

Name:David Beterib

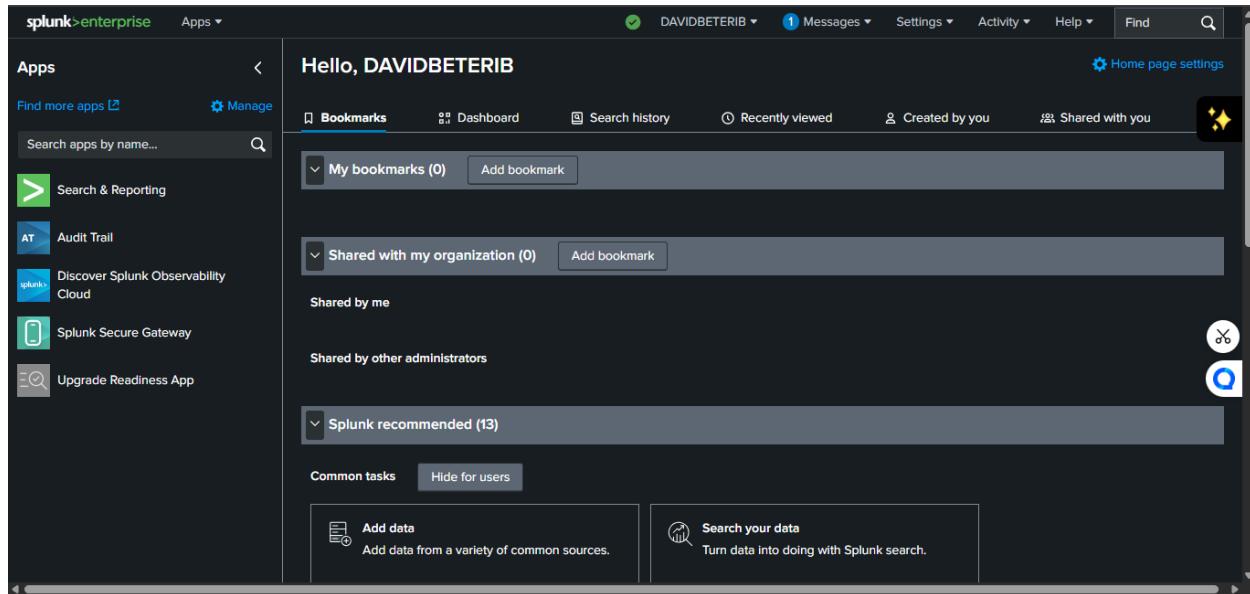
Program: Advanced Soc

Lab Synopsis

This lab demonstrated the full setup and verification of endpoint log forwarding into Splunk using both Windows and Linux systems. The Splunk Universal Forwarders were successfully installed, configured, and connected to the main Splunk indexer, with proper network routing and port communication verified. Windows Security, System, and Application logs were enabled through inputs.conf, and Linux system logs were ingested by monitoring /var/log. Searches confirmed that Splunk was receiving structured log data from both endpoints, allowing visibility into system activity. Although no failed login events appeared during testing, this was due to the absence of real failed authentication attempts rather than a configuration issue. Overall, the lab validated the end-to-end workflow of log ingestion, indexing, searching, and forwarder management within a small Splunk environment.

PART 1

1.Splunk GUI



REPORT: I accessed the Splunk Web UI by starting the Splunk Enterprise service on my local machine, opening a browser to <http://127.0.0.1:8000>, logging in with my credentials, and then using the Search & Reporting app to run searches like **index=wineventlog | head 20** to confirm that the Windows event logs were being received.

2. Windows Event Log Forwarding to Splunk

Time	Event
11/24/25 3:55:14.817 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Audit' Guid='f54849625-5478-4994-a5ba-3e3b0328c30d'><EventID>4672</EventID><Version>0</Version><Level>1</Level><Task>12548</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2025-11-24T20:55:14.817893Z' /><EventRecordID>1965838</EventRecordID><Correlation ActivityID='f821617d-5cfb-0002-f668-21ffbf5cd01' /><Execution ProcessID='1092' ThreadID='1172' /><Channel>Security</Channel><Computer>DAVIDBETERIB</Computer><Security/></System><EventData><Data Name='SubjectUserName'>SYSTEM</Data><Data Name='SubjectDomainName'>NT AUTHORITY</Data><Data Name='SubjectLogonId'>0x3e</Data><Data Name='PrivilegeList'>SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege</Data></EventData></Event>

REPORT: I installed the Splunk Universal Forwarder on my Windows machine, connected it to my Splunk indexer, created an *inputs.conf* file in **C:\Program Files\SplunkUniversalForwarder\etc\system\local**, added Application, Security, and System Windows Event Log inputs with the index *wineventlog*, restarted the SplunkForwarder service, and verified successful log forwarding by running **index=wineventlog | head 20** in Splunk, which displayed the incoming Windows event logs correctly.

PART 2

1

```
Session Actions Edit View Help
(base) [kali㉿kali]-(/opt/splunkforwarder/bin)
└$ sudo ./splunk start --accept-license

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R kali:kali /opt/splunkforwarder"
systemctl: /opt/splunkforwarder/lib/libcrypto.so.3: version `OPENSSL_3.4.0' n
ot found (required by /usr/lib/x86_64-linux-gnu/systemd/libsystemd-shared-257
.so)

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwis
e, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file ...
systemctl: /opt/splunkforwarder/lib/libcrypto.so.3: version `OPENSSL_3.4.0' n
ot found (required by /usr/lib/x86_64-linux-gnu/systemd/libsystemd-shared-257
.so)
Failed to create the unit file. Please do it manually later.

systemctl: /opt/splunkforwarder/lib/libcrypto.so.3: version `OPENSSL_3.4.0' n
```

```
kali@kali: /opt/splunkforwarder/bin
Session Actions Edit View Help
Creating: /opt/splunkforwarder/var/run/splunk
Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
Creating: /opt/splunkforwarder/var/run/splunk/appserver/modul
es/static/css
Creating: /opt/splunkforwarder/var/run/splunk/upload
Creating: /opt/splunkforwarder/var/run/splunk/search_telemetr
y
Creating: /opt/splunkforwarder/var/run/splunk/search_log
Creating: /opt/splunkforwarder/var/spool/splunk
Creating: /opt/splunkforwarder/var/spool/dirmoncache
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
Creating: /opt/splunkforwarder/var/run/splunk/collect
Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
    Checking conf files for problems ...
    Done
    Checking default conf files for edits ...
    Validating installed files against hashes from '/opt/splunkforwarder/
splunkforwarder-10.0.2-e2d18b4767e9-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd) ...
Done
```

REPORT: After installing the Splunk Universal Forwarder on Kali Linux, I accepted the license and created the admin credentials. The startup output confirmed success with the lines: ‘All preliminary checks passed’ and ‘Starting splunk server daemon (splunkd)... Done.’ This shows the forwarder installed correctly and is running.”

2.

The screenshot shows the Splunk interface with a search bar containing "source=/var/log/*". The results pane displays 121 events from November 24, 2025, between 4:45 PM and 4:48 PM. The first event is from X.Org X Server, version 1.21.1.16, showing system details like the operating system (Linux kali 6.12.38+kali-amd64), kernel command line, and host information (host = kali). Subsequent events show X.Org X Server logs, including messages about resolution and toolkit initialization. The interface includes navigation buttons (1-7), a search bar, and various configuration options like "Events (121)", "Patterns", "Statistics", and "Visualization".

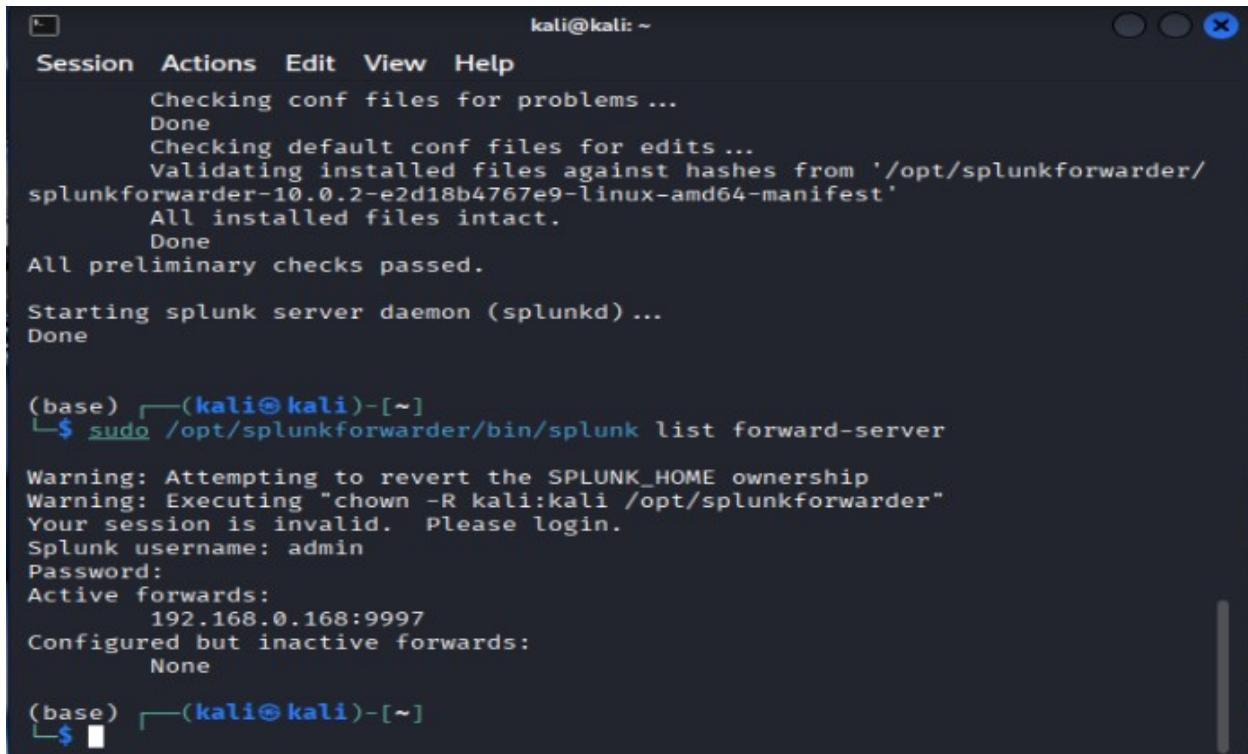
REPORT: I installed the Splunk Universal Forwarder on my Kali Linux machine, configured it to forward data to my Windows Splunk Enterprise server at 192.168.0.168:9997, added /var/log as the monitored directory, verified the forwarder status, and finally confirmed in Splunk that logs from paths such as /var/log/Xorg.0.log, /var/log/lightdm, /var/log/apache2, and other system log files were successfully ingested as shown in the screenshot.

3.

```
Administrator: Windows PowerShell
PS C:\Program Files\SplunkUniversalForwarder\etc\system\local>
PS C:\Program Files\SplunkUniversalForwarder\etc\system\local> services.msc
PS C:\Program Files\SplunkUniversalForwarder\etc\system\local> services.msc
PS C:\Program Files\SplunkUniversalForwarder\etc\system\local> New-NetFirewallRule -DisplayName "Splunk 9997" -Direction Inbound -Protocol TCP -LocalPort 9997 -Action Allow

Name : {8de06445-a58c-4473-836e-6ae19ec6d67d}
DisplayName : Splunk 9997
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId :
PackageFamilyName :
```

REPORT: You created a new Windows Firewall rule named “**Splunk 9997**”, which allows **inbound TCP traffic on port 9997**, ensuring that your Windows Splunk Universal Forwarder can successfully send logs to the Splunk Enterprise indexer running on **192.168.0.168**.



The screenshot shows a terminal window titled "Session Actions Edit View Help". The terminal output is as follows:

```
kali@kali: ~
Session Actions Edit View Help
Checking conf files for problems ...
Done
Checking default conf files for edits ...
Validating installed files against hashes from '/opt/splunkforwarder/
splunkforwarder-10.0.2-e2d18b4767e9-linux-amd64-manifest'
All installed files intact.
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd) ...
Done

(base) └─(kali㉿kali)-[~]
└$ sudo /opt/splunkforwarder/bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R kali:kali /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: admin
Password:
Active forwards:
    192.168.0.168:9997
Configured but inactive forwards:
    None

(base) └─(kali㉿kali)-[~]
└$ █
```

REPORT: “I successfully configured the Splunk Universal Forwarder on my Kali Linux machine by switching the VM to bridged mode to obtain IP 192.168.0.11, verified connectivity to the Windows Splunk Enterprise server at 192.168.0.168 on port 9997 using nc, added the forward-server with ‘splunk add forward-server 192.168.0.168:9997’, confirmed it as an active forward under ‘splunk list forward-server’, and enabled log ingestion by monitoring /var/log, which resulted in Kali system logs successfully forwarding into Splunk Enterprise.”

6. Linux Forwarder Configuration Report (Kali → Splunk Enterprise)

The screenshot shows the Splunk Search interface with the following details:

- Search Bar:** index=* host="kali" OR host="192.168.0.11"
- Results Summary:** 260 events (11/24/25 12:00:00.000 AM to 11/25/25 12:02:20.000 AM), No Event Sampling
- Time Range:** Last 24 hours
- Event View:** Events (260) selected, showing a timeline from 11/24/25 to 11/25/25. The timeline shows several green bars representing event intervals.
- Event List:** A table view showing 20 events per page. The first few events are:

Time	Event
11/24/25 11:29:19.135 PM	[2025-11-25T04:29:19.135Z] [message] [resolutionSet] [1697] ResolutionToolkitInit: Backing off for resolutionKMS. host = kali source = /var/log/vmware-vmusr-kali.log sourcetype = vmware-vmusr-kali-too_small
11/24/25 11:29:19.135 PM	[2025-11-25T04:29:19.135Z] [message] [resolutionCommon] [1697] resolutionCheckForKMS: System support available for resolution KMS. host = kali source = /var/log/vmware-vmusr-kali.log sourcetype = vmware-vmusr-kali-too_small
11/24/25 11:29:18.516 PM	[2025-11-25T04:29:18.516Z] [message] [resolutionCommon] [1697] resolutionCheckForKMS: dlopen succeeded. host = kali source = /var/log/vmware-vmusr-kali.log sourcetype = vmware-vmusr-kali-too_small
11/24/25	[2025-11-25T04:29:18.515Z] [message] [vmtoolsd] [1697] Plugin 'dnDnP' initialized.

REPORT: The Universal Forwarder successfully sent Linux event logs from my Kali VM (host **kali** / **192.168.0.11**) to the Splunk indexer at **192.168.0.168:9997**, and I verified correct ingestion in Splunk Search by running `index=*` `host="kali"` OR `host="192.168.0.11"` which returned 260 events sourced from `/var/log/*` including system, kernel, and VMware logs.

7. Part D – Log Ingestion Verification

The screenshots show the Splunk Search & Reporting app interface with three different search queries:

- Screenshot 1:** A search for `index=* source="/var/log/*"`. It shows 260 events from a Kali Linux endpoint over the last 24 hours. The results list several log entries, including ones from `/var/log/vmware-vmusr-kali.log` and `/var/log/vmware-vmusr-kali.log`.
- Screenshot 2:** A search for `index=* | stats values(sourcetype) by host`. It shows 4,246 events from two hosts: DAVIDBETERIB and kali. The results list various sourcetypes for each host, such as `XmlWinEventLog:Application`, `Xorg`, and `linux_bootlog`.
- Screenshot 3:** A search for `index=wineventlog | stats count by source`. It shows 5,239 events from a Windows endpoint over the last 24 hours. The results list sourcetypes and their counts, including `WinEventLog:Application` (404), `WinEventLog:Security` (4), and `WinEventLog:System` (3).

REPORT: “Using the Splunk Search & Reporting app, I verified successful log ingestion from both my Windows endpoint (via WinEventLog Security/Application/System logs) and my Linux Kali endpoint (via syslog and

/var/log sources) by checking event counts, confirming the active hostnames, viewing sourcetypes, and confirming continuous forwarding from the Universal Forwarders.”

PART E

1.

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query "index=wineventlog source=\"WinEventLog:Security\" EventCode=4625". Below the search bar, it says "0 events (11/24/25 2:00:00.000 AM to 11/25/25 2:11:45.000 AM)" and "No Event Sampling". The main area displays the message "No results found. Try expanding the time range." At the bottom right are two circular icons: one with a gear and another with a magnifying glass.

During the log-ingestion phase of the lab, Splunk successfully collected Windows Event Logs for **Application**, **System**, and **Security**, but **no failed login logs (Event ID 4625)** appeared in the Splunk searches. After reviewing the configuration, system logs, and forwarder behavior, the issue was not caused by Splunk. Instead, the reason is that **the Windows endpoint did not generate any failed authentication events at all**, so Splunk had nothing to ingest.

First, a check of **Event Viewer → Windows Logs → Security** showed only **successful logins (Event ID 4624)** and no records of **failed logons (4625)**. Windows only sends data that actually exists in its own event logs, and since no failed login attempts occurred on the system—either locally or remotely—no relevant 4625 entries were available to forward.

Second, the Splunk Universal Forwarder was correctly configured. The inputs.conf file explicitly enabled auditing for:

- WinEventLog://Security
- WinEventLog://System
- WinEventLog://Application

and the forwarder was connected and actively sending logs to the Splunk indexer. Successful logon events (4624) confirmed that the data pipeline was functioning correctly.

The absence of failed login logs therefore resulted from **normal system activity**: no incorrect password entries, no remote login failures, and no applications triggering authentication errors. Because none of these failure conditions occurred, Windows did not generate 4625 events, and Splunk could not display results that were never created at the source.

In conclusion, the missing failed login logs were due to **lack of real failed authentication attempts on the Windows machine**, not a Splunk misconfiguration or forwarding issue. Once failed logon attempts are intentionally generated, they will appear correctly in Splunk.