Project: System-to-System Log Forwarding using Rsyslog on Ubuntu

🧑‍💻 By: **Afroz Shaikh**
✉️ Email: **afrozshaikh8086@gmail.com**

📓 Overview

This project demonstrates how to configure **log forwarding** from one Ubuntu system to another using **rsyslog**. This technique is commonly used in **SOC environments**, **log management systems**, and **SIEM platforms** to centralize and monitor logs from multiple sources.

🛠️ Prerequisites

- Ubuntu OS installed on both systems.
- **`rsyslog`** service enabled (default on most Ubuntu installs).
- Network connectivity between the source and destination systems.
- Root or sudo access.

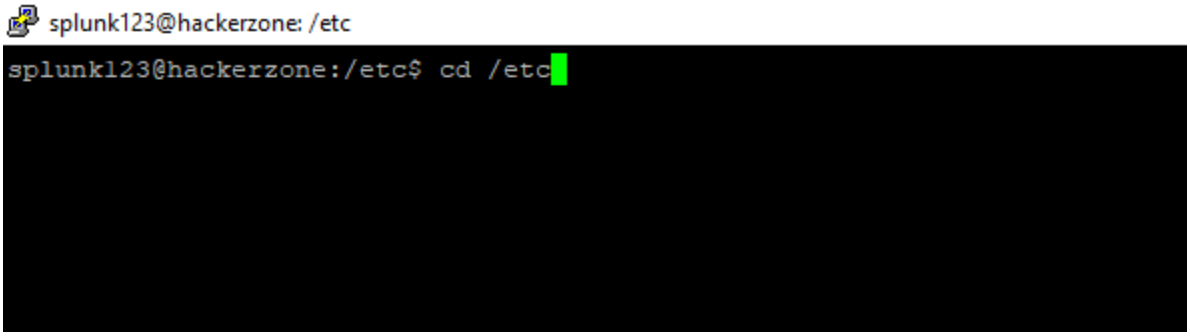
🎯 Step-by-Step Configuration

1. **Launch Terminal**

   Start by opening the terminal on your Ubuntu system.

2. **Navigate to Configuration Directory**

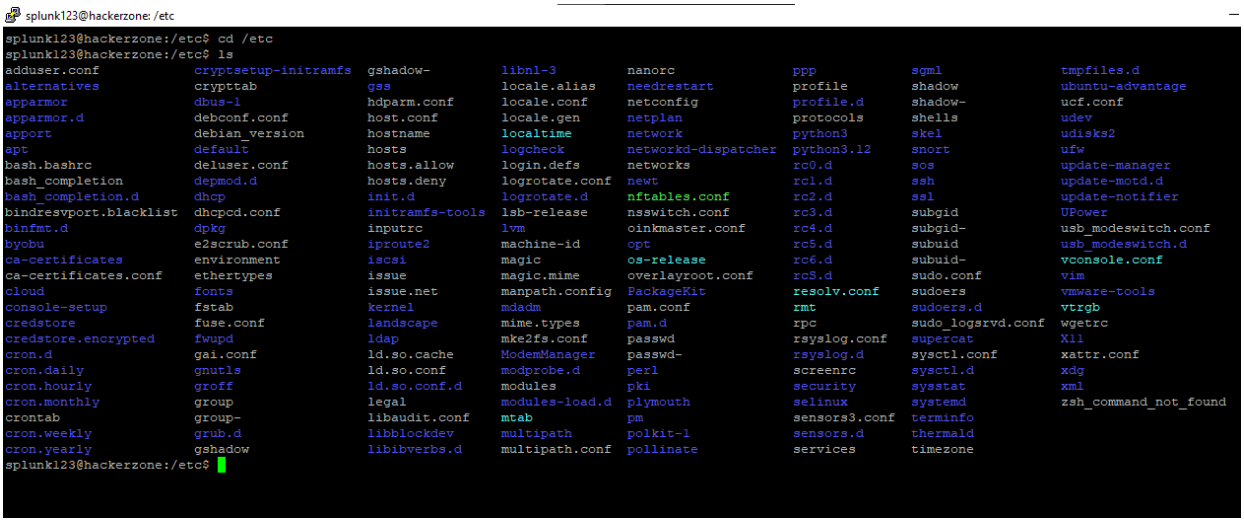
***Run the following command to go to the `/etc` directory:**



This folder contains system-wide configuration files, including those for **rsyslog**.

3. Locate rsyslog Configuration

Use `ls` to verify the presence of the configuration files:



Look for:

- **`rsyslog.conf`**
- **`rsyslog.d/` directory**

4. **Edit the rsyslog Configuration**

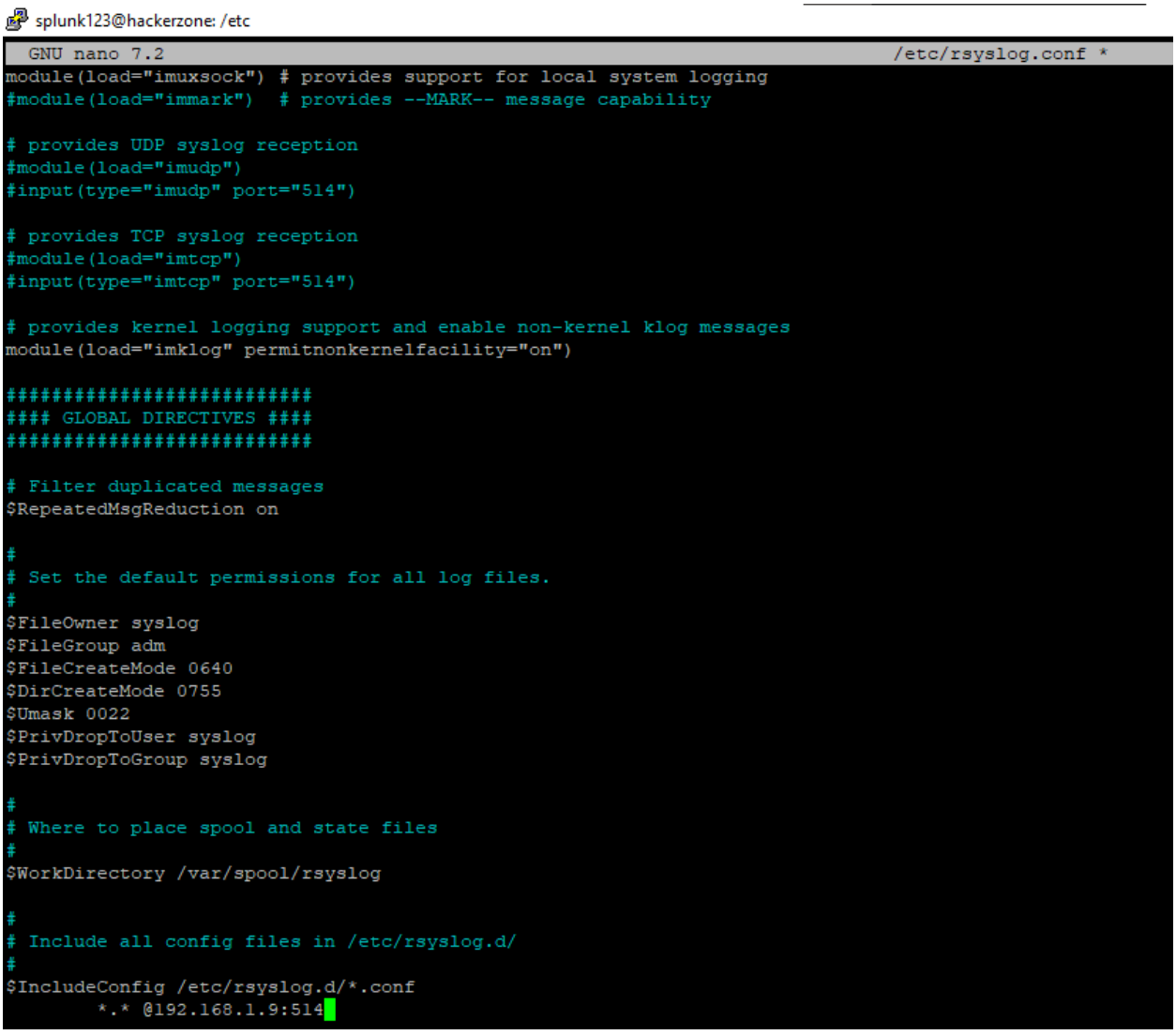
Open the config file with elevated privileges:

```
sudo nano /etc/rsyslog.conf
```

Add the following line at the end of the file:

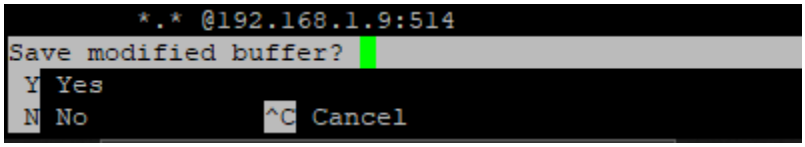
```
*.* @192.168.1.9:514
```

- `*.*` → forward all logs from all facilities and severity levels
- `@` → indicates use of **UDP** (use `@@` for **TCP**)
- `192.168.1.9:514` → destination IP and port of the log collector



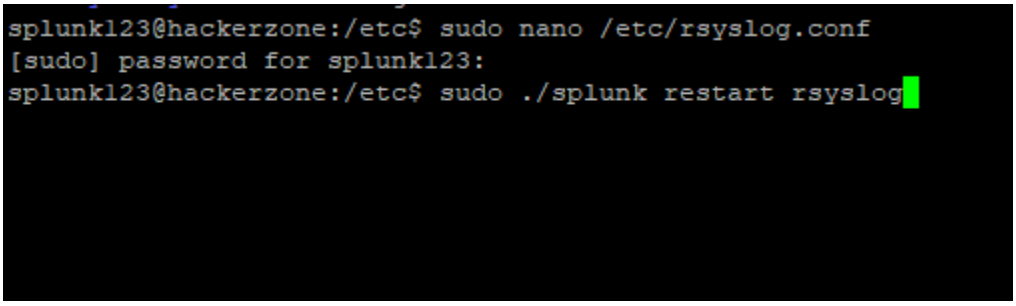
5. Save and Exit

- Press `Ctrl + X`
- Press `Y` to confirm
- Hit `Enter` to save



6. Restart rsyslog Service

```
sudo systemctl restart rsyslog
```



☑ Output

Now, logs from your system will be **forwarded in real time** to the destination system or SIEM platform for centralized analysis and monitoring.

📌 Notes

- Ensure that port `514` is open on the destination.
- Use `firewall-cmd` or `ufw` to allow traffic if needed.
- Recommended: monitor `/var/log/syslog` to verify forwarding is working.

🧠 Use Cases

- Security Operations Centers (SOC)
- SIEM integration
- Lab-based log collection projects
- Centralized log monitoring
