Michele Novack Abugosh

Project : Linux Server Configuration

This project call to setup and configure a Linux (Ubuntu) web server using Amazon AWS. The server must be secure and serve and application previously developed in the course (Catalog) . Prepare it to host your web application to include installing updates, securing it from attacks.

Table of Contents:

|  |  |
| --- | --- |
| **Name** | **Value** |
| **IP Address** | 3.84.147.247 |
| **SSH Port** | **2200** |
| **Username** | **grader** |
| **URL of Applicaiton** |  |

ec2-3-84-147-247.compute-1.amazonaws.com (3.84.147.247)

To connect to EC2 instance you need the Lightsail\_key.rsa ( supplied separately in the submit process)

|  |
| --- |
| ssh -I lightsail\_key.rsa ubuntu@3.84.147.247 |

Launch your EC2 Terminal

Check for updates:

|  |
| --- |
| sudo apt-get update  sudo apt-get upgrade  sudo apt-get dist-upgrade |

Create New User: Create a new user named grader and grant this user sudo access permissions

|  |
| --- |
| sudo adduser grader |

Followed the instructions in command line and added a secure password. After that I granted (sudo) permission to the grader

|  |
| --- |
| Sudo nano /etc/sudoers.d/grader  grader ALL-(ALL:ALL)ALL - close and save |

Then Log in temporarily into the grader :

|  |
| --- |
| Sudo -su grader |

Securing the Server:

Added a Key based login to new grader user:

|  |
| --- |
| su - grader |

Then added directory .ssh

|  |
| --- |
| mkdir .ssh |

Added file .ssh/authorized\_keys and copy the public key contents of the Lightsail\_key to authorized\_keys and finally restrict permission to the .shh and authorized\_key

|  |
| --- |
| Chmod 700 .ssh  Chmod 644 .ssh/authorized\_keys |

Only allow Key Based Authentication

To force key based authentication edit the /etc/ssh/sshd\_config file

|  |
| --- |
| sudo nano /etc/ssh/sshd\_config |

Update the following field and then save

|  |
| --- |
| PasswordAuthentication yes |

TO :

|  |  |
| --- | --- |
| **PasswordAuthentication NO** |  |

Then, restart the ssh service

|  |
| --- |
| Sudo service ssh restart |

The SSH is hosted on non-default port - Change the Default to host on Port 2200 - edit the /etc/ssh/sshd\_config file

|  |
| --- |
| Port 22 |

TO

|  |
| --- |
| Port 2200 |

The Restart the Service:

|  |
| --- |
| Sudo service ssh restart |

Configure the Firewall (UFW)

To set up the UFE , first check the firewall status:

|  |
| --- |
| Sudo ufw status |

Then, DENY incoming Traffic

|  |
| --- |
| Sudo ufw default deny incoming |

Then ALLOW outgoing traffic

|  |
| --- |
| Sudo ufw allow outgoing |

Establish the rules for SSH (port 2200) –

|  |
| --- |
| Sudo ufw allow 2200/tcp |

For HTTP (port 80)

|  |
| --- |
| Sudo ufw allow www |

And for NTP (port 123)

|  |
| --- |
| Sudo ufw allow ntp |

Then ENABLE UFW

|  |
| --- |
| Sudo ufw enable |