**Unauthorized Remote Desktop Access**

1. Attempt RDP logins (both failed and successful).
2. Capture and analyze logs, specifically:
   * Event ID 4624 (successful login) with Logon Type 10 (RemoteInteractive/RDP)
   * Event ID 4625 (failed login)

Step 1: Enable RDP on the Victim Windows Machine

1. Open System Properties:
2. Run → sysdm.cpl
3. Go to Remote tab.
4. Check "Allow remote connections to this computer".
5. Make sure "Allow connections only from computers running Remote Desktop with Network Level Authentication" is checked.

Step 2: Add a Test User

To simulate unauthorized access:

net user rdpuser Rdp@1234 /add

net localgroup "Remote Desktop Users" rdpuser /add

Step 3: Attempt RDP Logins (from Attacker Machine)

Successful RDP Login

From your attacker machine:

1. Open Remote Desktop Connection:
   * Run → mstsc+
2. Enter the IP address of the victim machine.
3. Enter correct credentials of an authorized user.
4. Observe successful connection.

Failed RDP Login

Try to:

1. Enter wrong username or password.
2. Observe login failure.

Step 4: Analyze Security Logs (on Victim)

1. On victim machine, open:
2. Event Viewer → Windows Logs → Security
3. Look for:
   * Event ID 4624 = Successful login
   * Logon Type 10 = RemoteInteractive (RDP)
   * Event ID 4625 = Failed login attempts
4. Filter logs:
   * Right-click Security → Filter Current Log
   * Enter 4624,4625 in the Event IDs field

How to Read Event 4624

* Subject → Account Name: Who initiated the login
* Logon Type:
  + 10 = RemoteInteractive (RDP)
  + 3 = Network (e.g., file share)
* Network Information → Workstation Name / Source Network Address: Shows the IP address of the source