

IRIS BUSINESS SERVICES LIMITED

Document Control:

Document Name	Ubuntu 22,04 OS Hardening
Version Number	V1.1
Prepared By	Vishal Vare
Reviewed By	Mahesh Tilave
Date of Review	27-09-2023
Approved By	PKX Thomas
Date of Release	27-09-2023

Version Control:--

Version No.	Date	Prepared by / Modified by	Overview of Changes
V1.0	28-08-2023	Vishal Vare	Draft
V1.1	27-09-2023	Vishal Vare	First Release

Table of Contents

1. Introduction----------Page| 3

2.Warning Banner----------Page| 3

3. System Updates----------Page| 3

4. Installation of Necessary Software----------Page| 3

5. Firewall Configuration----------Page| 4

6. Securing SSH Access----------Page| 4

7. User Accounts and Passwords----------Page|5

8. File Permissions----------Page| 5

9. Disable Unnecessary Services ----------Page|5

10. Backups----------Page| 5

11. Security Tools----------Page| 5

INTRODUCTION -

Hardening an Ubuntu 22.04 system involves implementing security measures to protect it from various threats and vulnerabilities. Here are some steps you can follow to harden your Ubuntu 22.04 operating system:

1. **Warning Banner on Server Login:** Ensure that your system has enabled with Organization warning message Policy.

a) vim /etc/iris_banner

* * * * * * * W A R N I N G * * * * * * * * * *

This computer system is the property of the IRIS Business Services Ltd. It is for authorized use only. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil charges/criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

* * * * * * * W A R N I N G * * * * * * * * * *

b) vim /etc/ssh/sshd_config

Uncomment the Banner Header and make changes as below

Banner /etc/iris_banner

c) Restart sshd service using below command

systemctl restart sshd

2. **Keep Your System Updated:** Ensure that your system is regularly updated with the latest security patches and updates. Use

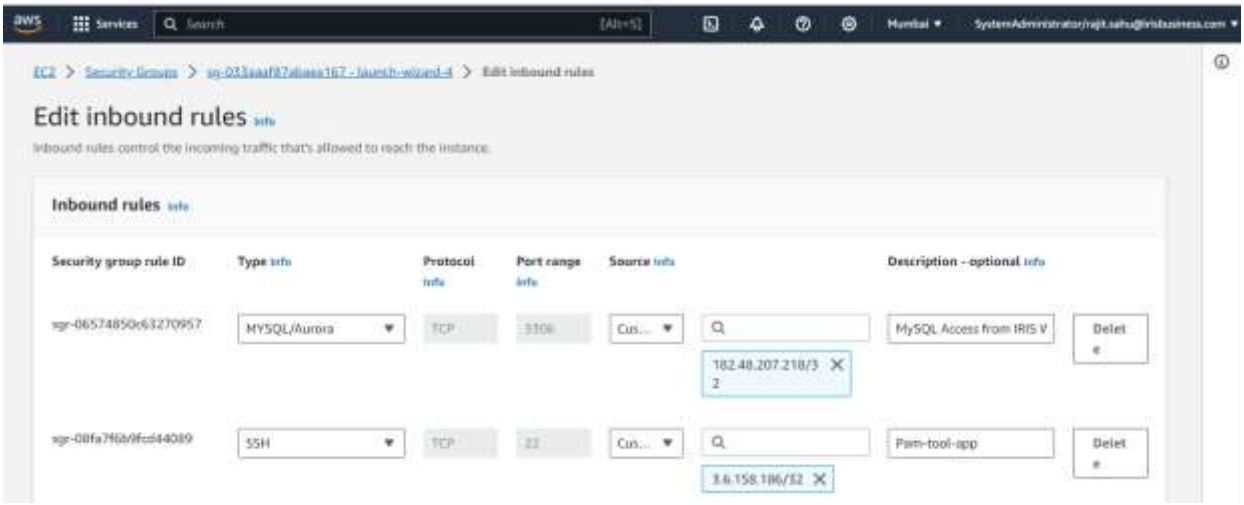
```
sudo apt update
```

3. **Install Only Necessary Software:** Remove any unnecessary software and packages from your system to reduce the attack surface. Use the apt command to uninstall software you don't need.

```
sudo apt autoremove
```

4. Firewall Configuration: Configure the firewall to restrict incoming and outgoing network traffic. Only allow necessary services and ports.

This is achived using AWS Security group. Hence we are using AWS Security group for server level port blocking /restriction.
Below is the screenshot of AWS security group and how blocking of port level restriction applied in Security Groups.



5. Secure SSH Access: If SSH is required, disable root login and password-based authentication. Use SSH keys and consider using a non-standard port.

```
sudo nano /etc/ssh/sshd_config
```

Ensure the following settings are set:

```
PermitRootLogin no
PasswordAuthentication yes
```

After making changes, restart SSH:

```
sudo systemctl restart sshd
```

6. User Accounts and Passwords: Enforce strong password policies, and regularly audit and remove unnecessary user accounts.

The server login is performed using PAM 360 Web Interface tool which is using Microsoft 2 factor Authentication in the PAM 360 Tool.

The Password Authentication is enable in case of event of Server access failure from the PAM 360 Tool.

7. File Permissions: Limit file and directory permissions to the minimum necessary for users and services.

Currently we have segregate production and development server access to iris developers using “irisdev” and irisprod users. Which have limited access to the server. We have only provide /virtualhost directory ownership to the irisdev and irisprod users.

We also provide sudo access to specific service requested by user such as start and stop of Apache and Tomcat services, also if they want any read, write permission to specific directory and files.

8. Disable Unnecessary Services: Disable or remove any unnecessary services running on your system to reduce the attack surface.

To disable services, we use below command:

systemctl disable service_name

Or we remove the service completely by using below command:

apt remove package_name

9. Regular Backups: Implement regular backups of critical data to recover from potential data loss or ransomware attacks.

Regular backup is perform using AWS AMI image backup and weekly incremental using snapshot backup.

10. Security Tools: We use Sophos antivirus tool for security which help us in preventing server level attacks such as ransomware, Ddos, and MySQL injection attacks and consider using security tools like intrusion detection systems (IDS) and antivirus software to enhance your system's security.