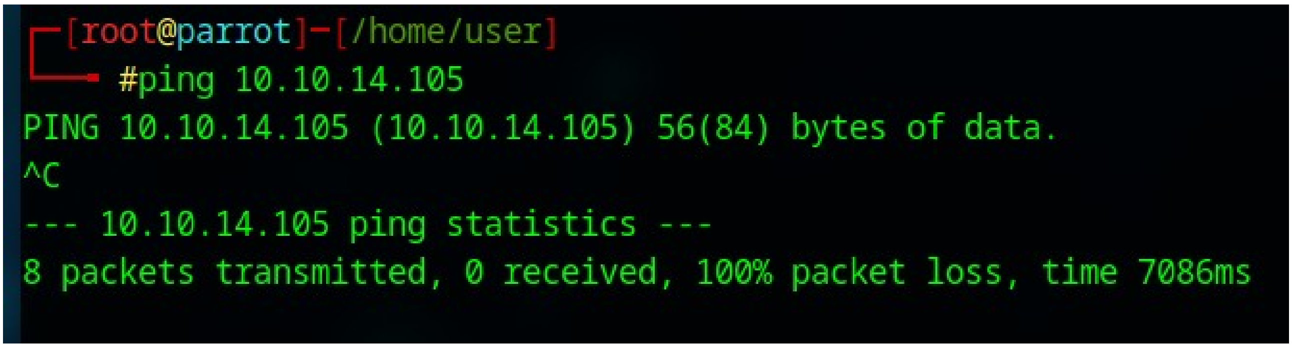
Anthem – TryHackMe

This challenge includes multiple flags and questions. I'll answer them as I go through the write-up.

Contents

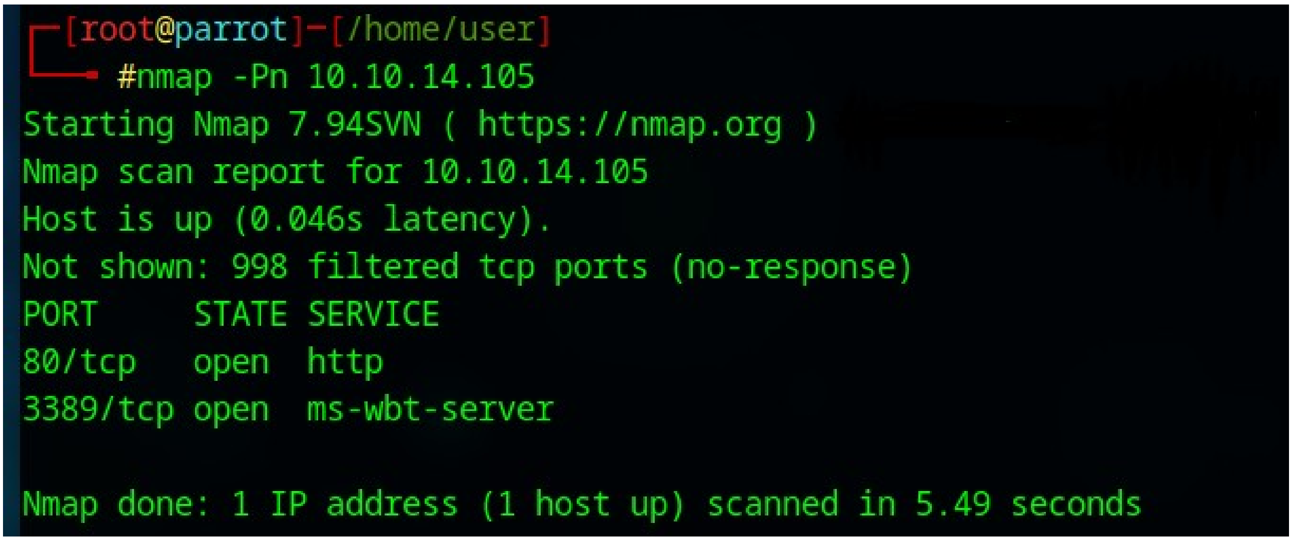
1.Reconnaissance

We start by checking if the host is alive.



```
┌─[root@parrot]─[/home/user]
└──╼ #ping 10.10.14.105
PING 10.10.14.105 (10.10.14.105) 56(84) bytes of data.
^C
--- 10.10.14.105 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7086ms
```

There's no ICMP response – ping appears to be blocked.
So we run **Nmap** to check for open ports despite this.

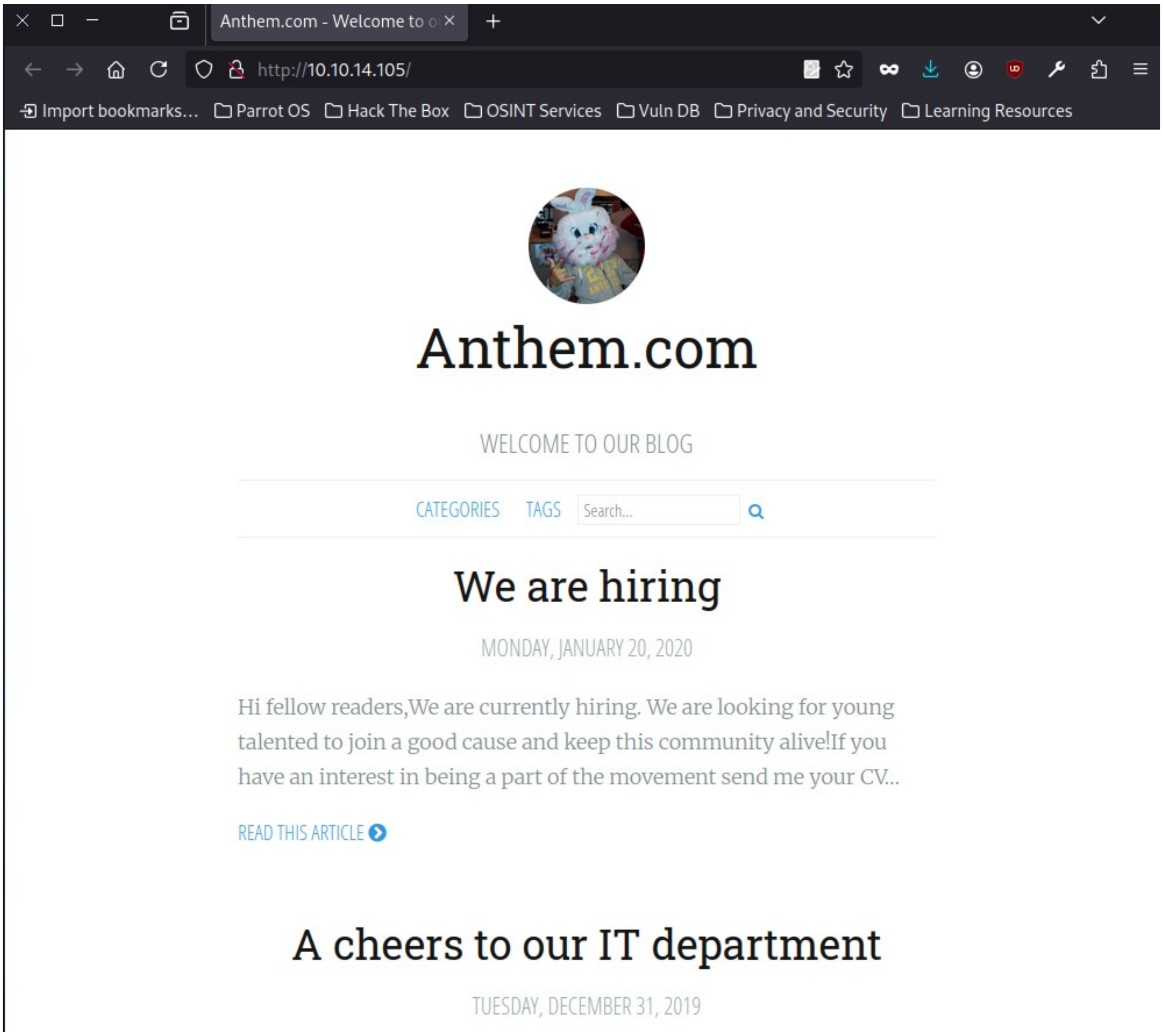


```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -Pn 10.10.14.105
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.10.14.105
Host is up (0.046s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 5.49 seconds
```

Question - What port is for the web server? **80**.
Question - What port is for remote desktop service? **3389**.

2.Website

Let's check what's on the web server.



Anthem.com

WELCOME TO OUR BLOG

We are hiring

MONDAY, JANUARY 20, 2020

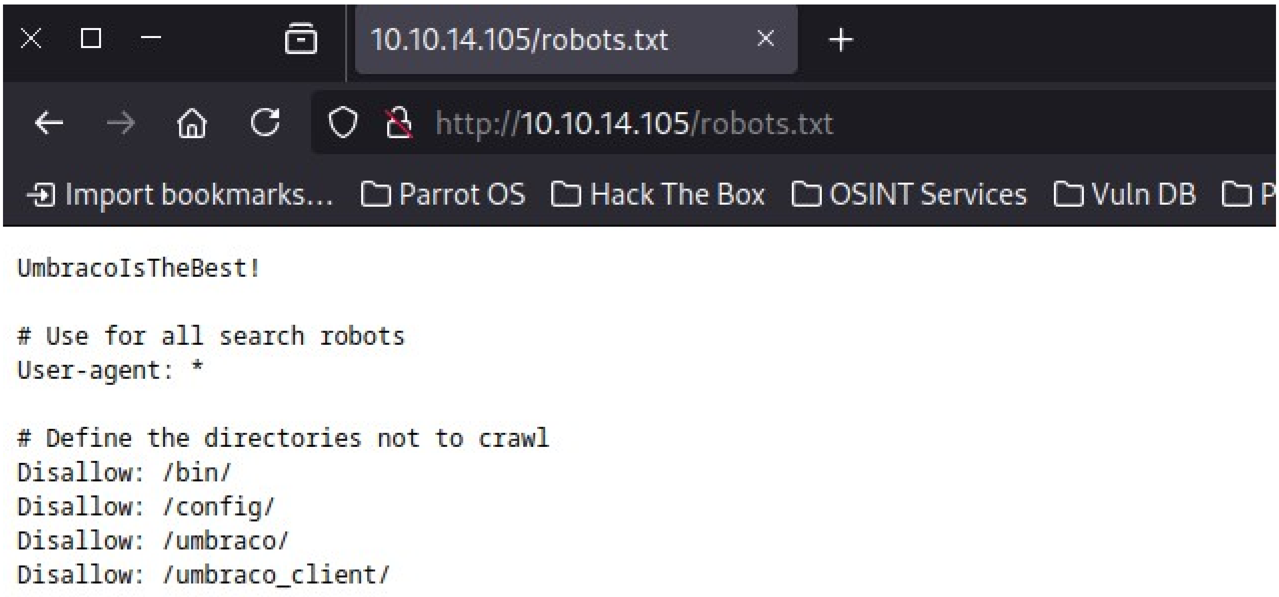
Hi fellow readers,We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!If you have an interest in being a part of the movement send me your CV...

READ THIS ARTICLE

A cheers to our IT department

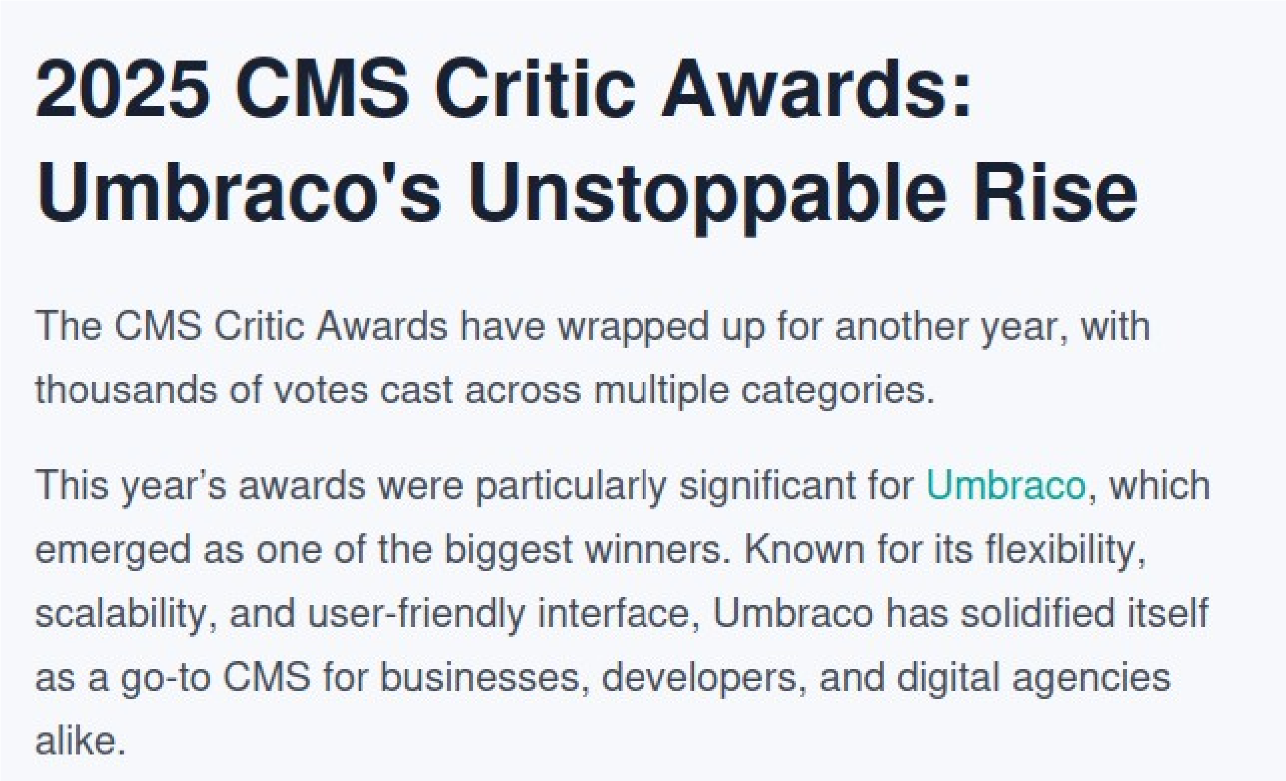
TUESDAY, DECEMBER 31, 2019

In **robots.txt**, we find an interesting entry:



```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

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

Question - What is a possible password in one of the pages web crawlers check for?
UmbracoIsTheBest!
I determined the CMS is Umbraco based on the context of this password.

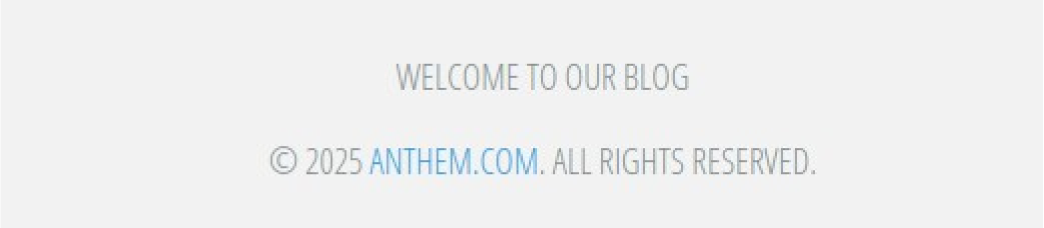


2025 CMS Critic Awards: Umbraco's Unstoppable Rise

The CMS Critic Awards have wrapped up for another year, with thousands of votes cast across multiple categories.

This year’s awards were particularly significant for Umbraco, which emerged as one of the biggest winners. Known for its flexibility, scalability, and user-friendly interface, Umbraco has solidified itself as a go-to CMS for businesses, developers, and digital agencies alike.

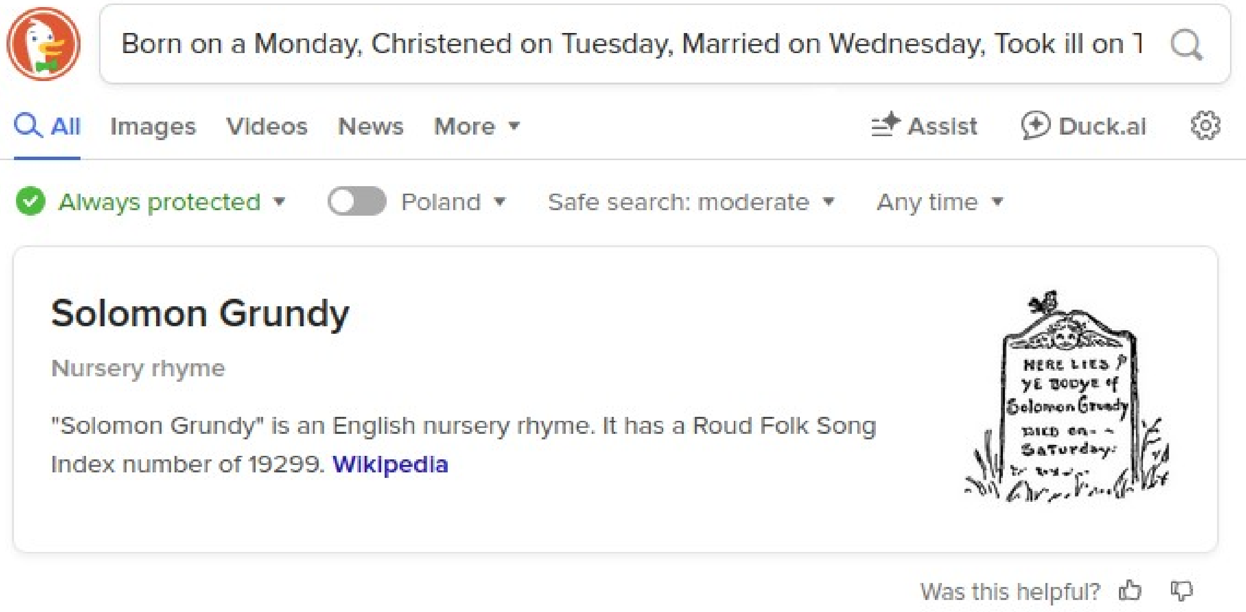
Question - What CMS is the website using? **Umbraco**.
At the bottom of the webpage, we find a domain reference:



WELCOME TO OUR BLOG

© 2025 ANTHEM.COM. ALL RIGHTS RESERVED.

Question - What is the domain of the website? **Anthem.com**
I also found a nursery rhyme on the site, attributed to **Solomon Grundy**.



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

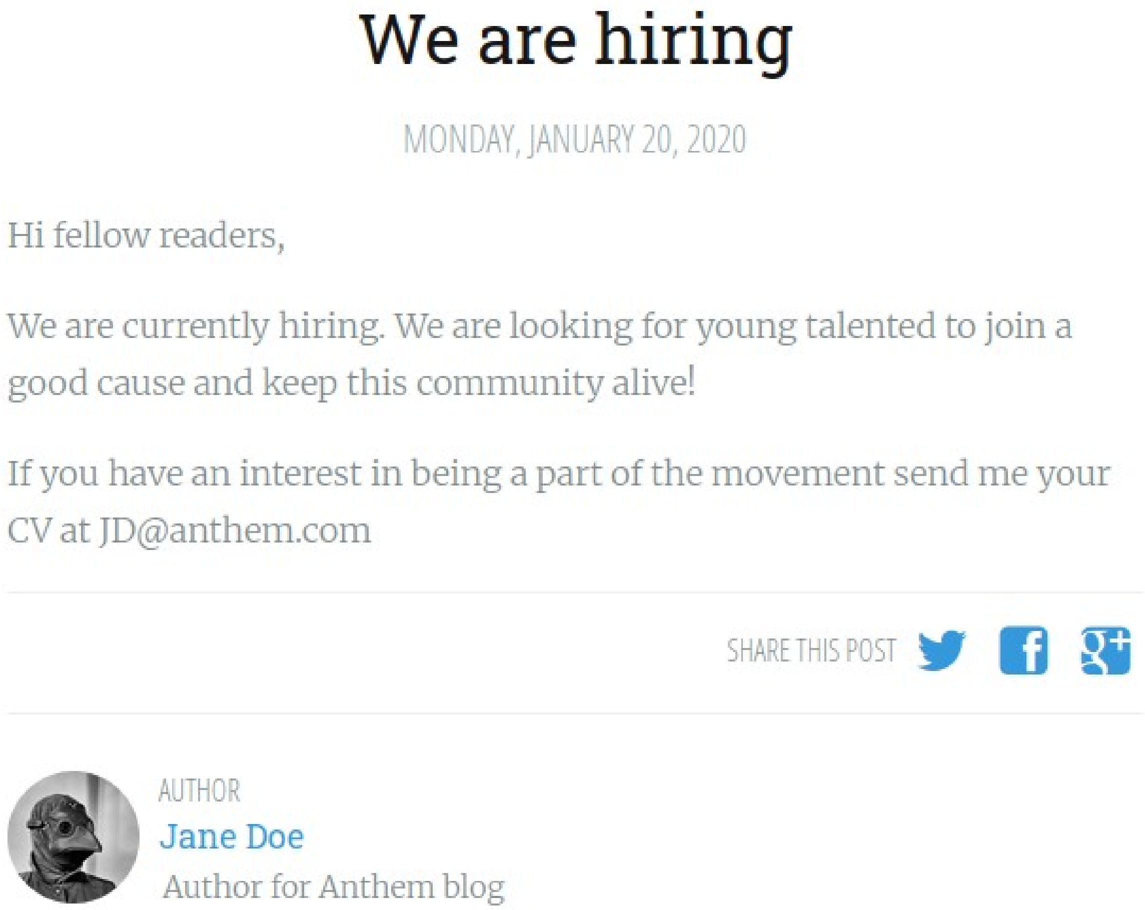
Solomon Grundy

Nursery rhyme

"Solomon Grundy" is an English nursery rhyme. It has a Roud Folk Song Index number of 19299. Wikipedia

Question - What's the name of the Administrator? **Solomon Grundy**.

Another person is mentioned on the site – **Jane Doe**. Her email likely follows the pattern of initials.



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!

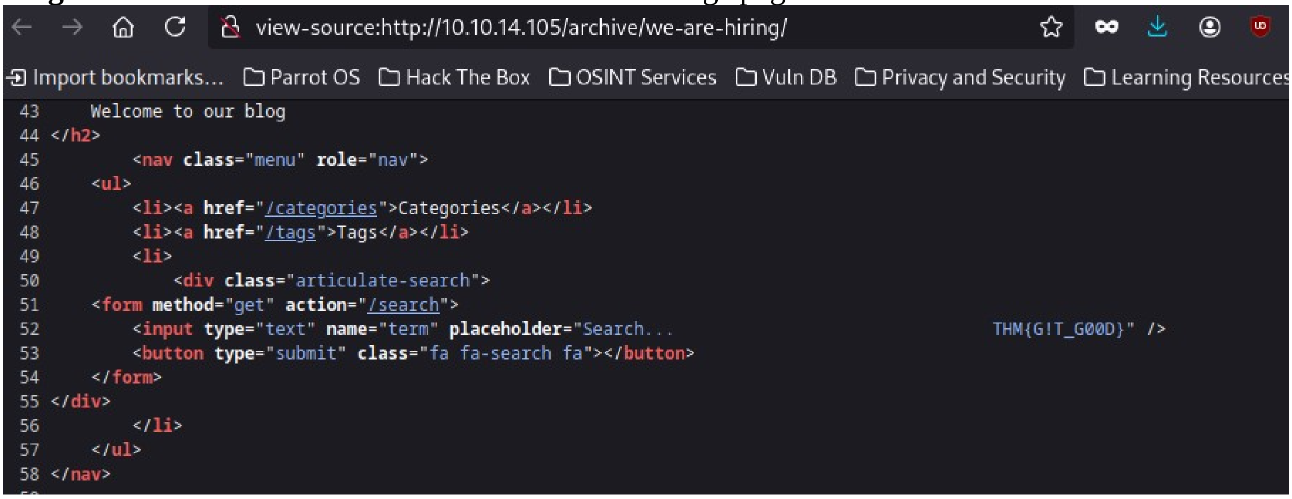
If you have an interest in being a part of the movement send me your CV at JD@anthem.com

Question - Can we find find the email address of the administrator? **SG@anthem.com**
Following the naming convention (first name + last initial), we deduce the admin’s email.

3.Website Flags

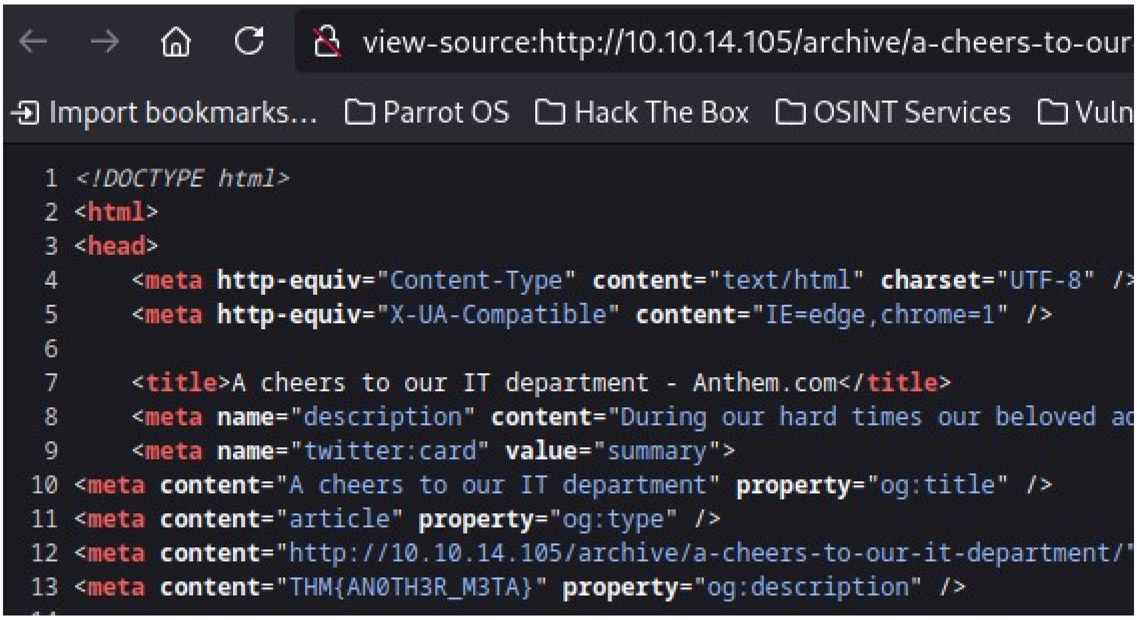
Now we need to locate **four flags** hidden in the site:

Flag 2 – Found in the source code of the "we-are-hiring" page.



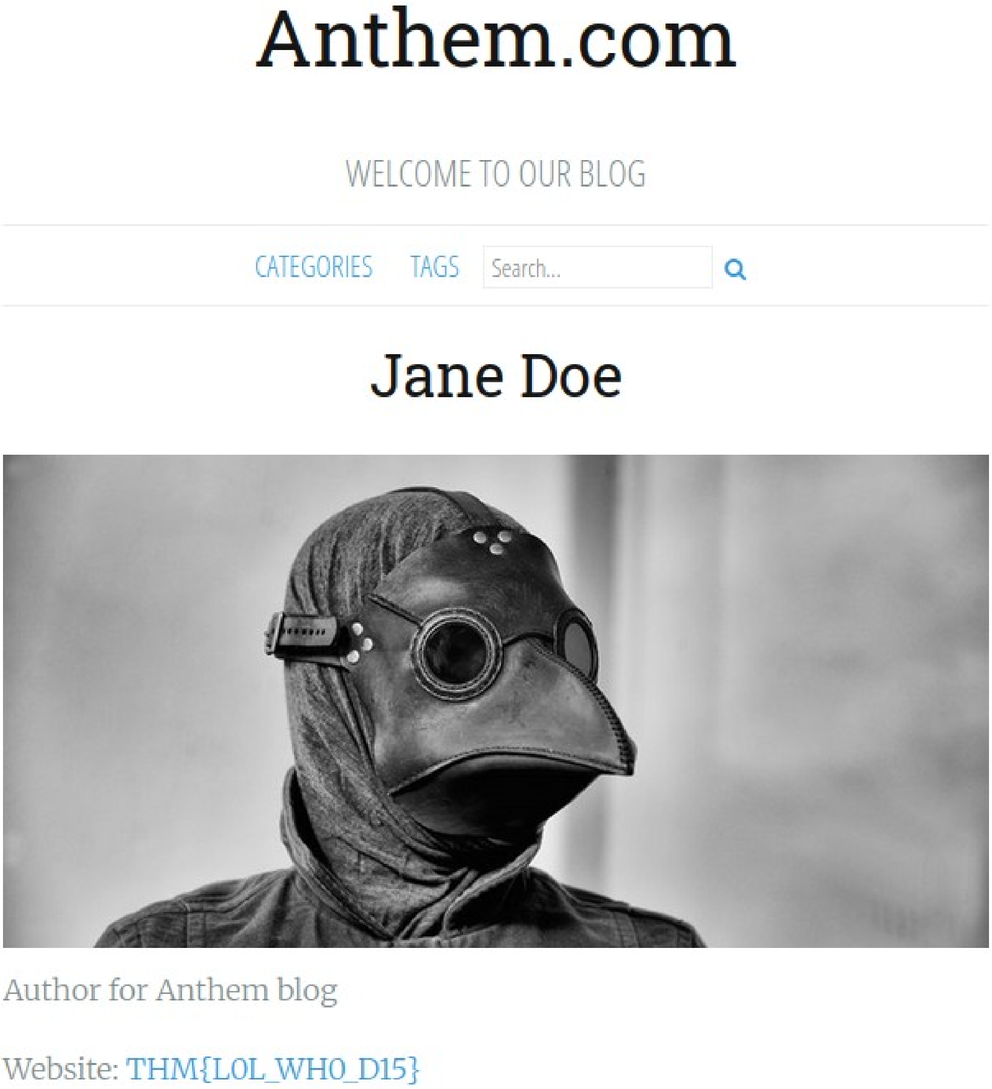
```
    Welcome to our blog
</h2>
        <nav class="menu" role="nav">
    <ul>
        <li><a href="/categories">Categories</a></li>
        <li><a href="/tags">Tags</a></li>
        <li>
            <div class="articulate-search">
    <form method="get" action="/search">
        <input type="text" name="term" placeholder="Search...                              THM{G!T_G00D}" />
        <button type="submit" class="fa fa-search fa"></button>
    </form>
</div>
        </li>
    </ul>
</nav>
```

Flag 4 – Found in the source code of another subpage.



```
<!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 ac
    <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://10.10.14.105/archive/a-cheers-to-our-it-department/"
<meta content="THM{AN0TH3R_M3TA}" property="og:description" />
```

Flag 3 – Found in the "Jane Doe" information section.

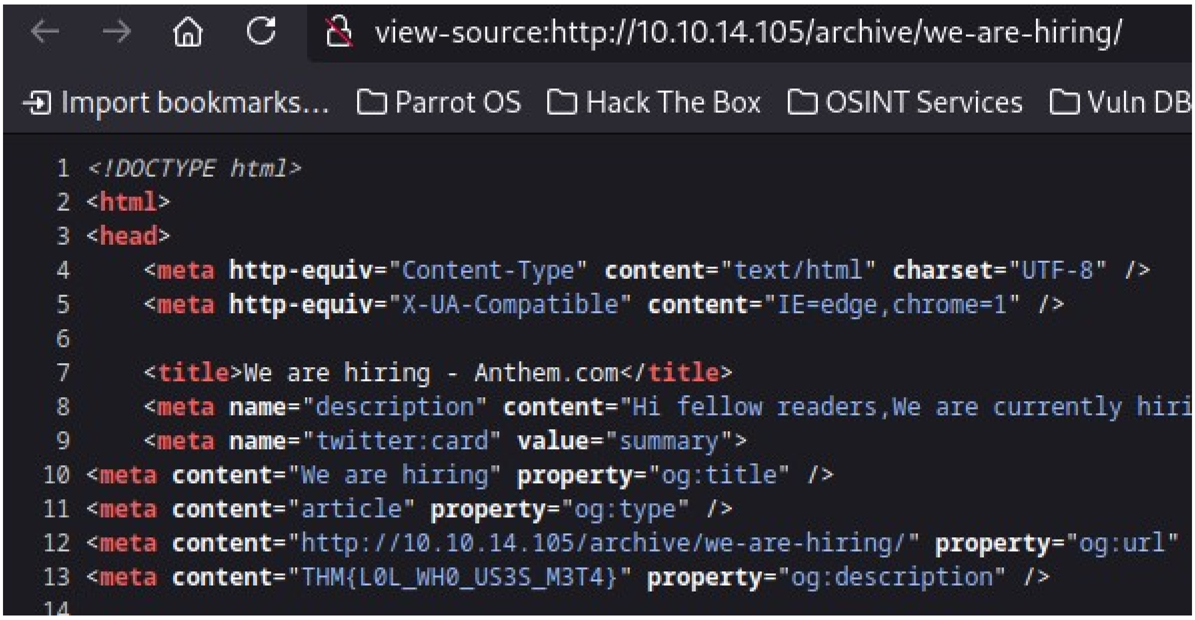


Jane Doe

Author for Anthem blog

Website: THM{L0L_WH0_D15}

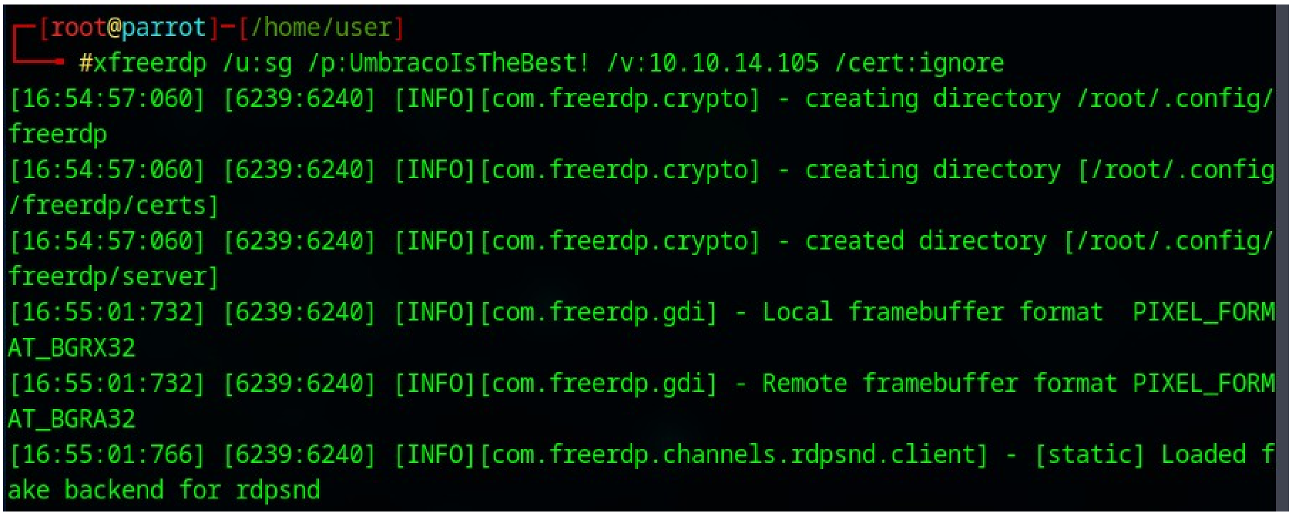
Flag 1 – Also in the source of the "we-are-hiring" page.



```
<!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 hiri
    <meta name="twitter:card" value="summary">
<meta content="We are hiring" property="og:title" />
<meta content="article" property="og:type" />
<meta content="http://10.10.14.105/archive/we-are-hiring/" property="og:url"
<meta content="THM{L0L_WH0_US3S_M3T4}" property="og:description" />
```

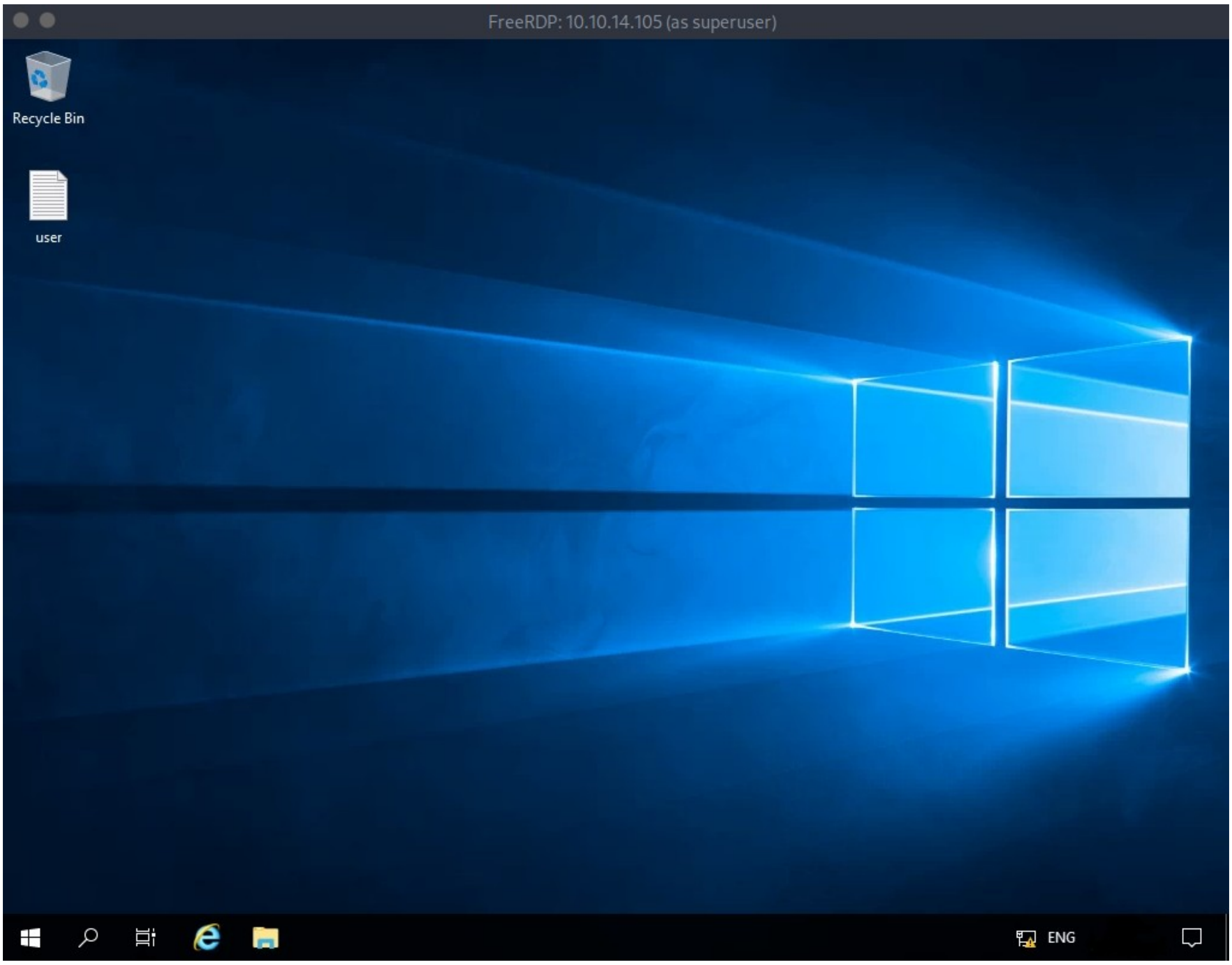
4.RDP Access

Using the acquired data, we connect via **RDP**.

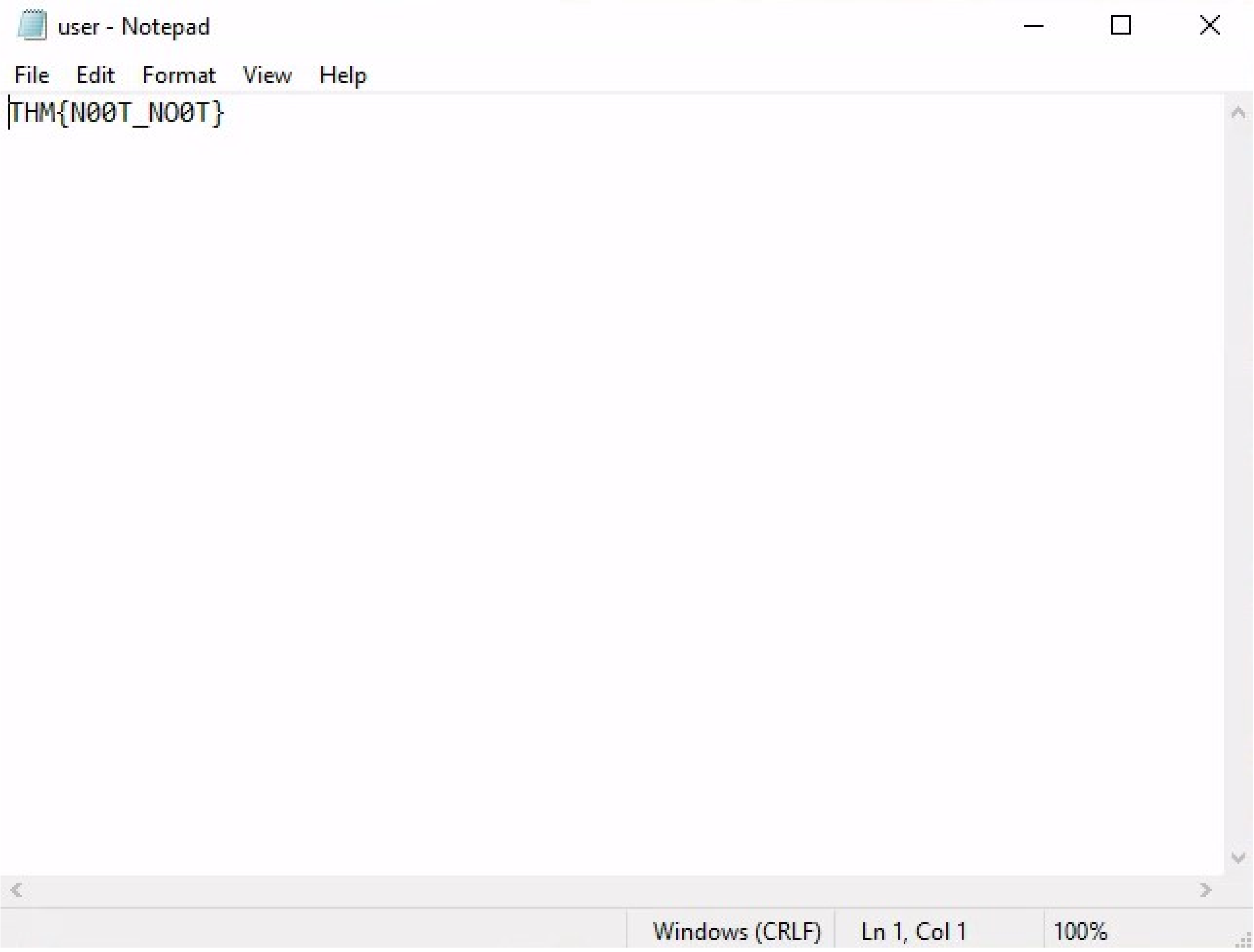


```
┌─[root@parrot]─[/home/user]
└──╼ #xfreerdp /u:sg /p:UmbracoIsTheBest! /v:10.10.14.105 /cert:ignore
[16:54:57:060] [6239:6240] [INFO][com.freerdp.crypto] - creating directory /root/.config/
freerdp
[16:54:57:060] [6239:6240] [INFO][com.freerdp.crypto] - creating directory [/root/.config
/freerdp/certs]
[16:54:57:060] [6239:6240] [INFO][com.freerdp.crypto] - created directory [/root/.config/
freerdp/server]
[16:55:01:732] [6239:6240] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORM
AT_BGRX32
[16:55:01:732] [6239:6240] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORM
AT_BGRA32
[16:55:01:766] [6239:6240] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded f
ake backend for rdpsnd
```

It works – credentials are valid.

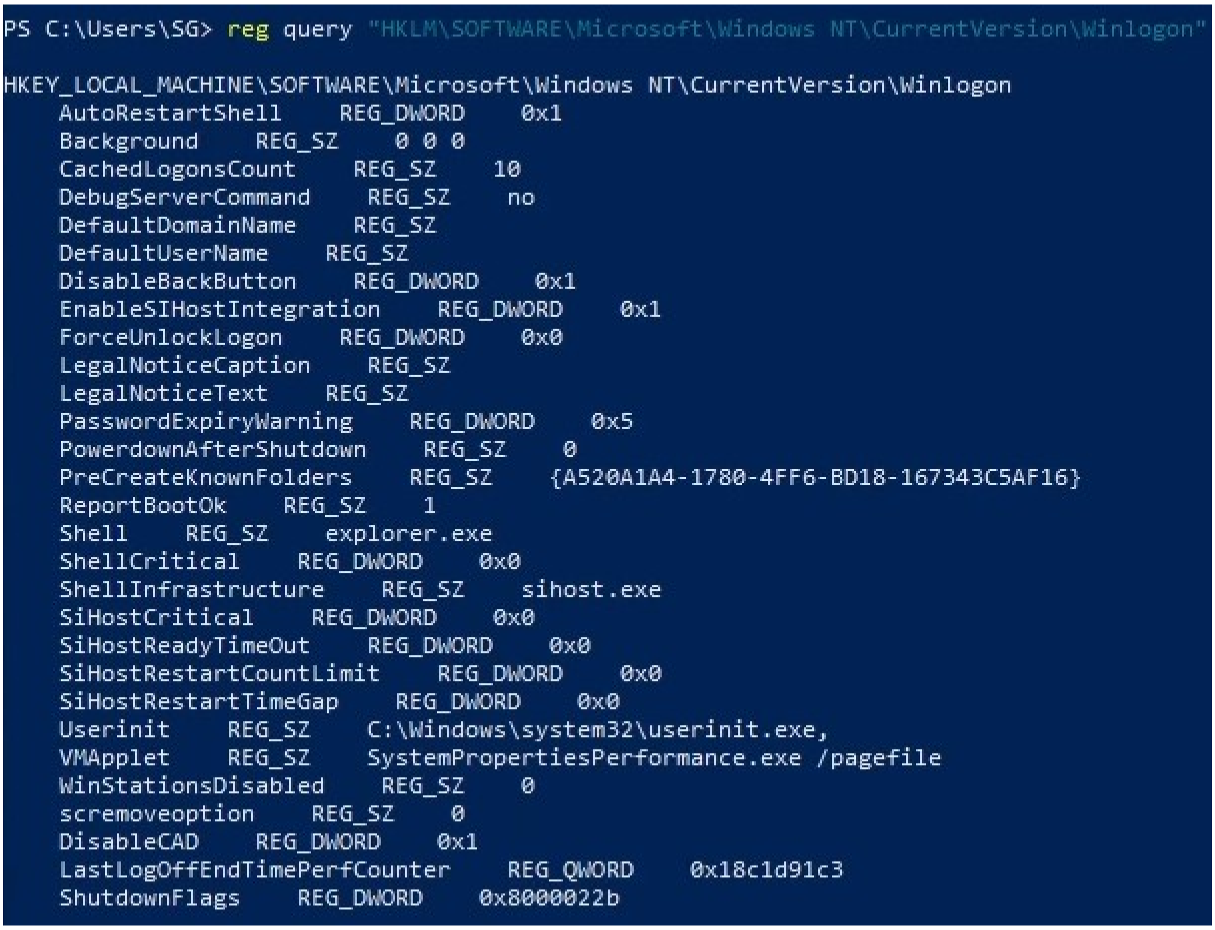


On the desktop, we immediately find the **user flag**.



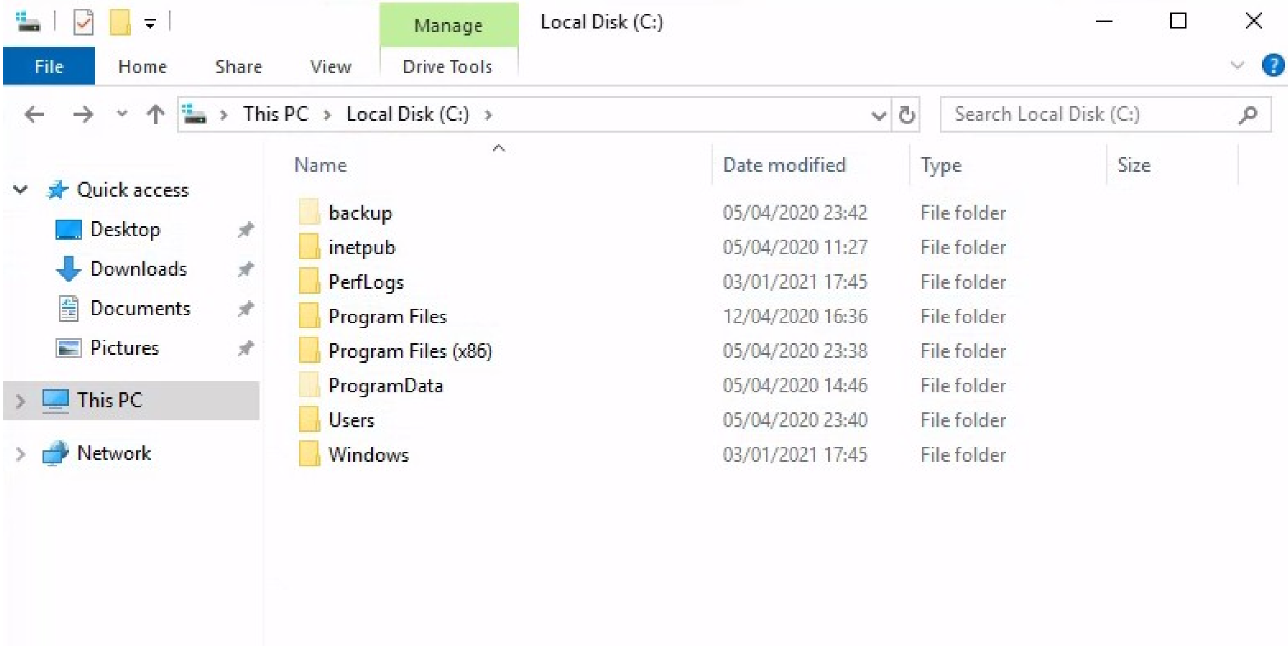
```
THM{N00T_NO0T}
```

Next, we need the **admin password**.
I started by checking the registry using PowerShell and the Winlogon key – but no success there.



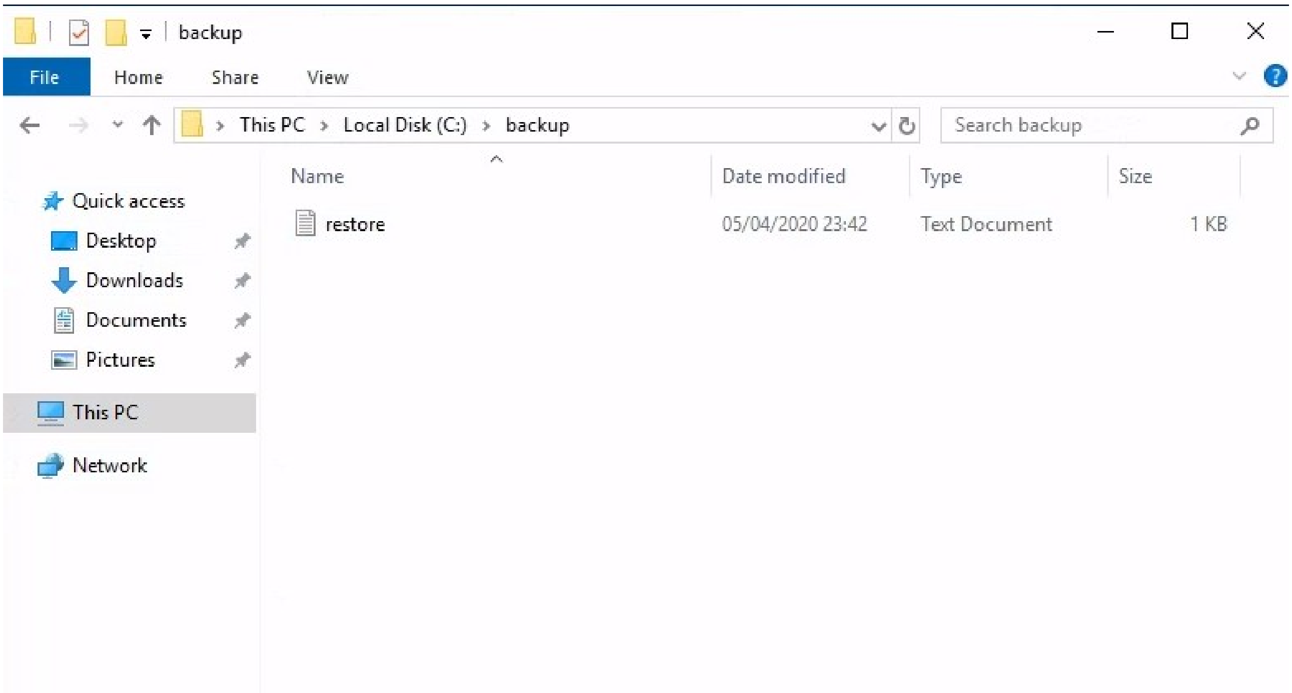
```
PS C:\Users\SG> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DefaultDomainName    REG_SZ
    DefaultUserName    REG_SZ
    DisableBackButton    REG_DWORD    0x1
    EnableSIHostIntegration    REG_DWORD    0x1
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe
    ShellCritical    REG_DWORD    0x0
    ShellInfrastructure    REG_SZ    sihost.exe
    SiHostCritical    REG_DWORD    0x0
    SiHostReadyTimeOut    REG_DWORD    0x0
    SiHostRestartCountLimit    REG_DWORD    0x0
    SiHostRestartTimeGap    REG_DWORD    0x0
    Userinit    REG_SZ    C:\Windows\system32\userinit.exe,
    VMApplet    REG_SZ    SystemPropertiesPerformance.exe /pagefile
    WinStationsDisabled    REG_SZ    0
    scremoveoption    REG_SZ    0
    DisableCAD    REG_DWORD    0x1
    LastLogOffEndTimePerfCounter    REG_QWORD    0x18c1d91c3
    ShutdownFlags    REG_DWORD    0x8000022b
```

After enabling hidden files in File Explorer, I noticed a **backup** folder on drive *C:*



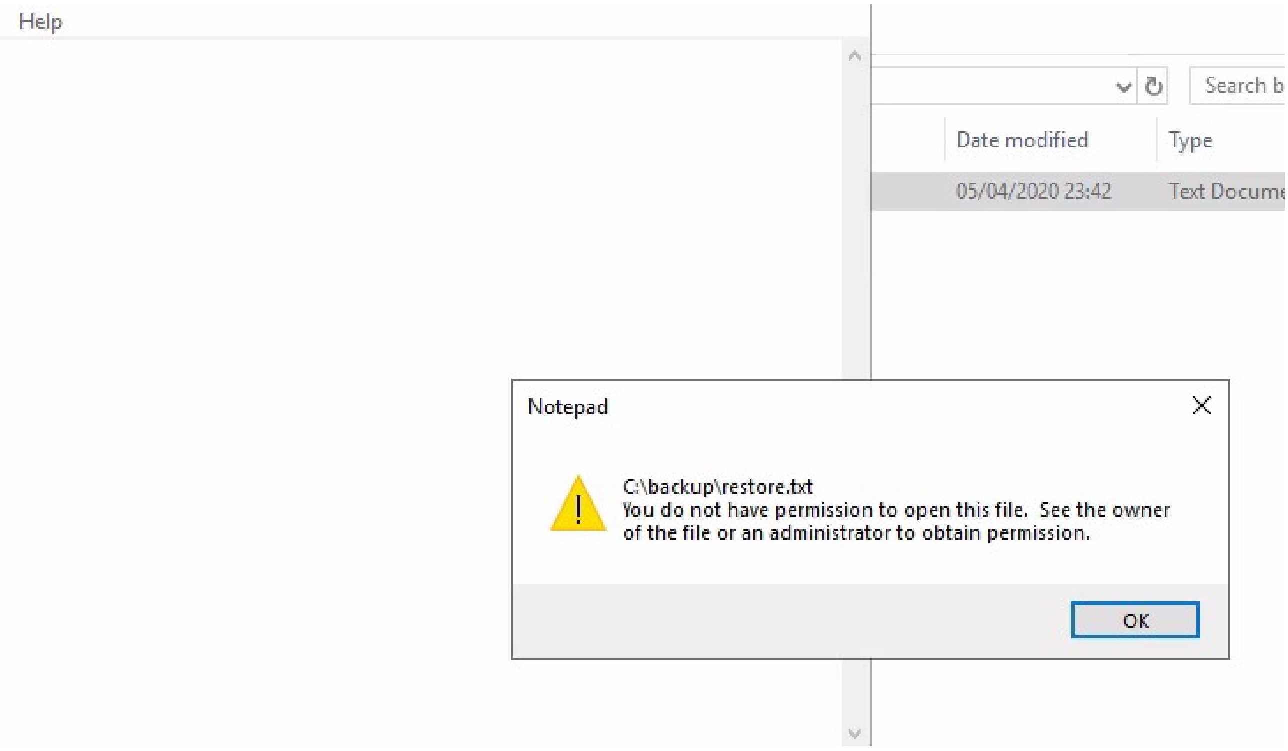
Name	Date modified	Type	Size
backup	05/04/2020 23:42	File folder	
inetpub	05/04/2020 11:27	File folder	
PerfLogs	03/01/2021 17:45	File folder	
Program Files	12/04/2020 16:36	File folder	
Program Files (x86)	05/04/2020 23:38	File folder	
ProgramData	05/04/2020 14:46	File folder	
Users	05/04/2020 23:40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

Inside, there was a file – **restore.txt**.



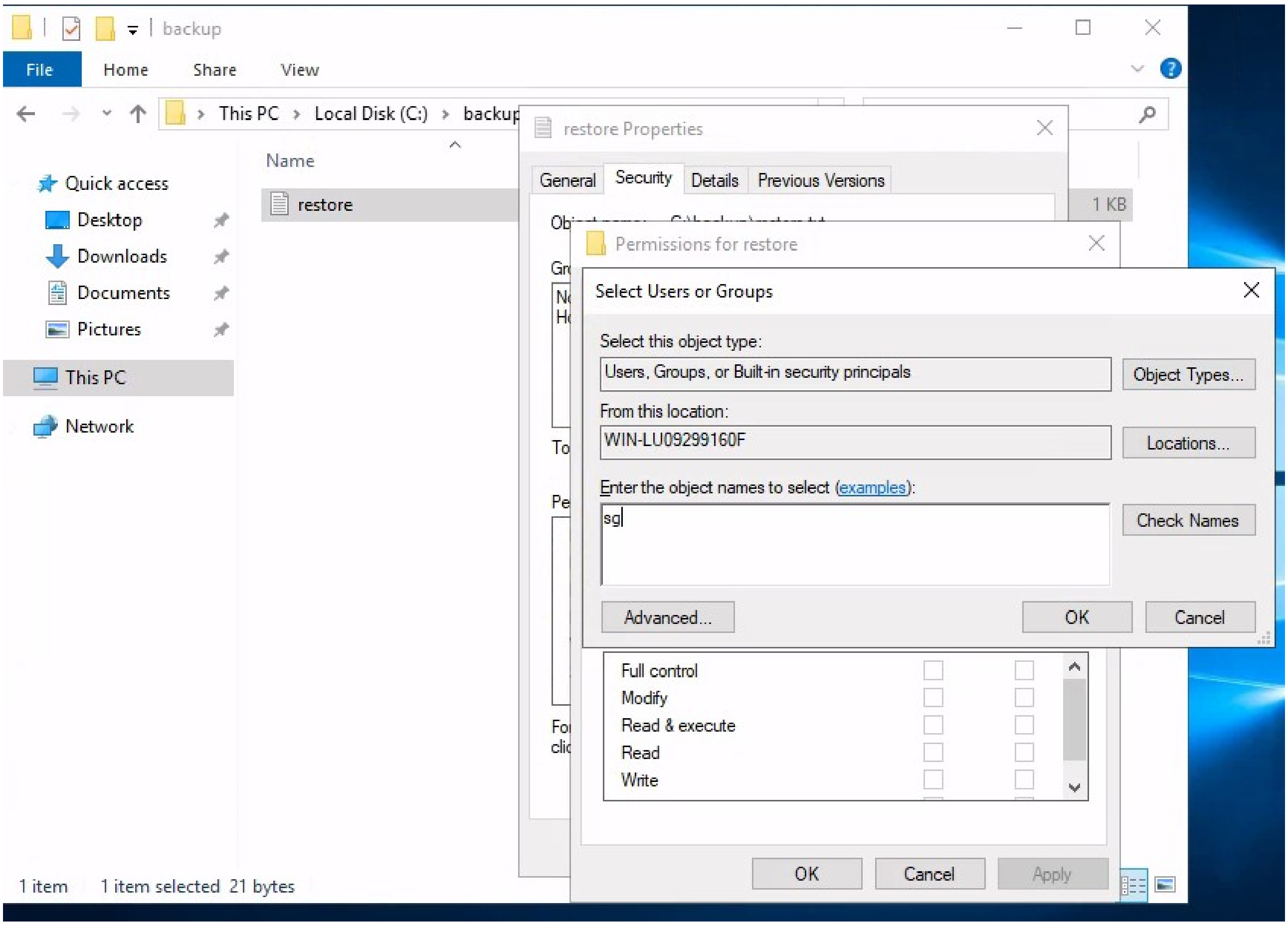
Name	Date modified	Type	Size
restore	05/04/2020 23:42	Text Document	1 KB

Trying to open it results in a **permission error**.



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.

In the file's properties, I gave myself permission as user **SG**.

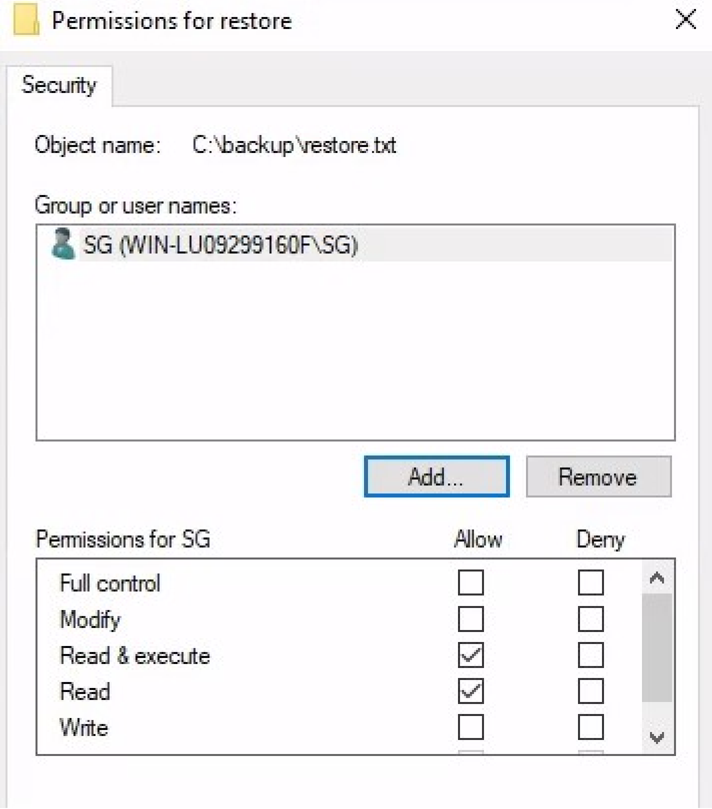


Select this object type:
Users, Groups, or Built-in security principals

From this location:
WIN-LU09299160F

Enter the object names to select (examples):
sg

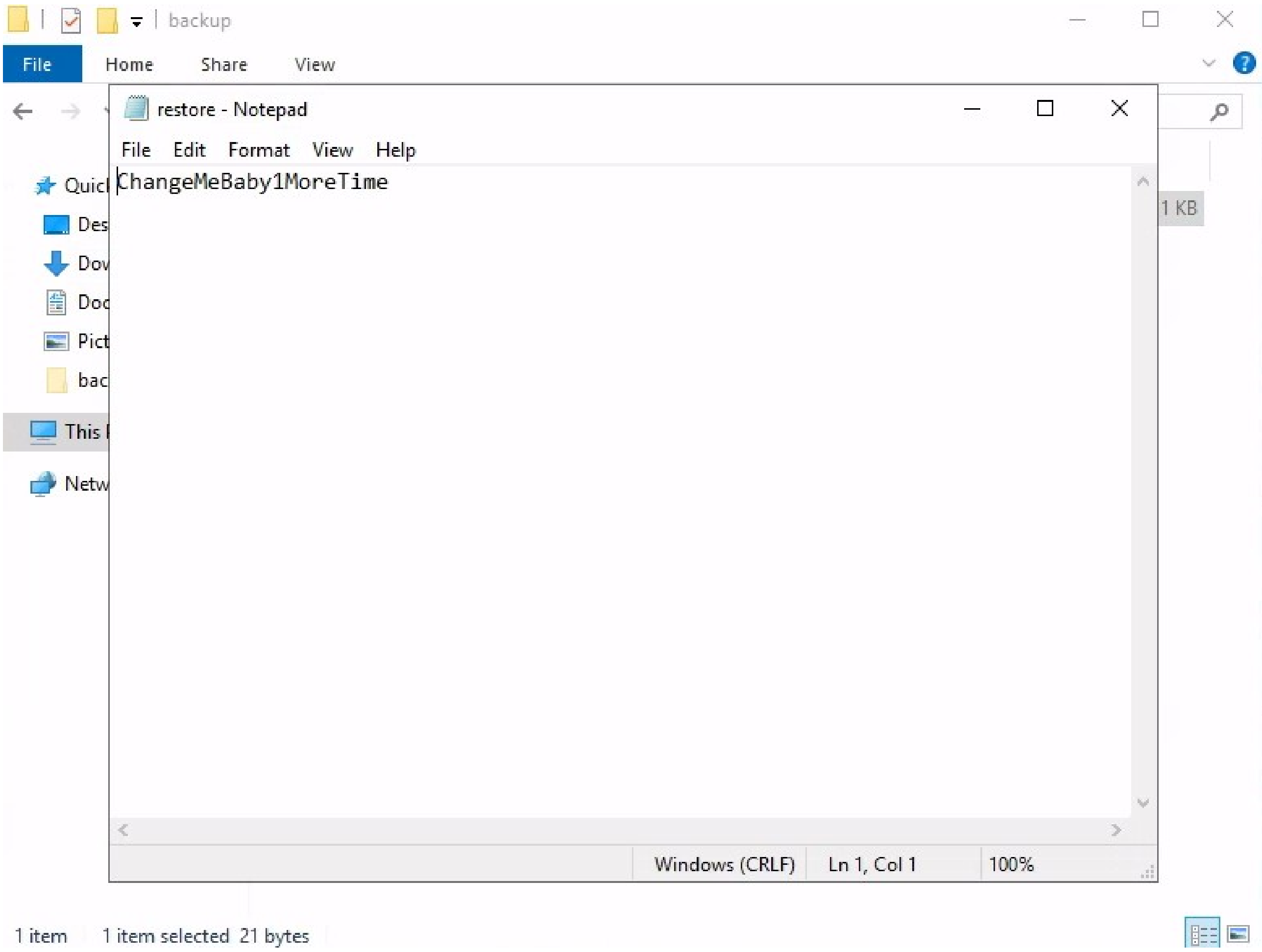
Now we can open the file – it contains the **admin password**.



Object name: C:\backup\restore.txt

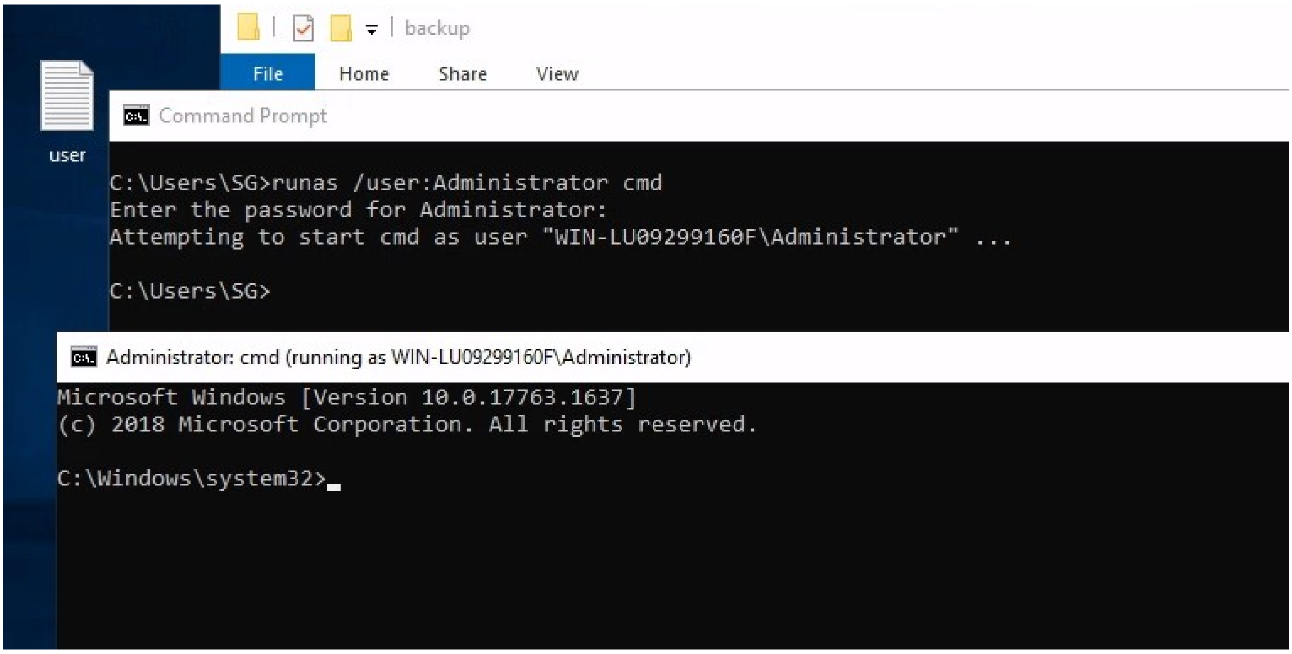
Group or user names:
SG (WIN-LU09299160F\SG)

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



```
ChangeMeBaby1MoreTime
```

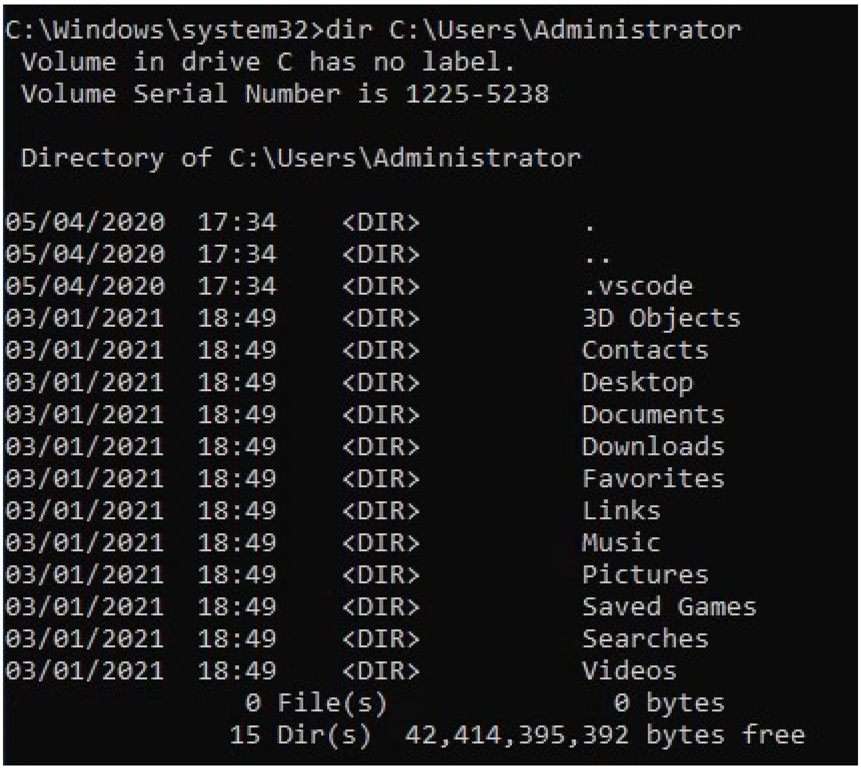
We launch a console as **administrator**.


user
backup
File
Home
Share
View
Command Prompt
Administrator: cmd (running as WIN-LU09299160F\Administrator)

```
C:\Users\SG>runas /user:Administrator cmd
Enter the password for Administrator:
Attempting to start cmd as user "WIN-LU09299160F\Administrator" ...

C:\Users\SG>
```

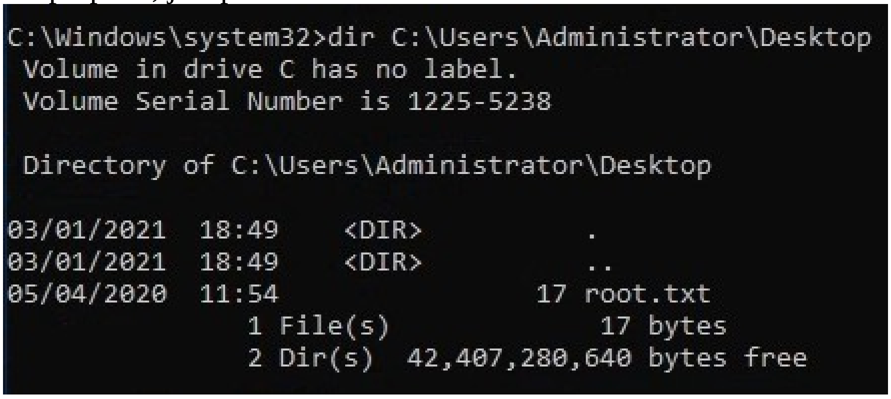
```
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```

I explore the admin's folders – on the desktop, there's **root.txt**.



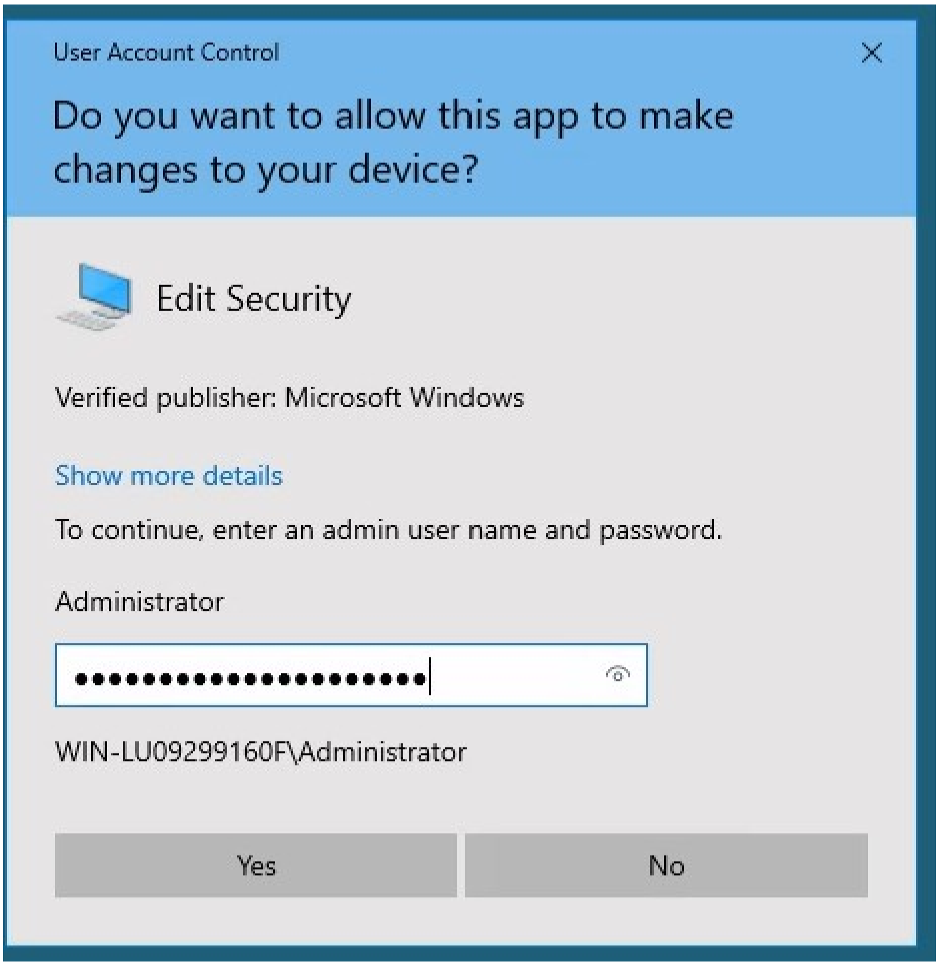
```
C:\Windows\system32>dir C:\Users\Administrator
 Volume in drive C has no label.
 Volume Serial Number is 1225-5238

 Directory of C:\Users\Administrator

05/04/2020  17:34    <DIR>          .
05/04/2020  17:34    <DIR>          ..
05/04/2020  17:34    <DIR>          .vscode
03/01/2021  18:49    <DIR>          3D Objects
03/01/2021  18:49    <DIR>          Contacts
03/01/2021  18:49    <DIR>          Desktop
03/01/2021  18:49    <DIR>          Documents
03/01/2021  18:49    <DIR>          Downloads
03/01/2021  18:49    <DIR>          Favorites
03/01/2021  18:49    <DIR>          Links
03/01/2021  18:49    <DIR>          Music
03/01/2021  18:49    <DIR>          Pictures
03/01/2021  18:49    <DIR>          Saved Games
03/01/2021  18:49    <DIR>          Searches
03/01/2021  18:49    <DIR>          Videos
               0 File(s)              0 bytes
              15 Dir(s)  42,414,395,392 bytes free
```

Na pulpicie, jest plik root.txt



```
C:\Windows\system32>dir C:\Users\Administrator\Desktop
 Volume in drive C has no label.
 Volume Serial Number is 1225-5238

 Directory of C:\Users\Administrator\Desktop

03/01/2021  18:49    <DIR>          .
03/01/2021  18:49    <DIR>          ..
05/04/2020  11:54                17 root.txt
               1 File(s)             17 bytes
               2 Dir(s)  42,407,280,640 bytes free
```

I opened it via the file explorer and entered the admin password.



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

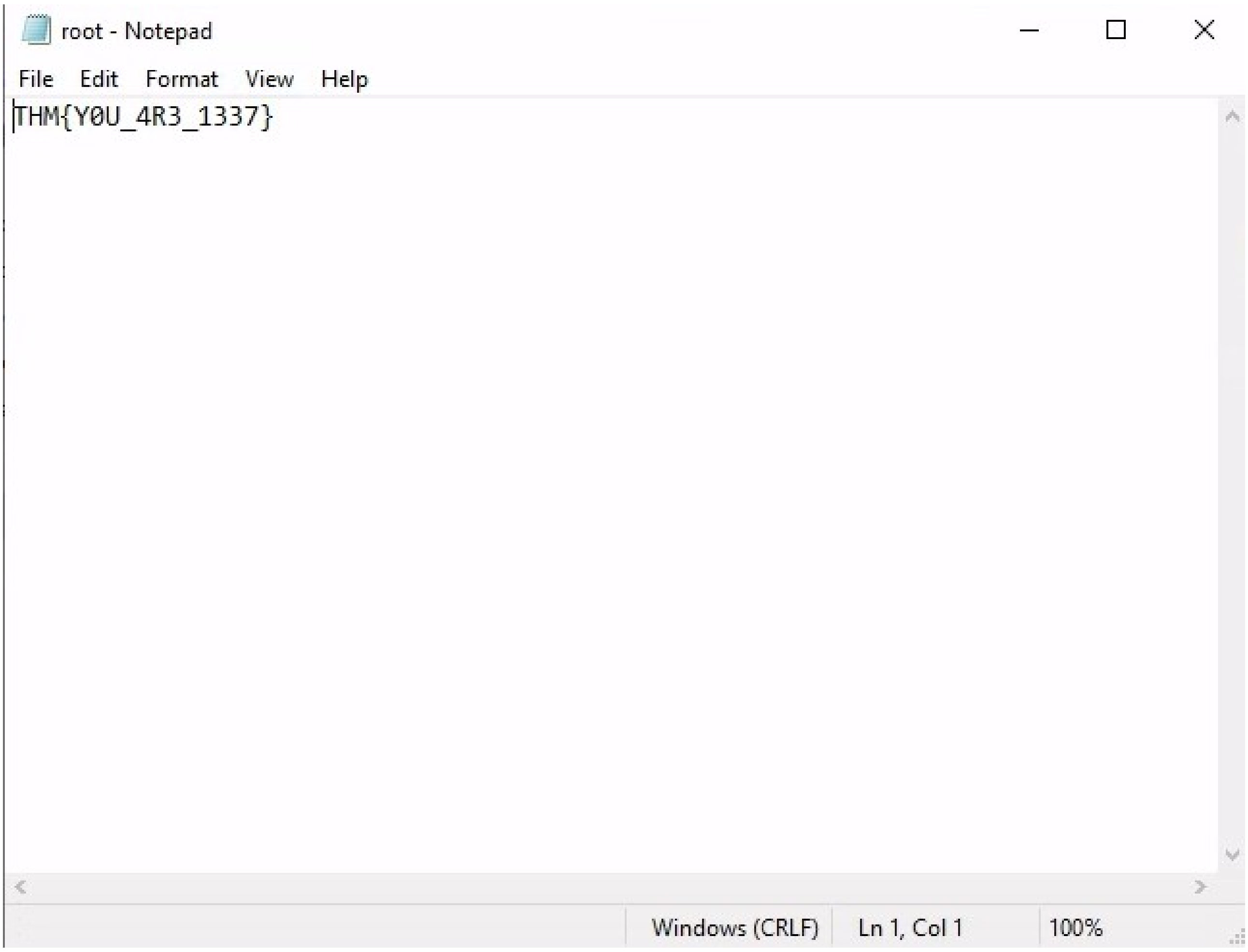
To continue, enter an admin user name and password.

Administrator

••••••••••••••••••••••

WIN-LU09299160F\Administrator

And that gives us the **root flag**.



THM{Y0U_4R3_1337}

5.Summary

This was a CTF focused on **web enumeration and file discovery**.
The hardest part was finding the hidden backup folder on the C: drive.
A solid and enjoyable challenge for practicing **basic privilege escalation** in Windows.