# 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

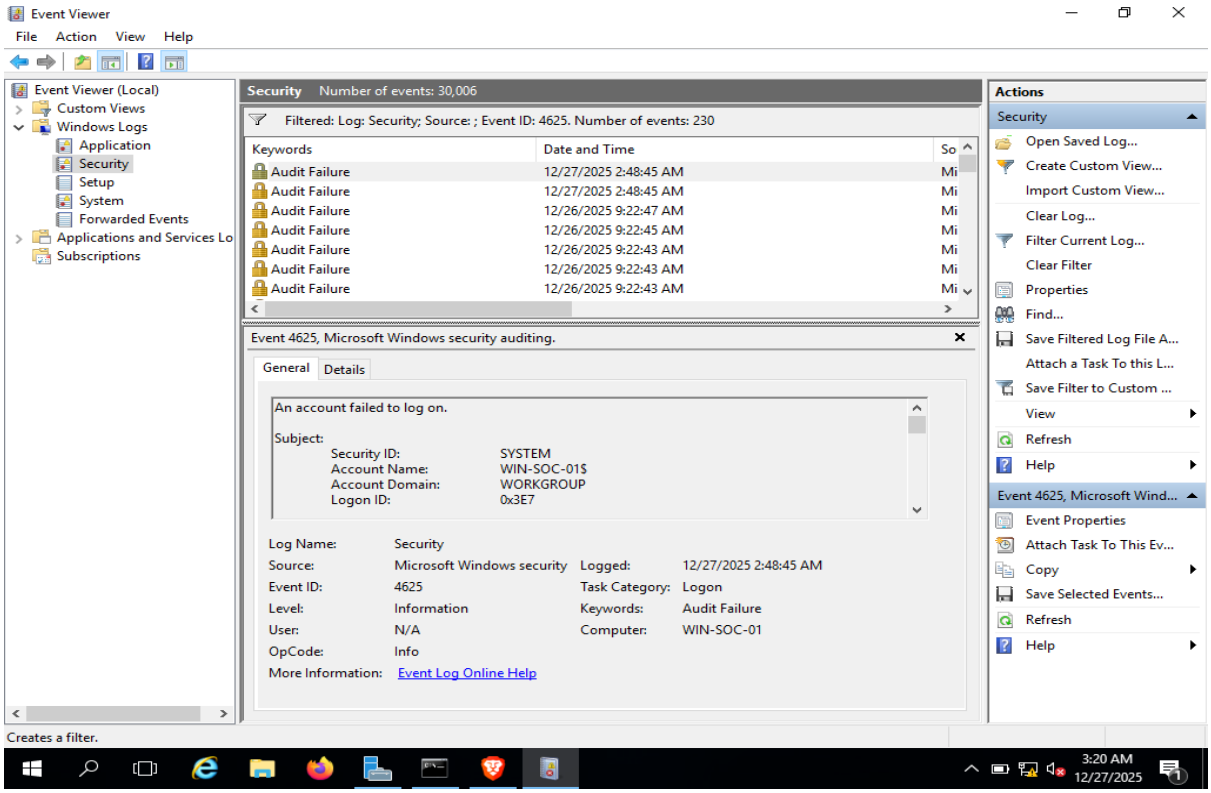
### Windows Security Logging

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).*

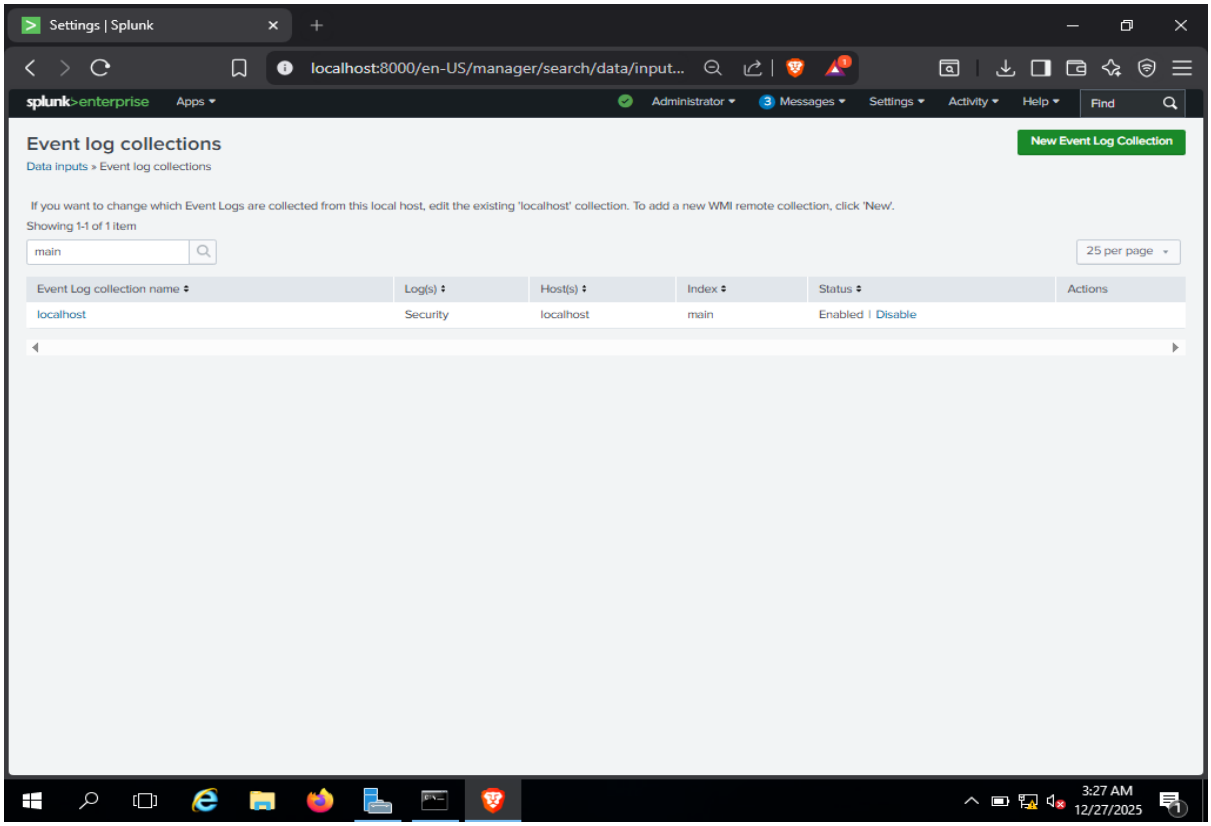
---

## 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

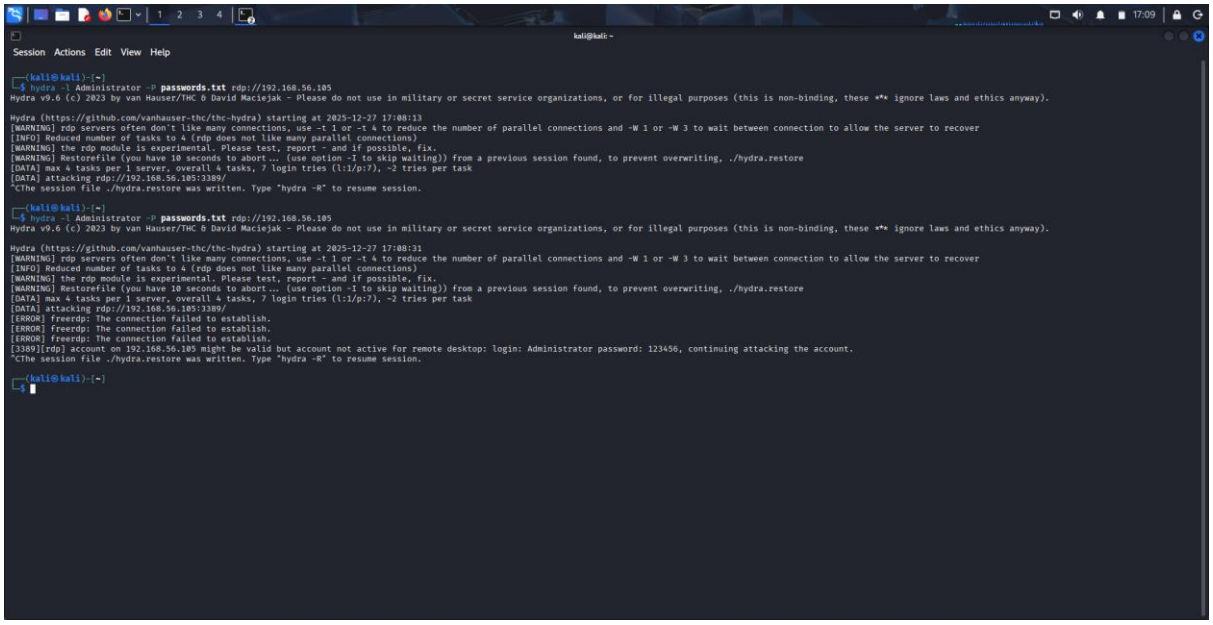
---

## 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)

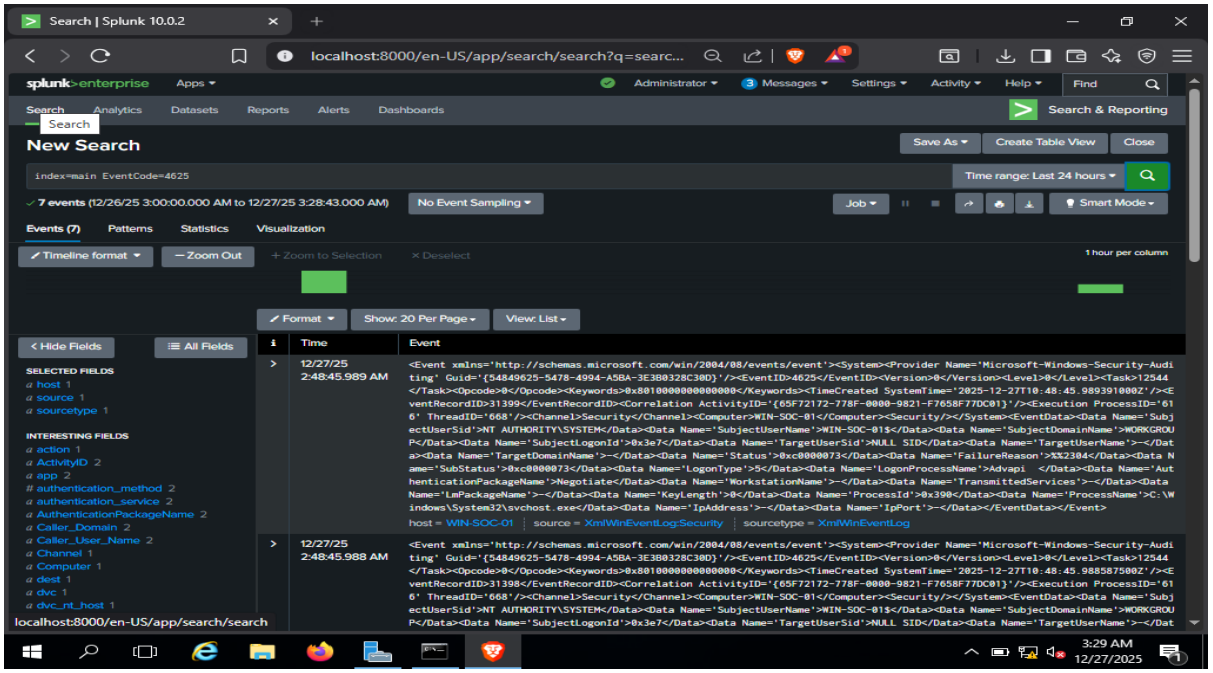
### View Failed RDP Logins

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



*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**

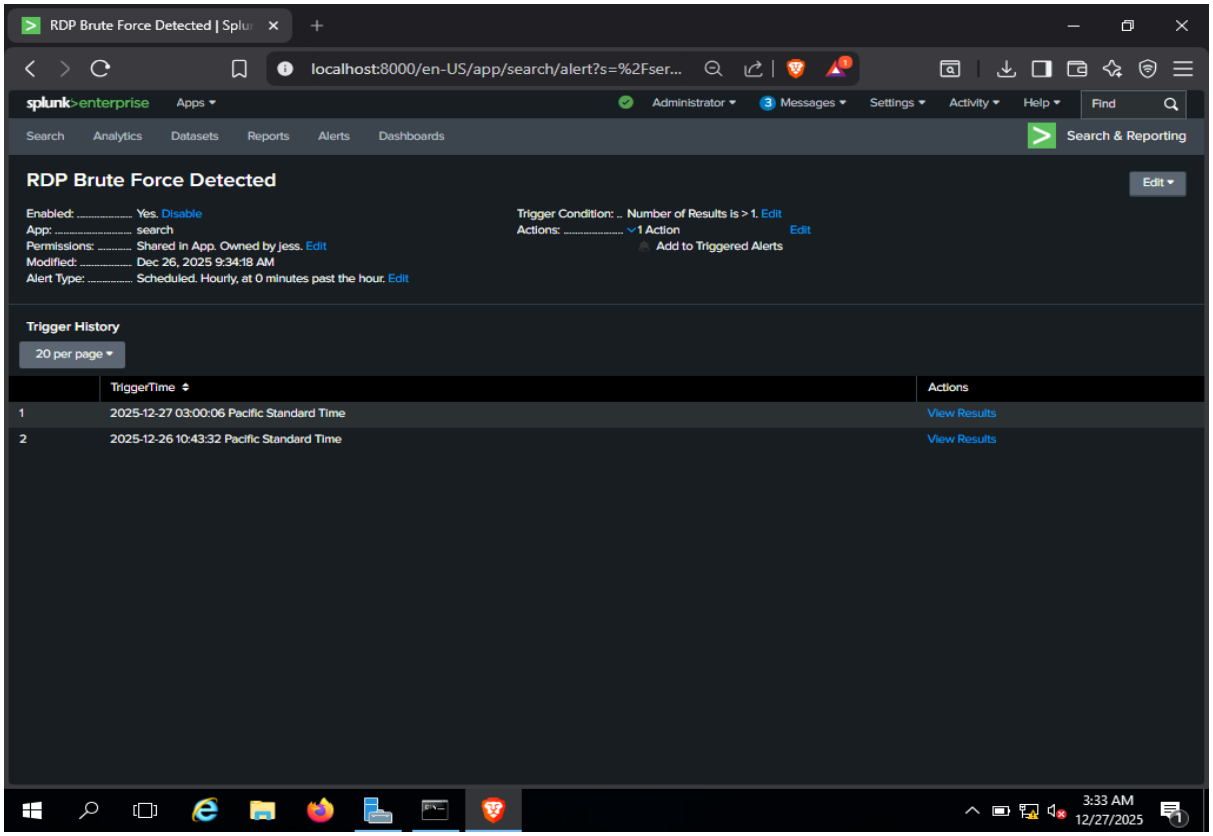
- Detects successful login after multiple failures
- Indicates possible account compromise

---

## 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

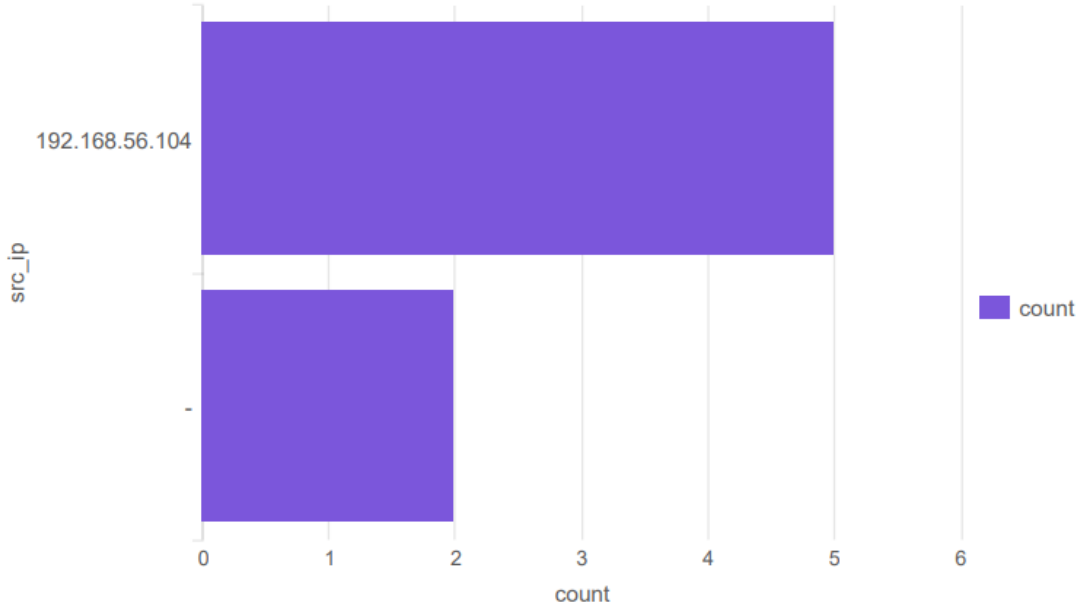
### Dashboard: RDP Attack Monitoring

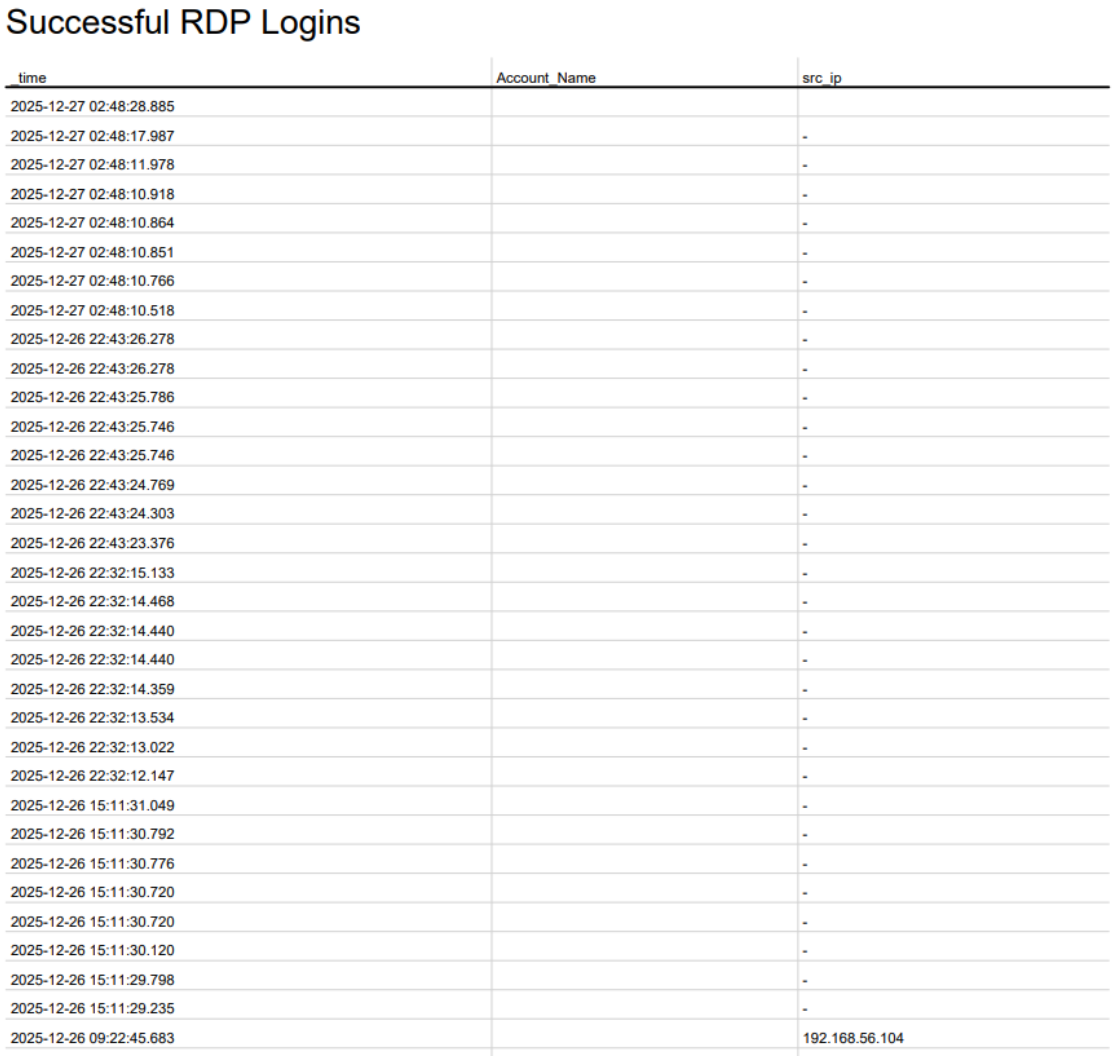
Panels:

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

## Failed RDP Logins Over Time


## Top Source IPs






*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**.