EH LAB WEEK – 1

1. **Creating new user account in Ubuntu using the following command:**
   Syntax: *sudo useradd -m username*

   Eg: *sudo useradd -m prajwal*

   The password for the account was then able to set using the following command:

   Syntax: *sudo passwd username*

   Eg: $sudo passwd prajwal

   It then asks for a password, and later, we can login to our own profile.

2. **Granting superuser privilege to our newly created account. The following commands were used:**
   i. su Student
   //Here, Student is the user with superuser privileges.

   ii. Enter the password of the Student.

   iii. sudo usermod -aG sudo prajwal
   //To add our account to the sudo list.

   iv. Enter the password of the Student.

   v. Either logout from the account or restart for the changes to get applied.

3. Update ubuntu

Go to Synaptic Packet Manager and click on “Mark All Upgrades” to update the system packages, and later click on “Apply All”.

4. To change the command shell to bash, the following command was used:

```
$sudo chsh -s bin/bash username
```

5. Hardening the ubuntu server.

The Ultimate Guide to Harden the Ubuntu Server- Linux Server Hardening - The Sec Master

The above link was referred to.

6. Secure SSH Access

Install openssh:

```
$sudo apt install openssh-client
$sudo apt install openssh-server
```

Check the status of SSH server:

```
$sudo systemctl status sshd
```

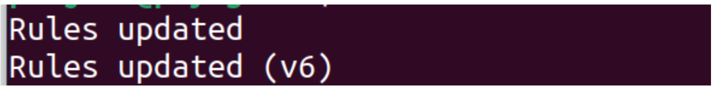
To start the server: sudo systemctl enable sshd

To allow ssh connections:

```
$sudo ufw allow ssh
```

To deny ssh connections:

```
$sudo ufw deny ssh
```



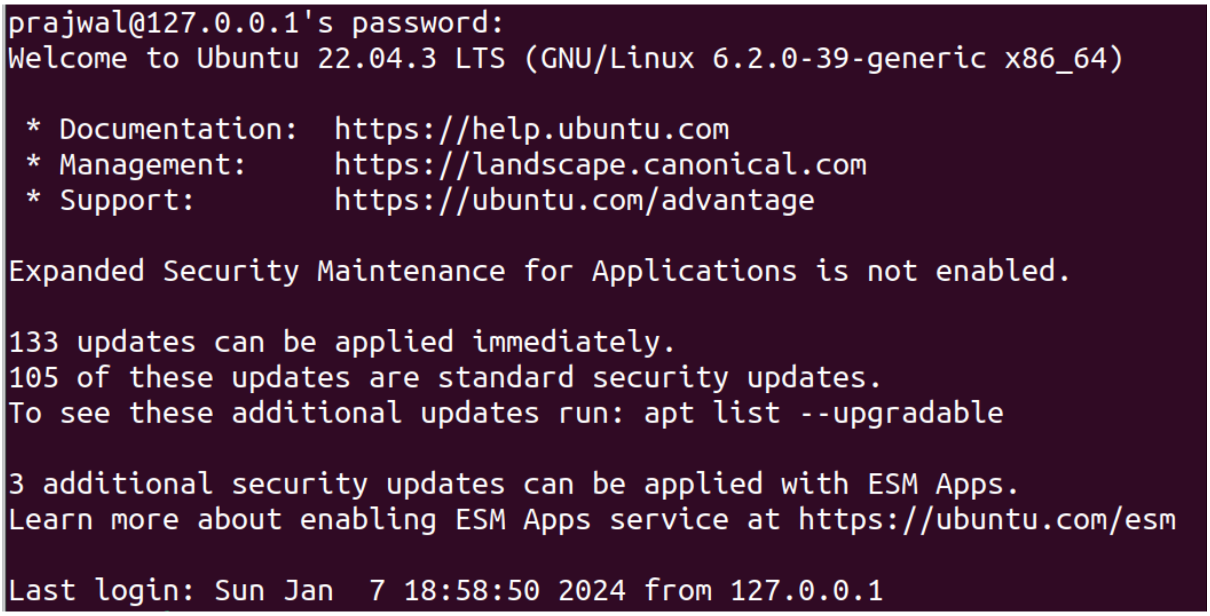
```
Rules updated
Rules updated (v6)
```

Login command:

To access a remote server one can use below command:

```
$ssh -l <username> <ipaddress>
```

```
$ssh -l prajwal 127.0.0.1
```

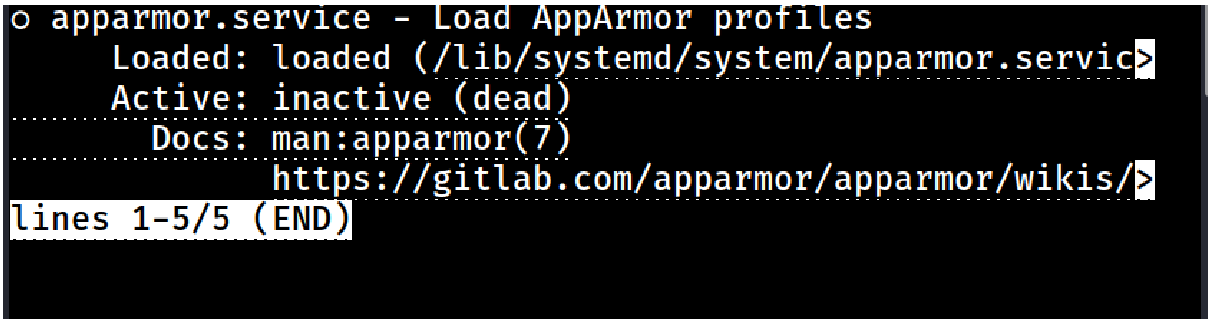


```
prajwal@127.0.0.1's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-39-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

133 updates can be applied immediately.
105 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Sun Jan  7 18:58:50 2024 from 127.0.0.1
```

7. App Armor

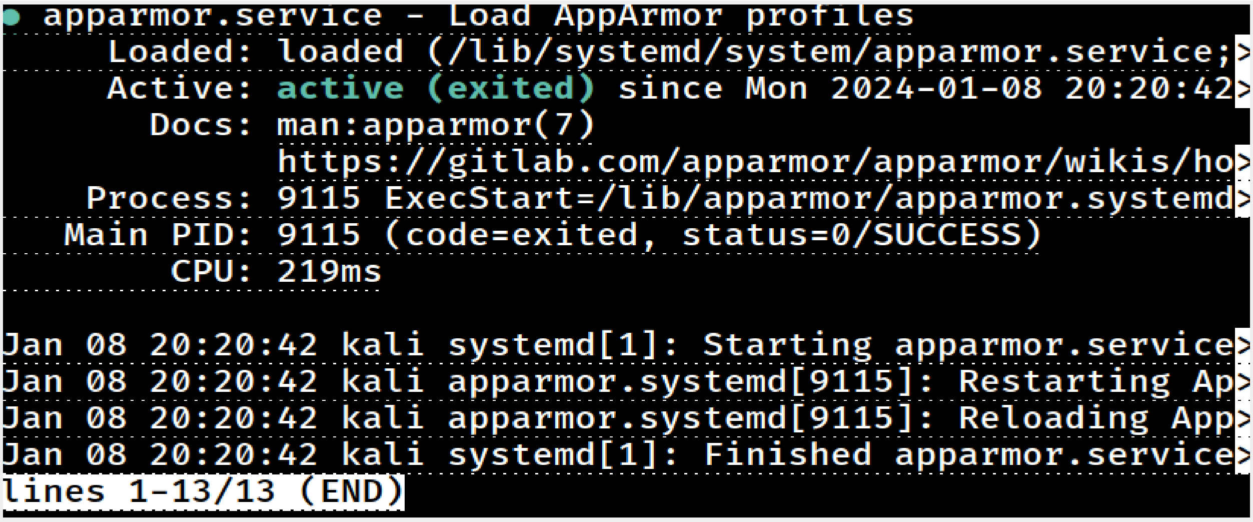
Application Armor is a security module that allows you to set custom restrictions for every application on your system. You can use it to limit everything from network access to read and write permissions. It comes preinstalled on Ubuntu and supports the creation of individual application profiles.

$ sudo systemctl status apparmor



```
○ apparmor.service - Load AppArmor profiles
     Loaded: loaded (/lib/systemd/system/apparmor.servic>
     Active: inactive (dead)
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/>
lines 1-5/5 (END)
```

$ sudo systemctl start apparmor



```
● apparmor.service - Load AppArmor profiles
     Loaded: loaded (/lib/systemd/system/apparmor.service;>
     Active: active (exited) since Mon 2024-01-08 20:20:42>
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/ho>
    Process: 9115 ExecStart=/lib/apparmor/apparmor.systemd>
   Main PID: 9115 (code=exited, status=0/SUCCESS)
        CPU: 219ms

Jan 08 20:20:42 kali systemd[1]: Starting apparmor.service>
Jan 08 20:20:42 kali apparmor.systemd[9115]: Restarting Ap>
Jan 08 20:20:42 kali apparmor.systemd[9115]: Reloading App>
Jan 08 20:20:42 kali systemd[1]: Finished apparmor.service>
lines 1-13/13 (END)
```

8. Update Everything

To keep Ubuntu system safe, make sure to run regular updates.

1. Update the package information.

sudo apt-get update

2. Simulate an upgrade of all packages.

Simulate the upgrade of all packages to prevent unintended alterations or removals during the process, ensuring a safe and controlled update experience.

sudo apt-get upgrade -s

3. Upgrade all packages.

sudo apt-get upgrade

You can upgrade individual packages one at a time by substituting "$packagename" with the name of each specific package.

sudo apt-get install --only-upgrade $packagename

4. Update your CMS, plugins, and any other manually installed software.

Ensure the security and performance of your system by regularly updating your Content Management System (CMS), plugins, and any other manually installed software. Keeping these components up to date helps patch vulnerabilities, improve features, and maintain compatibility with the latest technologies. Regular updates are a crucial aspect of overall system maintenance and cybersecurity.

9. Use Strong Passwords

An essential aspect of securing a Linux server involves the establishment of robust passwords. Constructed from a lengthy and randomized combination of uppercase and lowercase letters, numbers, and symbols, strong passwords should avoid using words or dates. Regular password updates for all users are imperative, as implementing password policies effectively mitigates the risk of brute force attacks by discouraging the reuse of passwords across various services.

1. Use pwgen to generate a strong password.

Install pwgen.

```
sudo apt install pwgen
```

Generate a set of highly secure passwords, incorporating symbols, with the command "pwgen -ys 20" where the flags "y" indicate inclusion of symbols and "s" ensures the creation of a strong password string consisting of 20 characters.

```
pwgen -ys 20
```

2. Set a password expiration policy.

Utilize the etc/login.defs file to implement a shorter password expiration policy, ranging from 30 to 90 days. Adjust PASS_MAX_DAYS to determine the period after which passwords expire, set PASS_MIN_DAYS to specify the minimum days before password changes are allowed, and configure PASS_WARN_AGE to determine the number of days for login warnings before password expiration, noting that this doesn't extend the PASS_MAX_DAYS expiration period.

10 . Installing kali linux

GParted is a premier disk partition management utility that is available for Ubuntu. It is a graphical tool that allows you to create, delete, resize, move, copy, and check partitions, as well as their file systems.

$df -> this command lists partitions in ubuntu terminal and through this we can check /root or home directory

1. Insert the USB bootable drive with the kali linux .dd image.
2. Get into the BIOS and disable secure boot, as Linux does not support secure boot and enable virtualization.

3. Restart the System -> Press F12 -> Select Graphical install option from the list -> Select Language: English -> Select Country: India -> Select Keyboard layout: American English-> Enter Hostname: kali -> Domain name: Leave it blank -> Enter Prefered Username and Password -> Under Force UEFI: Select Yes -> Under

Partition option: Choose Manual -> Select Free space which is to be partitioned -> Create three partitions for SWAP AREA of size 8GB(Choose EFI storage type) another for startup 512MB(choose EXT4 storage type) -> then using rest of the storage create EXT4 storage type partition, then press continue. -> next tick list of software to install softwares which are required -> under GRUB boot loader select yes -> then restart -> system will boot into kali linux(pendrive can be removed).