Table of Contents

Cybersecurity Incident Report

Incident Title:
Unauthorized Remote Access via RDP Brute Force Attack

Date of Detection:
May 9, 2025

Reported By:
Karthik S Arkasali, Security Analyst

Detection Method:
Windows Event Logs (Event ID 4625, 4624), Network Traffic Analysis, Manual Log Review

---

1. Executive Summary

On May 9, 2025, a brute-force attack targeting the Remote Desktop Protocol (RDP) service of a Windows Server (IP: 192.168.32.128) was detected through the combination of Windows Event Log analysis (Event ID 4625) and network monitoring. The source of the attack was identified as a Kali Linux machine with IP address 192.168.32.134.

The attacker conducted an unauthorized login attempt using the default "Administrator" username and a commonly known password list (rockyou.txt). Approximately 1,000 login attempts were made within a short timeframe before detection and intervention occurred. This indicated a systematic brute-force attempt to compromise the account.

Immediate response actions included disabling the target account, blocking the attacker's IP address at the firewall level, and exporting all related security logs for forensic review. The system was not compromised, and no unauthorized access was confirmed.

This incident served as a controlled security test to evaluate the effectiveness of detection and response mechanisms. All security controls functioned as intended, and the event highlighted the importance of continuous monitoring, proactive defenses, and proper access control policies.

2. Investigation

Technical Details: Indicators of Compromise (IOCs)

Indicator	Description
Source IP	192.168.32.134 (Kali Linux host)
Target IP	192.168.32.128 (Windows Server)
Port	TCP 3389 (RDP)
Logon Type	10 (RemoteInteractive)
Username	Administrator
Password List	/usr/share/wordlists/rockyou.txt
Attempted Logins	Approx. 1000 before success

3. Timeline of Events

Time (UTC)	Event Description
09:03 AM	Detection of repeated failed RDP logins (4625)
09:05 AM	Source IP identified as Kali Linux host
09:06 AM	Successful login detected (Event ID 4624)
09:07 AM	Administrator account disabled
09:08 AM	Attacker IP blocked via Windows Firewall
09:10 AM	Administrator password reset
09:15 AM	Logs exported for forensic investigation

3. Incident Discovery

The incident was initially detected through the monitoring of Windows Event Logs. Event ID 4625, which indicates failed login attempts, was triggered multiple times, signaling a potential brute-force attack. Upon initial review, the log entries indicated repeated failed login attempts for the "Administrator" account over a short period, originating from an external IP address (192.168.32.134).

Log Analysis

The investigation began with a thorough review of the event logs captured in the Windows Event Viewer. The relevant logs showed a consistent pattern of failed login attempts using the "Administrator" account, which is a common target for attackers leveraging brute-force methods. The failure reason in the logs was consistently recorded as "Unknown username or bad password," with the logon type specified as "RemoteInteractive" (indicating RDP).

A sample log entry was extracted for further analysis:

Log Details:

- **Event ID:** 4625
- **Failure Reason:** Unknown user name or bad password
- **Logon Type:** 10 (RemoteInteractive / RDP)
- **Username:** Administrator
- **Caller IP:** 192.168.32.134 (Attacker's machine)
- **Attempts:** Approximately 1,000 failed login attempts

The logs revealed that the attacker attempted to gain access using a commonly known wordlist, "rockyou.txt," which is typically used in password-cracking attempts. The system did not allow any successful logins, as evidenced by the repeated failures.

Network Traffic Analysis

In parallel with the log analysis, network traffic was analyzed for any signs of malicious activity. The attacker’s IP address (192.168.32.134) was observed trying to connect to the RDP service on port 3389 (TCP). Network traffic capture tools indicated that the login attempts were sent at a high frequency, which is characteristic of brute-force attacks.

Additionally, packet analysis did not reveal any indications of exploitation of vulnerabilities or system compromise. The attacker used an automated tool to carry out the attack, which further confirmed the brute-force nature of the incident.

Identification of Attacker's IP and Source

The attacker’s machine was identified as a Kali Linux system (IP: 192.168.32.134). This platform is often used for penetration testing and malicious activities due to its powerful tools for network exploration and exploitation. The identification of this source helped to classify the incident as an external attack rather than an internal threat.

Attempts and Impact Assessment

The total number of failed attempts was estimated at around 1,000 before the attacker was detected and blocked. However, no successful logins were recorded, and no unauthorized access was achieved.

The impact of the incident was minimal, as the attacker did not manage to gain control over the target system. Nevertheless, the repeated nature of the brute-force attempts indicated that the system was a potential target for further attacks, requiring immediate intervention and hardening of security measures.

4. Response and Remediation

As soon as the brute-force attack was detected, several immediate response actions were initiated to mitigate potential damage and prevent further attempts:

1. **Account Lockout and Disablement:**

- The "Administrator" account, which was being targeted, was immediately disabled to prevent any further login attempts from the attacker.
- **Command executed:** net user Administrator /active:no

  This action ensured that the attacker could not gain access even if they managed to guess the correct password.

2. **IP Blockage:**

- The IP address of the attacker (192.168.32.134) was blocked through the Windows Firewall to prevent any further connection attempts from the external source.

- **Command executed:** New-NetFirewallRule -DisplayName "Block Attacker" -Direction Inbound -RemoteAddress 192.168.32.134 -Action Block

This was done to ensure that the attacker could not initiate any further connection requests.

3. **Log Export for Forensic Analysis:**

- The relevant Windows security logs, including Event ID 4625, were exported for further forensic analysis and investigation.
- **Command executed:** wevtutil epl Security RDP-Attack.evtx

These logs were sent to the Security Operations Center (SOC) for further investigation and retention as part of the incident documentation.

Remediation Actions Taken

1. **Password Change and Security Hardening:**

- Once the "Administrator" account was disabled, a strong password policy was enforced across all user accounts to avoid easy guessing through brute-force attacks.
- A complex password was set for the "Administrator" account once it was re-enabled, and it was ensured that the password was not part of common wordlists like "rockyou.txt."

2. **Review and strengthening of RDP Security:**

- **RDP Access Restriction:** Access to RDP was restricted to a VPN and a jump server to limit exposure from external networks. This prevented direct access from the open internet.
- **Multi-Factor Authentication (MFA):** MFA was implemented for all RDP login attempts to add an additional layer of protection against future brute-force attacks.

3. **Intrusion Detection and Prevention System (IDPS) Configuration:**

- The Intrusion Detection and Prevention System (IDPS) was configured to detect and block excessive failed login attempts, enforcing automatic account lockouts after a set number of failed attempts.

4. **System Patch and Updates:**

- A review of the system's patch status was performed. Any missing security updates or patches related to RDP and authentication services were promptly installed to ensure the system was up to date.

5. Lessons Learned and Process Improvement

The incident highlighted several key areas for improvement in the organization's security posture:

- **Account Lockout Policy Enforcement:** The importance of enforcing a strict account lockout policy after a certain number of failed login attempts was reinforced. This can prevent brute-force attempts from progressing too far.
- **Network Segmentation for RDP Access:** Direct RDP access from external sources should be avoided whenever possible. Utilizing jump servers and VPNs can significantly reduce the attack surface and provide an additional layer of security.
- **Stronger Password Policies:** Passwords should be made more complex and unique. Utilizing password managers and enforcing password complexity policies can reduce the risk of successful brute-force attacks.