Anthem Walkthrough (tryhackme)

Difficulty : Easy

Task 1:

What port is for the web server

What port is for remote desktop service

After running your nmap command we can answer the questions above

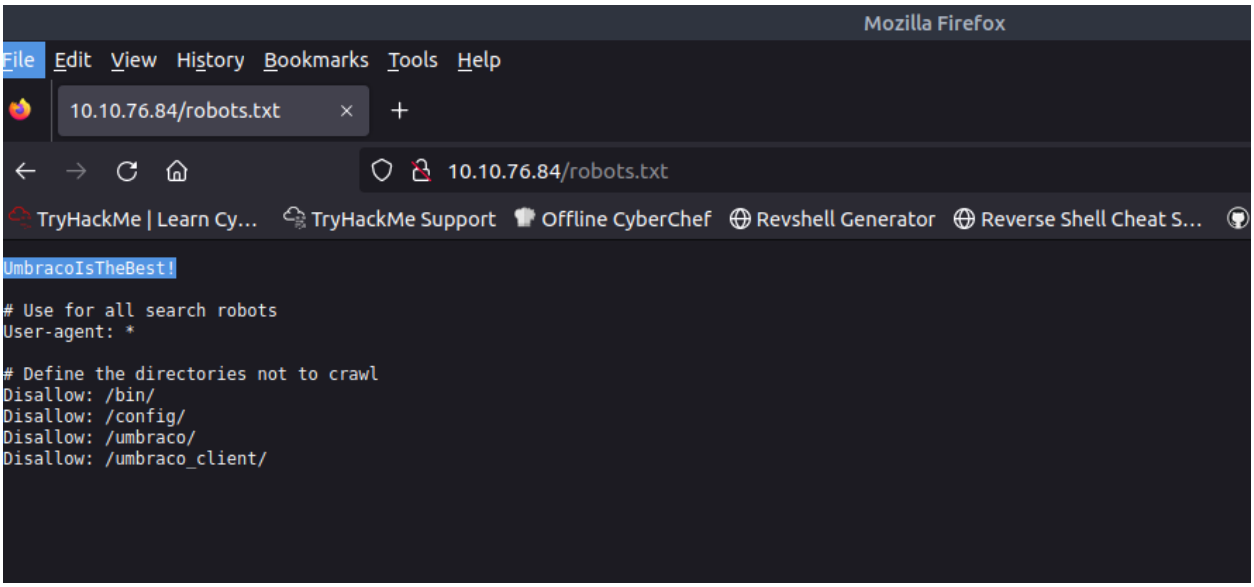
```
root@ip-10-10-25-241:~# nmap -sSVC 10.10.76.84

Starting Nmap 7.60 ( https://nmap.org ) at 2024-07-09 03:19 BST
Nmap scan report for ip-10-10-76-84.eu-west-1.compute.internal (10.10.76.84)
Host is up (0.0038s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-LU09299160F
| Not valid before: 2024-07-08T01:53:34
|_Not valid after:  2025-01-07T01:53:34
|_ssl-date: 2024-07-09T02:19:59+00:00; +1s from scanner time.
MAC Address: 02:14:99:35:4C:11 (Unknown)
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 101.80 seconds
root@ip-10-10-25-241:~#
```

What is a possible password in one of the pages web crawlers check for?

To answer the next question we check the robots.txt file (http://ip/robots.txt) many web crawlers look for pages like robots.txt , using dirb or gobuster we can see the different web pages



what CMS is the website using?

Looking at the robots.txt file we can see a CMS

What is the domain of the website?

Can be seen on the site

What's the name of the Administrator

Tricky question, alot time wasted on this question, basically there an article or poem on one of the pages. you have then to google about that to answer this question

Can we find the email address of the administrator?

While looking at the pages we find an article with an email, using the format of that email just using common sense and you will get the right email.

Task 2

To find the flags hers just follow what the hints tells you and would find the flags of this task

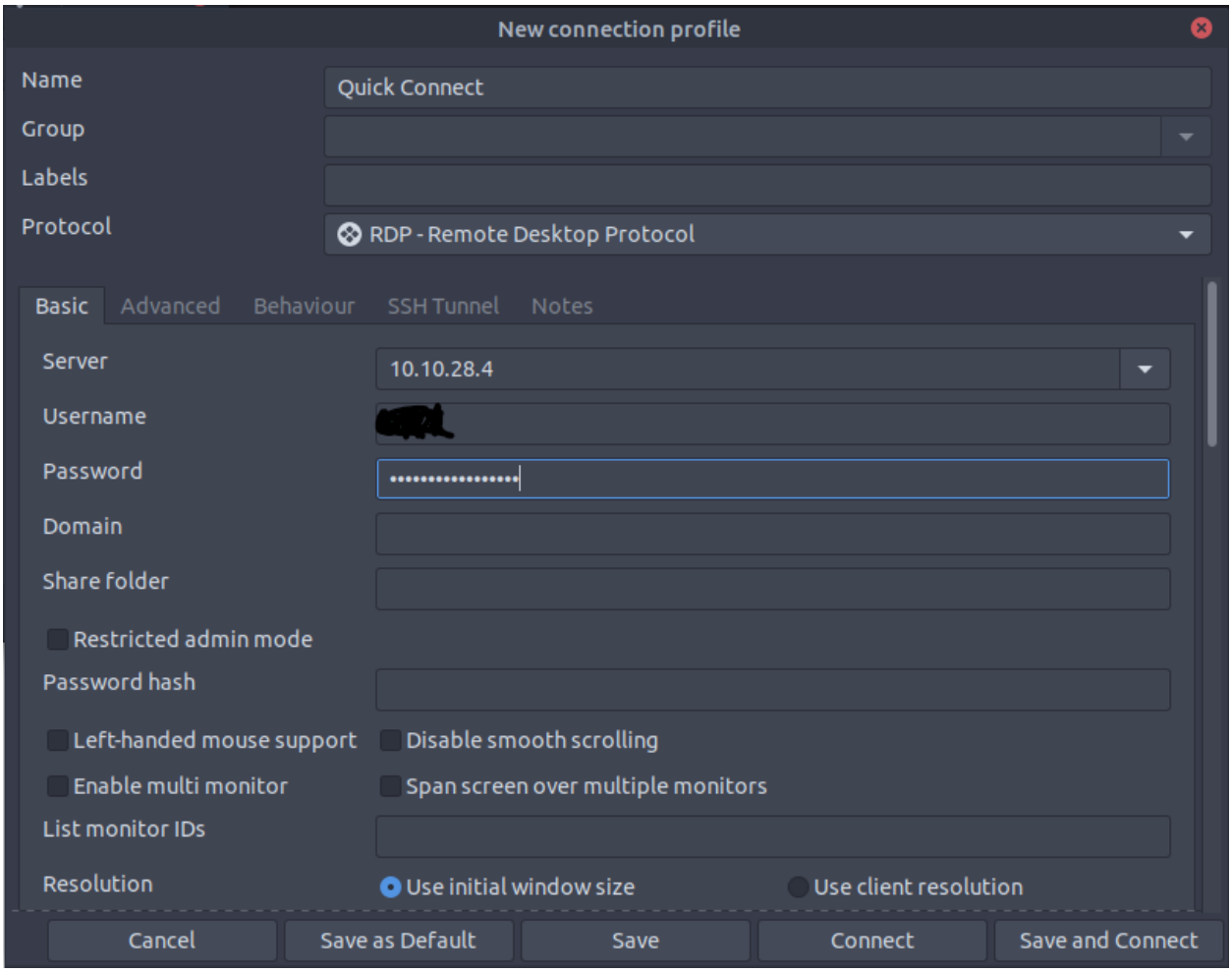
Task 3

Let’s figure out the username and password to log in to the box.(The box is not a domain)

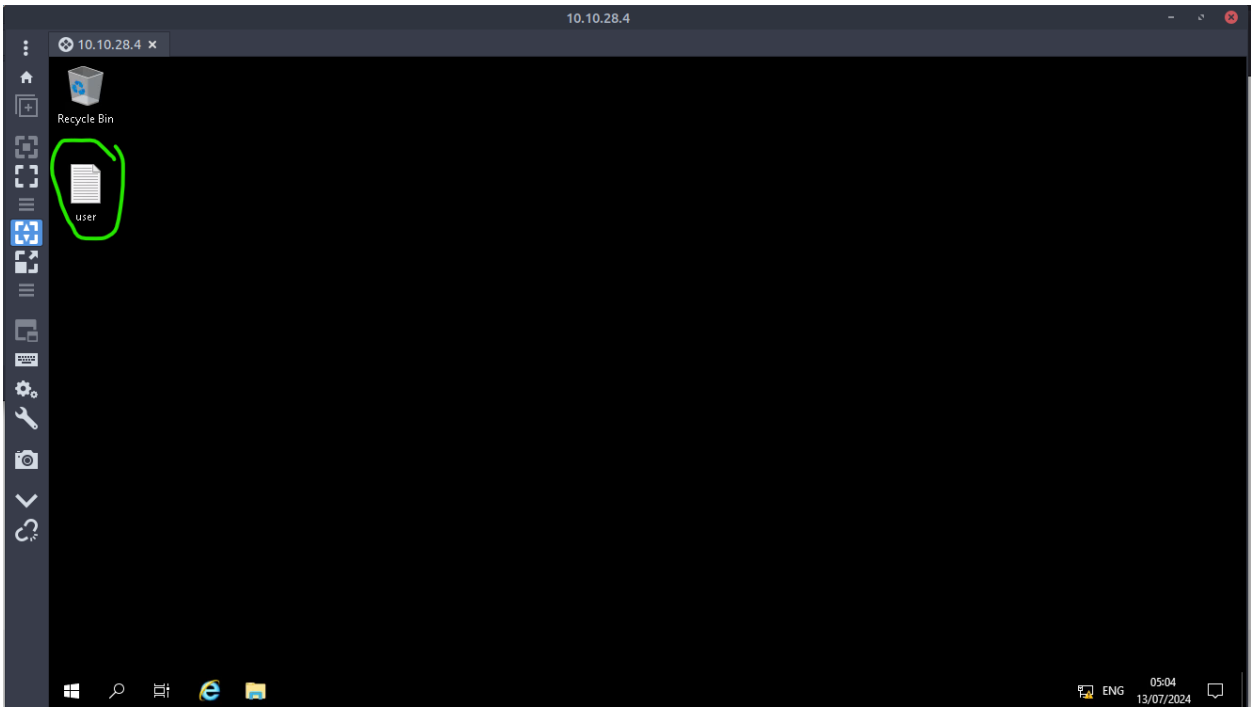
If you did the previous task we can easily figure out our password and username from the previous task

Gain inituak access to the machine, what is the contents of user.txt?

loging in using remmina remote desktop client

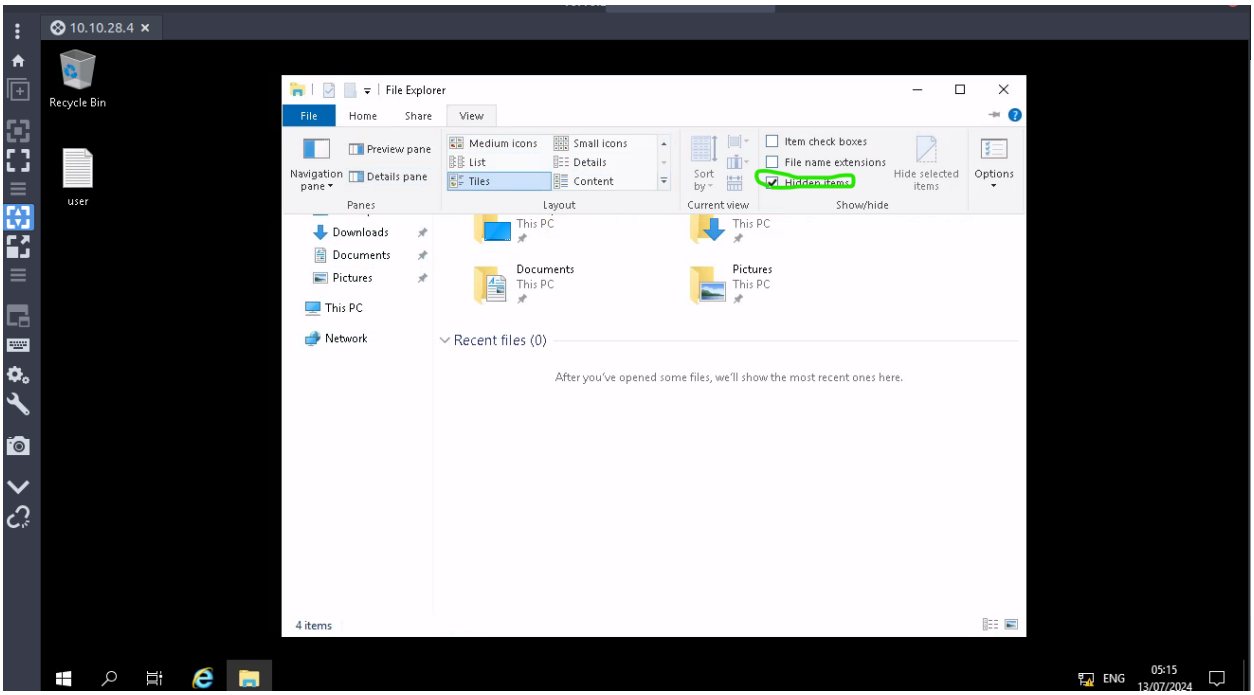


Now you can view the contents of the user.txt file



Can we spot the admin password?

Following the hint we thick the hidden items box on tab so it will enable us to see hidden documents or folders or files

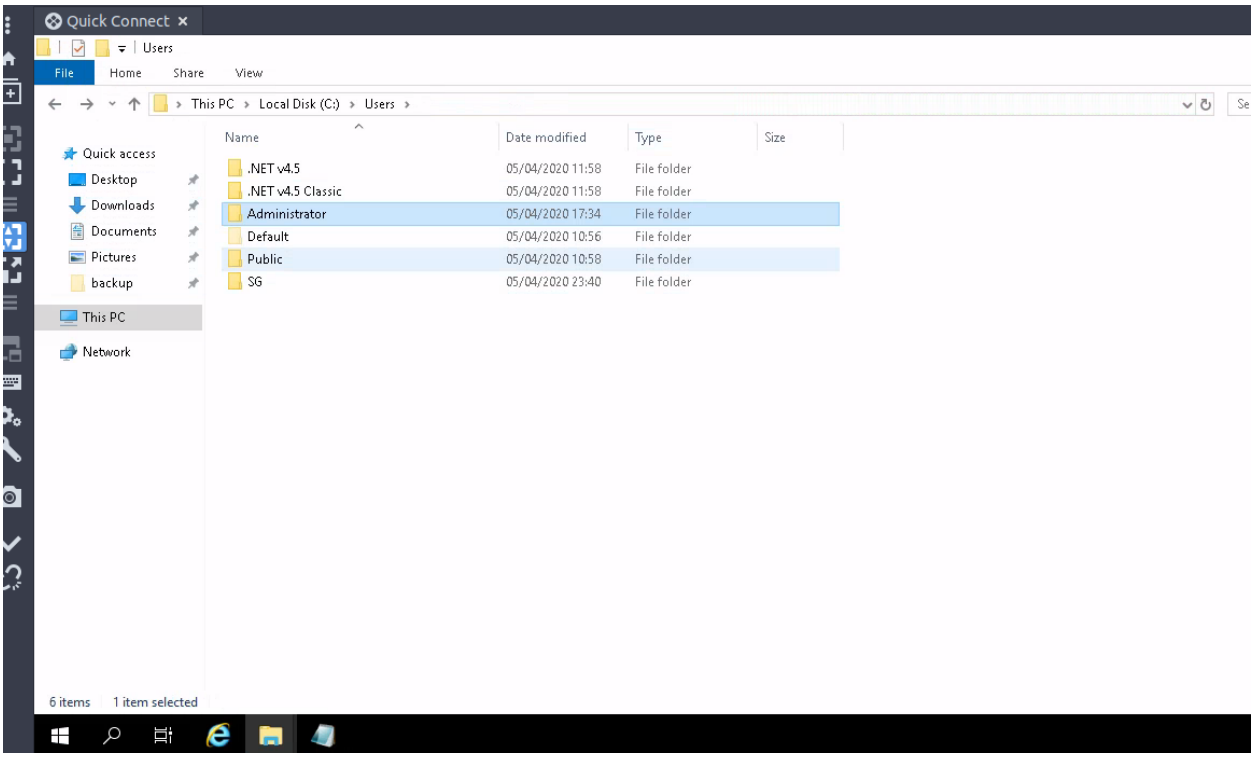


Then we head to the Local Disk C: , found the file but we don't have permission to open this file so we change permissions so we can be able to see the password

To change the permissions we right click on the file , choose properties, then choose security , then choose edit, then choose add, and type our username, then click on check names , the username will appear in the box then we choose apply. Now we can open the file and view the admin password

Escalate your privileges to root, what is the contents of root.txt?

Now we have the admin password we can escalate privilege by login in as Administrator . We can do that by opening remmina and putting in the credential or we just go to the location of the Administrator on the already open remmina session



clicking on the folder will ask for a password and we have it , the root.txt is found in the admin’s Desktop folder