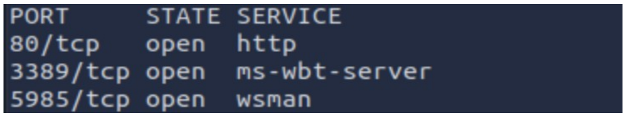
Anthem walkthrough Tryhackme
Exploit a windows machine

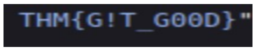
Task 1 Website analysis
The first tasks asks us to run nmap on the target website to see what ports are open.

nmap -sT -p- target ip
result:



```
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5985/tcp open  wsman
```

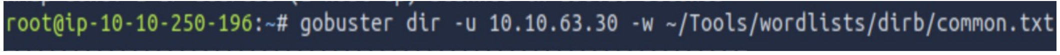
Question 1
What port is for the web server
Answer: 80
Question 2
What port is for the remote desktop service?
Answer: 3389
Question 3
What is the possible password in one of the pages the web crawlers check for?
This requires a bit more digging. After pulling up the website, we look at the source code with no luck in finding anything leading to the password, but we did find some possible information on a later task.



```
THM{G!T_G00D}"
```

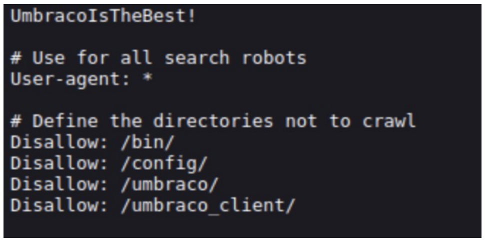
This was in the source code of the main page, but not sure yet how it is applicable.

Next idea is to use gobuster to scan the website for other common pages that may be accessible.



```
root@ip-10-10-250-196:~# gobuster dir -u 10.10.63.30 -w ~/Tools/wordlists/dirb/common.txt
```

After letting the program run, we find numerous directories. After searching through a few of them, we come across the robots.txt directory. Here is where we find some uselful information.



```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

# Define the directories not to crawl
Disallow: /bin/
Disallow: /config/
Disallow: /umbraco/
Disallow: /umbraco_client/
```

The top line starting with Umbraco looks similar to the format of the password, and so we try that and it is indeed the password.
Answer: UmbracoIsTheBest!

Question 4 – Wht CMS is the website using?
Answer : Umbraco

Question 5 – What is the domain of the website?
This is on the page when you first visit the website.
Answer: anthem.com

Question 6 – What is the name of the Administrator?
This one requires a little bit of OSINT. When navigating through the website, there is a blog post that has a poem about the administrator.
The poem starts with born on a Monday, christened on a tuesday and so on...
Taking this poem and putting into google, brings up comic book villain named Solomon Grundy.
Answer: Solomon Grundy

Question 7 – Can we find the email addreess of the administrator?
Looking around the website we cannot find any email for the administrator, but one of the emails is available for prosective employees in the we are hiring page. It is an email for Jane doe, and the format is jd@anthem.com
Using the deductive logic we try sg@anthem.com, and sure enough that is the answer.
Answer:sg@anthem.com

Task 2 -Spot the flags

Question 1: What is flag 1?
This is where We circle bag to the flag that was found in the source code earlier. Sure enough it was actually for the second flag in this task. The first flag is actually in the source code of the we are hiring page.
Answer: THM{L0L_WH0_US3S_M3T4}

Question 2: What is flag 2?
This is the flag that We were able to find earlier on the home page of the website.
Answer: THM{G!T_G00D}

Question 3: What is flag 3?
The hint on this question is Profile. We look around and find the profile of Jane doe, and the flag is actually on the page and not in the source code.
Answer:THM{L0L_WH0_D15}

Question 4: What is flag 4?
The hint on this question is have we inspected all pages yet. So we look around at some of the other pages available. Finally, we find the flag looking at the source code under the /archive/a-cheers-to-our-it-department.
Answer: THM{AN0TH3R_M3TA}

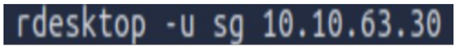
Task 3 Final Stage
Lets get into the box using the intel that we gathered.

Question 1: Let's figure out the username and password to log into the box. (The box is not in the domain)

This one took me a bit of time to figure out how we were going to log in. After using some OSINT, we learned about a program called rdesktop. It was not installed on the Kali linux attack box, so we went ahead and did this.

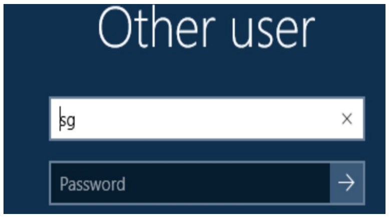
```
apt install rdesktop
```

looking at the command options the format looks like
rdesktop -u username target_ip



```
rdesktop -u sg 10.10.63.30
```

This gets us to the login page



Other user

sg

We use the password from the first task that we discovered earlier and sure enough we are logged into the remote desktop.

Question 2: what are the contents of the user.txt?
We open the file that is on the desktop and it reveals the flag.
Answer: THM{N00T_NO0T}

Question 3: can we spot the admin password?
We got to the file explorer and the users folder and try to open the administrator folder, but are unsuccessful, because we dont have access to the folder.
The hint says it is hidden. We alter the view to show hidden files in the file explorer. After doing this, We get back into the folder explorer to look at item that are hidden. This pulls up two more folders that we have not seen before, backup and program data.
In the backup folder we see a file called restore. Trying to open the file we do not have access.
Doing some more OSINT, we are actually able to edit the file permissions. It actually lets us add the user sg to allow us to access the file! I wouldn't have thought of this, but was able to get that intel from online.
After modifying the security access to the file we can open it up and find the answer.
Answer: ChangeMeBaby1MoreTime

Question 4: Escalate your privileges to root, what is the contents of root.txt?
For this we need to log into the administrator account for the remote desktop. After doing this with out newly found password, the root.txt is located on the desktop.
Answer: THM{Y0U_4R3_1337}