Get access to another window pc by rdp port open with known username

First I always ping ip add ( 10.129.1.13) to check the connectivity

And it is working

So I will start using nmap scanning for 10000 ports to see which one is open

Nmap –top-ports 10000 10.129.1.13

This –top-ports 10000 allow me to scan 10000 first 10000ports to see which one Is open

A screen shot of a computer

AI-generated content may be incorrect.

Now I know that port 3389 is opening and it services is ms-wbt-server

And I know it is remote desktop protocol

So now I will use xfreerdp -help to find information of how to get access

And I found using /c: and /u:

Since I know that using administrator for username can somehow bypass the blank password

Then I use xfreerdp /v: 10.129.1.13 /u:Adminstrator

So in some case if we login domain with administrator and just let the password blank we can get access

A screenshot of a computer

AI-generated content may be incorrect.

And now we get the flag- information we need

A screenshot of a computer

AI-generated content may be incorrect.