SOC Home Lab Deployment Report

Project Title: SOC Home Lab: SIEM Deployment & Threat Detection
Author: Scofield Lori Tosan
Environment: VirtualBox (Ubuntu Server + Windows VM)
Date: 30-12-2025

1. Objective

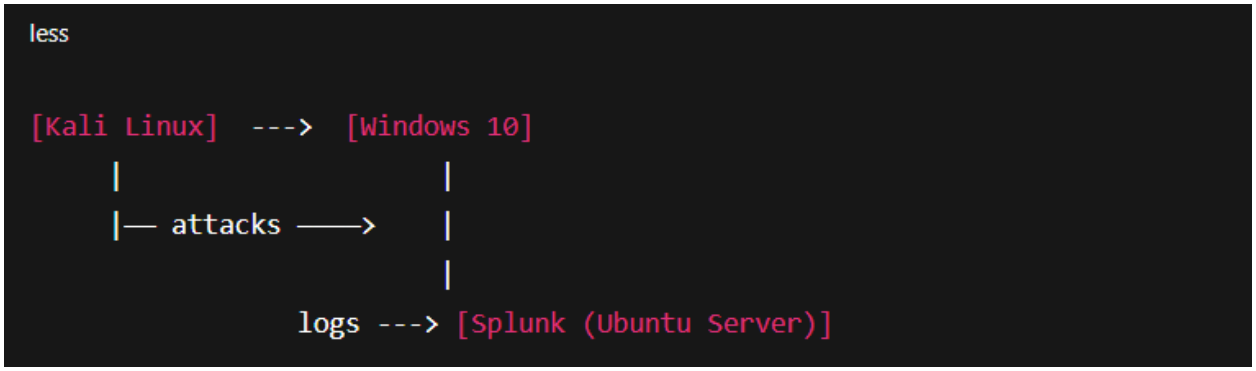
The objective of this project was to design and deploy a functional **Security Operations Center (SOC) home lab** using virtualization. The lab focuses on real-world blue-team skills, including SIEM deployment, log ingestion, troubleshooting system issues, and preparing an environment suitable for security monitoring and incident detection.

2. Lab Architecture

The lab was built using the following architecture:

[Windows VM (Endpoint)]
|
| Splunk Universal Forwarder (Port 9997)
v
[Ubuntu Server (Splunk Enterprise SIEM)]
|
v
[SOC Analyst – Dashboards, Alerts, SPL Queries]

Screenshot Placeholder – Lab Architecture Diagram:



3. Tools & Technologies Used

- **VirtualBox** – Virtualization platform
- **Ubuntu Server (LTS)** – SOC / SIEM server
- **Windows VM** – Endpoint / log source
- **Splunk Enterprise** – SIEM platform
- **Splunk Universal Forwarder** – Log forwarding agent
- **Linux LVM (Logical Volume Manager)** – Disk management

4. Ubuntu Server Setup (SOC Server)

4.1 Initial Installation

- Ubuntu Server installed on VirtualBox
- Default disk size initially allocated was insufficient for Splunk
- System configured with networking enabled for VM-to-VM communication

4.2 Splunk Enterprise Installation

Splunk Enterprise was downloaded directly from the official Splunk website using `wget`.

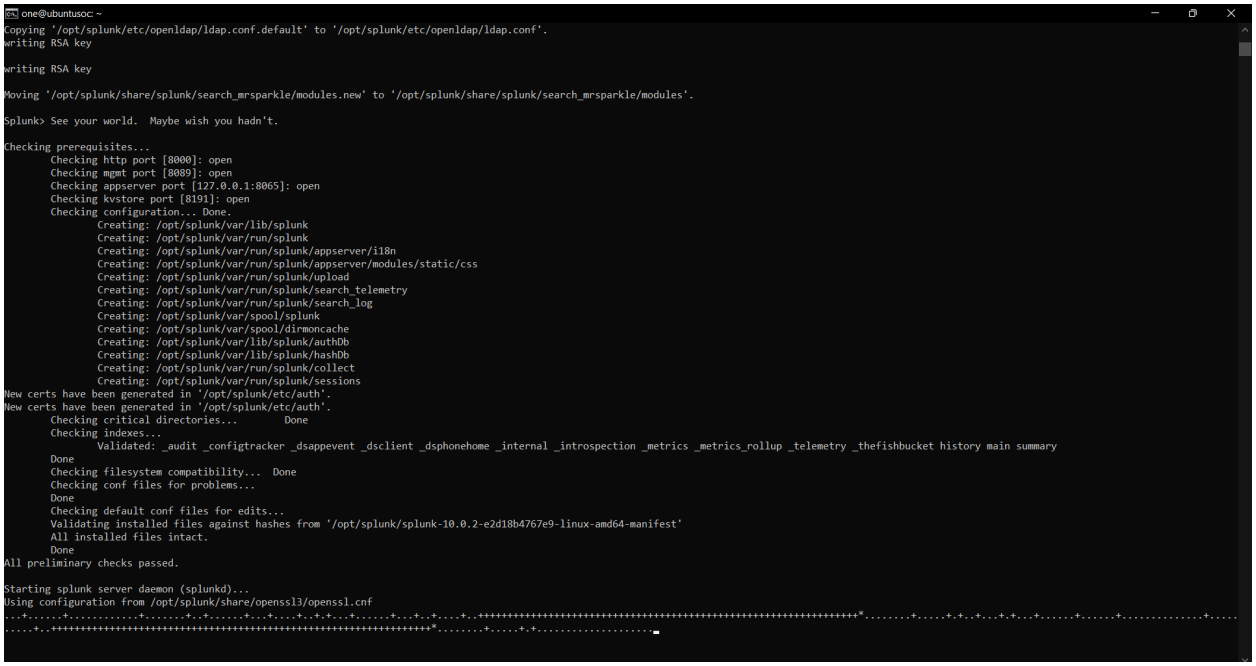
Download Command:

sudo wget -O splunk-10.0.2-linux-amd64.deb <Splunk download URL>

```
systemd-private-33ef988a8fdc49e287ffd94d945bdff8-systemd-logind.service-FbqzM4
systemd-private-33ef988a8fdc49e287ffd94d945bdff8-systemd-resolved.service-RZAvvz
systemd-private-33ef988a8fdc49e287ffd94d945bdff8-systemd-timesyncd.service-rxbFbS
one@ubuntusoc:/tmp$ wget -O splunk-10.0.2-e2d18b4767e9-linux-amd64.deb "https://download.splunk.co
m/products/splunk/releases/10.0.2/linux/splunk-10.0.2-e2d18b4767e9-linux-amd64.deb"
--2025-12-26 13:55:19--  https://download.splunk.com/products/splunk/releases/10.0.2/linux/splunk-
10.0.2-e2d18b4767e9-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 108.157.78.52, 108.157.78.4, 108.157.78.10,
 ...
Connecting to download.splunk.com (download.splunk.com)|108.157.78.52|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1356540912 (1.3G) [binary/octet-stream]
Saving to: ‘splunk-10.0.2-e2d18b4767e9-linux-amd64.deb’

splunk-10.0.2-e2d18b4767 100%[==============================>]   1.26G  4.81MB/s    in 7m 26s

2025-12-26 14:02:51 (2.90 MB/s) - ‘splunk-10.0.2-e2d18b4767e9-linux-amd64.deb’ saved [1356540912/1
356540912]

one@ubuntusoc:/tmp$
```

Installation Attempt:

sudo dpkg -i splunk-10.0.2-linux-amd64.deb



4.3 Errors Encountered During Installation

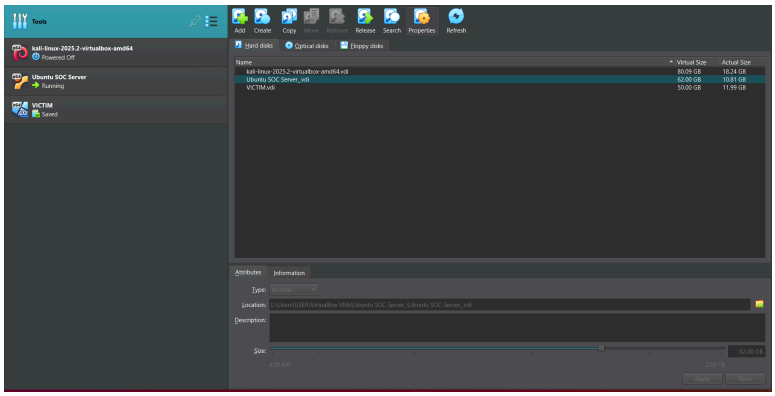
❌ Error: No Space Left on Device

During installation, the following error occurred:

failed to write (No space left on device)

This prevented Splunk from completing installation.

Screenshot Placeholder – Disk Space Error:



4.4 Root Cause Analysis

- Initial Ubuntu root filesystem was only **~11.5GB**
- Splunk Enterprise requires significantly more disk space
- The VM disk had unused space that was not allocated to the root filesystem

4.5 Disk Expansion & LVM Fix (Critical Troubleshooting)

The issue was resolved by expanding the disk using **LVM**.

Steps Performed:

1. Extended the partition:

```
sudo growpart /dev/sda 3
```

2. Resized the physical volume:

```
sudo pvresize /dev/sda3
```

3. Extended the logical volume:

```
sudo lvextend -l +100%FREE /dev/mapper/ubuntu--vg-ubuntu--lv
```

4. Resized the filesystem:

```
sudo resize2fs /dev/mapper/ubuntu--vg-ubuntu--lv
```

Result:
df -h
Root filesystem expanded to ~60GB

- Sufficient space for Splunk installation

4.6 Successful Splunk Installation

After disk expansion:

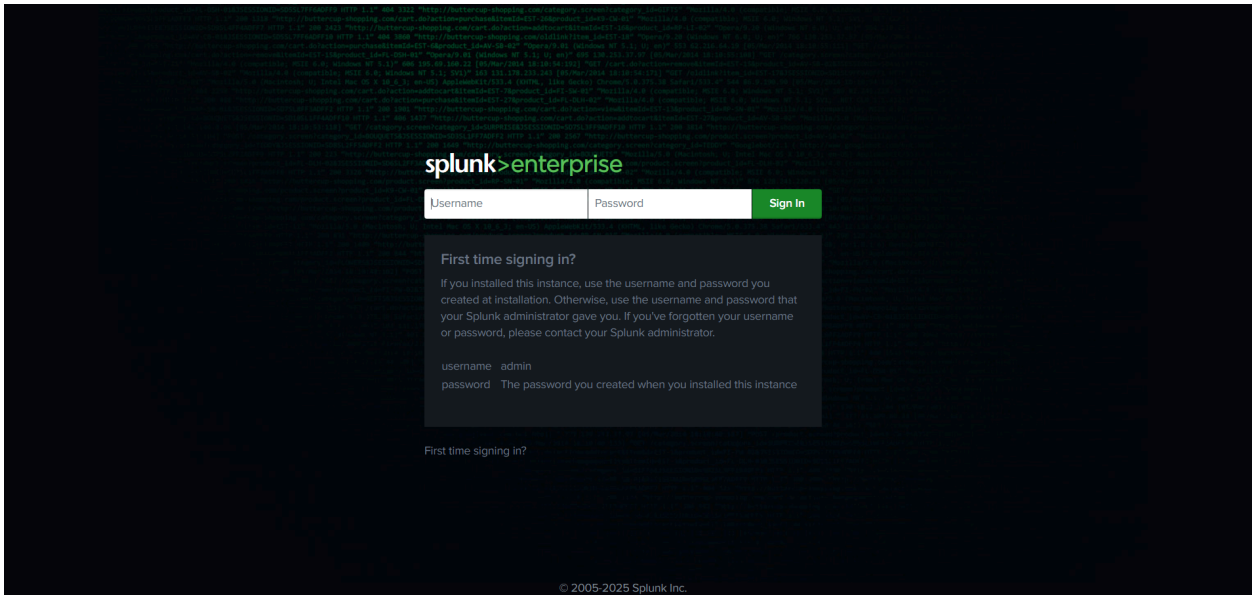
```
sudo dpkg -i splunk-10.0.2-linux-amd64.deb
```

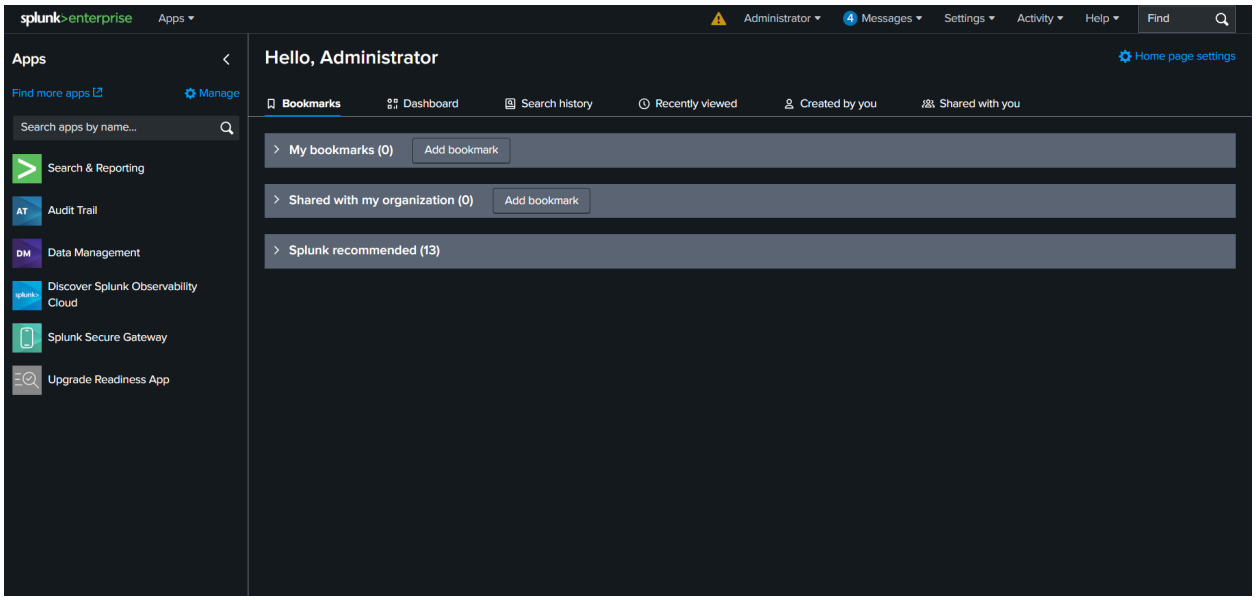
Installation completed successfully.

Splunk was started using

sudo /opt/splunk/bin/splunk start --accept-license

An administrator account was created during first launch.





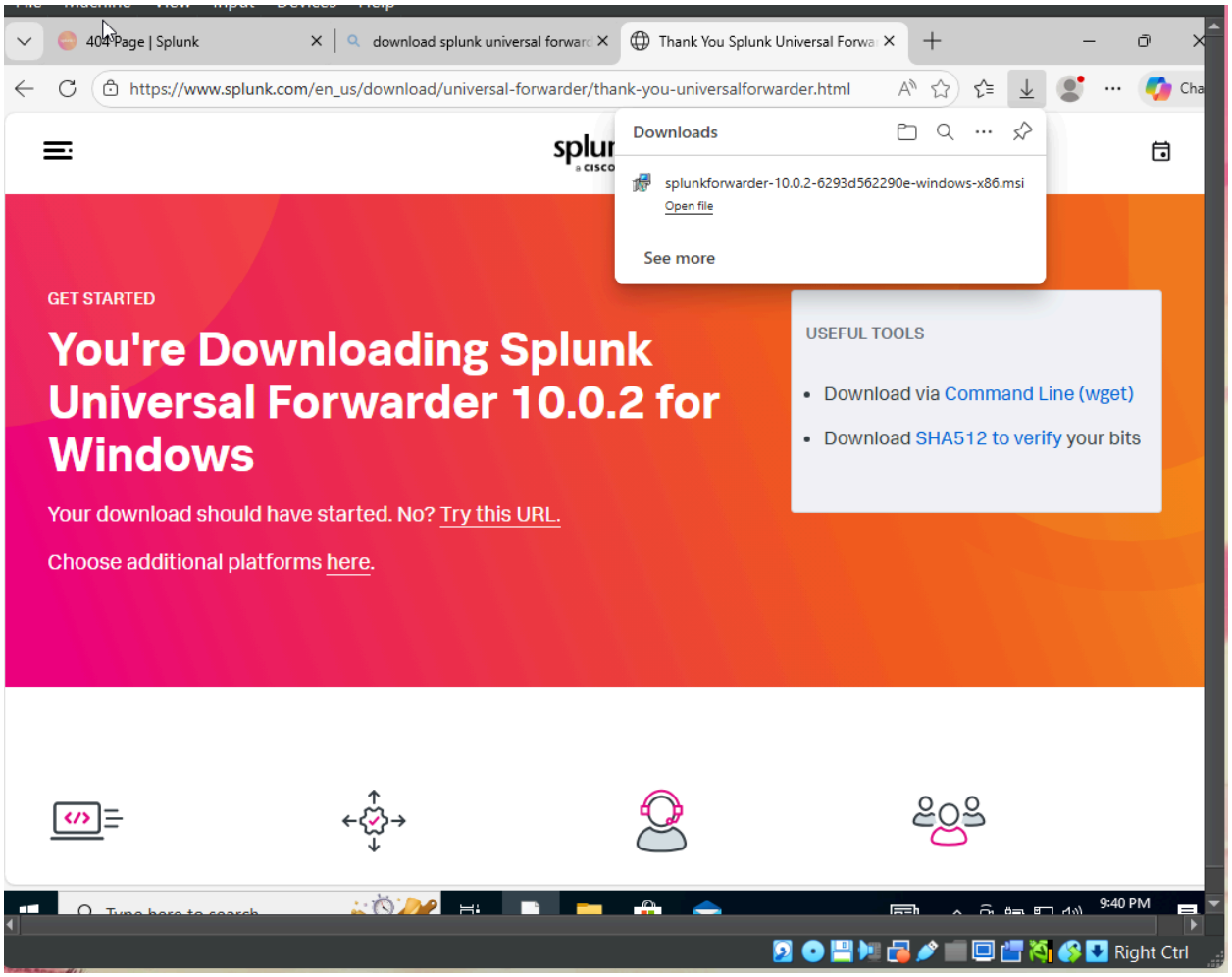
5. Windows VM Setup (Endpoint)

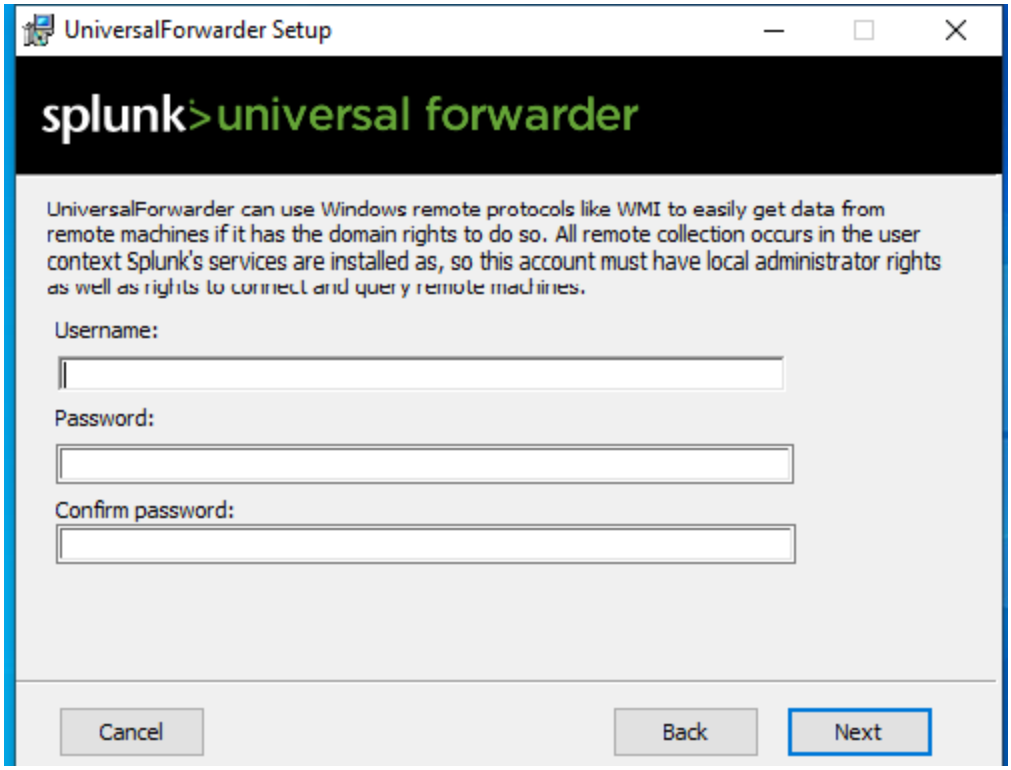
5.1 Purpose

The Windows VM acts as a **victim endpoint**, generating security telemetry such as authentication events and system activity.

5.2 Splunk Universal Forwarder Installation

- Installed Splunk Universal Forwarder (Windows x64)
- Selected **On-Premises Splunk Enterprise**
- Configured to forward logs to Ubuntu Splunk server





Key Configuration:

- **Splunk Server IP:** <UBUNTU_SERVER_IP>
- **Receiving Port:** 9997
- **Service Account:** Local System

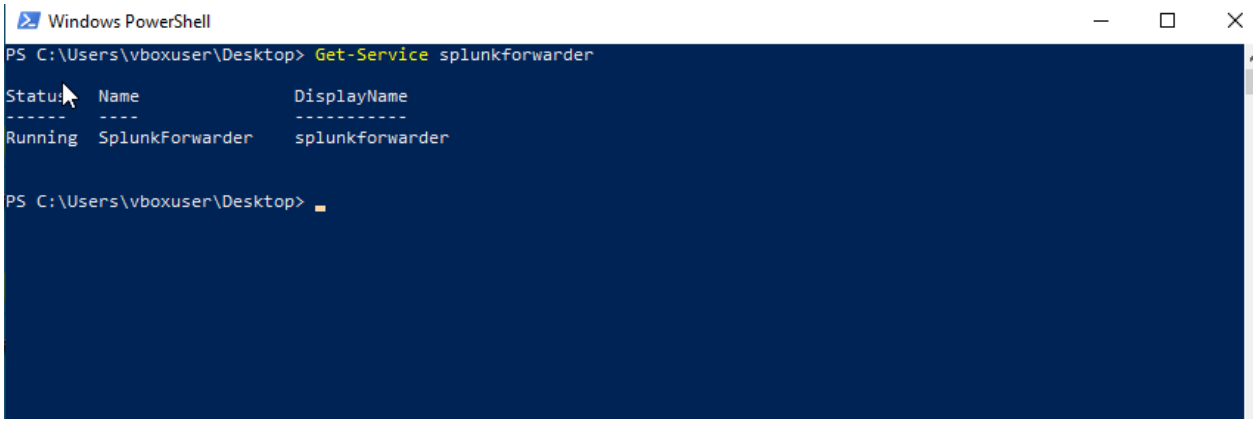
5.3 Installation Challenges

During installation, confusion occurred regarding:

- Service account credentials
- Local System vs Domain Account
- Port 8089 vs Port 9997

These were resolved by:

- Selecting **Local System**
- Using **Port 9997** for log forwarding
- Leaving management port (8089) unchanged



6. Splunk Service Management

Starting Splunk After Shutdown

To restart Splunk after it was closed:

sudo /opt/splunk/bin/splunk start

To check status:

sudo /opt/splunk/bin/splunk status

7. Security & SOC Relevance

This lab simulates a real SOC workflow:

- Endpoint generates logs
- Logs forwarded securely to SIEM
- Analyst investigates events via dashboards and SPL

Skills demonstrated:

- SIEM deployment
- Linux troubleshooting
- Disk and LVM management
- Windows log ingestion
- Forwarder configuration
- Real-world SOC problem solving

8. Conclusion

This SOC home lab was successfully deployed after resolving multiple real-world technical challenges. The troubleshooting process closely mirrored issues faced by SOC analysts and security engineers in production environments. The lab now provides a strong foundation for practicing detections, investigations, and incident response.

9. Future Improvements

- Enable Windows Event Logs via `inputs.conf`
- Install Sysmon for enhanced telemetry
- Create dashboards and alerts
- Simulate attacks (brute force, scans)
- Expand to multi-endpoint ingestion

End of Report