**Lab #0**

**Lab Space Set Up Using AWS Educate & the AWS Cloud**

# Background

We will be using the Amazon Web Services (AWS) cloud instead of our Virtual CyberSecurity Lab (VCSL) to create the virtual environments for the labs in this course. The purpose of this lab is to set up the AWS environment and to familiarize yourself with its capabilities. You should have received an email regarding your AWS Educate account.

# Objectives

* Become familiar with using virtual lab environments via AWS Educate & the AWS Cloud
* Brush up on networking topics needed for this course including:
* sockets
* client/server model
* tunnels/proxies

# Resources

* AWS Educate Environment
* Lab #0 AWS creation link https://console.aws.amazon.com/cloudformation/home? region=us-east-1#/stacks/new?stackName=CEG-3400-new&templateURL=https:%2F

%2Fwsu-cecs-cf-templates.s3.us-east-2.amazonaws.com%2Fcourse-templates %2Fceg3400.yml

**Access to Resources**

# Tasks (20) Task 1 - Setup

* You should have received an email with your AWS Educate information
* If you haven't receive it, check your spam folders
* If you still don't have the email, let Mr. Saunders know right away
* Once you receive your AWS Educate information, complete the AWS Educate Registration
* Install Python 2.7, recommend using Anaconda python

(https://www.anaconda.com/distribution/)

* Windows 10 Setup
* Install Windows Subsystem for Linux (WSL)

(https://docs.microsoft.com/en-us/windows/wsl/install-win10)

* Install Ubuntu 18.04 LTS from the Windows store
* Launch Ubuntu 18.04 LTS Bash and create login account (username/password)
* Install MobaXterm Home Edition (https://mobaxterm.mobatek.net/download.html)
* **Launch MobaXterm, start a WSL-Ubuntu session & provide screenshot**

<https://graspingtech.com/ubuntu-desktop-18.04-virtual-machine-macos-qemu/>

Graphical user interface, application

Description automatically generated

# (30) Task 2 - Provision the AWS Lab Environment

**You must have registered for your AWS Educate account in order to accomplish the rest of this task**

* Sign in to AWS educate (https://www.awseducate.com/signin/SiteLogin)
* Click on `My Classrooms` in the AWSEducate banner at the top of the page
* Click the blue `Go to classroom` button for *Introduction to Cyber Security*
* Click ‘continue’
* Click the light blue `AWS Console` button
* This will launch the AWS console (may require two clicks if you were already signed in to AWS with your personal account)
* Your username in the top right should look something like this:

`vocstartsoft/user236529=lastname.number@wright.edu`

* Generate an SSH key pair so that you can sign in to your virtual machines once they are provisioned
* Select the EC2 service from the AWS console
* At the top of the center area you should see a list of all Resources you have available - right now they should all be 0
* Click on 0 Key Pairs
* From here you should see no existing SSH key pairs
* Click on the `Create Key Pair` orange button located at the top right portion of the screen
* Chose a name for your key pair
* Select *pem* for the File format
* Click 'Create key pair' orange button located at the bottom center portion of the screen
* This will create a public/private key pair
* It will store the public key in AWS
* It will download the private key to your local machine (probably in your Downloads folder)
* **Do not lose this private key** - you can't access your virtual environments in AWS without it
* VIP NOTE: You can recover if you do lose your private key, but it requires deleting all of your VMs using CloudFormation, creating a new key pair using EC2, and reprovisioning your VMs using CloudFormatoin.

* Once you have created your SSH key, go back up to the Resources section of this document and click on the Lab #0 AWS creation link that is listed there. Note:

Disregard the *404 page not found* error if you get one

* This will take you to another AWS service called CloudFormation (AWS CF). You will use CloudFormation to actually provision the AWS virtual environment for Lab #0.
* There are several screens required to provision the cloud stack. All fields in all screens will automatically be filled, except for the SSH key box on the 2nd screen
* Select the SSH key you just created from the drop down menu provided then click thru the rest of the screens and click *create stack* to finalize creation of your lab space
* Return to the EC2 service to view the additional resources that have been created
* **Take a screen shot showing all of the resources provisioned for this lab**

Graphical user interface

Description automatically generated

* Click on Running Instances to see information about the servers created as a part of the cloud formation template. **Take a screen shot showing your running instances.** Graphical user interface, application

  Description automatically generated
* Retrieve the Elastic IP of the Ubuntu instances by selecting it and looking at the information in the description below it.
* **Take a screen shot showing your Elastic IP for each VM.**

Graphical user interface, text, application, email

Description automatically generated

* Now select your Windows Server 2019 instance, select Actions  Security  Get Windows Password
* You will need this password to remote desktop connect to your Windows VM
* Note this may take 15-20 minutes
* Once the password is generated, follow the instructions to decrypt it. Once decrypted, save that password somewhere as you will need it everytime you remote desktop connect to your windows VM
* **Write down the Elastic IP addresses (and the user name and password for Windows) for each of your running instances. Remember these IP addresses are only good for this instance of the VMs. If you have to delete your VMs and reprovision them you will get different Elastic IP addresses.**
* Private IP address
* 107.22.249.217
* User name
* Administrator
* Password
* CzhK7FH&py&.yzW7G8iuY$aX==lZTN(I

# (20) Task 3 - Connecting to the AWS environment

* Using MobaXterm, start a WSL-Ubuntu session and perform the following actions:
* Find and copy the AWS private SSH key to your home directory
* Remember: your private SSH key was automatically downloaded to your local machine as part of creating it on AWS
* You need to find the key (probably in your Downloads file) and copy it to your home directory in your WSL-Ubuntu session in MobaXterm
* Note the contents WSL-Ubuntu is your C:\ directory on your local machine **cp /mnt/c/Users/yourusername/Downloads/private-key-name.pem ./**
* Make the key only readable by your user (chmod)
* **chmod 600** **private-key-name.pem**
* To connect to linux VMs use SSH
* *ssh -i /path/to/private/key ubuntu@ElasticIP*
* (replace /path/to/private/key & ElasticIP with your information)
* To connect to windows VMs use Remote Desktop
* Select the Windows 10 Start icon & type *Remote Desktop Connection*
* Enter the Elastic IP address for your Windows 10 VM
* User Name =
* Password =
* **Take a screen shot showing connection to each of your virtual machines on the AWS server**Text

  Description automatically generated
* **I have a mac and have been having trouble with this. Should’ve started earlier**

# Deliverables

 This Lab #0 Assignment Document, with your name at the top of the first page, with all necessary information showing accomplishment of each task, posted to the appropriate Pilot Lab #0 dropbox NLT 9:30 a.m. Tues, 26 Jan 2021.

# Acknowledgement

Contents of this lab derived from lab project originally created by Matt Kijowski. Portions of Matt's lab projected were derived from [Black Hat Python: Python Programming for Hackers and Pentesters, by Justin eitz](https://nostarch.com/blackhatpython).

Ubuntu 2

ssh -i /Users/AlyanaBarrera/desktop/ssh/ceg3400-aws-vm.pem ubuntu@23.21.21.42

Windows

ssh -i /Users/AlyanaBarrera/desktop/ssh/ceg3400-aws-vm.pem ubuntu@107.22.249.217

Ubuntu 1

ssh -i /Users/AlyanaBarrera/desktop/ssh/ceg3400-aws-vm.pem ubuntu@34.195.122.147