

# 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.

## Remote Desktop

Remote Desktop lets you connect to and control this PC from a remote device by using a Remote Desktop client (available for Windows, Android, iOS and macOS). You'll be able to work from another device as if you were working directly on this PC.

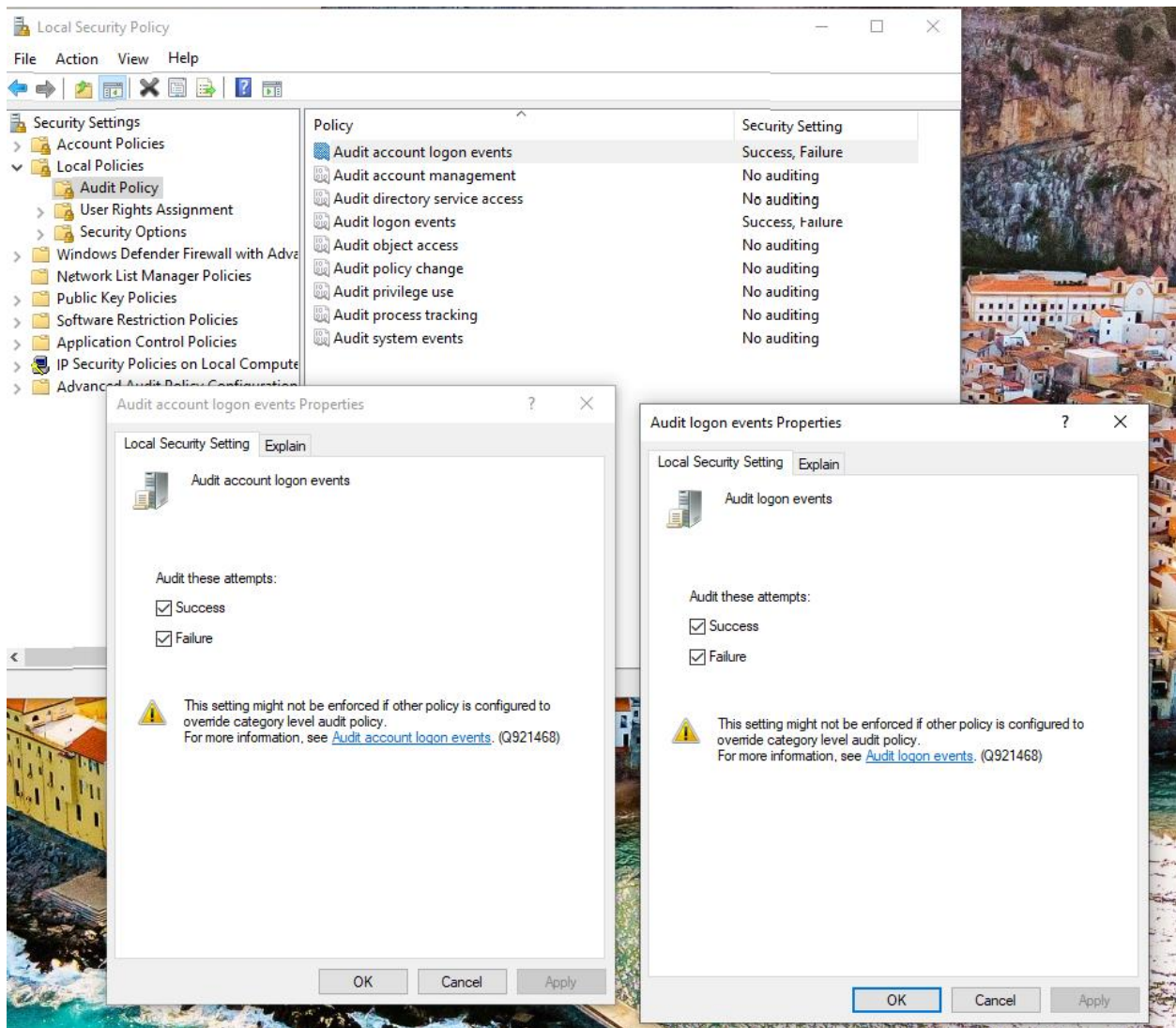
Enable Remote Desktop



Step 2:

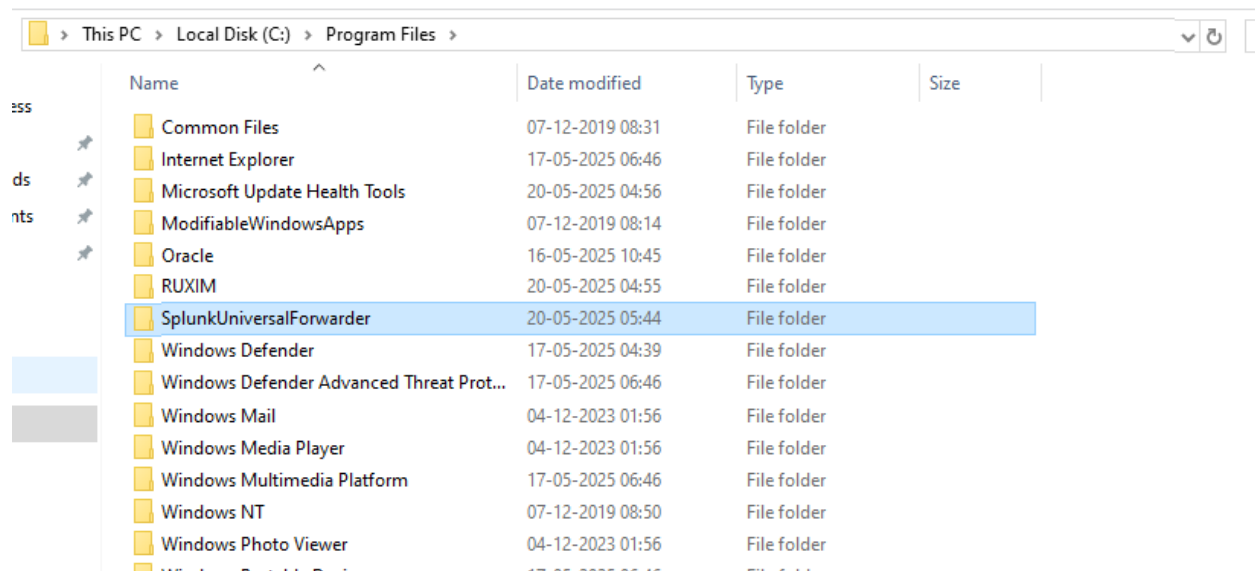
### Set up Event Logging

- 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**

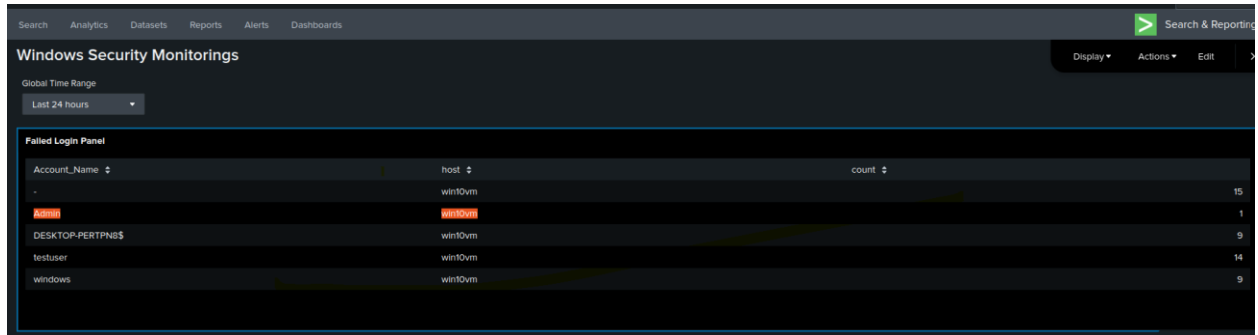
**xfreerdp /u:username /p:password /v:<windows\_vm\_ip>**

## 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:

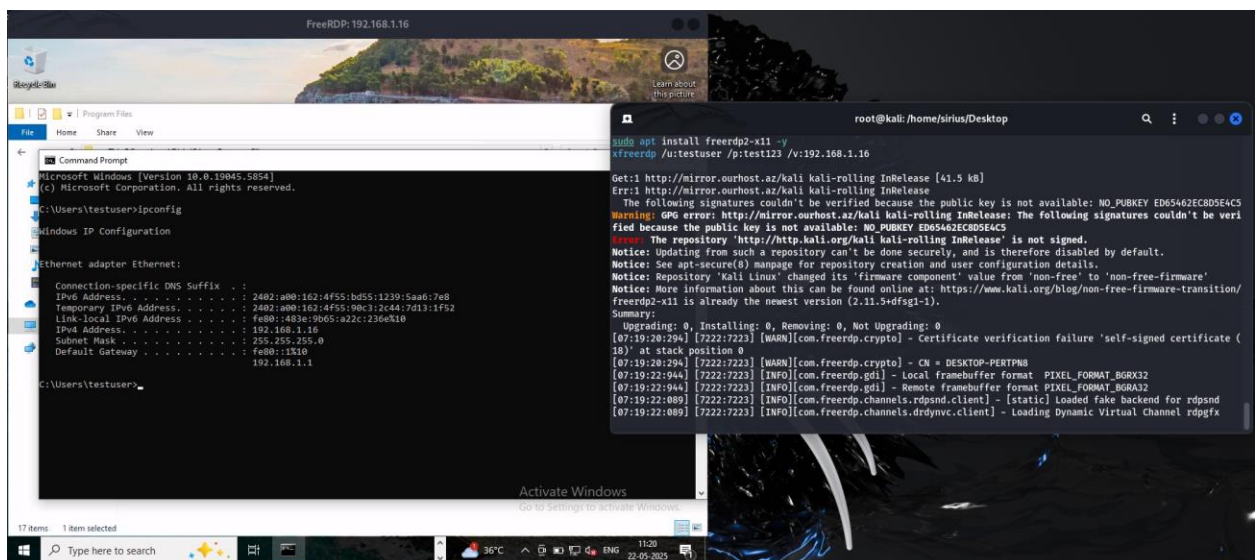


The screenshot shows the 'Windows Security Monitorings' interface. Under the 'Failed Login Panel' section, there is a table with columns: Account\_Name, host, and count. The table contains the following data:

Account_Name	host	count
-	wint0vm	15
Admin	wint0vm	1
DESKTOP-PERTPNB\$	wint0vm	9
testuser	wint0vm	14
windows	wint0vm	9

## 5. Detect Successful RDP Login

And now try to right password and login:



SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

Index\*\* OR Index=winEventLog.EventCode=4625

Last 24 hours

Search

26 events (5/21/25 4:30:00.000 PM to 5/22/25 5:14:15.000 PM)

No Event Sampling

JobPauseRefreshDownloadSmart Mode

Events (26)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect

1 hour per column

FormatShow: 20 Per PageView: List

Prev12Next

Hide FieldsAll Fields

SELECTED FIELDS

host 1source 2sourcetype 2

INTERESTING FIELDS

Account\_Domain 4Account\_Name 5

Time	Event
5/22/25 8:48:24 PM	LogName=Security
4:48:24.000 PM	EventCode=4625
	EventType=0
	ComputerName=DESKTOP-PERTPN6
	Show all 61 lines
	host = win2um source = WinEventLogSecurity sourcetype = WinEventLogSecurity