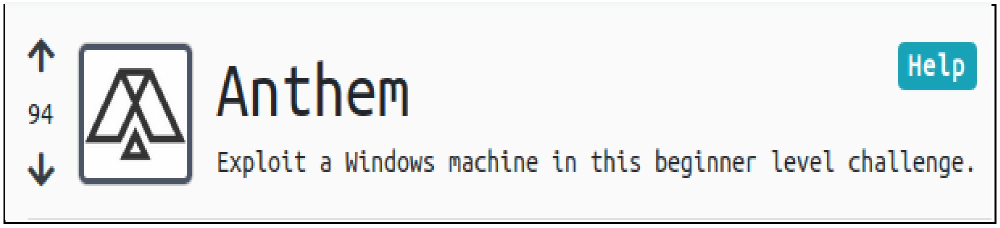
Hey,

This time we have a windows machine "Anthem" from tryhackme, this is good for beginner level but some of the time it made me frustrated to finding flags. You can access this machine from this URL: https://tryhackme.com/room/anthem.

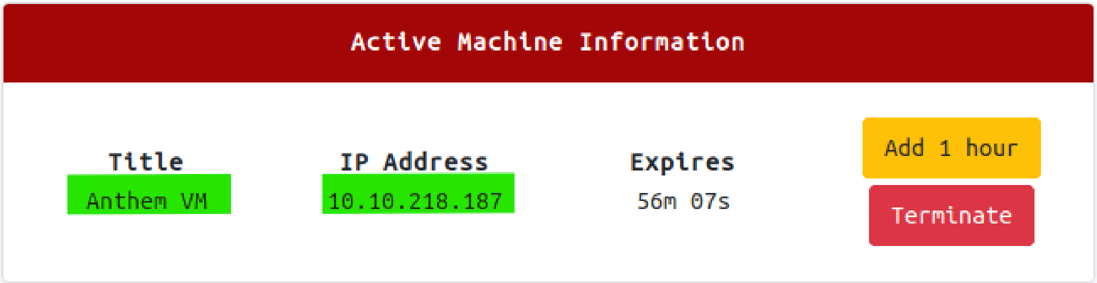


Anthem

Exploit a Windows machine in this beginner level challenge.

So, Let's Deploy the machine first,

We can see our machine IP which is 10.10.218.187 and the title "Anthem VM"



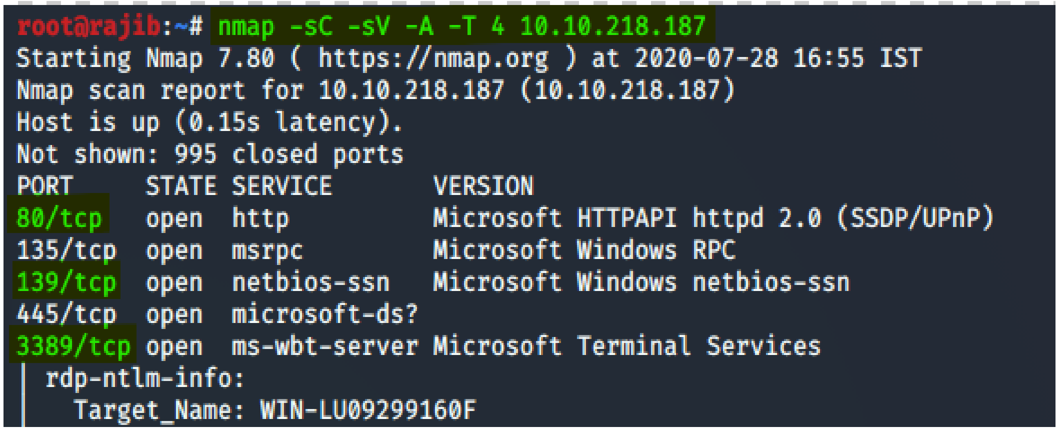
Active Machine Information

Title	IP Address	Expires
Anthem VM	10.10.218.187	56m 07s

[Task 1] Website Analysis

After checking connectivity with my Kali machine,

#1 I started NMAP scan to see open ports & services. Which will be more help full to understand the machine.



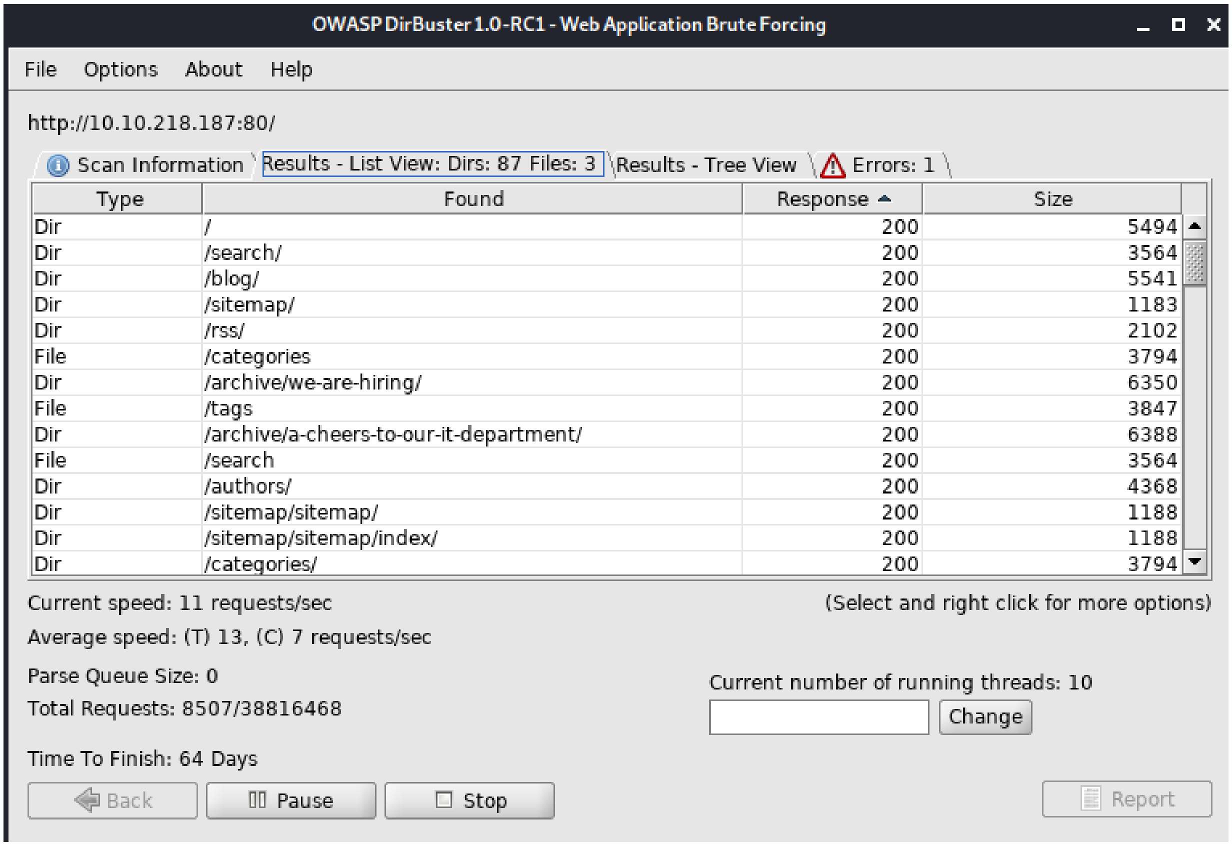
```
root@rajib:~# nmap -sC -sV -A -T 4 10.10.218.187
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-28 16:55 IST
Nmap scan report for 10.10.218.187 (10.10.218.187)
Host is up (0.15s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: WIN-LU09299160F
```

So, here we have got Port 80, Port 135, Port 445 & Port 3389 which is an RDP port.

#2 What port is for the web server? --- Clearly, we can understand that Port 80 is for the web server.

#3 What port is for remote desktop service? ---- we can identify this one also from NMAP is 3389.

So, no other Information from here, let's search some hidden directory with Dirbuster.

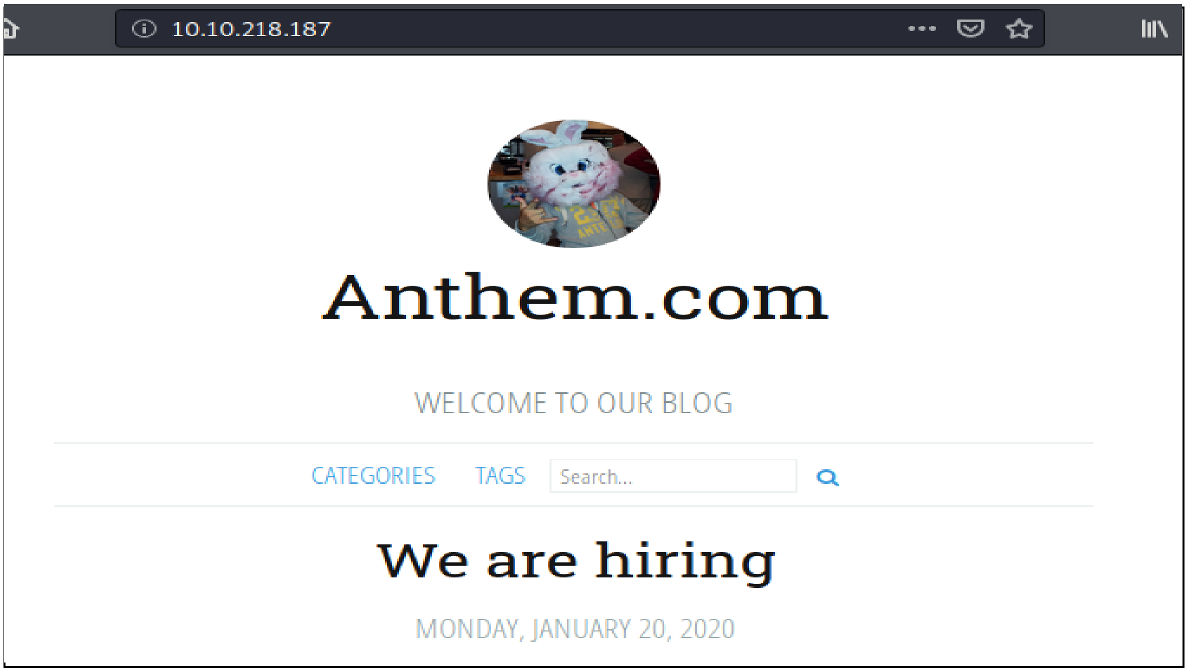

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 87 Files: 3
Results - Tree View
Errors: 1
Back
Pause
Stop
Change
Report

http://10.10.218.187:80/

Type	Found	Response	Size
Dir	/	200	5494
Dir	/search/	200	3564
Dir	/blog/	200	5541
Dir	/sitemap/	200	1183
Dir	/rss/	200	2102
File	/categories	200	3794
Dir	/archive/we-are-hiring/	200	6350
File	/tags	200	3847
Dir	/archive/a-cheers-to-our-it-department/	200	6388
File	/search	200	3564
Dir	/authors/	200	4368
Dir	/sitemap/sitemap/	200	1188
Dir	/sitemap/sitemap/index/	200	1188
Dir	/categories/	200	3794

Current speed: 11 requests/sec
(Select and right click for more options)
Average speed: (T) 13, (C) 7 requests/sec
Parse Queue Size: 0
Total Requests: 8507/38816468
Current number of running threads: 10
Time To Finish: 64 Days

Ok from here we have found some directories, I went through some of the interesting links, but nothing really interesting information I have got nor any vector we can exploit. So decided to do manual enumeration.



10.10.218.187

Anthem.com

WELCOME TO OUR BLOG

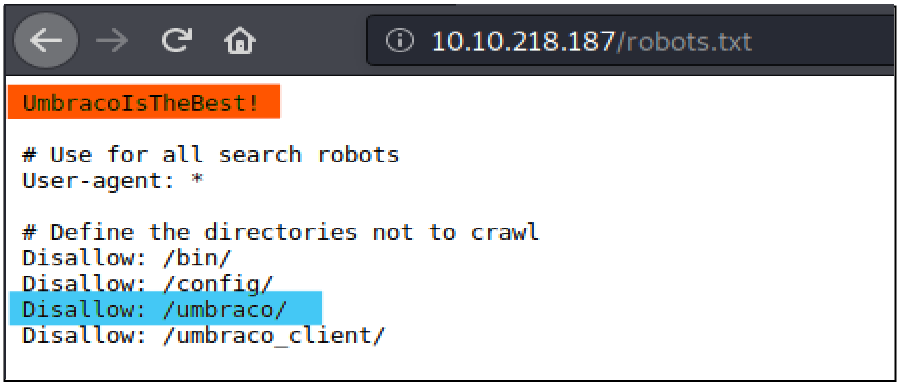
We are hiring

MONDAY, JANUARY 20, 2020

Here we can see it is a blog post site.

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

Now let's check what we can find with "robots.txt"…!!



10.10.218.187/robots.txt

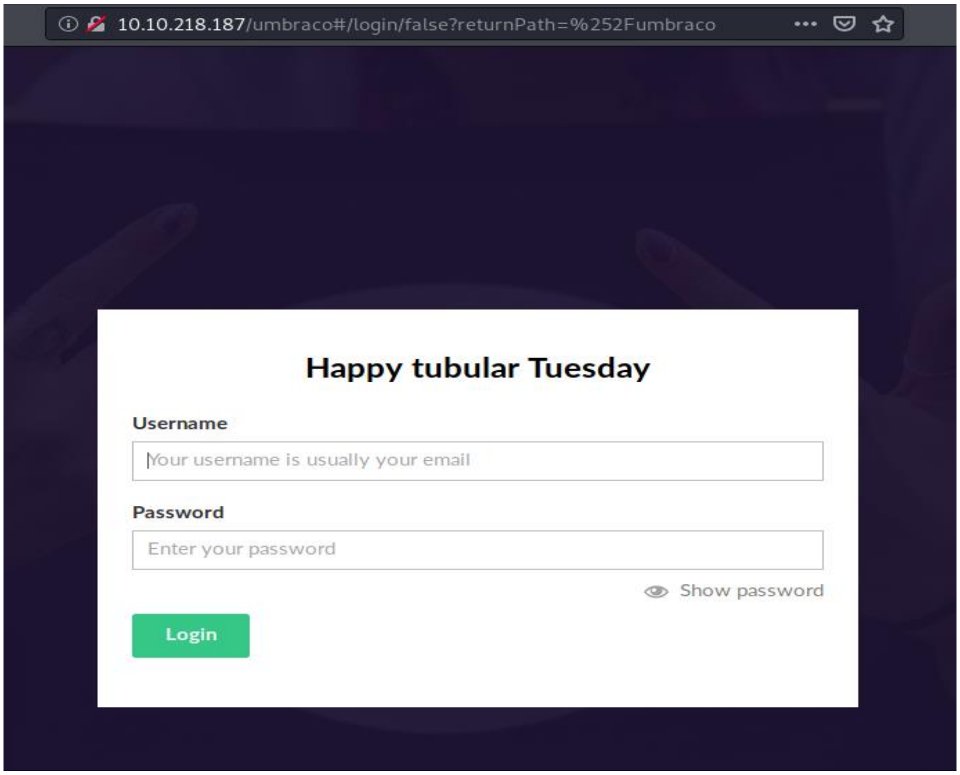
```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

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

So here I have got some information…!!

"UmbracoIsTheBest" it looks like a password.

Robots.txt (Read about them here): https://www.cloudflare.com/learning/bots/what-is-robots.txt/

Also Here are some directories which already kept in disallow, & not to crawl. But as a hacker we have to try every thing & have to think out of the box. After trying all "/umbraco" leads us to a administrator's login page but we still don't have credentials to log into the page. So, started investigate deeply.



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

Happy tubular Tuesday

Username

Your username is usually your email

Password

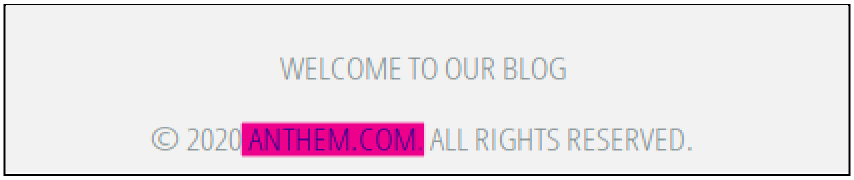
Enter your password

#5 What CMS is the website using? --- From above login page we can understand, it is using “umbraco” CMS

#6 What is the domain of the website? ----Here we have found domain of the website, “ANTHEM.COM”

Also, we can find this with NMAP also,

Command: nmap -n -p80 –script=http-title <ip of target machine>



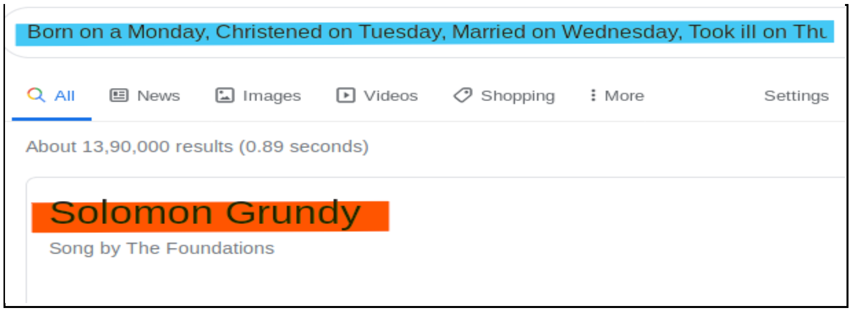
WELCOME TO OUR BLOG

© 2020 ANTHEM.COM ALL RIGHTS RESERVED.

#7 What's the name of the Administrator?

Don’t think too much for this, I have also stuck here. Just read properly content of the page you can able to find the administrator. *Hint*- There is no standard name for Admin user...!!!

Looking at the Second post we get some interesting information a poem about admin I spend a while here trying to work things out but finally, I got the username. I copied the entire poem and did a google search thereon, and therefore the first result was a username



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

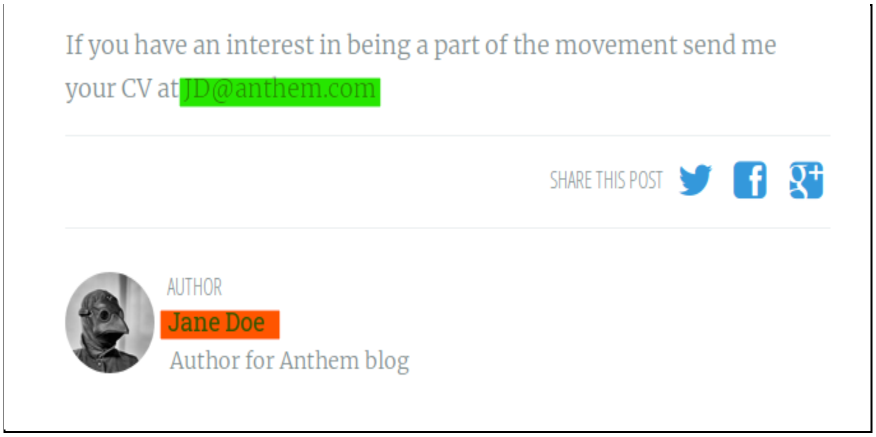
About 13,90,000 results (0.89 seconds)

Solomon Grundy

Song by The Foundations

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

-- Format is in one of the webpages. Look for it. Looking at the “we are hiring post” we see that the author of that post is Jane Doe and that we find the way naming is perhaps done by the utilization of an email, It will be SG@anthem.com.



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

AUTHOR

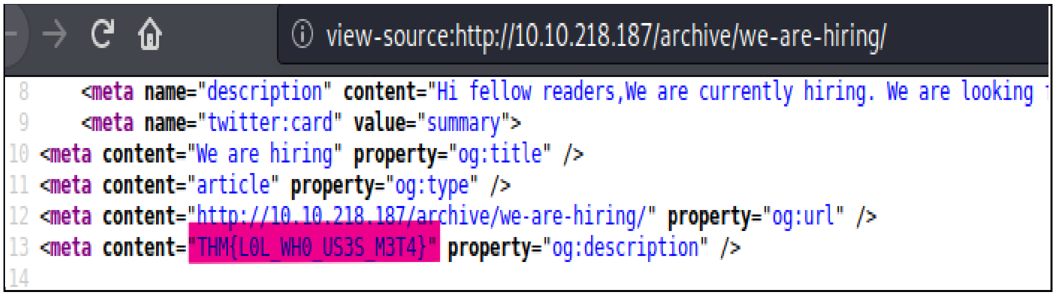
Jane Doe

Author for Anthem blog

[Task 2] Spot the flags

#1 What is flag 1?

Always check the Page Source of the Web Pages…!! I got this from blog post "we are hiring"

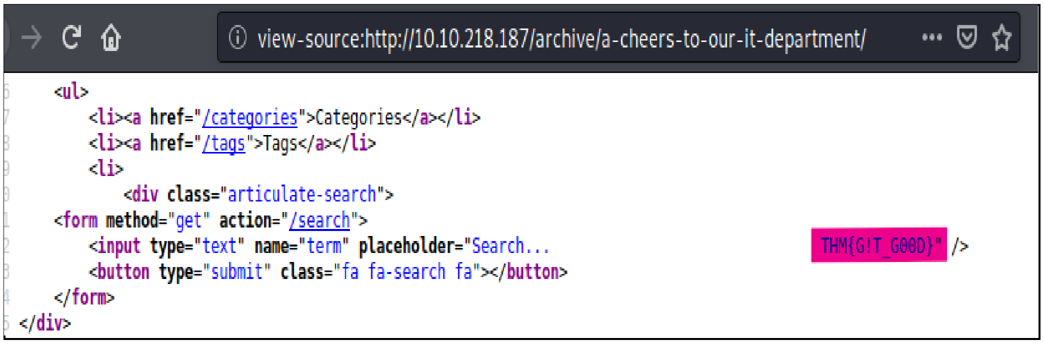


view-source:http://10.10.218.187/archive/we-are-hiring/

```
    <meta name="description" content="Hi fellow readers,We are currently hiring. We are looking
    <meta name="twitter:card" value="summary">
<meta content="We are hiring" property="og:title" />
<meta content="article" property="og:type" />
<meta content="http://10.10.218.187/archive/we-are-hiring/" property="og:url" />
<meta content="THM{L0L_WH0_US3S_M3T4}" property="og:description" />
```

#2 What is flag 2?

Again, always check the Page Source of the Web Pages…!! It always gives us some important information. Developers are often forgetting to delete that information which they have put there for their own purpose.

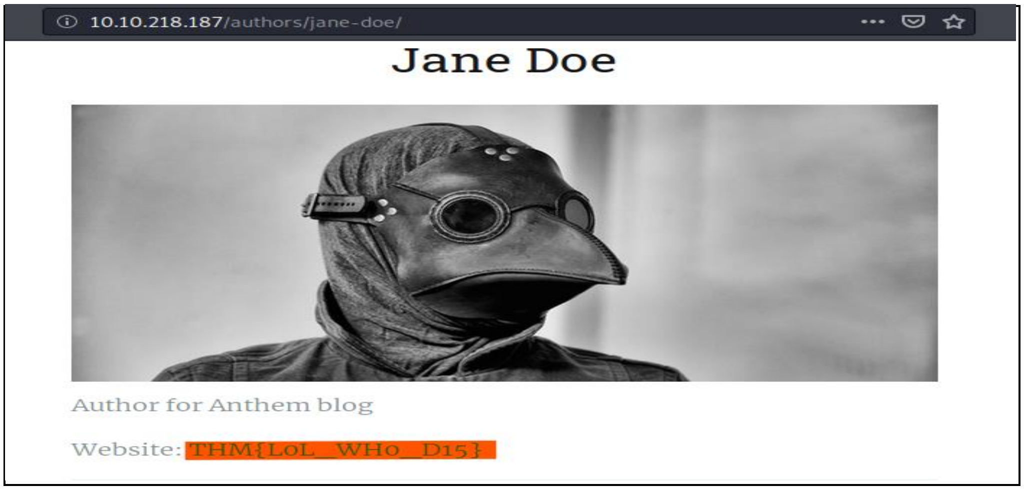


view-source:http://10.10.218.187/archive/a-cheers-to-our-it-department/

```
    <ul>
        <li><a href="/categories">Categories</a></li>
        <li><a href="/tags">Tags</a></li>
        <li>
            <div class="articulate-search">
    <form method="get" action="/search">
        <input type="text" name="term" placeholder="Search...                    THM{G!T_G00D}" />
        <button type="submit" class="fa fa-search fa"></button>
    </form>
</div>
```

#3 What is flag 3?

Look deeply on web pages…!!



10.10.218.187/authors/jane-doe/

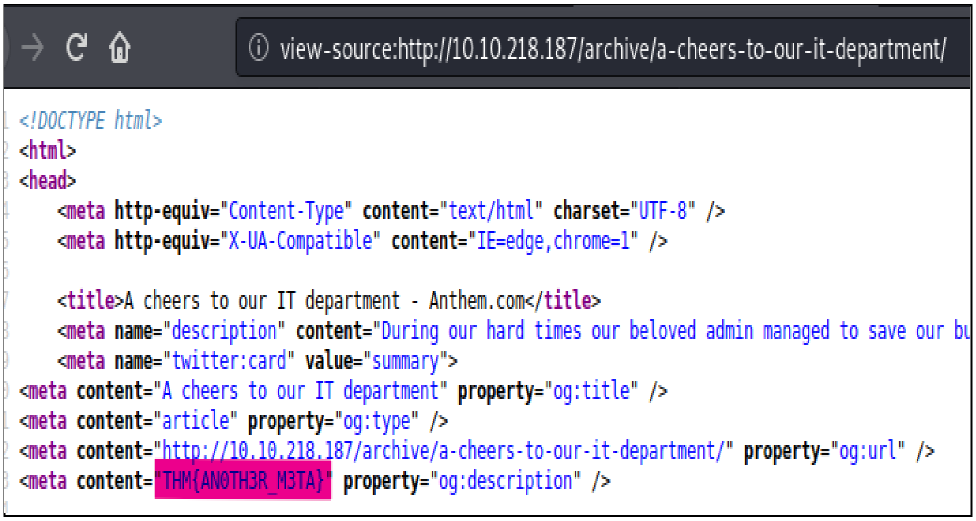
Jane Doe

Author for Anthem blog

Website: THM{LoL_WHo_D15}

#4 What is flag 4?

Look more, and try harder…!!



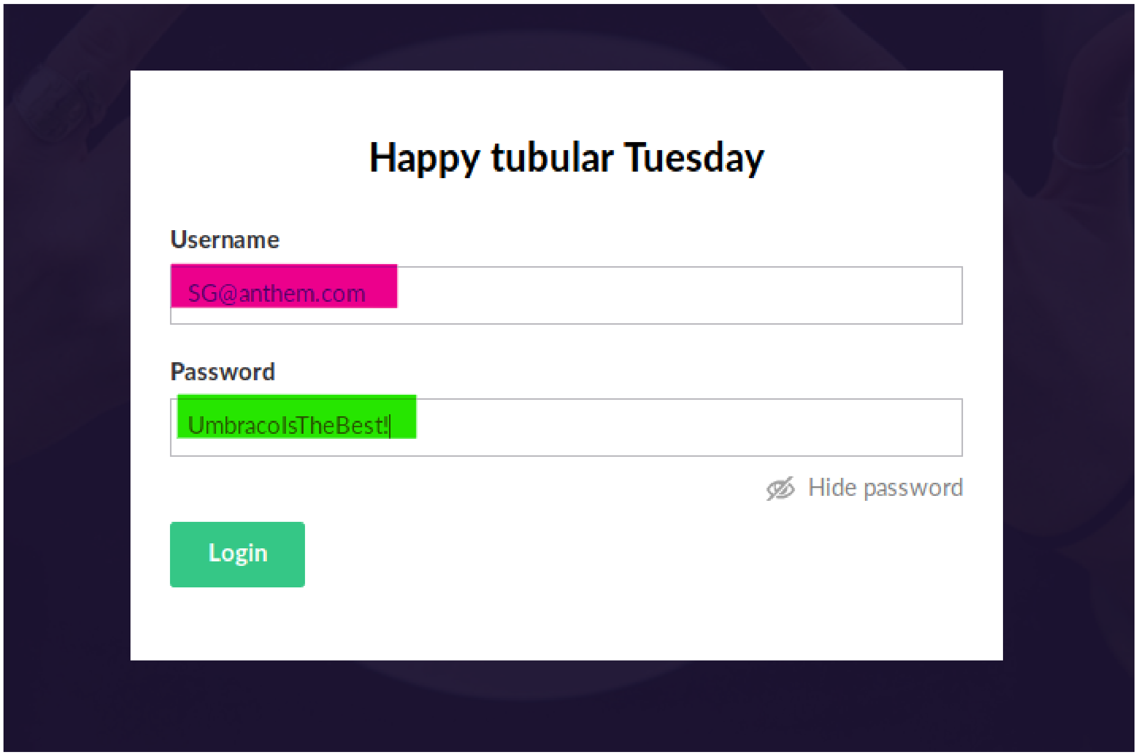
view-source:http://10.10.218.187/archive/a-cheers-to-our-it-department/

```
<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html" charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />

    <title>A cheers to our IT department - Anthem.com</title>
    <meta name="description" content="During our hard times our beloved admin managed to save our bu
    <meta name="twitter:card" value="summary">
<meta content="A cheers to our IT department" property="og:title" />
<meta content="article" property="og:type" />
<meta content="http://10.10.218.187/archive/a-cheers-to-our-it-department/" property="og:url" />
<meta content="THM{AN0TH3R_M3TA}" property="og:description" />
```

[Task 3] Final stage

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

So, we have the Admin Username which we have got previously and the password which we found from "robots.txt". Let's try with those credentials.

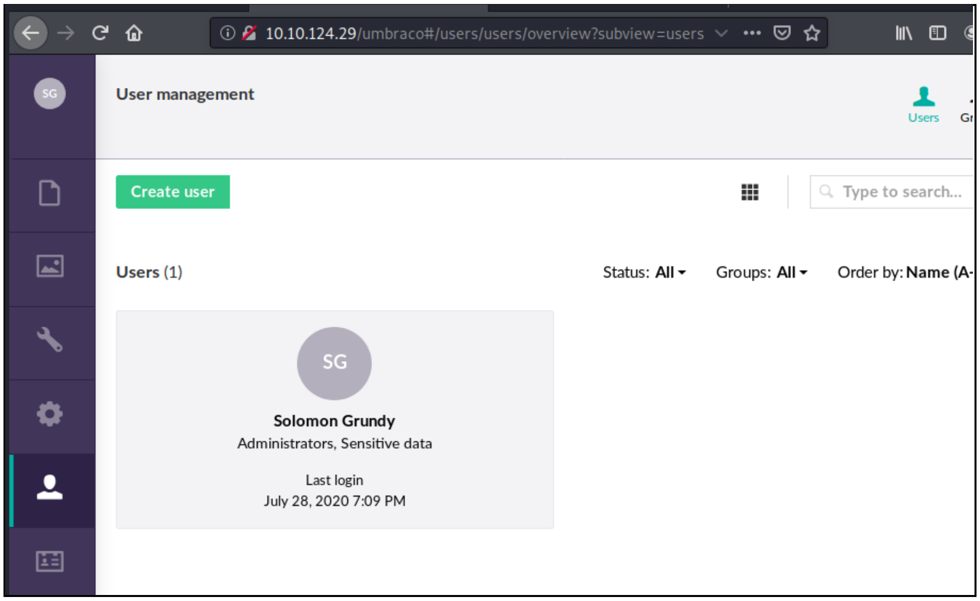


Happy tubular Tuesday

Username: SG@anthem.com

Password: UmbracoIsTheBest!

Oh, we have successfully login with username "SG@anthem.com"



10.10.124.29/umbraco#/users/users/overview?subview=users

User management

Users (1)

Status: All Groups: All Order by: Name (A-

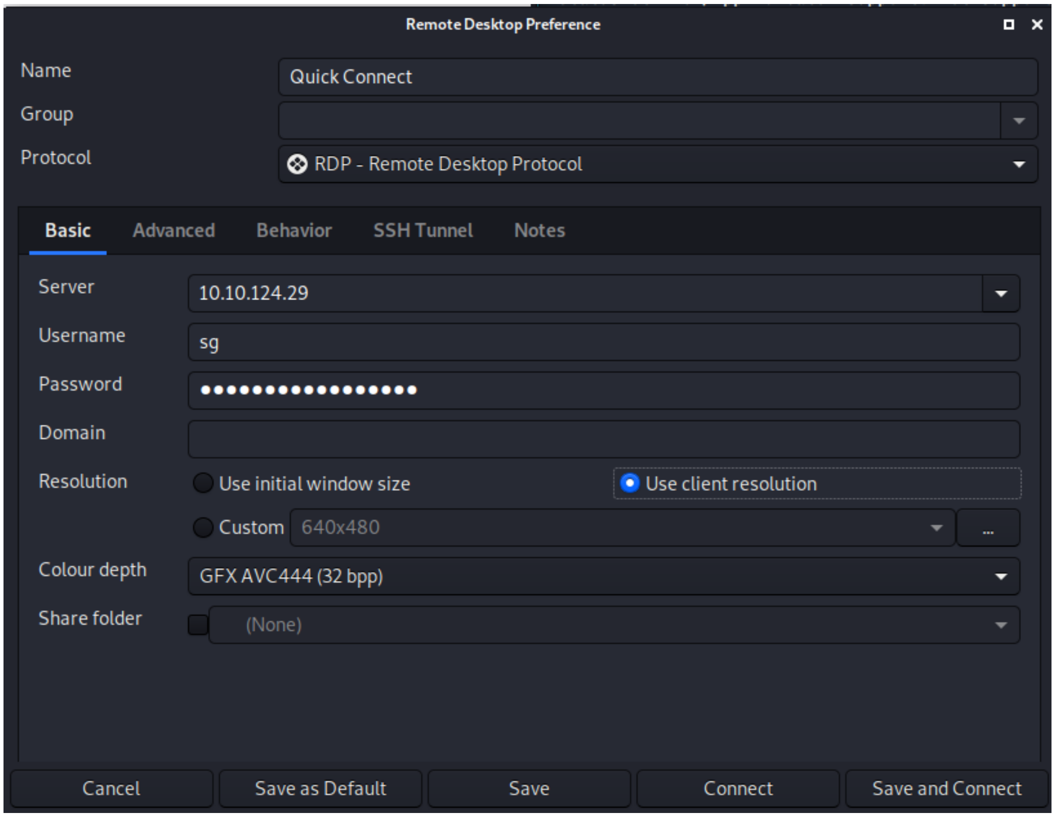
Solomon Grundy
Administrators, Sensitive data

Last login
July 28, 2020 7:09 PM

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

So now we have user name along with password, also have the server IP. There is an RDP port open. Now we can try to login with RDP port.

I have used "remmina" tool to get RDP access on target machine



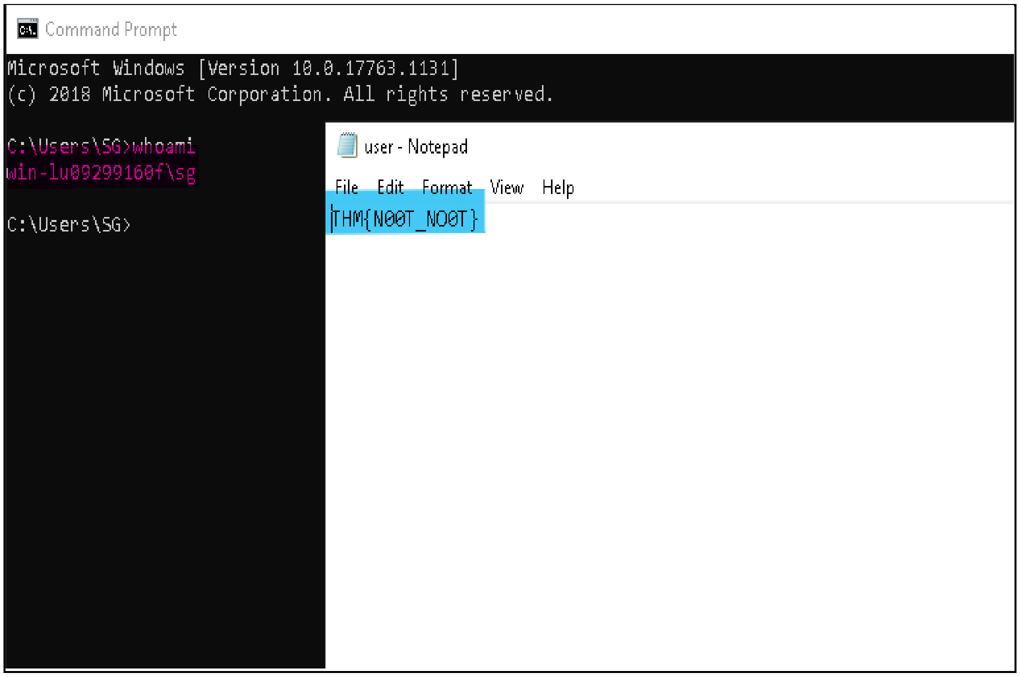
Remote Desktop Preference

Name: Quick Connect
Group:
Protocol: RDP - Remote Desktop Protocol

Server: 10.10.124.29
Username: sg
Password: ●●●●●●●●●●●●●●●●●●
Domain:
Resolution: ○ Use initial window size ● Use client resolution
○ Custom 640x480
Colour depth: GFX AVC444 (32 bpp)
Share folder: □ (None)

After providing server IP and user credential, we have got access on target machine.

After getting access of the user account, I have easily got our next flag which is inside of “user.txt”



Command Prompt

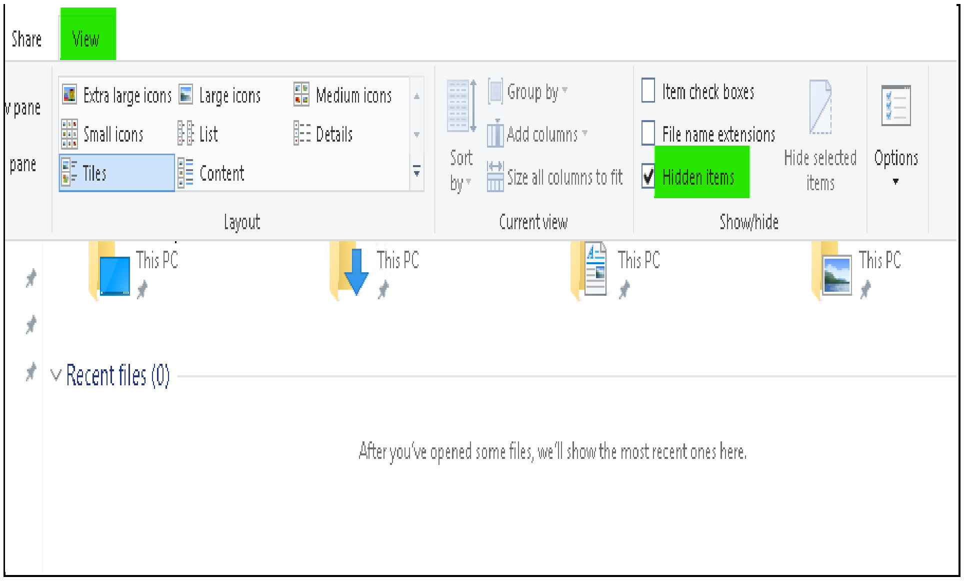
```
Microsoft Windows [Version 10.0.17763.1131]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\SG>whoami
win-lu09299160f\sg

C:\Users\SG>
```

user - Notepad

```
THM{N00T_NO0T}
```

#3 Can we spot the admin password?

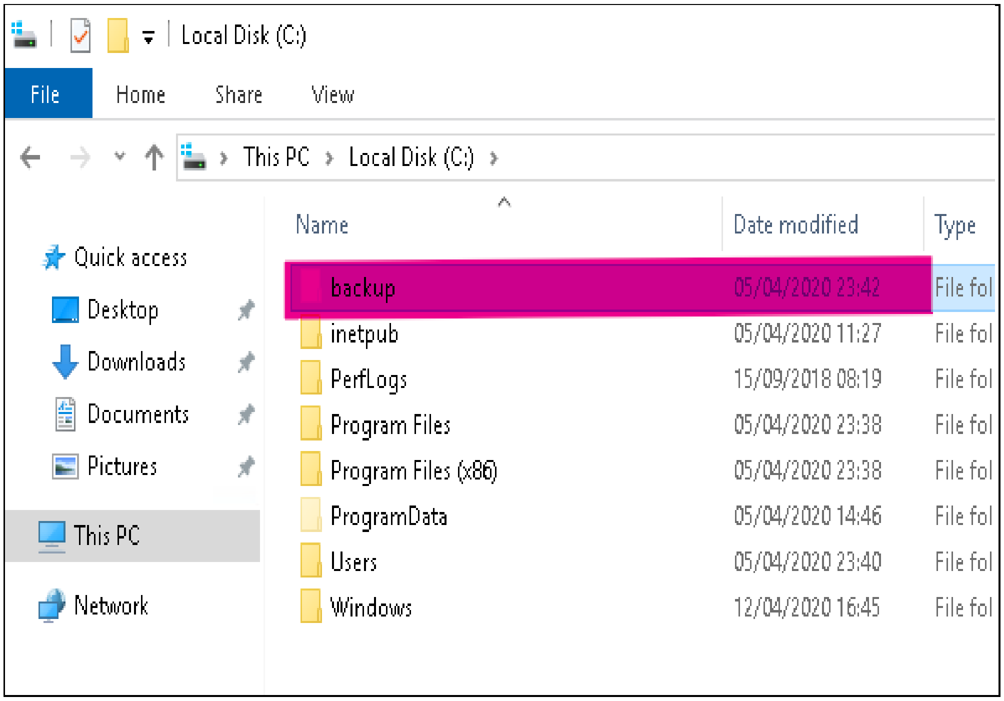
After searching for sometime I could not able to find any kind of interesting file which may contain admin password. So, I thought it may be hidden. So, unhide all (view --> hidden items).



☐ Item check boxes
☐ File name extensions
☑ Hidden items

After you've opened some files, we'll show the most recent ones here.

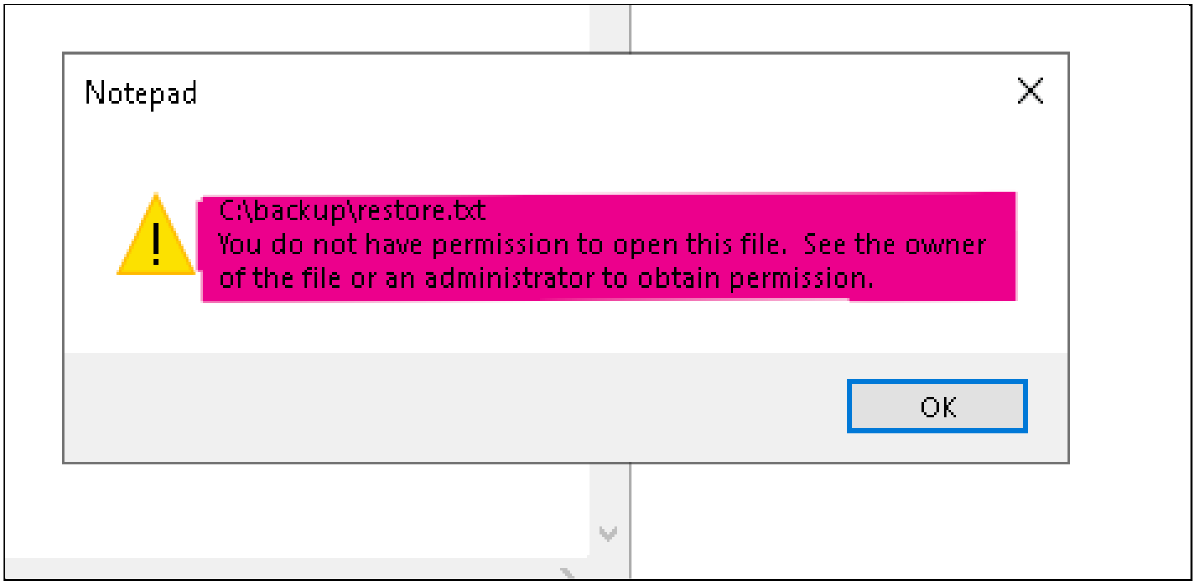
After unhiding the files, I have found one interesting folder name “backup”, and inside that there was “restore.txt” file. Yes, it is now more interesting.



Name	Date modified	Type
backup	05/04/2020 23:42	File fol
inetpub	05/04/2020 11:27	File fol
PerfLogs	15/09/2018 08:19	File fol
Program Files	05/04/2020 23:38	File fol
Program Files (x86)	05/04/2020 23:38	File fol
ProgramData	05/04/2020 14:46	File fol
Users	05/04/2020 23:40	File fol
Windows	12/04/2020 16:45	File fol

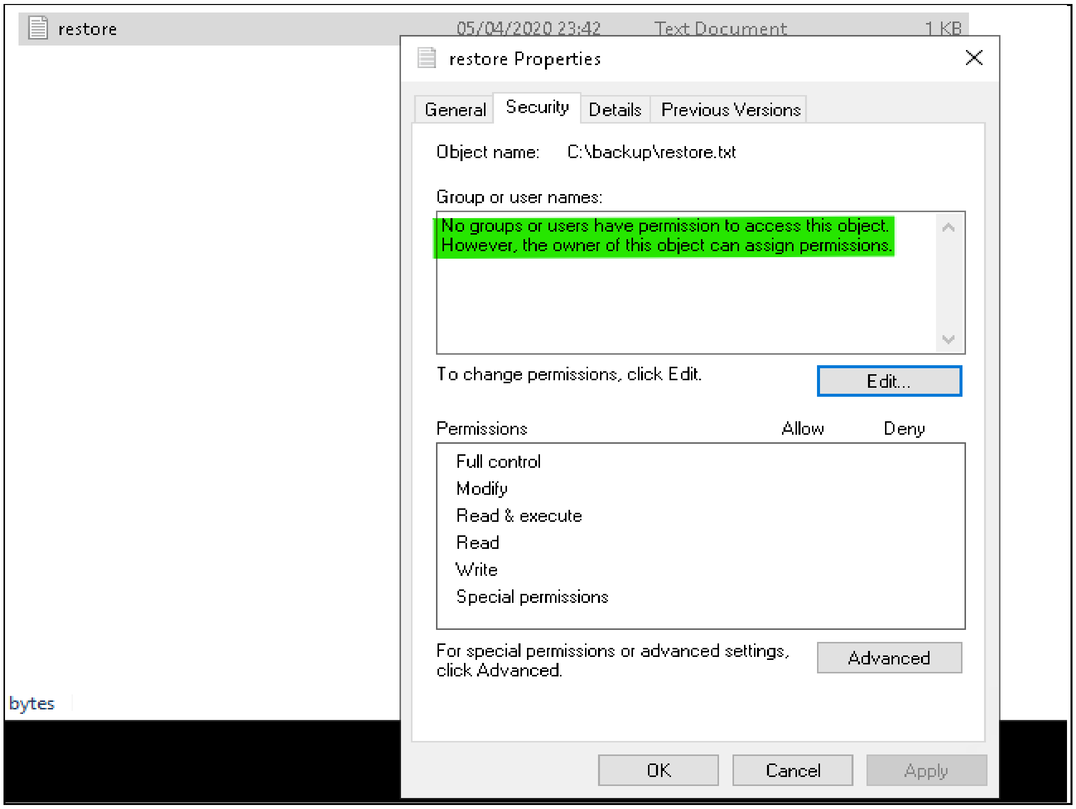
#4 Escalate your privileges to root, what is the contents of root.txt?

But when I have tried to open that, I cannot read the file. It shows I have not permission to open this file. Let's check on properties of this file, maybe we can do some thing with this permission issue.



C:\backup\restore.txt
You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.

On file properties it shows that “user have no permission to open this file”. But here is edit option, lets try if we can malipulate our permission.



Object name: C:\backup\restore.txt

Group or user names:

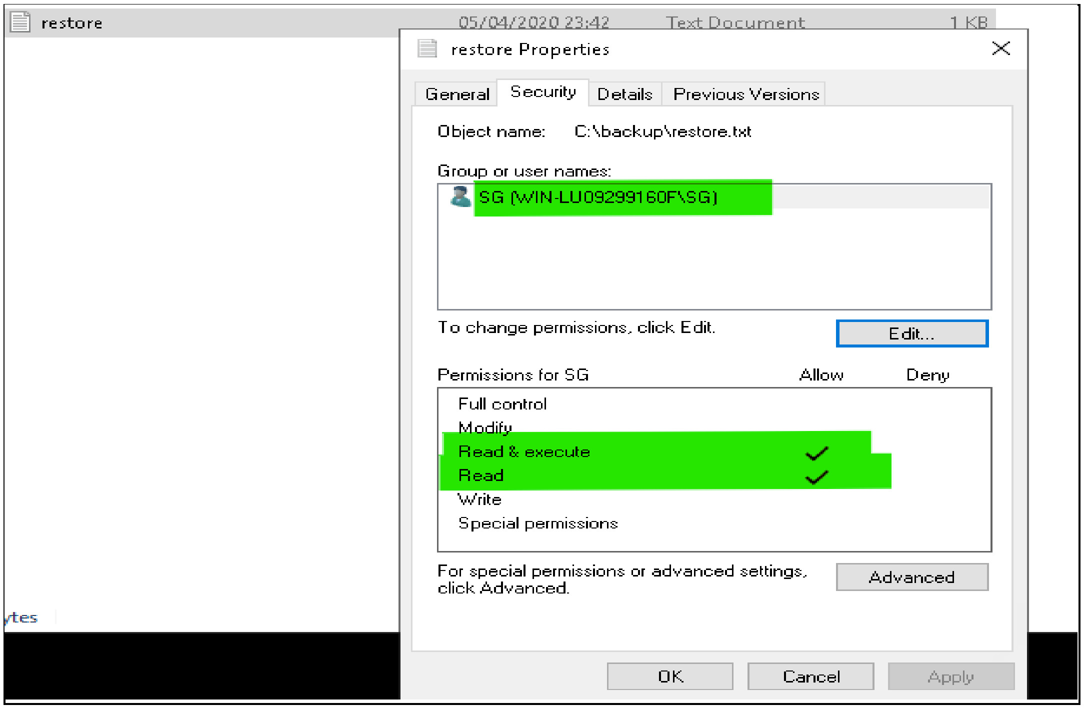
No groups or users have permission to access this object. However, the owner of this object can assign permissions.

To change permissions, click Edit.

Permissions	Allow	Deny
Full control		
Modify		
Read & execute		
Read		
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

Yes, we have done this, successfully add the permission to read, write and execute. Now let’s try to open again that “restore.txt” file



Object name: C:\backup\restore.txt

Group or user names:

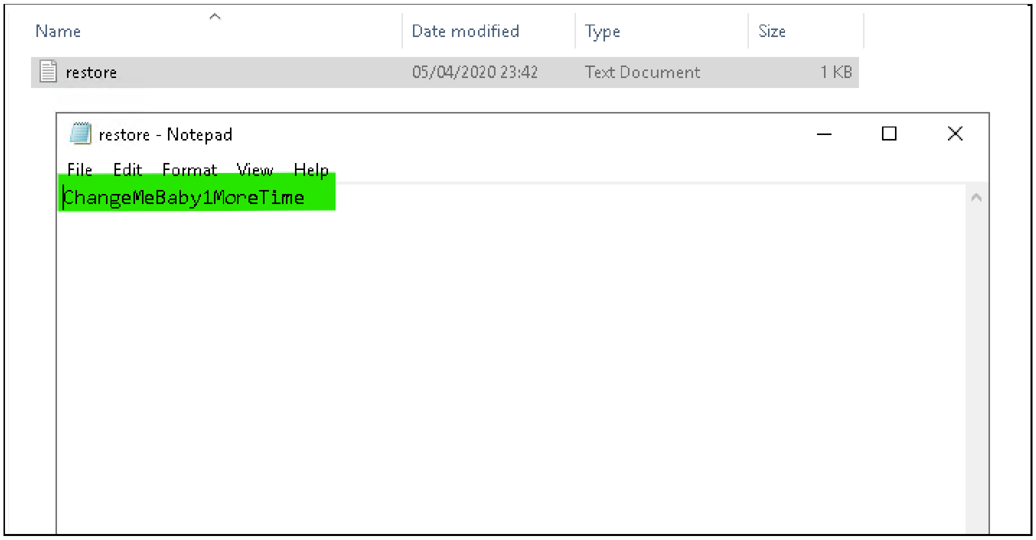
SG (WIN-LU09299160F\SG)

To change permissions, click Edit.

Permissions for SG	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

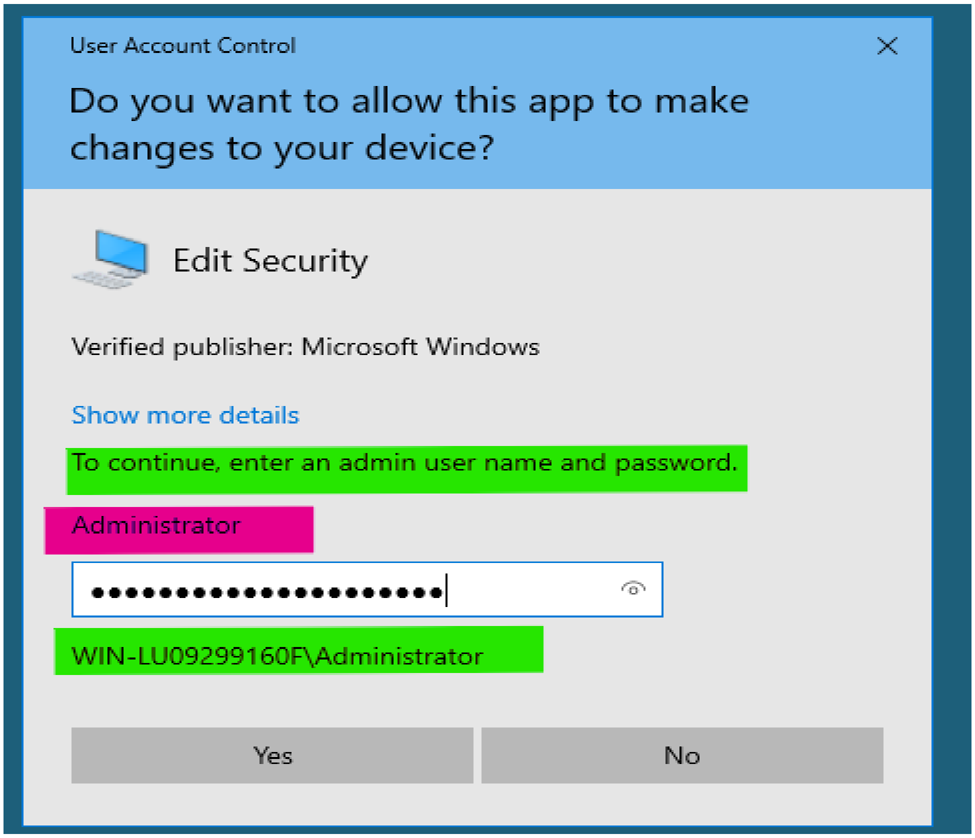
Yeah, this time, Got Access. Here is the password of administrator.



Name	Date modified	Type	Size
restore	05/04/2020 23:42	Text Document	1 KB

restore - Notepad

```
ChangeMeBaby1MoreTime
```



User Account Control

Do you want to allow this app to make changes to your device?

Edit Security

Verified publisher: Microsoft Windows

Show more details

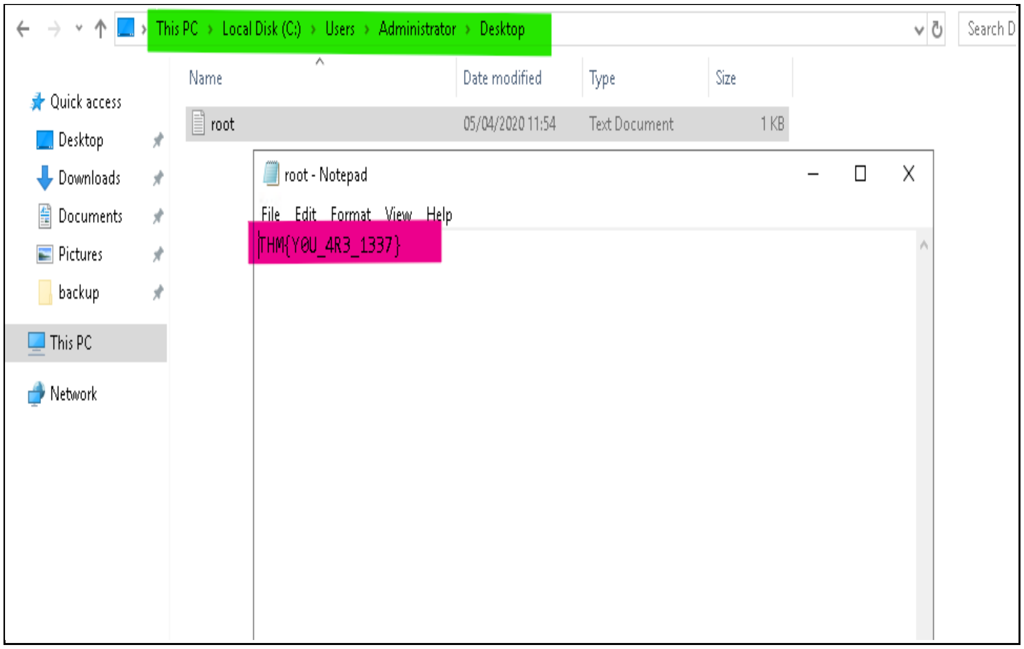
To continue, enter an admin user name and password.

Administrator

•••••••••••••••••••••

WIN-LU09299160F\Administrator

After successfully login to the administrator account, I have got my final flag inside the “root.txt”.



Name	Date modified	Type	Size
root	05/04/2020 11:54	Text Document	1 KB

```
THM{Y0U_4R3_1337}
```

Conclusion:

This room is good for understanding about windows machine in beginning level. When we do a Nmap scan we discover port 80 is open and it's running Umbraco CMS (content management system) on investigating bit deeper we have found the "organization" running the server creates username is by using the given name and surname initials and there is a hint on getting a user's password. After finding the credentials we log into the box using RDP (Remote Desktop Protocol) and that we found files that are recently modified and that we find a file that provides us the Administrator's credentials. Thanks for reading. Happy Hacking...!!