RDP Enumeration & Weak Password Access

A project in the Cybersecurity Skill Tree

Project description

In this project, I will demonstrate the fundamentals of RDP enumeration using various tools to discover RDP services, enumerate user accounts, and exploit weak passwords to gain unauthorized access.

Verify Connectivity to Target with Ping

First, I will send four packets to the target server to confirm accessibility.

```
labex:~/ $ ping -c 4 target
PING target (172.17.0.2) 56(84) bytes of data.
64 bytes from target (172.17.0.2): icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from target (172.17.0.2): icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from target (172.17.0.2): icmp_seq=3 ttl=64 time=0.030 ms
64 bytes from target (172.17.0.2): icmp_seq=4 ttl=64 time=0.039 ms

--- target ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.030/0.038/0.053/0.009 ms
```

Scan Open Ports with Nmap

Next, I will use the “nmap” utility to scan for an open RDP service and check its security configuration.

```
labex:~/ $ nmap --script rdp-enum-encryption -p3389 target
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-06 23:16 CST
Nmap scan report for target (172.17.0.2)
Host is up (0.00016s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|     Native RDP: SUCCESS
|     RDSTLS: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: High
|     128-bit RC4: SUCCESS
|_  RDP Protocol Version:  RDP 5.x, 6.x, 7.x, or 8.x server

Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

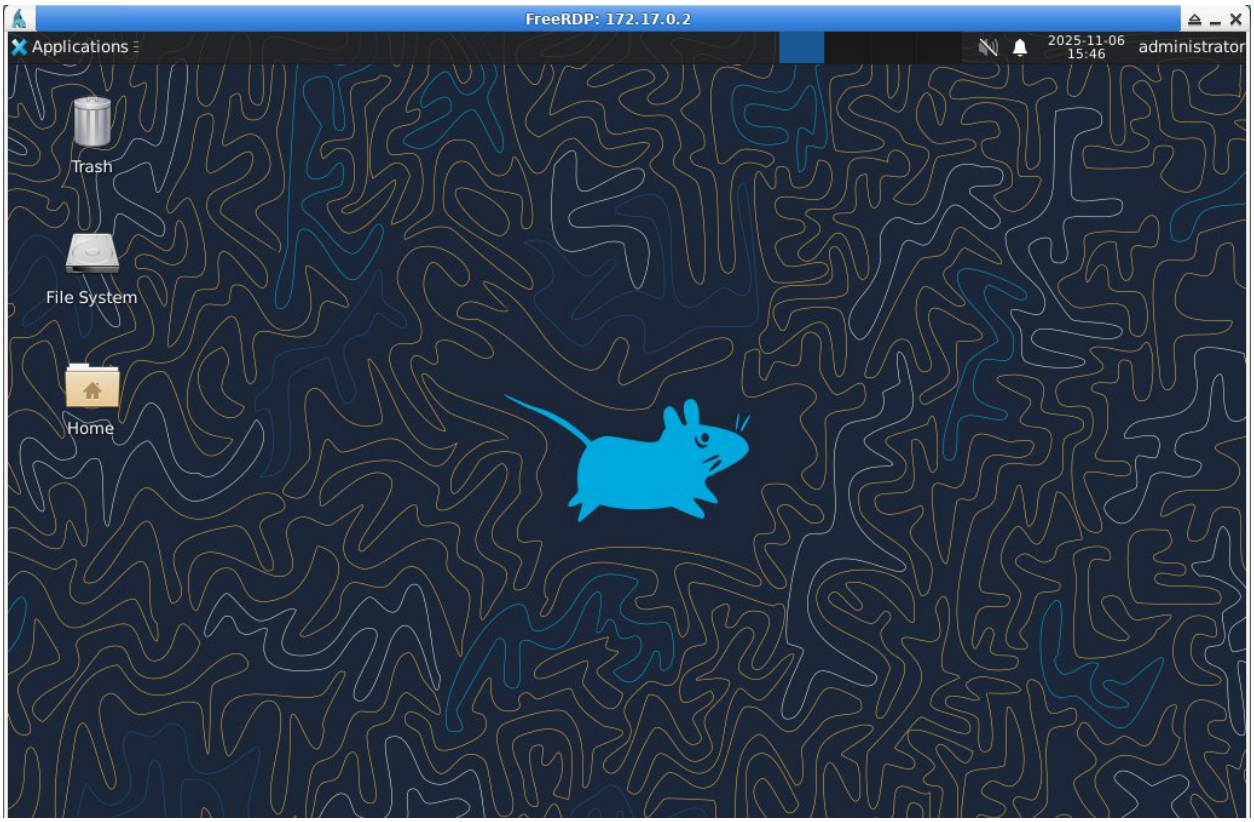
Connect to Target via RDP

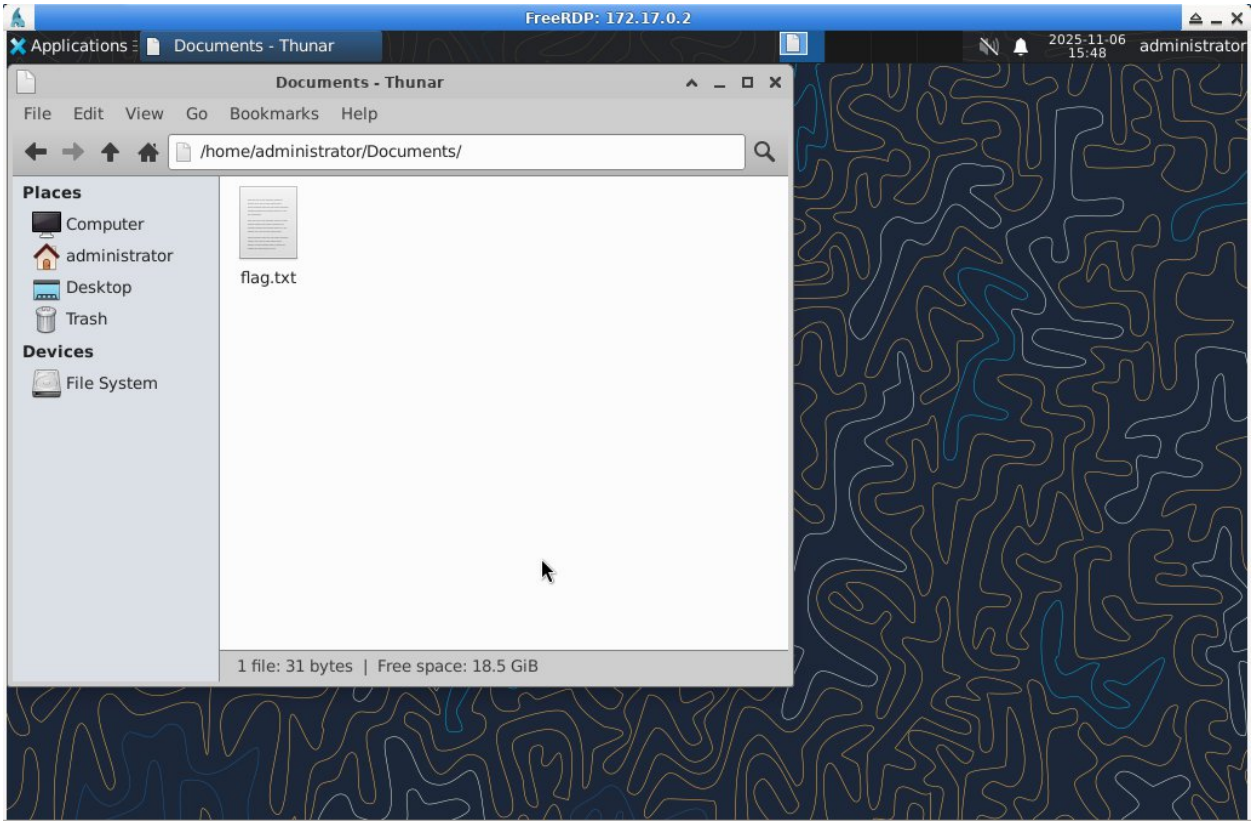
According to the scan results, the RDP service has been configured with weak encryption mechanisms, so now I will use xfreerdp to exploit this misconfiguration using common default admin credentials.

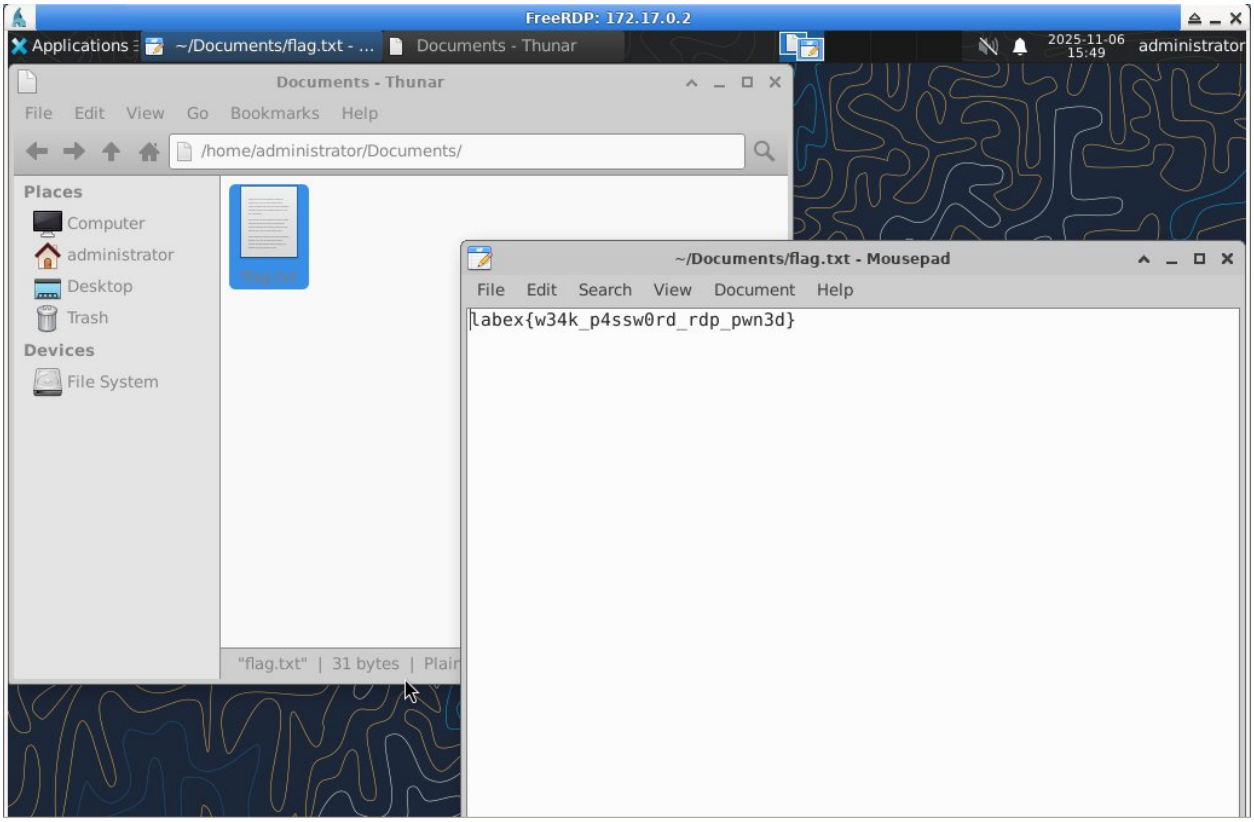
```
labex:~/ $ xfreerdp /u:administrator /p:password /v:172.17.0.2
[23:33:48:412] [18256:18261] [INFO][com.freerdp.crypto] - creating directory /home/labex/.config/freerdp
[23:33:48:412] [18256:18261] [INFO][com.freerdp.crypto] - creating directory [/home/labex/.config/freerdp/cert
s]
[23:33:48:412] [18256:18261] [INFO][com.freerdp.crypto] - created directory [/home/labex/.config/freerdp/serve
r]
[23:33:48:422] [18256:18261] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certif
icate (18)' at stack position 0
[23:33:48:422] [18256:18261] [WARN][com.freerdp.crypto] - CN = localhost
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!
      @
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] - The hostname used for this connection (172.17.0.2:3
389)
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] - does not match any of the names given in the certif
icate:
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] - Common Name (CN):
[23:33:48:422] [18256:18261] [ERROR][com.freerdp.crypto] -      localhost
[23:33:48:423] [18256:18261] [ERROR][com.freerdp.crypto] - Alternative names:
[23:33:48:423] [18256:18261] [ERROR][com.freerdp.crypto] -       localhost
[23:33:48:423] [18256:18261] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT b
e trusted!
Certificate details for 172.17.0.2:3389 (RDP-Server):
        Common Name: localhost
        Subject:     CN = localhost
        Issuer:      CN = localhost
        Thumbprint:  eb:45:51:d6:9b:99:39:35:3d:29:f3:49:1b:39:75:8b:fc:2e:c0:83:5b:69:0b:c3:60:c6:65:cc:88:24
:85:1b
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
[23:34:26:580] [18256:18261] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[23:34:26:580] [18256:18261] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[23:34:26:633] [18256:18261] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdp
snd
[23:34:26:633] [18256:18261] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdp
gfx
```

Explore Target System and Locate Flag

I have successfully logged into the target machine over RDP. My final objective will be to find the flag in the machine's Documents folder.







Summary

This exercise emphasizes the importance of changing default credentials as measure to prevent unauthorized access to critical network assets.