INCIDENT REPORT – USE CASE 4

Successful RDP Brute Force Attack (Windows Agent)

Incident ID: SOC-RDP-004
Incident Title: Successful RDP Brute Force Leading to Unauthorized Access
Date & Time: Jan 18, 2026 @ 20:53:30.969
Detection Source: Wazuh SIEM – Windows Authentication Monitoring

Affected Asset
Host: Windows Endpoint
Asset Type: Windows Server / Workstation
Severity: Critical

Incident Summary
Wazuh SIEM detected a series of repeated failed RDP authentication attempts against a Windows system followed by a successful RDP logon from the same external source. This activity indicates a successful brute force attack resulting in unauthorized access. The incident represents a confirmed security compromise requiring immediate containment and response.

Detection Details
Detection Tool: Wazuh SIEM
Detection Type: Host-based (Windows Security Event Logs)
Target Service: Remote Desktop Protocol (RDP) – Port 3389
Source IP: External Host (Lab Simulation)
Destination Host: Windows Agent
Event Pattern: Multiple failed logon events followed by a successful logon
Log Source: Windows Security Logs

Investigation and Analysis
The SOC analyst reviewed authentication alerts in the Wazuh dashboard and identified a high volume of failed RDP logon attempts originating from a single source IP within a short time window. Shortly after the failed attempts, a successful RDP logon event was recorded using the same source IP and target user account. This sequence confirmed that the attacker successfully gained access after repeated credential attempts. Additional log review was performed to identify post-authentication activity such as process execution and file access.

Classification
True Positive – Confirmed Security Incident (Unauthorized Access)

Root Cause
Weak or compromised credentials allowed an attacker to successfully authenticate to the system following a brute force attempt.

Impact Assessment
Unauthorized access to the Windows system was confirmed.
Potential exposure of system data and configurations.
Risk of further actions such as lateral movement or malware execution.
No evidence of data exfiltration observed during initial analysis (lab scenario).

Response Actions
The incident was escalated due to confirmed compromise.
The affected Windows system was isolated from the network (simulated).
The compromised user account was disabled and credentials were reset.
The attacking source IP was blocked at the firewall level.
Enhanced monitoring was enabled for related accounts and systems.

Lessons Learned

RDP brute force attacks can quickly escalate into full system compromise if weak credentials are used. Correlating failed and successful authentication events is critical for identifying successful attacks. Immediate containment actions significantly reduce the risk of further attacker activity.

MITRE ATT&CK Mapping

mitre.id T1550.002 T1078.002 T1021.001
mitre.tactic   Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access
mitre.technique Pass the Hash, Domain Accounts, Remote Desktop Protocol

Incident Status

Closed – Remediated (Test Case Validation)