**Write-up Anthem Room (Try Hack Me)**

Task 1

1. Let's run nmap and check what ports are open.

I use the following command: nmap -sT 10.10.68.214 -p- -vv -A. The following ports are open: 80, 3389, 5985.

2. What port is for the web server?

The port for the web server is the http server: port 80.

3. What port is for remote desktop service?

The number of digits in the answer format gives the answer away: port 3389.

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

I initially did not understand the question, so I looked at the hint. The hint says: ‘fill in the gap \*\*\*\*\*\*.txt’. So I went to the website (http://10.10.57.119:80) and went to the robots.txt page (http://10.10.57.119:80/robots.txt). The first word seems a promising possible password: UmbracoIsTheBest!

5. What CMS is the website using?

I started by looking at the raw code with developer tools, but I couldn’t identify any clues for the CMS.

So I looked at any words with 7 letters that might be a CMS. I then remembered the password found in robots.txt that mentioned Umbraco. I had never heard of this CMS before.

6. What is the domain of the website?

This is clearly visible on the home page: anthem.com

7. What's the name of the Administrator?

With this domain name, I can run whois on the Linux terminal. The Admin name is listed as ‘Domain Administrator’. However, this answer does not fit the answer format.

The blog post on the website on December 31 2019 mentions the admin, describing him with a poem. When googling this poem, I get the name: Solomon Grundy.

8. Can we find the email address of the administrator?

The email address listed for the administrator in the whois information also does not fit the answer format.

I did find an email address on the website initially which fit the answer format (JD@anthem.com), but this is not the correct answer.

Maybe I need to find the actual email address of Solomon Grundy. Googling this name further reveals that this name is fictional.

Then I figured that the @anthem.com part of the email address of JD would also be in the email address of the administrator. Leaving only two letters to spare, I guessed that these would have to be the initials of Solomon Grundy, thus resulting in SG@anthem.com.

Task 2

Flag 1:

To find flags, I went through the source code of the blog posts and searched for THM. In the blog post ‘We are hiring’ I was able to find a flag in the source code in the meta content: THM{L0L\_WH0\_US3S\_M3T4}

Flag 2:

I came across this flag when looking through the source code to look for clues on the CMS of the website. The input text field for the search bar includes the flag: THM{G!T\_G00D}.

Flag 3:

I came across this flag when browsing the website looking for clues on the name of the administrator. In the blog post of ‘We are hiring’ the name of the author is clickable. The next page shows a flag: THM{LoL\_WHo\_D15}.

Flag 4:

Looking through the source code of the other blog post ‘A cheers to our IT department’, I got another hit for THM, in the flag located in the meta content: THM{AN0TH3R\_M3TA}.

**Task 3**

1. Let’s figure out the username and password to log in to the box.

To continue enumeration, I perform a Gobuster directory scan, additionally scanning for files with file extensions .conf, .config, .html, .php, or .txt. This scan reveals a number of directories, of which the /install directory seems particularly promising. Navigating to this page reveals a redirection to /umbraco/#/login. We are encountered with a log in page. When I enter ‘SG@anthem.com’ as username and ‘UmbracoIsTheBest!’ as password, I am granted access.

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

Looking around the back-end of Umbraco, I can’t find any files like user.txt.

Maybe I can find an exploit to gain access to a shell. I open Metasploit using msfconsole and then search for Umbraco (the CMS that is used for the website). This returns one hit, an exploit for remote command execution. To execute the exploit, I need to set RHOSTS, which is 10.10.217.119. The exploit seems to run fine, but no shell is instantiated. When checking the version of Umbraco that is vulnerable to the exploit (4.7.0.378), it is a different one than the version of Umbraco that the website is running on (7.15.4).

Reading through the website analysis of task 1 again, I figure that I might need to do something with the remote desktop service. Googling how to connect to an RDP from Linux takes me to Remmina program. Apparently, this program is already installed on the Attackbox. When opening it, I get prompted to enter a password. I don’t know a password for the local machine, so I click cancel. Still, Remmina is able to open. Now I need to input the target IP address. Then, I am prompted to fill in the username, password and domain. So the password is known (UmbracoIsTheBest!) and so is the domain (anthem.com). The username I should be able to guess. Since the email address is SG@anthem.com, my first guess is that the username is SG. This seems to work! On the desktop I can see the user.txt file, with the flag: THM{N00T\_NO0T}.

3. Can we spot the admin password?

NTLM hashes for all user passwords in Windows are located in C:\Windows\System32\config. However, I need to be administrator to access this directory. Looking around I can’t find any interesting files.

The hint says: ‘it is hidden’. I didn’t think of this, but we can choose to show hidden files and directories in the File Explorer by toggling the hidden items checkbox in the View tab. After doing this, a folder called ‘backup’ shows up in the Local Disk. In this folder is one file named ‘restore’, which might be interesting. When clicking on the file, I get notification that I don’t have permission to the access the file. Let’s see if I can set the permissions to this file myself. So I go to Properties and then to the Security tab. It says that no groups or users have access. So I click on Edit and add user SG. This actually seems to work! I can now open the file which contains the flag: ChangeMeBaby1MoreTime.

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

Now I know the password for the administrator account, let’s try to open the RDP connection with those credentials. This works and I can immediately see the root.txt file on the Desktop which holds the final flag: THM{Y0U\_4R3\_1337}.