

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

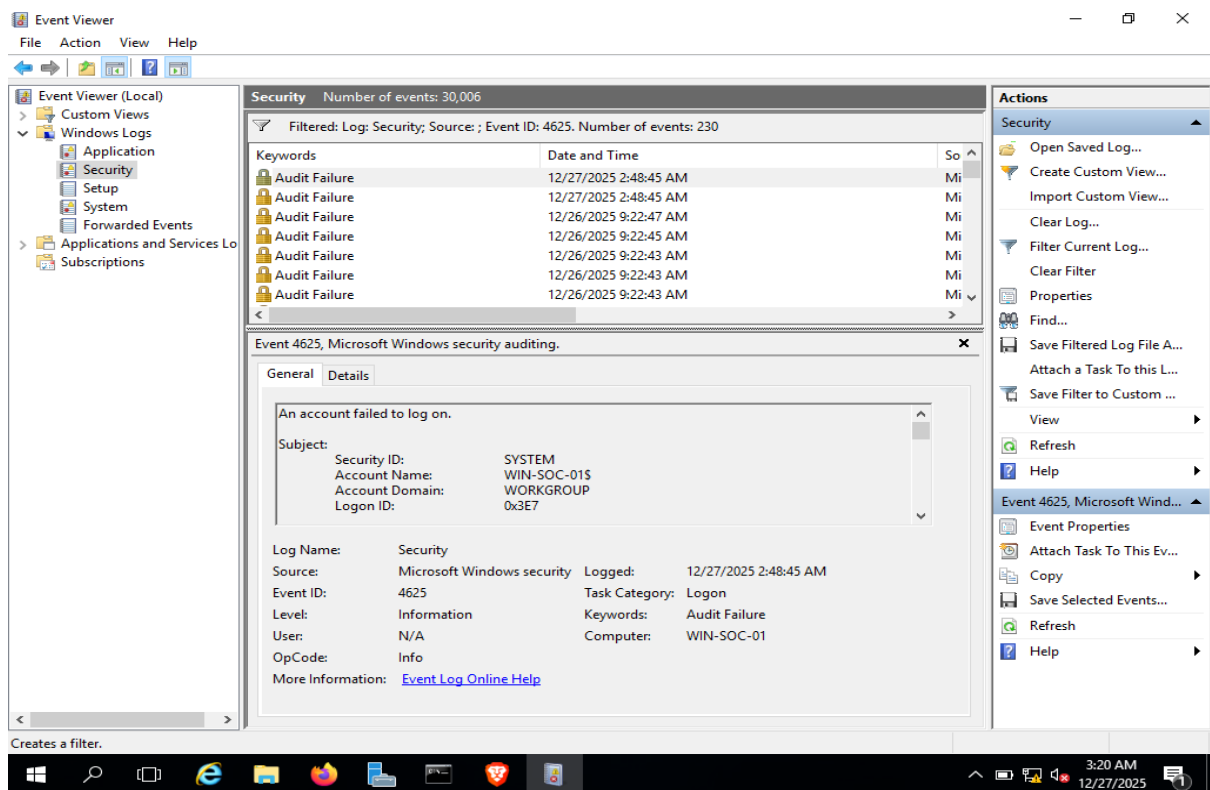
Windows Security Logging

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.



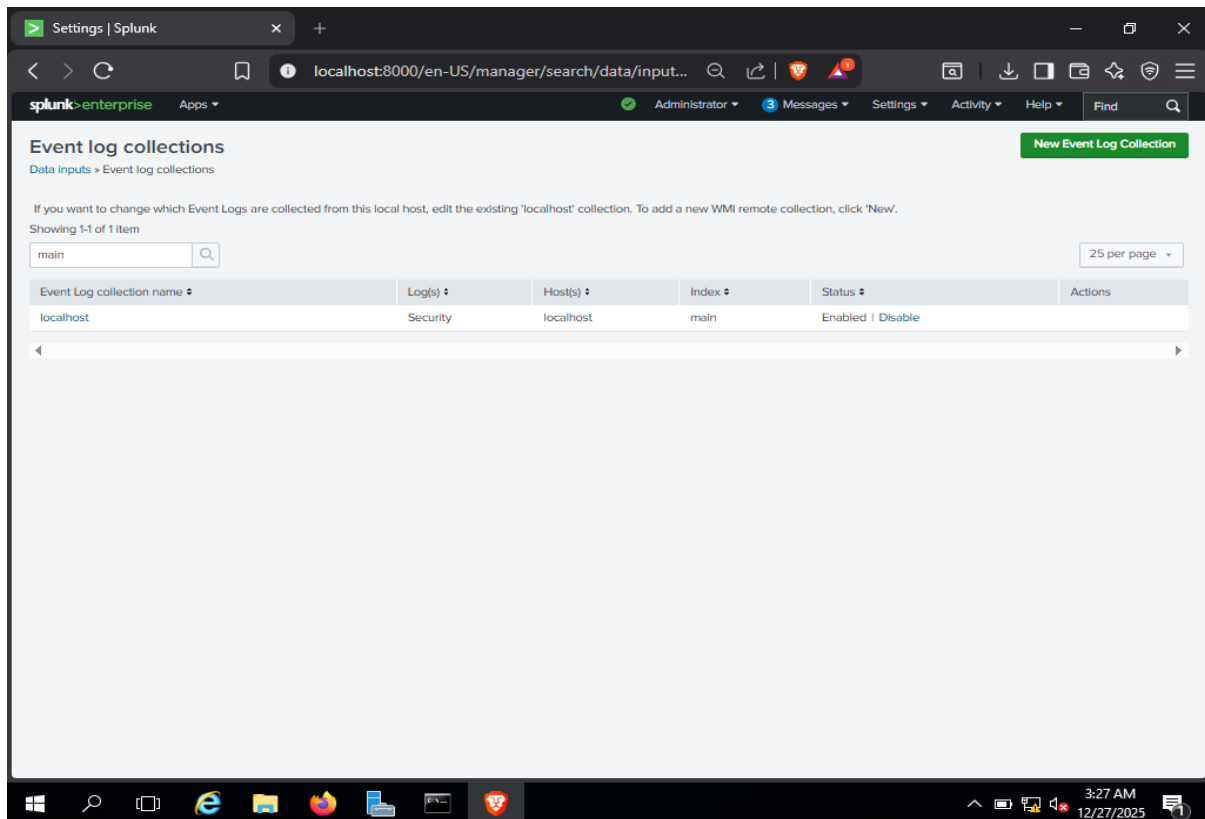
Windows Security Event Log showing Event ID 4625 (failed RDP logon attempt).

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

```
kali@kali:~$ hydra -i Administrator -P passwords.txt rdp://192.168.56.185
Hydra v9.6 (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 2025-12-27 17:00:13
[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 recover
[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.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries (1:1/p??), ~2 tries per task
[DATA] attacking rdp://192.168.56.185:3389/
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.

kali@kali:~$ hydra -i Administrator -P passwords.txt rdp://192.168.56.185
Hydra v9.6 (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 2025-12-27 17:00:31
[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 recover
[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.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries (1:1/p??), ~2 tries per task
[DATA] attacking rdp://192.168.56.185:3389/
[ERROR] Freerdp: The connection failed to establish.
[ERROR] Freerdp: The connection failed to establish.
[3389][rdp] account on 192.168.56.185 might be valid but account not active for remote desktop: login: Administrator password: 123456, continuing attacking the account.
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.

kali@kali:~$
```

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

The screenshot shows the Splunk Enterprise web interface. The search bar contains the query: `index=main EventCode=4625`. The results are displayed in a table format. The table has columns for Time, Event, and details. The first result shows a failed RDP login attempt on 12/27/25 at 2:48:45.989 AM. The event details include the source IP (192.168.56.185) and the account name (Administrator).

Time	Event	Details
12/27/25 2:48:45.989 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-A5BA-3E380328C380}' /><EventID>4625</EventID><Version>8</Version><Level>8</Level><Task>12544</Task><Opcode>8</Opcode><Keywords>0x8010000000000000</Keywords><TimeCreated SystemTime='2025-12-27T10:48:45.989391000Z' /><EventRecordID>31399</EventRecordID><Correlation ActivityID='{65F72172-778F-0000-9821-F7658F77DC01}' /><Execution ProcessID='616' ThreadID='668' /><Channel>Security</Channel><Computer>WIN-SOC-01</Computer><Security></Security></System><EventData><Data Name='SubjectUserSid'>NT AUTHORITY\SYSTEM</Data><Data Name='SubjectUserName'>WIN-SOC-01</Data><Data Name='SubjectDomainName'>WORKGROU</Data><Data Name='SubjectLogonId'>0x3e7c</Data><Data Name='TargetUserSid'>NULL SID</Data><Data Name='TargetUserName'></Data><Data Name='TargetDomainName'></Data><Data Name='Status'>0xc0000073</Data><Data Name='FailureReason'>X32384</Data><Data Name='SubStatus'>0xc0000073</Data><Data Name='LogonType'>5</Data><Data Name='LogonProcessName'>Advapi</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'></Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>8</Data><Data Name='ProcessId'>0x399</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'></Data><Data Name='IpPort'></Data></EventData></Event>	host = WIN-SOC-01 source = XmlWinEventLog\Security sourcetype = XmlWinEventLog
12/27/25 2:48:45.989 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-A5BA-3E380328C380}' /><EventID>4625</EventID><Version>8</Version><Level>8</Level><Task>12544</Task><Opcode>8</Opcode><Keywords>0x8010000000000000</Keywords><TimeCreated SystemTime='2025-12-27T10:48:45.989391000Z' /><EventRecordID>31398</EventRecordID><Correlation ActivityID='{65F72172-778F-0000-9821-F7658F77DC01}' /><Execution ProcessID='616' ThreadID='668' /><Channel>Security</Channel><Computer>WIN-SOC-01</Computer><Security></Security></System><EventData><Data Name='SubjectUserSid'>NT AUTHORITY\SYSTEM</Data><Data Name='SubjectUserName'>WIN-SOC-01</Data><Data Name='SubjectDomainName'>WORKGROU</Data><Data Name='SubjectLogonId'>0x3e7c</Data><Data Name='TargetUserSid'>NULL SID</Data><Data Name='TargetUserName'></Data><Data Name='TargetDomainName'></Data><Data Name='Status'>0xc0000073</Data><Data Name='FailureReason'>X32384</Data><Data Name='SubStatus'>0xc0000073</Data><Data Name='LogonType'>5</Data><Data Name='LogonProcessName'>Advapi</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'></Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>8</Data><Data Name='ProcessId'>0x399</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'></Data><Data Name='IpPort'></Data></EventData></Event>	host = WIN-SOC-01 source = XmlWinEventLog\Security sourcetype = XmlWinEventLog

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
```

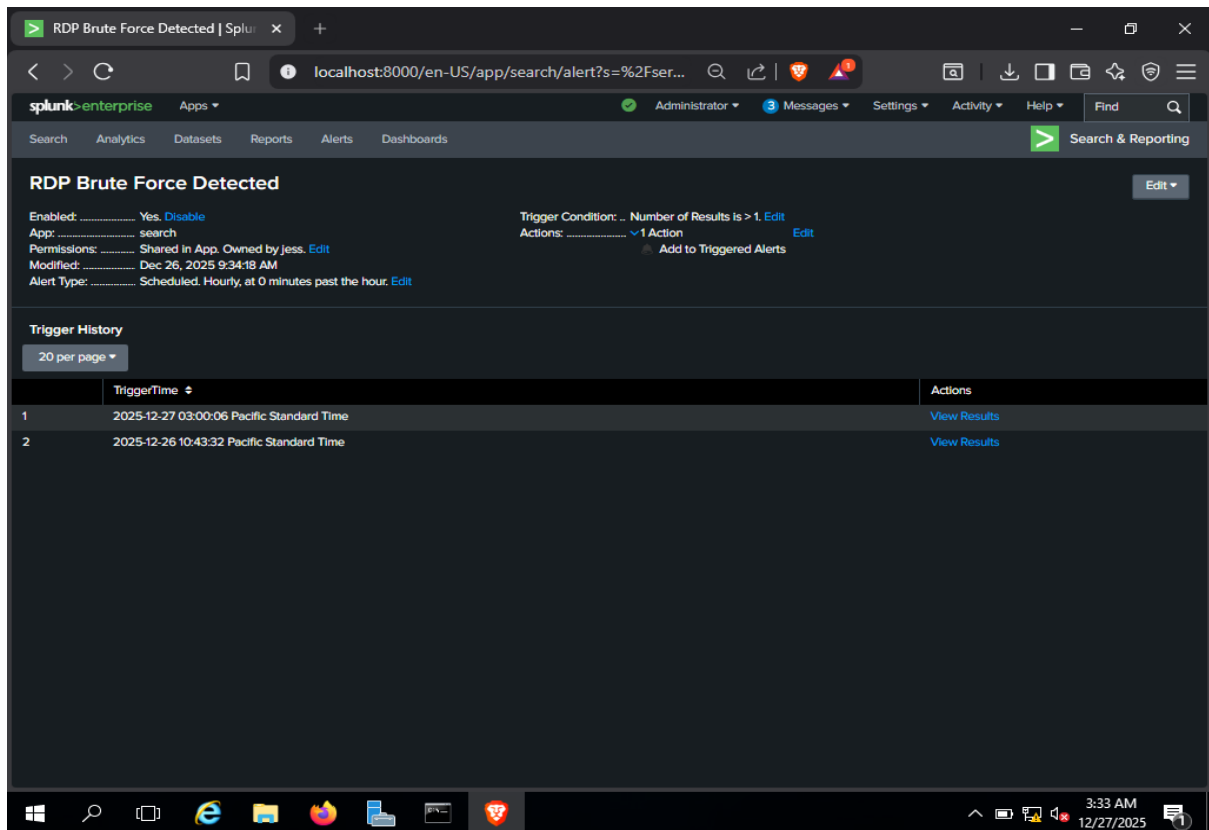
Purpose

- 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



Splunk alert configured to detect RDP brute-force attacks.

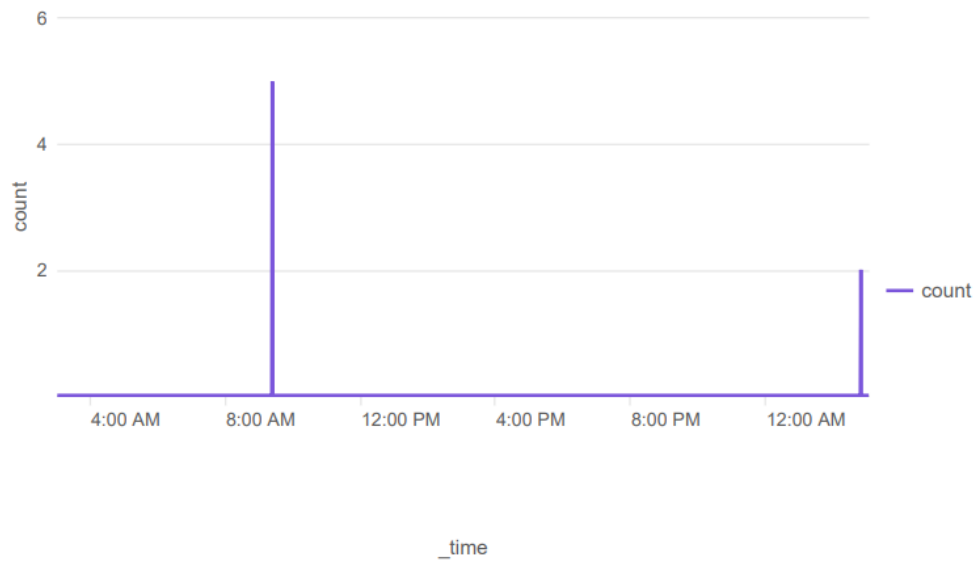
Dashboards & Visualization

Dashboard: RDP Attack Monitoring

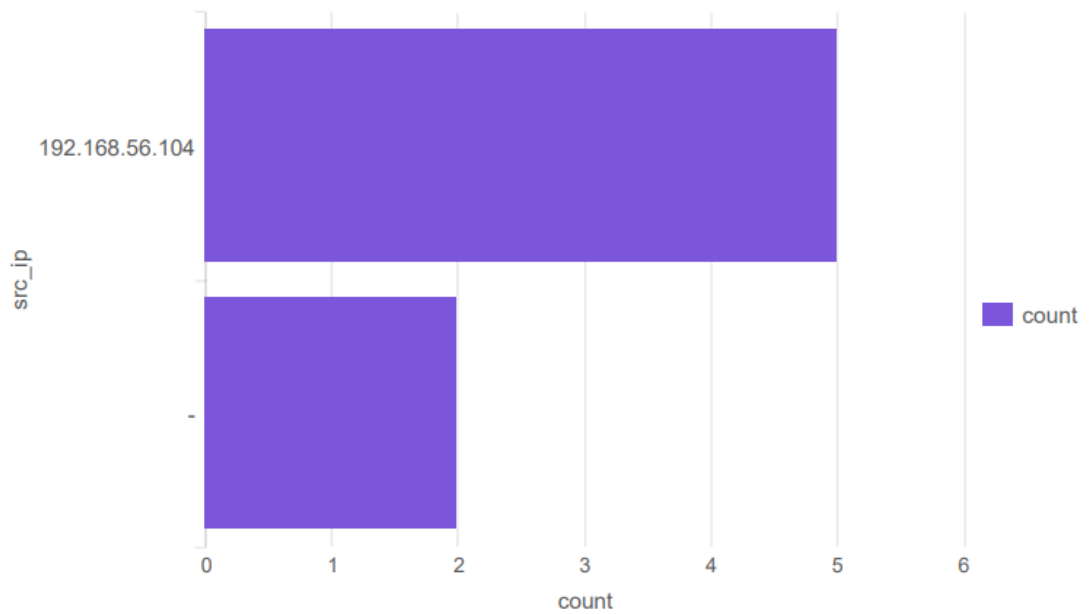
Panels:

- 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**.