

RDP Brute-Force Detection using Splunk SIEM

Project Overview

This project demonstrates an end-to-end SOC detection workflow by simulating an RDP brute-force attack against a Windows Server and detecting it using Splunk SIEM.

The project covers:

- Log ingestion
- Attack simulation
- Detection engineering
- Alerting
- Dashboard creation

Goal: Detect and respond to RDP brute-force attacks using Windows Security logs.

Lab Architecture

Environment Overview

- **Windows Server 2016** – Victim & log source
- **Kali Linux** – Attacker
- **Splunk Enterprise** – SIEM
- **VirtualBox** – Virtualization

Network

- Host-only adapter (isolated lab)
-

Tools & Technologies Used

- Splunk Enterprise
 - Splunk Add-on for Microsoft Windows
 - Kali Linux
 - Hydra
 - Windows Server 2016
 - VirtualBox
-

Windows Log Source Configuration

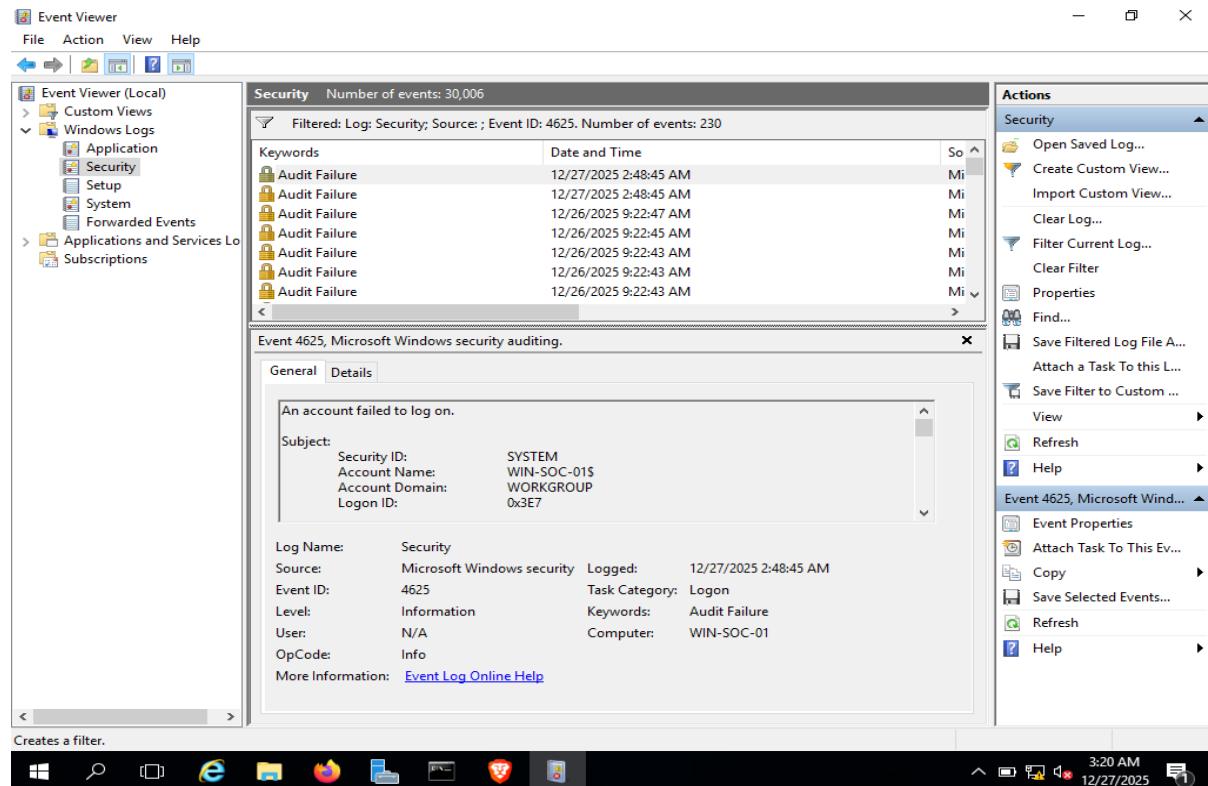
Windows Security Logging

Windows records authentication activity in the **Security Event Log**.

Relevant Event IDs:

- **4625** – Failed logon attempt
- **4624** – Successful logon
- **Logon Type 10** – Remote Interactive (RDP)

These logs are critical for detecting brute-force and compromise activity.



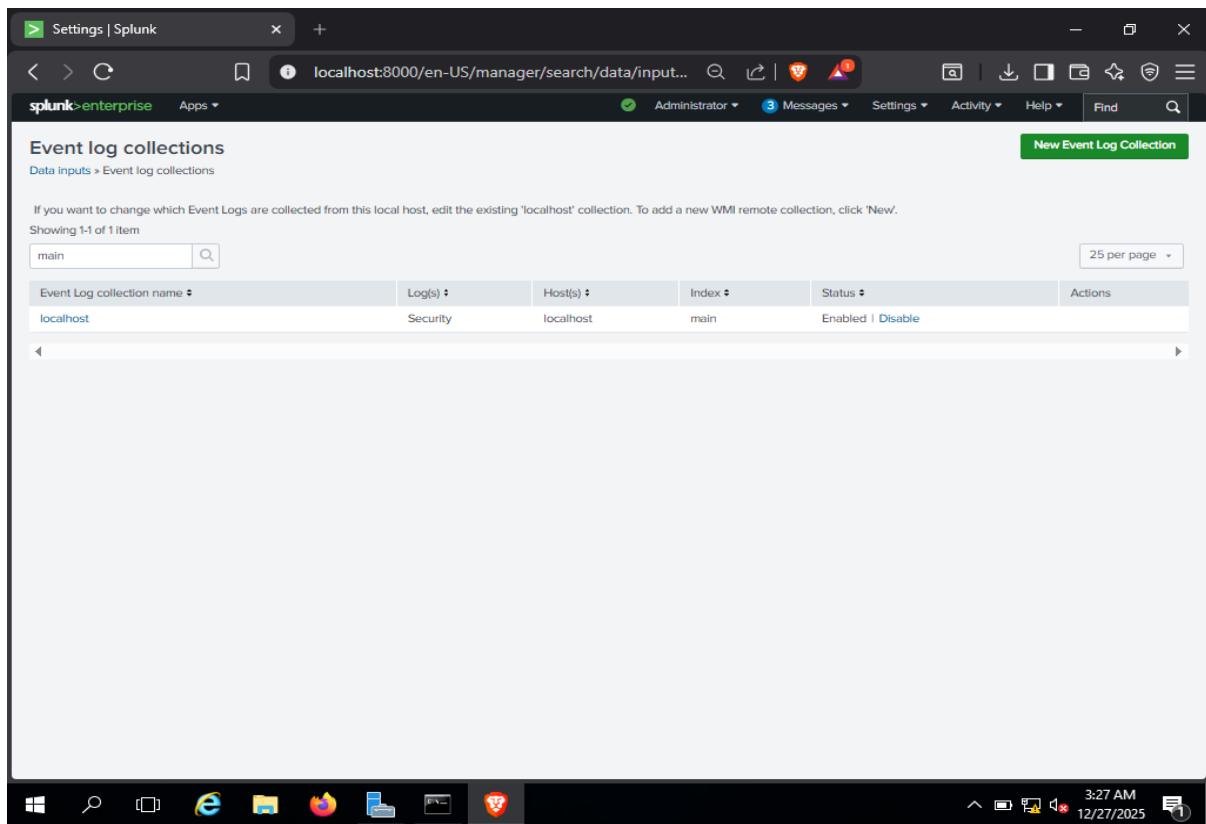
Windows Security Event Log showing Event ID 4625 (failed RDP logon attempt).

Splunk Log Ingestion

Configuration Details

- Input Type: Local Event Log Collection
- Log: Security
- Index: main
- Sourcetype: WinEventLog:Security

Splunk ingests **only new events**, so failed logins were generated after configuration.



Splunk configured to ingest Windows Security Event Logs.

Attack Simulation (Kali Linux)

Password Wordlist Creation

```
echo -e "admin\npassword\n123456\nPassword@123\nWelcome1\nWelcome@123\nAdmin123!" > passwords.txt
```

Explanation

- Creates a test password list
 - Simulates weak and commonly used credentials
-

RDP Brute-Force Attack

```
hydra -l Administrator -P passwords.txt rdp://192.168.56.105
```

Explanation

- hydra brute-forces credentials
- Targets RDP service on port 3389
- Generates multiple failed login attempts

Hydra performing an RDP brute-force attack from Kali Linux.

Detection Using Splunk (SPL Queries)

View Failed RDP Logins

index=main EventCode=4625 Logon_Type=10

| table _time Account_Name src_ip Logon_Type

Purpose

- Confirms attack activity
 - Identifies attacker IP and targeted account

Search | Splunk 10.0.2

localhost:8000/en-US/app/search/search?q=search... Administrator Messages Settings Activity Help Find

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

New Search

index=main EventCode=4625

7 events (12/26/25 3:00:00.000 AM to 12/27/25 3:28:43.000 AM) No Event Sampling

Time range: Last 24 hours

Save As Create Table View Close

Events (7) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

1 hour per column

Format Show: 20 Per Page View: List

< Hide Fields All Fields

Time	Event
12/27/25 2:48:45.989 AM	<event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <system><provider guid="35489625-5478-4994-A0BA-3E3B832C38D0" name="Microsoft-Windows-Security-Auditing"></provider><eventid>4625</eventid><version>0</version><level>1</level><task>12544</task><opcode>0</opcode><keywords>0x8010000000000000</keywords><timecreated systemtime="2025-12-27T12:48:45.989587900Z"></timecreated><eventrecordid>31399</eventrecordid><correlation activityid="055f7217-778F-0000-9821-F7658F77DC01"></correlation><execution processid="6161" threadid="668"></execution><channel>Security</channel><computer>WIN-SOC-01</computer><security></security><system><eventid>4625</eventid><data name="SubjectUserSid">>NT AUTHORITY\SYSTEM</data><data name="SubjectUserName">WIN-SOC-01\$</data><data name="SubjectDomainName">>WORKGROUP</data><data name="LogonProcessName">System</data><data name="LogonType">3</data><data name="TargetDomainName">WORKGROUP</data><data name="TargetUserName">Administrator</data><data name="Status">0x00000073</data><data name="SubStatus">0x00000000</data><data name="LogonType">3</data><data name="LogonProcessName">Adapi</data><data name="AuthenticationPackageName">Negotiate</data><data name="WorkstationName"></Data><Data Name="AuthName">ImPackagine3></Data><Data Name="KeyLength">0</Data><Data Name="ProcessId">0x390</Data><Data Name="ProcessName">C:\Windows\System32\avhost.exe</Data><Data Name="IpAddress">></Data><Data Name="IPPort">></Data></EventData></Event></data></system></system>
12/27/25 2:48:45.988 AM	<event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <system><provider guid="35489625-5478-4994-A0BA-3E3B832C38D0" name="Microsoft-Windows-Security-Auditing"></provider><eventid>4625</eventid><version>0</version><level>1</level><task>12544</task><opcode>0</opcode><keywords>0x8010000000000000</keywords><timecreated systemtime="2025-12-27T12:48:45.98857900Z"></timecreated><eventrecordid>31398</eventrecordid><correlation activityid="055f7217-778F-0000-9821-F7658F77DC01"></correlation><execution processid="6161" threadid="668"></execution><channel>Security</channel><computer>WIN-SOC-01</computer><security></security><system><eventid>4625</eventid><data name="SubjectUserSid">>NT AUTHORITY\SYSTEM</data><data name="SubjectUserName">WIN-SOC-01\$</data><data name="SubjectDomainName">>WORKGROUP</data><data name="LogonProcessName">System</data><data name="LogonType">3</data><data name="TargetDomainName">WORKGROUP</data><data name="TargetUserName">Administrator</data><data name="Status">0x00000073</data><data name="SubStatus">0x00000000</data><data name="LogonType">3</data><data name="LogonProcessName">Adapi</data><data name="AuthenticationPackageName">Negotiate</data><data name="WorkstationName"></Data><Data Name="AuthName">ImPackagine3></Data><Data Name="KeyLength">0</Data><Data Name="ProcessId">0x390</Data><Data Name="ProcessName">C:\Windows\System32\avhost.exe</Data><Data Name="IpAddress">></Data><Data Name="IPPort">></Data></EventData></Event></data></system></system>

localhost:8000/en-US/app/search/search

Splunk search results showing multiple failed RDP login attempts.

Brute-Force Detection Query

```
index=main EventCode=4625 Logon_Type=10  
| stats count by src_ip Account_Name  
| where count > 5
```

Purpose

- Detects brute-force behavior
 - Reduces noise from single failures
-

Compromise Detection Query

```
index=main (EventCode=4625 OR EventCode=4624) Logon_Type=10  
| transaction Account_Name maxspan=5m
```

Purpose

- Detects successful login after multiple failures
 - Indicates possible account compromise
-

Alerts Configuration

Configured Alerts

Alert	Condition	Severity
RDP Brute Force Detected	>5 failed logins	Medium
RDP Account Compromise	4624 after 4625	High

The screenshot shows a Splunk interface with a dark theme. At the top, there's a header bar with the title 'RDP Brute Force Detected | Splunk'. Below the header, the URL 'localhost:8000/en-US/app/search/alert?s=%2Fser...' is visible. The main content area is titled 'RDP Brute Force Detected' and contains the following details:

- Enabled: Yes. [Disable](#)
- App: search
- Permissions: Shared in App. Owned by Jess. [Edit](#)
- Modified: Dec 26, 2025 9:34:18 AM
- Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: Number of Results is > 1. [Edit](#)

Actions: 1 Action [Edit](#)

[Add to Triggered Alerts](#)

Trigger History

20 per page ▾

	TriggerTime	Actions
1	2025-12-27 03:00:06 Pacific Standard Time	View Results
2	2025-12-26 10:43:32 Pacific Standard Time	View Results

At the bottom of the window, there's a toolbar with various icons and a status bar showing '3:33 AM 12/27/2025'.

Splunk alert configured to detect RDP brute-force attacks.

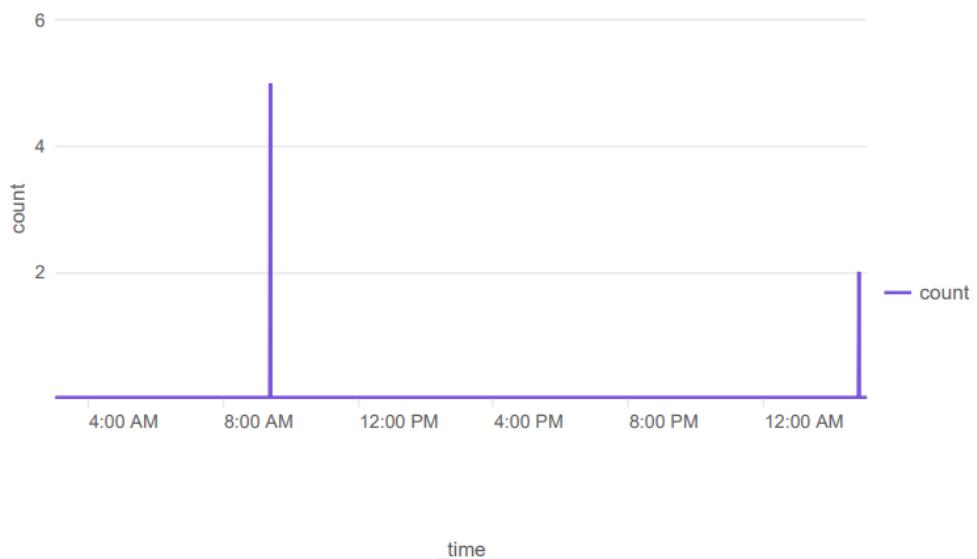
Dashboards & Visualization

Dashboard: RDP Attack Monitoring

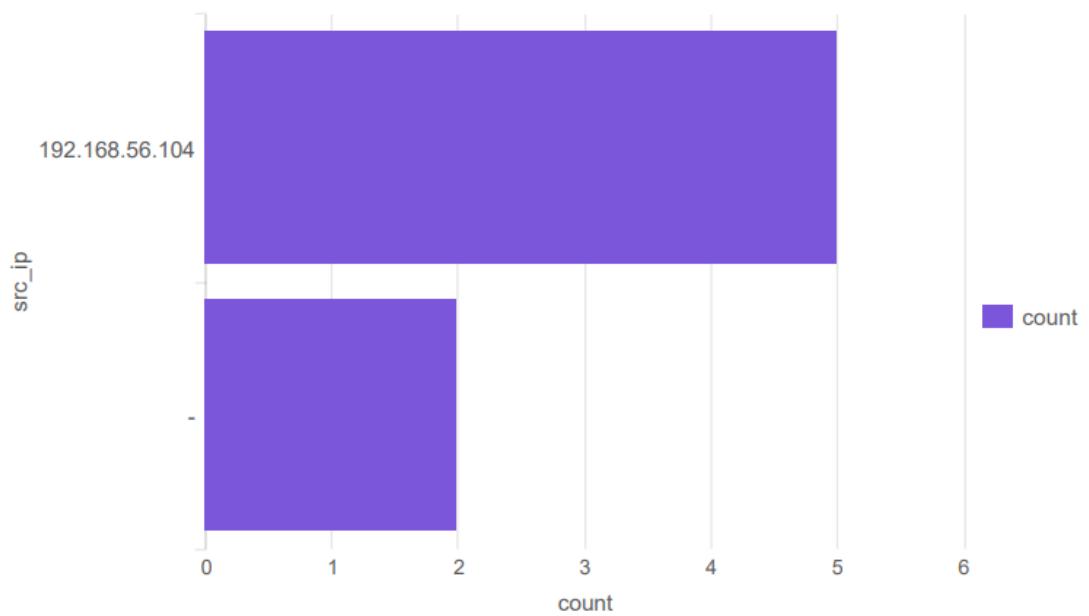
Panels:

- Failed RDP logins over time
- Top attacking IPs
- Targeted accounts
- Successful RDP logins

Failed RDP Logins Over Time



Top Source IPs



Successful RDP Logins

time	Account Name	src_ip
2025-12-27 02:48:28.885	-	
2025-12-27 02:48:17.987	-	
2025-12-27 02:48:11.978	-	
2025-12-27 02:48:10.918	-	
2025-12-27 02:48:10.864	-	
2025-12-27 02:48:10.851	-	
2025-12-27 02:48:10.766	-	
2025-12-27 02:48:10.518	-	
2025-12-26 22:43:26.278	-	
2025-12-26 22:43:26.278	-	
2025-12-26 22:43:25.786	-	
2025-12-26 22:43:25.746	-	
2025-12-26 22:43:25.746	-	
2025-12-26 22:43:24.769	-	
2025-12-26 22:43:24.303	-	
2025-12-26 22:43:23.376	-	
2025-12-26 22:32:15.133	-	
2025-12-26 22:32:14.468	-	
2025-12-26 22:32:14.440	-	
2025-12-26 22:32:14.440	-	
2025-12-26 22:32:14.359	-	
2025-12-26 22:32:13.534	-	
2025-12-26 22:32:13.022	-	
2025-12-26 22:32:12.147	-	
2025-12-26 15:11:31.049	-	
2025-12-26 15:11:30.792	-	
2025-12-26 15:11:30.776	-	
2025-12-26 15:11:30.720	-	
2025-12-26 15:11:30.720	-	
2025-12-26 15:11:30.120	-	
2025-12-26 15:11:29.798	-	
2025-12-26 15:11:29.235	-	
2025-12-26 09:22:45.683		192.168.56.104

Splunk dashboard visualizing RDP brute-force activity.

MITRE ATT&CK Mapping

Tactic	Technique
--------	-----------

Initial Access	T1021.001 – RDP
----------------	-----------------

Credential Access	T1110 – Brute Force
-------------------	---------------------

Key Learnings

- SIEM log ingestion and troubleshooting
- Writing SPL detection queries
- Brute-force detection logic
- SOC alerting workflows
- Attack visualization

Conclusion

This project demonstrates a **complete SOC detection lifecycle**:

Attack Simulation → Detection → Alerting → Visualization → Response

It reflects **real-world SIEM and detection engineering practices**.