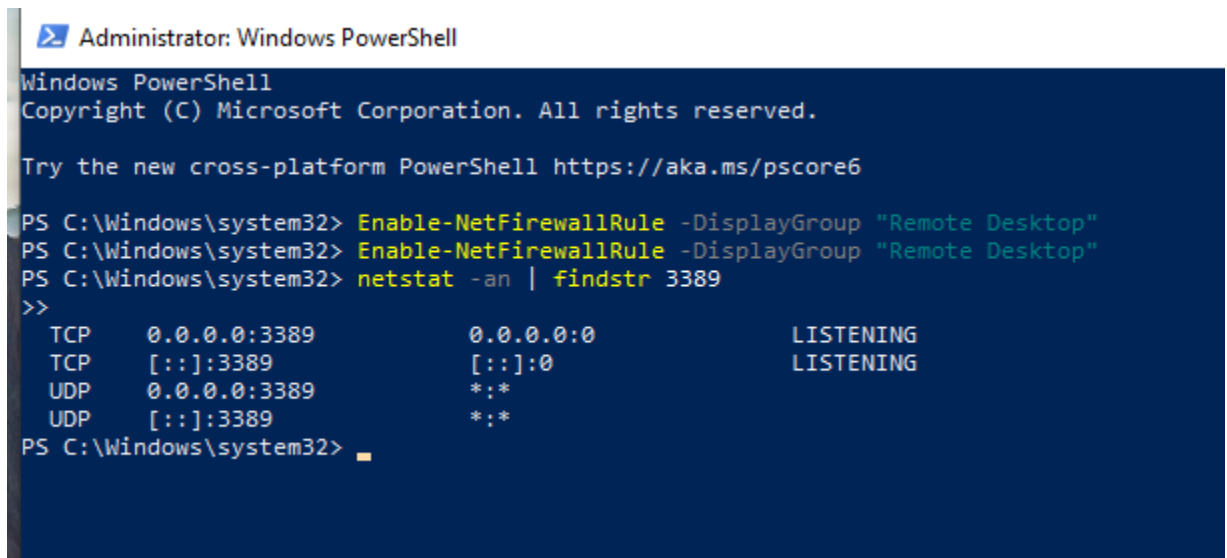


## SCENARIO 2: Lateral Movement via RDP Brute Force

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



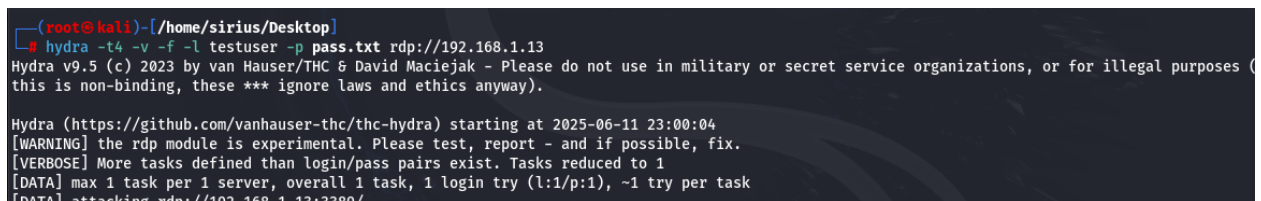
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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:

The screenshot shows the Splunk Enterprise interface with a search query: `host=DESKTOP-PERTPNB EventCode=4624`. The search results show 106 events. The first event is a failed login attempt on 6/12/2025 at 8:27:40 AM. The event details are as follows:

Time	Event
6/12/2025 8:27:40 AM	LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-PERTPNB host = <b>DESKTOP-PERTPNB</b>   source = WinEventLog:Security   sourcetype = WinEventLog:Security
6/12/2025 8:26:05 AM	LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-PERTPNB host = <b>DESKTOP-PERTPNB</b>   source = WinEventLog:Security   sourcetype = WinEventLog:Security
6/12/2025 8:26:05 AM	LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-PERTPNB host = <b>DESKTOP-PERTPNB</b>   source = WinEventLog:Security   sourcetype = WinEventLog:Security

Successful attempt :

The screenshot shows the Splunk Enterprise interface with a search query: `host=DESKTOP-PERTPNB EventCode=4625`. The search results show 8 events. The first event is a successful login attempt on 6/12/2025 at 8:30:04 AM. The event details are as follows:

Time	Event
6/12/2025 8:30:04 AM	LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-PERTPNB host = <b>DESKTOP-PERTPNB</b>   source = WinEventLog:Security   sourcetype = WinEventLog:Security
6/12/2025 8:29:32 AM	LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-PERTPNB host = <b>DESKTOP-PERTPNB</b>   source = WinEventLog:Security   sourcetype = WinEventLog:Security
6/12/2025 8:28:17 AM	LogName=Security EventCode=4625 ComputerName=DESKTOP-PERTPNB

Step 4: Now create alert

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

3 Alerts

All

Yours

This App's

filter

Q

i	Title	Actions	Owner	App	Sharing	Status
>	Brute Force Detection - Multiple Failed Logins	<a href="#">Open in Search</a> <a href="#">Edit</a>	splunk_admin	search	Private	Enabled