# **📄 🔹 Incident Investigation Report Template (Copy-Paste into Word)**

# **Incident Investigation Report – RDP Brute Force Attack**

**Author:** *shrushty pandey* **Date:** *04/12/2025* **Project:** RDP Brute Force Attack Detection (Windows + Hydra)  
 **Tools Used:** Windows Event Viewer, Parrot OS, Hydra,

## **1. Executive Summary**

This investigation analyzes multiple failed Remote Desktop Protocol (RDP) login attempts generated from a controlled brute-force attack in a SOC home lab environment. The goal was to identify, detect, and analyze brute-force behavior using Windows Security logs.

## **2. Objective**

* To simulate a real brute-force attack using Hydra
* To generate Windows Event Logs (4625 – failed login)
* To analyze patterns and identify the attack source
* To create a detection rule (optional)
* To document the findings professionally

## **3. Lab Environment**

| **Component** | **Details** |
| --- | --- |
| **Target Machine** | Windows 10 VM |
| **Attacker Machine** | Parrot OS / Kali Linux |
| **Attack Tool** | Hydra |
| **Network** | Host-only / NAT |
| **User under attack** | FunnyPhisher |
| **Weak Password Used** | abc@123 |

## **4. Attack Simulation**

The following Hydra command was executed from Parrot OS:

hydra -l FunnyPhisher -P /usr/share/wordlists/rockyou.txt -t 1 rdp://192.168.80.134

### **Results:**

* Multiple failed RDP login attempts were generated
* Windows logged Event ID **4625 (Failed login)**
* In some cases Hydra stopped due to RDP throttling
* No successful authentication occurred (intended)

## **5. Log Analysis (Windows Event Viewer)**

### **Navigation Path:**

Event Viewer → Windows Logs → Security → Filter Current Log → Event ID: 4625

### **Key Fields Observed:**

| **Field** | **Example Value** |
| --- | --- |
| Account Name | FunnyPhisher |
| Failure Reason | Unknown username or bad password |
| Source Network Address | 192.168.x.x |
| Logon Type | 10 (Remote / RDP) |
| Timestamp | DD/MM/YYYY HH:MM |

### **Sample Log Entry (summarized):**

Event ID: 4625

Account Name: FunnyPhisher

Logon Type: 10

Source IP Address: 192.168.80.134

Failure Reason: Bad password

## **6. Indicators of Attack**

| **Indicator** | **Details** |
| --- | --- |
| **Source IP** | 192.168.80.134 |
| **Target Username** | FunnyPhisher |
| **Repeated Failures** | 50+ failed attempts |
| **Technique** | Brute Force Attack |
| **MITRE ID** | T1110 – Brute Force |

## **7. Detection Rule (Optional)**

If using SIEM like Splunk/ELK/Wazuh:

### **Sample SIEM Query:**

EventID=4625 OR event.code:4625

| stats count by account.name, source.ip

| where count > 5

### **Wazuh Rule Example:**

<rule id="100050" level="6">

<if\_sid>60107</if\_sid>

<frequency>5</frequency>

<timeframe>60</timeframe>

<description>Possible RDP brute-force detected</description>

</rule>

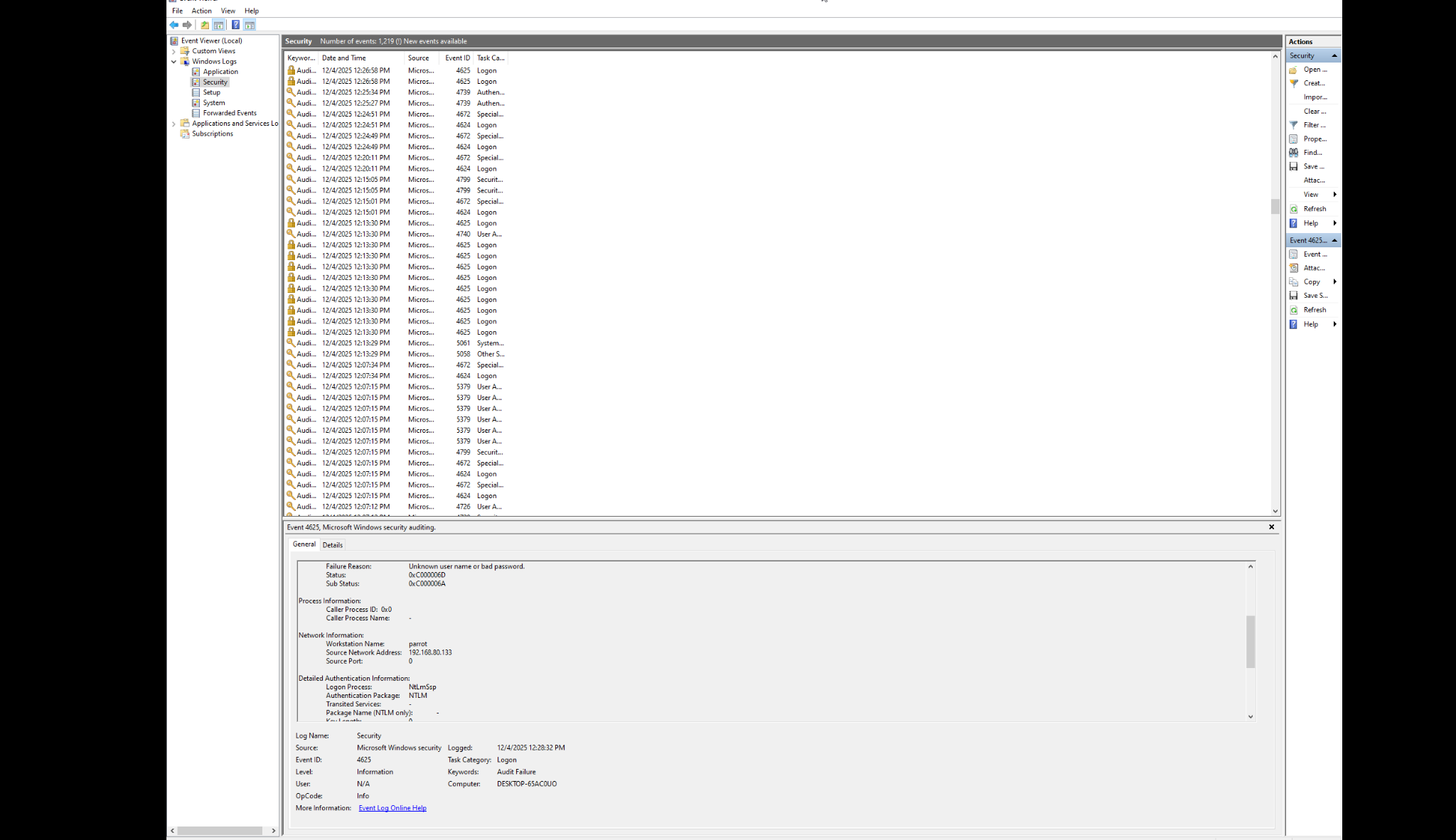
## **8. Conclusion**

The brute-force attack was successfully detected using Windows Event ID 4625.  
 Logs clearly indicate repeated failed RDP login attempts from attacker IP 192.168.x.x.  
 These findings confirm that monitoring Security logs is effective for detecting brute-force behavior.

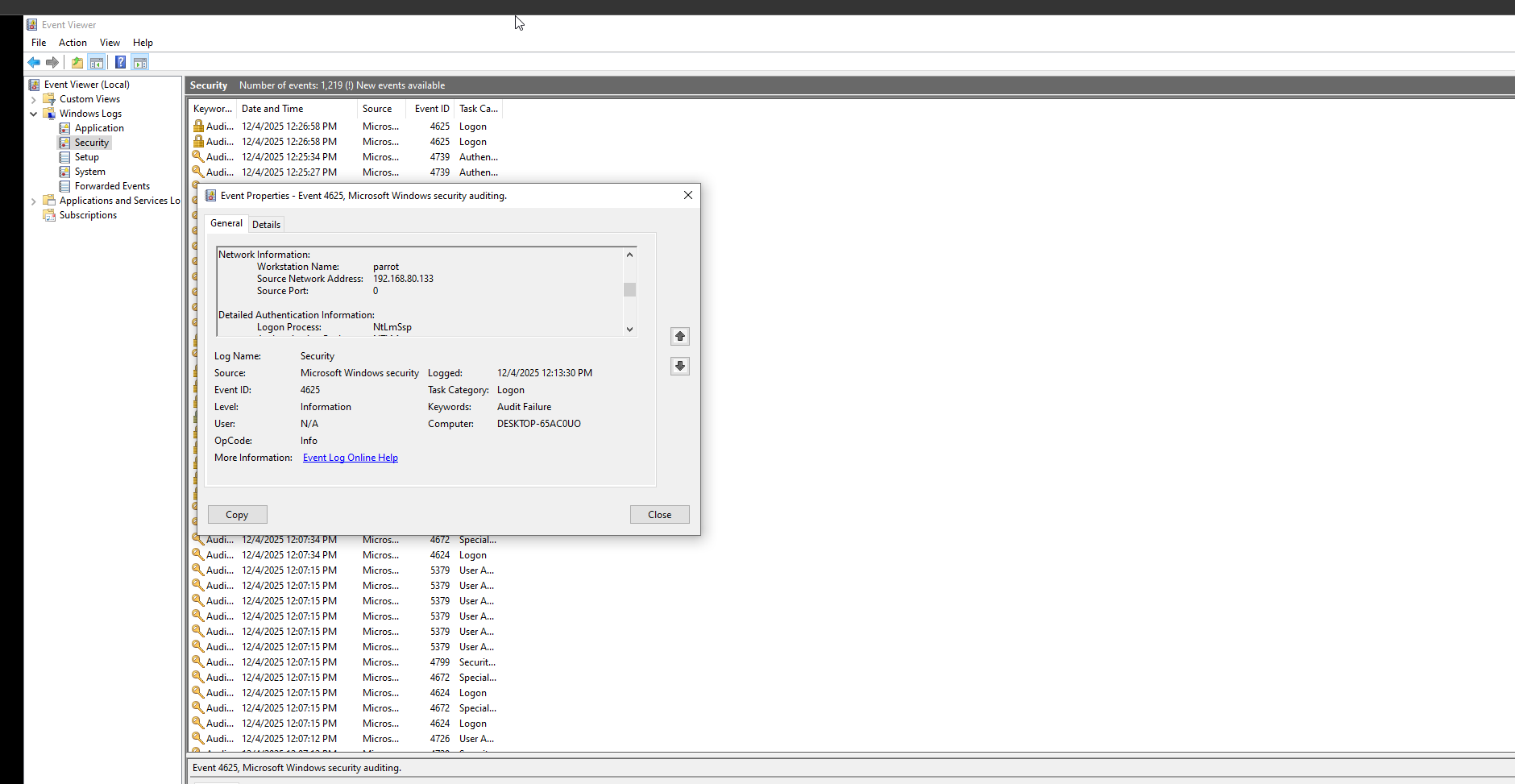
## **9. Recommendations**

* Disable RDP if not required
* Enable **Account Lockout Policy**
* Configure Firewall rules
* Enable **MFA**
* Move RDP behind VPN
* Regular log monitoring

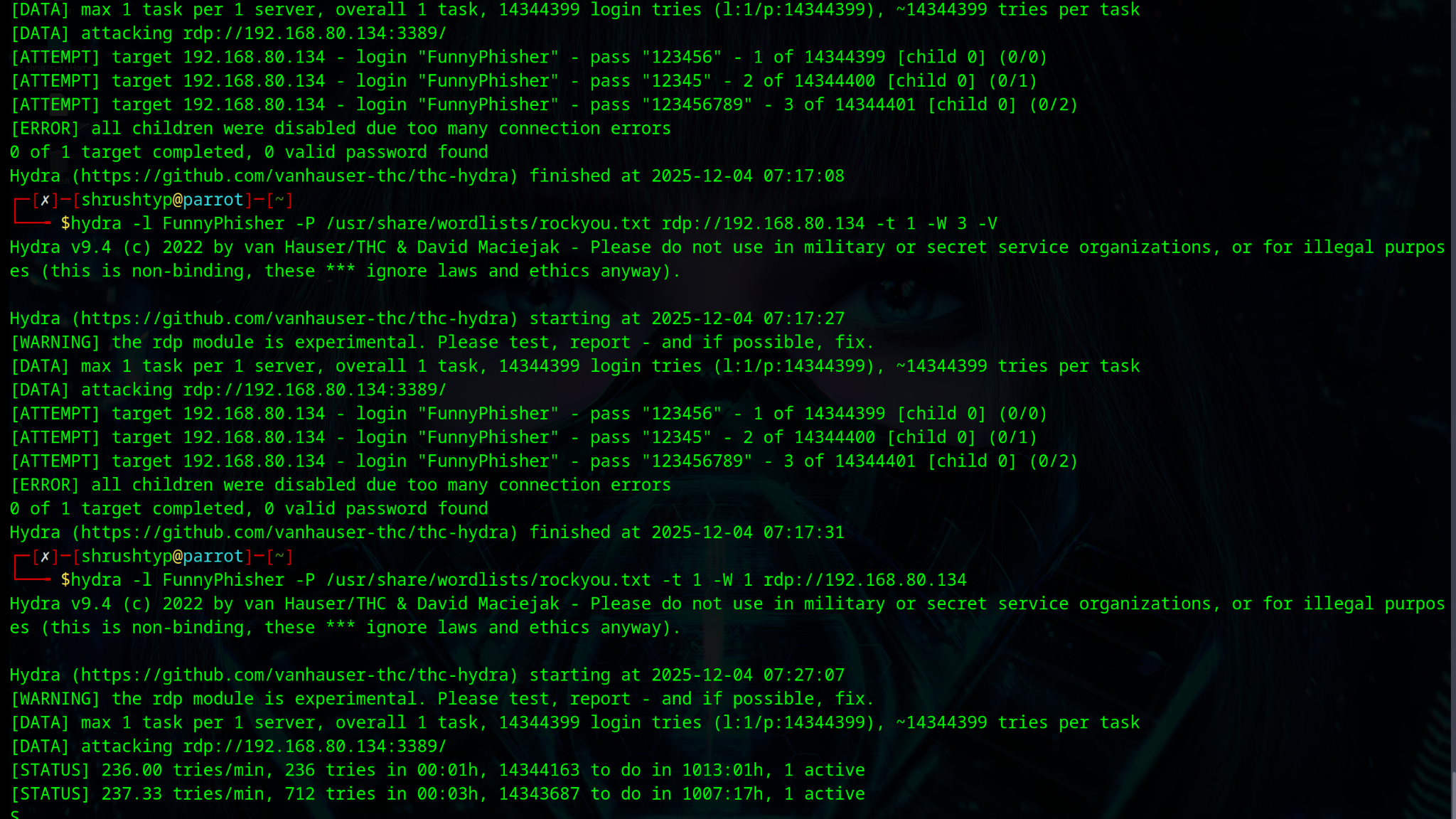
## **10. Screenshots**

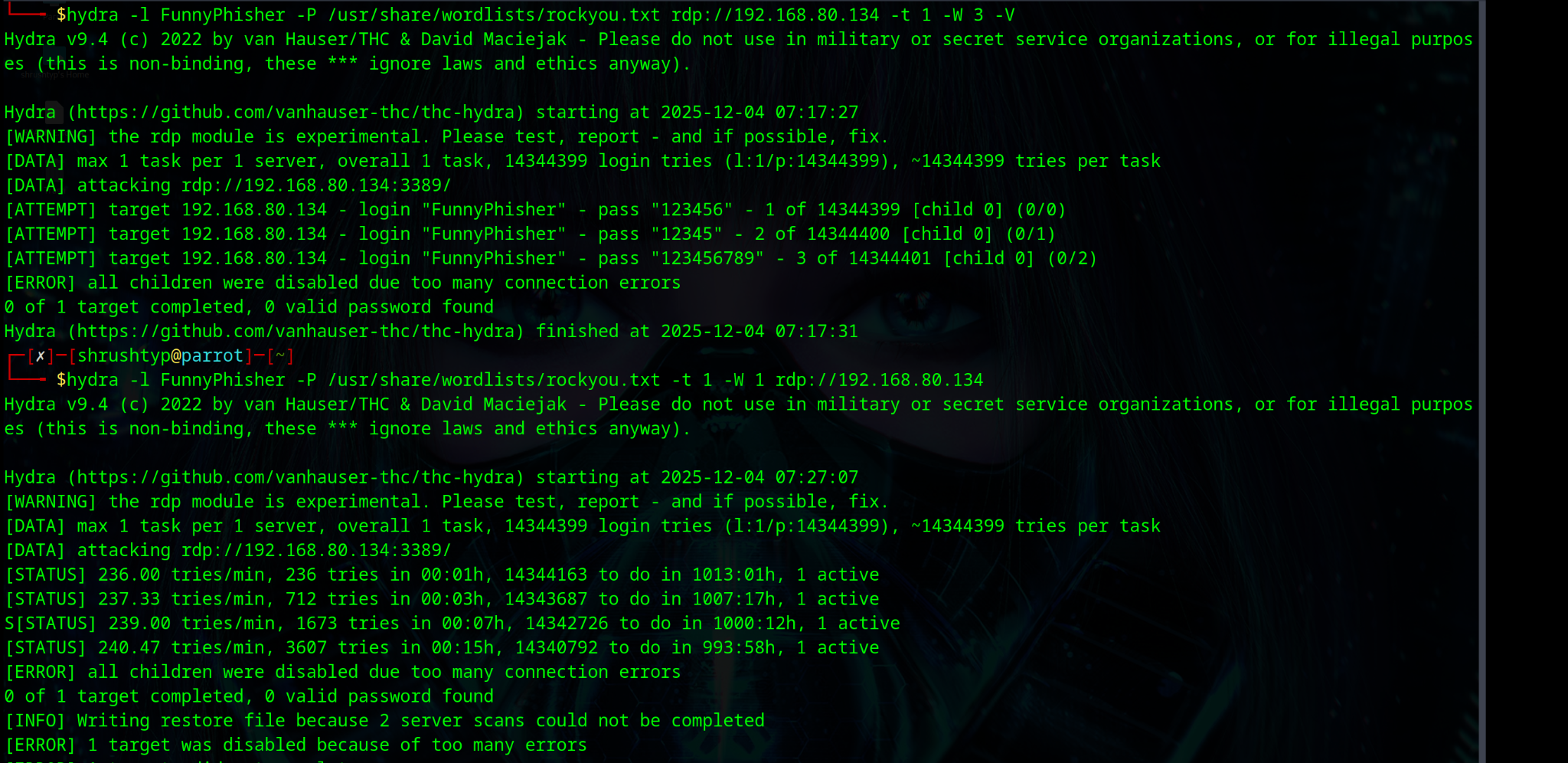


Windows Event Viewer (4625 logs)

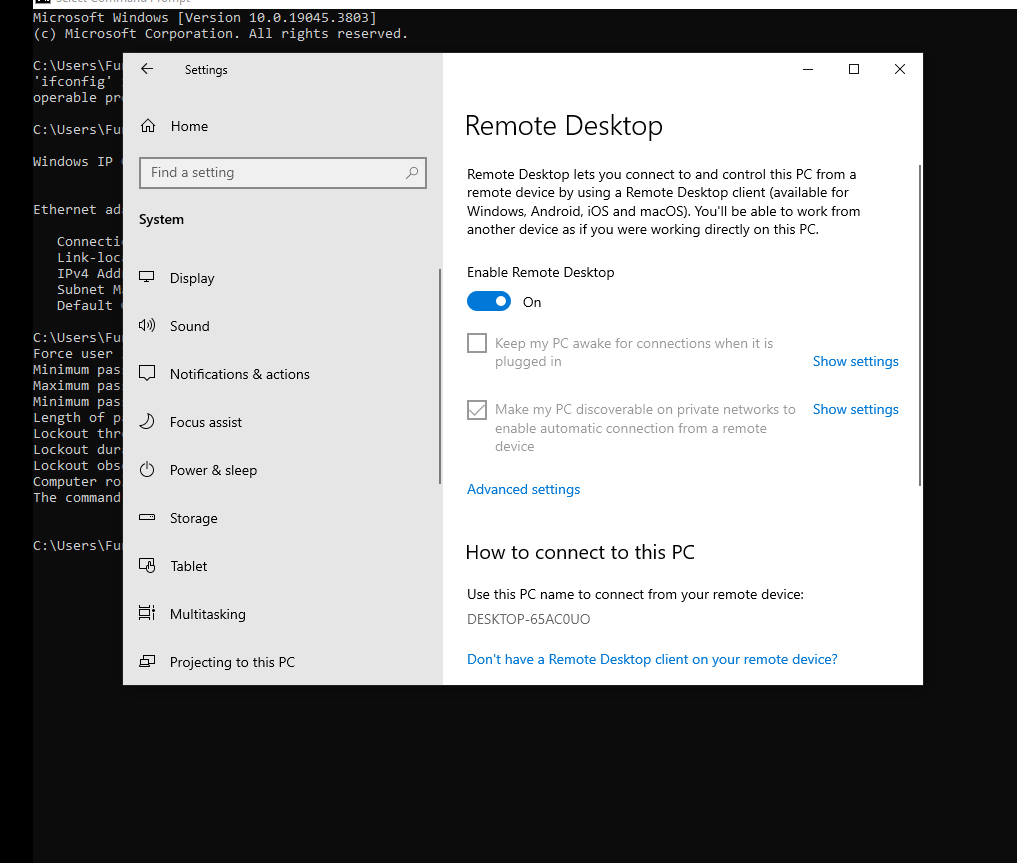




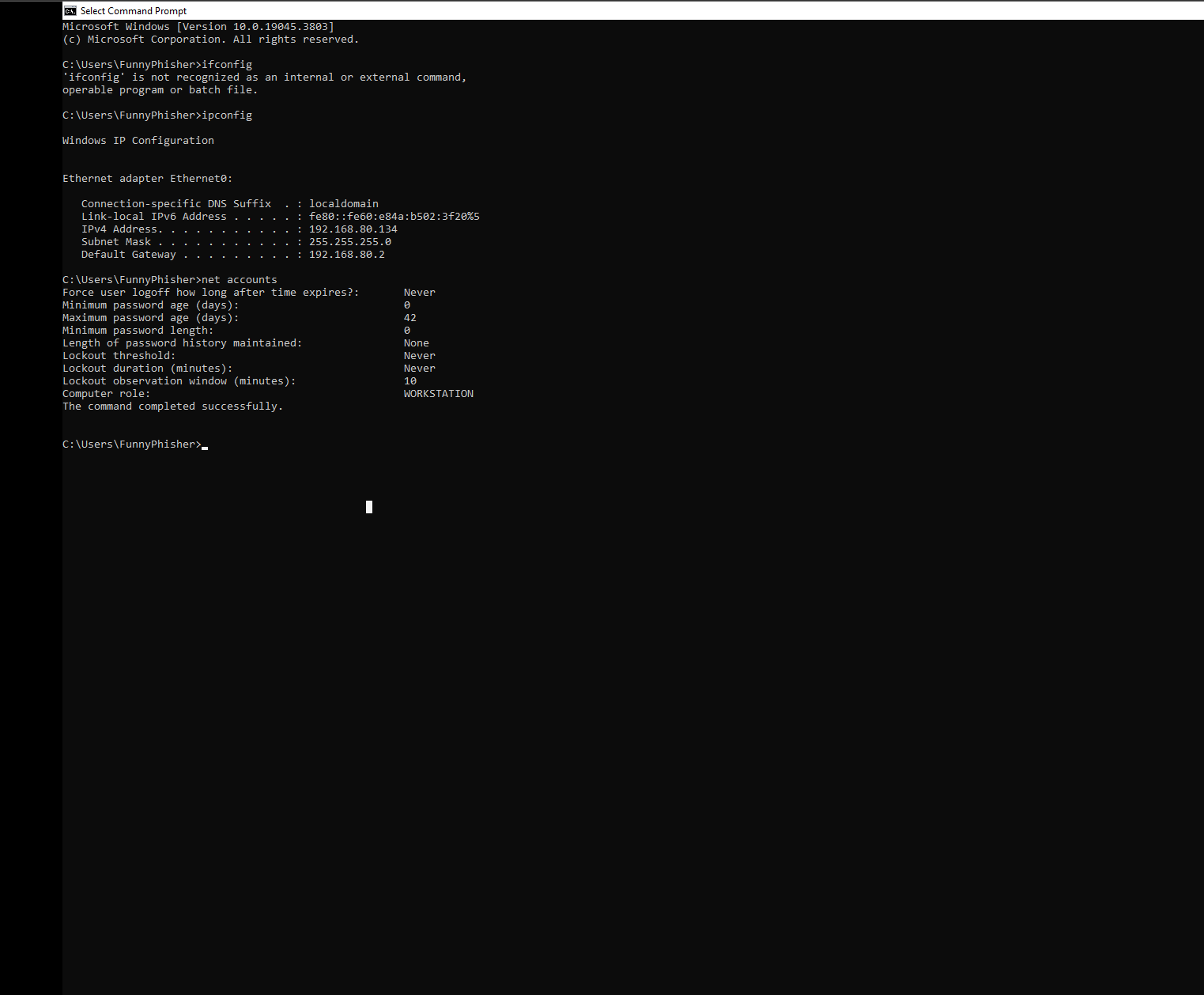
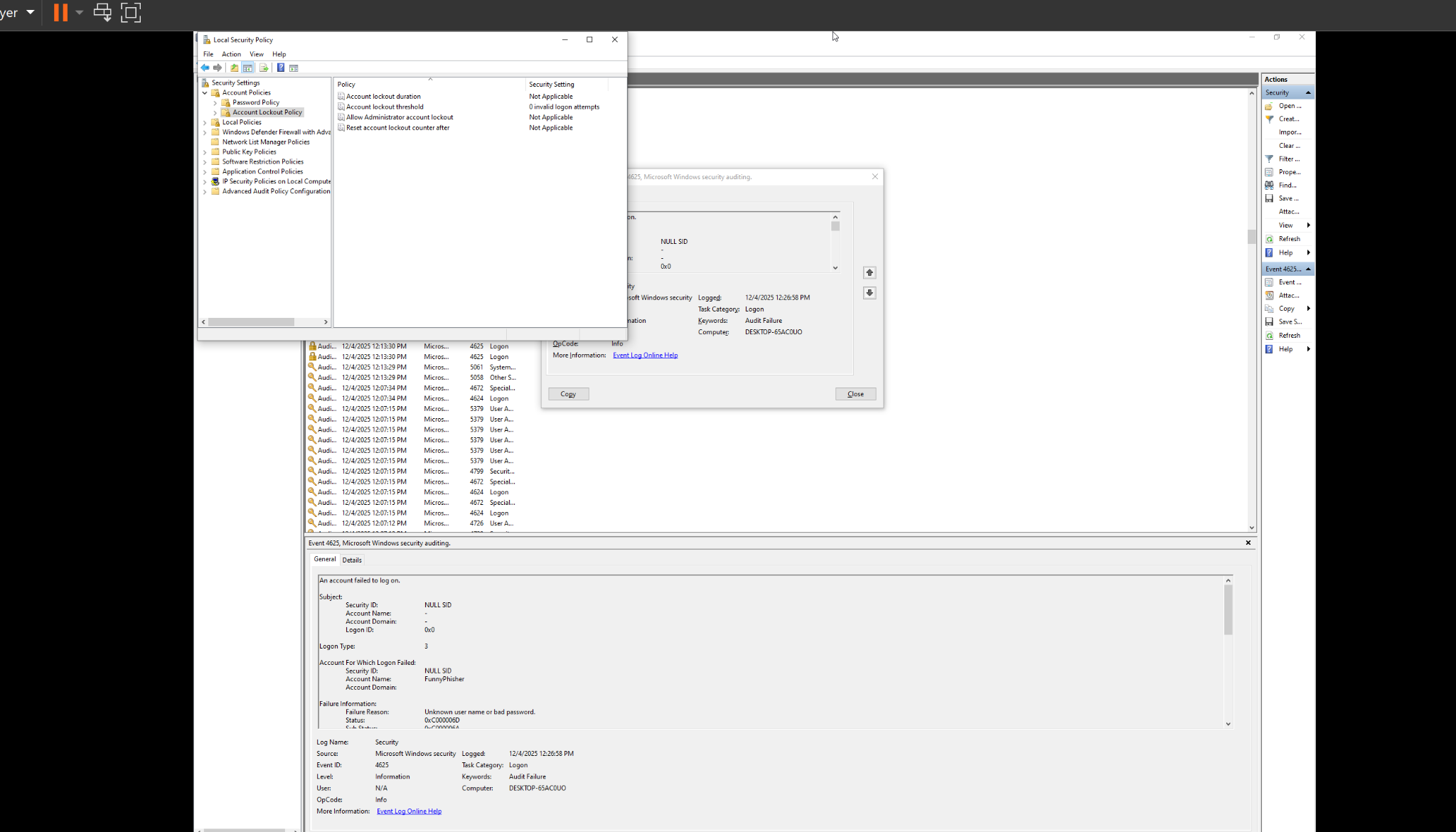
Hydra attack window  




RDP settings



User account details

# **✔ Report Done!**