Windows Security Log Monitoring with Splunk Universal Forwarder

Prepared by:
Faizanullah Syed
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

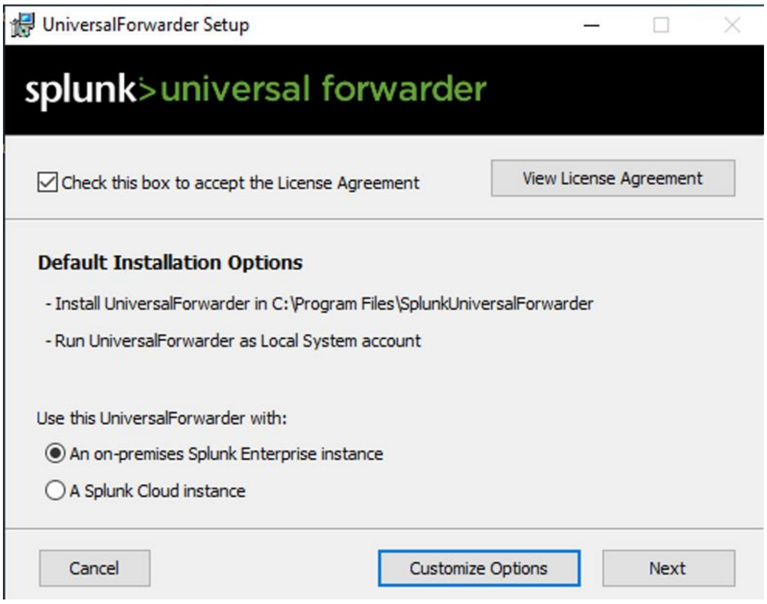
Environment Setup

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.



☑ Check this box to accept the License Agreement

Default Installation Options

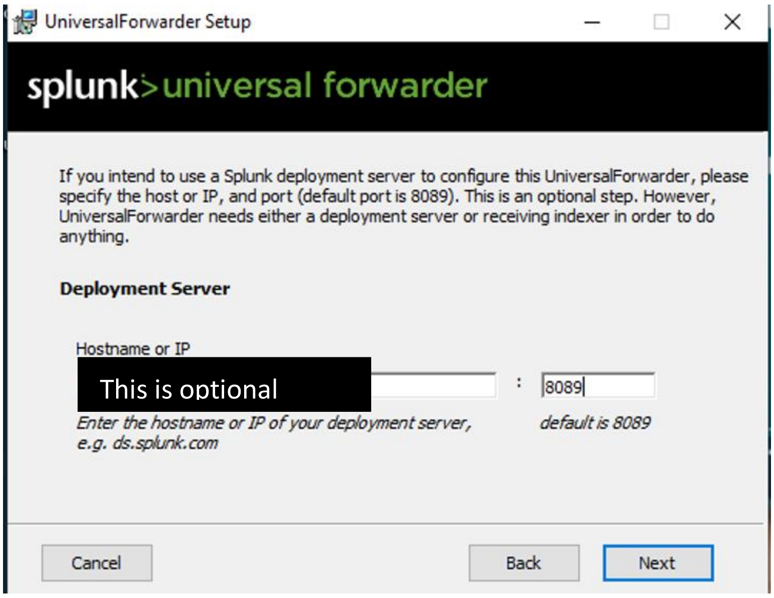
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder

- Run UniversalForwarder as Local System account

Use this UniversalForwarder with:

● An on-premises Splunk Enterprise instance

○ A Splunk Cloud instance



If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

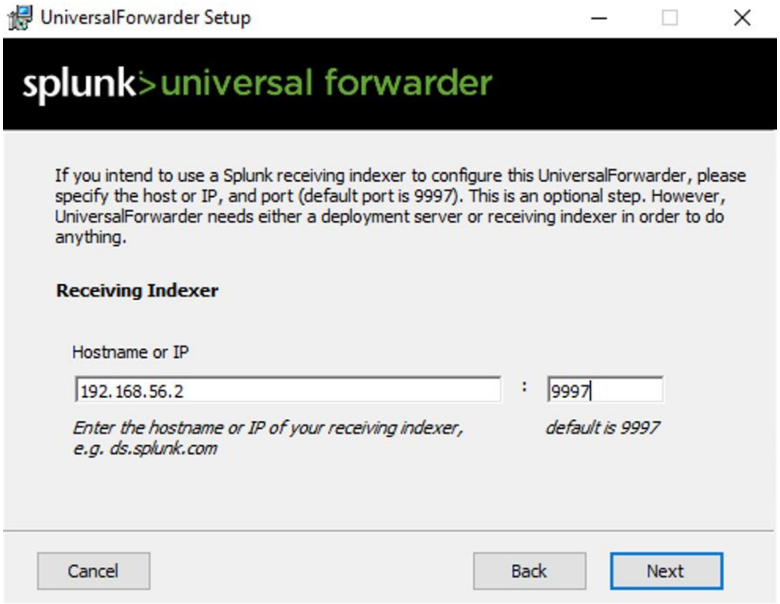
Hostname or IP

This is optional

: 8089

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com

default is 8089



If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP

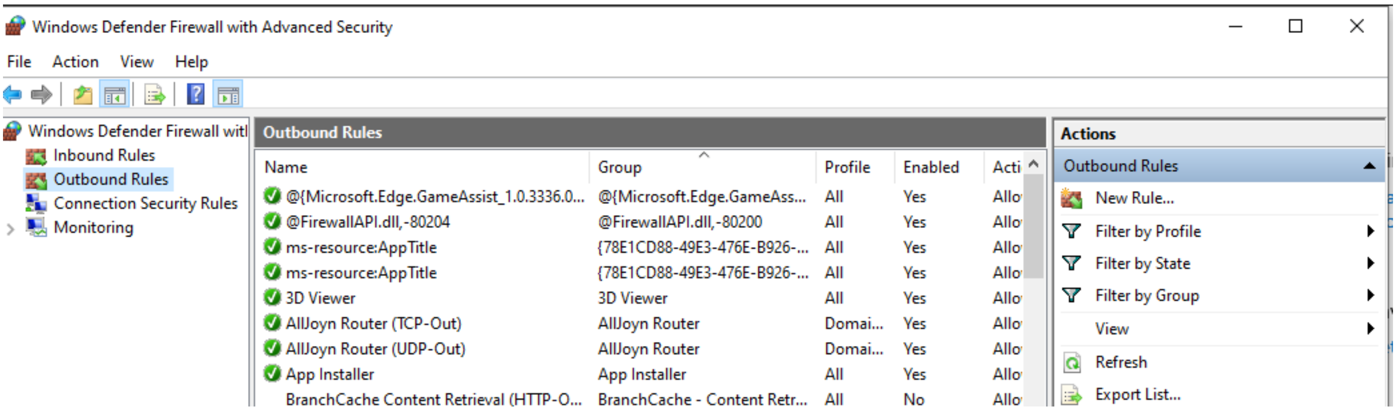
192.168.56.2 : 9997

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com

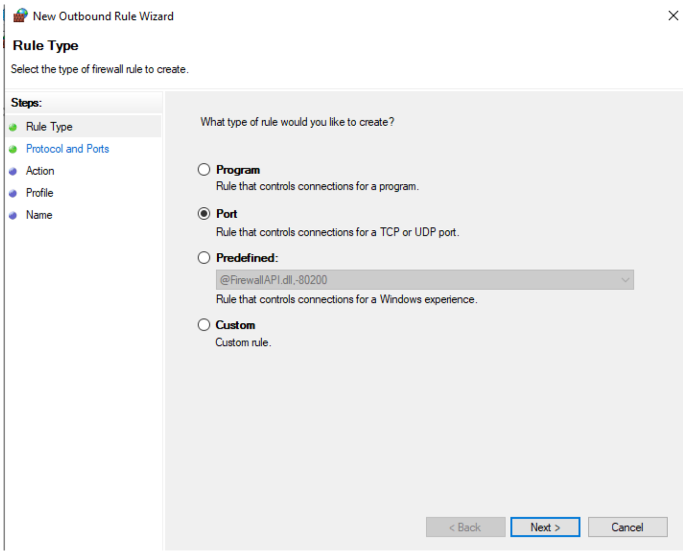
default is 9997

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`



Name	Group	Profile	Enabled	Acti
✓ @{Microsoft.Edge.GameAssist_1.0.3336.0...	@{Microsoft.Edge.GameAss...	All	Yes	Allo
✓ @FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes	Allo
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allo
✓ ms-resource:AppTitle	{78E1CD88-49E3-476E-B926-...	All	Yes	Allo
✓ 3D Viewer	3D Viewer	All	Yes	Allo
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allo
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allo
✓ App Installer	App Installer	All	Yes	Allo
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allo



Rule Type

Select the type of firewall rule to create.

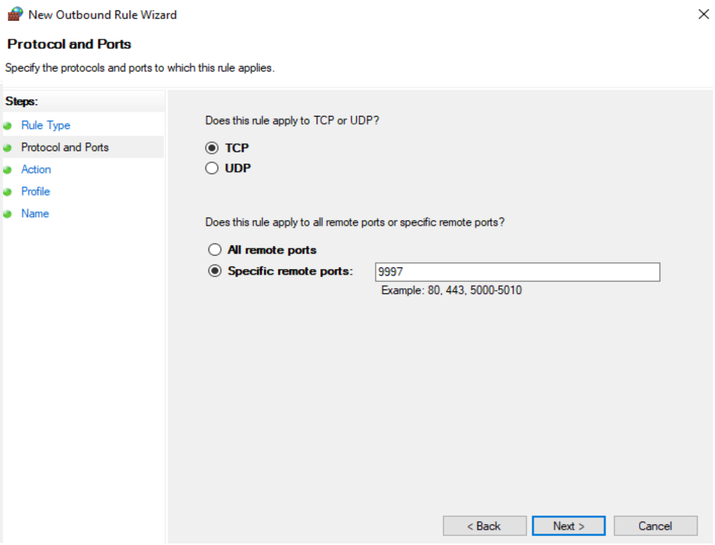
What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.



Protocol and Ports

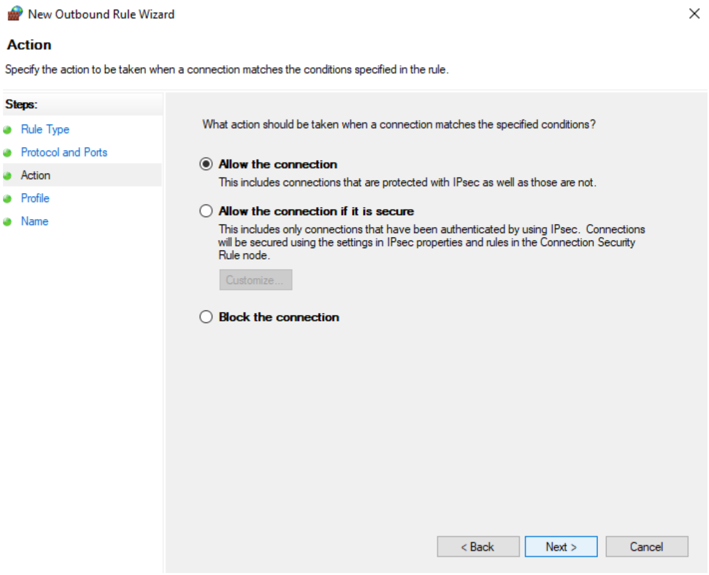
Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all remote ports or specific remote ports?

○ **All remote ports**
● **Specific remote ports:** 9997
Example: 80, 443, 5000-5010



Action

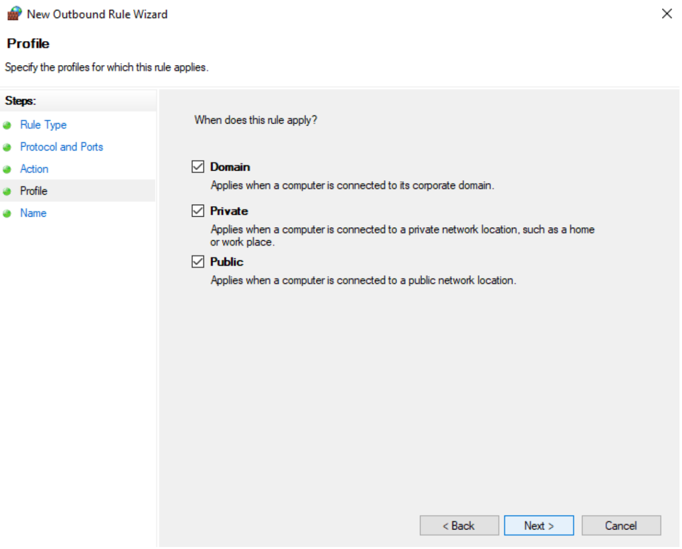
Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**



Profile

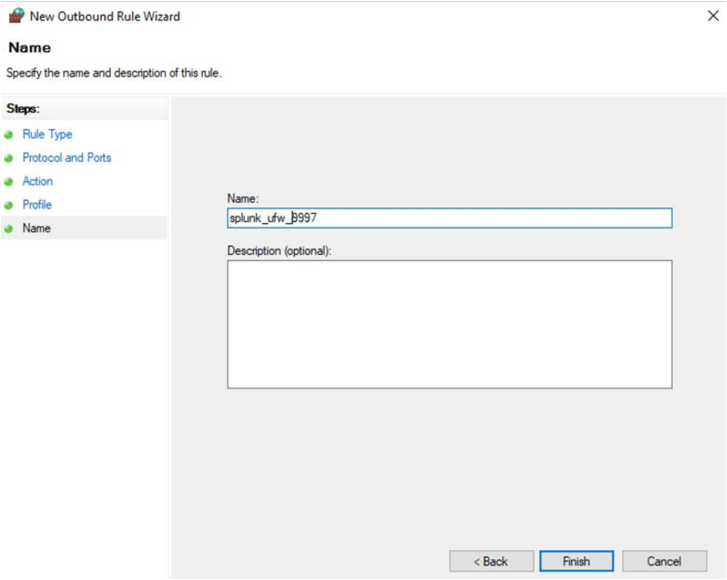
Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.



New Outbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: splunk_ufw_9997

Description (optional):

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:

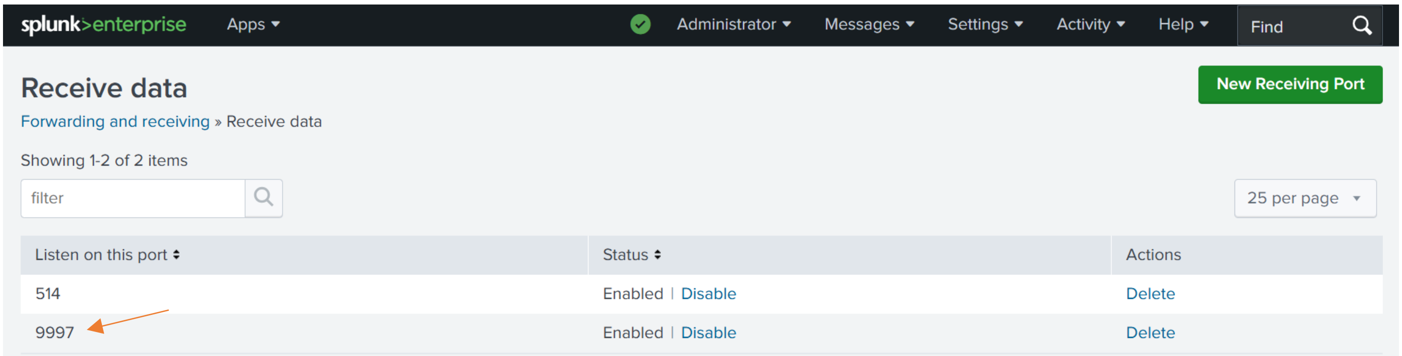
```
[tcpout]

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.



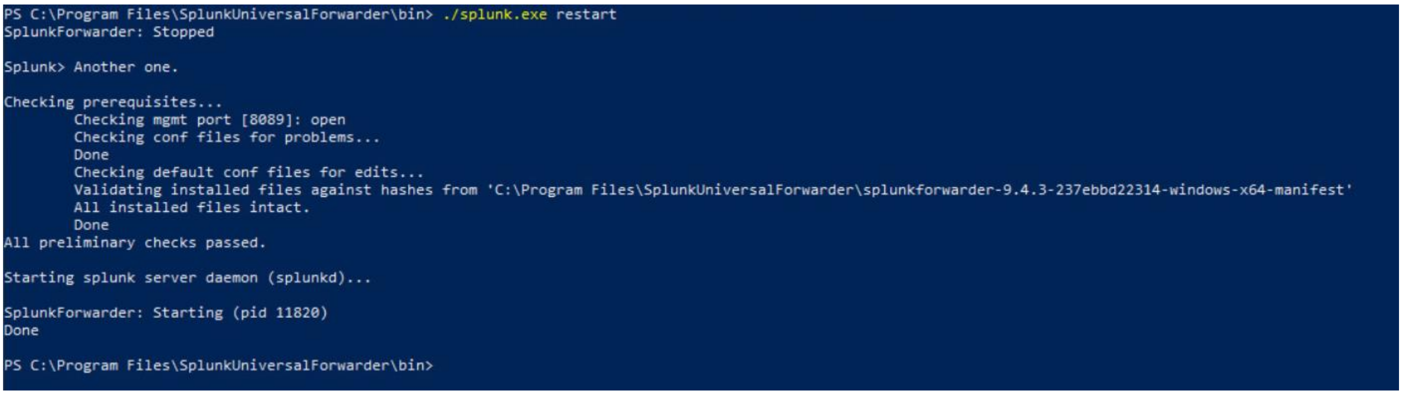
Receive data

Forwarding and receiving » Receive data

Showing 1-2 of 2 items

Listen on this port ⬍	Status ⬍	Actions
514	Enabled | Disable	Delete
9997	Enabled | Disable	Delete

Step 6: Restart Splunk UF



```
PS C:\Program Files\SplunkUniversalForwarder\bin> ./splunk.exe restart
SplunkForwarder: Stopped

Splunk> Another one.

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from 'C:\Program Files\SplunkUniversalForwarder\splunkforwarder-9.4.3-237ebbd22314-windows-x64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

SplunkForwarder: Starting (pid 11820)
Done

PS C:\Program Files\SplunkUniversalForwarder\bin>
```

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:

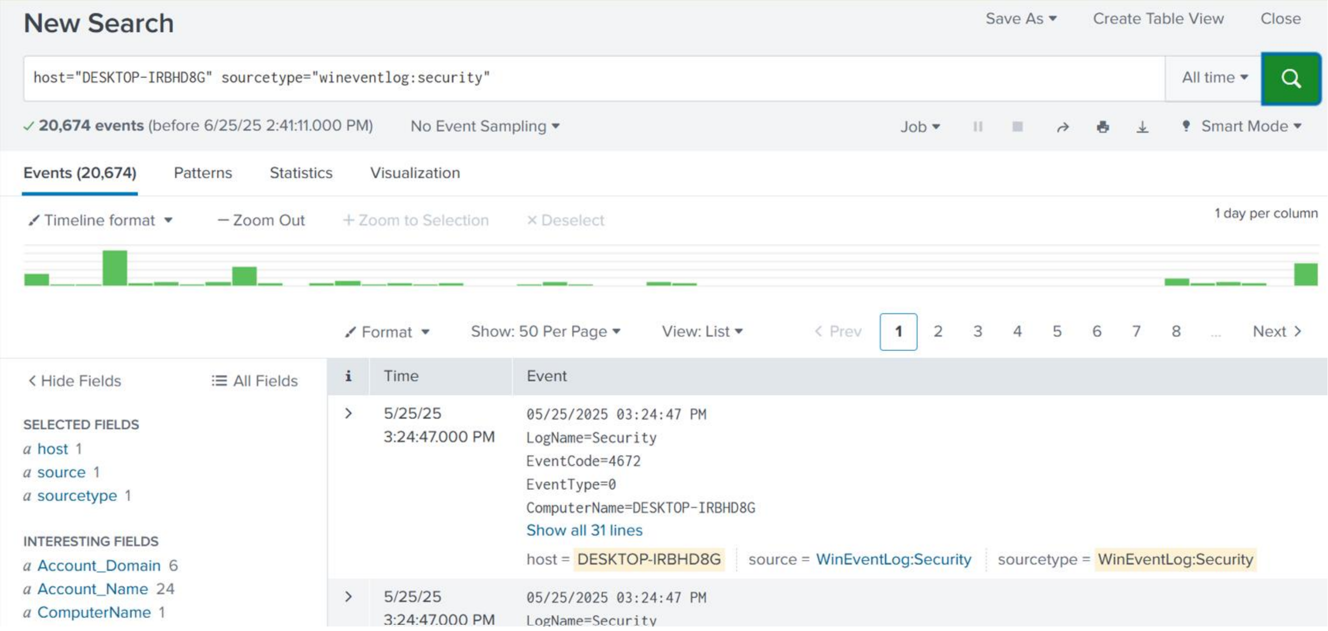
✓ Step 1: Generate Events

- 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"
```



```
host="DESKTOP-IRBHD8G" sourcetype="wineventlog:security"
```

✓ 20,674 events (before 6/25/25 2:41:11.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 6
a Account_Name 24
a ComputerName 1

> 5/25/25 3:24:47.000 PM

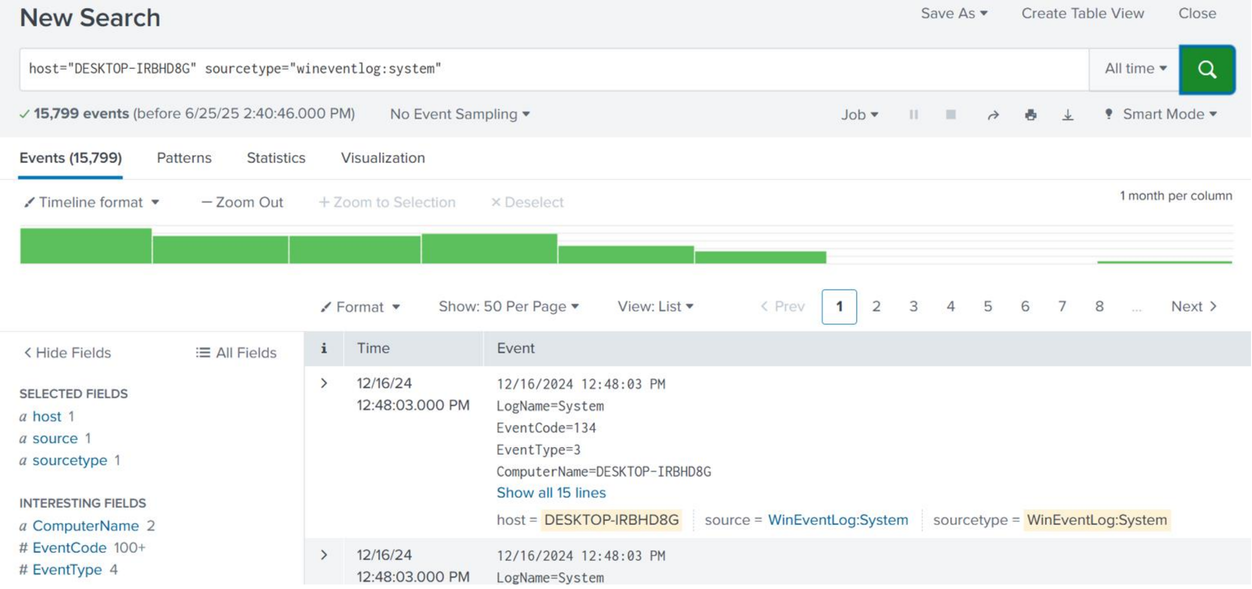
```
05/25/2025 03:24:47 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=DESKTOP-IRBHD8G
```

Show all 31 lines

host = DESKTOP-IRBHD8G | source = WinEventLog:Security | sourcetype = WinEventLog:Security

> 5/25/25 3:24:47.000 PM

```
05/25/2025 03:24:47 PM
LogName=Security
```



```
host="DESKTOP-IRBHD8G" sourcetype="wineventlog:system"
```

✓ 15,799 events (before 6/25/25 2:40:46.000 PM)

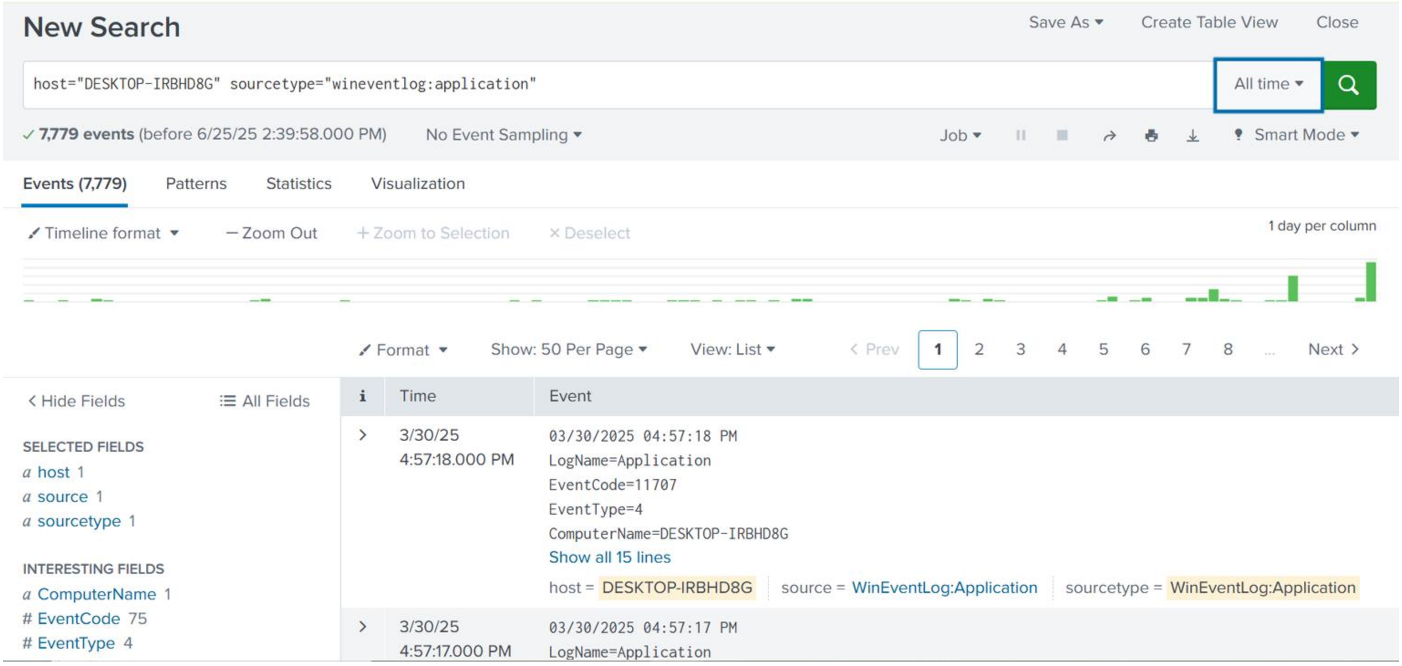
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a ComputerName 2
EventCode 100+
EventType 4

Time	Event

12/16/24
12:48:03.000 PM
	12/16/2024 12:48:03 PM
	LogName=System
	EventCode=134
	EventType=3
	ComputerName=DESKTOP-IRBHD8G
	Show all 15 lines
	host = DESKTOP-IRBHD8G source = WinEventLog:System sourcetype = WinEventLog:System

12/16/24 12:48:03.000 PM	12/16/2024 12:48:03 PM LogName=System



```
host="DESKTOP-IRBHD8G" sourcetype="wineventlog:application"
```

✓ 7,779 events (before 6/25/25 2:39:58.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a ComputerName 1
EventCode 75
EventType 4

Time	Event

3/30/25
4:57:18.000 PM
	03/30/2025 04:57:18 PM
	LogName=Application
	EventCode=11707
	EventType=4
	ComputerName=DESKTOP-IRBHD8G
	Show all 15 lines
	host = DESKTOP-IRBHD8G source = WinEventLog:Application sourcetype = WinEventLog:Application

3/30/25 4:57:17.000 PM	03/30/2025 04:57:17 PM LogName=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.