Incident Response Report – Brute Force Login Detection

# 1. Executive Summary

This report documents a simulated brute-force login attack detection scenario on a Windows 10 system in a virtual SOC lab environment. The attack was executed both internally via a PowerShell script and externally using Hydra from a Kali Linux VM. Detection was achieved through Splunk SIEM log correlation using Event ID 4625 (logon failures) and validated through SPL-based statistical aggregation. The attack successfully triggered account lockouts (Event ID 4740), confirming detection logic.

# 2. Threat Intelligence Summary

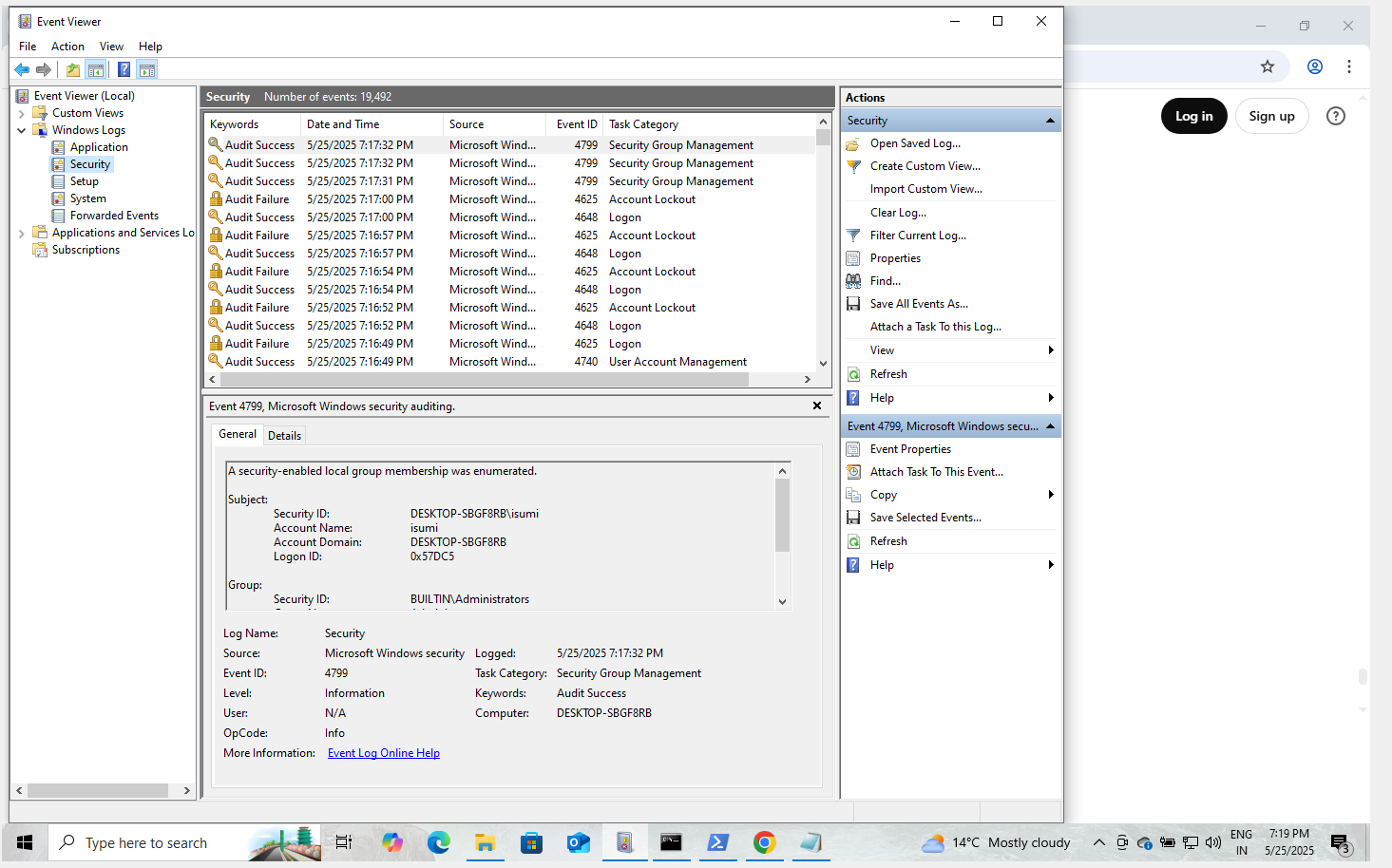
|  |  |
| --- | --- |
| Field | Value |
| Tactic | Credential Access |
| Technique | T1110.001 – Brute Force: Password Guessing |
| Detection Method | Log Correlation (SPL) |
| Tool Used | PowerShell (internal), Hydra (external) |
| Affected User | testuser |
| Log Source | WinEventLog:Security |
| Outcome | Account Lockout (Event ID 4740) |

# 3. Attack Simulation Overview

The attack was simulated in two phases:  
  
1. Internal brute-force using PowerShell to simulate repeated login failures on localhost (127.0.0.1).  
2. External brute-force using Hydra (rdp module) from Kali Linux targeting Windows RDP service over LAN.

## Internal PowerShell Simulation Script:

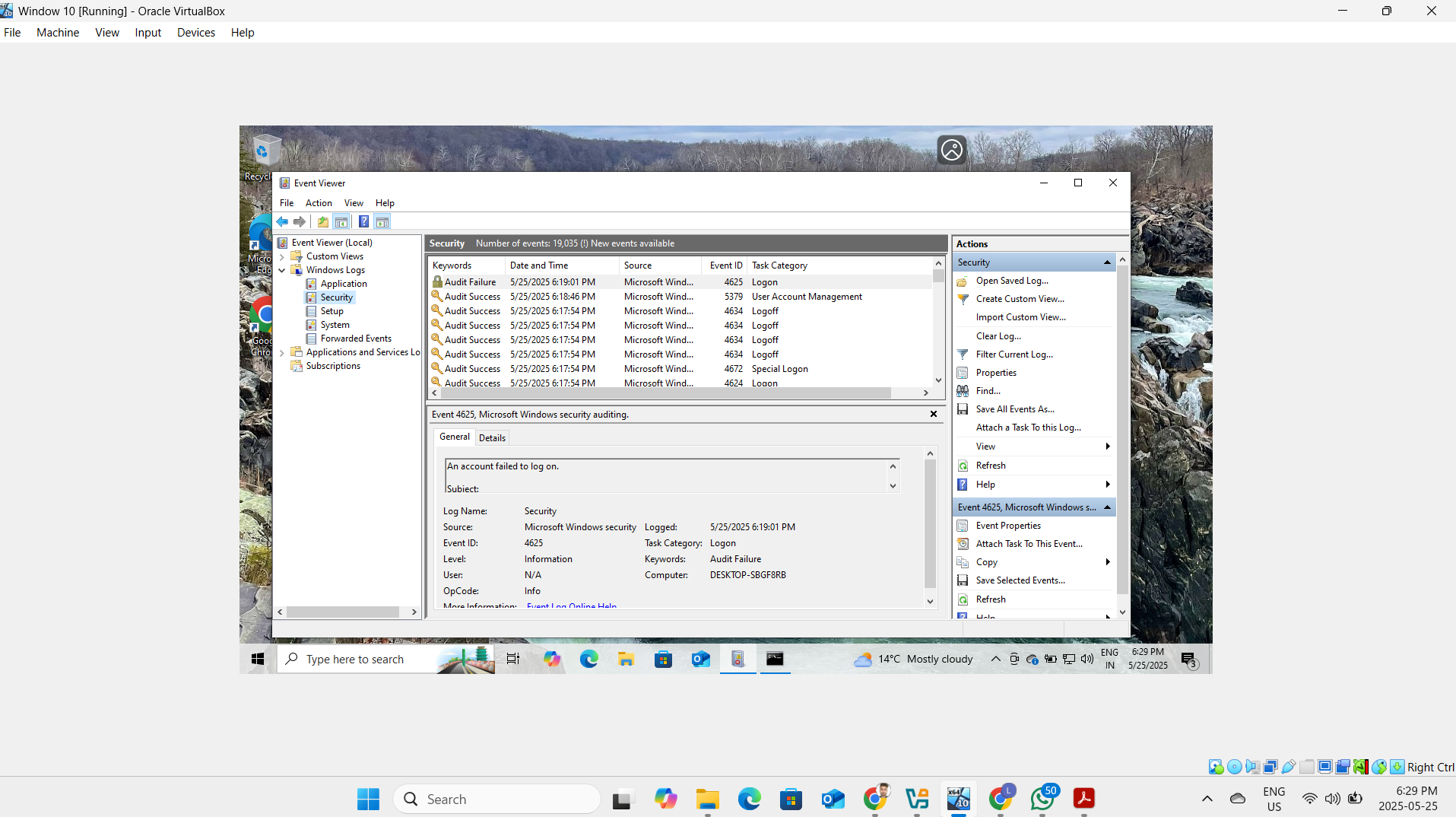
$user = "testuser"  
$wrongpass = "WrongPassword123"  
for ($i = 1; $i -le 15; $i++) {  
 cmd /c "net use \\127.0.0.1\IPC$ /user:$user $wrongpass"  
 Start-Sleep -Milliseconds 500  
}

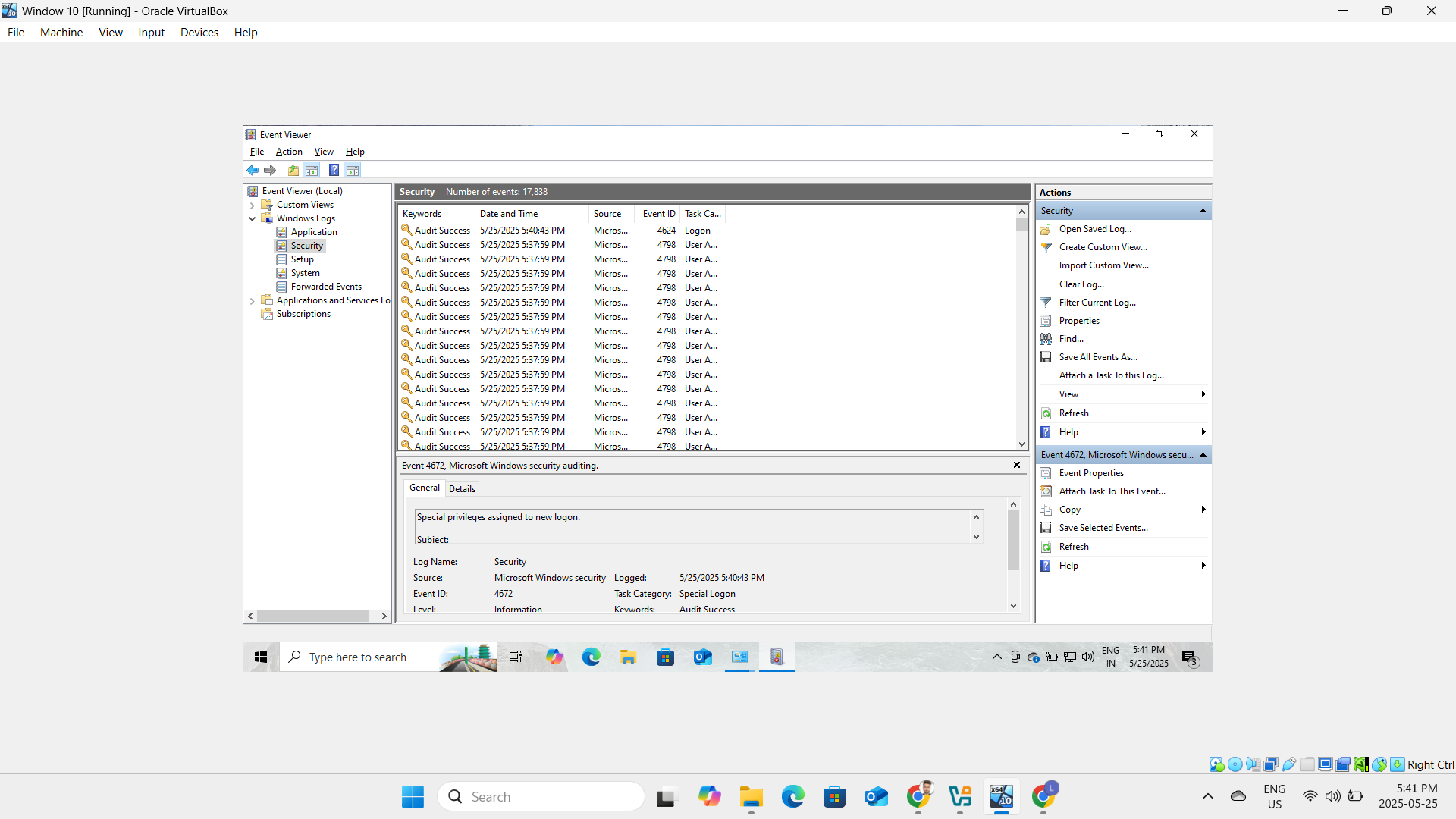


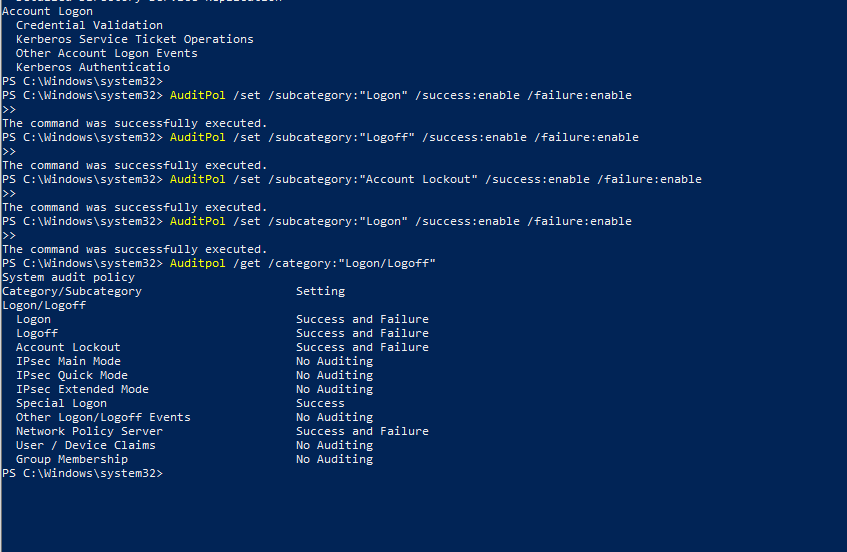
# 4. Log Evidence and Artifacts

Key Windows Event IDs observed:

|  |  |  |
| --- | --- | --- |
| Event ID | Description | Log Source |
| 4625 | Failed Login Attempt | Security |
| 4740 | Account Lockout | Security |
| 4672 | Special Logon | Security |



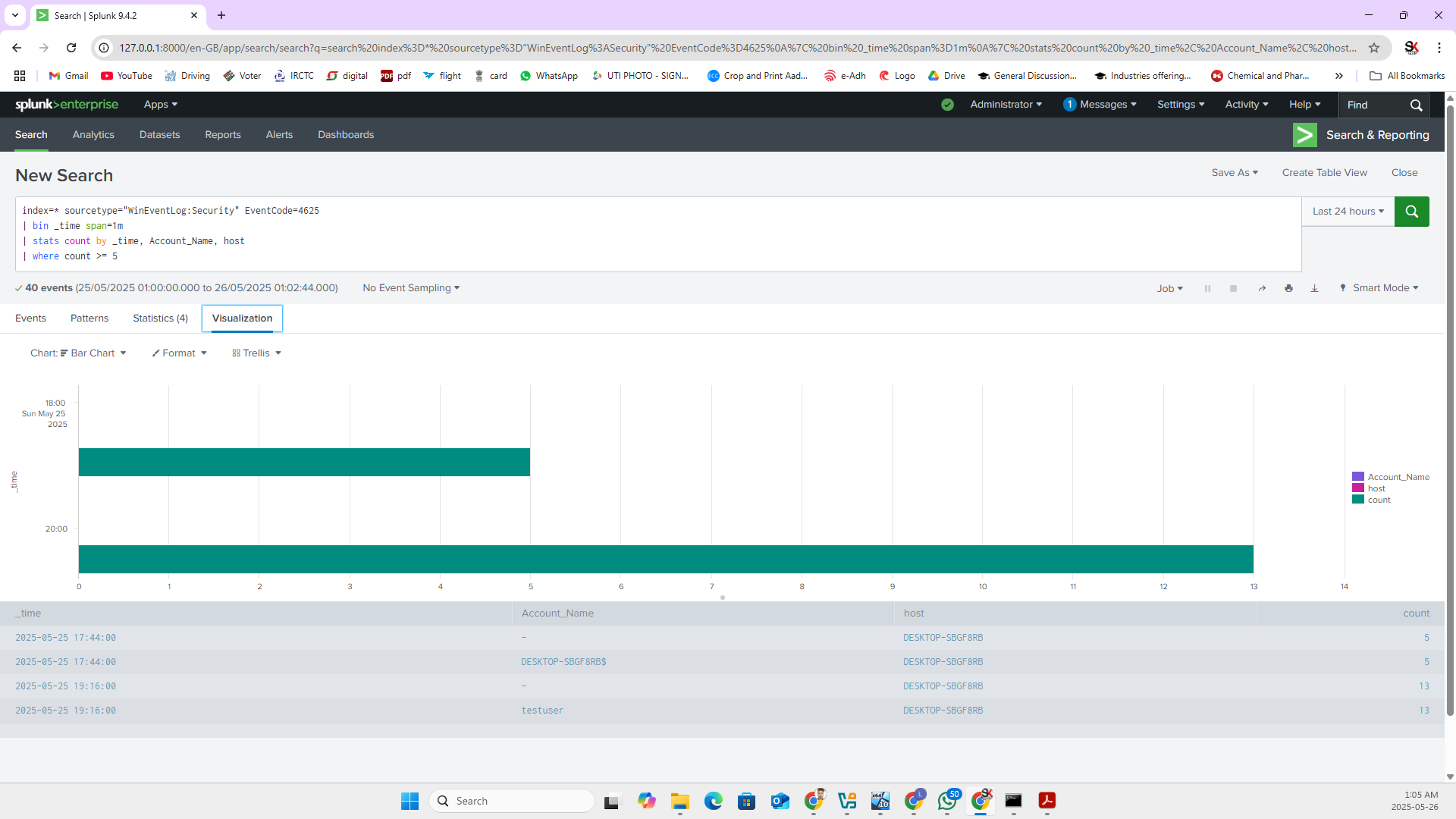


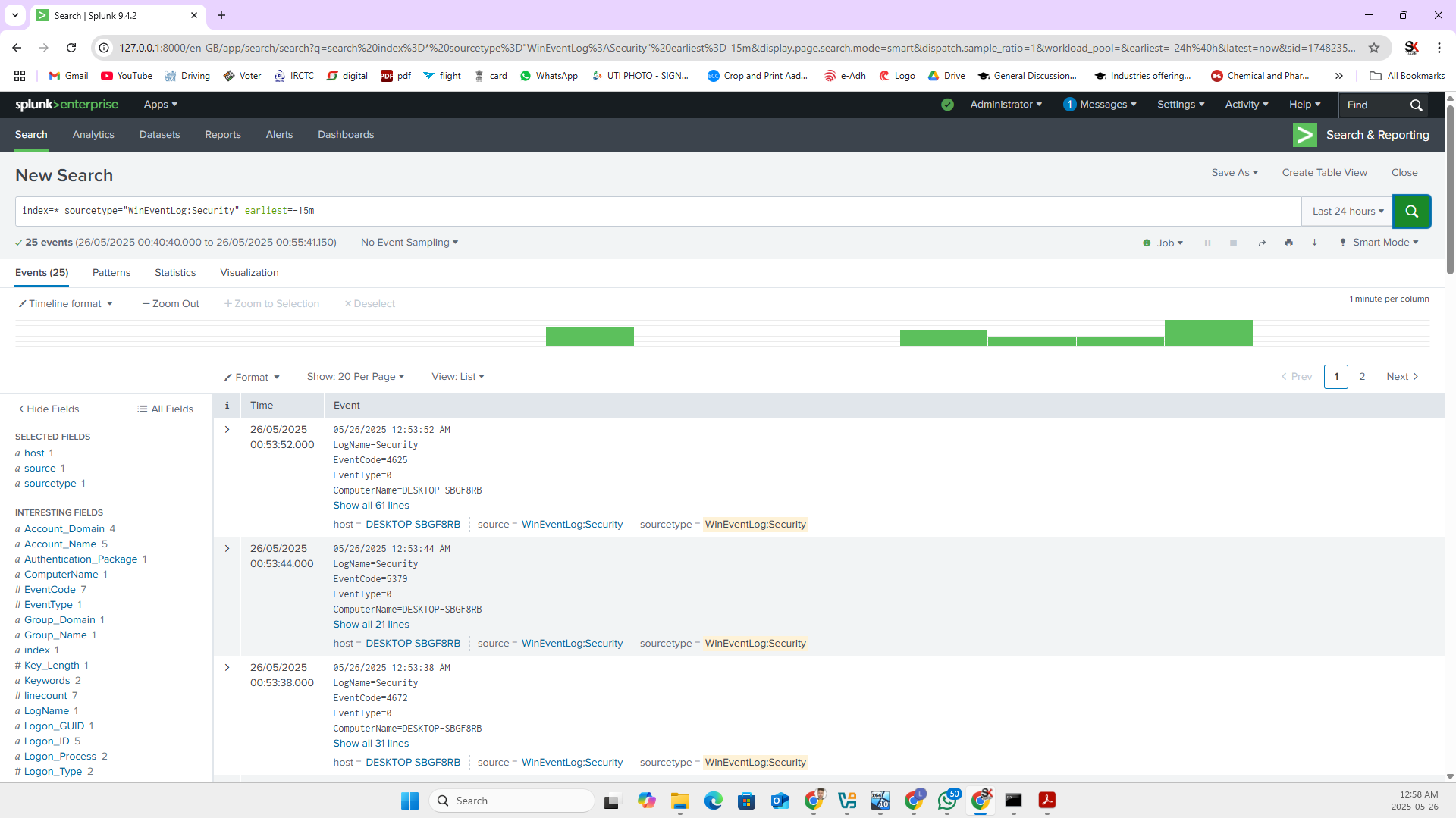


# 5. SPL Query and Detection Logic

Splunk query used to detect excessive login failures within a 1-minute time span:

index=\* sourcetype="WinEventLog:Security" EventCode=4625  
| bin \_time span=1m  
| stats count by \_time, Account\_Name, host  
| where count >= 5

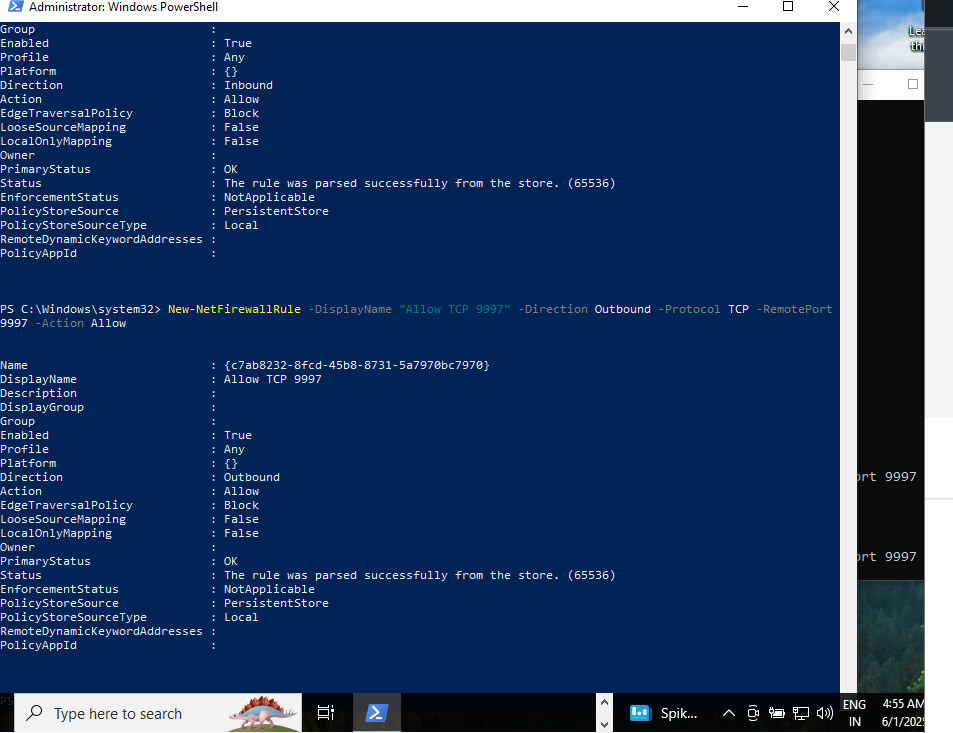




# 6. Network Logging & Configuration

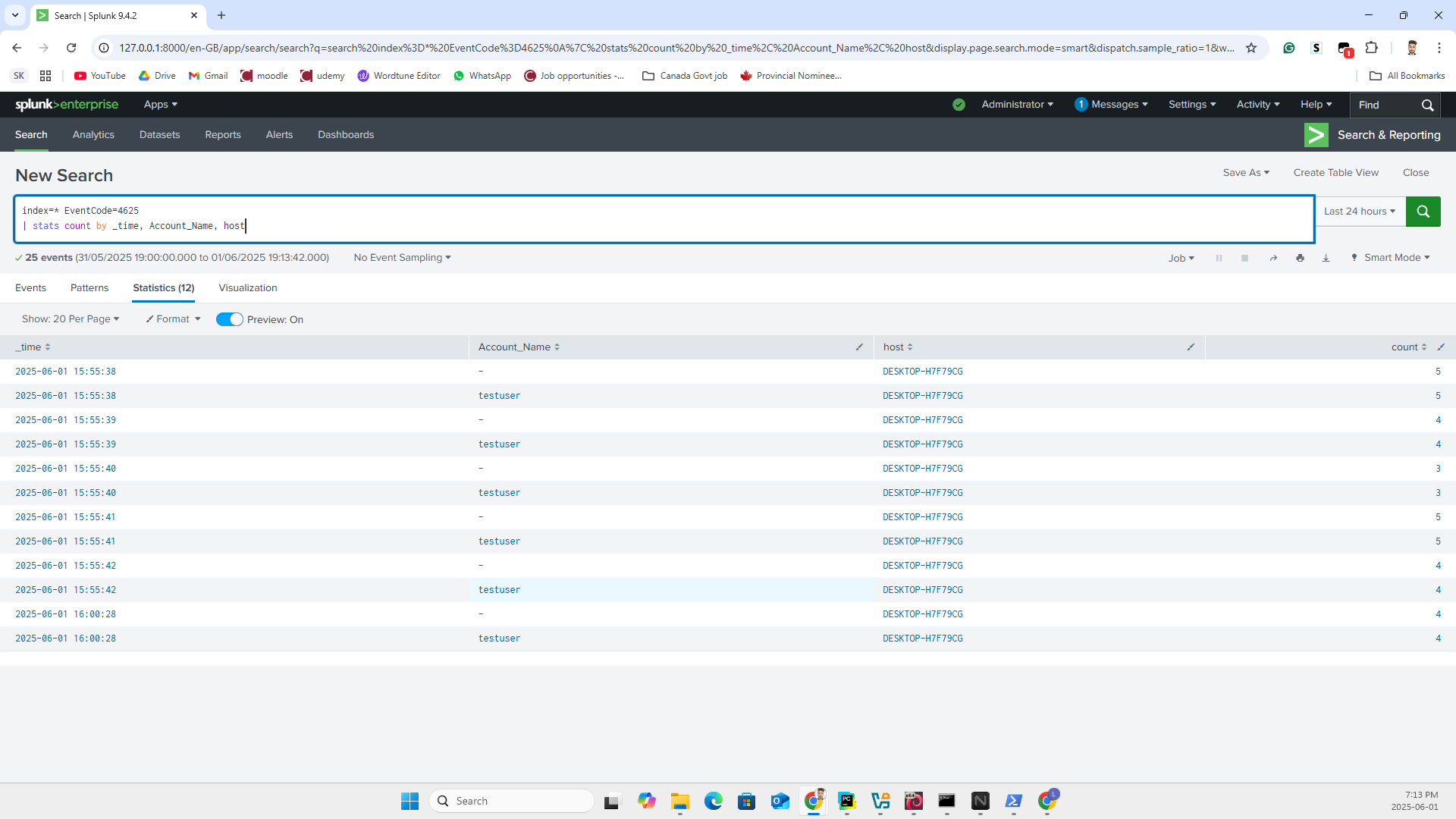
Universal Forwarder was configured to send security logs to the Splunk host over TCP port 9997. Windows Firewall rules were added to allow traffic:

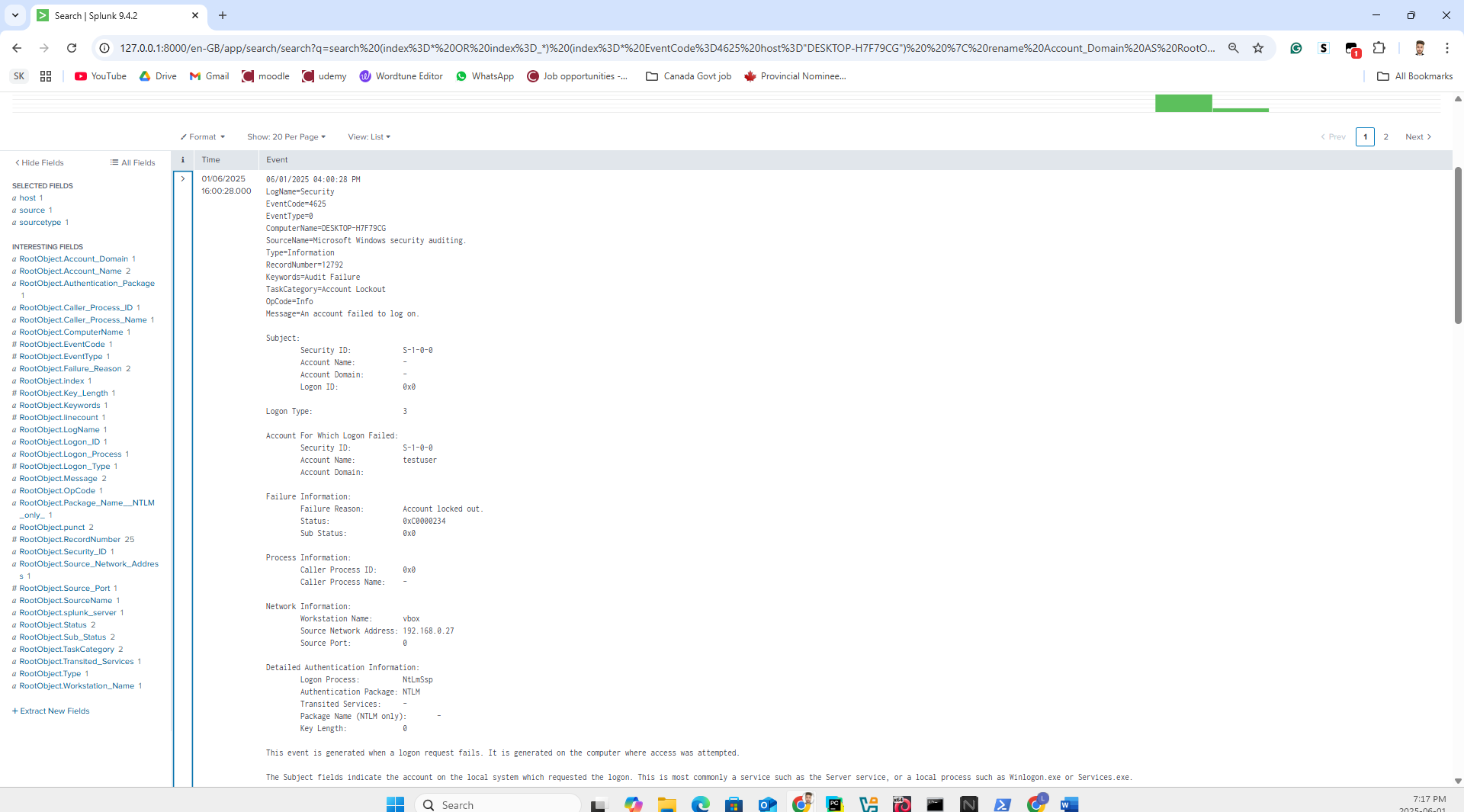
New-NetFirewallRule -DisplayName "Allow TCP 9997" -Direction Outbound -Protocol TCP -RemotePort 9997 -Action Allow

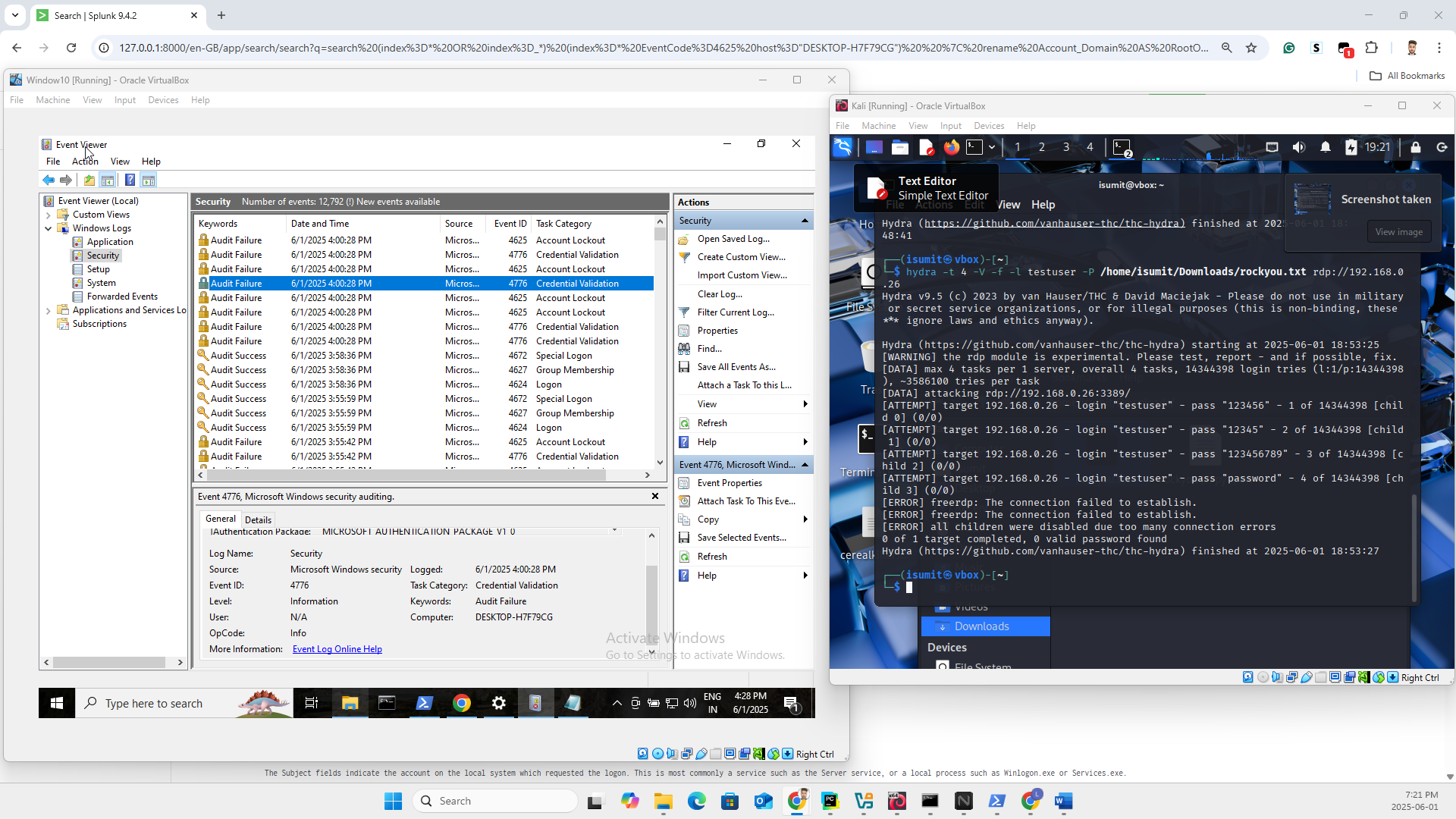


# 7. External Brute-Force Simulation (Hydra)

Hydra was executed from Kali Linux using the rdp module. The RDP brute-force attempt was executed against the target Windows machine (IP masked). The attempt triggered failed login logs visible in both Windows Event Viewer and Splunk interface.







# 8. MITRE ATT&CK Mapping

Technique ID: T1110.001  
Technique Name: Brute Force - Password Guessing  
Tactic: Credential Access  
Platform: Windows  
Data Source: Authentication Logs, Process Logs

# 9. Analyst Summary & Recommendations

• Windows auditing was manually verified and enabled via AuditPol.  
• Splunk Universal Forwarder successfully ingested Event ID 4625/4740 from Windows host.  
• Detection threshold (5 failed logons within 1 minute) correctly triggered alerts.  
• Suggested improvement: Incorporate Event ID 4648 (Explicit Logon) and Event ID 4776 (NTLM Failure).  
• Recommendation: Enable Sysmon with Event ID 1, 3 for process/network context in future detection pipelines.  
• Real-world deployment should include geolocation/IP enrichment and lockout policy enforcement.