# Section 1:

# Task 1.1: Bare-Metal Server Setup and Configuration

1. Install the latest stable version of Ubuntu Server:

* Download the Ubuntu Server ISO from the official website:

A screenshot of a computer

Description automatically generated

* Create a bootable USB drive using tools like Rufus

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

2. Configure SSH access with public key authentication:

* Generate an SSH key pair on your local machine using ssh-keygen.

A computer screen shot of a black screen

Description automatically generated

* Copy the public key to the server using ssh-copy-id or manually by adding

it to the ~/.ssh/authorized\_keys file.

A screenshot of a computer program

Description automatically generated

* Disable password-based SSH login by editing the /etc/ssh/sshd\_config

file (PasswordAuthentication no).



A screenshot of a computer screen

Description automatically generated

3. Set up basic firewall rules using ufw to allow SSH and web traffic:

* Enable ufw (Uncomplicated Firewall)

Update system

A screen shot of a computer program

Description automatically generated

Install ufw:

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Check process status:

A black background with white text

Description automatically generated

Enable process:



Allow SSH traffic:

A black screen with white text

Description automatically generated

Allow HTTP/HTTPS traffic for web server:

A screenshot of a computer program

Description automatically generated

Check the status.

A screenshot of a computer

Description automatically generated

# Task 1.2: Managed Server Upgrade

Update Packages:

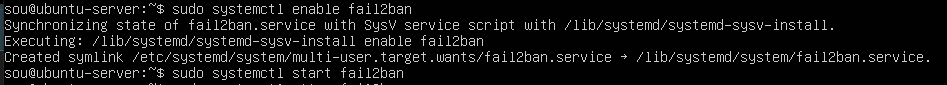
A screen shot of a computer program

Description automatically generated

Install and Configure Fail2ban:

A screen shot of a computer

Description automatically generated









A screen shot of a computer

Description automatically generated

The process wasn’t running, according the to the logs, it’s not finding the log file for ssh. I tracked the log file for ssh which is /var/log/fail2ban.log, and modified it in the config file

A screen shot of a computer

Description automatically generated

Now it runs properly

A computer screen shot of a black screen

Description automatically generated

* Verify the Upgrade

A black background with white text

Description automatically generated

* Set Up Automatic Security Updates

A black screen with white text

Description automatically generated

A computer screen with white text

Description automatically generated

Configuriting it

Verify config file



A screen shot of a computer code

Description automatically generated

Enable automatic updates



Update packages everyday and remove unsued packages automaticall

A green text on a black background

Description automatically generated

Dry run to try config

A screenshot of a computer program

Description automatically generated

Apply changes

A screen shot of a computer

Description automatically generated

* Configure SELinux or AppArmor

Install packages

A black screen with white text

Description automatically generated

Enable selinux

A screenshot of a computer

Description automatically generated

Reboot to apply changes



Check status

A screen shot of a computer

Description automatically generated

Set enforcing mode to override other rules



A screenshot of a computer error

Description automatically generated

List selinux Booleans

A screen shot of a computer program

Description automatically generated