SCENARIO 2: Lateral Movement via RDP Brute Force

The goal is to:

- Detect brute-force login attempts.
- Identify lateral movement patterns.
- Understand log artifacts and correlate them in **Splunk**.

STEP 1: Enable and Confirm RDP on Victim Machine

-

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
PS C:\Windows\system32> Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
PS C:\Windows\system32> netstat -an | findstr 3389
>>
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    [::]:3389              [::]:0                 LISTENING
  UDP    0.0.0.0:3389           *:*
  UDP    [::]:3389              *:*
PS C:\Windows\system32>
```

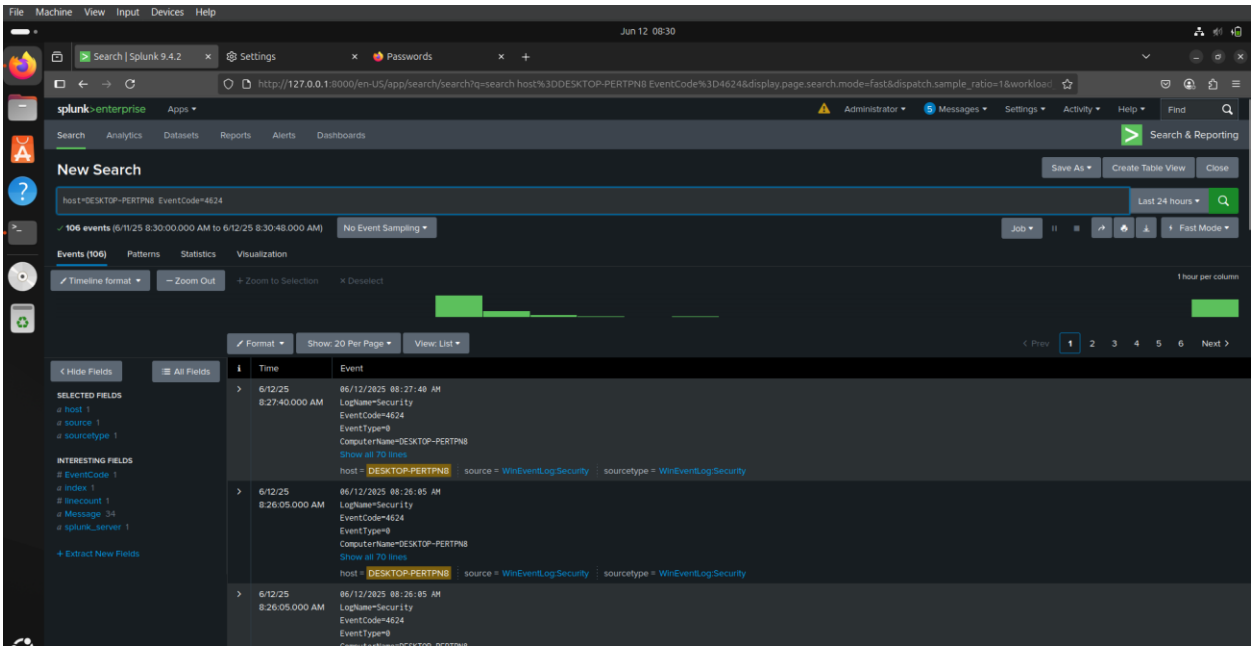
STEP 2: Simulate RDP Brute-Force Attack from Kali Linux

Use hydra:

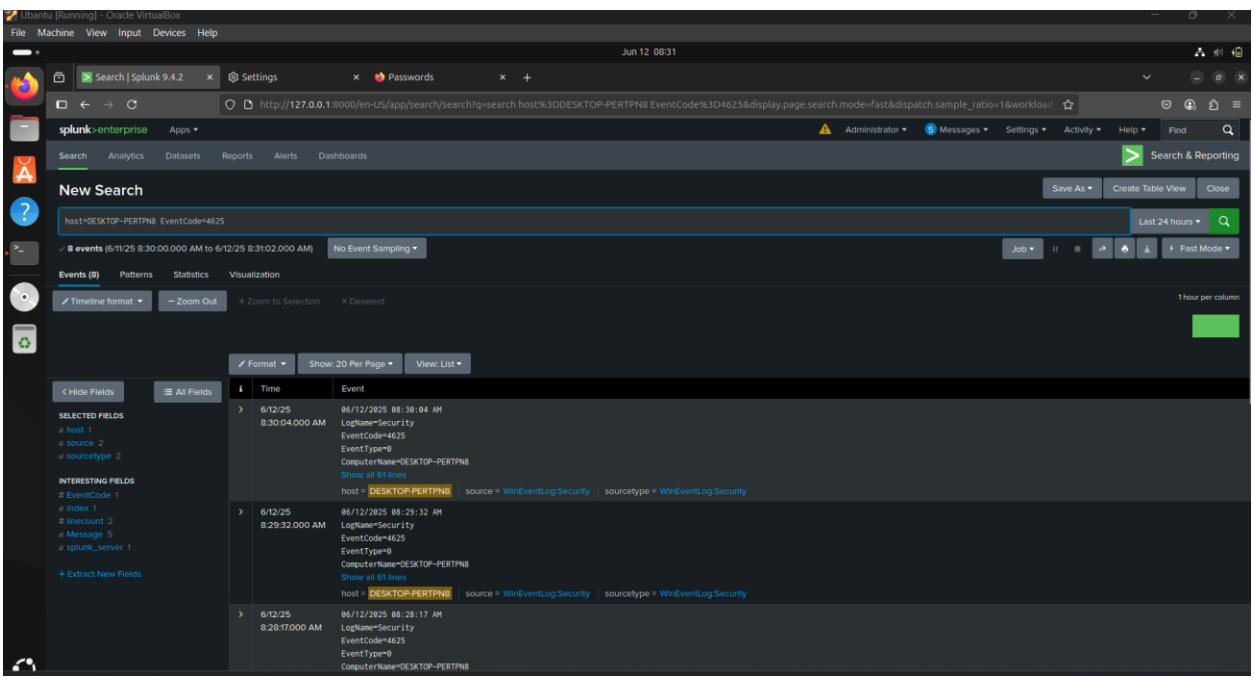
```
┌──(root㉿kali)-[/home/sirius/Desktop]
└─# hydra -t4 -v -f -l testuser -p pass.txt rdp://192.168.1.13
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-11 23:00:04
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to 1
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://192.168.1.13:3389/
```

Step 3: Detect Failed Logins (Brute-Force Indicator)

Failed attempt:



Successful attempt :



Step 4: Now create alert

-