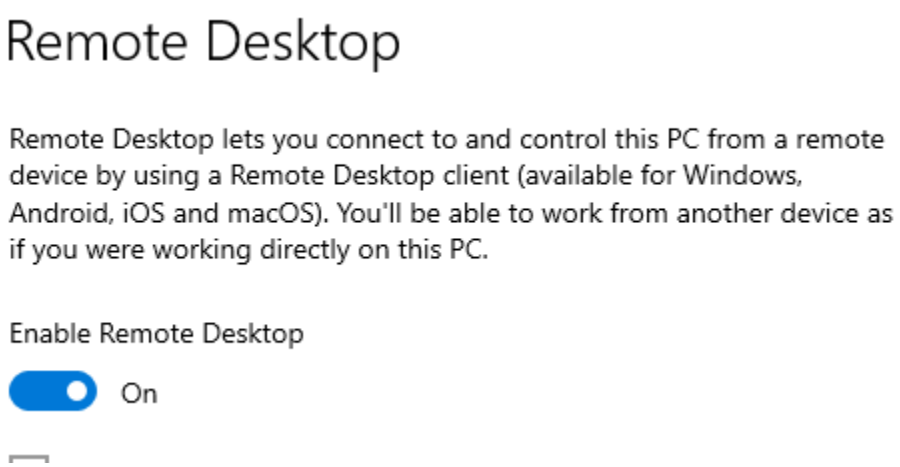
Modified Step-by-Step Guide for Scenario 3 (Single Windows 10 VM)

1. Enable RDP on the Windows 10 VM

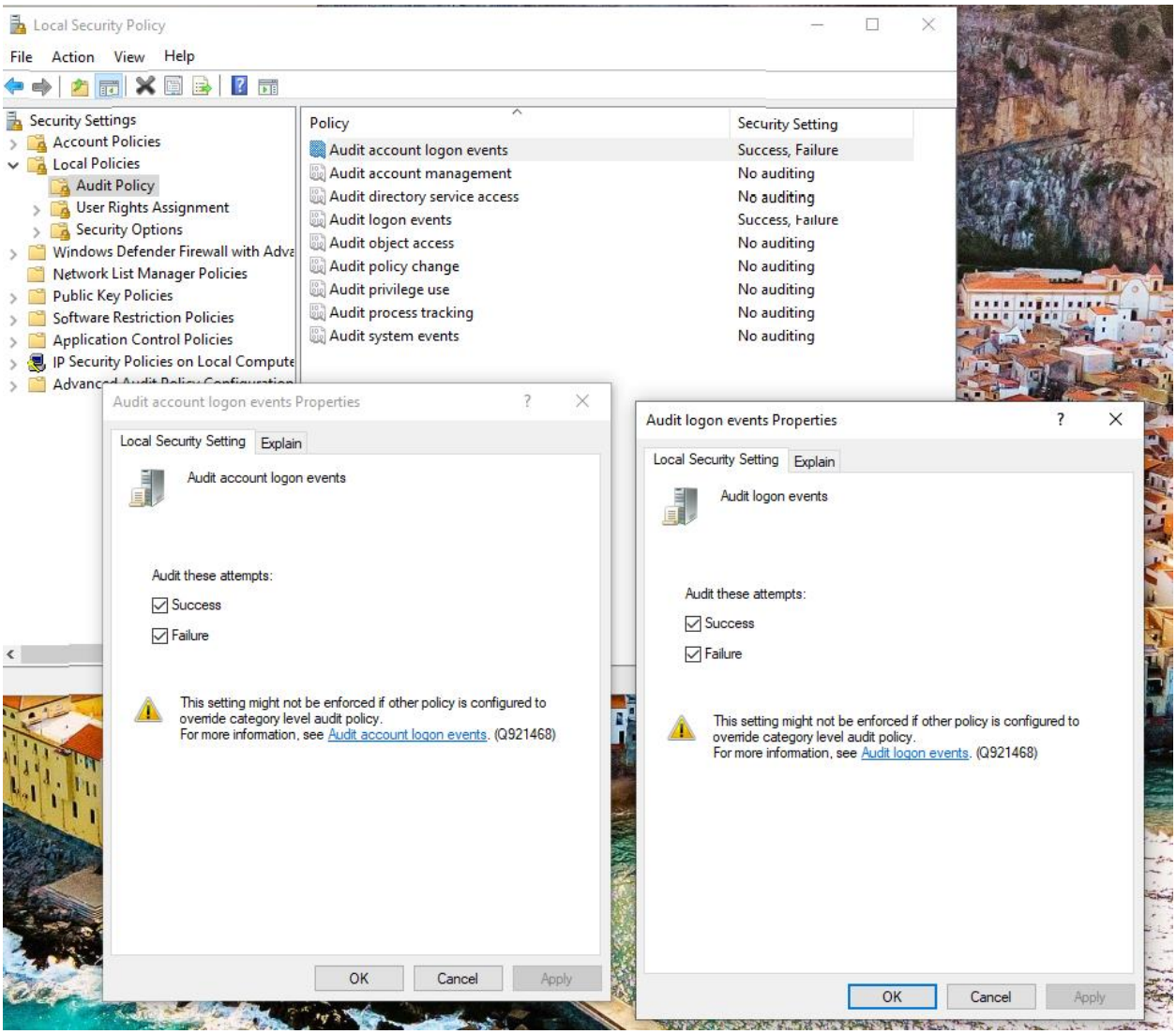
- On your **Windows 10 VM**:
  - Open **System Properties > Remote** → Enable "Allow remote connections to this computer".
  - Allow **RDP** through the Windows Firewall.



Step 2:

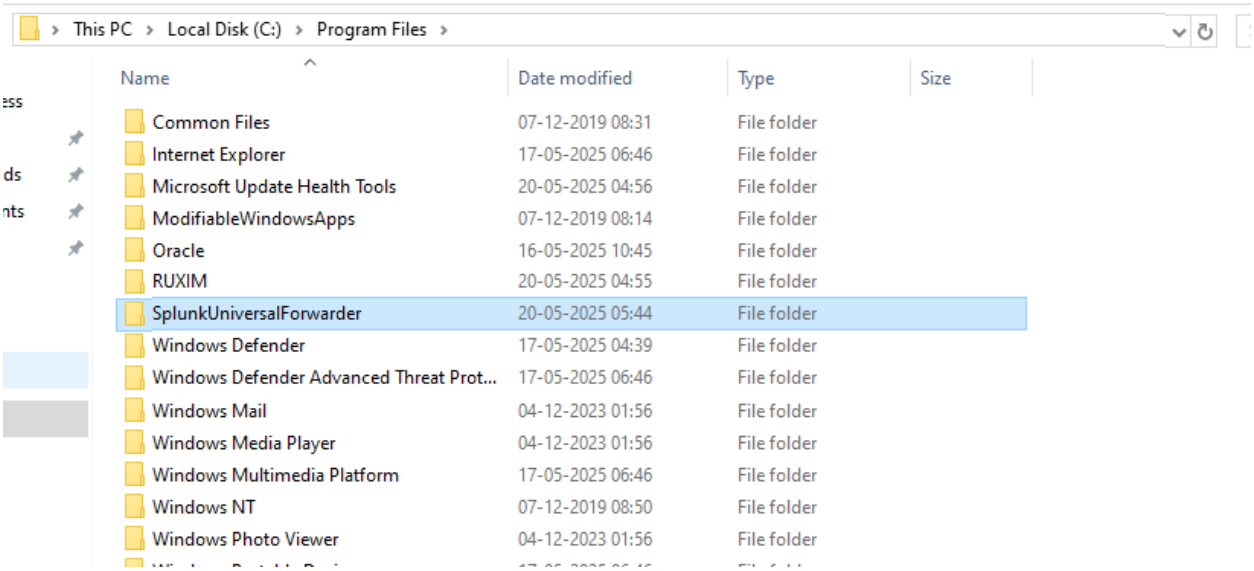
Set up Event Logging

- Open secpol.msc > **Local Policies** > **Audit Policy**:
  - Enable:
    - Audit logon events — Success and Failure
    - Audit account logon events — Success and Failure



3. Install and Configure Winlogbeat (or Universal Forwarder)

- Install Winlogbeat on the **Windows 10 VM**.
- Configure to forward logs to your **Ubuntu Splunk Server**.
- Ensure forwarding of logs from the **Security log** channel.



4. Simulate RDP Attack from Kali

A. From Kali Linux, try RDP connections:

Install and use xfreerdp or rdesktop:

sudo apt update

sudo apt install freerdp2-x11 -y

first try wrong try
and try right try

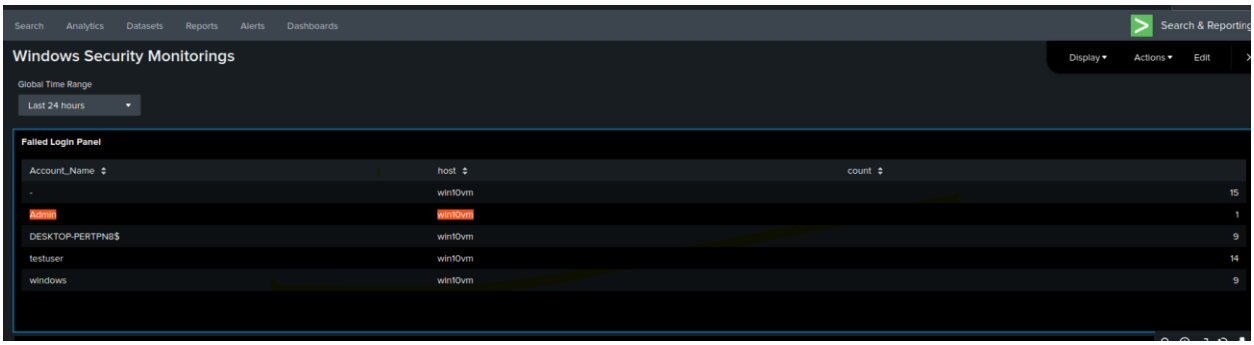
xfreerdp /u:username /p:password /v:<windows_vm_ip>

4. Detect Failed RDP Attempts

index=winlogbeat OR index=wineventlog EventCode=4625 LogonType=10

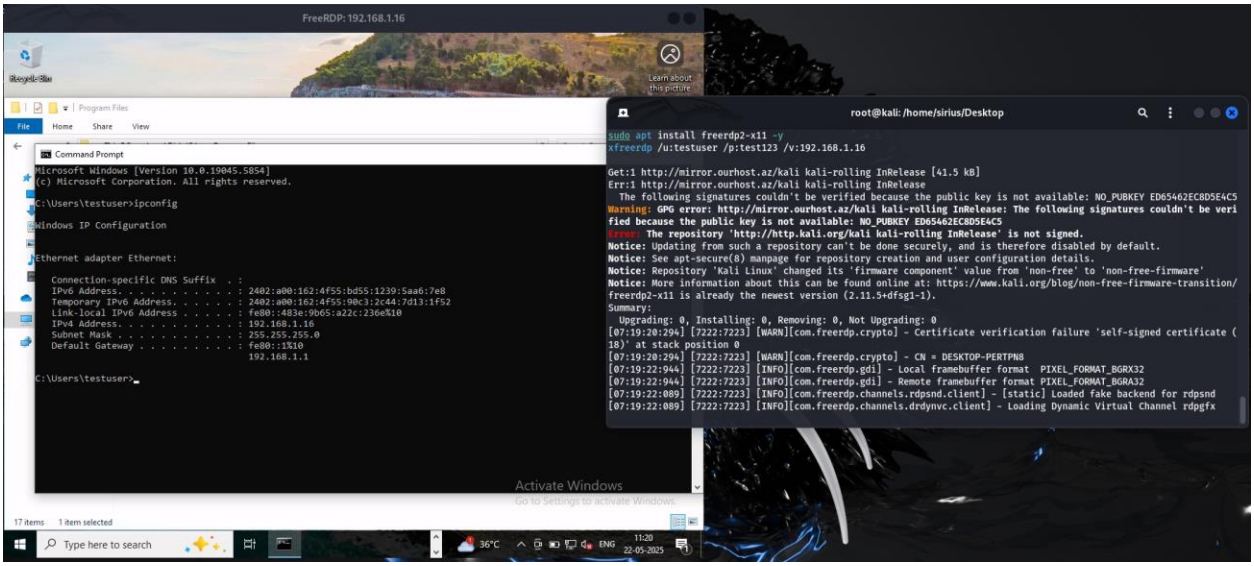
| stats count by Account_Name, IpAddress, _time

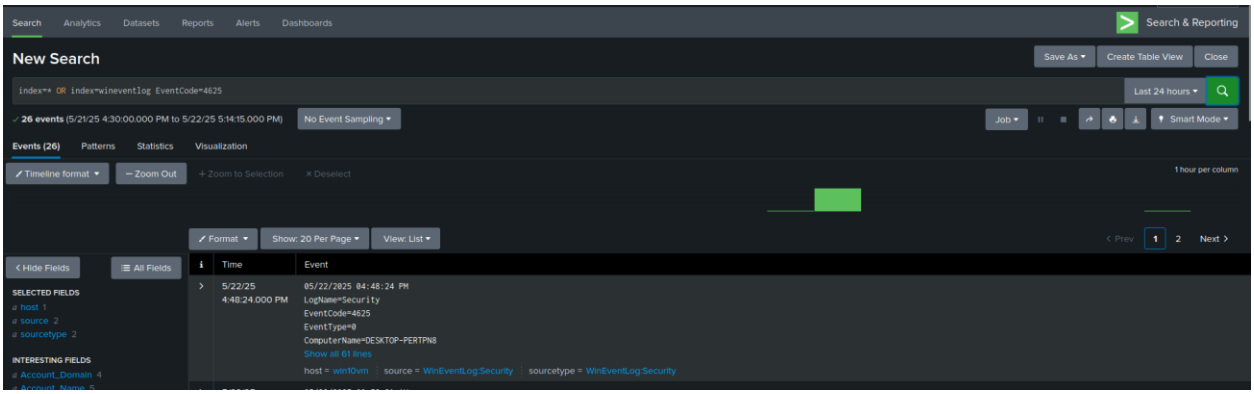
With wrong password and user name:



5. Detect Successful RDP Login

And now try to right password and login:




Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=* OR index=wineventlog EventCode=4625
Last 24 hours
26 events (5/21/25 4:30:00.000 PM to 5/22/25 5:14:15.000 PM)
No Event Sampling
Job
Smart Mode
Events (26)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1
2
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 2
sourcetype 2
INTERESTING FIELDS
Account_Domain 4
Time
Event
5/22/25
4:48:24.000 PM
05/22/2025 04:48:24 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-PERTPN8
Show all 61 lines
host = win10vm
source = WinEventLog:Security
sourcetype = WinEventLog:Security