# 

# Brute-Force Investigation Report

## Investigation Summary – What Happened?

I received an alert about multiple failed logins. Using KQL I answered the following: Which accounts are experiencing the most failed logons? Were there any successful logins for those accounts, if so, where? What I would recommend if this was a real client incident.

After analysing the events in Microsoft Sentinel, the pattern clearly showed a brute force attack using NTLM authentication against administrator accounts. No successful logons occurred. The attack was high volume against RDP enabled systems.

## Stakeholder Impact - Who was involved?

No external compromise occurred but the attack targeted administrator-level accounts.

## Findings - What did I find?

* Roughly 10,000 failed logons in a minute
* Targeted administrator accounts
* Affected hosts: SOC-FW-RDP and SHIR-Hive
* Authentication method: NTLM
* No successful logons

## Immediate Actions - When did this occur and is it still happening?

The burst occurred at 15:34 on 4 October 2025 and lasted about a minute. No further attempts were seen.

Actions taken immediately:

* Verified no 4624 success events
* Created Sentinel bookmark and manual incident
* Built Sentinel Analytics Rule for future auto-detection

## Affected Systems and Data - Where in the environment did this happen?

* **Hosts:** SOC-FW-RDP, SHIR-Hive, SOC-FW, SHIR-SAP
* **Accounts:** \ADMINISTRATOR, \admin, \administrator
* **Data:** None accessed — all logon attempts failed
* **Scope:** Local authentication failures only; no lateral movement or file access

## Indicators of Compromise (IoCs)

* **Accounts:** \ADMINISTRATOR, \admin, \administrator
* **Auth method:** NTLM
* **Event IDs**: 4625 (failed logons)
* **Hosts:** SOC-FW-RDP, SHIR-Hive

## Root Cause - Why did this happen?

RDP was exposed and NTLM authentication remained enabled, making it easy for automated tools to attempt credential sprays. Strong passwords prevented success but the exposure increased attack surface.

## Nature of the Attack - How did this happen?

An automated brute force campaign targeted RDP logons using NTLM. Thousands of rapid attempts hit administrator accounts within a minute with no success or follow-on activity.

## Recommendations - What steps should be taken to reduce risk or stop the activity?

* Restrict RDP
* Disable NTLM
* Enforce MFA

## Summary

This was a brute force attack that did not get a successful login.