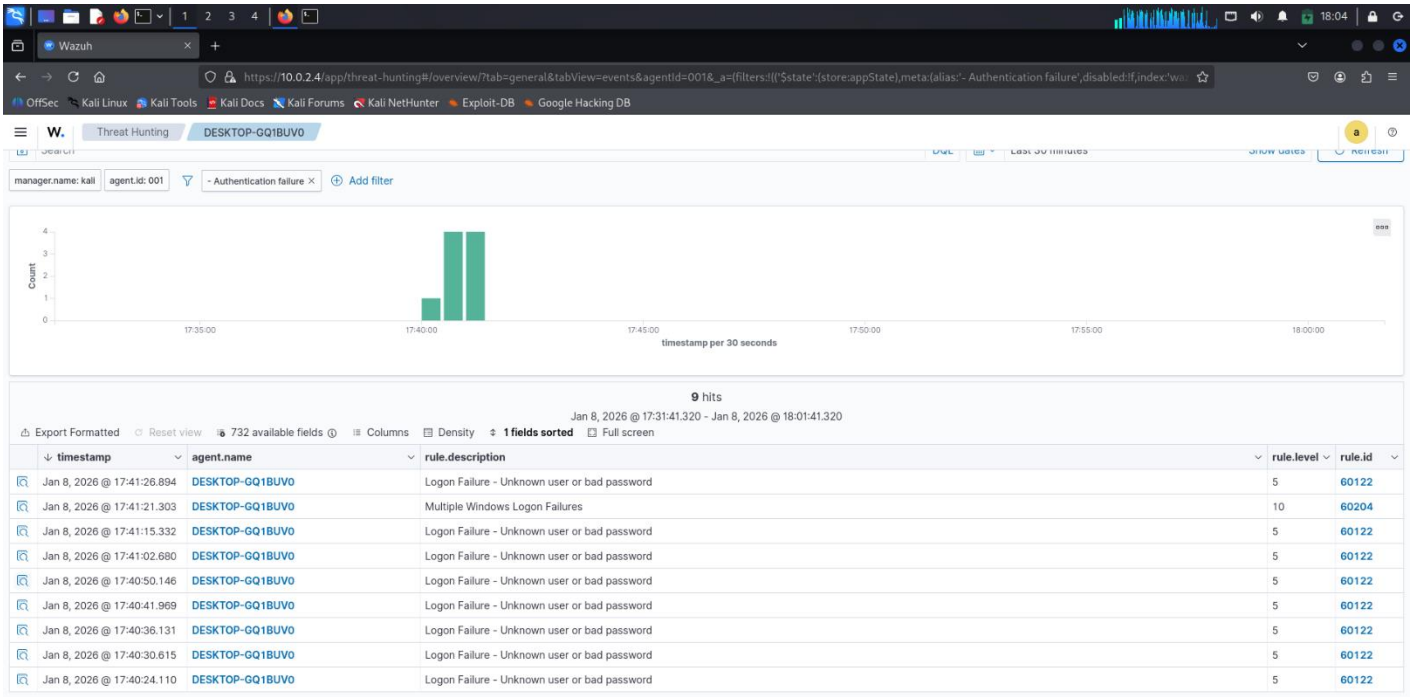
RDP Brute Force Followed By Successful Login & File Modification

INCIDENT ID: SOC-LAB-001
DETECTION SOURCE: WazuhSIEM

DATE: 08.01.26
ANALYST: Stephenraj

Find RDP Failed Login (4625)

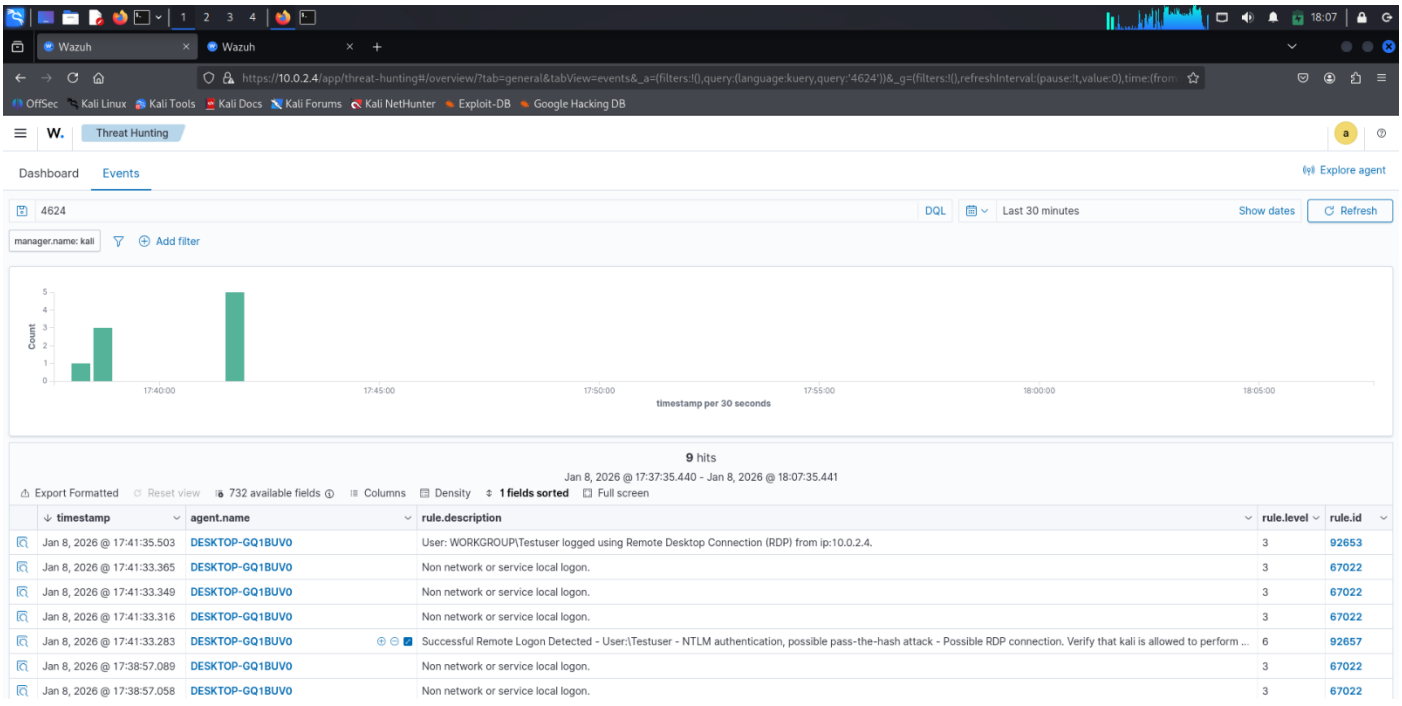


timestamp	agent.name	rule.description	rule.level	rule.id
Jan 8, 2026 @ 17:41:26.894	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:41:21.303	DESKTOP-GQ1BUV0	Multiple Windows Logon Failures	10	60204
Jan 8, 2026 @ 17:41:15.332	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:41:02.680	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:40:50.146	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:40:41.969	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:40:36.131	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:40:30.615	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122
Jan 8, 2026 @ 17:40:24.110	DESKTOP-GQ1BUV0	Logon Failure - Unknown user or bad password	5	60122

OBSERVATION:

Multiple Event ID 4625 (Failed RDP logins) observed from a single source IP targeting the same user account.

Find RDP Successful Login (4624)

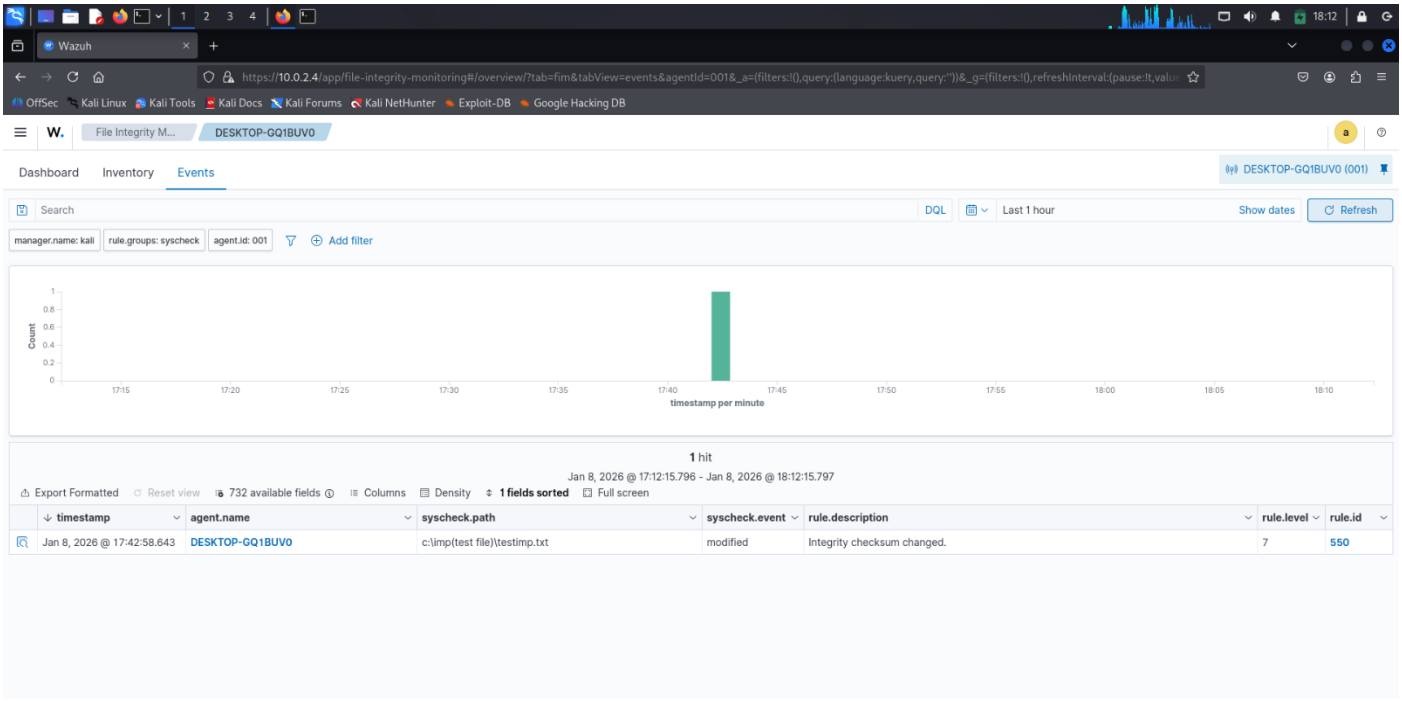


timestamp	agent.name	rule.description	rule.level	rule.id
Jan 8, 2026 @ 17:41:35.503	DESKTOP-GQ1BUV0	User: WORKGROUP\Testuser logged using Remote Desktop Connection (RDP) from ip:10.0.2.4.	3	92653
Jan 8, 2026 @ 17:41:33.365	DESKTOP-GQ1BUV0	Non network or service local logon.	3	67022
Jan 8, 2026 @ 17:41:33.349	DESKTOP-GQ1BUV0	Non network or service local logon.	3	67022
Jan 8, 2026 @ 17:41:33.316	DESKTOP-GQ1BUV0	Non network or service local logon.	3	67022
Jan 8, 2026 @ 17:41:33.283	DESKTOP-GQ1BUV0	Successful Remote Logon Detected - User:\Testuser - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that kali is allowed to perform ...	6	92657
Jan 8, 2026 @ 17:38:57.089	DESKTOP-GQ1BUV0	Non network or service local logon.	3	67022
Jan 8, 2026 @ 17:38:57.058	DESKTOP-GQ1BUV0	Non network or service local logon.	3	67022

OBSERVATION:

A successful RDP login (Event ID 4624) was observed shortly after multiple failed login attempts from the same source IP and user account.

Find File Integrity Alert (FIM)



OBSERVATION:

File Integrity Monitoring alert detected: a file modification event after the successful RDP login.

ATTACK TIMELINE:

T1 – Jan 8th 2026 @ 17:40:24 to 17:41:26

Multiple Event ID 4625 – Failed RDP login attempts detected.

T2 – Jan 8th 2026 @ 17:41:33

Event ID 4624 – Successful RDP login from the same IP and user.

T3 – Jan 8th 2026 @ 17:42:58

File Integrity Monitoring alert – File modification detected.

FALSE POSITIVE ANALYSIS:

- Source IP is not a known VPN or trusted admin IP.
- No approved maintenance window during this time.
- Login time is outside normal working hours.

• The file modified is sensitive.

• CONCLUSION: This activity is confirmed as a TRUE POSITIVE.

MITRE ATT&CK MAPPING:

T1110 – Brute Force

Justification: Multiple failed login attempts observed before success.

T1021.001 – Remote Services (RDP)

Justification: Remote Desktop Protocol (RDP) is used for remote access.

T1078 – Valid Accounts

Justification: Attacker successfully authenticated using valid credentials.

T1565 – Data Manipulation

Justification: File modification detected after compromise.

SEVERITY: High

IMPACT: Unauthorised access to the system with confirmed post-compromise activity.

ANALYST CONCLUSION:

Based on log correlation and timeline analysis, the system experienced an RDP brute-force attack that resulted in successful authentication and unauthorised file modification. Immediate containment and credential reset are recommended.