

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.

UniversalForwarder Setup

splunk>universal forwarder

☒ Check this box to accept the License Agreement [View 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

[Cancel](#) [Customize Options](#) [Next](#)

UniversalForwarder Setup

splunk>universal forwarder

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*

[Cancel](#) [Back](#) [Next](#)

UniversalForwarder Setup

splunk>universal forwarder

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

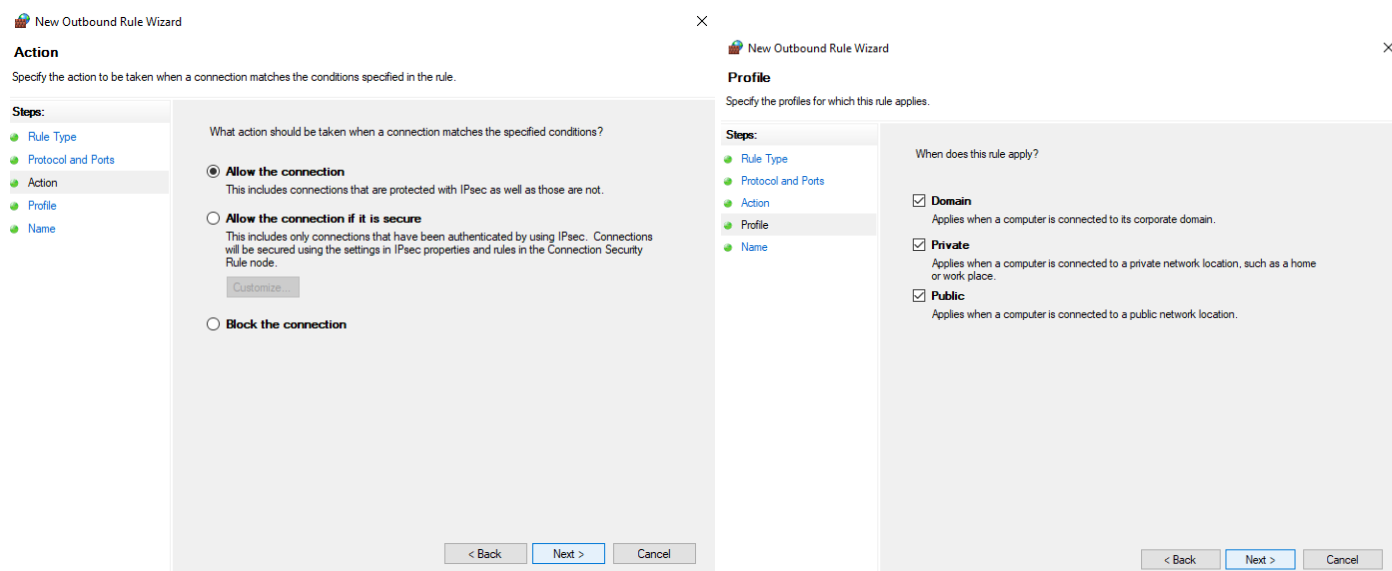
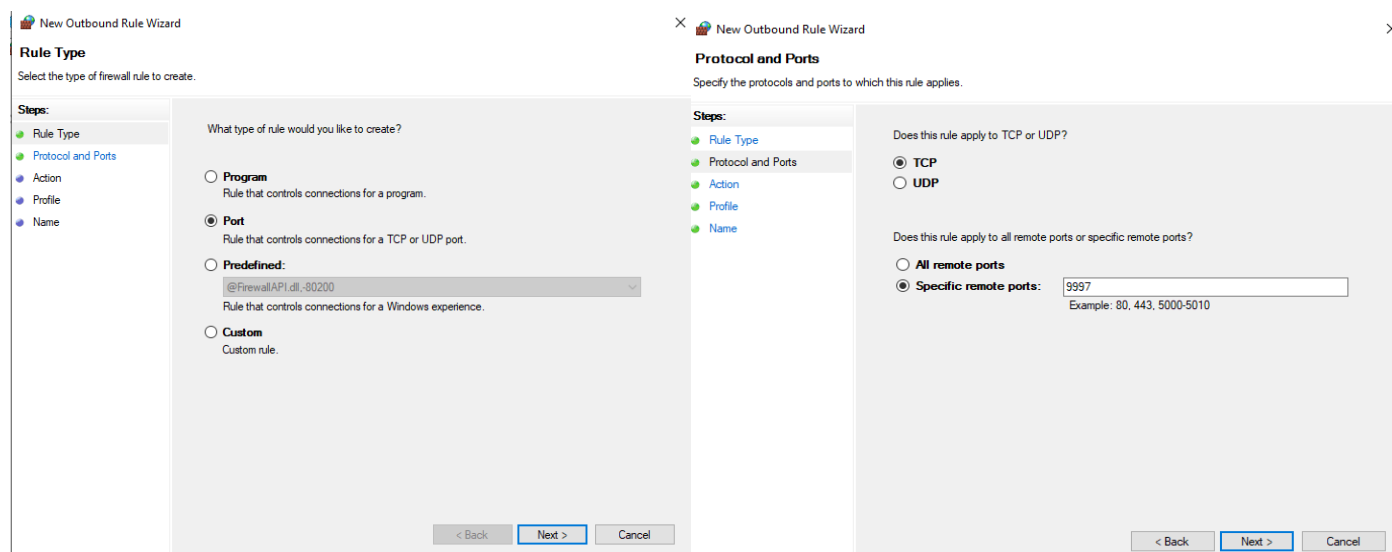
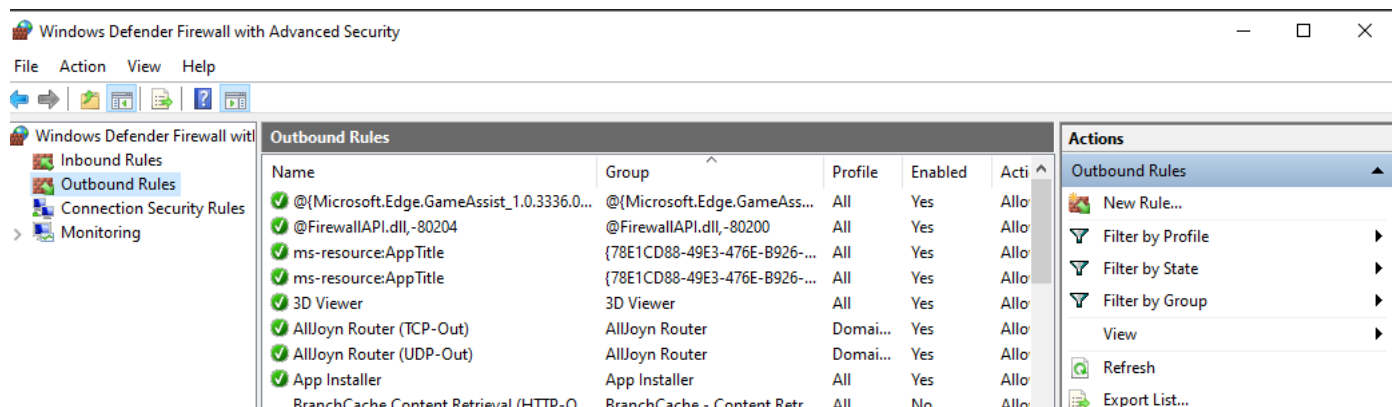
192.168.56.2 : 9997

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

[Cancel](#) [Back](#) [Next](#)

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



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):

< Back Finish Cancel

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
```

```
default-autolb-group]
```

```
s
```

```
[tcpout:default-server = 192.168.1.100:9997
```

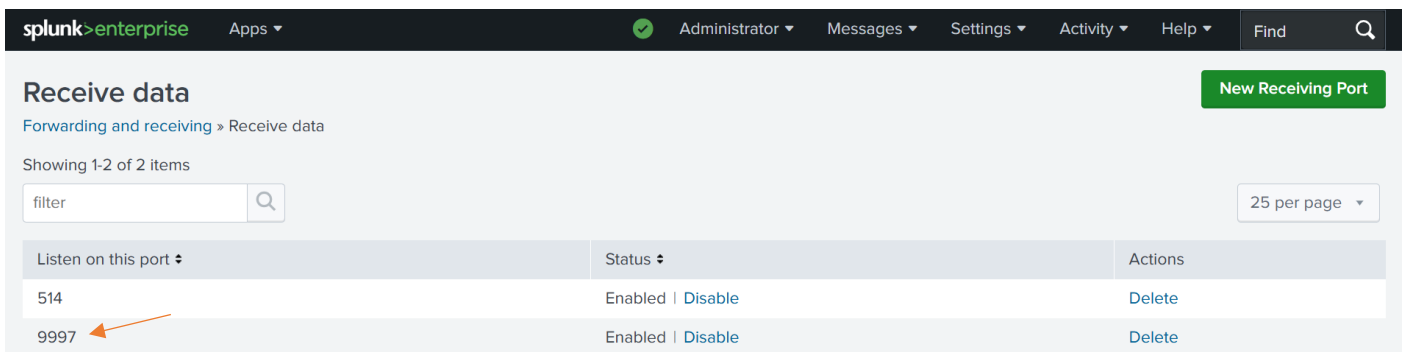
```
[tcpout-server://192.168.1.100:9997]
```



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.




splunk>enterprise Apps ▾  Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 

Receive data

Forwarding and receiving » Receive data

Showing 1-2 of 2 items

filter  25 per page ▾

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"
```

New Search Save As Create Table View Close

host="DESKTOP-IRBHD8G" sourcetype="wineventlog:security" All time 🔍

✓ 20,674 events (before 6/25/25 2:41:11.000 PM) No Event Sampling Job ⌵ ⏸ ⏹ ↶ ⏴ ⏵ ⏷ ⚙ Smart Mode ⌵

Events (20,674) Patterns Statistics Visualization

Timeline format ⌵ Zoom Out Zoom to Selection Deselect 1 day per column

Format ⌵ Show: 50 Per Page ⌵ View: List ⌵ < Prev 1 2 3 4 5 6 7 8 ... Next >

i	Time	Event
>	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

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 6
a Account_Name 24
a ComputerName 1

New Search

Save As ▾ Create Table View Close

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

All time ▾ 🔍

✓ 15,799 events (before 6/25/25 2:40:46.000 PM) No Event Sampling ▾

Job ▾ || ▣ ↶ ↷ ⬇ ⚡ Smart Mode ▾

Events (15,799)

Patterns

Statistics

Visualization

Timeline format ▾

— Zoom Out

+ Zoom to Selection

× Deselect

1 month per column

Format ▾

Show: 50 Per Page ▾

View: List ▾

< Prev

1

2

3

4

5

6

7

8

...

Next >

< Hide Fields

☰ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a ComputerName 100+

EventCode 100+

EventType 4

i	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

New Search

Save As

Create Table View

Close

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

All time

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

No Event Sampling

Job

Smart Mode

Events (20,674)

Patterns

Statistics

Visualization

Timeline format

Zoom Out

Zoom to Selection

Deselect

1 day per column

Format

Show: 50 Per Page

View: List

Prev

1

2

3

4

5

6

7

8

...

Next

Hide Fields

All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Account_Domain 6

a Account_Name 24

a ComputerName 1

	Time	Event
>	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

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.