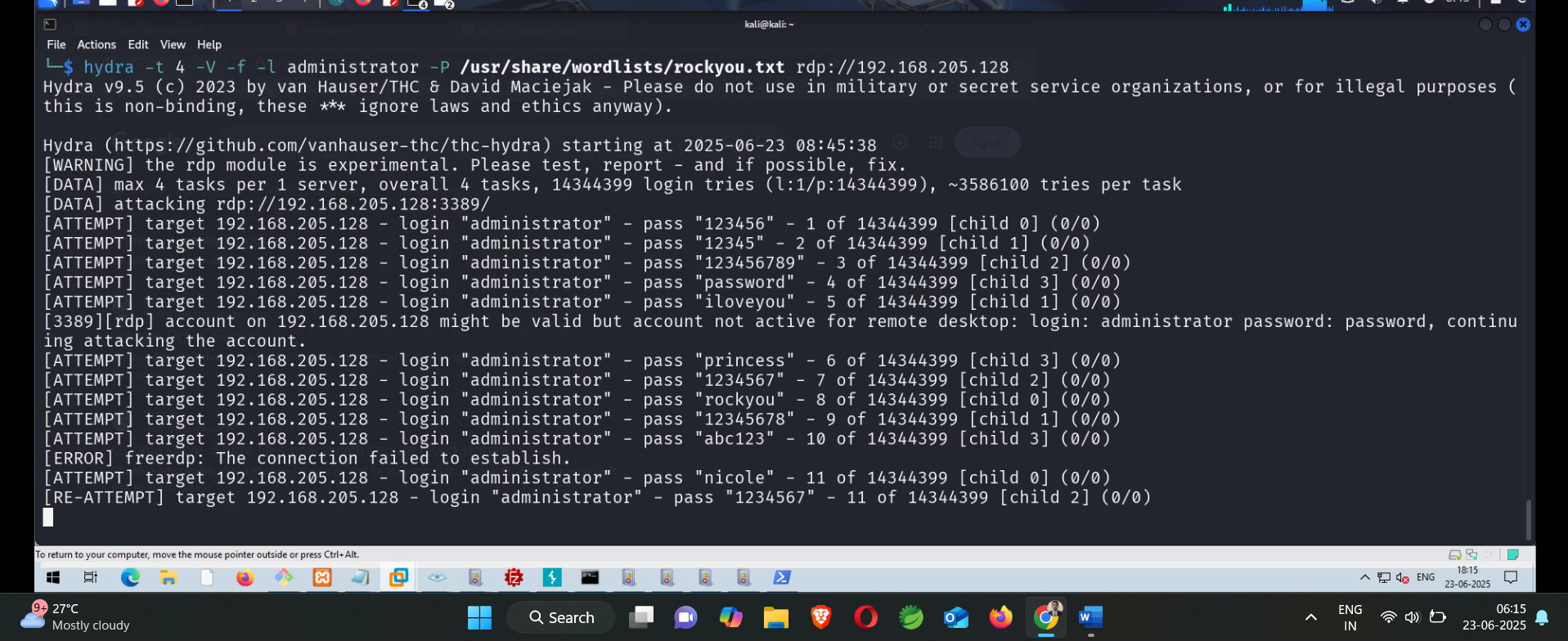
Brute-Force Attack & Account Lockout Response

This presentation details a simulated brute-force attack. We explore detection, response, and mitigation strategies.

This project used Kali Linux and Windows Server 2022.

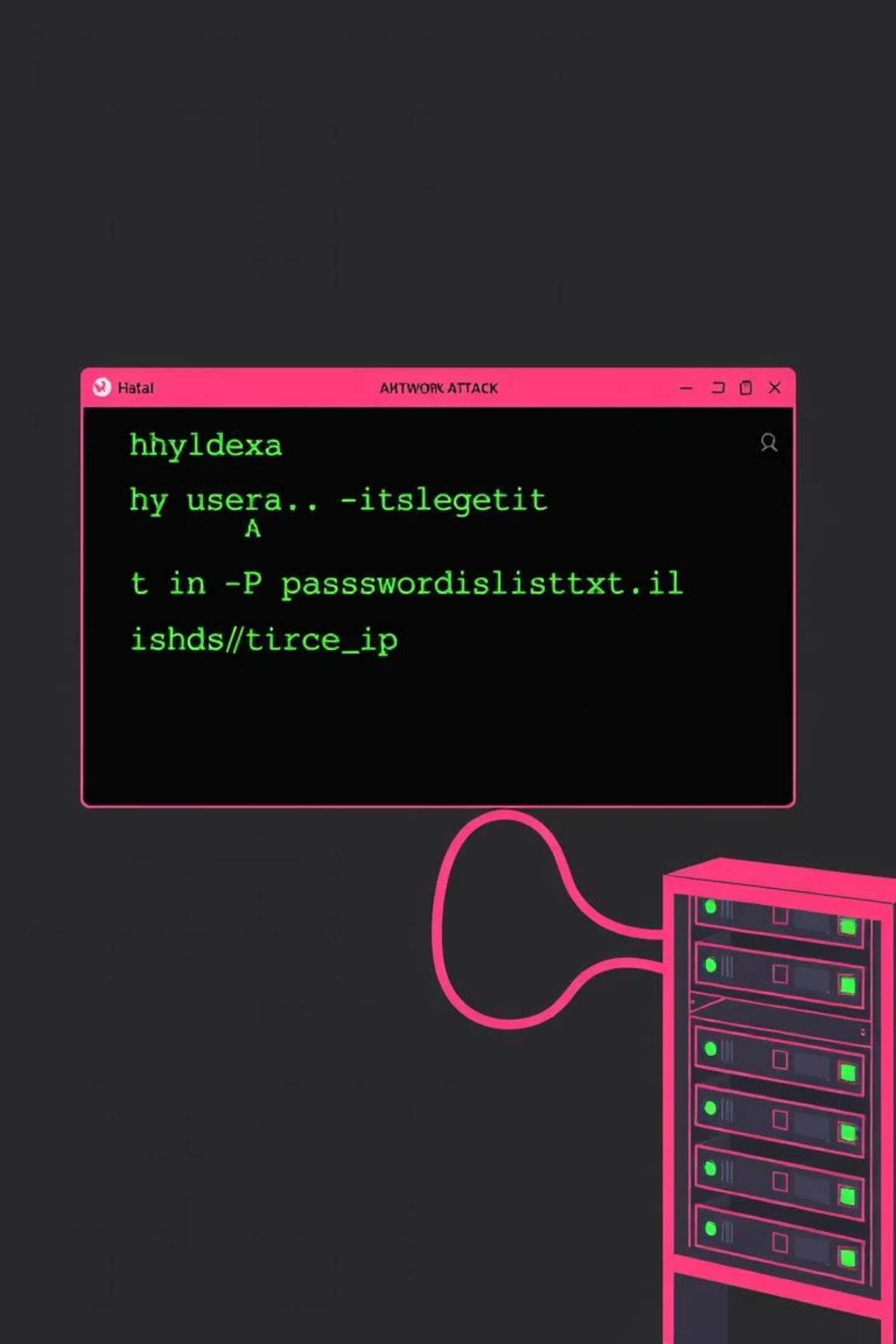




**Step 1 :** hydra -t 4 -V -f -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://<target-ip>

**Step 2:This will Trigger Various Logon Failed Attempts which can be viewed on Event Viewer where we can see Source IP and other details.**

**Step 3:This is how Attack Simulation Works (Phase 1)**



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

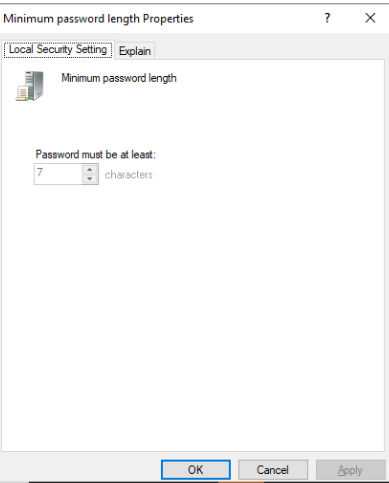
hydra -t 4 -V -f -l administrator -P

/usr/share/wordlists/rockyou.txt

rdp://192.168.205.128

# Event Log Analysis



Attack Identification Through Logs

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

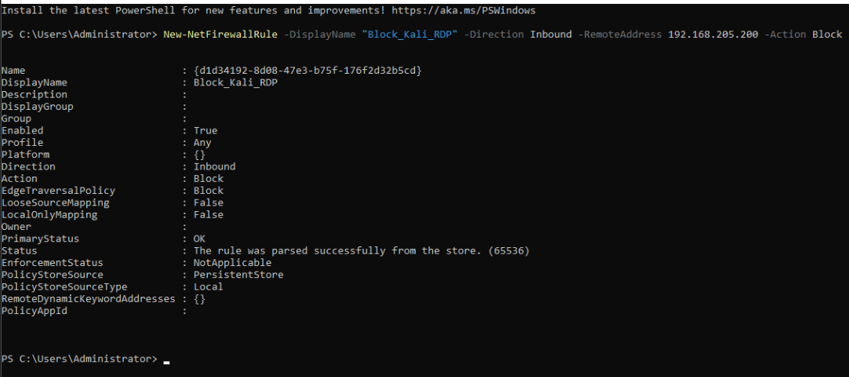
**Event ID 4740** confirmed automatic account lockouts. This indicates a protective

measure triggering.

Source & Target Tracing

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

**BruteTest1**.



Incident Response Plan

### 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.

## Password Policy & Remote Access Complexity & Length

Enforce strong password complexity. Require **12+**

**characters**, including special characters.

## Lockout Duration

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

## RDP & SSH Control

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

Recovery Actions: Post-Attack Response

### preencoded.png IP Blocked

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

### preencoded.pngAccount Locked

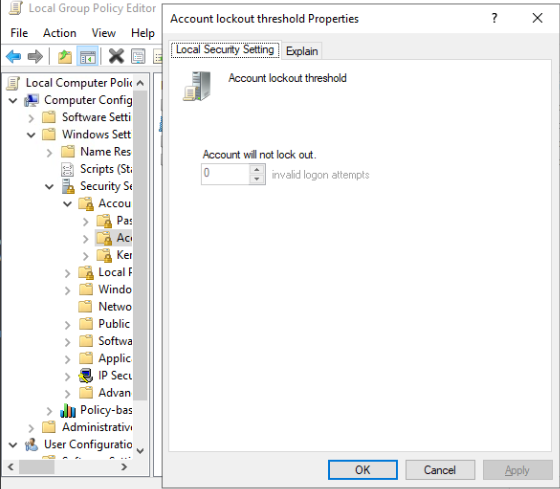
Account locked automatically by policy (Event ID 4740).

### preencoded.pngPassword Reset

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

### preencoded.pngPolicies Applied

New account lockout and password policies were fully enforced.



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.