

## 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.

```
Using username "kali".
Authenticating with public key "FreeTierKaliKey"
Linux kali 6.8.11-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
-- (Message from Kali developers)
|
| This is a minimal installation of Kali Linux, you likely
| want to install supplementary tools. Learn how:
| = https://www.kali.org/docs/troubleshooting/common-minimum-setup/
|
| This is a cloud installation of Kali Linux. Learn more about
| the specificities of the various cloud images:
| = https://www.kali.org/docs/troubleshooting/common-cloud-setup/
|
-- (Run: "touch ~/.hushlogin" to hide this message)
(kali@kali)-[~]
$
```

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.

```
Using username "ubuntu".
Authenticating with public key "FreeTierKaliKey"
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-1167-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

5 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

199 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 16.04 at
https://ubuntu.com/16-04

Last login: Thu May  9 15:00:03 2024 from 174.20.139.29
ubuntu@ip-172-31-55-14:~$
```

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

```
(kali@kali)-[~]
$ ping 52.87.219.188
PING 52.87.219.188 (52.87.219.188) 56(84) bytes of data:
64 bytes from 52.87.219.188: icmp_seq=1 ttl=63 time=0.706 ms
64 bytes from 52.87.219.188: icmp_seq=2 ttl=63 time=0.599 ms
64 bytes from 52.87.219.188: icmp_seq=3 ttl=63 time=1.63 ms
64 bytes from 52.87.219.188: icmp_seq=4 ttl=63 time=0.560 ms
^C
--- 52.87.219.188 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.560/0.873/1.629/0.439 ms

(kali@kali)-[~]
$ nmap 52.87.219.188
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 07:42 UTC
Nmap scan report for ec2-52-87-219-188.compute-1.amazonaws.com (52.87.219.188)
Host is up (0.00068s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds

(kali@kali)-[~]
$
```

## 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.