

Anthem write-up by ChickenLoner

This is a write-up for Anthem room in TryHackMe which we need to do recon and explore website, find potential credentials, and connect to RDP, elevate our privilege to rock this box

Site: <https://tryhackme.com/room/anthem>

The screenshot shows the Anthem room interface on TryHackMe. At the top, there's a header with the room name 'Anthem' and a description 'Exploit a Windows machine in this beginner level challenge.' Below this, there are tabs for 'Chart', 'Scoreboard', 'Discuss', 'Writeups', and 'More'. A message states: 'This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 9878 users are in here and this room is 455 days old. Created by Chevalier'. A section titled 'Active Machine Information' contains a table with columns: Title, IP Address, Expires, and actions. The table lists 'Anthem VM' with IP 'Shown in 16s' and expires in '59m 16s'. Below the table is a progress bar at 0%. The 'Task 1' section is titled 'Website Analysis' and contains instructions: 'This task involves you, paying attention to details and finding the 'keys to the castle'. This room is designed for beginners, however, everyone is welcomed to try it out! Enjoy the Anthem. In this room, you don't need to brute force any login page. Just your preferred browser and Remote Desktop.' A 'Start Machine' button is visible.

Title	IP Address	Expires	
Anthem VM	Shown in 16s	59m 16s	? Add 1 hour Terminate

0%

Task 1 Website Analysis

This task involves you, paying attention to details and finding the 'keys to the castle'.

This room is designed for beginners, however, everyone is welcomed to try it out!

Enjoy the Anthem.

In this room, you don't need to brute force any login page. Just your preferred browser and Remote Desktop.

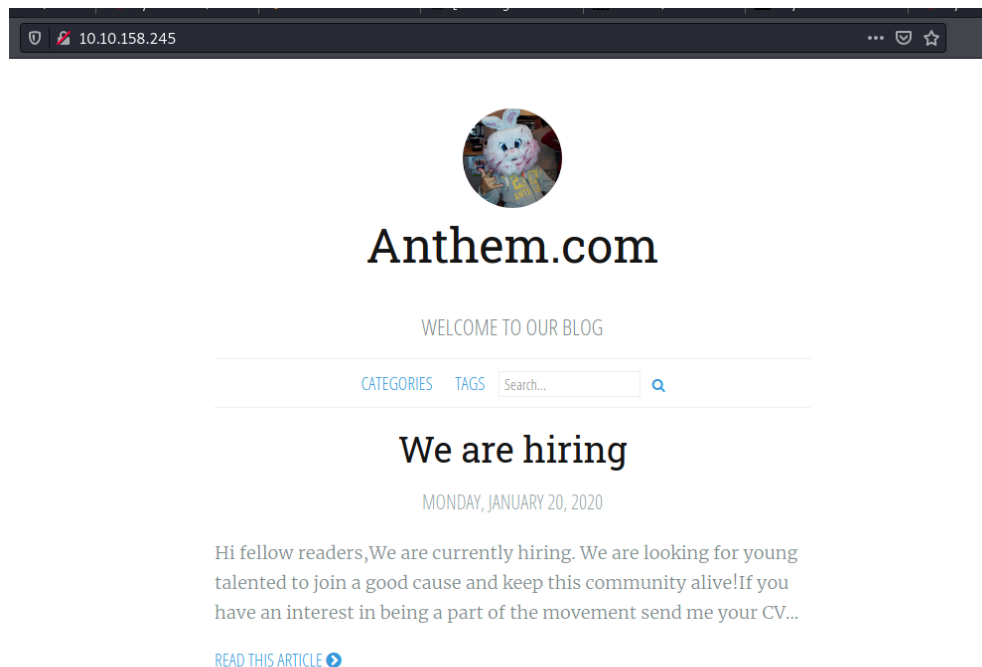
Let's do recon! Always start with nmap we can see that web server is running and RDP port is opened

```
(kali@kali)~[/snoopbees/CTF]
$ sudo nmap -Pn -sC -sV 10.10.158.245
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-13 09:38 EDT
Nmap scan report for 10.10.158.245
Host is up (0.23s 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
rdp-ntlm-info:
  Target_Name: WIN-LU09299160F
  NetBIOS_Domain_Name: WIN-LU09299160F
  NetBIOS_Computer_Name: WIN-LU09299160F
  DNS_Domain_Name: WIN-LU09299160F
  DNS_Computer_Name: WIN-LU09299160F
  Product_Version: 10.0.17763
  System_Time: 2021-08-13T13:39:20+00:00
  ssl-cert: Subject: commonName=WIN-LU09299160F
  Not valid before: 2021-08-12T13:35:37
  Not valid after: 2022-02-11T13:35:37
  ssl-date: 2021-08-13T13:40:10+00:00; -1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 85.65 seconds
```

It's time to check website, its blog website that has Anthem.com as domain name



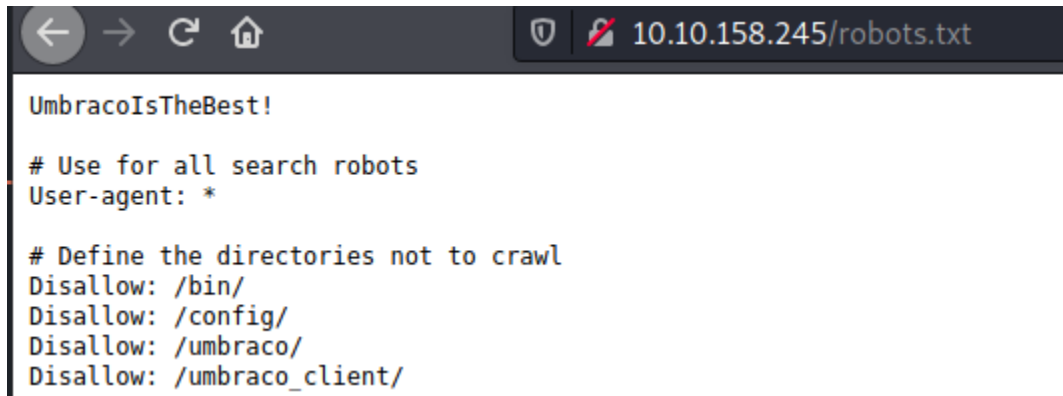
A cheers to our IT department

Inspect source code we can see a flag hidden in Search bar

```
view-source:http://10.10.158.245/

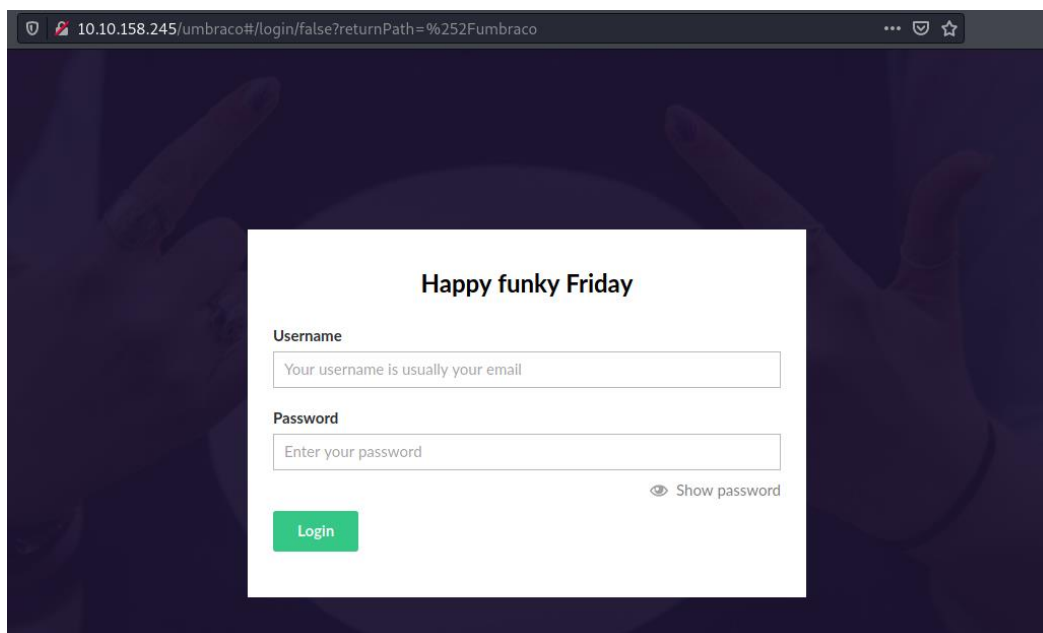
31     <a id="blog-logo" href="/">
32         <div class="bloglogo" style="background: url(/media/articulate/default/capture3.png?mode=max&rnd=
33     </a>
34
35     <h1 class="blog-title">
36         <a href="/">
37             Anthem.com
38         </a>
39     </h1>
40
41     <h2 class="blog-description">
42         Welcome to our blog
43 </h2>
44     <nav class="menu" role="nav">
45         <ul>
46             <li><a href="/categories">Categories</a></li>
47             <li><a href="/tags">Tags</a></li>
48             <li>
49                 <div class="articulate-search">
50                     <form method="get" action="/search">
51                         <input type="text" name="term" placeholder="Search..."
52                         <button type="submit" class="fa fa-search fa"></button>
53                     </form>
54                 </div>
55             </li>
56         </ul>
57     </nav>
58
59 </header>
```

Check robots.txt every times if possible and there are 4 directories that will be blocked from crawler and seem like UmbracoIsTheBest! could be the website owner's password



```
UmbracoIsTheBest!  
  
# Use for all search robots  
User-agent: *  
  
# Define the directories not to crawl  
Disallow: /bin/  
Disallow: /config/  
Disallow: /umbraco/  
Disallow: /umbraco_client/
```

After checked /bin and /config, there 2 are nothing but /umbraco is login page now we need only an email



10.10.158.245/umbraco#/login/false?returnPath=%252Fumbraco

Happy funky Friday

Username

Password

[Show password](#)

Login

I launched gobuster and found /sitemap which will tell us every directory of this blog that we could visit

```
10.10.158.245/SiteMap
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<urlset xmlns:schema="http://www.sitemaps.org/schemas/sitemap/0.9" http://www.sitemaps.org/schemas/sitemap/0.9/sitemap.xsd">
  <url>
    <loc>http://10.10.158.245/blog/</loc>
    <lastmod>2020-04-05T20:37:17+00:00</lastmod>
  </url>
  <url>
    <loc>http://10.10.158.245/archive/</loc>
    <lastmod>2020-04-05T19:11:38+00:00</lastmod>
  </url>
  <url>
    <loc>http://10.10.158.245/archive/we-are-hiring/</loc>
    <lastmod>2020-04-05T21:01:02+00:00</lastmod>
  </url>
  <url>
    <loc>http://10.10.158.245/archive/a-cheers-to-our-it-department/</loc>
    <lastmod>2020-04-05T21:02:29+00:00</lastmod>
  </url>
  <url>
    <loc>http://10.10.158.245/authors/</loc>
    <lastmod>2020-04-05T23:13:00+00:00</lastmod>
  </url>
  <url>
    <loc>http://10.10.158.245/authors/jane-doe/</loc>
    <lastmod>2020-04-05T21:11:16+00:00</lastmod>
  </url>
</urlset>
```

Check first post which posted by Jane Doe, we will get their email pattern here JD from Jane Doe and followed with @anthem.com

We are hiring

MONDAY, JANUARY 20, 2020

Hi fellow readers,

We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!

If you have an interest in being a part of the movement send me your CV at JD@anthem.com

SHARE THIS POST



AUTHOR

Jane Doe

Author for Anthem blog

Inspect web page and there is a flag hidden in source code

```
view-source:http://10.10.158.245/archive/we-are-hiring/


1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta http-equiv="Content-Type" content="text/html" charset="UTF-8" />
5   <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
6
7   <title>We are hiring - Anthem.com</title>
8   <meta name="description" content="Hi fellow readers,We are currently hiring. We are looking for young talented to join a good ca
9   <meta name="twitter:card" value="summary">
10  <meta content="We are hiring" property="og:title" />
11  <meta content="article" property="og:type" />
12  <meta content="http://10.10.158.245/archive/we-are-hiring/" property="og:url" />
13  <meta content="THM{LoL_WHo_US3S_M3T4}" property="og:description" />
14
15  <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.158.245/rsd/1073" />
16  <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.158.245/wlwmanifest/1073" />
17  <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.158.245/rss" />
18  <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.158.245/opensearch/1073" title="Search Blog"
19  <meta name="HandheldFriendly" content="True" />
20  <meta name="MobileOptimized" content="320" />
21  <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no" />
22
```

Let's see his/her profile and we also got a flag here!

10.10.158.245/authors/jane-doe/

CATEGORIES TAGS Search...

Jane Doe



Author for Anthem blog

Website: THM{LoL_WHo_D15}

We are hiring

MONDAY, JANUARY 20, 2020

Hi fellow readers,We are currently hiring. We are looking for young

Now let's go to the other post, this post is about the employer wrote something about his admin and we can do a little more osint base on this poem

A cheers to our IT department

TUESDAY, DECEMBER 31, 2019

During our hard times our beloved admin managed to save our business by redesigning the entire website.

As we all around here knows how much I love writing poems I decided to write one about him:

Born on a Monday,
Christened on Tuesday,
Married on Wednesday,
Took ill on Thursday,
Grew worse on Friday,
Died on Saturday,
Buried on Sunday.
That was the end...

And there is it! Solomon Grundy could be his admin, so his email would be SG@anthem.com

Born on a Monday, Christened on Tuesday, Married on Wednesday, Took ill on Th



All

News

Images

Videos

Shopping

More

Tools

About 3,450,000 results (1.20 seconds)

Solomon Grundy

Song by The Foundations

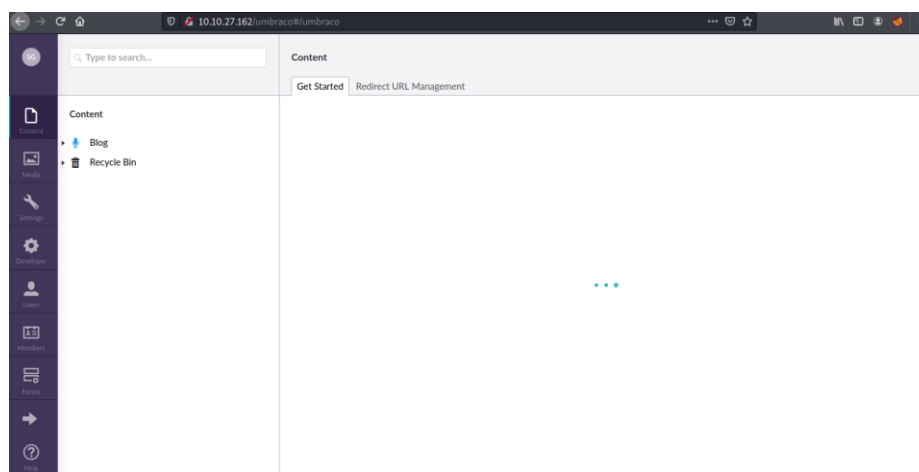


But we also need 1 flag left so inspect this post too we will get our last recon flag

```
view-source:http://10.10.158.245/archive/a-cheers-to-our-it-department/

1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta http-equiv="Content-Type" content="text/html" charset="UTF-8" />
5   <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
6
7   <title>A cheers to our IT department - Anthem.com</title>
8   <meta name="description" content="During our hard times our beloved admin managed to save our business by redesigning the entire website.As we all around here kno
9   <meta name="twitter:card" value="summary">
10  <meta content="A cheers to our IT department" property="og:title" />
11  <meta content="article" property="og:type" />
12  <meta content="http://10.10.158.245/archive/a-cheers-to-our-it-department/" property="og:url" />
13  <meta content="THM(AN0TH3R_M3TA)" property="og:description" />
14
15  <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.158.245/rsd/1073" />
16  <link rel="wlmanifest" type="application/wlmanifest+xml" href="http://10.10.158.245/wlmanifest/1073" />
17  <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.158.245/rss" />
18  <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.158.245/opensearch/1073" title="Search Blog" >
19  <meta name="HandheldFriendly" content="True" />
20  <meta name="MobileOptimized" content="320" />
21  <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no" />
22
```

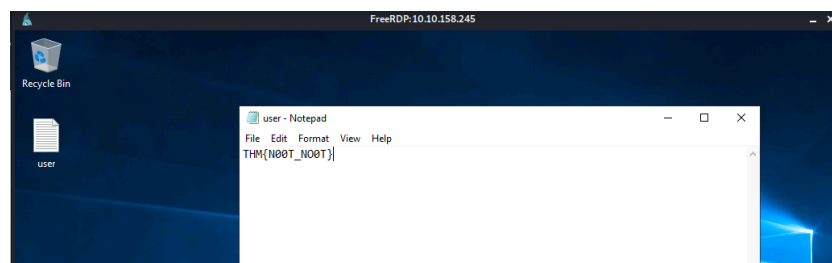
Now back to /umbraco and try to login with that credentials and its legit!



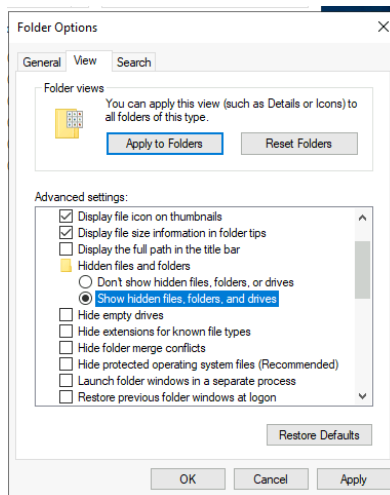
Now it's time to connect to his machine via RDP

```
(kali@kali)-[~/Tryhackme]
$ xfreerdp /u:SG /p:UmbracoIsTheBest! /cert:ignore /v:10.10.138.101
```

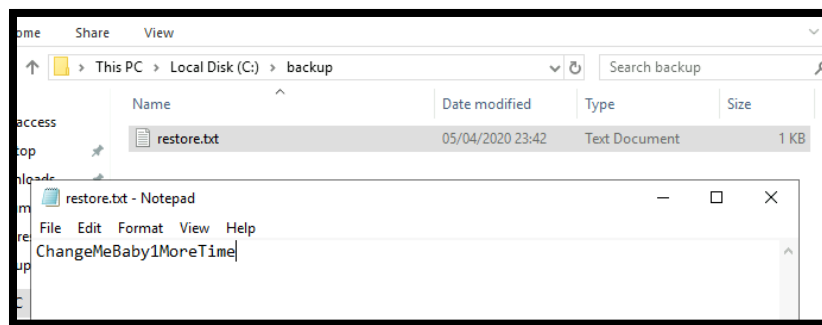
Once we connected we will get our user flag on Desktop



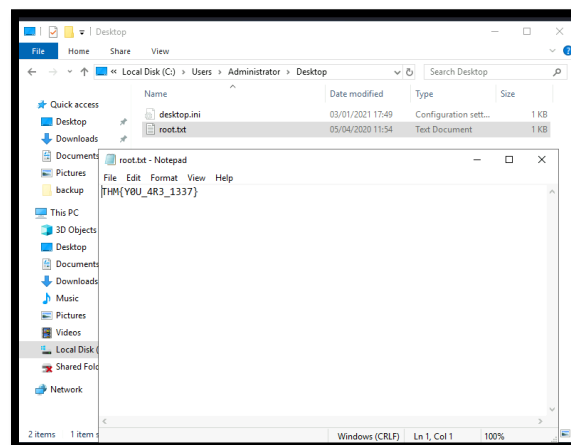
We don't have much to do here since I have no idea how to transfer file to this machine so I checked hint and it said that admin credential is hidden so I went to explorer and set up to show everything



I found out that backup directory have a text file which could be administrator password



Now we can go to Administrator directory directly and read root flag



Or you can use Administrator PowerShell and loot this flag

```
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----             05/04/2020      11:54           17 root.txt

PS C:\Users\Administrator\Desktop> more root.txt
THM{Y0U_4R3_1337}

PS C:\Users\Administrator\Desktop>
```

All answers and flags

Website Analysis

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

No answer needed

Question Done

What port is for the web server?

80

Correct Answer

What port is for remote desktop service?

3389

Correct Answer

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

UmbracolsTheBest!

Correct Answer

Hint

What CMS is the website using?

Umbraco

Correct Answer

What is the domain of the website?

anthem.com

Correct Answer

What's the name of the Administrator

Solomon Grundy

Correct Answer

Hint

Can we find the email address of the administrator?

SG@anthem.com

Correct Answer

Hint

Spot the flags

What is flag 1?

THM{LOL_WH0_US3S_M3T4}

Correct Answer

 Hint

What is flag 2?

THM{G!T_G00D}

Correct Answer

 Hint

What is flag 3?

THM{LOL_WH0_D15}

Correct Answer

 Hint

What is flag 4?

THM{AN0TH3R_M3TA}

Correct Answer

 Hint

Final stage

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

No answer needed

Question Done

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

THM{N00T_NO0T}

Correct Answer

Can we spot the admin password?

ChangeMeBaby1MoreTime

Correct Answer

 Hint

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

THM{YOU_4R3_1337}

Correct Answer