**Windows Security Log Monitoring with Splunk Universal Forwarder**

**Prepared by:**

**Shaikh Salman**

**Cybersecurity & SOC Analyst Trainee**

# Introduction

This assignment demonstrates the practical implementation of forwarding Windows Security Logs using Splunk Universal Forwarder (UF). The aim is to collect, monitor, and analyze security event data in real time, simulating a Security Operations Center (SOC) scenario.

# Objective

To configure a Windows endpoint to forward Security Event Logs (such as logon events and privilege escalation attempts) to a central Splunk Enterprise server for centralized monitoring and alerting.

# Tools & Technologies

* Splunk Universal Forwarder (UF)
* Splunk Enterprise Server
* Windows 10/11 (Client Machine)
* TCP Port 9997 (default for Splunk forwarding)
* Configuration files: inputs.conf, outputs.conf

# Environment Setup

**Component Description**

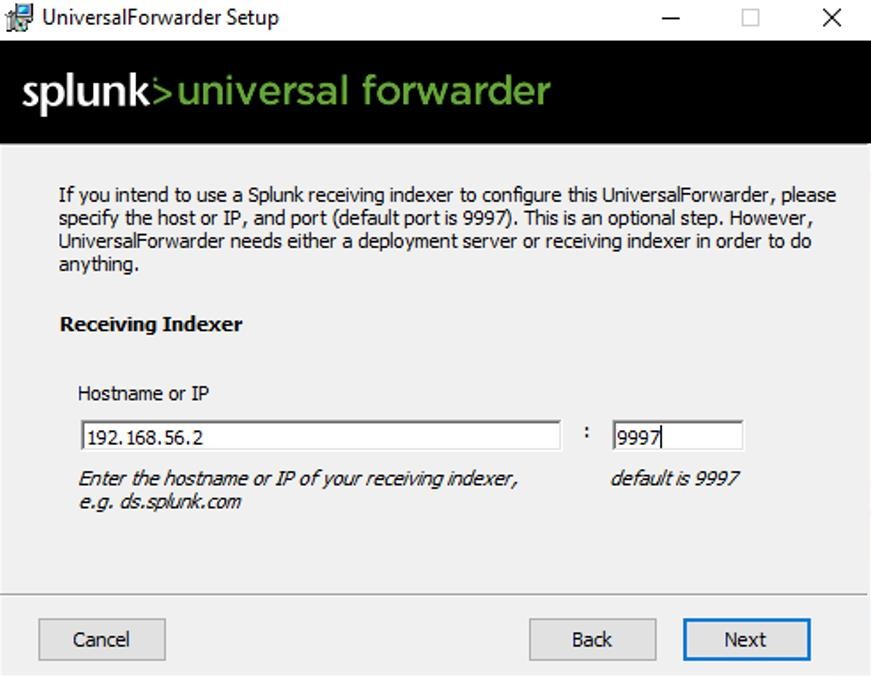
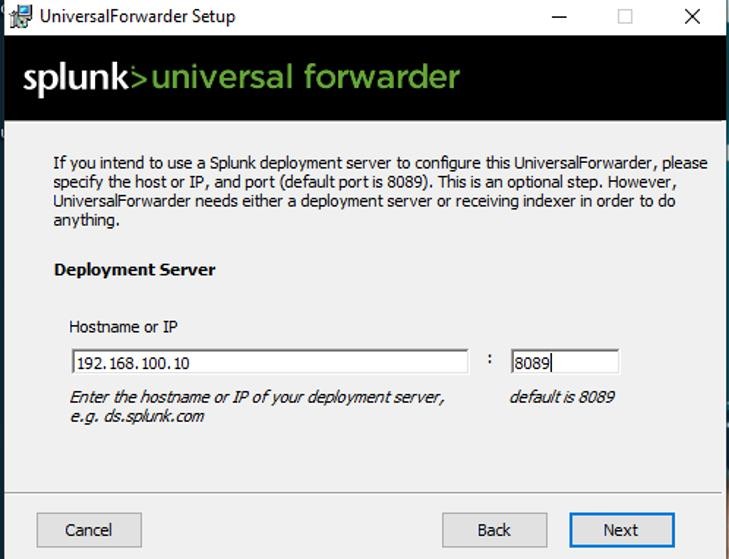
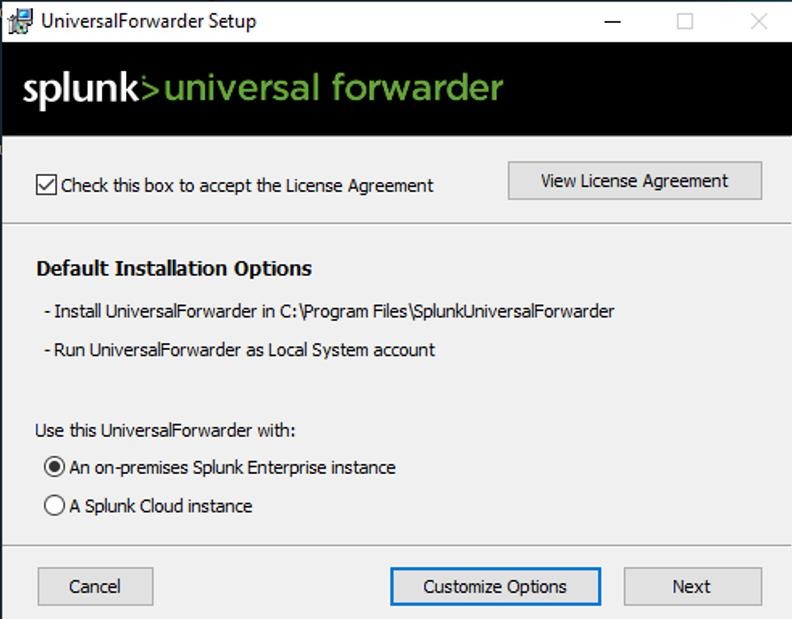
Machine A Splunk Enterprise

Machine B Windows Client with Splunk UF

# Step-by-Step Implementation

## Step 1: Install Splunk Universal Forwarder on Machine B

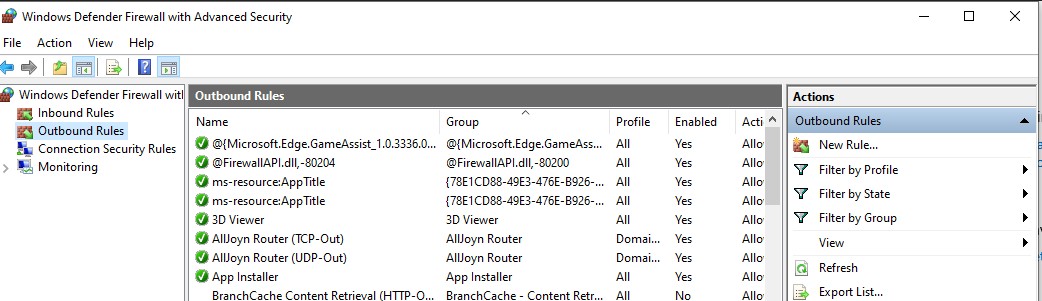
* Download from official Splunk site.
* Install as Local System user.

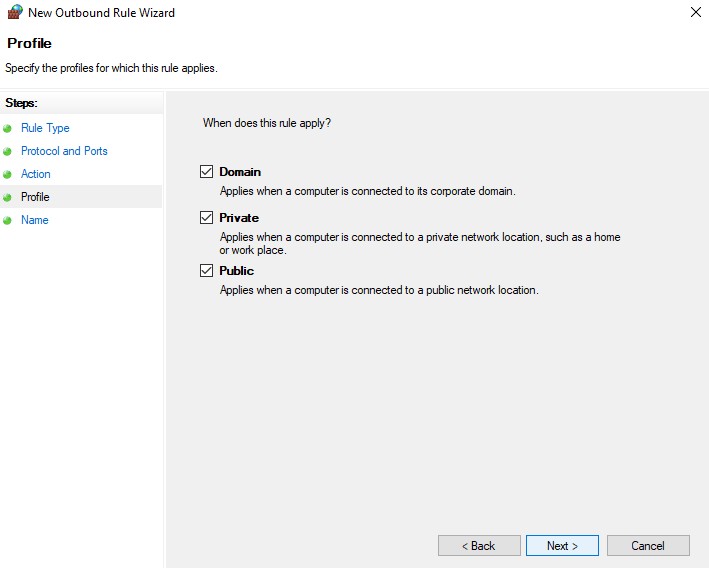
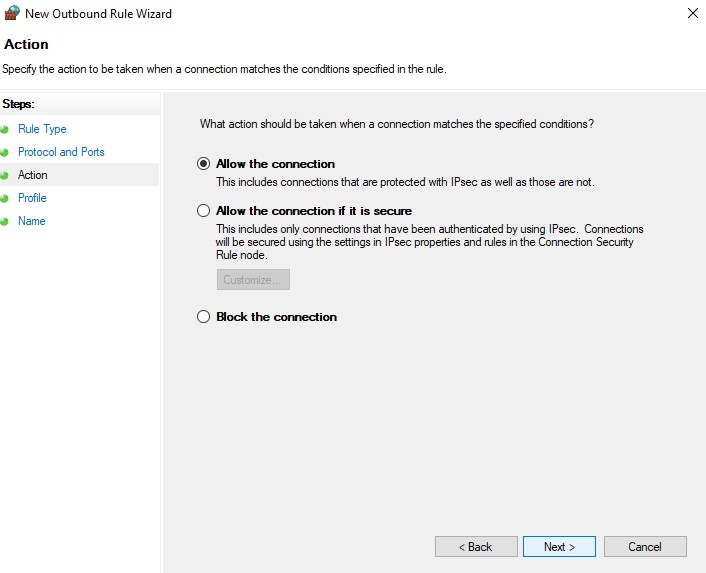
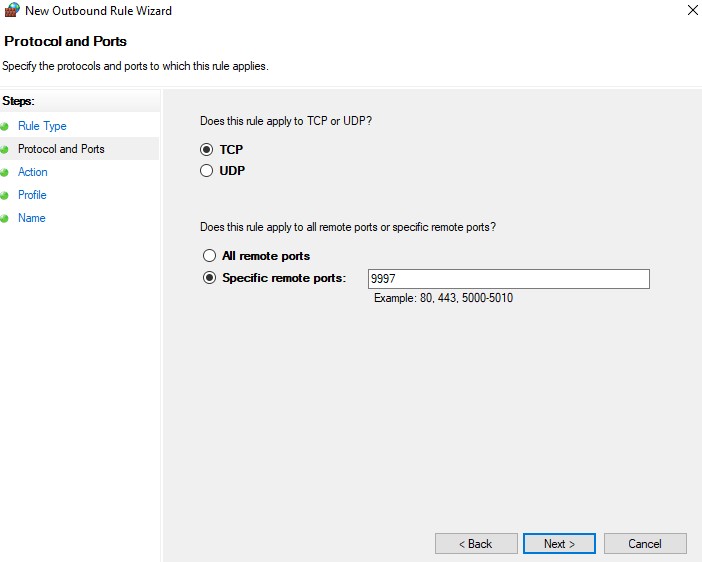
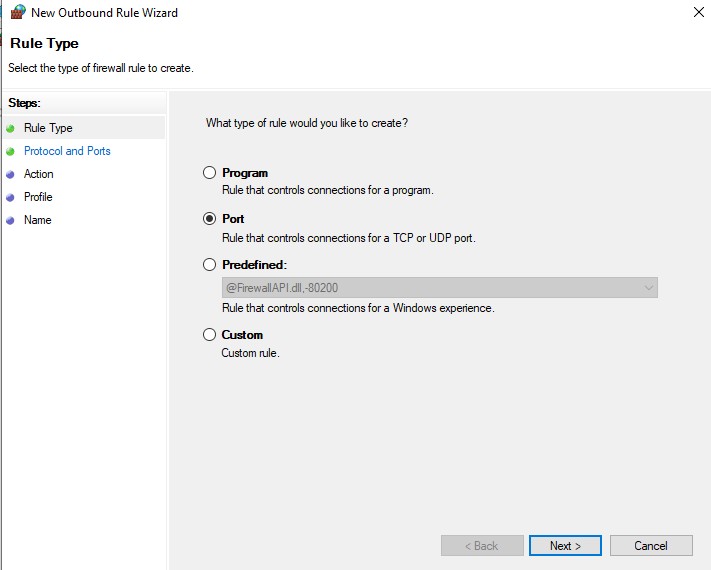


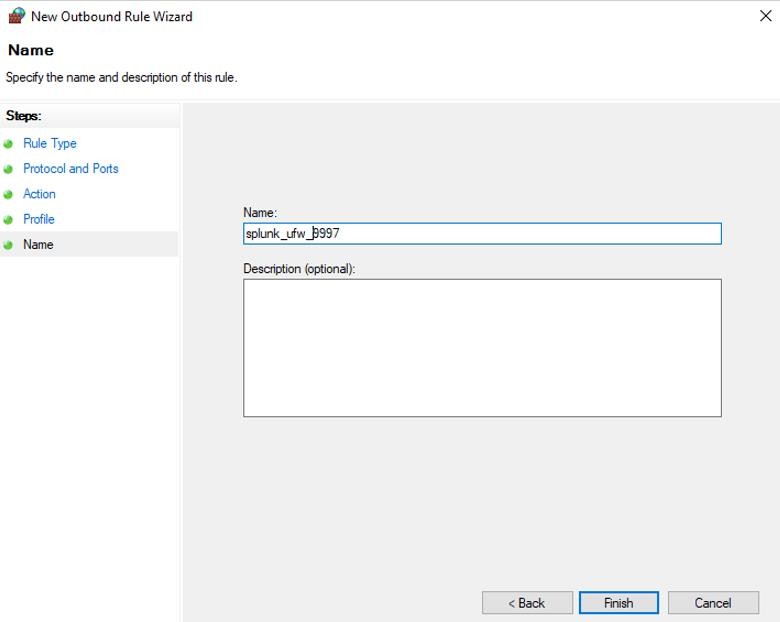
This is optional

## Step 2: Rule Creation Firewall Outbound

1. Open Windows Defender Firewall with Advanced Security
2. Go to **Outbound Rules**
3. Look for a rule that allows splunkd.exe outbound access
4. Confirm that it's enabled and targeting port 9997







## Step 3: Configure inputs.conf

Location: C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf

[

WinEventLog://Security

]

disabled = 0

index = wineventlog

]

WinEventLog://System

[

disabled = 0

index = wineventlog

WinEventLog://Application

]

[

disabled = 0

index = wineventlog

## Step 4: Configure outputs.conf

**Location:**

C:\Program Files\SplunkUniversalForwarder\etc\system\local\outputs.conf

The outputs.conf file tells the Splunk Universal Forwarder where to send the collected logs. This is critical for forwarding data to your Splunk Enterprise Indexer.

**Sample Configuration:**

[

tcpout

]

defaultGroup = default

-

autolb

-

group

efault

-

autolb

-

group]

[

tcpout:d erver

= 192.168.1.100:9997

[

tcpout

-

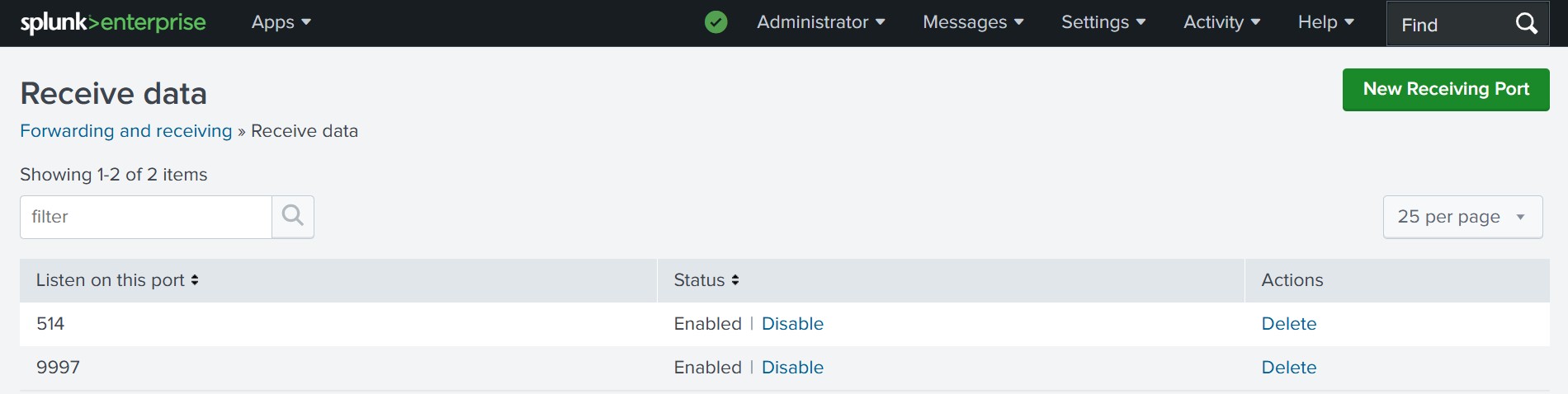
server://192.168.1.100:9997]

🔍 *Explanation:*

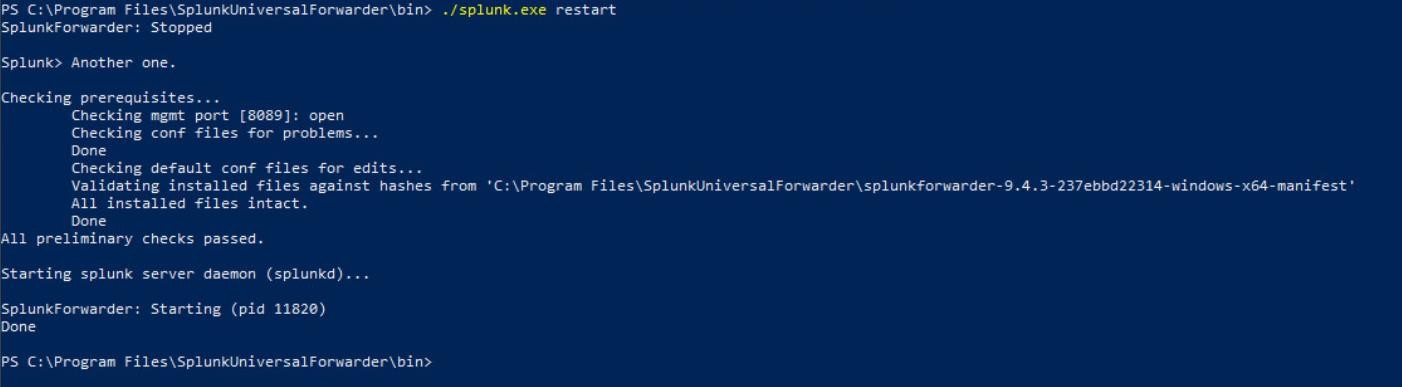
* defaultGroup defines the forwarding group to be used.
* server is the IP and port of your Splunk Enterprise (receiver/indexer).
* TCP port 9997 is the default receiving port for forwarders.

## Step 5: Enable Receiving on Splunk Enterprise

 Navigate to Splunk Web > Settings > Forwarding and receiving > Configure receiving > Add port 9997.



## Step 6: Restart Splunk UF



# Validation

To confirm the successful setup of Splunk Universal Forwarder and validate that security logs are being forwarded from the client machine to the Splunk Enterprise server, the following steps were performed:

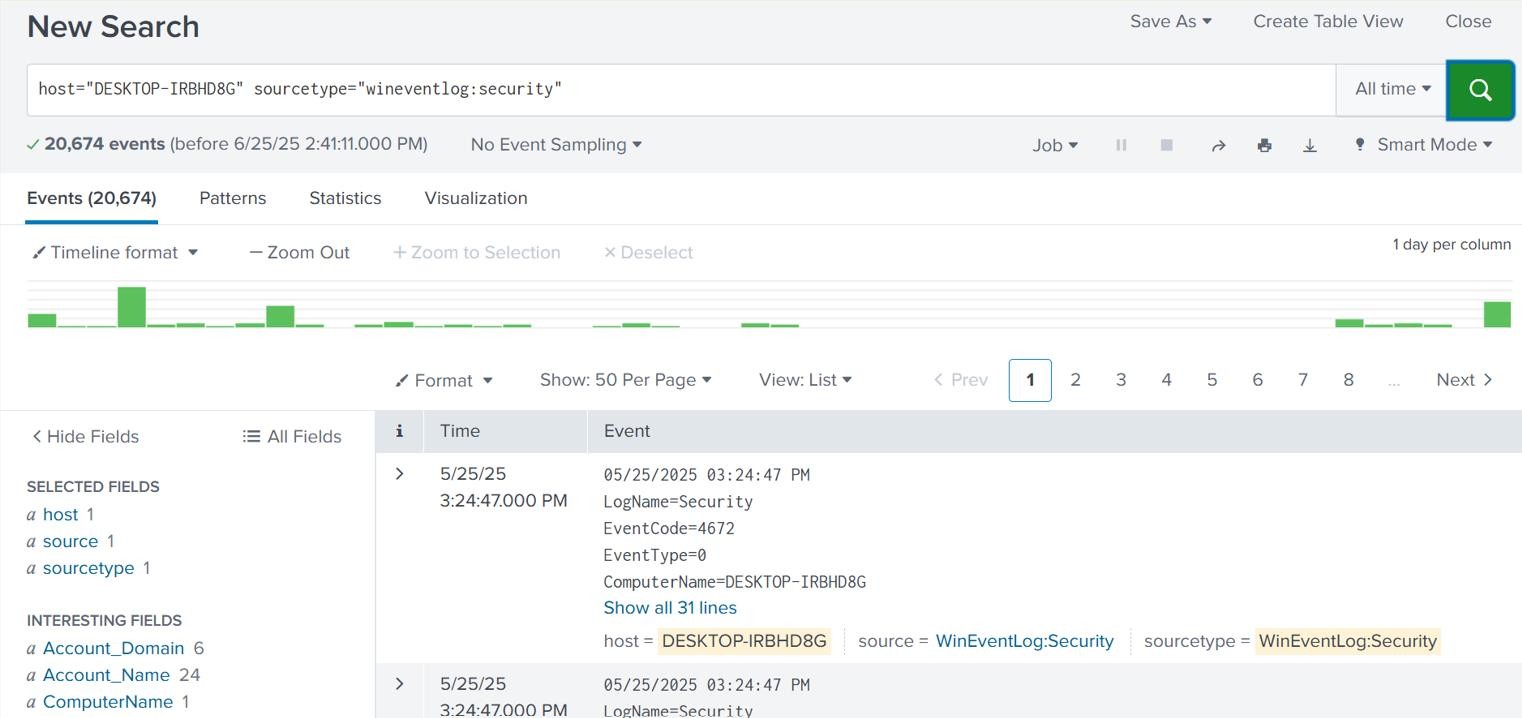
✔️ Step 1: Generate Events

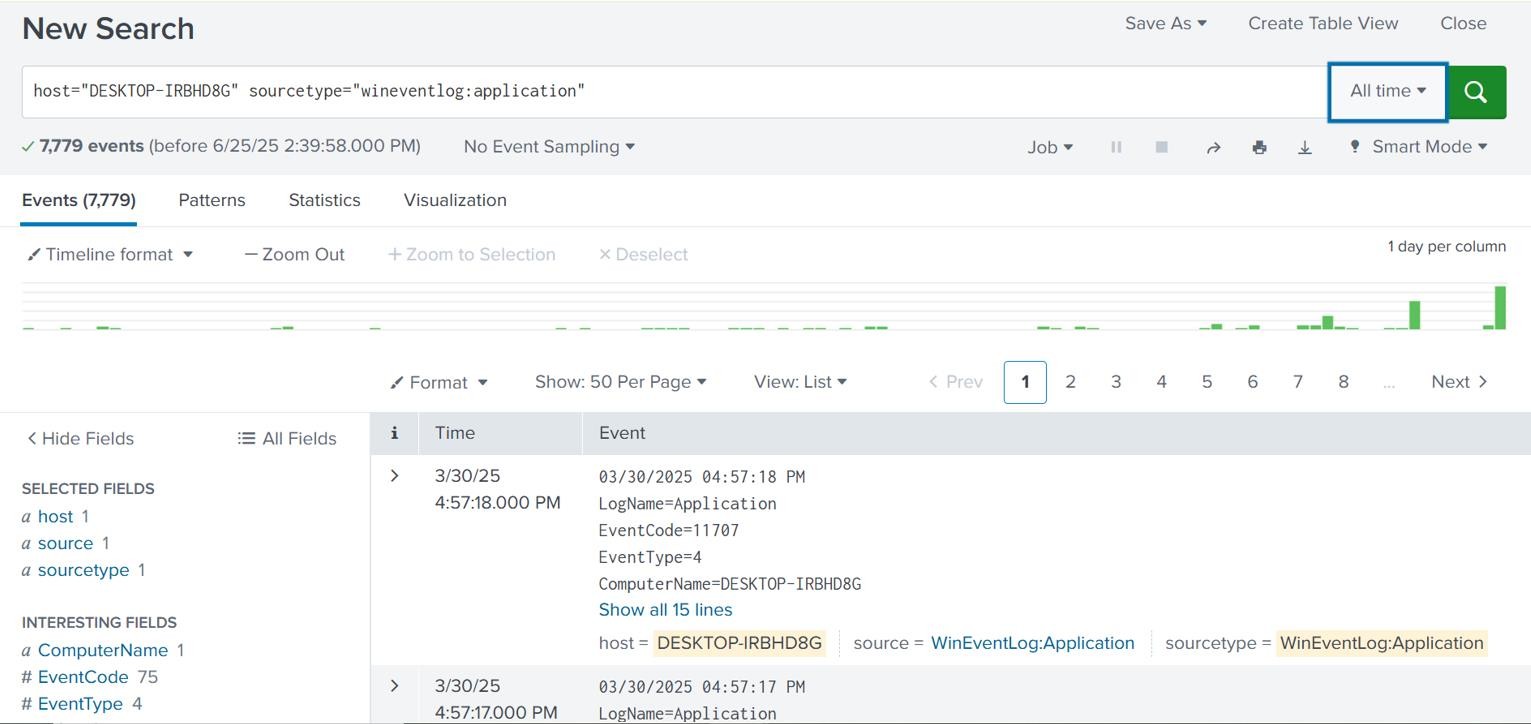
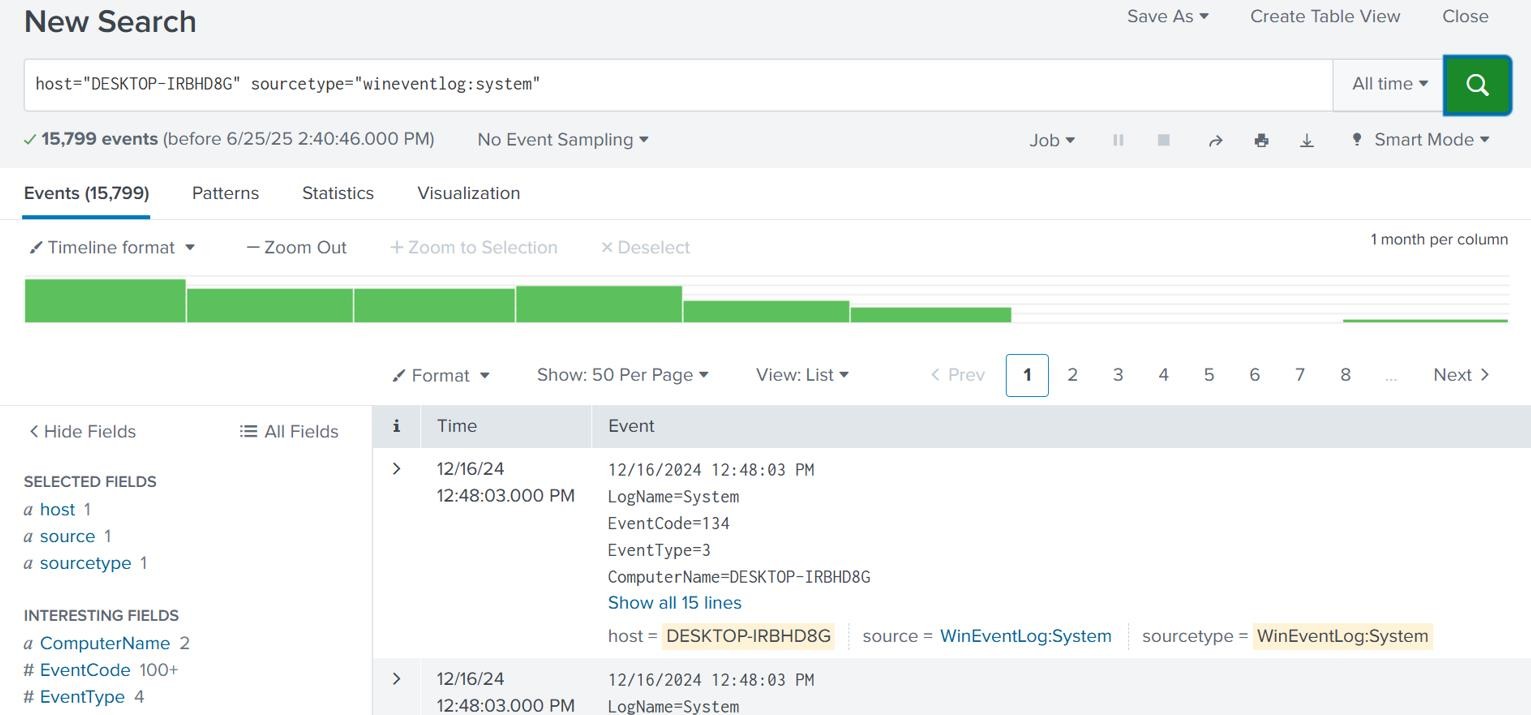
 User logon activity was simulated on the client machine (Machine B) to trigger Security EventCodes such as 4624 (successful logon) and 4672 (special privilege assignment).

✔️ Step 2: Run Search Query in Splunk Web

A search query was executed from Splunk Enterprise using the following syntax:

host="DESKTOP-IRBHD8G" sourcetype="WinEventLog:Security" host="DESKTOP-IRBHD8G" sourcetype="WinEventLog:System" host="DESKTOP-IRBHD8G" sourcetype="WinEventLog:Application"





screenshot of the Splunk Search UI confirms:

* Indexed log source: WinEventLog:Security/System/application
* Hostname: DESKTOP-IRBHD8G
* Relevant EventCodes such as 4672 were visible
* Timeline activity confirms continuous data flow

**Outcome**

* Successfully forwarded Windows Security Logs to Splunk.
* Verified real-time log ingestion and indexing.
* Demonstrated essential SOC monitoring use case.

# Conclusion

This project provides foundational skills in log forwarding and centralized monitoring. It demonstrates a key SOC analyst competency—setting up reliable log pipelines using Splunk.