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

---

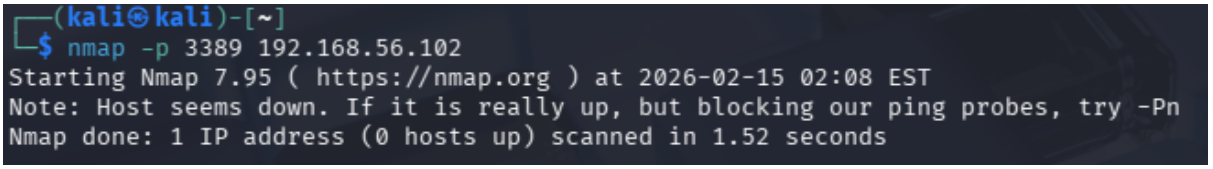
3. Reconnaissance Phase

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.



---

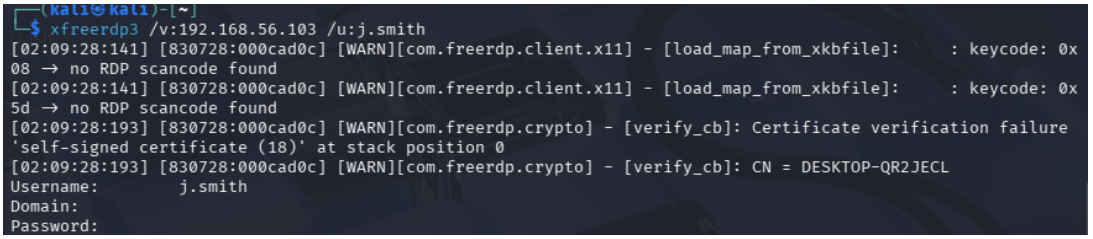
4. Service Verification

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.



---

5. Brute Force Attack

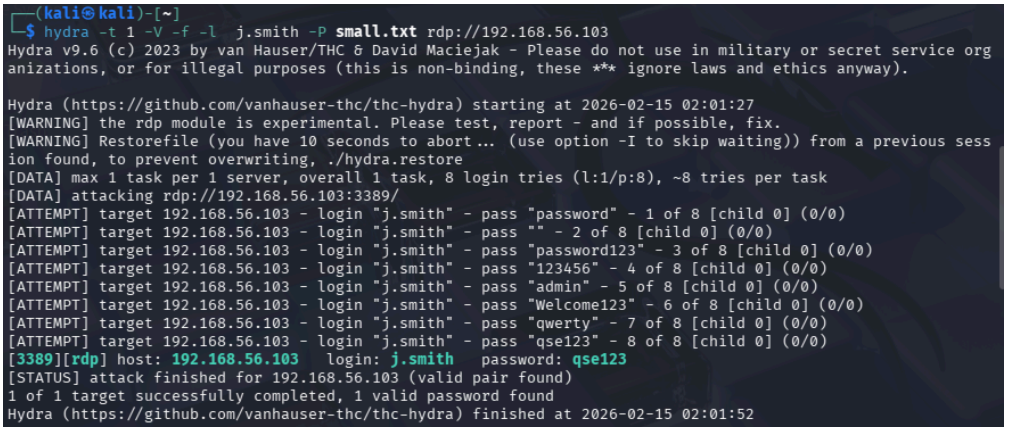
Hydra was used to perform a dictionary-based brute force attack against the RDP service.

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.

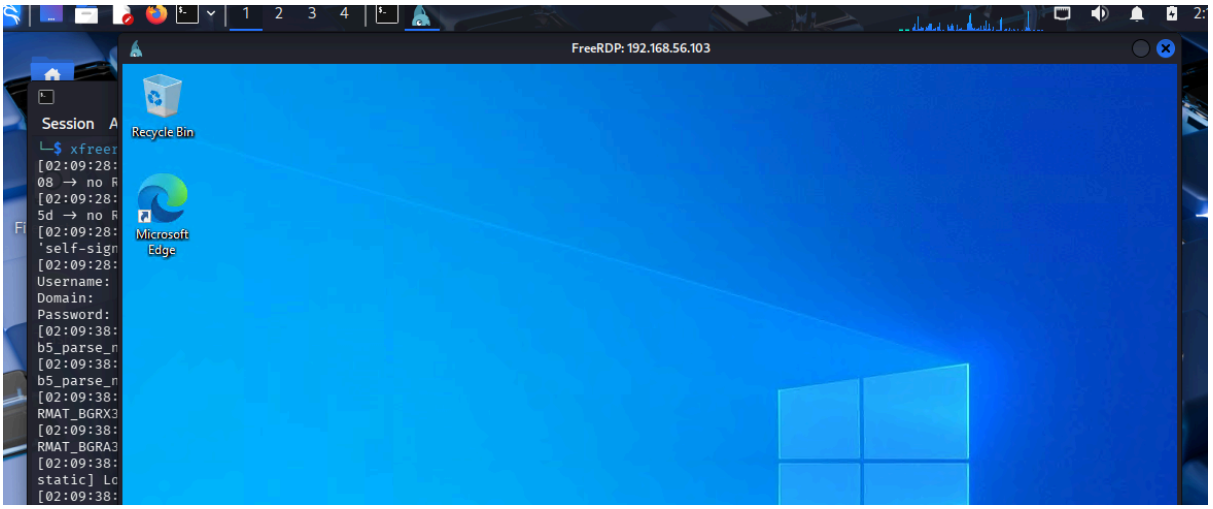
Hydra successfully identified valid credentials for the target account.



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