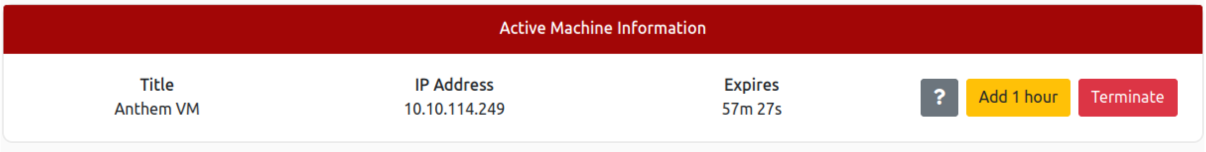
Anthem

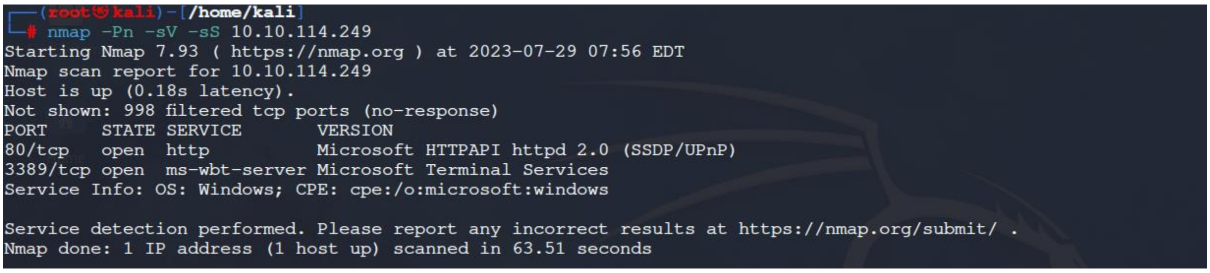


Active Machine Information

Title	IP Address	Expires
Anthem VM	10.10.114.249	57m 27s

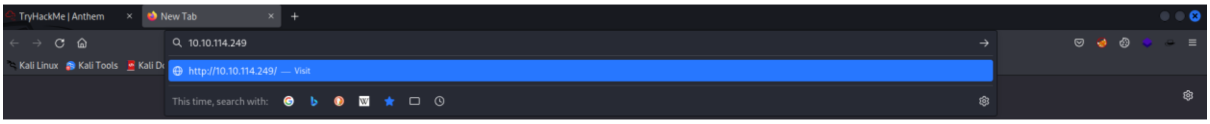
At first we will do nmap scan to get information about ports.

```
nmap -Pn -sV -sS 10.10.114.249
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sV -sS 10.10.114.249
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-29 07:56 EDT
Nmap scan report for 10.10.114.249
Host is up (0.18s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
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 63.51 seconds
```

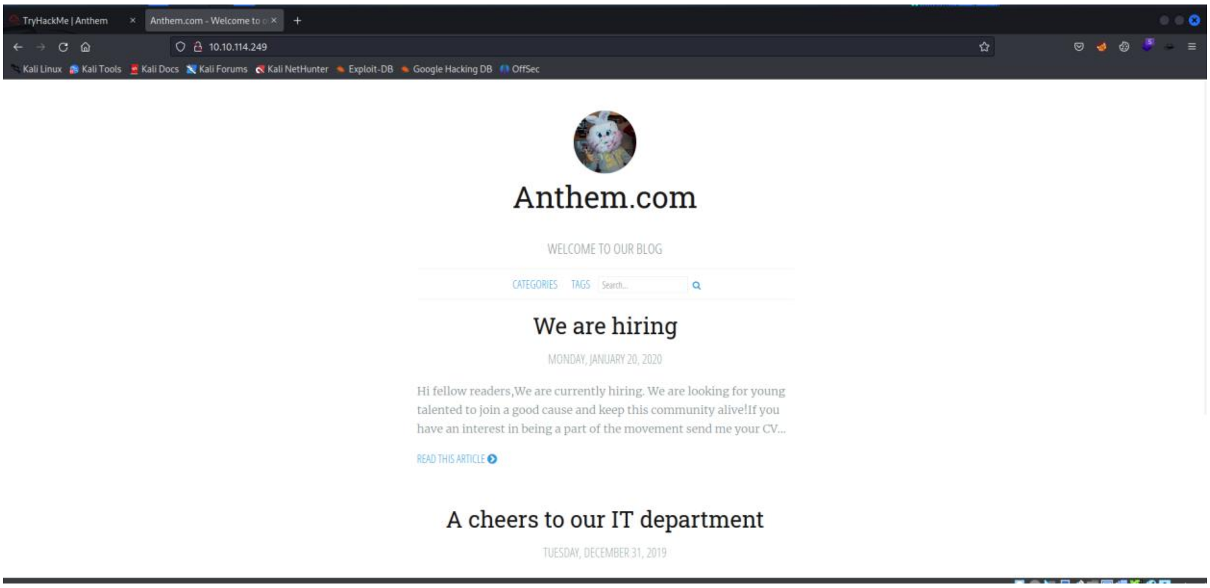
Here we can see 2 ports are open, **port 80** and **port 3389**. As port 80 is open there must be a website.



10.10.114.249

http://10.10.114.249/ — Visit

We found the website. Now we will try to find out what we get from this.



10.10.114.249

Anthem.com

WELCOME TO OUR BLOG

We are hiring

MONDAY, JANUARY 20, 2020

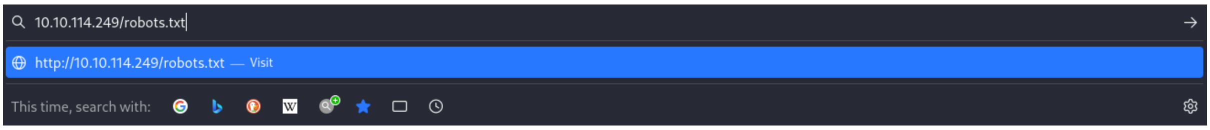
Hi fellow readers,We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!If you have an interest in being a part of the movement send me your CV...

READ THIS ARTICLE

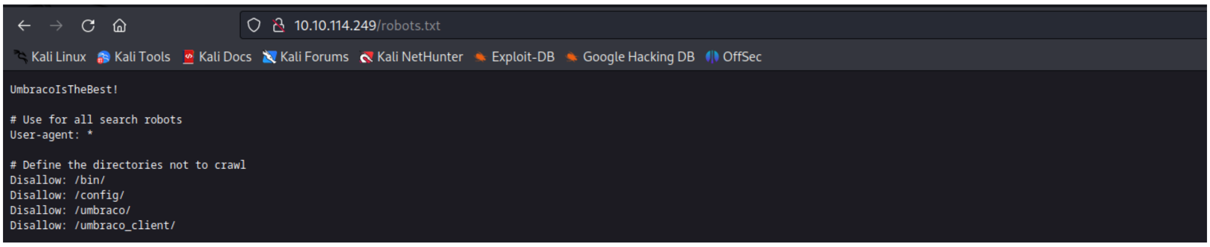
A cheers to our IT department

TUESDAY, DECEMBER 31, 2019

At first we will search for the **robots.txt** file, if that is available or not.

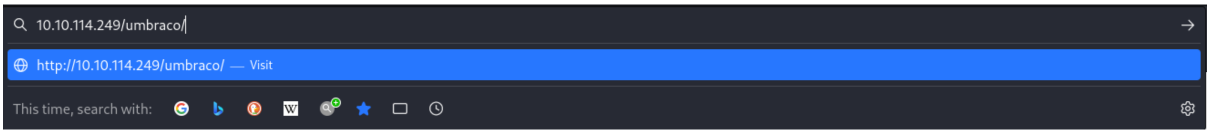


Looks like we found a text which looks like a possible password for something and we also got some directories which are disallow.

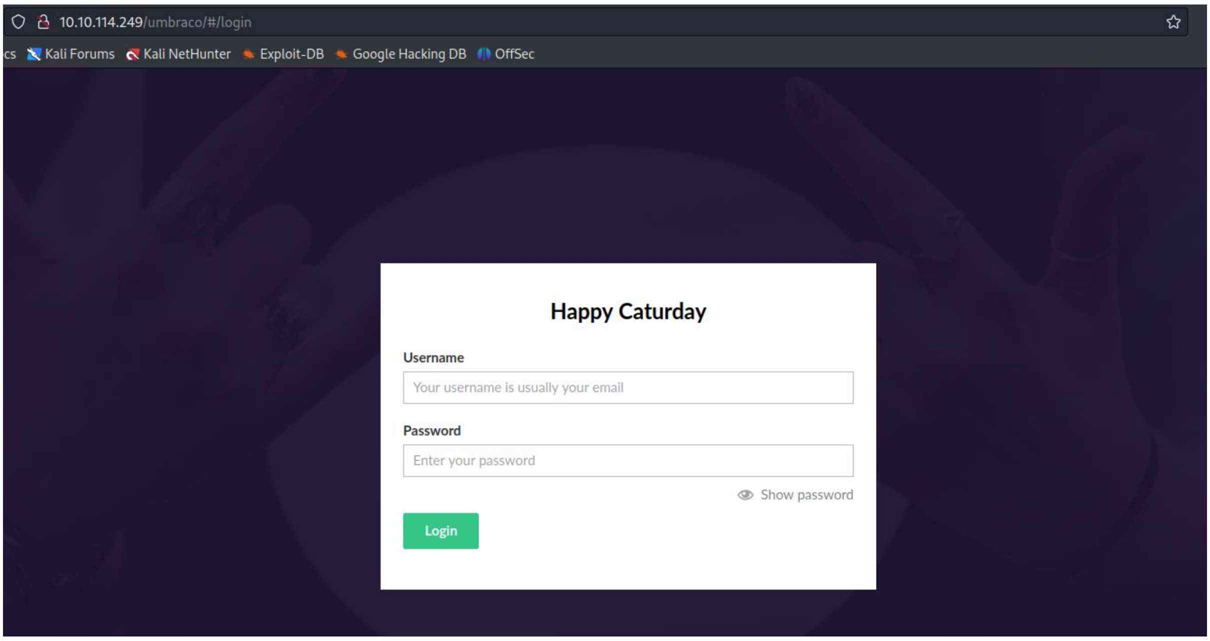


```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

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

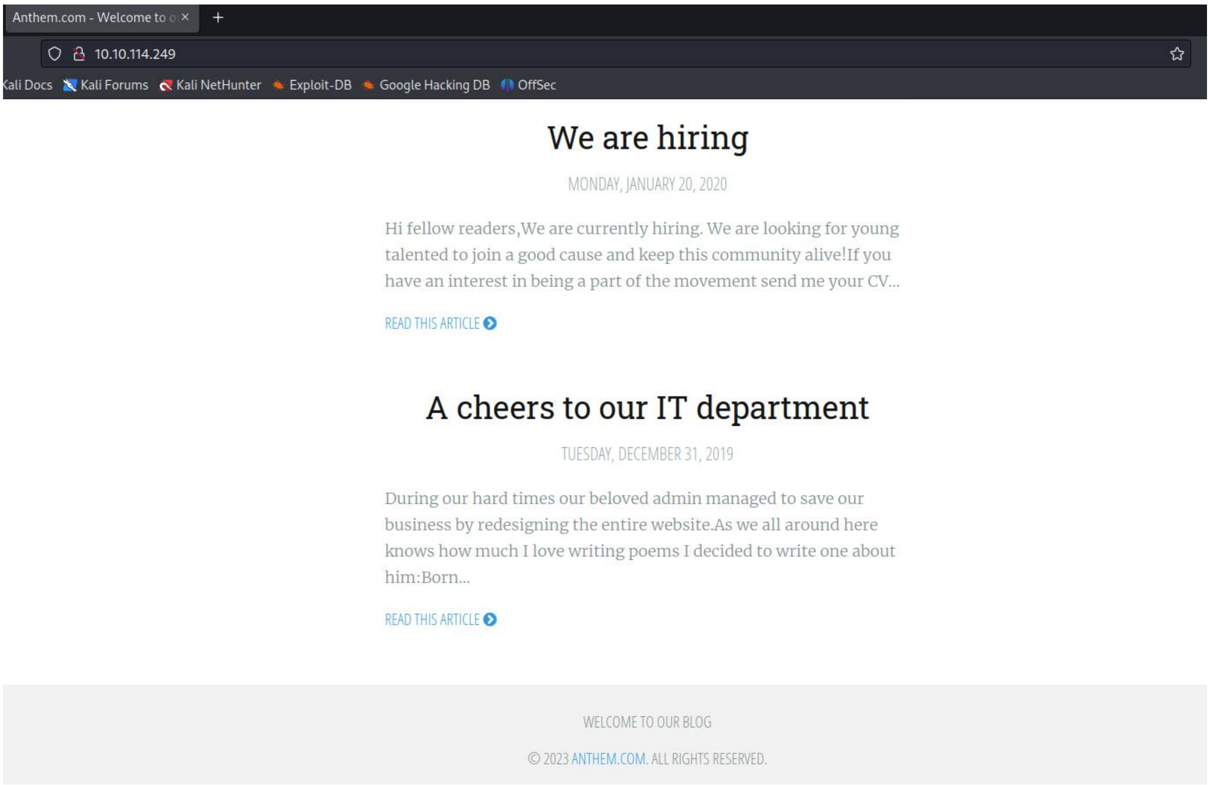
Let’s try to go to /umbraco/ one.



Here we found out a login page. But we don’t have any credentials to log in. Let’s try to find the potential user.



Let’s go back to the anthem.com. here we can see there is 2 blog post in this website.



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...

READ THIS ARTICLE

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...

READ THIS ARTICLE

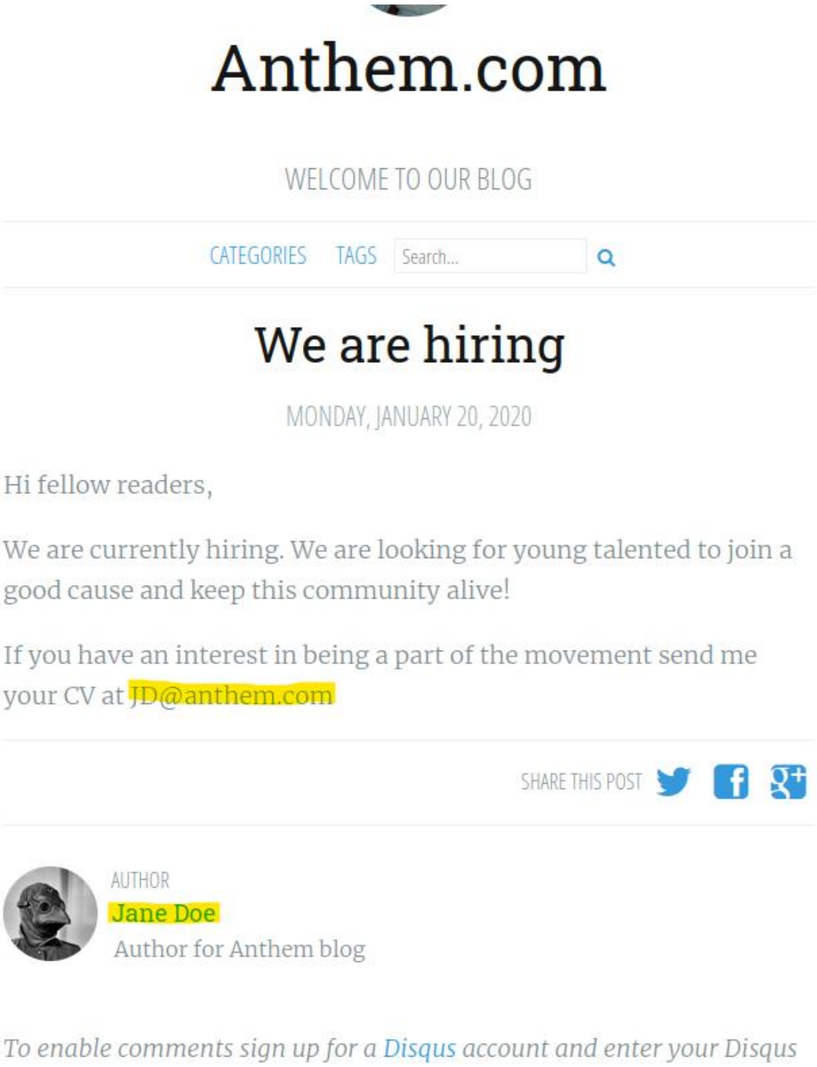
WELCOME TO OUR BLOG

© 2023 ANTHEM.COM. ALL RIGHTS RESERVED.

Now if we open the 1st blog post we can see there is an email id and author name of the anthem blog.

`Email id – JD@anthem.com`

`Name – Jane Doe`



Anthem.com

WELCOME TO OUR BLOG

We are hiring

MONDAY, JANUARY 20, 2020

Hi fellow readers,

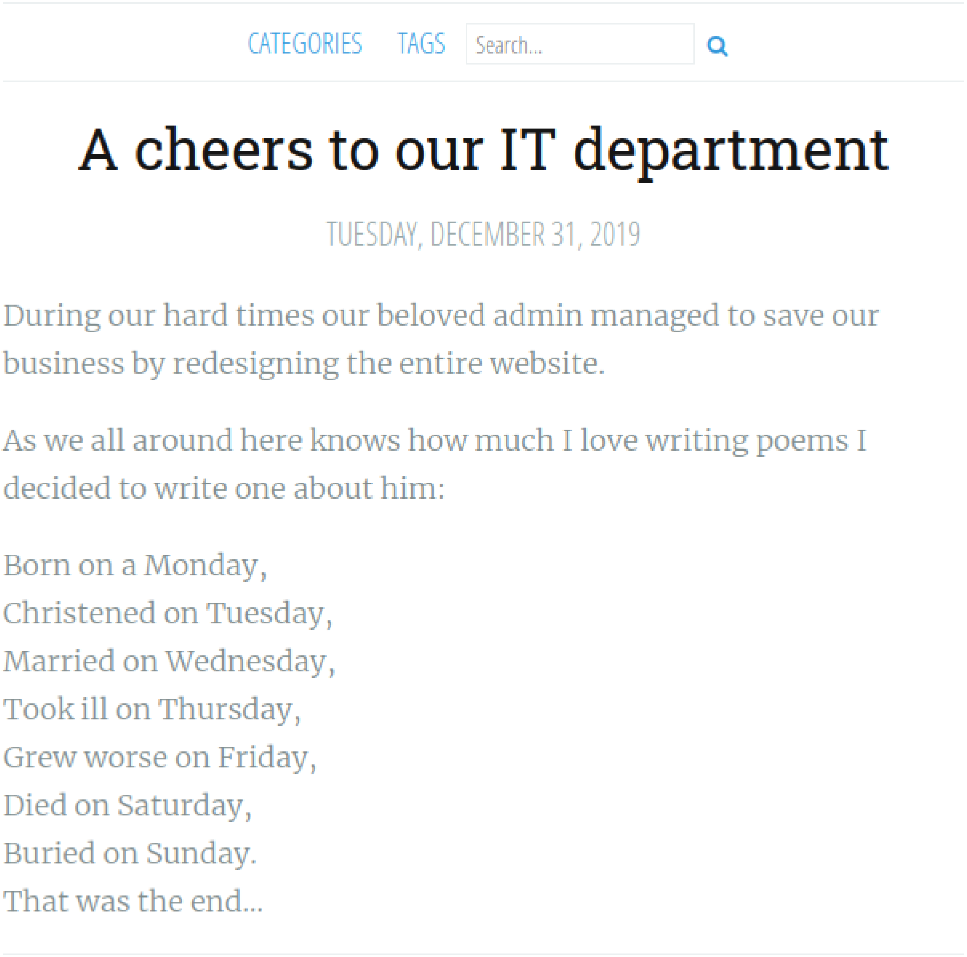
We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!

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

AUTHOR
Jane Doe
Author for Anthem blog

To enable comments sign up for a Disqus account and enter your Disqus

Now if we open the 2nd blog post we can see a rhyme posted in here.



A cheers to our IT department

TUESDAY, DECEMBER 31, 2019

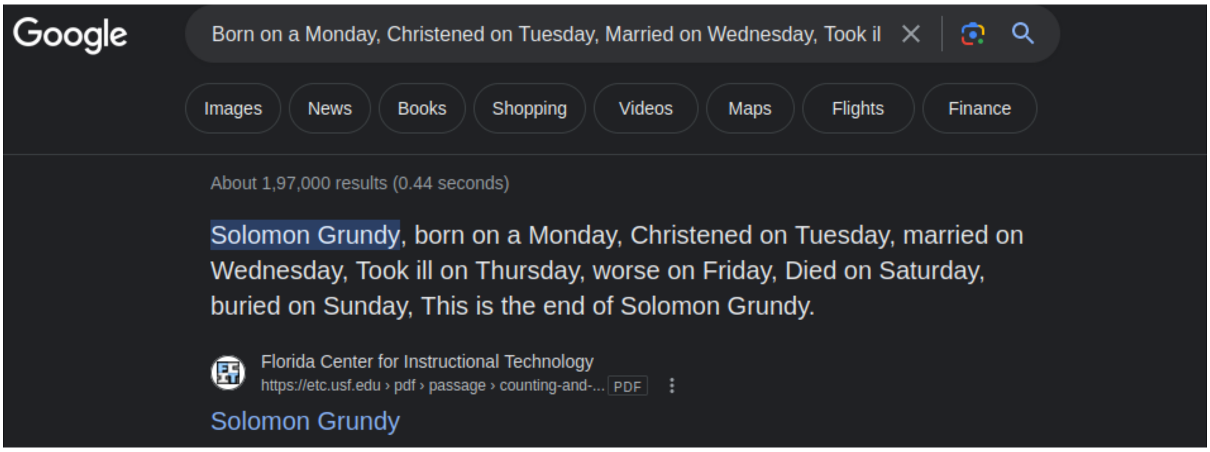
During our hard times our beloved admin managed to save our business by redesigning the entire website.

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...

Now if we search the poem in ant search engine we can easily find out the name of the admin.

```
Admin name – Solomon Grundy
```



Google
Born on a Monday, Christened on Tuesday, Married on Wednesday, Took il
Images
News
Books
Shopping
Videos
Maps
Flights
Finance

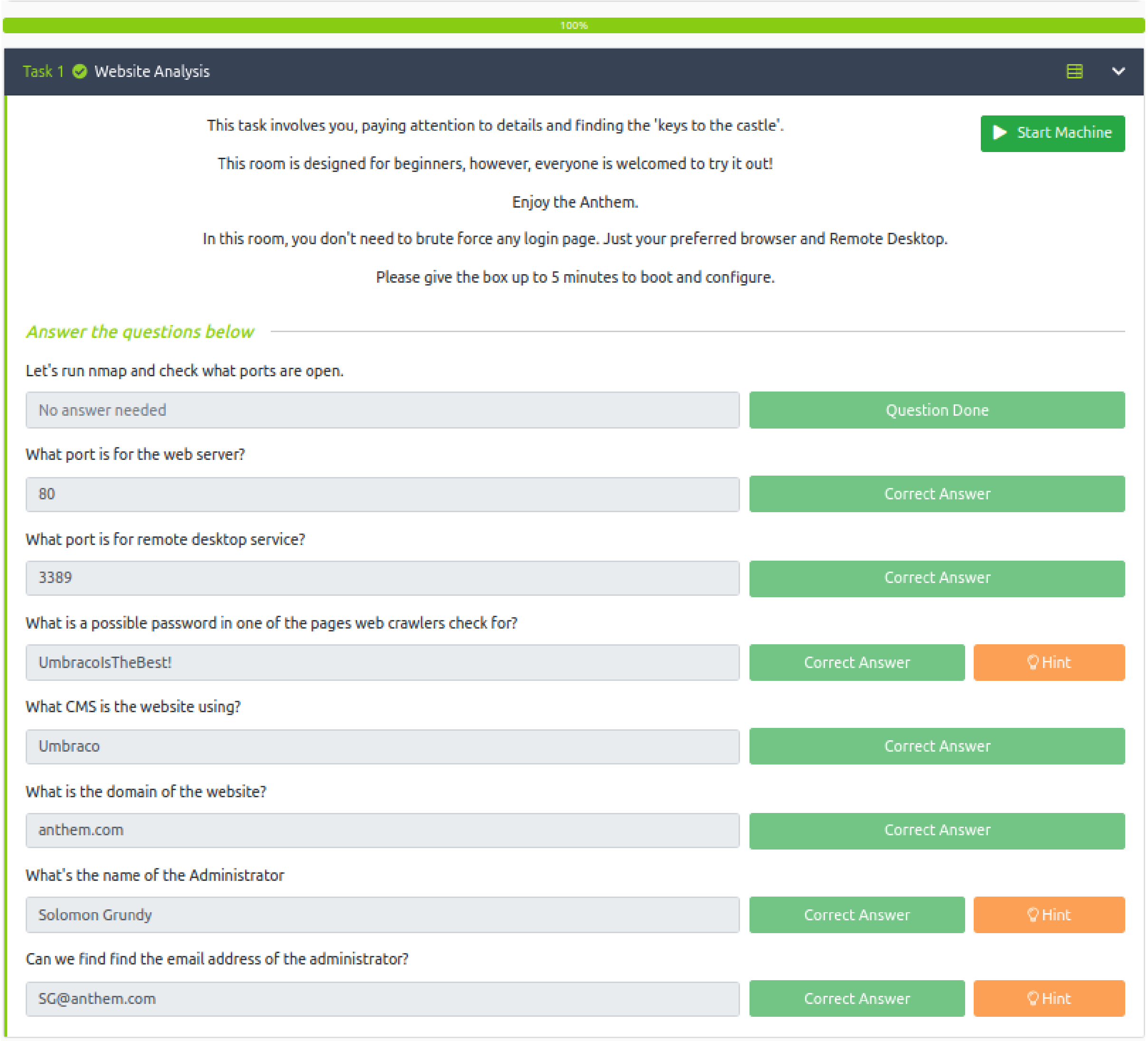
About 1,97,000 results (0.44 seconds)

Solomon Grundy, born on a Monday, Christened on Tuesday, married on Wednesday, Took ill on Thursday, worse on Friday, Died on Saturday, buried on Sunday, This is the end of Solomon Grundy.

Florida Center for Instructional Technology
https://etc.usf.edu › pdf › passage › counting-and-... PDF

Solomon Grundy

But the login page demands for email of the user. So let's find the email address of the admin. If we follow the pattern of the email that we got from the 1st blog post then the email id of the admin will be ***`sg@anthem.com`***.



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.

Please give the box up to 5 minutes to boot and configure.

Answer the questions below

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?

UmbracoIsTheBest! — 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

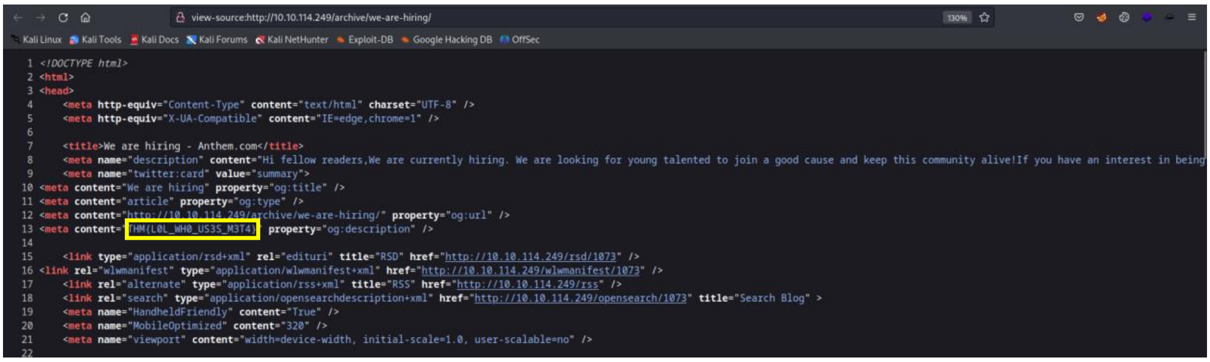
Can we find find the email address of the administrator?

SG@anthem.com — Correct Answer — Hint

Now we will try to find out the flags.

now if we will go to the page source of the 1st blog post. Here we will get our 1st flag.

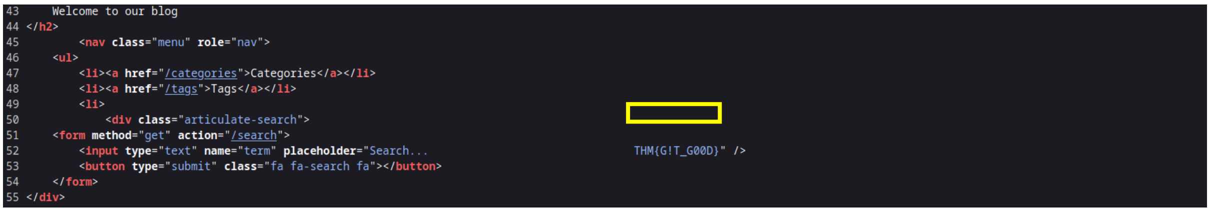
1st flag -THM{L0L_WH0_US3S_M3T4}



```
<!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>We are hiring - Anthem.com</title>
    <meta name="description" content="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
    <meta name="twitter:card" value="summary">
<meta content="We are hiring" property="og:title" />
<meta content="article" property="og:type" />
<meta content="http://10.10.114.249/archive/we-are-hiring/" property="og:url" />
<meta content="THM{L0L_WH0_US3S_M3T4}" property="og:description" />

    <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.114.249/rsd/1073" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.114.249/wlwmanifest/1073" />
    <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.114.249/rss" />
    <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.114.249/opensearch/1073" title="Search Blog" >
    <meta name="HandheldFriendly" content="True" />
    <meta name="MobileOptimized" content="320" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no" />
```

Now if we scroll down the source code we will get the 2nd flag.

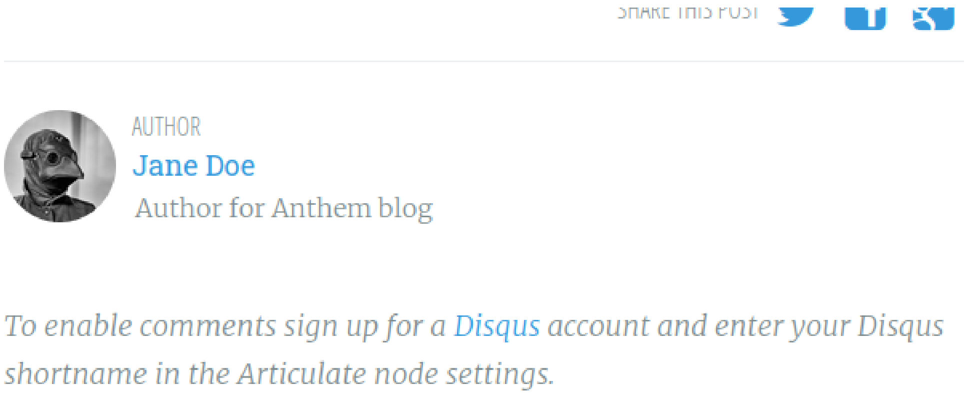
2nd flag – THM{G!T_G00D}



```
    Welcome to our blog
</h2>
        <nav class="menu" role="nav">
    <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>
```

Now in the 1st blog post if we go to the profile of the author we will get another flag there.

3rd flag – THM{L0L_WH0_D15}



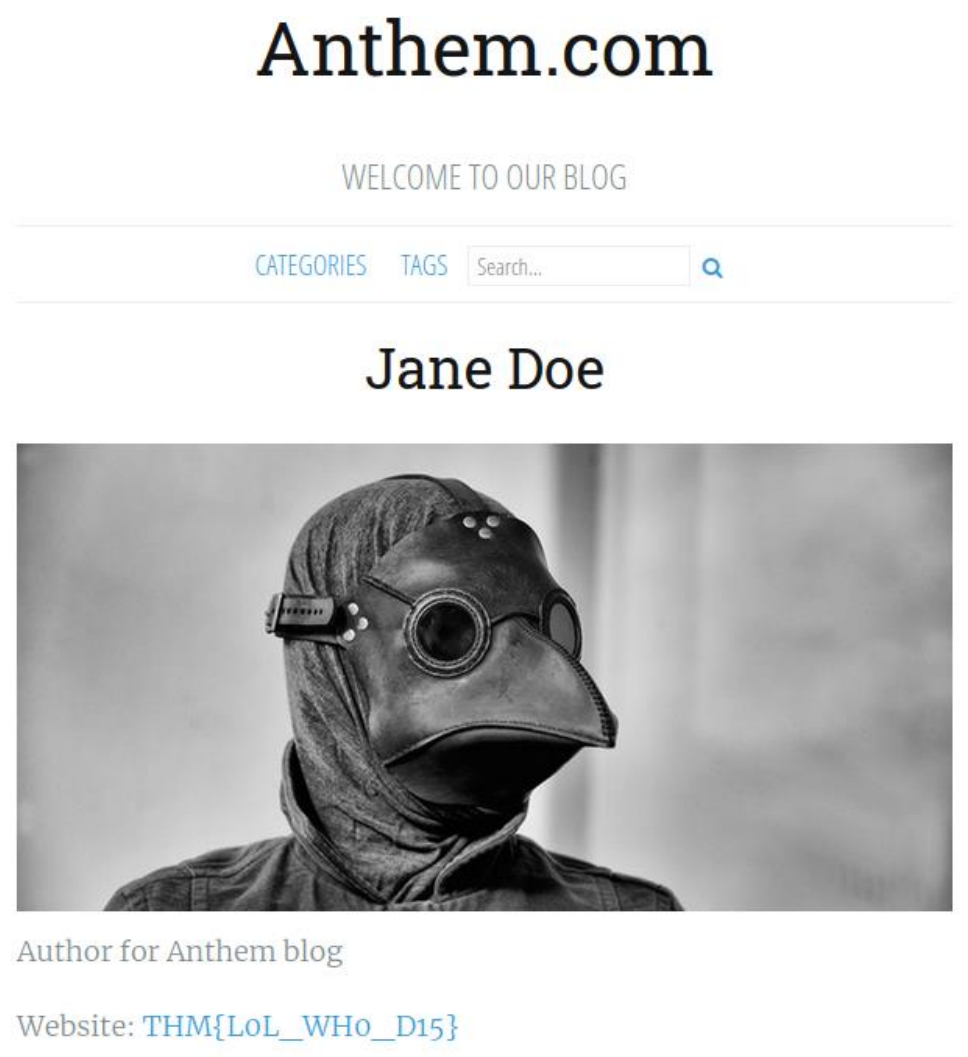
SHARE THIS POST

AUTHOR

Jane Doe

Author for Anthem blog

To enable comments sign up for a Disqus account and enter your Disqus shortname in the Articulate node settings.



Anthem.com

WELCOME TO OUR BLOG

CATEGORIES TAGS Search...

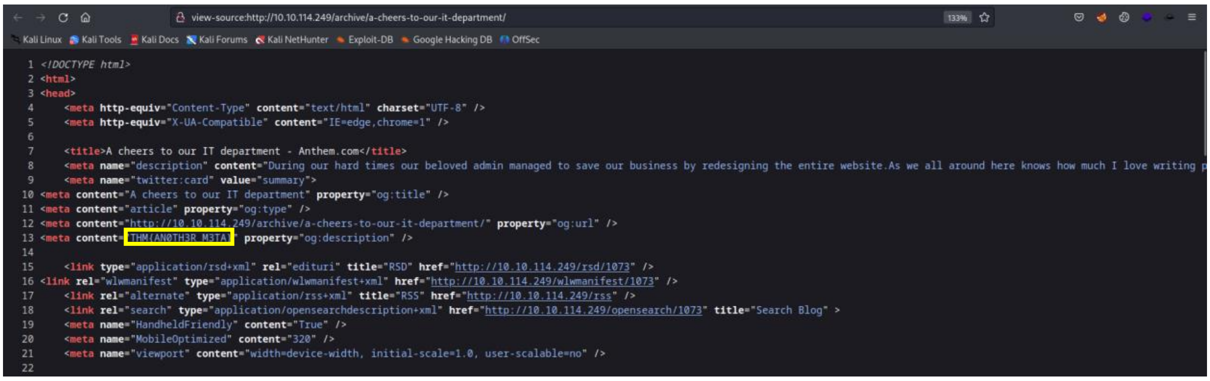
Jane Doe

Author for Anthem blog

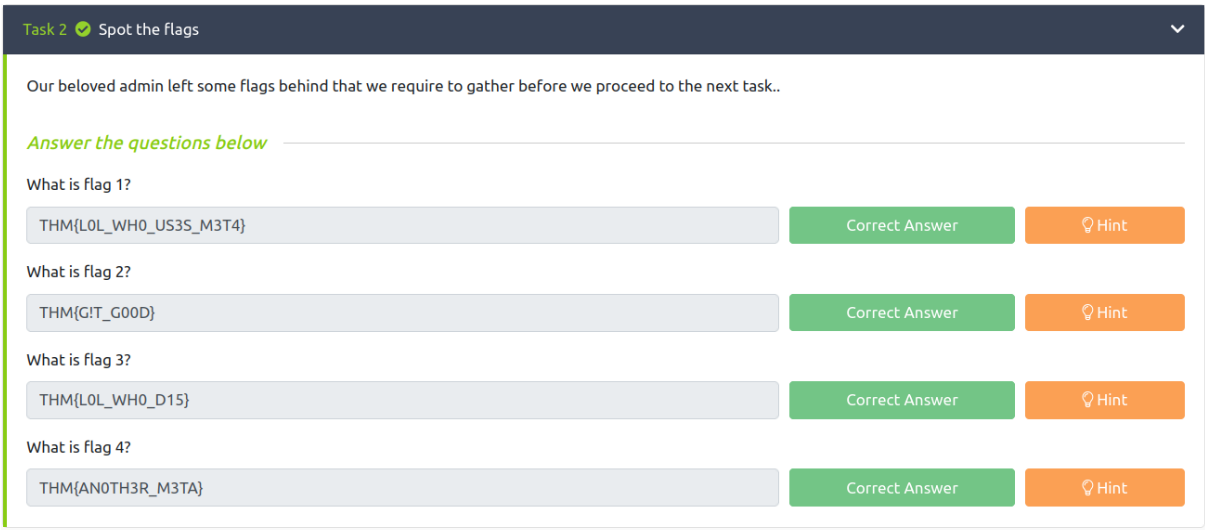
Website: THM{LoL_WHo_D15}

Now if we go to the page source of 2nd blog post we will get our 4th flag.

4th flag - THM{AN0TH3R_M3TA}



```
<!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 business by redesigning the entire website.As we all around here knows how much I love writing p
    <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://10.10.114.249/archive/a-cheers-to-our-it-department/" property="og:url" />
<meta content="THM{AN0TH3R_M3TA}" property="og:description" />

    <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.114.249/rsd/1073" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.114.249/wlwmanifest/1073" />
    <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.114.249/rss" />
    <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.114.249/opensearch/1073" title="Search Blog" >
    <meta name="HandheldFriendly" content="True" />
    <meta name="MobileOptimized" content="320" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no" />

```



Task 2 Spot the flags

Our beloved admin left some flags behind that we require to gather before we proceed to the next task..

Answer the questions below

What is flag 1?

THM{L0L_WH0_US3S_M3T4} | Correct Answer | Hint

What is flag 2?

THM{G!T_G00D} | Correct Answer | Hint

What is flag 3?

THM{L0L_WH0_D15} | Correct Answer | Hint

What is flag 4?

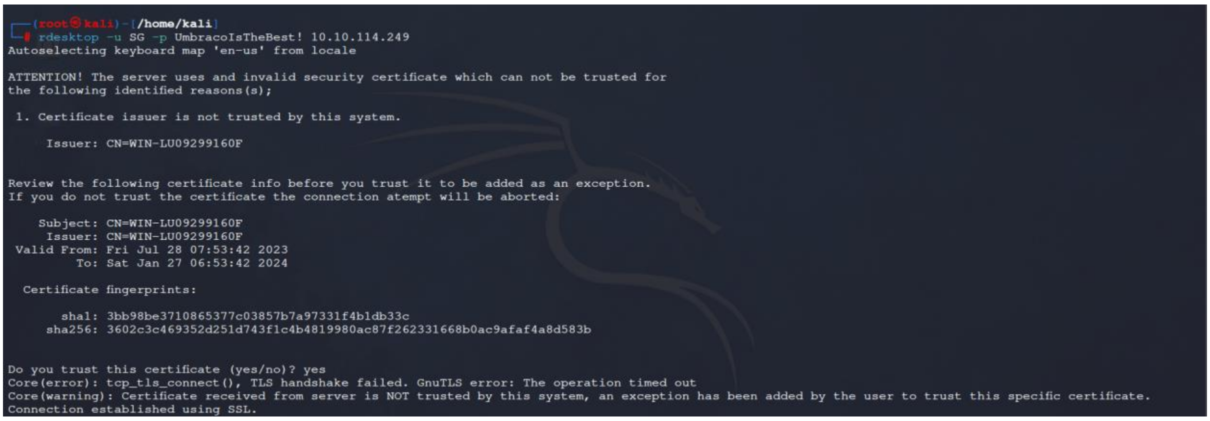
THM{AN0TH3R_M3TA} | Correct Answer | Hint

As we already know that we have a remote desktop port 3389 open, we use the already found credentials to log in.

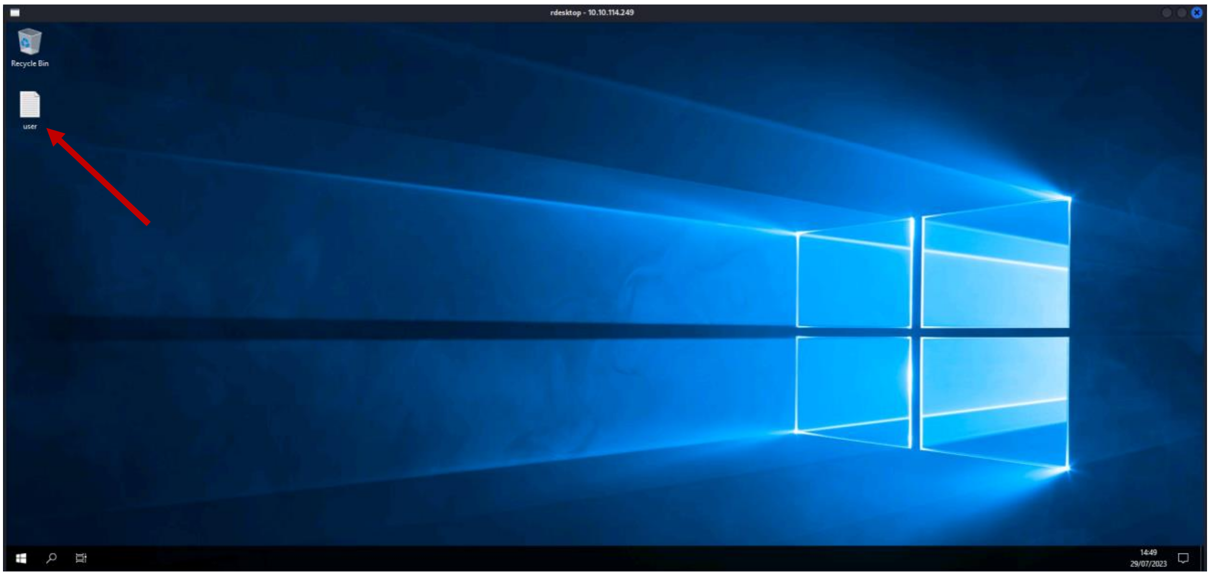
Username — SG

Password — UmbracoIsTheBest!

```
rdesktop -u SG -p UmbracoIsTheBest! 10.10.114.249
```

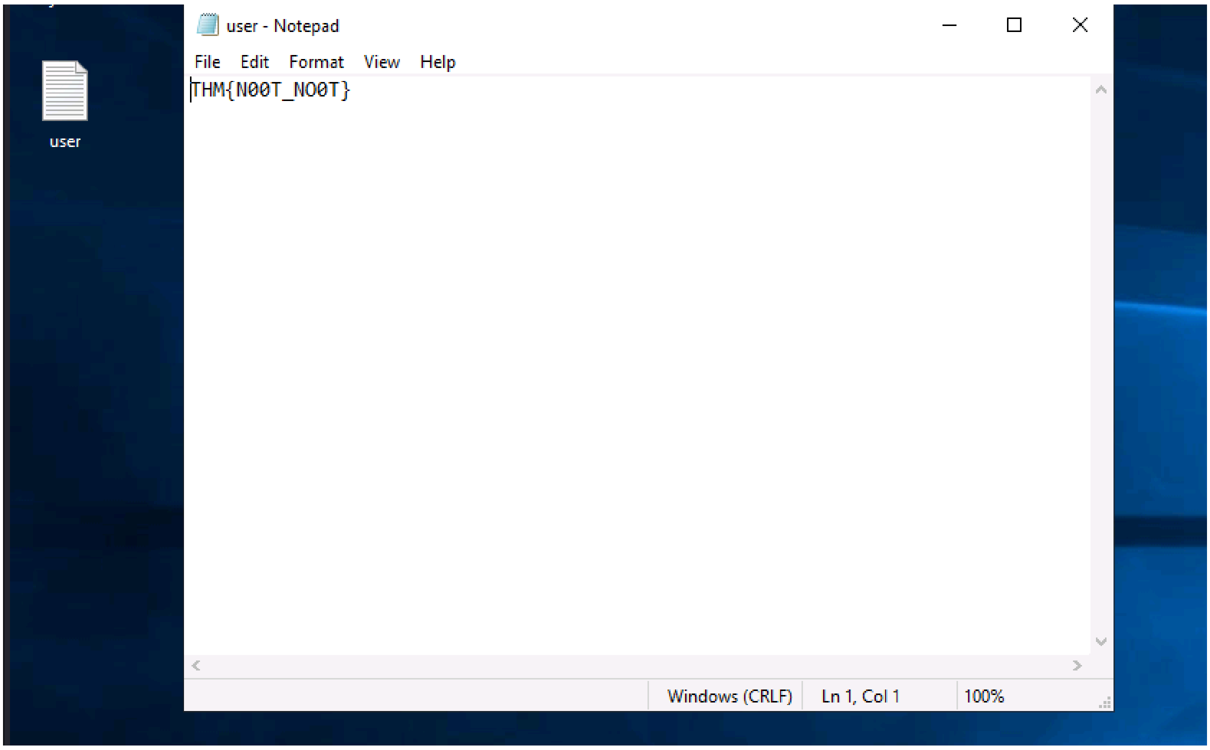


```
┌──(root㉿kali)-[/home/kali]
└─# rdesktop -u SG -p UmbracoIsTheBest! 10.10.114.249
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=WIN-LU09299160F


Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=WIN-LU09299160F
     Issuer: CN=WIN-LU09299160F
 Valid From: Fri Jul 28 07:53:42 2023
         To: Sat Jan 27 06:53:42 2024

  Certificate fingerprints:

       sha1: 3bb98be3710865377c03857b7a97331f4b1db33c
     sha256: 3602c3c469352d251d743f1c4b4819980ac87f262331668b0ac9afaf4a8d583b


Do you trust this certificate (yes/no)? yes
Core(error): tcp_tls_connect(), TLS handshake failed. GnuTLS error: The operation timed out
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
```



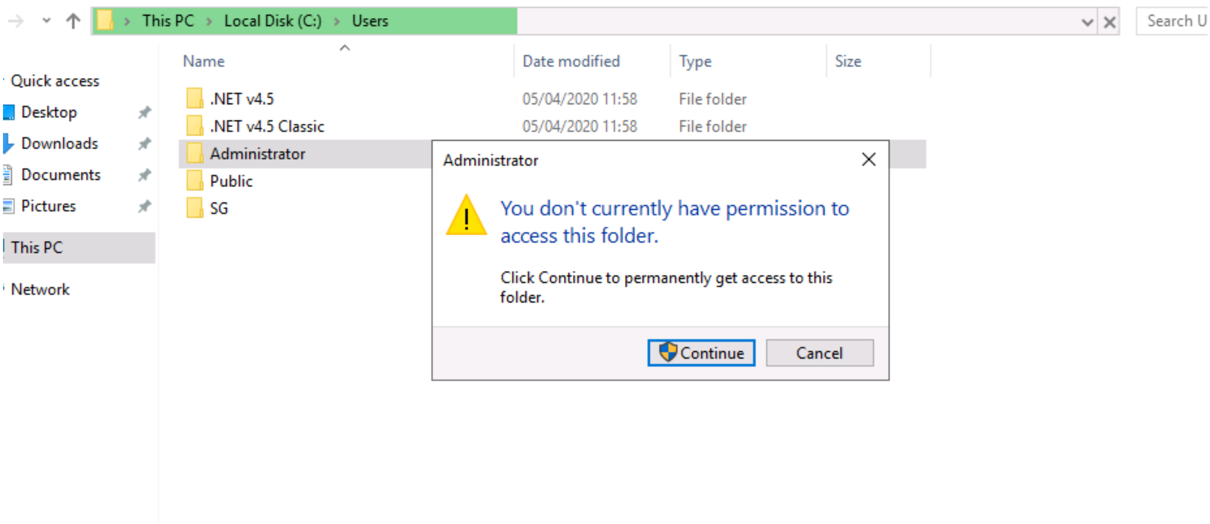
Now we can see that there is a user file on the desktop. Now we will open the user file.

`Content of user.txt - THM{N00T_NO0T}`



```
THM{N00T_NO0T}
```

Password is required to access the Administrator folder. There is a backup folder that has the password. Enable hidden items folder to view it.

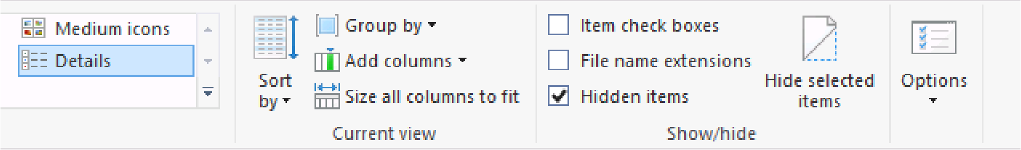


Name	Date modified	Type	Size
.NET v4.5	05/04/2020 11:58	File folder	
.NET v4.5 Classic	05/04/2020 11:58	File folder	
Administrator			
Public			
SG			

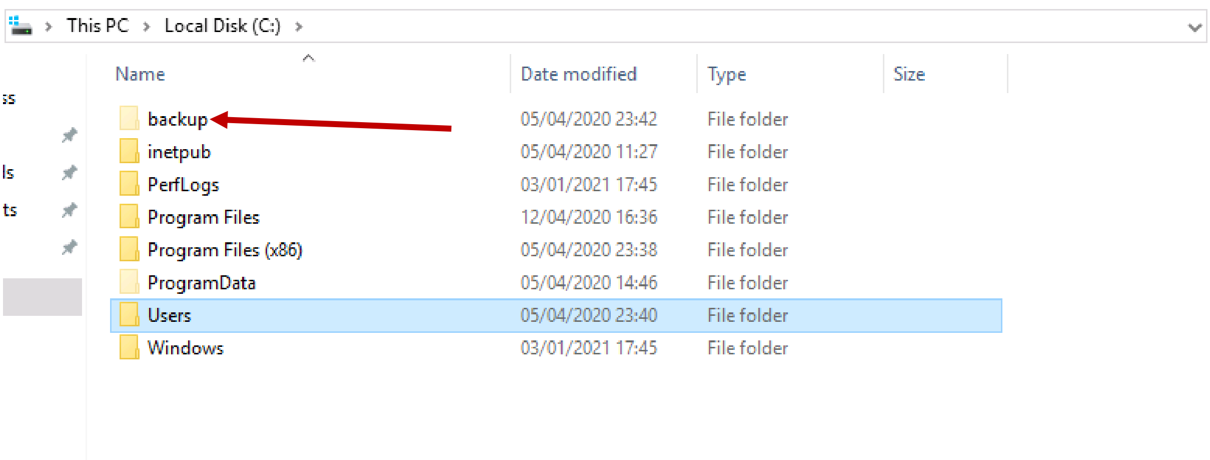
Administrator

You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.

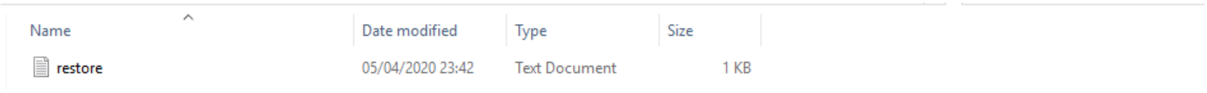


□ Item check boxes
□ File name extensions
☑ Hidden items

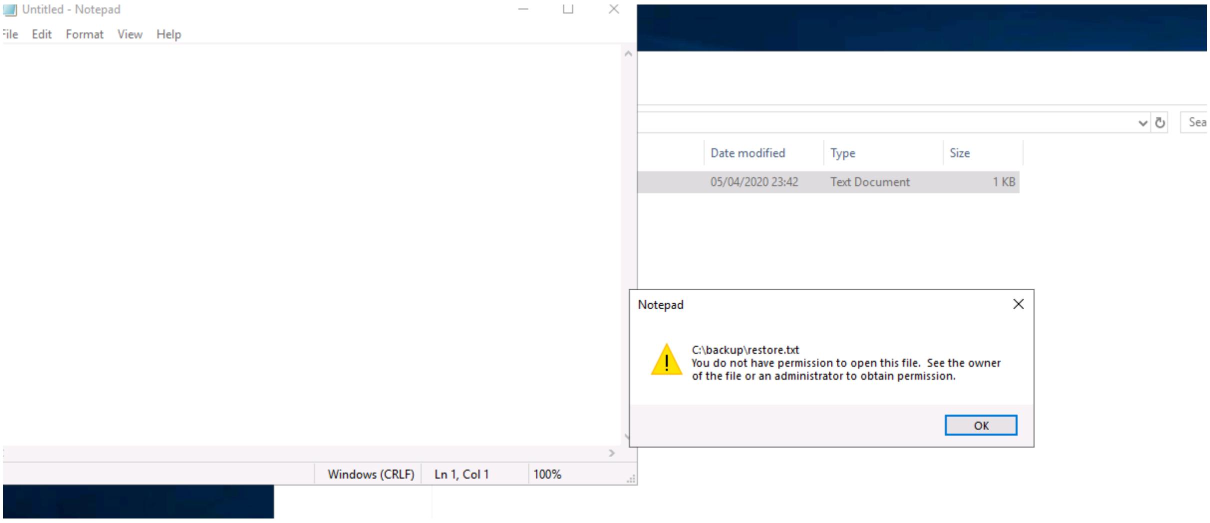


Name	Date modified	Type	Size
backup	05/04/2020 23:42	File folder	
inetpub	05/04/2020 11:27	File folder	
PerfLogs	03/01/2021 17:45	File folder	
Program Files	12/04/2020 16:36	File folder	
Program Files (x86)	05/04/2020 23:38	File folder	
ProgramData	05/04/2020 14:46	File folder	
Users	05/04/2020 23:40	File folder	
Windows	03/01/2021 17:45	File folder	

Inside the backup folder, we have a restore.txt file that we do not have permission to open. For that, we need to change permissions for this file.



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

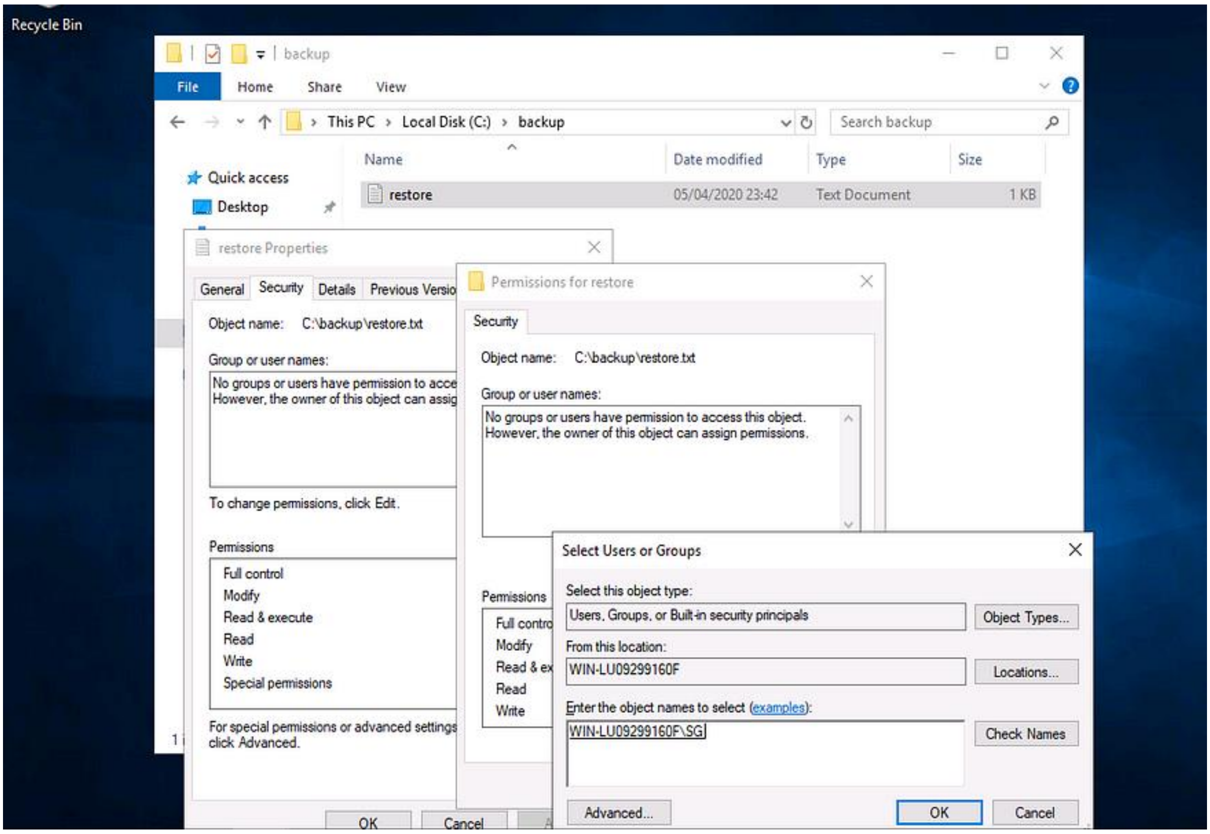


05/04/2020 23:42 Text Document 1 KB

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.

We will change the permission of the file through these following steps.

select restore.txt > Right click > properties > security > edit >add Group or Username > type WIN-LU09299160FSG **and click check names> ok>apply.**



restore 05/04/2020 23:42 Text Document 1 KB

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.

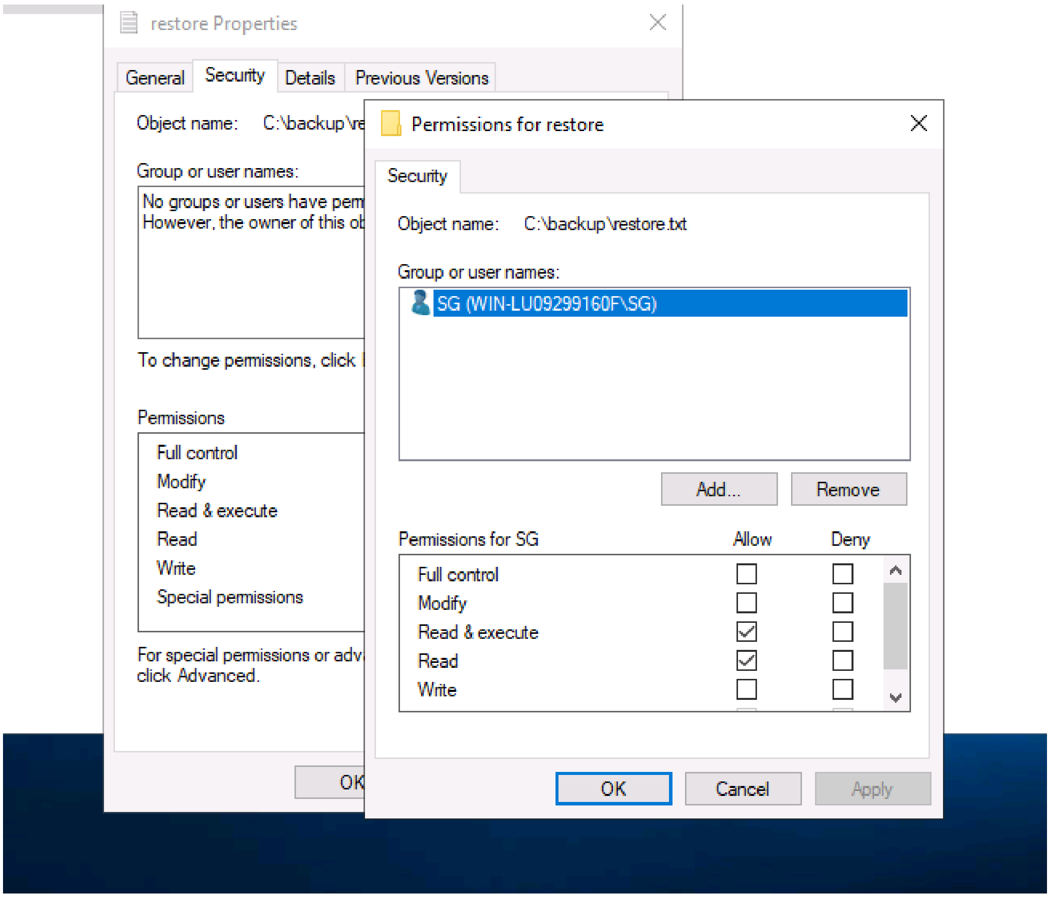
To change permissions, click Edit.

For special permissions or advanced settings, click Advanced.

Select this object type: Users, Groups, or Built-in security principals

From this location: WIN-LU09299160F

Enter the object names to select (examples): WIN-LU09299160F\SG



restore Properties

General | Security | Details | Previous Versions

Object name: C:\backup\re

Group or user names:

No groups or users have perm
However, the owner of this ob

To change permissions, click

Permissions

Full control
Modify
Read & execute
Read
Write
Special permissions

For special permissions or adv
click Advanced.

Permissions for restore

Security

Object name: C:\backup\restore.txt

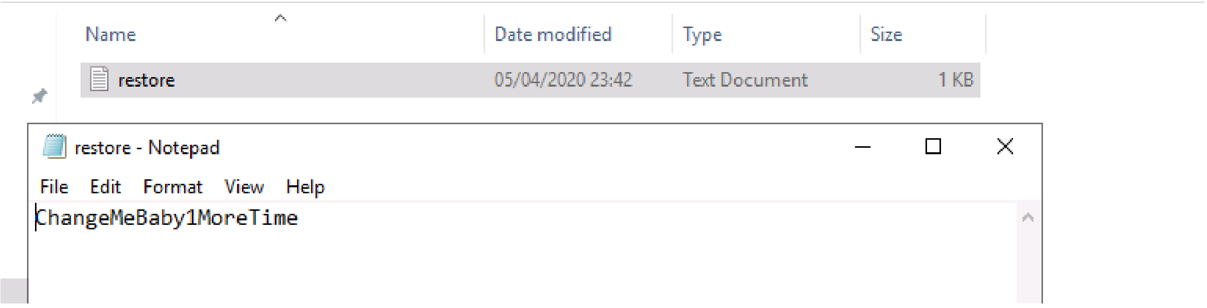
Group or user names:

SG (WIN-LU09299160F\SG)

Permissions for SG	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
Read	☑	□
Write	□	□

Now we can easily open the `restore.txt` file and see the admin password.

`Restore.txt - ChangeMeBaby1MoreTime`

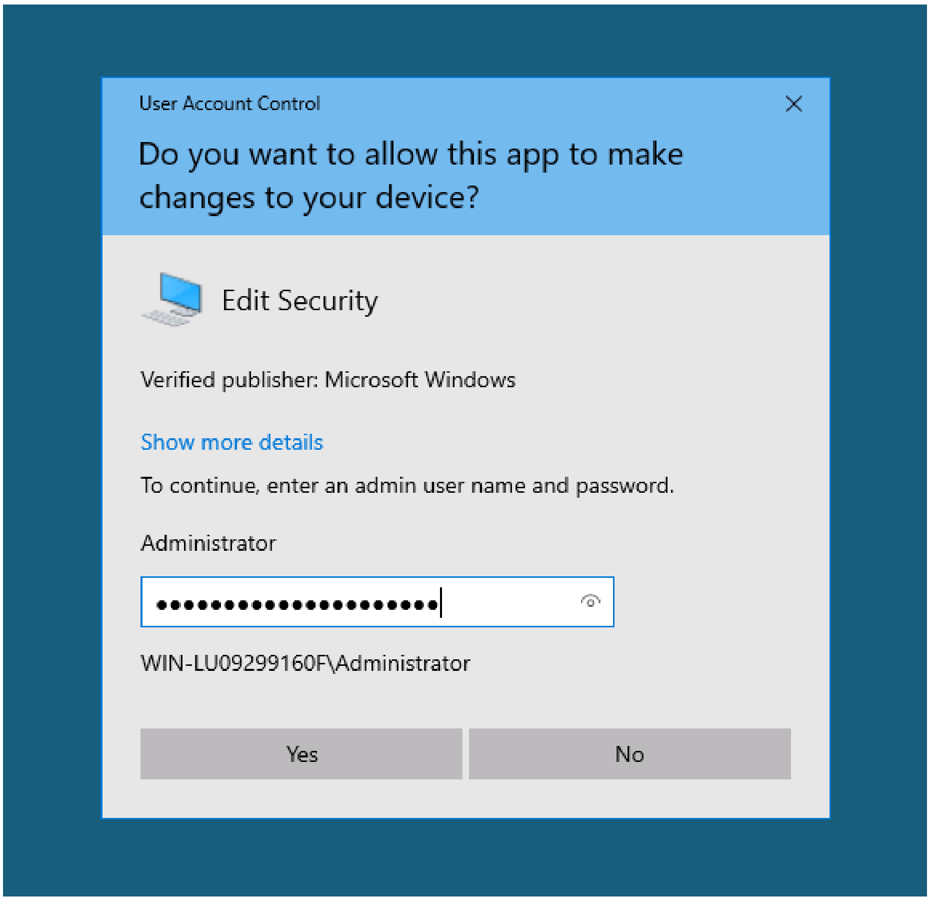


Name	Date modified	Type	Size
restore	05/04/2020 23:42	Text Document	1 KB

restore - Notepad

```
ChangeMeBaby1MoreTime
```

Using this we access the Administrator folder.



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

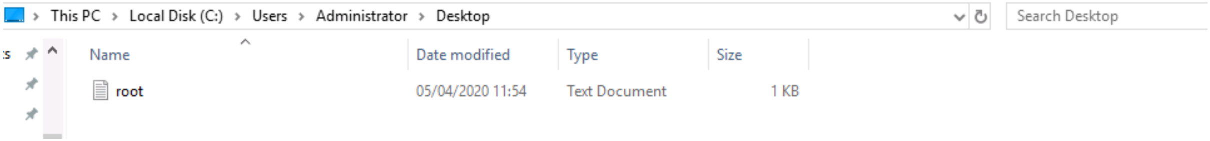
To continue, enter an admin user name and password.

Administrator

•••••••••••••••••••••

WIN-LU09299160F\Administrator

Under administrator folder in desktop there is a `root.txt` file.

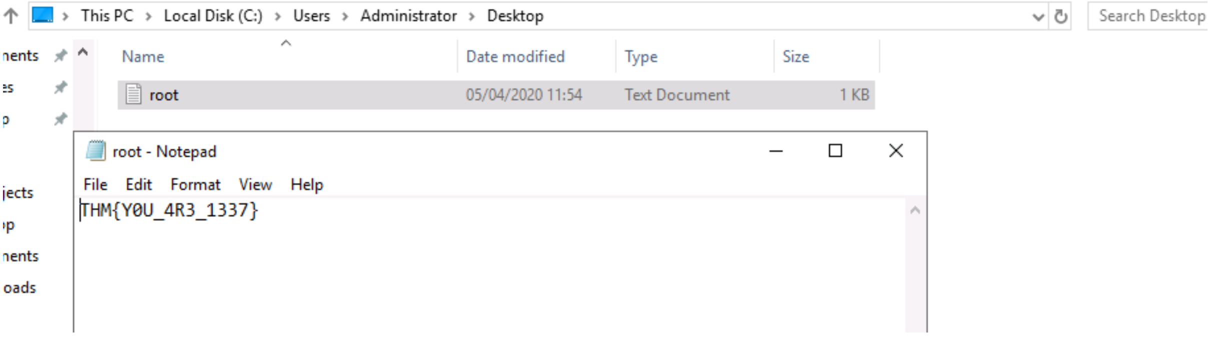


This PC › Local Disk (C:) › Users › Administrator › Desktop

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

Now if we open the root.txt file we will get the root flag.

```
Root.txt – THM{Y0U_4R3_1337}
```

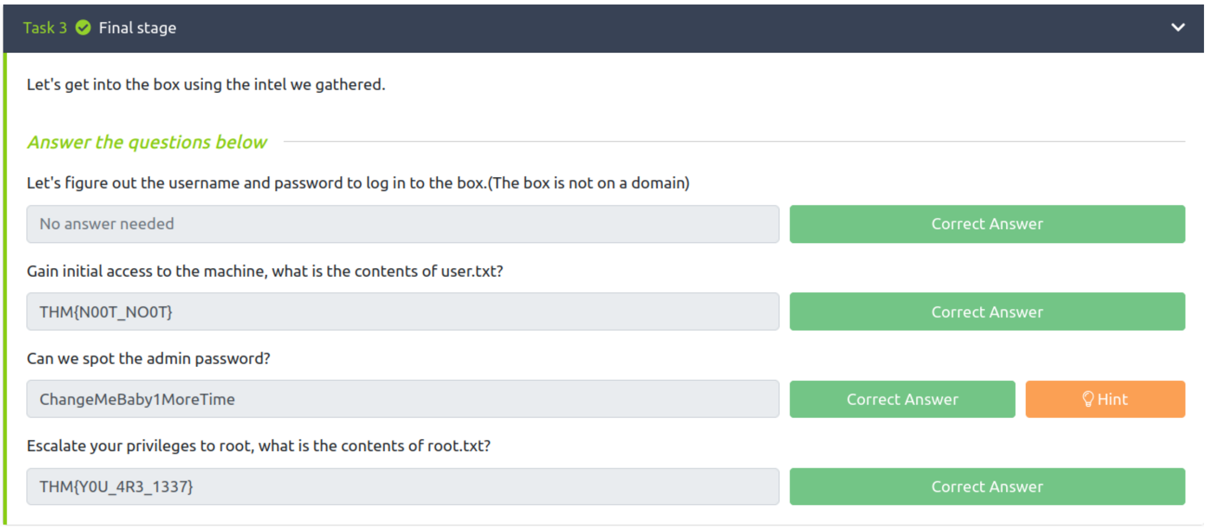


This PC › Local Disk (C:) › Users › Administrator › Desktop

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

root - Notepad

```
THM{Y0U_4R3_1337}
```



Task 3 Final stage

Let's get into the box using the intel we gathered.

Answer the questions below

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

No answer needed

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

THM{N00T_NO0T}

Can we spot the admin password?

ChangeMeBaby1MoreTime

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

THM{Y0U_4R3_1337}