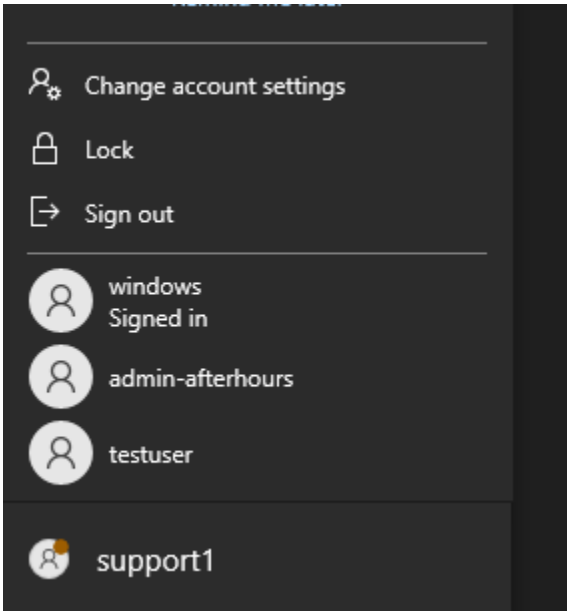
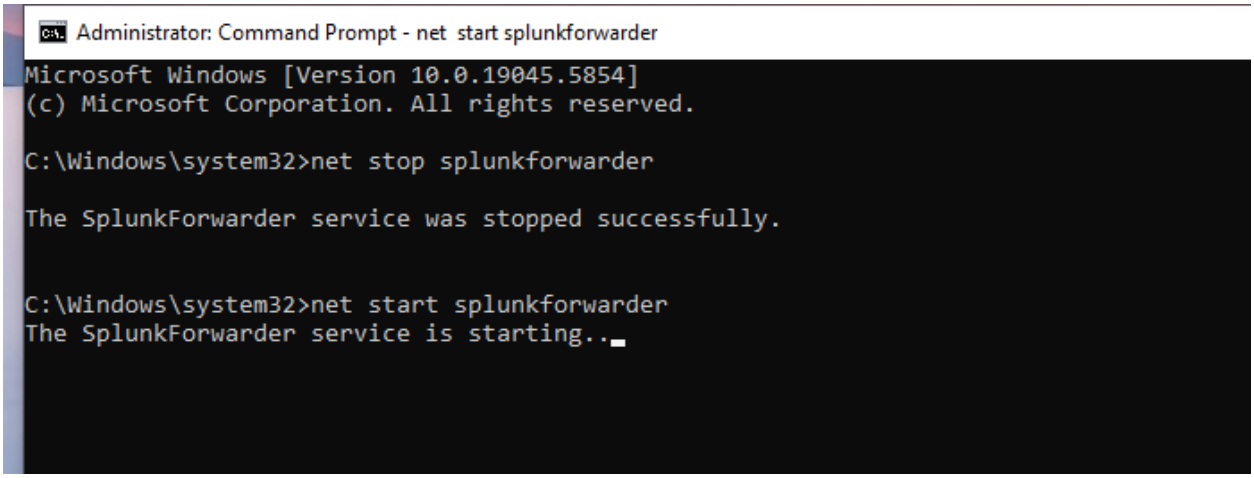
Scenario 5: Hidden User Account Creation (T1136)

1. Create new windows account:
    a. net user support1 Password123! /add
    b. net localgroup administrators support1 /add

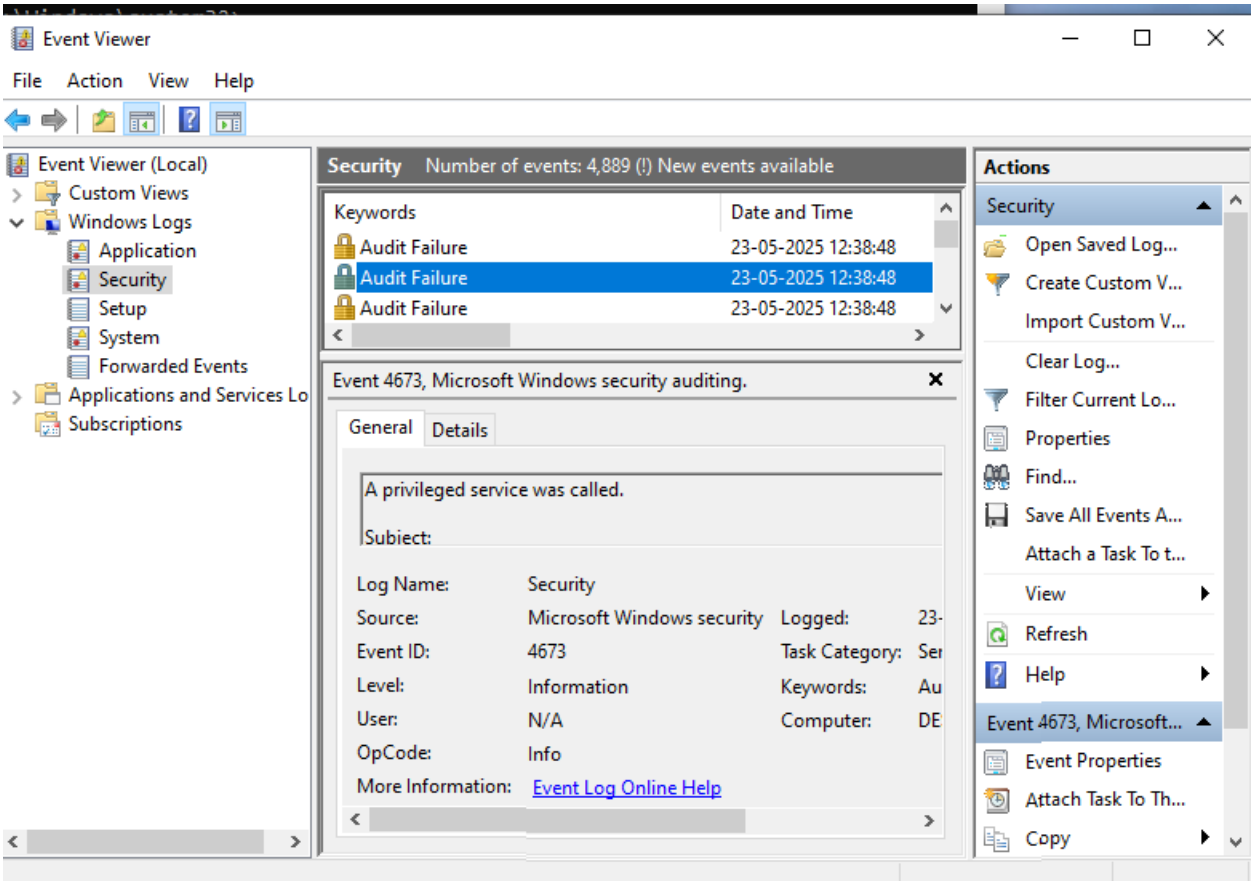


2. Enable Auditing on Windows (if not already):
    a. auditpol /set /category:"Account Management" /success:enable /failure:enable
        i. This ensures Event IDs 4720, 4728, and 4732 are logged.

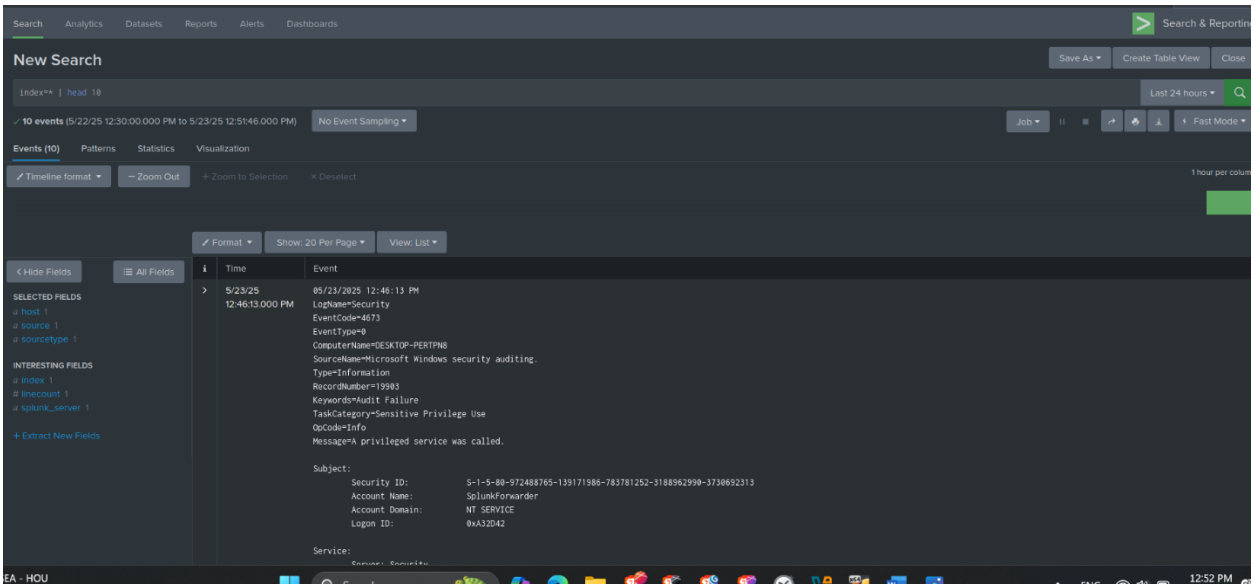
3. Configure and Forward Logs to Splunk
    a. Use **Universal Forwarder** on Windows 10
        i. Download and install Splunk Universal Forwarder on Windows 10.
        ii. During setup, input the Splunk server IP (Ubuntu machine) and receiver port (default is 9997).
        iii. Choose to forward Security Logs.
        iv. Restart the forwarder:
            1. net stop splunkforwarder
            2. net start splunkforwarder

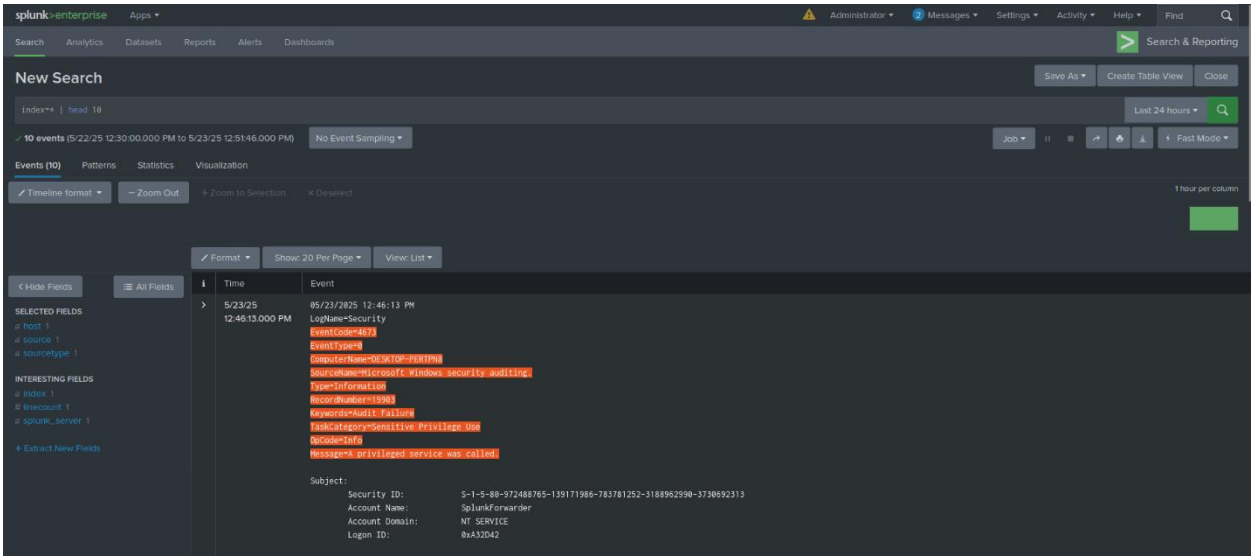


4. Verify Events in Windows Event Viewer
    a. **Event Viewer** → Windows Logs → **Security**
        i. Event ID 4720: A new account was created.
        ii. Event ID 4728 or 4732: The account was added to a privileged group.



5. Detect in Splunk (Ubuntu):
    a. index=wineventlog | head 10





Here are some powerful use cases you can start with:

Goal	Event Code	Description
Detect user creation	`4720`	New user account created
Detect group addition	`4728` , `4732`	User added to group
Detect login attempts	`4624` , `4625`	Successful/failed logins
Detect privilege use	`4670` , `4672`	Admin privilege use

This is multiple logs in few seconds: