**Continue Setup: Ubuntu**

1. **Install updates - “sudo apt-get update”**

A screenshot of a computer

Description automatically generated

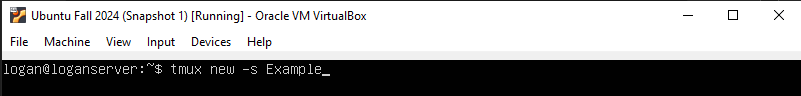
* To continue setting up our Ubuntu server, power on the VM and run this command to update the server. **Apt** is short for ‘Advance Packaging Tool’, which is used for installing, updating, and deleting packages in all Debian based Linux systems, like Ubuntu. The system will prompt for the admin password before executing the command.

1. **Install Tmux – “sudo apt install tmux” & “tmux new -s Example”**

A screenshot of a computer

Description automatically generated

* **What is Tmux?** Tmux is an abbreviation for ‘Terminal Multiplexer’. This tool allows you to create multiple terminals out of a single session. It gives the ability to run multiple programs with a single terminal, or connection, to the system.



A screenshot of a computer

Description automatically generated

* To open a new Tmux session, you can enter ‘Tmux’ into the command line and a session will begin. The command I used here applies a name to the new session, rather than a default name chosen by the server.

A screenshot of a computer

Description automatically generated

* Use the commands below to create new windows and navigate through them when using Tmux. The command ‘tmux ls’ shows how many active windows are open. At the bottom of the window highlighted in green, we can see the 3 windows that are opened with Tmux. The one with the asterisk (0:bash\*) is the current window displayed.

|  |  |
| --- | --- |
| Ctrl + B, C | Creates a new window. |
| Ctrl + B, N | Switch to the next window. |
| Ctrl + B, P | Switch to the previous window. |
| Ctrl + B, D | Detach from the session (session continues running in the background). |
| Ctrl + B, W | List all windows and switch between them. |
| Ctrl + B, X | Kill the current pane or window. |

1. **Install EMACS – “sudo apt install emacs”** **& “emacs SedLab”**

A screenshot of a computer

Description automatically generated

* **What is EMACS?** Emacs is a text editing tool on Linux distros that is worth learning because it can significantly improve your efficiency. It can be used to edit scripts and text files without having to use a text editor outside of the terminal session. The installation and output of the command is lengthy, be sure to select ‘Yes’ to confirm when it prompts you during the installation.

A screenshot of a computer

Description automatically generated

* The command **‘emacs SedLab’** will open the contents of the SedLab file. Here we can make manual edits to the text as needed. When finished, press ***CTRL + X*** followed by ***CTRL + C* to** exit the emacs editing tool.

1. **Install Fail2ban – “sudo apt install fail2ban”**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* **What is Fail2ban?** Fail2ban is a useful security tool that automatically blocks IP Addresses that fail to authenticate credentials to the server. For example, if a hacker was trying to get into a server, they might use a brute force attack which tried endless account credentials in attempt to gain access to the server. If Fail2ban recognizes a suspicious number of attempted logins from the same IP Address, it will then block the IP.

A screenshot of a computer screen

Description automatically generated

* Once installed, open the configuration file for Fail2ban, the location of this config file is /etc/fail2ban/jail.conf. Copy the jail.conf fle and save it as jail.local in the same directory, this will prevent the config settings from being overwritten during updates. Use emacs, or your preferred text editor, to open this file and edit the settings. In the config file, there are a few variables we can adjust like ‘bantime’ which is the number of seconds the IP Address is banned for if the system suspects repeated attacks. I changed this to 1800 seconds (on 14OCT24) to give more time between lockouts for suspected hackers. When you are finished making changes, press ***CTRL + X*** and then ***CTRL + S****,**if using emacs****,*** to exit and save the config.

A screenshot of a computer

Description automatically generated

* To set this up for SSH connections, scroll down in the Jail.local file to ‘SSH servers’, add the line **enabled = true** to activate this jail. I also changed the ‘**maxretry’** variable to 3 to block the IP Address after 3 attempted logins. Date changed – 14OCT24. When you are finished making changes, press ***CTRL + X*** and then ***CTRL + S****,**if using emacs****,*** to exit and save the config.

A screenshot of a computer error

Description automatically generatedA computer screen with white text

Description automatically generated

To start the Fail2ban service, enter the command **“sudo systemctl start fail2ban”.** And then enable it by entering **“sudo systemctl enable fail2ban”.** Last, confirm the service is running by running a status check command – **“sudo fail2ban-client status”.**

1. **Testing Fail2ban**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* To test Fail2ban, we need to confirm that SSH is enabled on the server. Command **“sudo ufw allow ssh” first** enables the ability to connect to the server with putty or other remote applications. The command result skipped adding the rule because it is setup already. **“Sudo ufw status”** shows the connections allowed to the server. Once this is set up, we can test Fail2ban.

A computer screen shot of a computer

Description automatically generated

A computer screen with a message

Description automatically generated

To test Fail2ban, download and run Putty ([Link Here](https://www.putty.org/)). Using the IP Address of the server, connection type ‘SSH’, and Port 22, open the terminal session, click ‘Accept’ on the security prompt.

A screenshot of a computer error

Description automatically generated

Try to login with credentials you know are invalid. Going back to the configuration file during the install process, the variable ‘maxretry’ is set to 5, which means after 5 failed login attempts from the same IP Address, Fail2ban will block all activity from that address for 30 minutes as per the ‘bantime’ variable we set during installation.

1. **Install Cowsay – “sudo apt install cowsay”**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* **What is Cowsay?** Cowsay is a program that takes text and outputs it as a spoken text, or bubble quote of an ASCII art Cow. In case you are unfamiliar, ASCII is an art style that uses only computer text and keyboard input to draw a picture. In this case, they drew a cow using mostly back slashes (\) and other special characters. Simply use the command ‘cowsay’ and put in quotes the words you would like to cow sketch to speak! Like previous installs, select yes when prompted to confirm the installation.

1. **Install LolCat – “sudo apt install lolcat”**

A screenshot of a computer

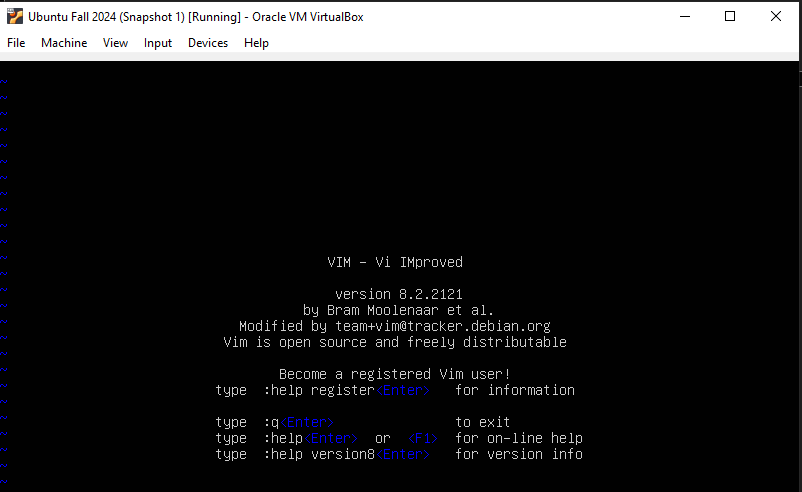
Description automatically generated

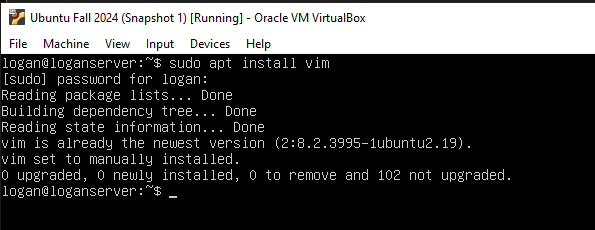
A screenshot of a computer screen

Description automatically generated

* **What is LolCat?** Lolcat is a command line utility that is like the command ‘cat’ (which is abbreviated for concatenate). The difference is the rainbow-colored text that lolcat outputs. In this example, I ran the command ‘lolcat Sedlab’. This displays the contents of the SedLab just like the cat command would, but with rainbow coloring.

1. **Install Vim – “sudo apt install vim”**

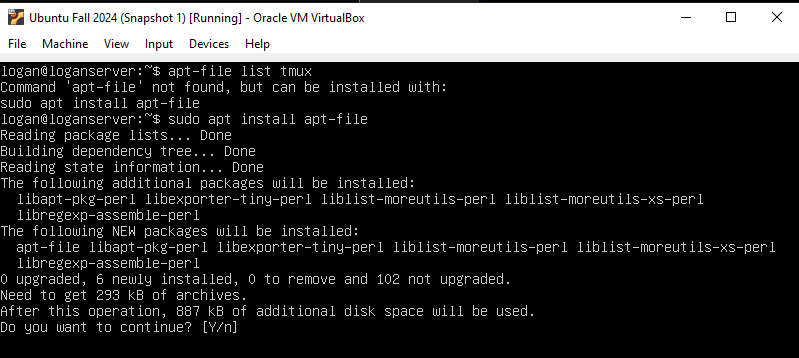




* Vim is the standard text editor used in Linux environments. It is a newer version of VI that added a more user-friendly experience that includes mouse support. We can check if Vim is installed by typing ‘Vim’ into the command line. If it is not installed, run the install command listed above to complete the installation.

1. **Find Files – “apt-file list *FileName*”**

To find the location of a package, or installation, use the **“apt-file list *filename*”** to list all files associated with that package. When I first ran this command, I was prompted to install ‘apt-file’ command before I was able to use it. See below for installation process for ‘apt-file’ package. Enter **“sudo apt-file update”** to begin the installation process.



A screenshot of a computer

Description automatically generated

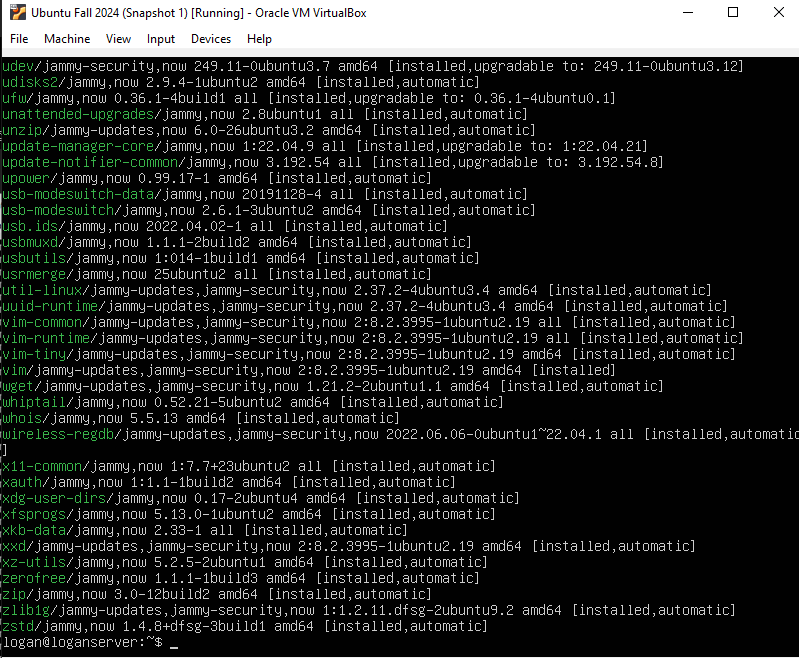
A screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Once installed, I was able to use the command. I tested it using Tmux and Fail2ban as the two filenames I was searching for with **‘apt-file list *TMux’*** and **‘apt-file list *Fail2ban’.***   
  
If we wanted to see everything installed on the server, rather than just one file name, I would use a slightly different command – **“apt-list –-installed”.** See below screenshot for output from this command. I would recommend directing the output of this command to a text file, because the results are lengthy, and it is much easier to sift through as a text file. So, the full command would look like **“apt-list –-installed >> *NewFile*”.**



**Sources:**

**https://help.ubuntu.com/community/Repositories/Ubuntu**

**https://github.com/busyloop/lolcat**

**https://www.aholdengouveia.name/LinuxAdmin/installs.html**