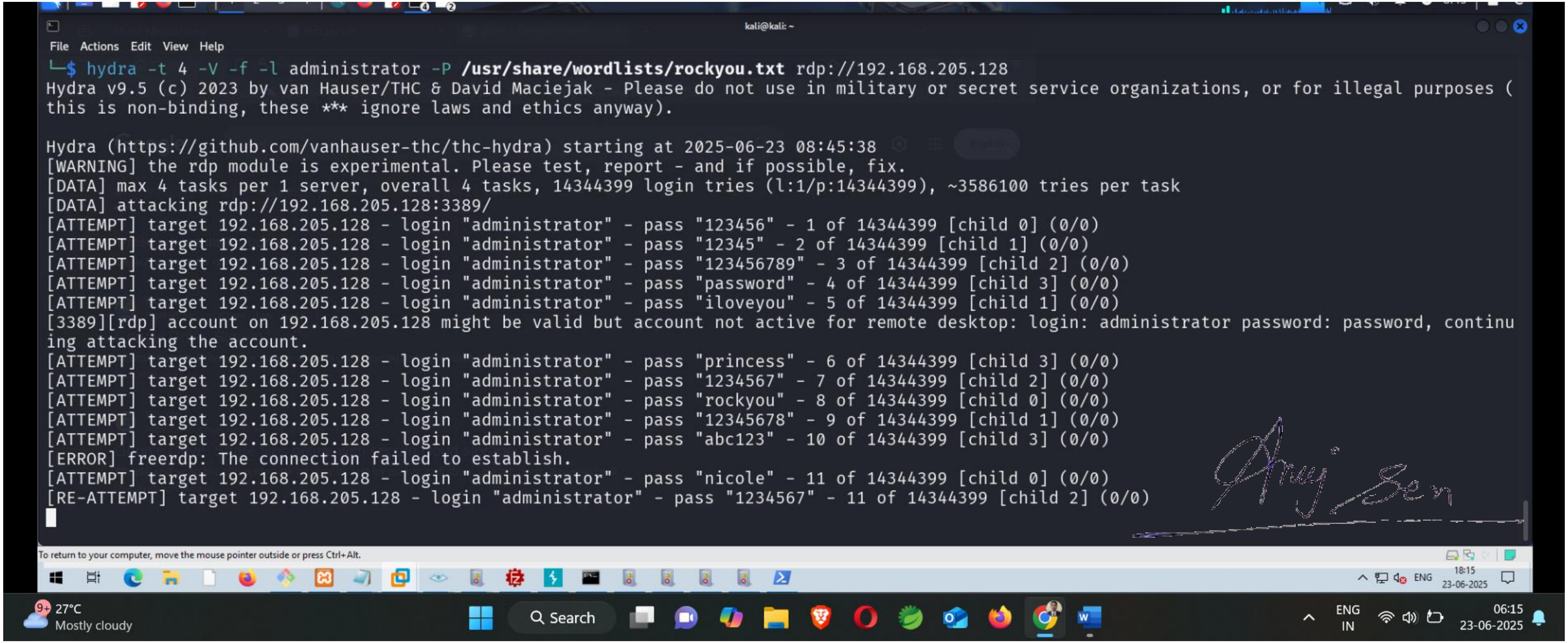
Brute-Force Attack & Account Lockout Response

This presentation details a simulated brute-force attack. We explore detection, response, and mitigation strategies. This project used Kali Linux and Windows Server 2022.


kali@kali: ~
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
ENG
18:15
23-06-2025
9+
27°C
Mostly cloudy
Search
ENG
IN
06:15
23-06-2025

```
└─$ hydra -t 4 -V -f -l administrator -P /usr/share/wordlists/rockyou.txt rdp://192.168.205.128
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-23 08:45:38
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking rdp://192.168.205.128:3389/
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[3389][rdp] account on 192.168.205.128 might be valid but account not active for remote desktop: login: administrator password: password, continu
ing attacking the account.
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "princess" - 6 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "1234567" - 7 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "rockyou" - 8 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "12345678" - 9 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "abc123" - 10 of 14344399 [child 3] (0/0)
[ERROR] freerdp: The connection failed to establish.
[ATTEMPT] target 192.168.205.128 - login "administrator" - pass "nicole" - 11 of 14344399 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.205.128 - login "administrator" - pass "1234567" - 11 of 14344399 [child 2] (0/0)
```

Anuj Sen

Attack Simulation: The Brute-Force

Hydra Execution

The brute-force attack was executed using Hydra. This tool is effective for testing login security.

Targeted RDP

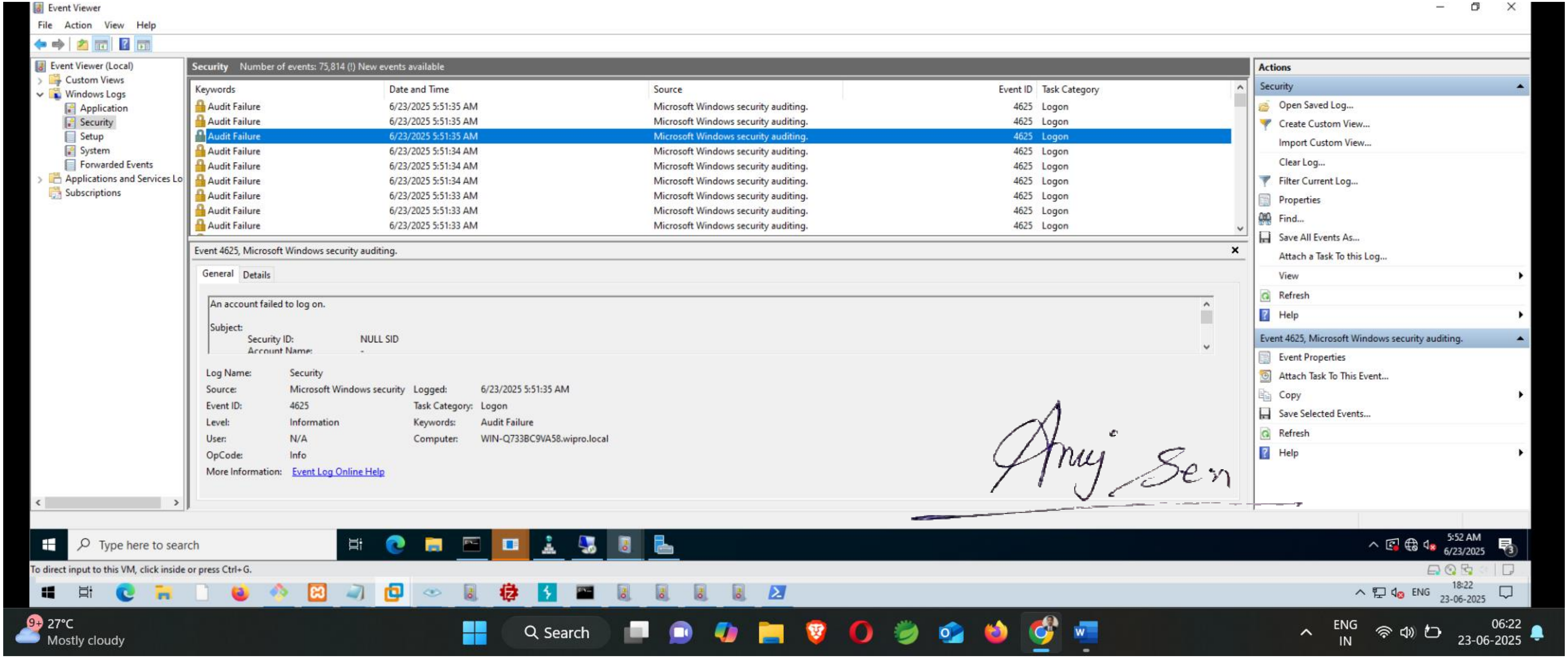
The attack specifically targeted the Remote Desktop Protocol (RDP) login. It aimed for the administrator account.

Command Example

```
hydra -t 4 -V -f -l administrator -P
/usr/share/wordlists/rockyou.txt
rdp://192.168.205.128
```

```
hhyldexa
hy usera.. -itslegetit
      A
t in -P passwordislisttxt.il
ishds//tirce_ip
```

Event Log Analysis



Security Number of events: 75,814 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	6/23/2025 5:51:35 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:35 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:35 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:34 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:34 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:34 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:33 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:33 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	6/23/2025 5:51:33 AM	Microsoft Windows security auditing.	4625	Logon

Event 4625, Microsoft Windows security auditing.

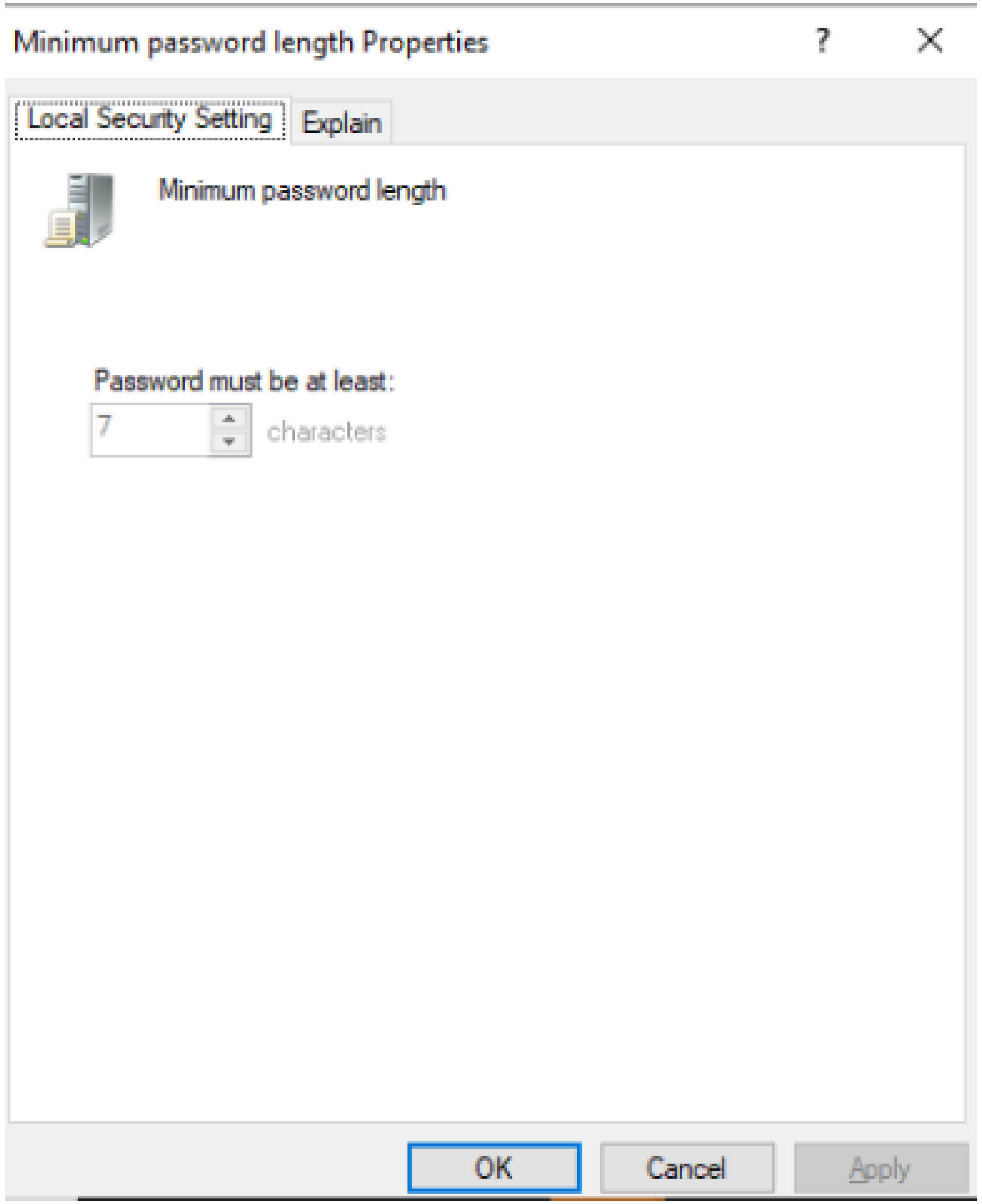
```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/23/2025 5:51:35 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	WIN-Q733BC9VA58.wipro.local
OpCode:	Info		
More Information:	Event Log Online Help		

Anuj Sen

To direct input to this VM, click inside or press Ctrl+G.

Attack Identification Through Logs



Minimum password length Properties

Minimum password length

Password must be at least:

7 characters

Event Viewer Analysis

Windows Event Viewer was crucial for identification. It provided detailed log data.

Identifying Failed Logins

Event ID 4625 clearly showed each failed login attempt. This log is vital for detection.

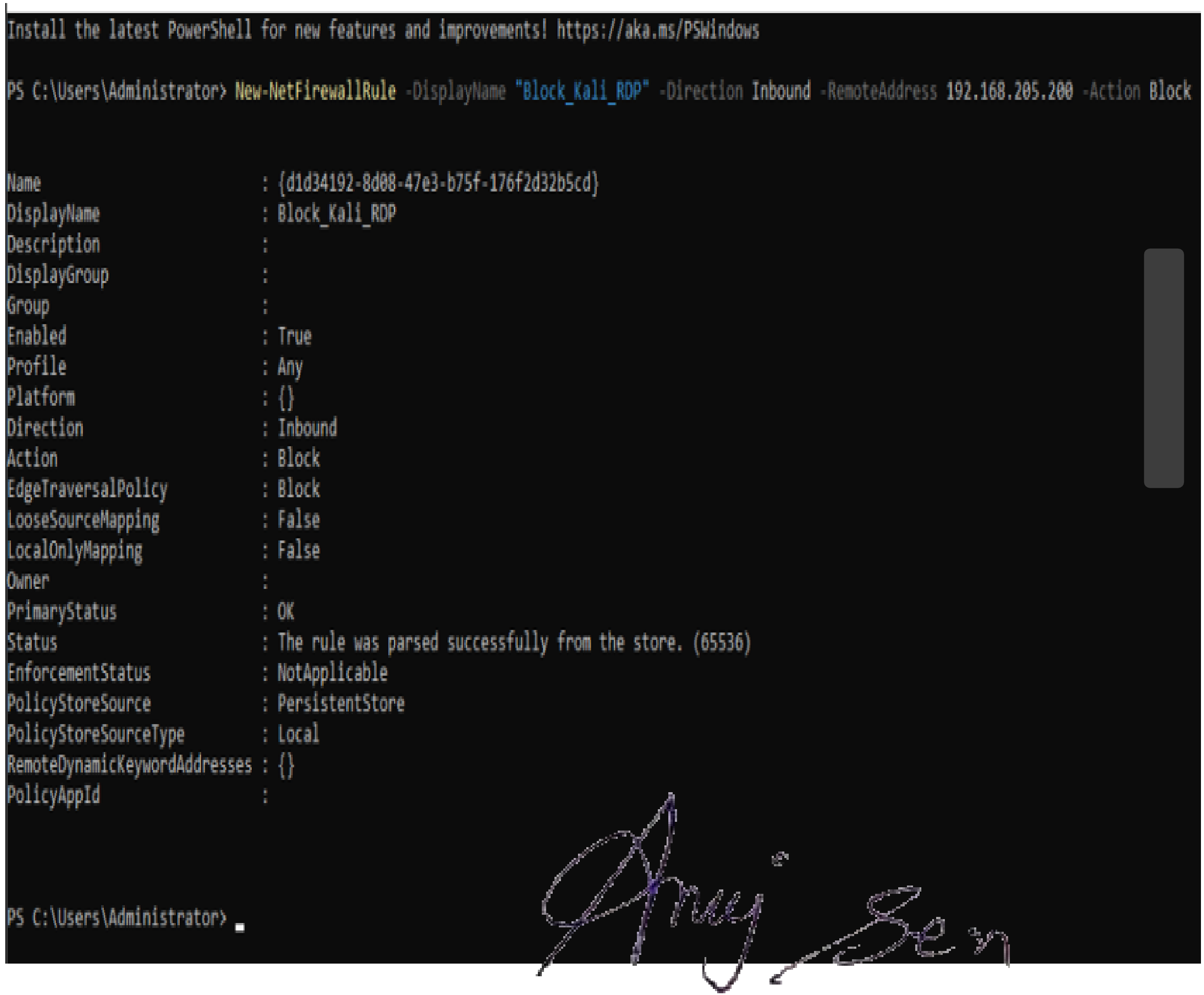
Account Lockout Detection

Event ID 4740 confirmed automatic account lockouts. This indicates a protective measure triggering.

Source & Target Tracing

The attacker IP was **192.168.205.200**. Targeted usernames were **administrator** and **BruteTest1**.

Incident Response Plan



```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "Block_Kali_RDP" -Direction Inbound -RemoteAddress 192.168.205.200 -Action Block


Name                          : {d1d34192-8d08-47e3-b75f-176f2d32b5cd}
DisplayName                   : Block_Kali_RDP
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :



PS C:\Users\Administrator>
```

Anuj Sen

Analyze & Extract

Analyze failed logins and extract the attacker's source IP address.

Block IP

Block the identified malicious IP using Windows Firewall rules.

Reset Password

Reset the password for the affected user account immediately.

Apply Lockout Policy

Implement a strong account lockout policy via Group Policy Objects (GPO).

Mitigation Measures & Policy Enforcement

Account Lockout Policy

Threshold

Configure lockout after **3** failed attempts. This prevents rapid guessing.

Lockout Duration

Set account lockout for **30 minutes**. This provides a cooling-off period.

Password Policy & Remote Access

Complexity & Length

Enforce strong password complexity. Require **12+ characters**, including special characters.

RDP & SSH Control

Limit RDP to VPN or IP allow-lists. Disable SSH root access for security.

Recovery Actions: Post-Attack Response

IP Blocked

The attacker's IP (192.168.205.200) was successfully blocked.

Account Locked

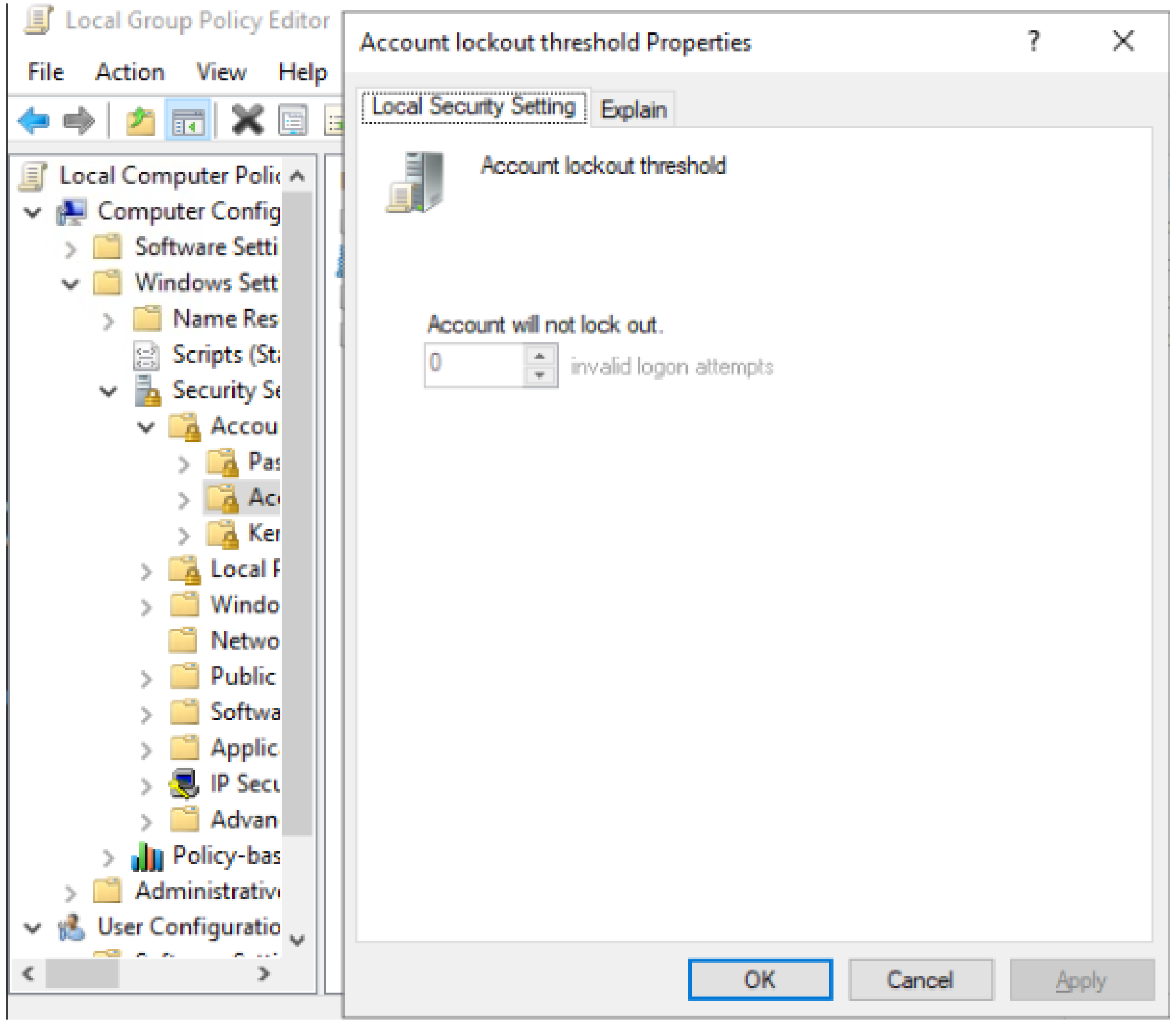
Account locked automatically by policy (Event ID 4740).

Password Reset

Administrator account password was reset to a new, strong value.

Policies Applied

New account lockout and password policies were fully enforced.



Account lockout threshold Properties

Account lockout threshold

Account will not lock out.

0 invalid logon attempts

Lessons Learned & Future Hardening

Password Vulnerability

Brute-force attacks can bypass weak passwords. Strong policies are key.

Proactive Lockout

Account lockout policy should be active from the start. Early detection is crucial.

Continuous Monitoring

Continuous log monitoring is vital for quick threat identification. Tools like Fail2Ban help.

Service Hardening

Harden remote access services before exposure. Regular security audits are necessary.