=== Splunk Universal Forwarder Setup & Troubleshooting ===

1. Download and Install Universal Forwarder (Linux):

```
wget -O splunkforwarder.tgz 'https://download.splunk.com/...'
tar -xvzf splunkforwarder.tgz
sudo ./splunkforwarder/bin/splunk start --accept-license
```

2. Enable Boot Start:

```
sudo ./splunkforwarder/bin/splunk enable boot-start
```

3. Check Forwarder Status:

```
sudo /opt/splunkforwarder/bin/splunk status
```

4. Create output.conf (to connect to indexer):

```
sudo nano /opt/splunkforwarder/etc/system/local/output.conf
[tcpout]
defaultGroup = default-autolb-group
[tcpout:default-autolb-group]
server = <indexer-ip>:9997
```

5. Create inputs.conf (to specify log sources):

```
sudo nano /opt/splunkforwarder/etc/system/local/inputs.conf
[monitor:///var/log/auth.log]
disabled = false
index = linux_logs
sourcetype = linux_secure
```

6. Restart Splunk Forwarder:

```
sudo /opt/splunkforwarder/bin/splunk restart
```

7. Use journalctl for modern system logs:

```
sudo journalctl -u ssh.service
sudo journalctl _SYSTEMD_UNIT=systemd-logind.service
```

sudo journalctl -xe | grep sshd

sudo journalctl -f -u sshd

8. Extract logs from journalctl into files:

sudo journalctl _COMM=sshd > /var/log/ssh_journal.log

9. Check if Splunk is listening on port 9997 (Windows):

netstat -an | findstr 9997

10. Verify connectivity from Linux to Indexer (Windows):

telnet <windows-ip> 9997

11. Deployment Client Config:

sudo nano /opt/splunkforwarder/etc/system/local/deploymentclient.conf

[deployment-client]

[target-broker:deploymentServer]

targetUri = <windows-ip>:8089

12. On Splunk Indexer: Create app folder (Windows):

mkdir C:\Program Files\Splunk\etc\deployment-apps\linux_log_inputs\local

Create inputs.conf inside it

13. Restart Splunk Services (Windows):

Restart via Services.msc or CMD: net stop splunkd && net start splunkd

14. Check Deployment Clients on Web UI:

Settings > Forwarder Management

15. Troubleshooting Useful Commands:

tail -f /opt/splunkforwarder/var/log/splunk/splunkd.log

sudo less /var/log/syslog

sudo less /var/log/auth.log

sudo less /var/log/kern.log

16. Example Search in Splunk:

```
index=linux_logs sourcetype=linux_secure
```