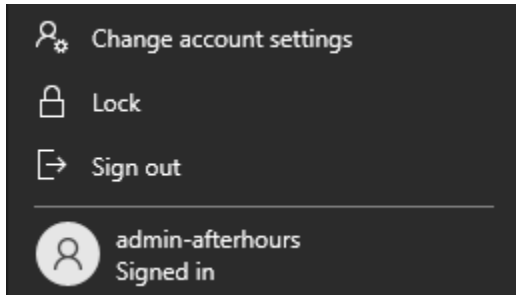


### ### ✅ Step 1: Create an Admin Account on Windows

powershell

```
net user "admin-afterhours" "SecurePass123" /add
```



### ✅ Step 2: Simulate After-Hours Login

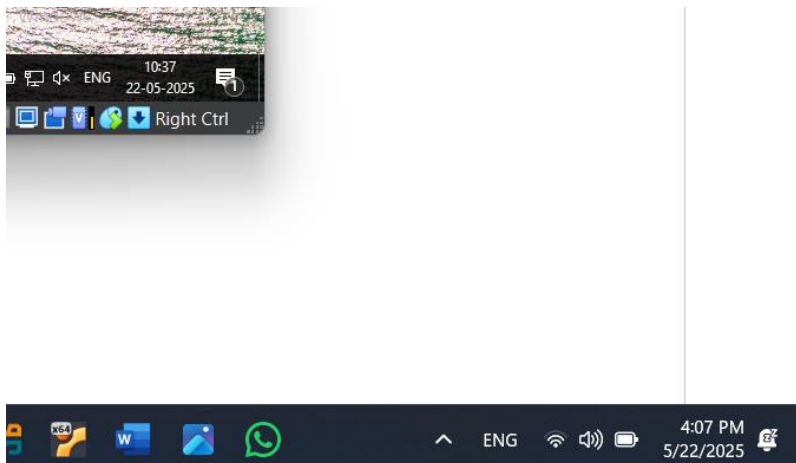
Temporarily change system time to 2:30 AM for testing:

cmd

CopyEdit

time 02:30:00

⚠️ Reset system time after test.



### Step 3: Perform Suspicious Activity

While logged in as admin-afterhours, access critical folders:

- C:\Users\Administrator\Documents
- C:\Windows\System32\config\

Use PowerShell to interact with services:

#### **Step 4: Ensure Log Forwarding to Splunk**

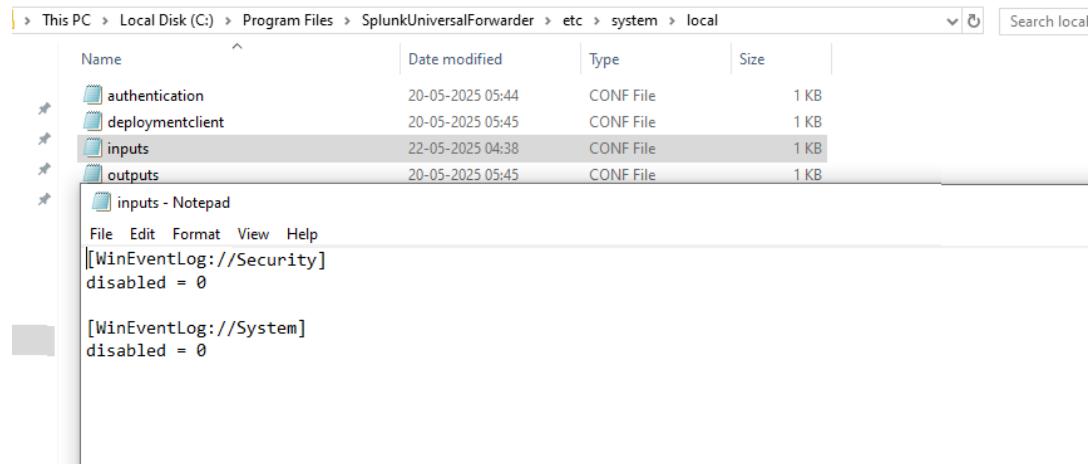
Verify the **Splunk Universal Forwarder** is installed on Windows 10 and configured to send logs.

Check the config:

perl

CopyEdit

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



The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Program Files > SplunkUniversalForwarder > etc > system > local'. The file list shows four files: 'authentication', 'deploymentclient', 'inputs', and 'outputs', all of which are 'CONF File' types and 1 KB in size. The 'inputs' file is selected. Below the file list, a Notepad window titled 'inputs - Notepad' is open, displaying the following configuration:

```
File Edit Format View Help
[WinEventLog://Security]
disabled = 0

[WinEventLog://System]
disabled = 0
```

## Step 5: Splunk Detection Query

Login to Splunk Web Interface (<http://localhost:8000>) and use this query:

spl

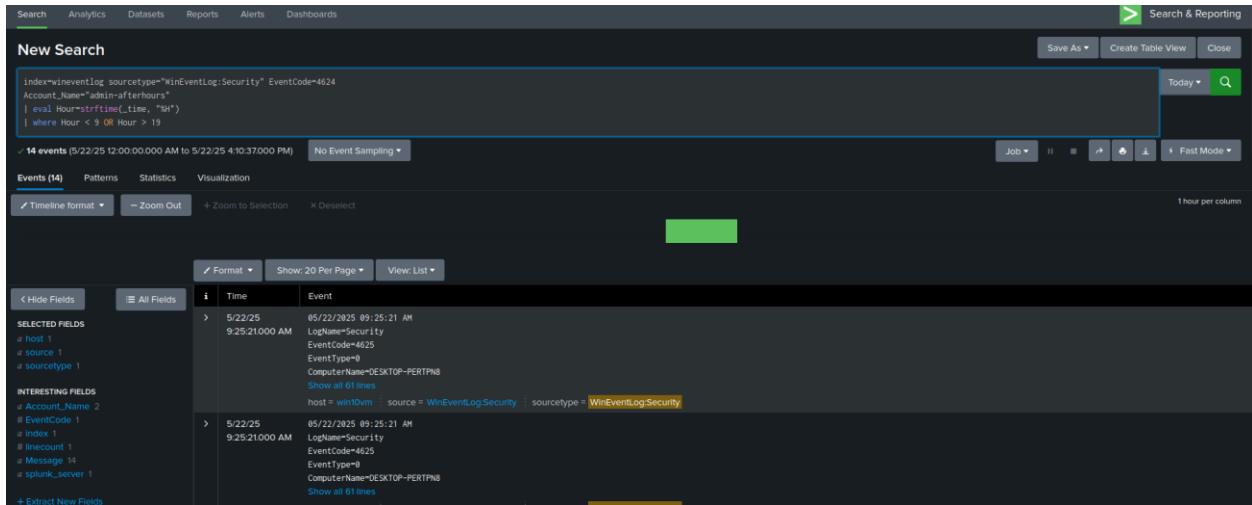
CopyEdit

```
index=wineventlog sourcetype="WinEventLog:Security" EventCode=4624
```

```
Account_Name="admin-afterhours"
```

```
| eval Hour=strftime(_time, "%H")
```

```
| where Hour < 9 OR Hour > 19
```



The screenshot shows the Splunk Web Interface with a search query entered in the 'New Search' bar. The query is: `index=wineventlog sourcetype="WinEventLog:Security" EventCode=4624 Account_Name="admin-afterhours" | eval Hour=strftime(_time, "%H") | where Hour < 9 OR Hour > 19`. The search results show 14 events. The first event is from 5/22/25 12:00:00.000 AM to 5/22/25 4:10:37.000 PM. The second event is from 5/22/25 09:25:21.000 AM to 5/22/25 09:25:21.000 AM. The third event is from 5/22/25 09:25:21.000 AM to 5/22/25 09:25:21.000 AM. The search results are displayed in a table with columns for Time, Event, and LogName. The table shows the following data:

Time	Event	LogName
5/22/25 12:00:00.000 AM	5/22/25 12:00:00.000 AM	WinEventLog:Security
5/22/25 09:25:21.000 AM	5/22/25 09:25:21.000 AM	WinEventLog:Security
5/22/25 09:25:21.000 AM	5/22/25 09:25:21.000 AM	WinEventLog:Security