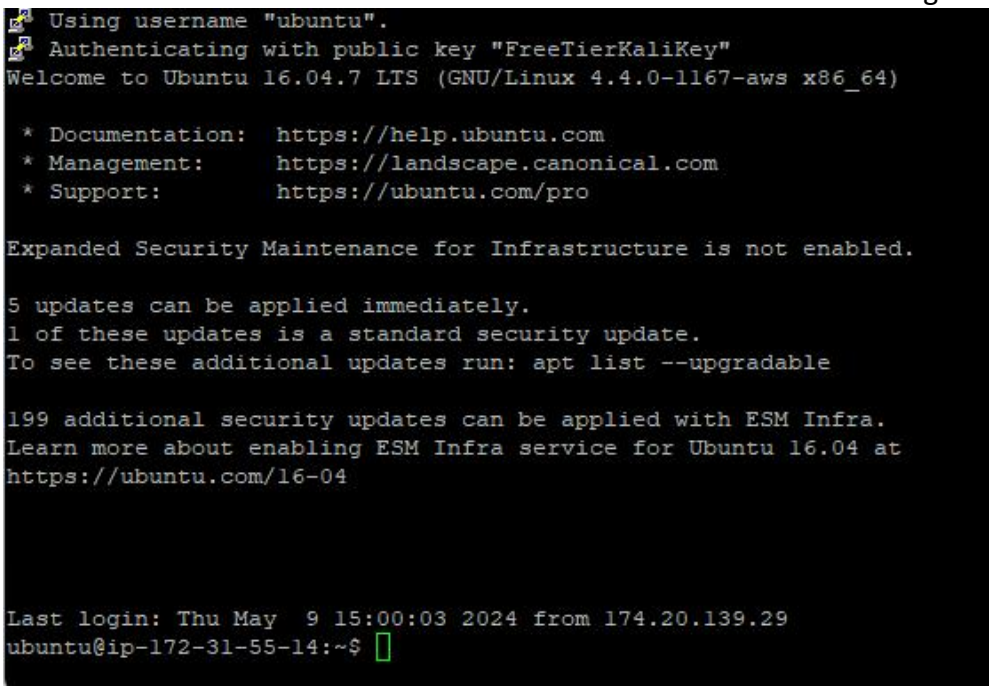
1. Your AWS Educate account does not have the necessary permissions required for the Penetration Testing Projects. Create a new AWS Free Tier Account if you haven't done so already. Most services within this account will be free for 12 months. After 12 months you will be charged for services. You should setup billing alerts to avoid charges and strongly consider disabling the account after the class is complete. There are videos regarding AWS billing within Blackboard.

2. Use the AWS Marketplace to create a new Kali Linux EC2 Instance.

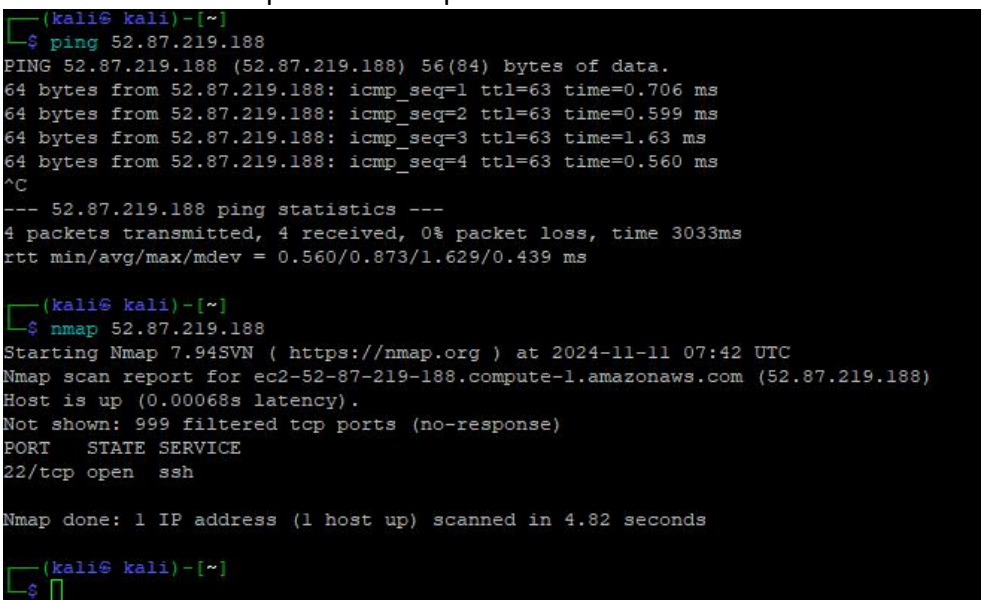
    a. Use default and free tier settings.
    b. Make sure to store the .pem key file in safe, yet accessible location on your local machine c. You may need to change the permission of the pem file to 400 on Linux systems or remove "Everyone" permission on Windows.
    d. Configure necessary AWS Security Groups to allow SSH.
    e. Start the instance
    f. Establish an SSH connection to the Kali EC2 instance using the assigned IP and the user "kali"
    g. Stop the instance when you are not using it.



3. Use the AWS Market Place to create a new Ubuntu 16.04 LTS EC2 Instance.
    a. Use default and free tier settings.
    b. Make sure to store the .pem key file in safe, yet accessible location on your local machine. You can use the same key pair and .pem file that was used for the Kali instance.
    c. You may need to change the permission of the pem file to 400 on Linux systems or remove "Everyone" permission on Windows.
    d. Configure necessary AWS Security Groups to allow SSH.
    e. Start the instance
    f. Establish an SSH connection to the Ubuntu instance using the assigned IP and the user ubuntu.



4. From the Kali instance, run an nmap scan against the Ubuntu instance. If nmap is not found, you may need to update your package list and install nmap.
    a. sudo apt update
    b. sudo apt install nmap



5. Stop all EC2 instances.

6. Write a brief synopsis of the assignment including key learning items, any challenges that you encountered, and questions that you may have.

   This first penetration testing assignment went smoothly for me with only minor issues. This assignment mainly involves launching a Kali instance and a Ubuntu instance within EC2, using PuTTY to form an SSH connection to each of them, then finally doing an nmap scan from the Kali instance to the Ubuntu instance. The only issue that I encountered was that nmap was not working initially on the Ubuntu instance. I spent a few minutes looking into it, mainly within the Security Group configurations, then added ICMP from anywhere IPv4 to ping it. I believe my initial attempts failed due to the Ubuntu instance not being fully launched before I started my nmap scan. I do not have any questions at this time, and I found the lab to be fun.

Deliverables / What to Submit

1. A single PDF with screenshots of all required steps clearly labeled.
2. A synopsis of the assignment.