**My Splunk Project: Configuring Splunk Universal Forwarder on Linux to Forward Logs to Splunk Enterprise on Windows**

**Introduction**

In this project, I set up **Splunk Enterprise** on my Windows machine and configured a **Splunk Universal Forwarder** on a Linux virtual machine (VirtualBox) to forward logs to Splunk. I also created a custom index called linux to store the forwarded logs. This document walks through the entire process step-by-step, including screenshots for clarity.

**Step 1: Install Splunk Enterprise on Windows**

**1.1 Download Splunk Enterprise**

1. I went to the [Splunk website](https://www.splunk.com/) and signed up for a free account.

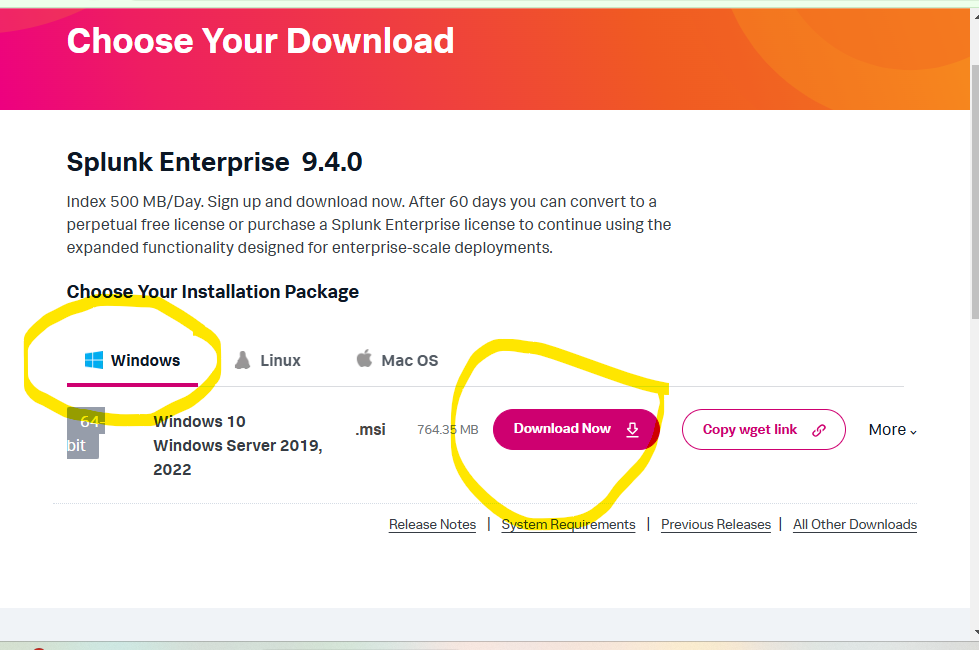


Figure 1: Splunk Enterprice download for windows

1. I downloaded the **Splunk Enterprise** installer for Windows.

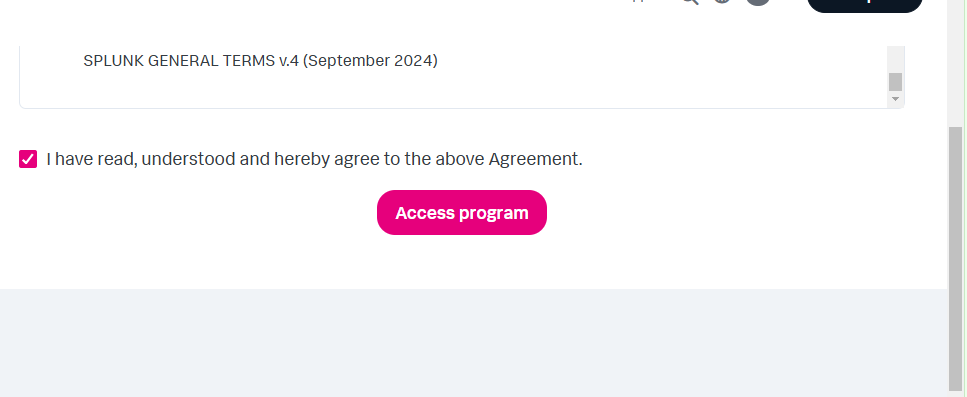
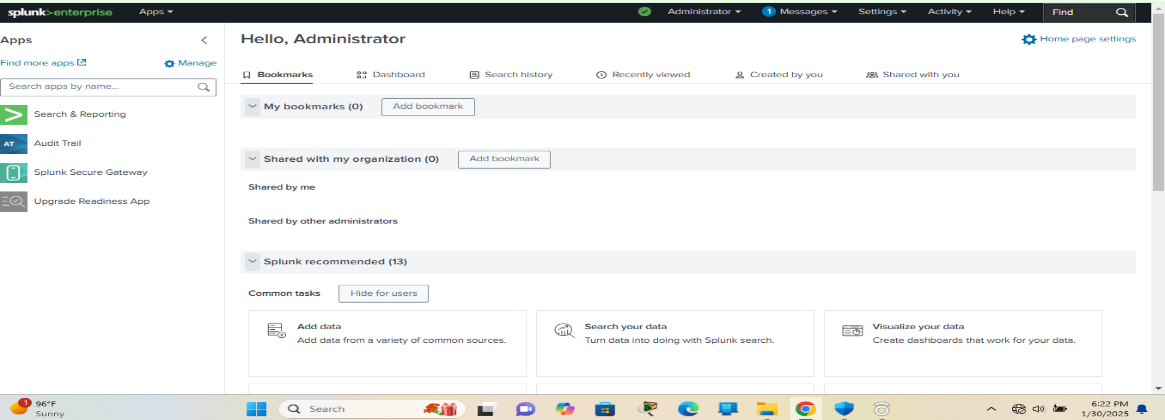


Figure 2 Licence Agreement

**1.2 Install Splunk Enterprise**

1. I located the downloaded .msi file and double-clicked to start the installation.
2. I followed the installation wizard:
   * Accepted the license agreement.
   * Add your user name and password
   * Chose the default installation directory.
   * Selected **Start Splunk Enterprise after installation**.
   * Clicked **Finish**
3. Once installed, Splunk started automatically.

**1.3 Access Splunk Enterprise**

1. I opened my web browser and went to http://localhost:8000.
2. I logged in with my credentials:
   * Username: admin
   * Password: \*\*\*\*\*\*\*\*\* (I changed this during the first login). Figure 3: Splunk Enterprice

**1.4 Create a Custom Index**

1. In Splunk Enterprise, I went to **Settings** > **Indexes**.

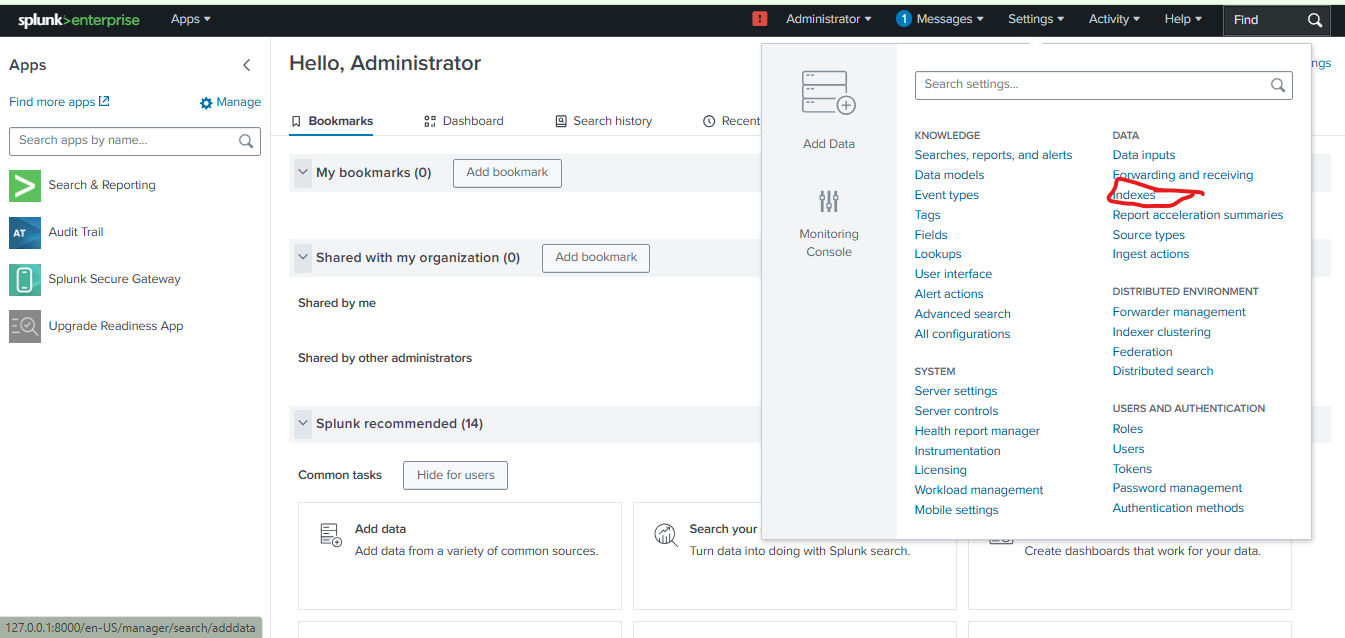


Figure 4: Index Splunk Configuration

1. I clicked **New Index** and created an index named linux.
   * This is where logs from my Linux VM will be stored.

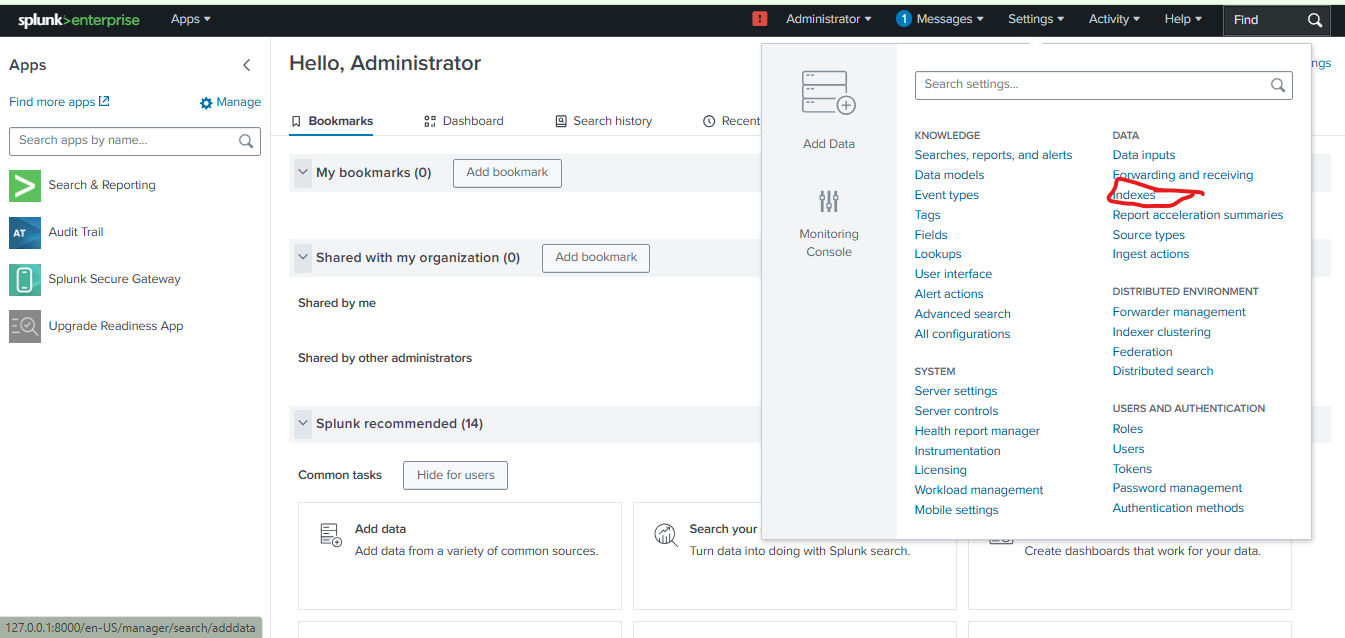


Figure 5: Index Configuration (B)

**1.5 Configure Receiving Port**

1. I went to **Settings** > **Forwarding and Receiving**.
2. I clicked **Configure Receiving** and added a new receiving port (9997).
   * This is the port the Universal Forwarder will use to send logs.

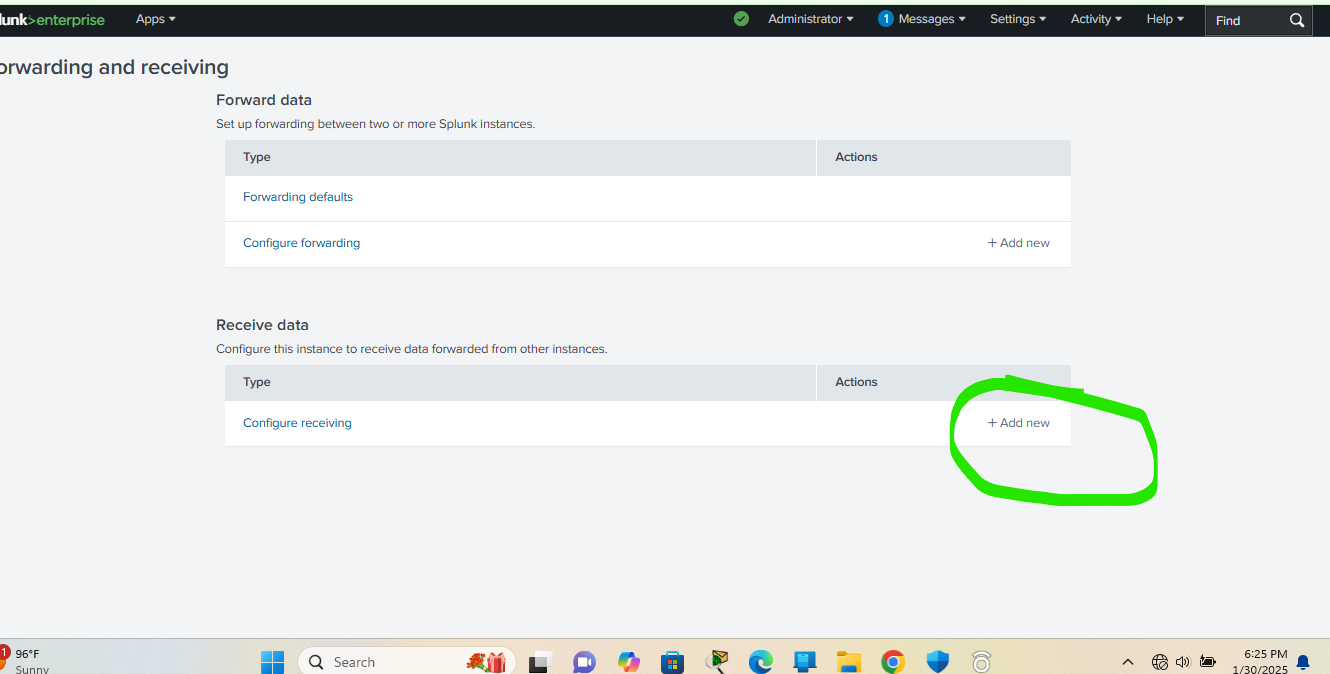


Figure 6: Confuguring Port 9997( for Data Forwarding)

**Step 2: Install Splunk Universal Forwarder on Linux (VirtualBox)**

**2.1 Download the Universal Forwarder**

1. On my Linux VM, I opened a terminal.
2. I downloaded the **Splunk Universal Forwarder** for Debian:

wget -O splunkforwarder.deb 'https://download.splunk.com/products/universalforwarder/releases/9.x.x/linux/splunkforwarder-9.x.x-xxxxxxx-linux-2.6-amd64.deb'

(I replaced the URL with the latest version from the [Splunk website](https://www.splunk.com/).)

**2.2 Install the Universal Forwarder**

1. I installed the .deb package using dpkg:

sudo dpkg -i splunkforwarder.deb

1. I resolved any dependencies using: sudo apt-get install -f

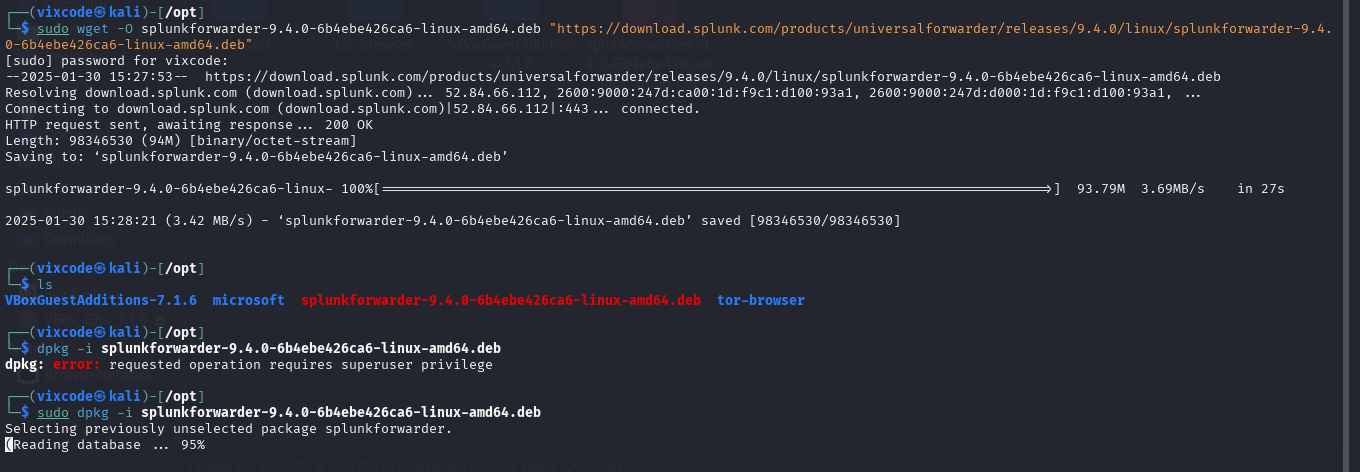
****

Figure 7 : Installing Splunk Forwarder on Linux

**2.3 Start the Universal Forwarder**

1. I navigated to the bin directory:

cd /opt/splunkforwarder/bin

1. I started the Universal Forwarder:

sudo ./splunk start

1. I accepted the license agreement when prompted.

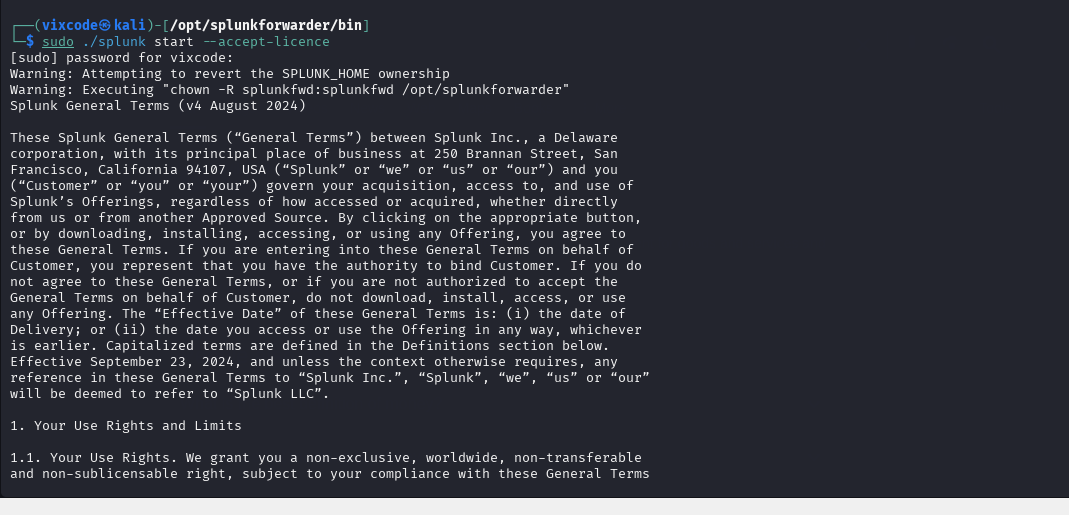


Figure 8:Starting the Splunk Forwarder on Linux

**Step 3: Configure the Universal Forwarder to Forward Logs**

**3.1 Set the Forward Server**

1. Set the Firewall rule to allow Traffic to the windows server

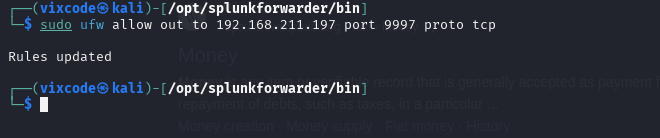


Figure 9: Firewall rule (you may have to Install ufw if not installed)

b. **On the Windows Server: I opened the terminal using the Administrator Privilege, I allowed Inbound Traffic.**

C:\Windows\System32> netsh advfirewall firewall add rule name="Splunk Forwarder" dir=in action=allow protocol=TCP localport=9997

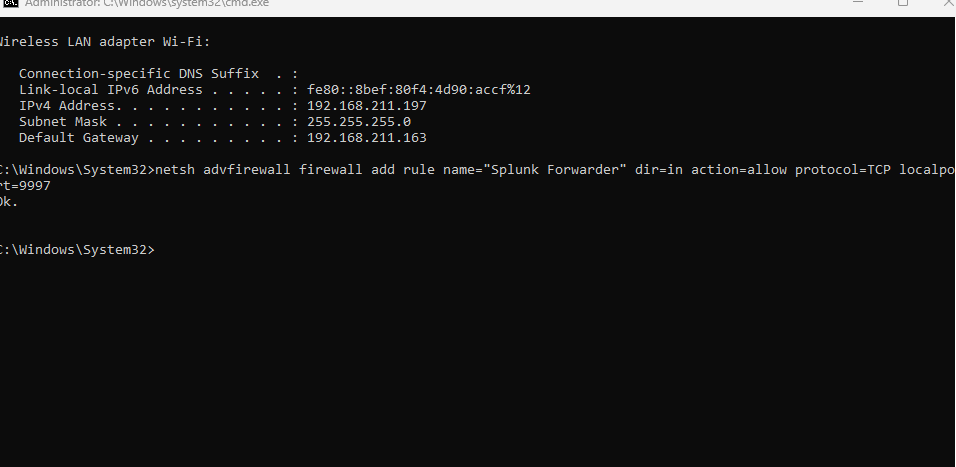


Figure 10:Windows Terminal running the inbound traffic Cmd

1. I configured the Universal Forwarder to send logs to my Windows machine:

sudo ./splunk add forward-server <windows\_ip>:9997

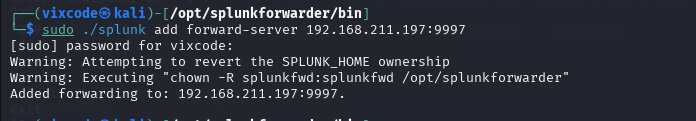


Figure 11: Added my windows IP address

**3.2 Add Logs to Monitor**

1. I told the Universal Forwarder which logs to send. For example, to forward /var/log/syslog:

sudo ./splunk add monitor /var/log/syslog -index linux

(I used the -index linux flag to ensure logs are sent to the linux index I created earlier.)

1. I added the input.conf script using the following command



Figure 12: opening a nano fille, nputs.conf to allow fowarded logs to Spunk Server.

1. I added the Syslog script

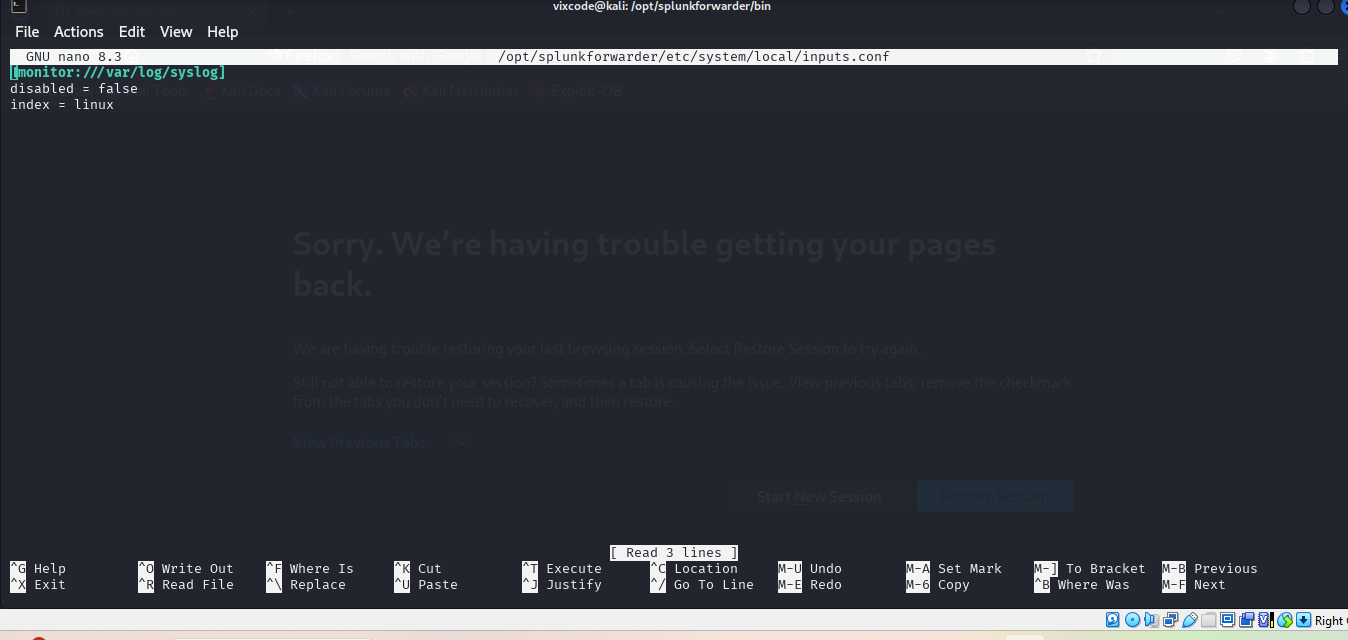


Figure 13: configured logs and index location

**3.3 Restart the Universal Forwarder**

1. I restarted the Universal Forwarder to apply the changes:

sudo ./splunk restart

**Step 4: Verify Logs in Splunk Enterprise**

**4.1 Confirm Logs are Received**

1. I saw logs from my Linux VM in the search results, which confirmed the setup was successful!

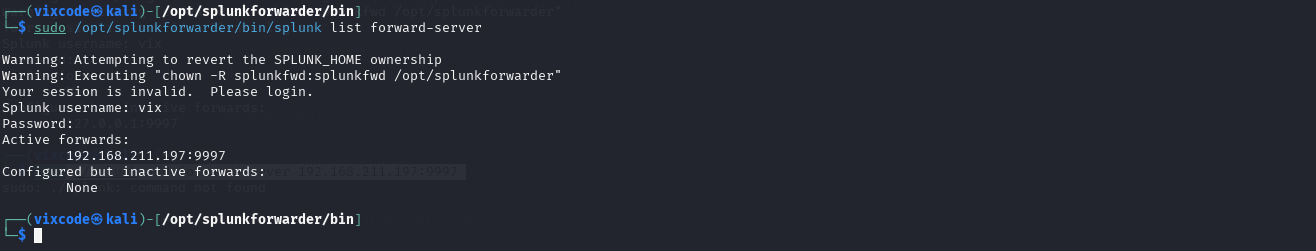


Figure 14: Successful forwarder setup

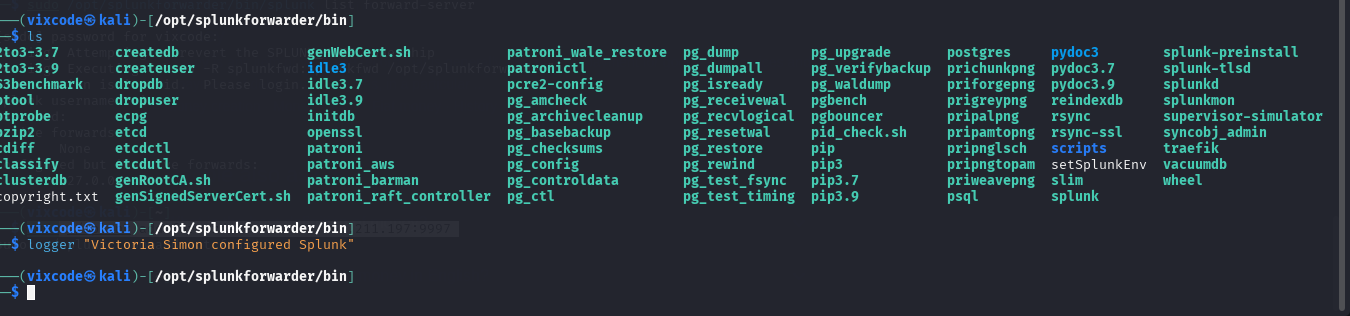


Figure 15: Added a log using the logger cmd

**4.2 Check the Splunk Enterprise Interface**

1. On my Windows machine, I opened Splunk Enterprise in my browser (http://localhost:8000).
2. I went to **Search & Reporting**.
3. I ran a search for the logs I’m forwarding:

index=”linux “

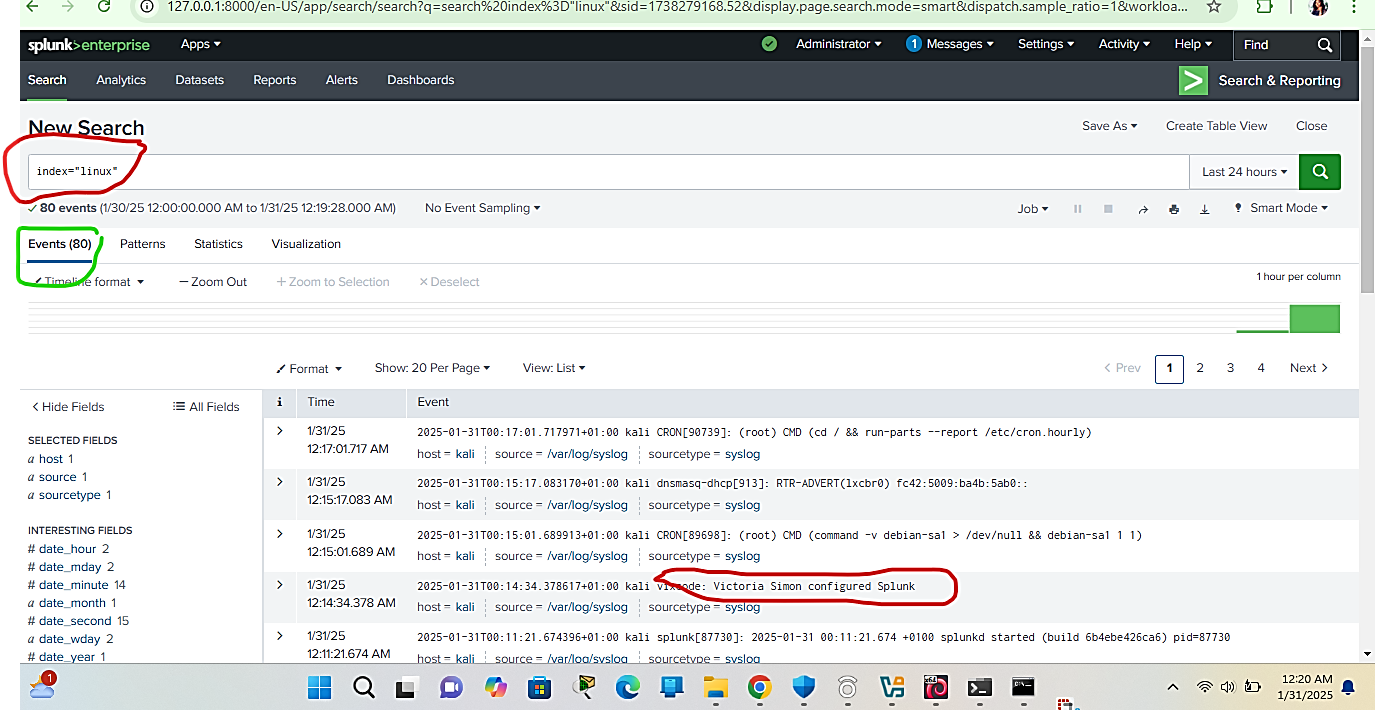


Figure 16: Splunk enterprise showing the forwarded logs to index= linux

1. If I didn’t see logs, I would check the Universal Forwarder logs for errors:

cat /opt/splunkforwarder/var/log/splunk/splunkd.log

**Troubleshooting Tips**

* **Firewall Issues**: I ensured port 9997 was open on both my Linux VM and Windows machine.
* **Permissions**: I made sure the Universal Forwarder had read access to the logs I was monitoring.
* **Network Connectivity**: I verified my Linux VM could reach my Windows machine using ping or telnet.

**Conclusion**

This project was an incredibly rewarding experience that allowed me to dive deep into the world of **log management and analysis** using Splunk. I successfully set up **Splunk Enterprise** on my Windows machine, installed the **Splunk Universal Forwarder** on my Linux VM (running on VirtualBox), and configured it to forward logs to a custom index I created called linux. Here’s a summary of what I accomplished and learned:

1. **Splunk Enterprise Setup:**

I installed Splunk Enterprise on my Windows machine, created a custom index (linux), and configured a receiving port (9997) to accept logs from the Universal Forwarder. This gave me a centralized platform to store, search, and analyze logs.

1. **Splunk Universal Forwarder on Linux:**

I downloaded and installed the Universal Forwarder using the Debian package on my Linux VM. By configuring it to monitor specific log files (like /var/log/syslog) and forward them to Splunk Enterprise, I gained hands-on experience with log collection and forwarding.

1. **Custom Indexing:**

Creating the linux index allowed me to organize and isolate logs from my Linux VM, making it easier to search and analyze them separately from other data in Splunk.

1. **Troubleshooting and Validation**:

I learned how to troubleshoot common issues, such as firewall rules, network connectivity, and file permissions. Verifying that logs were successfully forwarded and appeared in Splunk Enterprise was a satisfying milestone.

1. **Practical Application:**

This project gave me a clear understanding of how Splunk can be used in real-world scenarios, such as Security Operations Centers (SOCs) or IT monitoring. Centralizing logs from multiple systems into a single platform is a powerful way to detect anomalies, troubleshoot issues, and improve overall system security.

1. **Next Steps:**

Moving forward, I plan to explore more advanced Splunk features, such as:

* + Creating dashboards and alerts for proactive monitoring.
  + Using Splunk Search Processing Language (SPL) for more complex queries.
  + Integrating other data sources, such as Windows Event Logs or network devices.

**Knowledge gained**

* **Centralized Log Management**: Splunk provides a powerful way to collect, store, and analyze logs from multiple sources in one place.
* **Hands-On Learning**: Setting up the Universal Forwarder and configuring log forwarding gave me practical experience with Splunk’s architecture.
* **Customization**: Creating a custom index and tailoring the setup to my needs helped me understand how flexible and scalable Splunk can be.

This project not only enhanced my technical skills but also deepened my appreciation for the importance of log management in cybersecurity and IT operations. I’m excited to continue building on this foundation and exploring more ways to leverage Splunk in my career.