Anthem - Copy

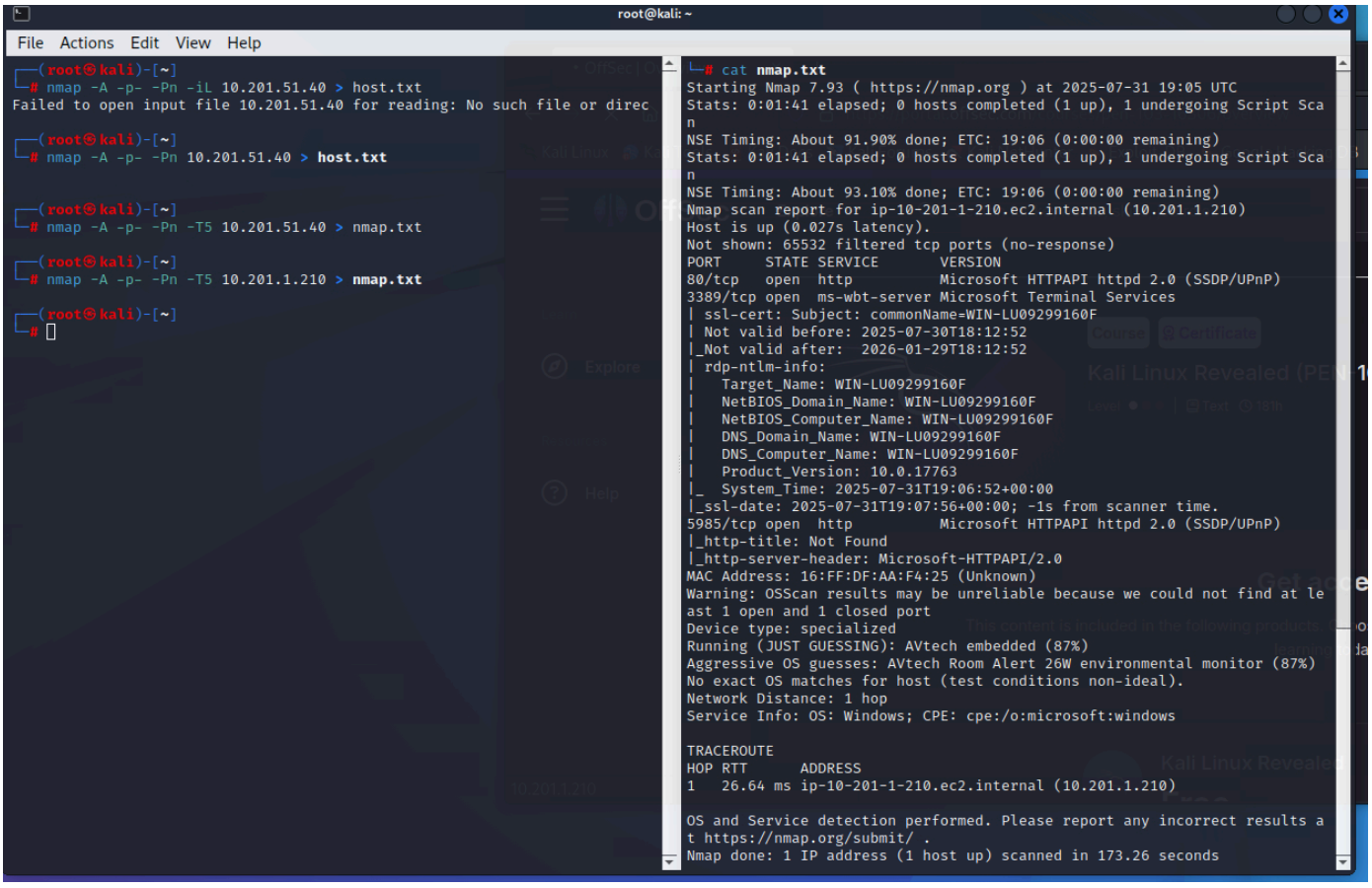
Link --> https://tryhackme.com/room/anthem

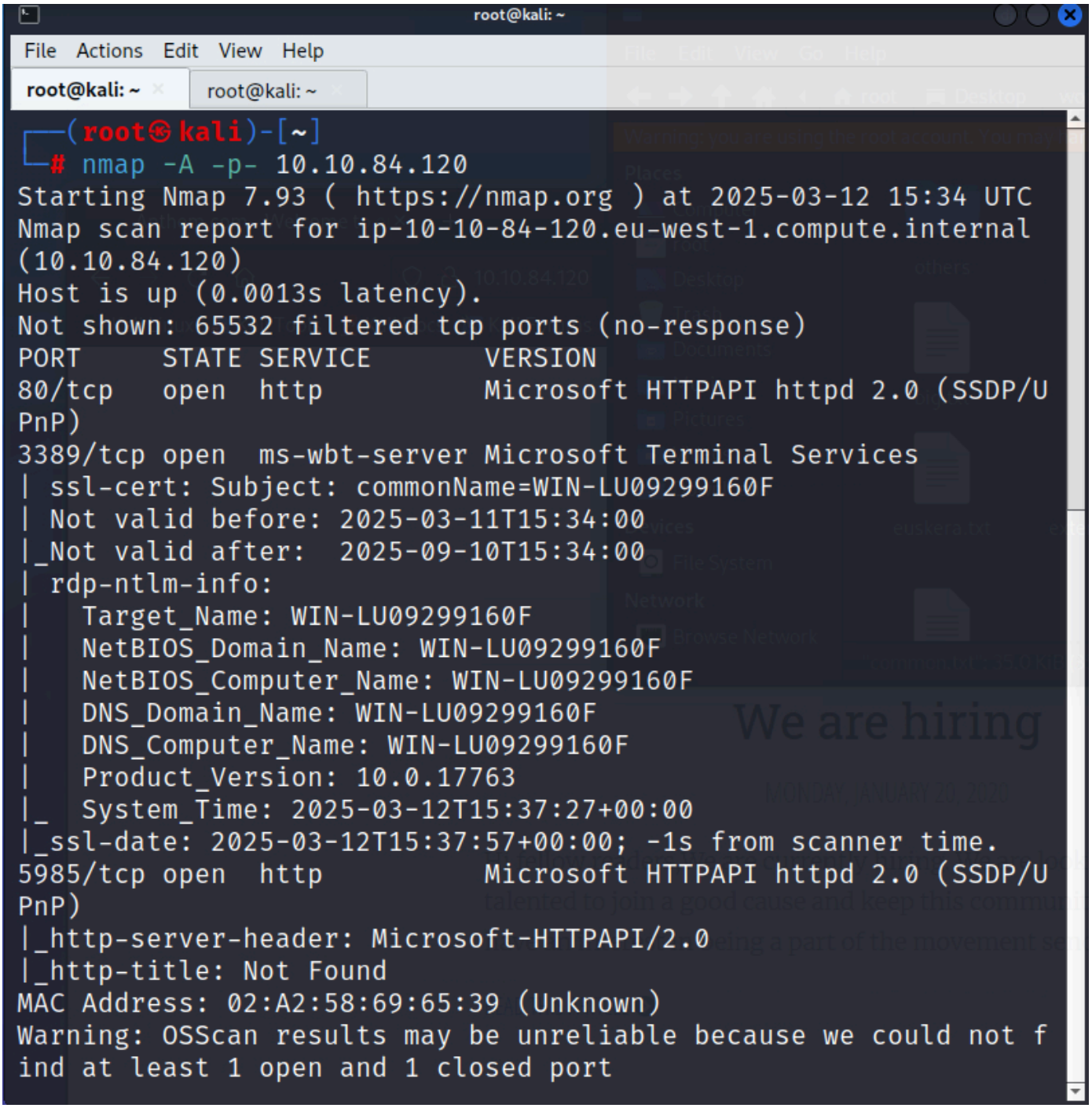
This task involves you, paying attention to details and finding the 'keys to the castle'.

Task 1: Website Analysis

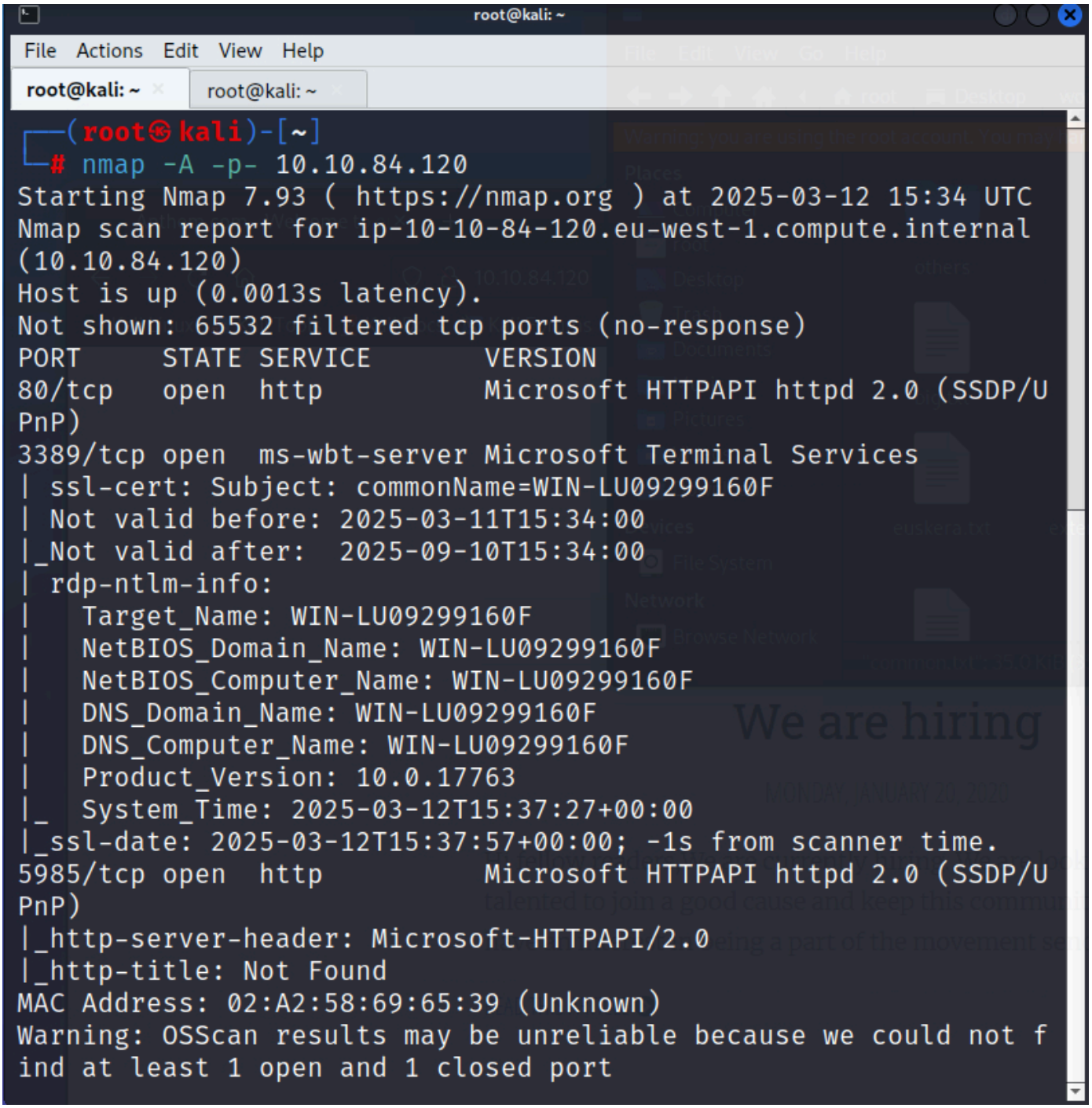
Let's run nmap and check what ports are open.

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

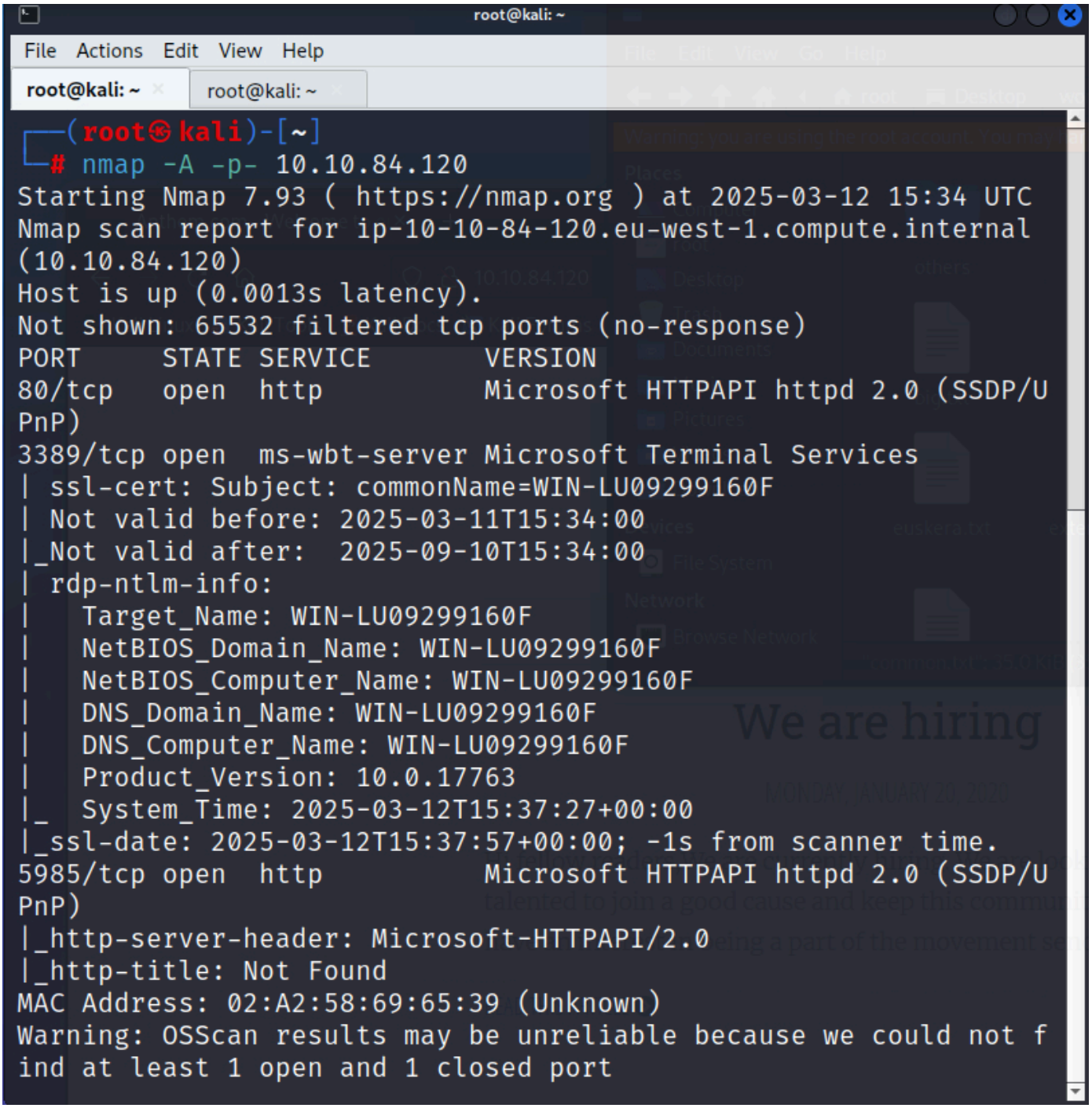




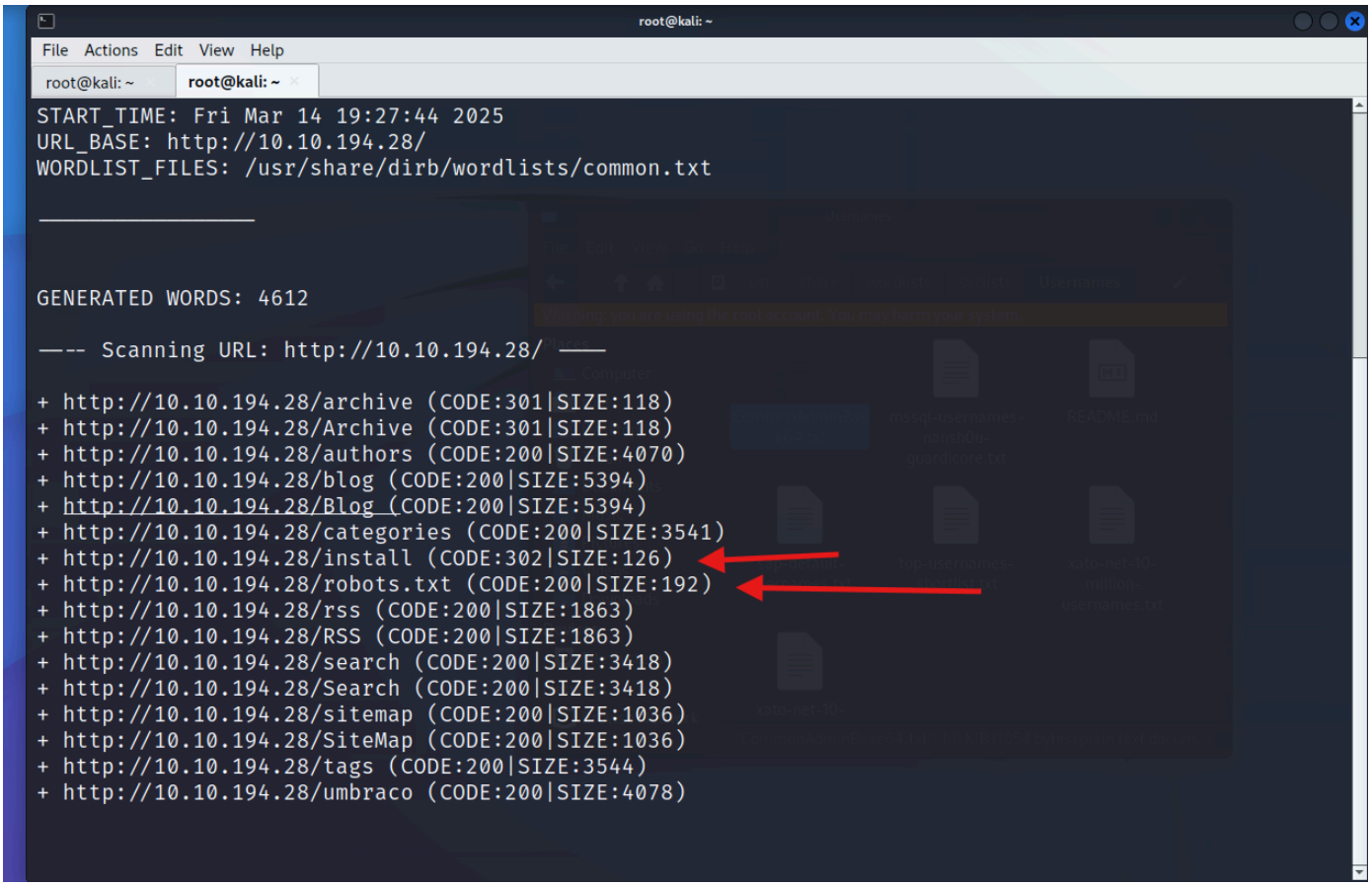
What port is for the web server?



What port is for remote desktop service?

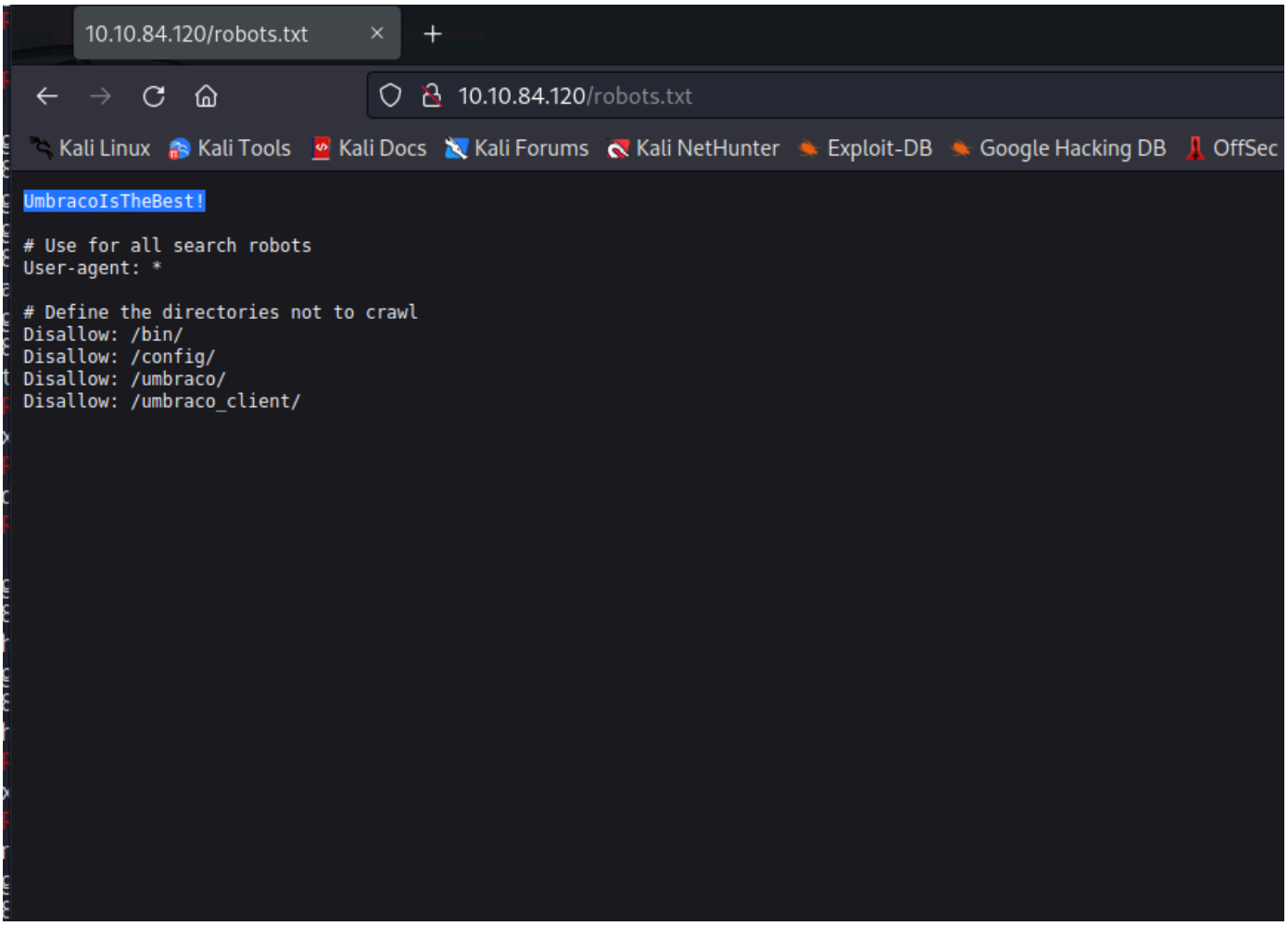


What is a possible password in one of the pages web crawlers check for?



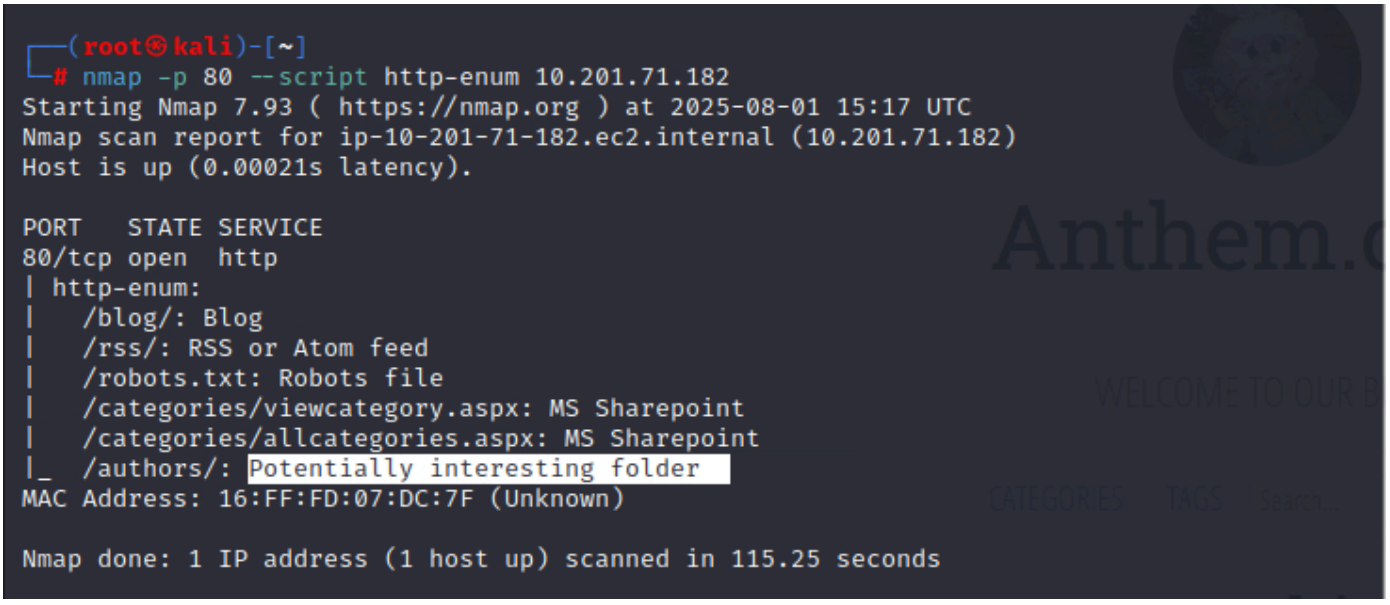
Let's started Enumeration and Exploitation

As per the hint to get the password, We have a populer 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.



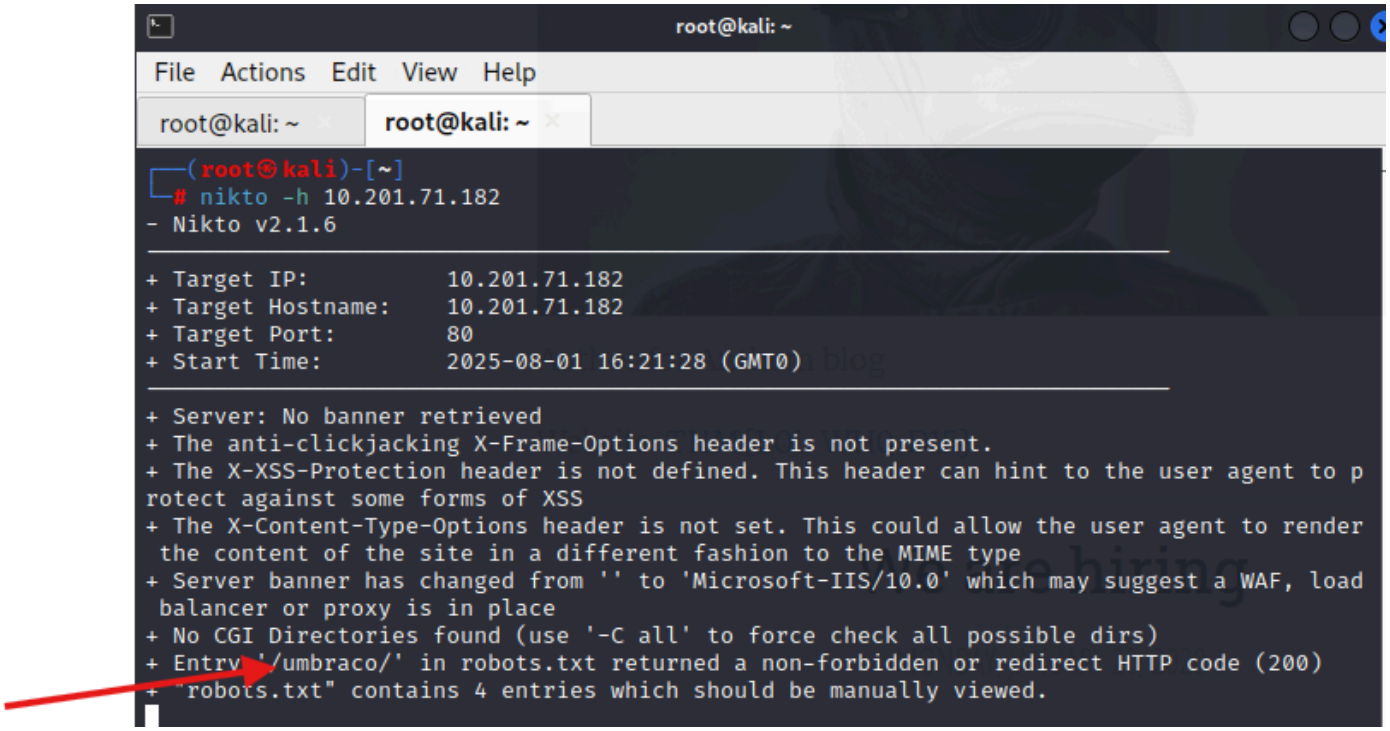
What CMS is the website using?

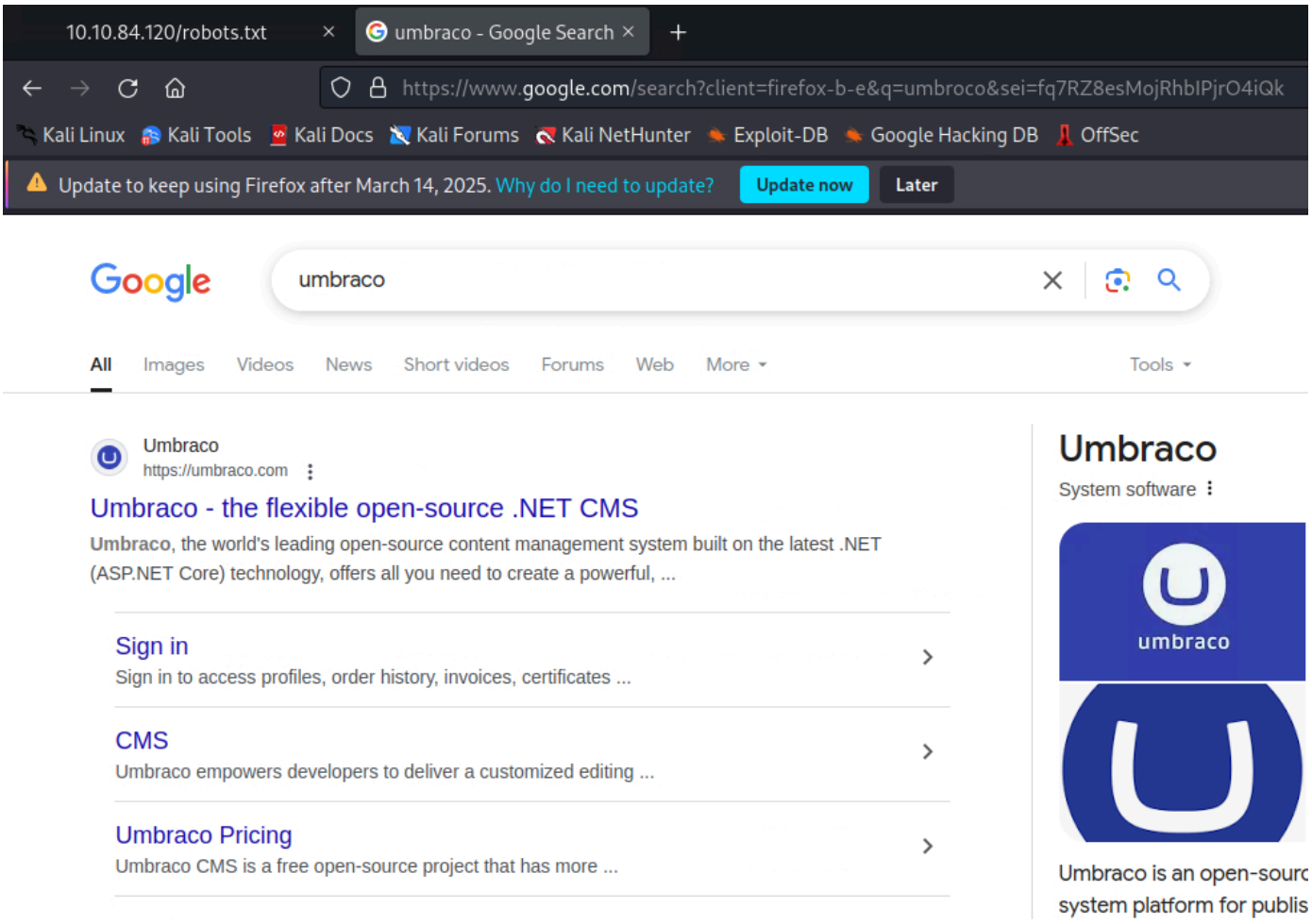
nmap -p 80 --script http-enum 10.201.71.182



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>
```





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.

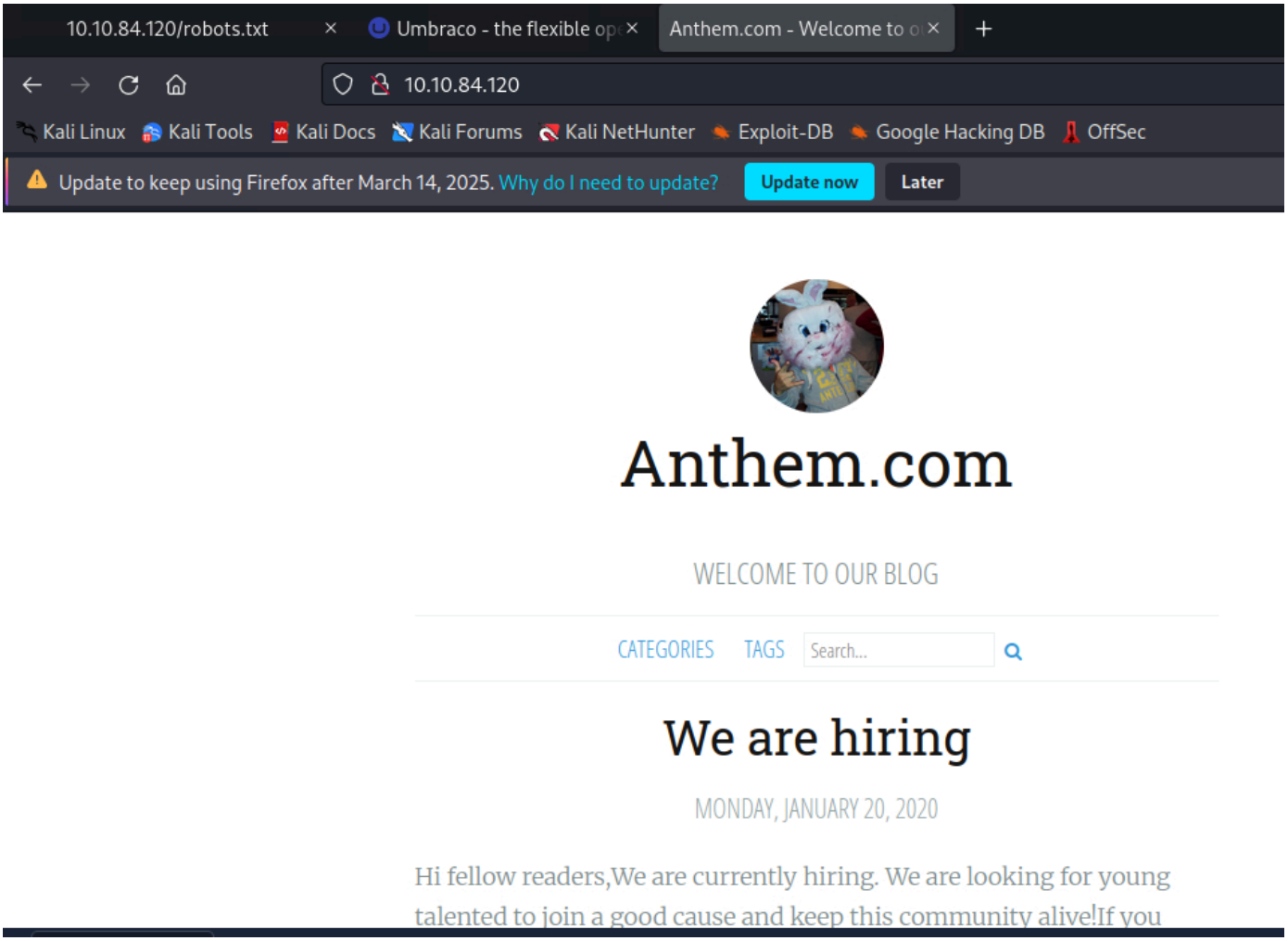
How Can a Pentester Exploit Umbraco?

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?



What's the name of the Administrator

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

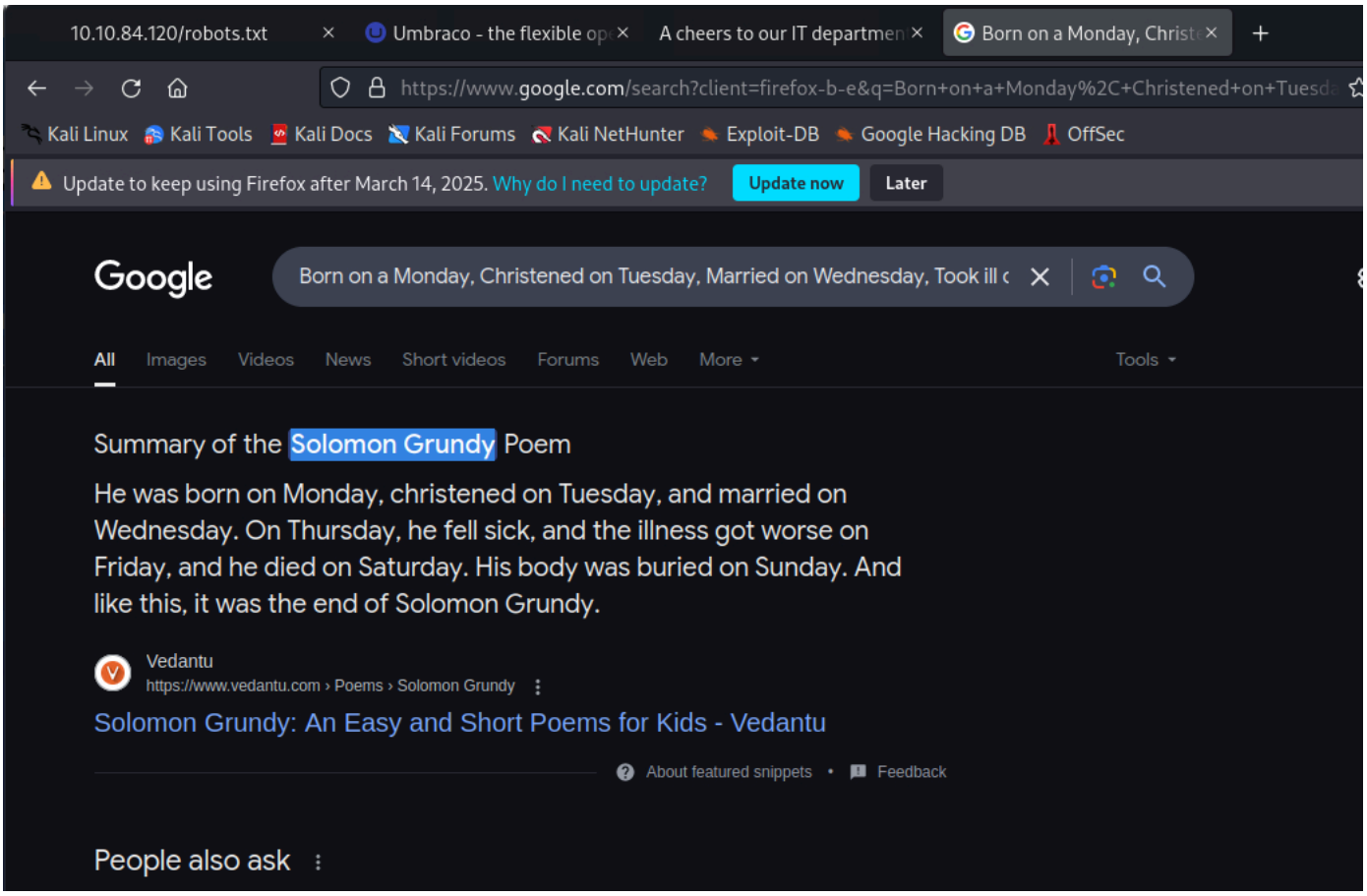
A cheers to our IT department

TUESDAY, DECEMBER 31, 2019

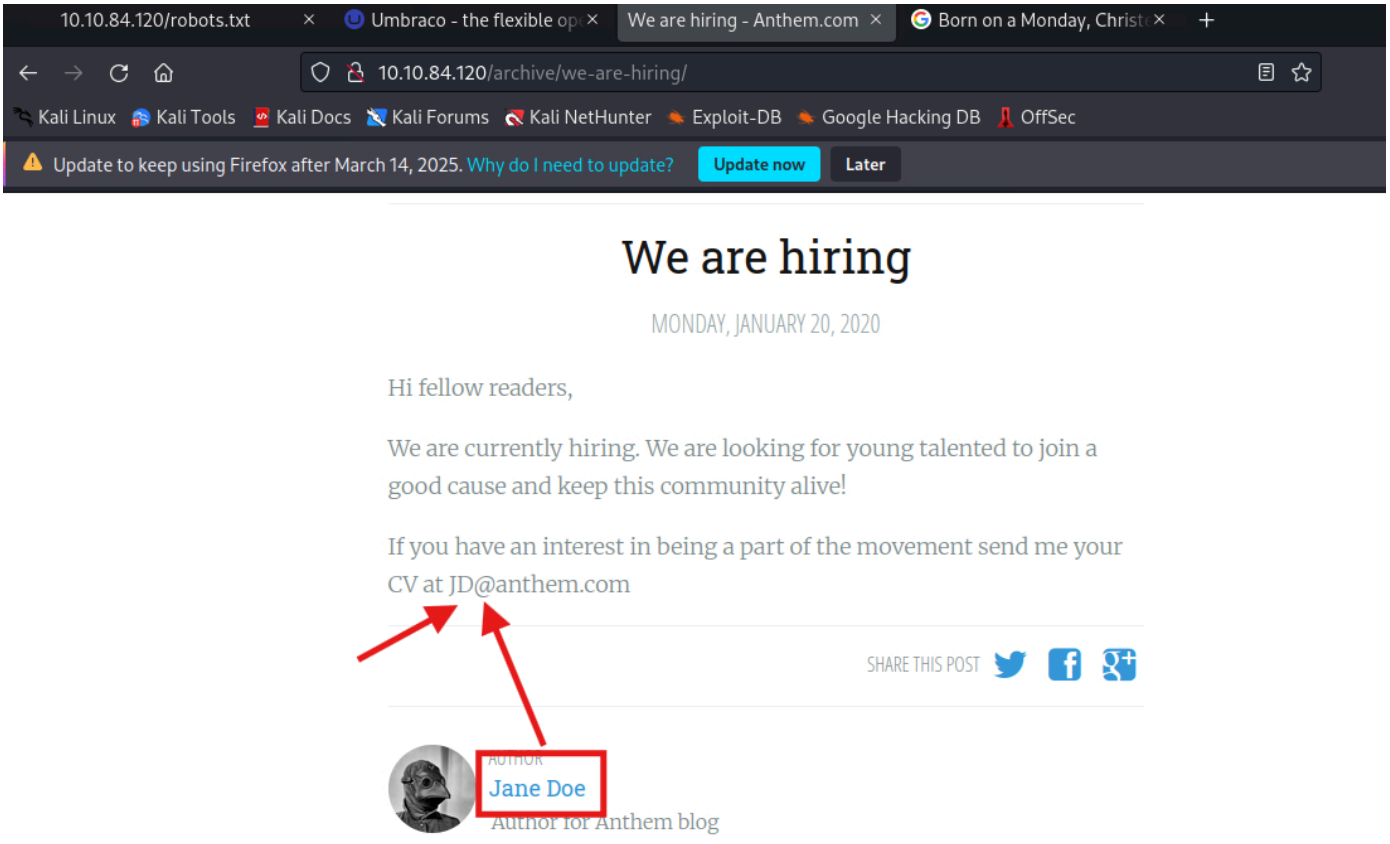
During our hard times our beloved admin managed to save our business by redesigning the entire website.

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...



Can we find find the email address of the administrator?

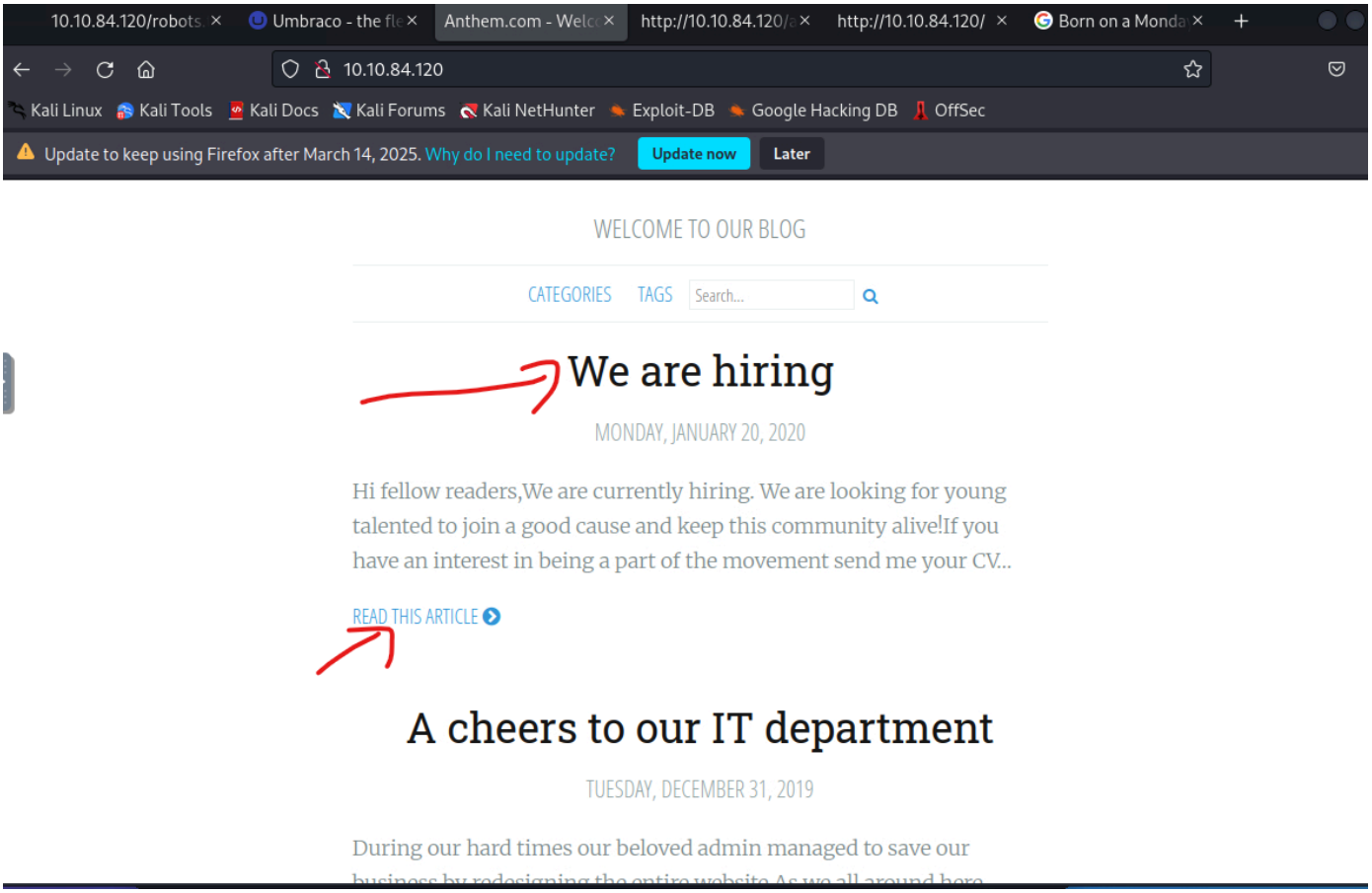


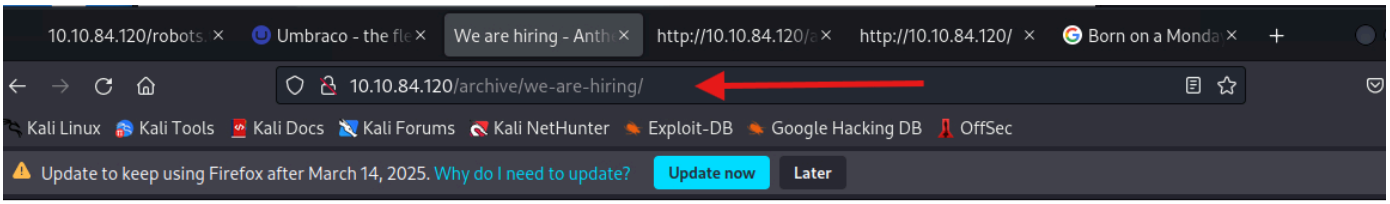
based on above information the Administartor email could be sg@anthem.com

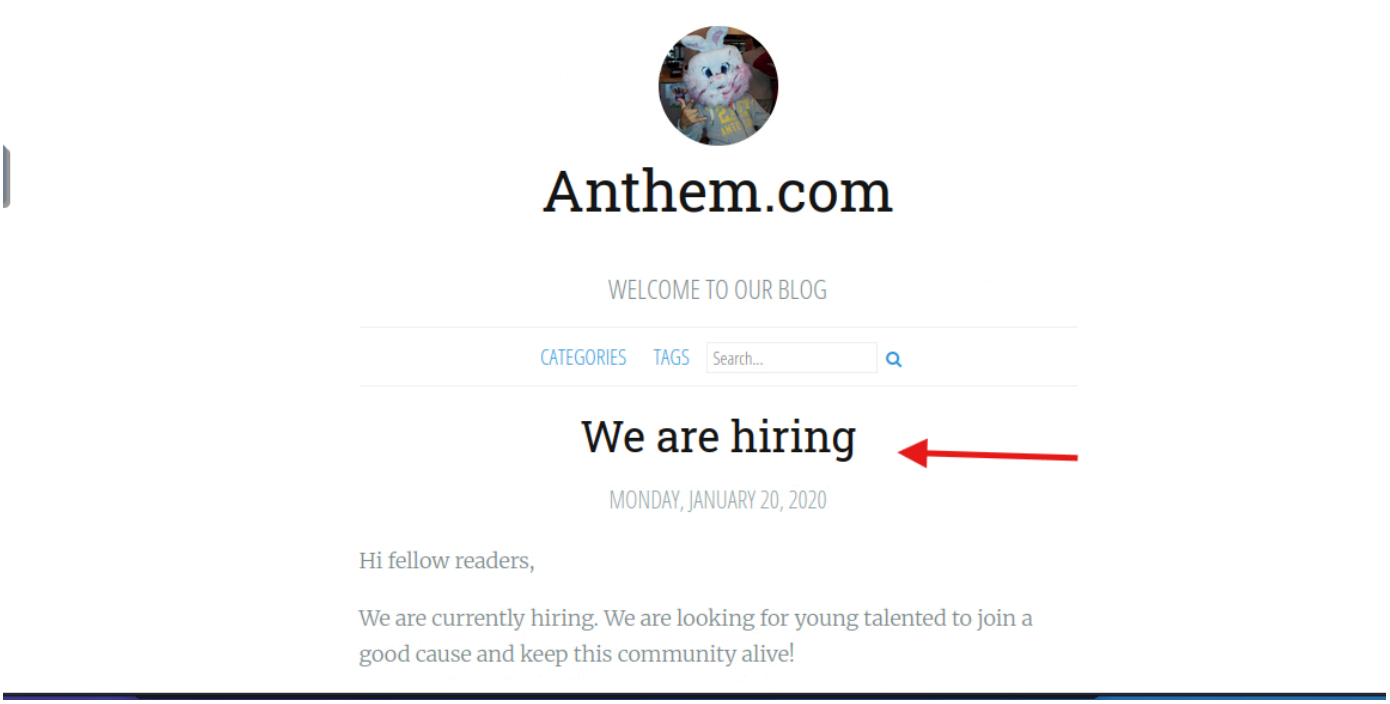
Task 2 --> Spot the flags

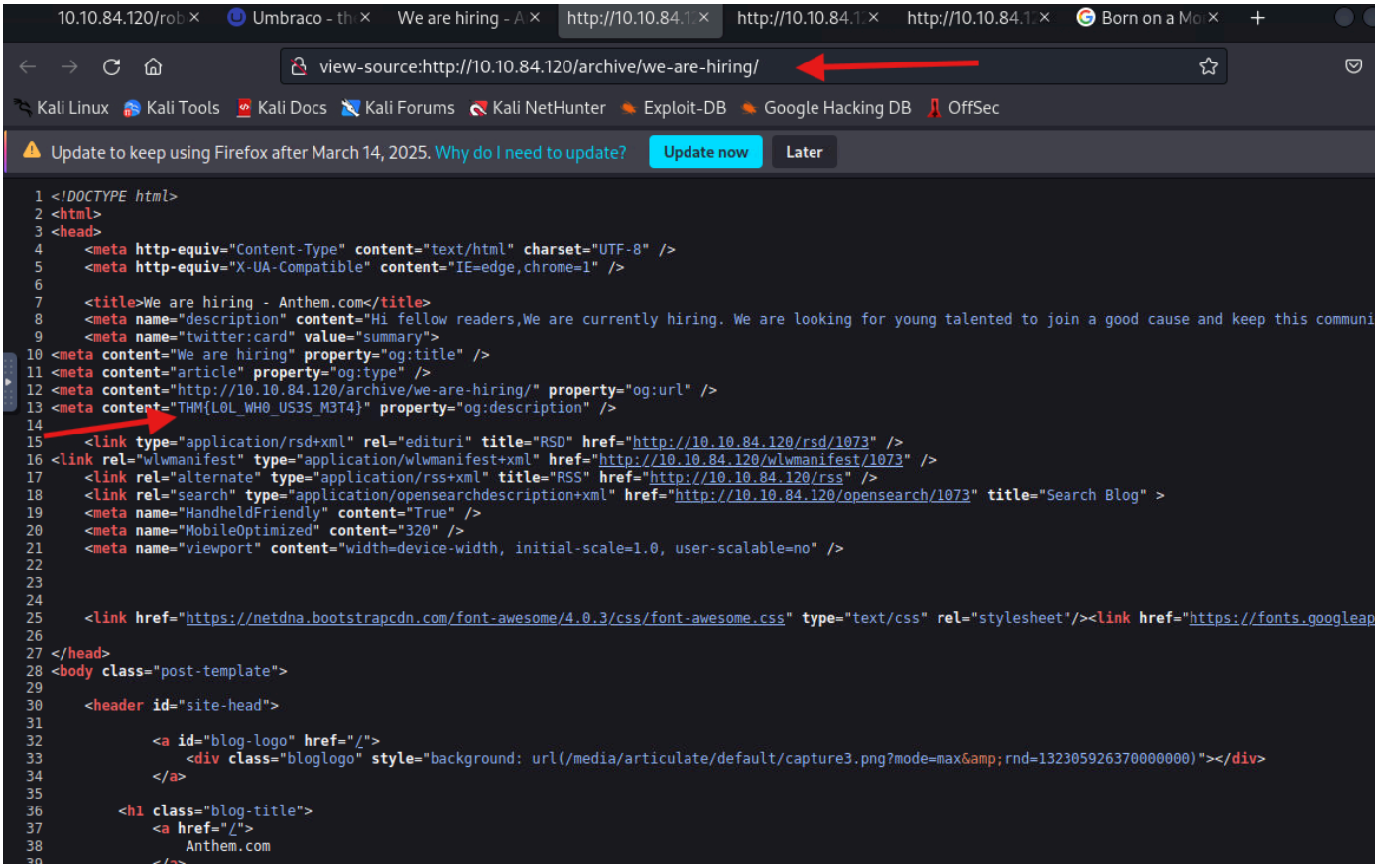
Anthem are hiring!

What is flag 1?

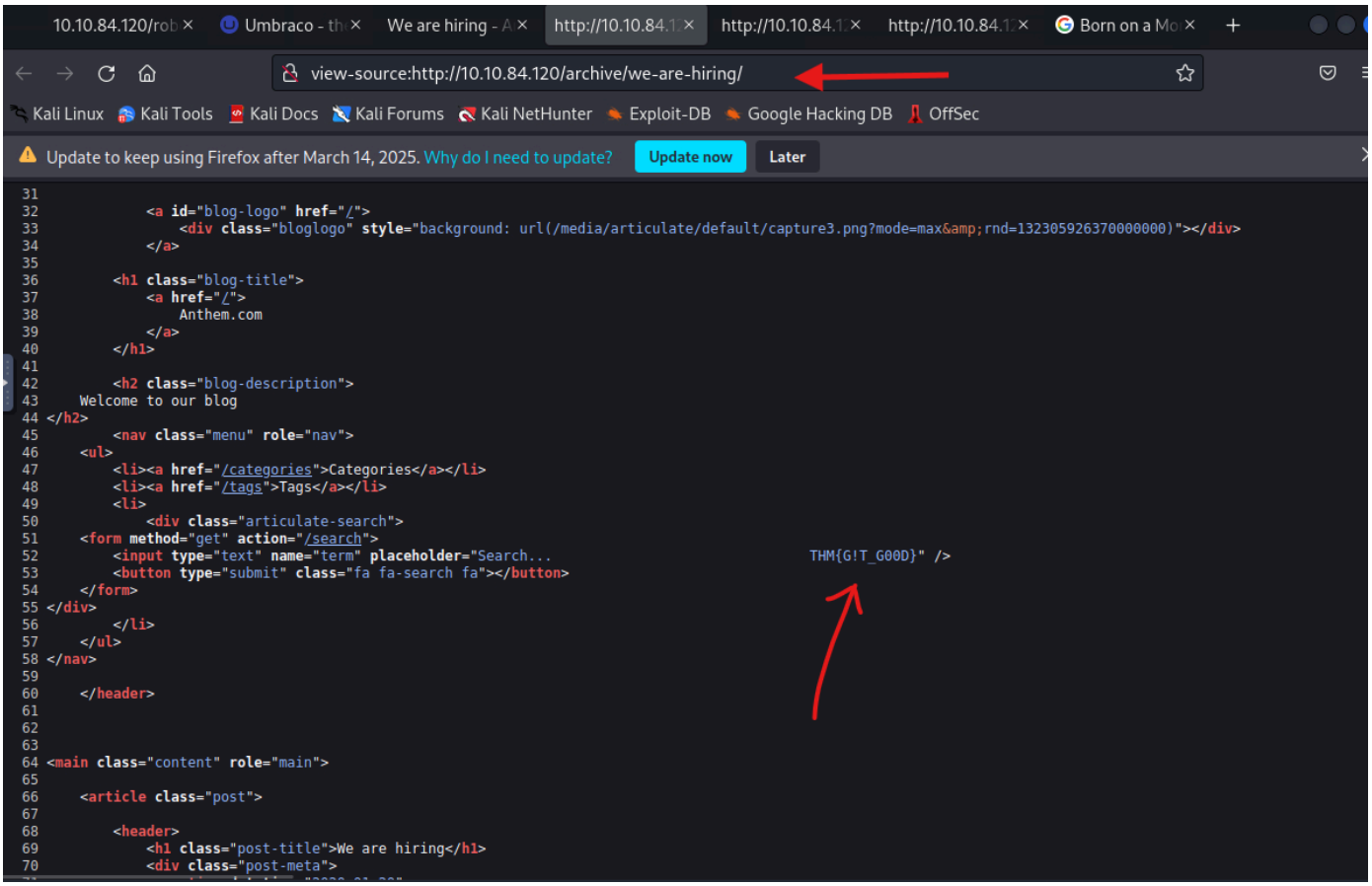




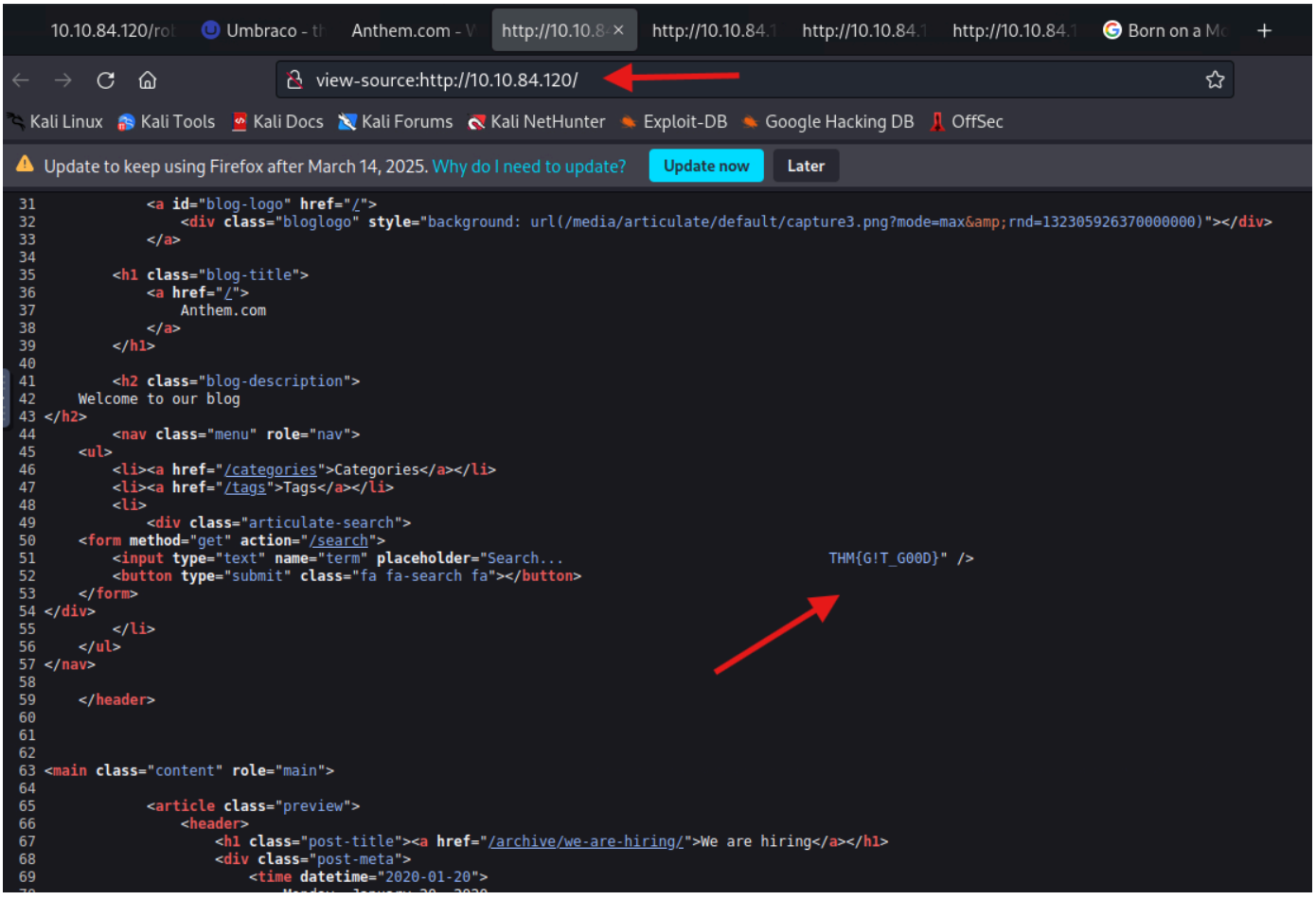




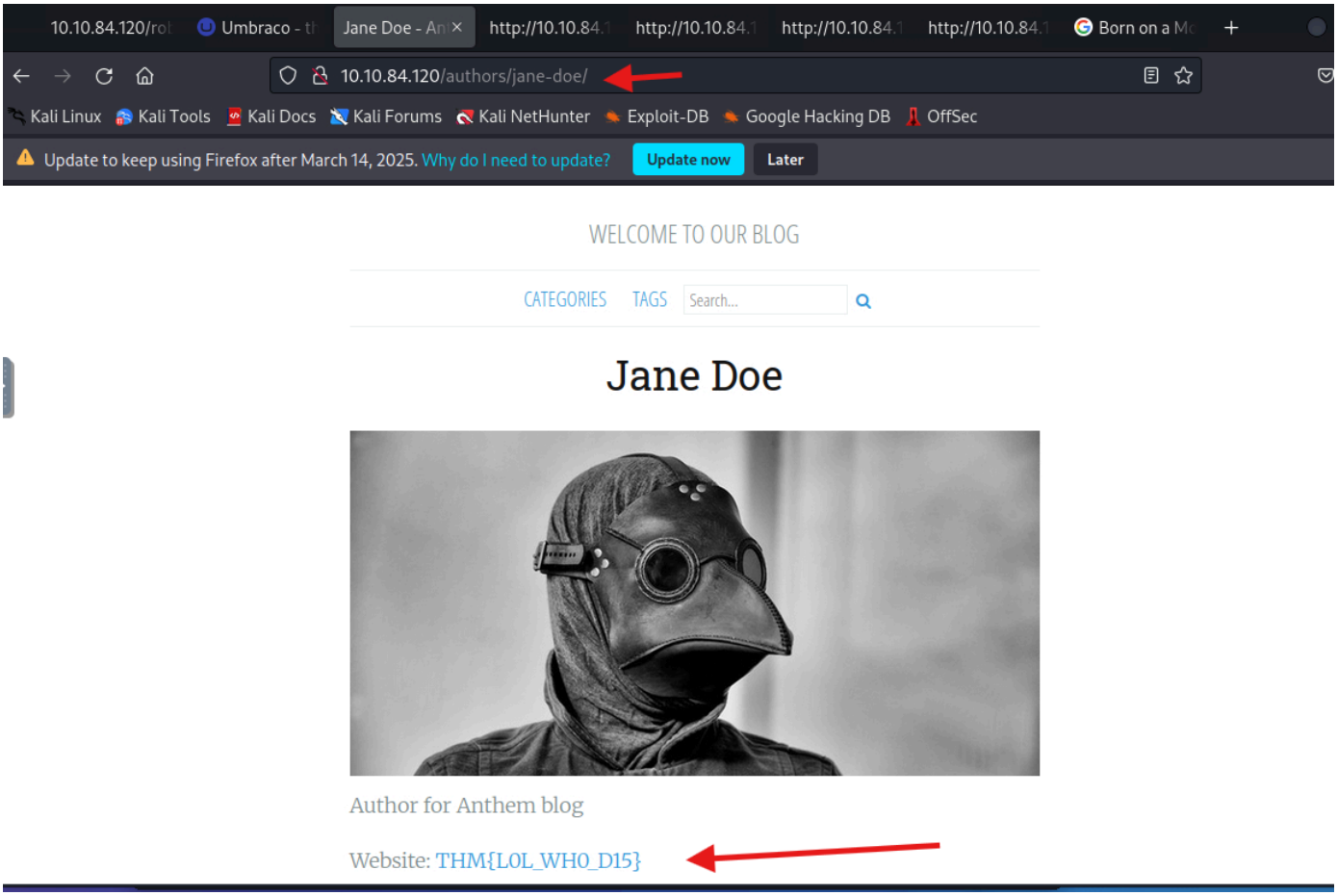
What is flag 2?



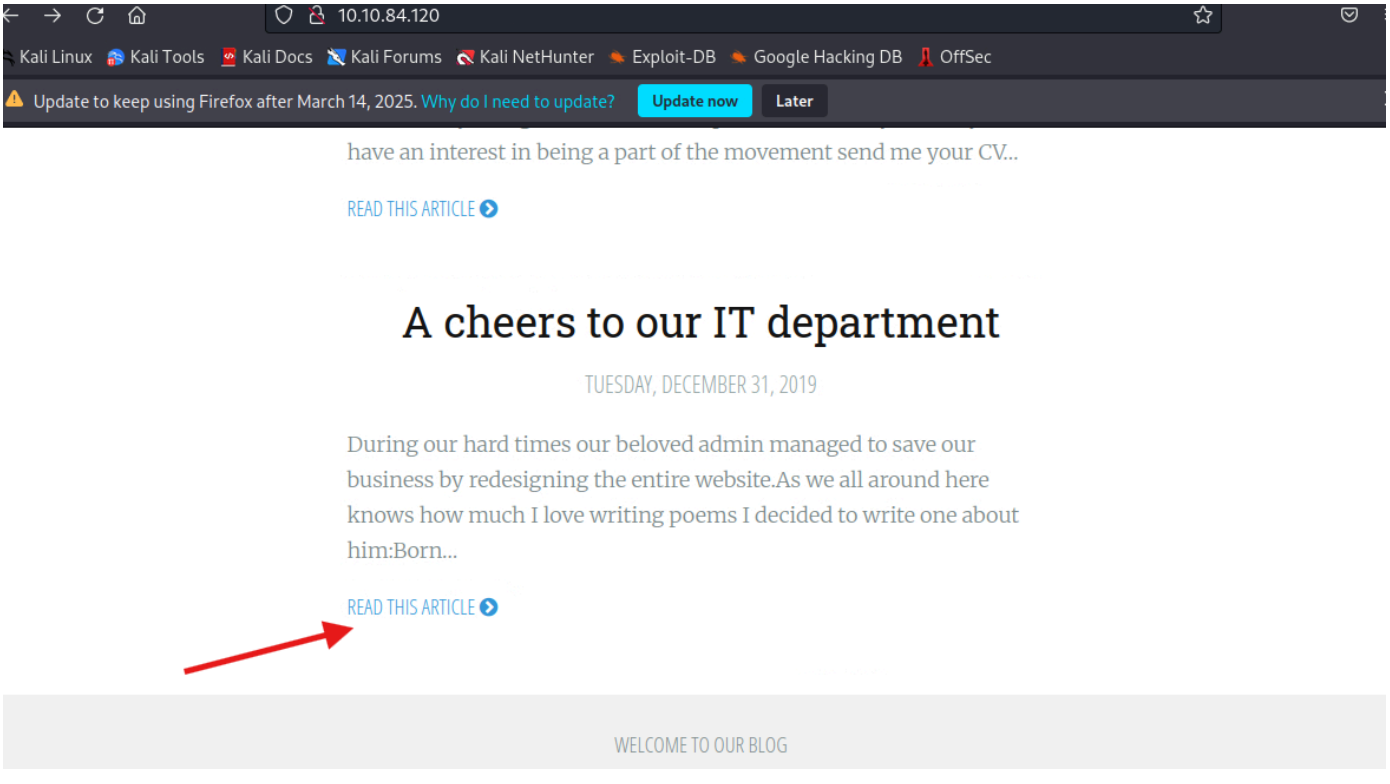
or in main page

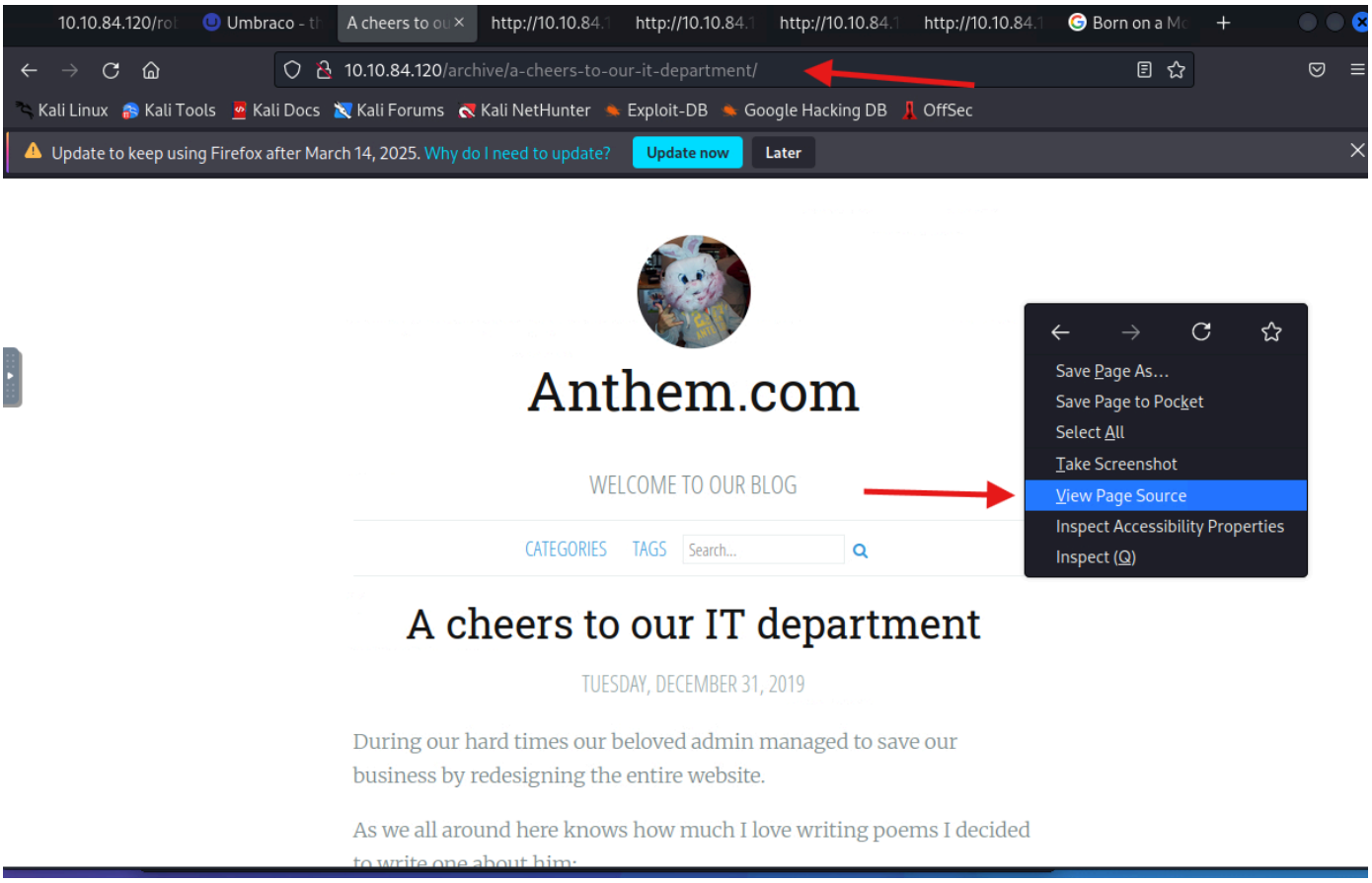


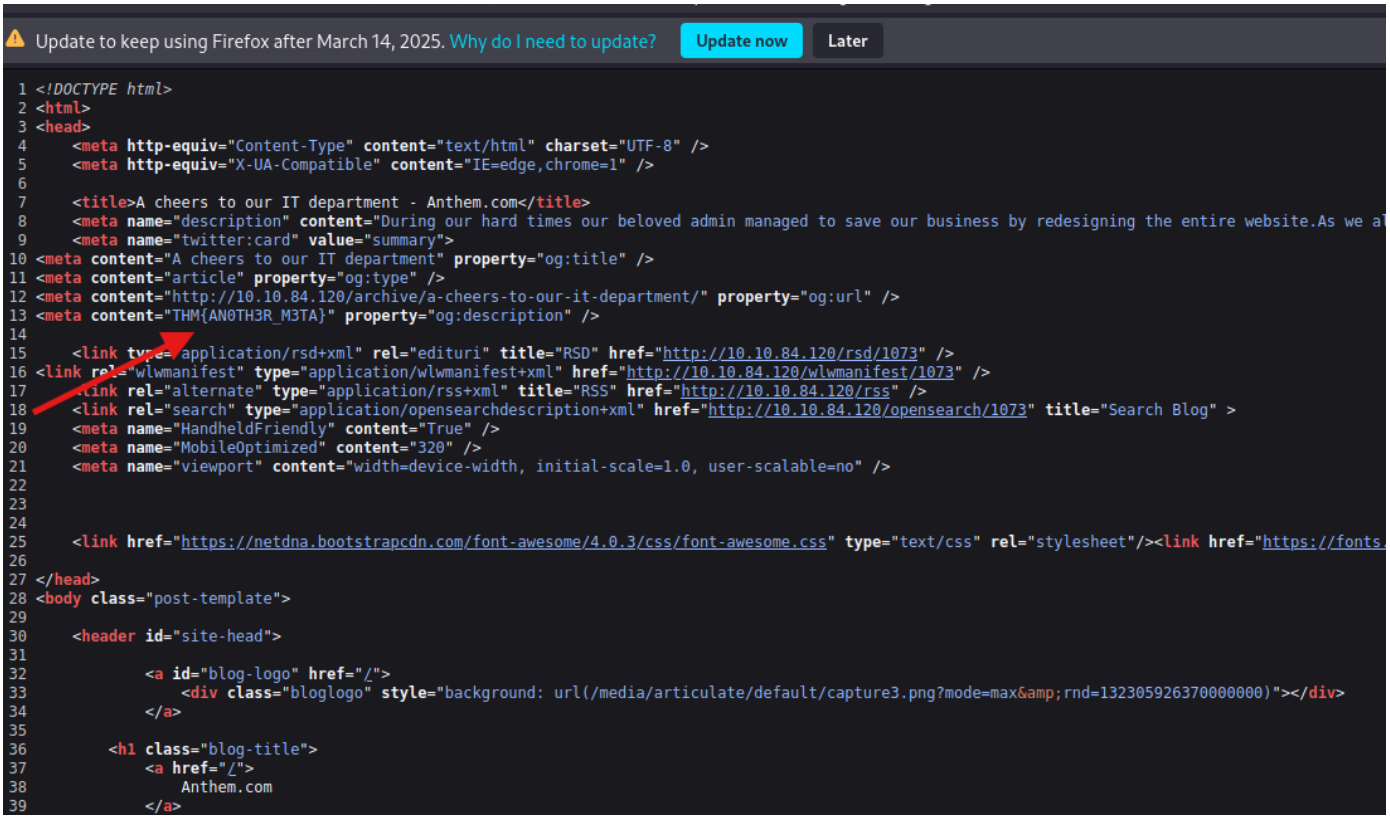
What is flag 3?



What is flag 4?







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?

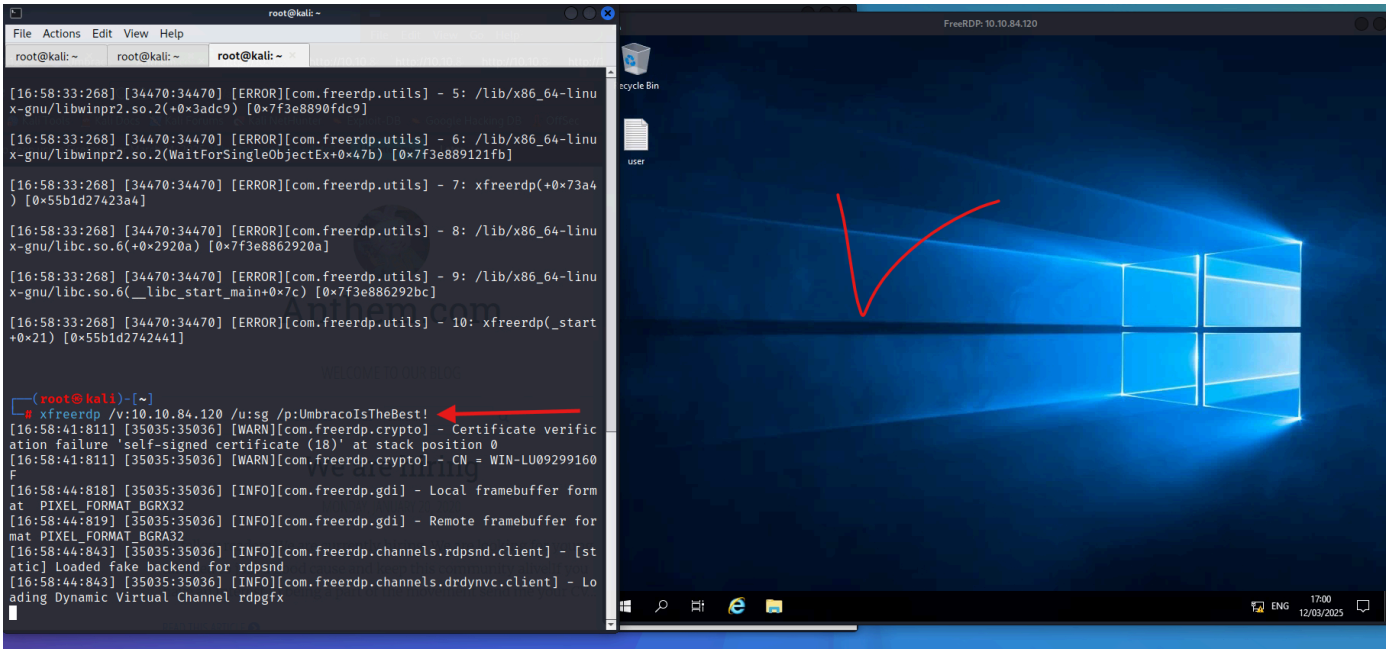
Lets do RDP

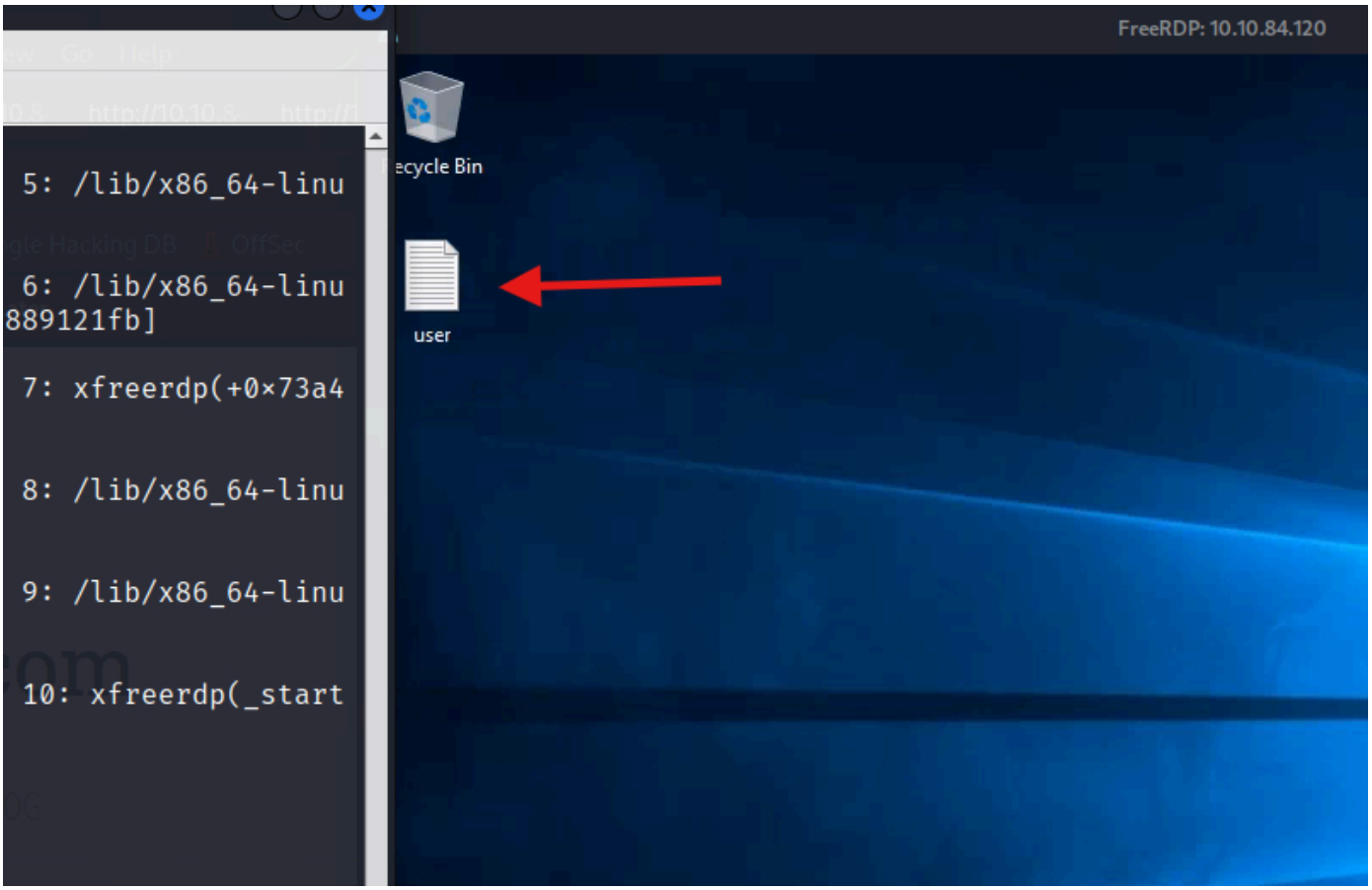
xfreerdp /v:10.10.84.120 /u:sg /p:UmbracoIsTheBest! /dynamic-resolution

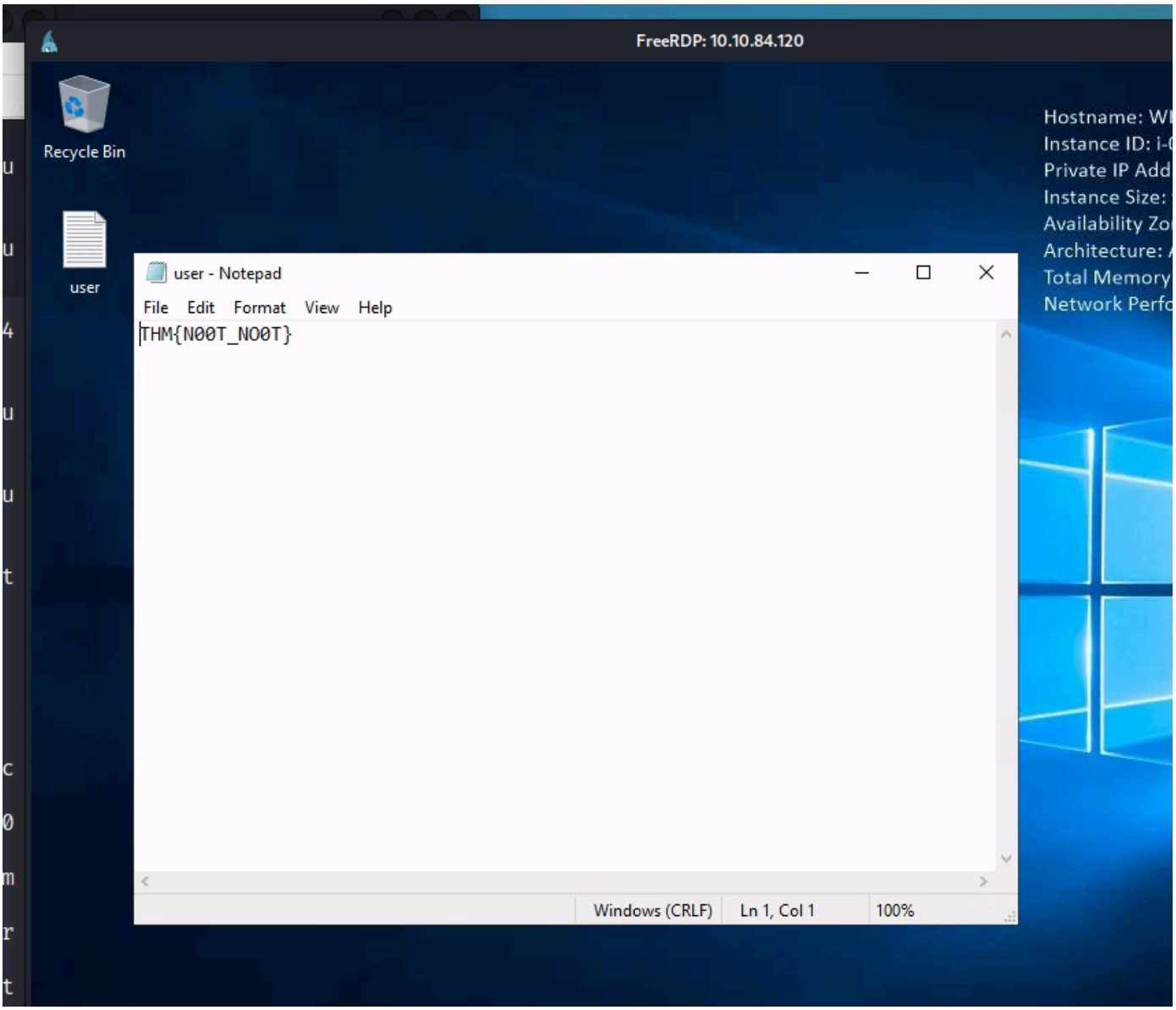
`/v` = "virtual desktop server" or "remote target"

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.




FreeRDP: 10.10.84.120
ecycle Bin
user
5: /lib/x86_64-linu
6: /lib/x86_64-linu
889121fb]
7: xfreerdp(+0×73a4
8: /lib/x86_64-linu
9: /lib/x86_64-linu
10: xfreerdp(_start



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
```

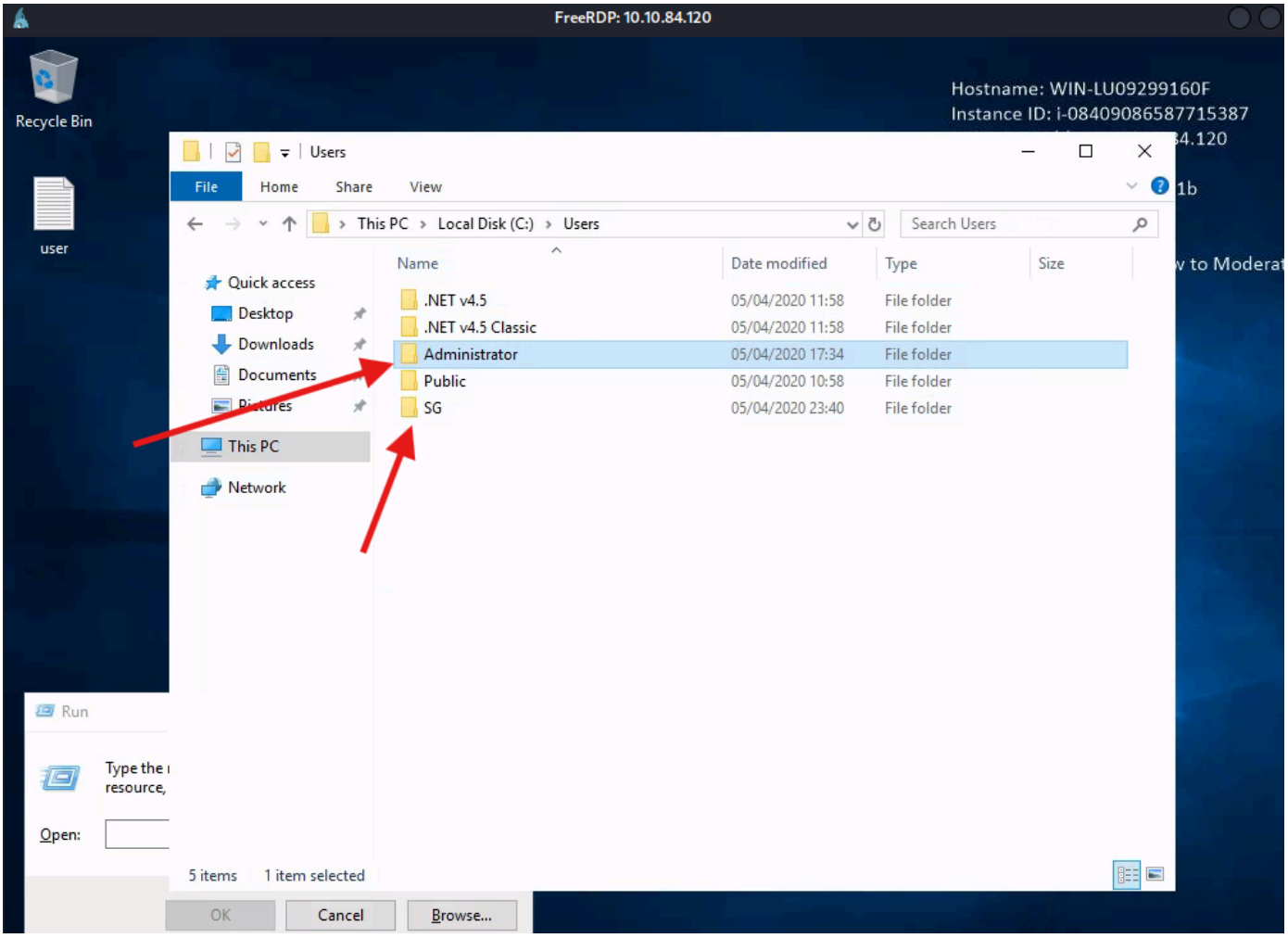
- This lists **all** files, including **hidden (H)** and **system (S)** files.

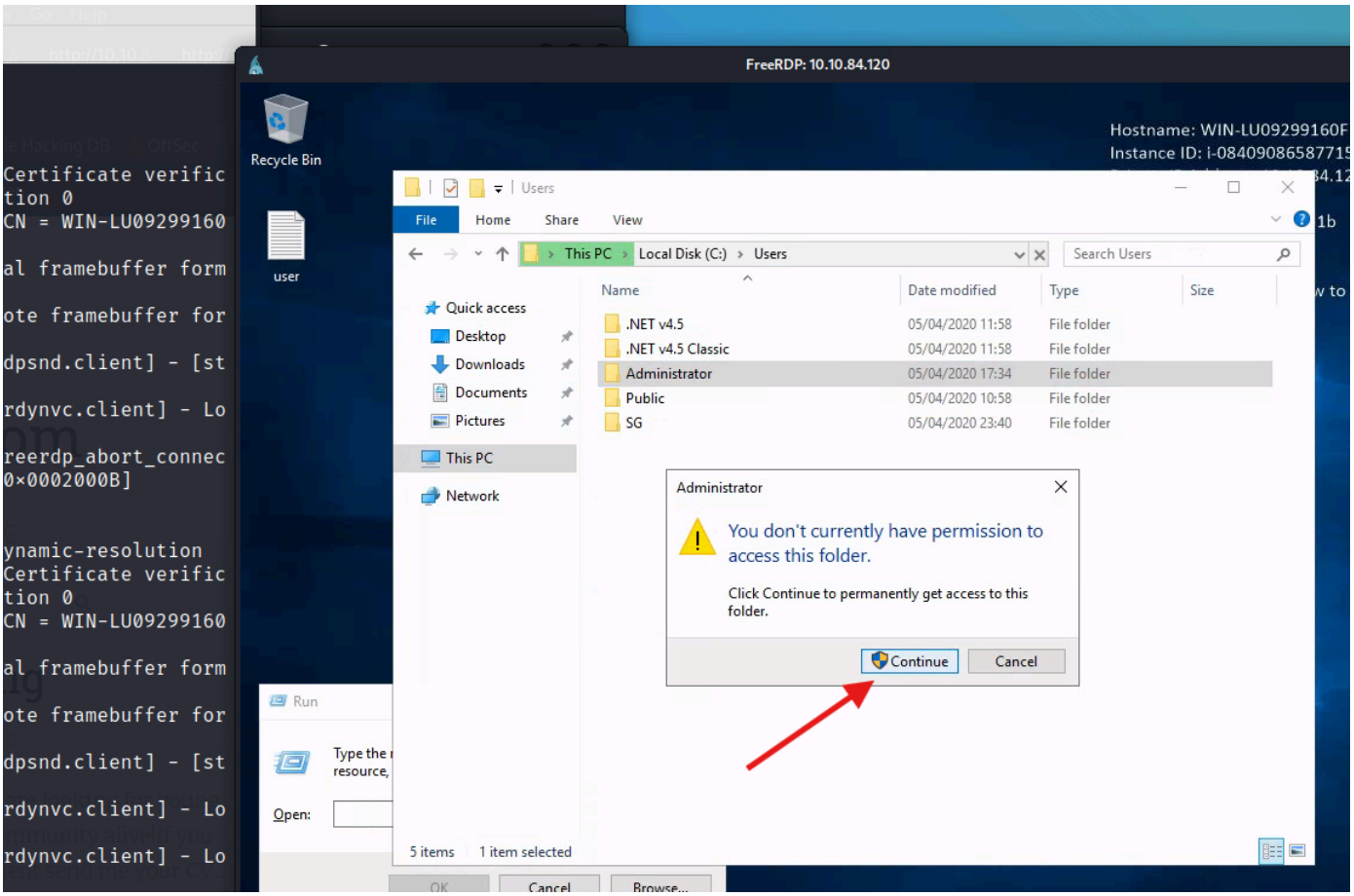
4️⃣ Find Hidden Files in a Specific Directory

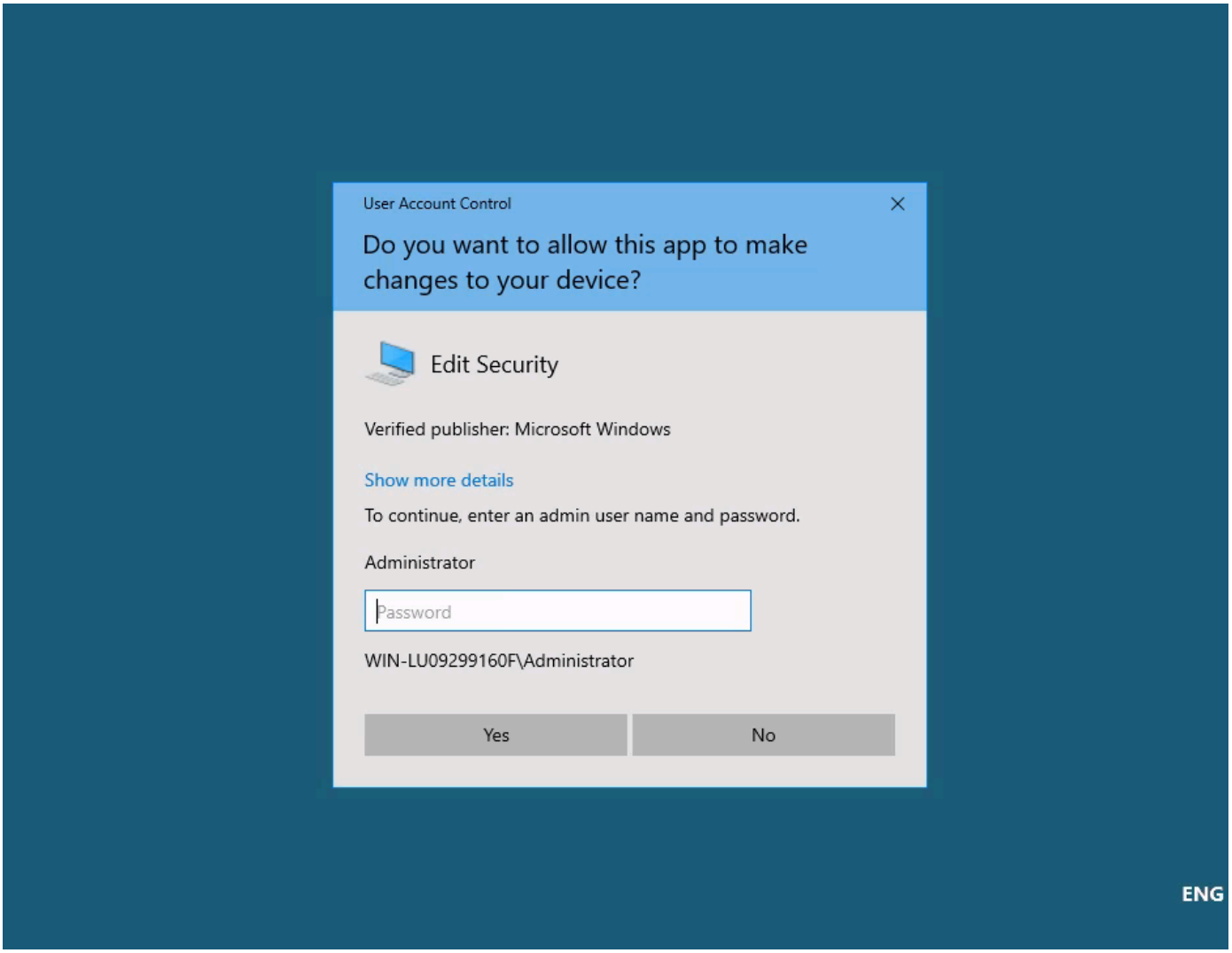
```
dir C:\Users\YourUsername\Desktop /A:H
```

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.



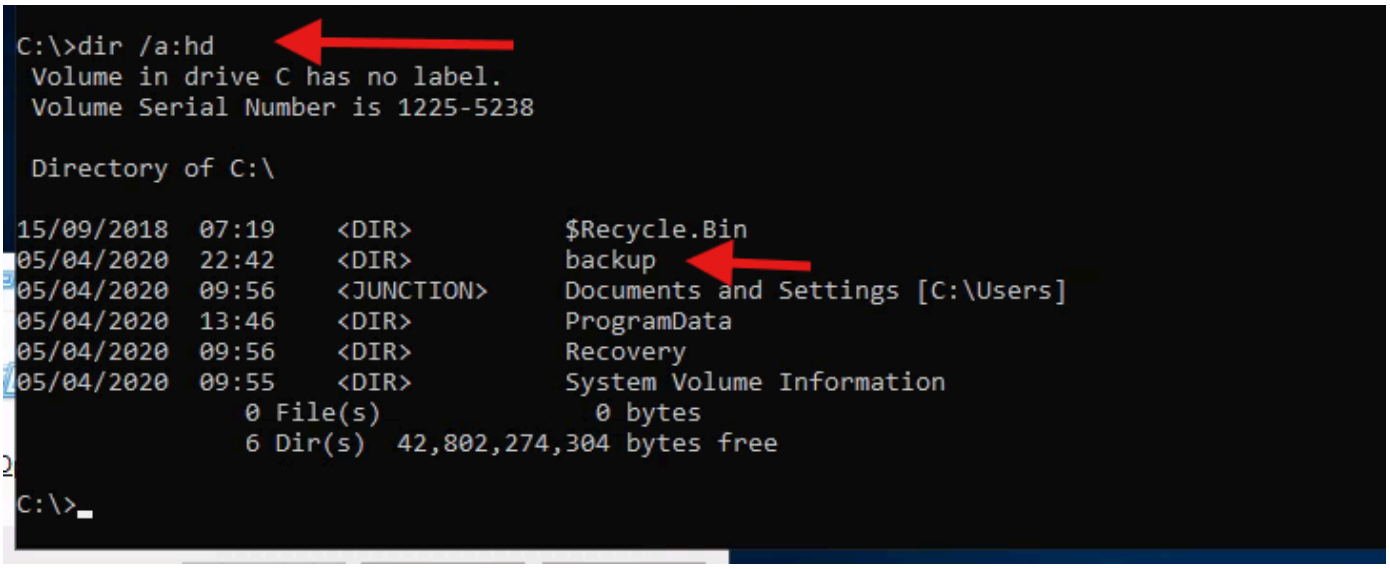

FreeRDP: 10.10.84.120
Recycle Bin
user
Hostname: WIN-LU09299160F
Instance ID: i-0840908658771
Users
File
Home
Share
View
This PC
Local Disk (C:)
Users
Search Users
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
.NET v4.5
.NET v4.5 Classic
Administrator
Public
SG
05/04/2020 11:58
05/04/2020 11:58
05/04/2020 17:34
05/04/2020 10:58
05/04/2020 23:40
File folder
5 items
1 item selected
Administrator
You don't currently have permission to access this folder.
Click Continue to permanently get access to this folder.
Continue
Cancel
Run
Open:
OK
Cancel
Browse...
Certificate verific
tion 0
CN = WIN-LU09299160
al framebuffer form
ote framebuffer for
dpsnd.client] - [st
rdynvc.client] - Lo
reerdp_abort_connec
0×0002000B]
ynamic-resolution
Certificate verific
tion 0
CN = WIN-LU09299160
al framebuffer form
ote framebuffer for
dpsnd.client] - [st
rdynvc.client] - Lo
rdynvc.client] - Lo

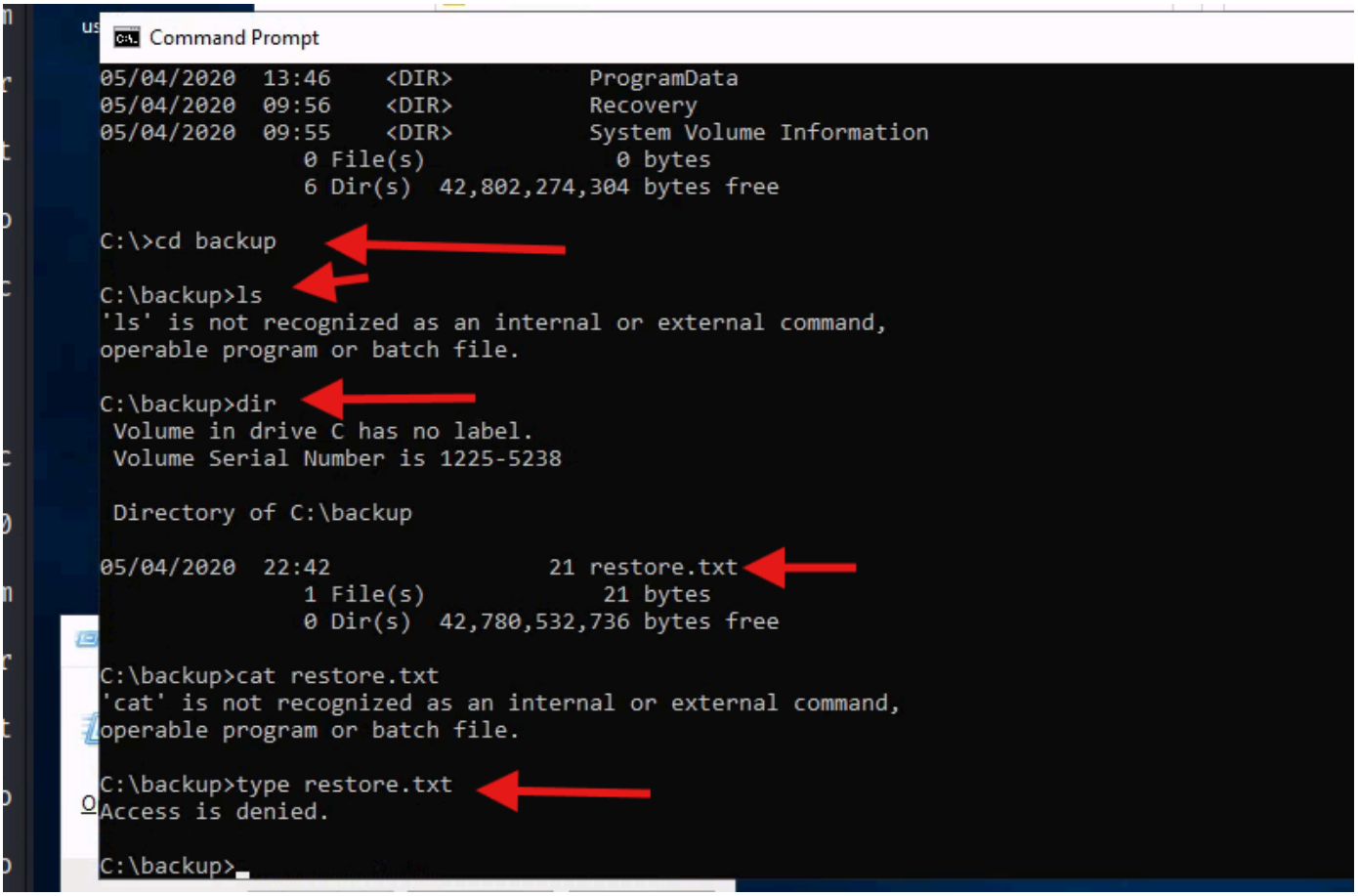

User Account Control
Do you want to allow this app to make changes to your device?
Edit Security
Verified publisher: Microsoft Windows
Show more details
To continue, enter an admin user name and password.
Administrator
Password
WIN-LU09299160F\Administrator
Yes
No
ENG

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.





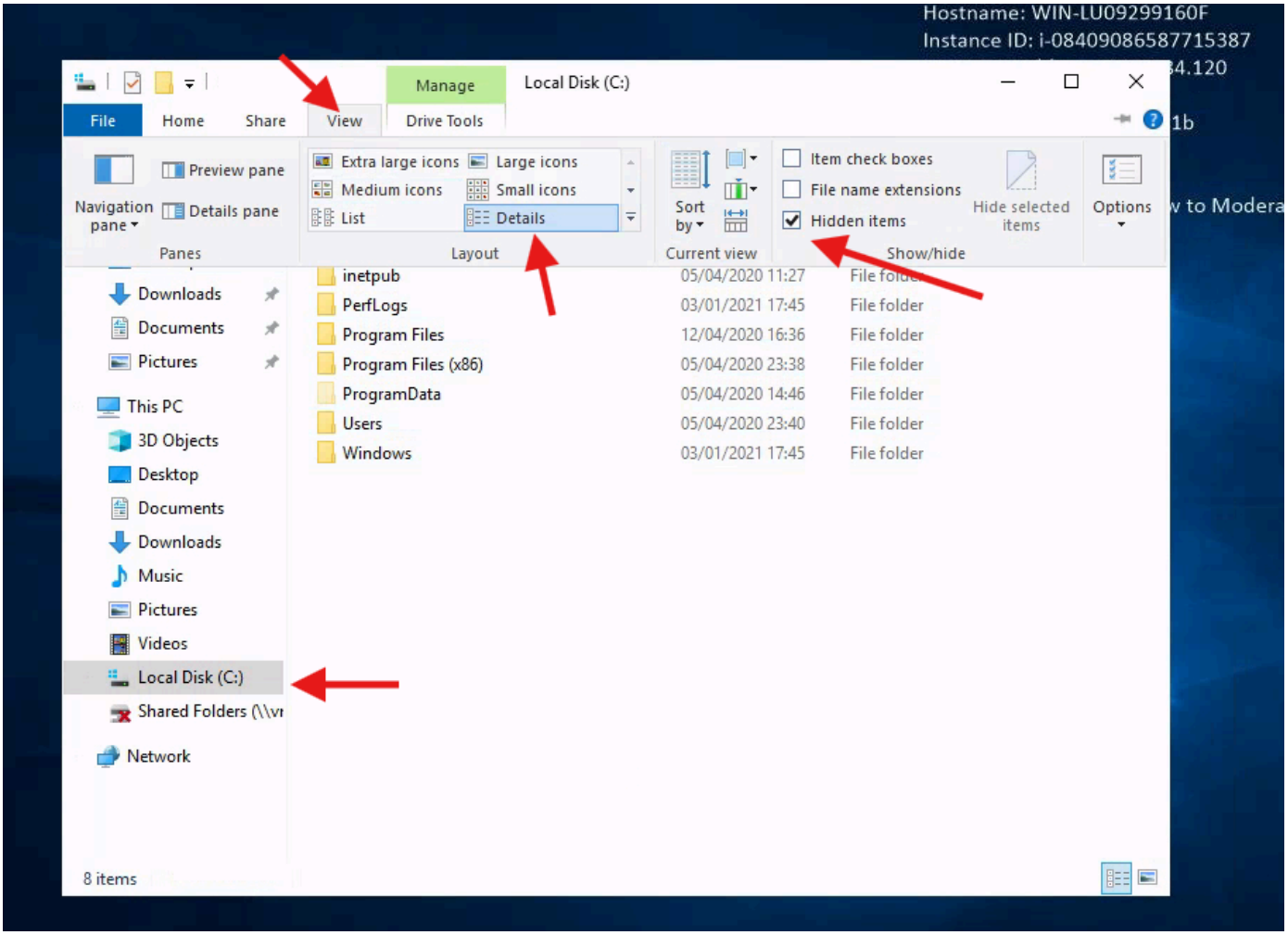
So we don't have permission to view it, but I mentioned earlier that poor permissions can help us… maybe we can change those permissions?

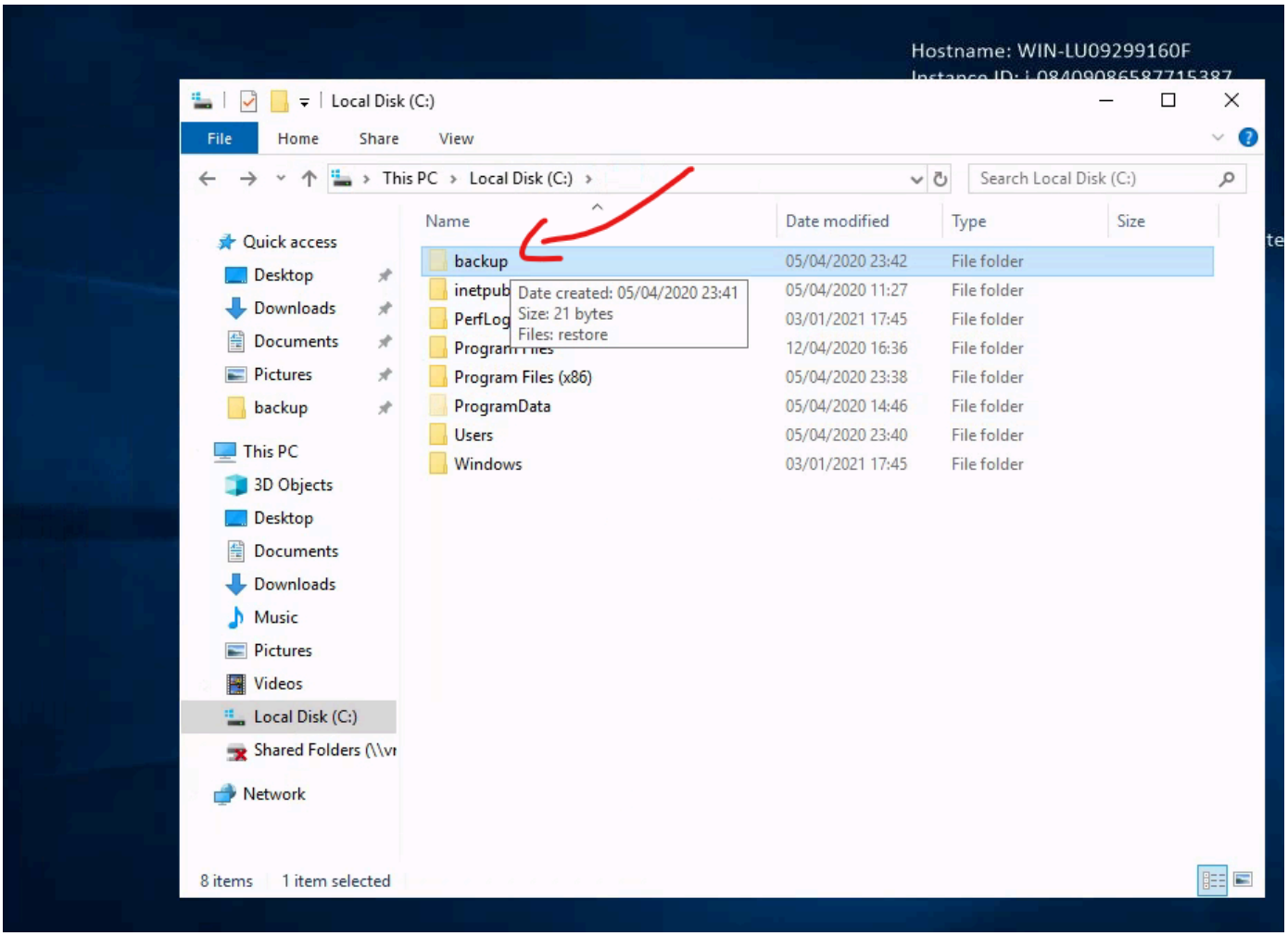
There are two ways we can do this. We can use the CLI or GUI. I will showcase both. Overtime, CLI becomes the quicker way — but the GUI will always be ‘easier’.

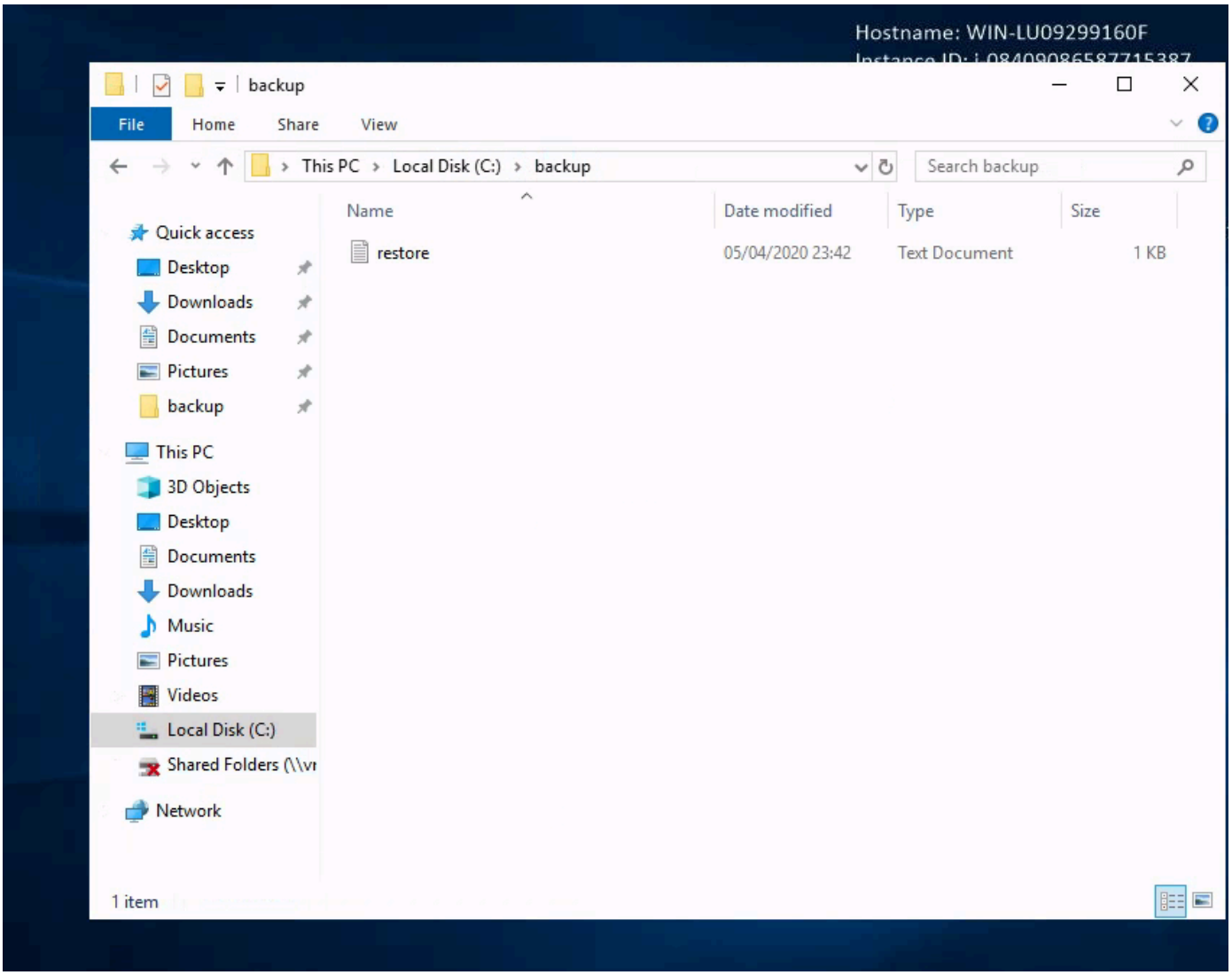
However, it seems CLI may not be possible?

So with that in mind, GUI it is.

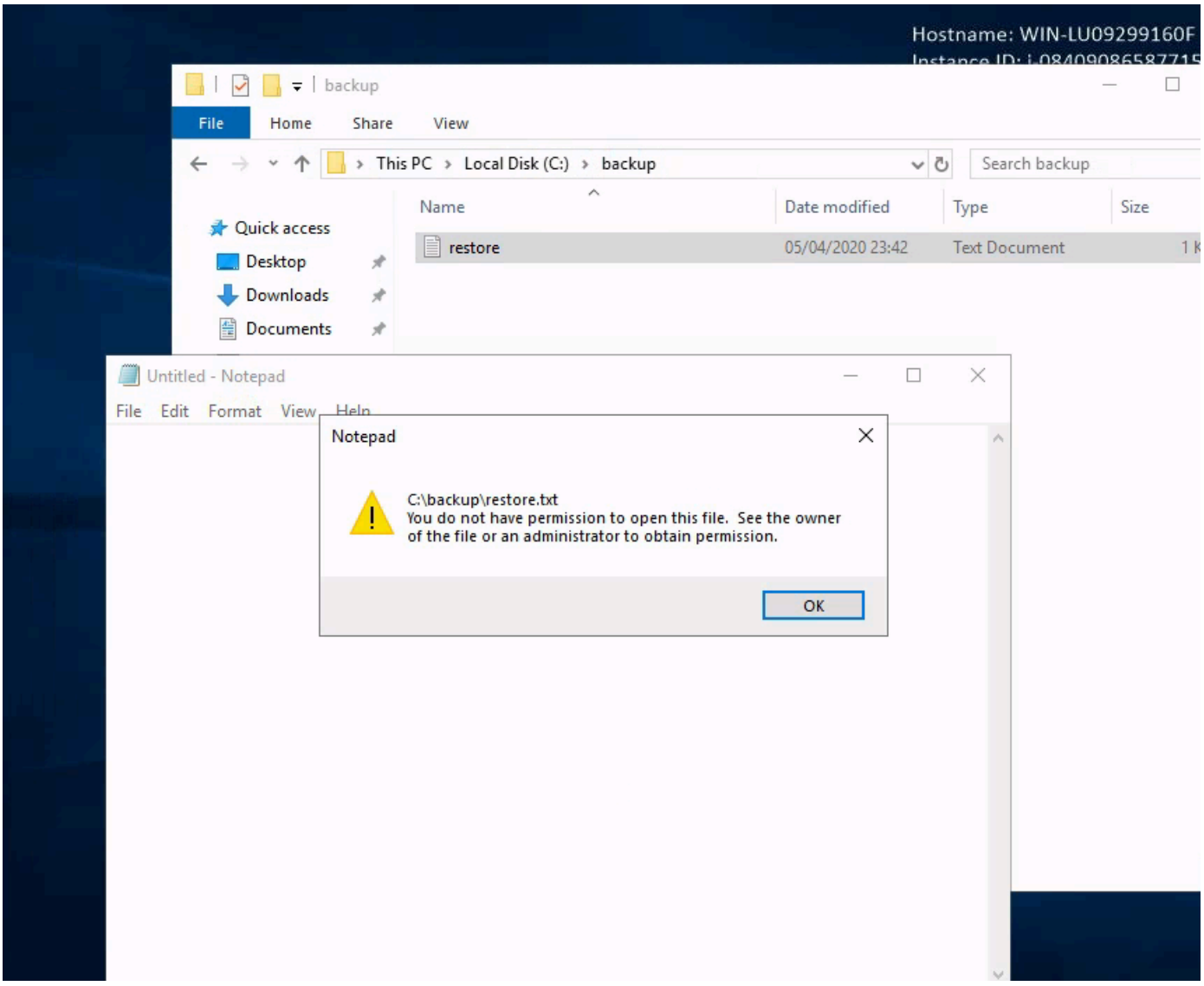
Let’s enable hidden files to be seen in the GUI

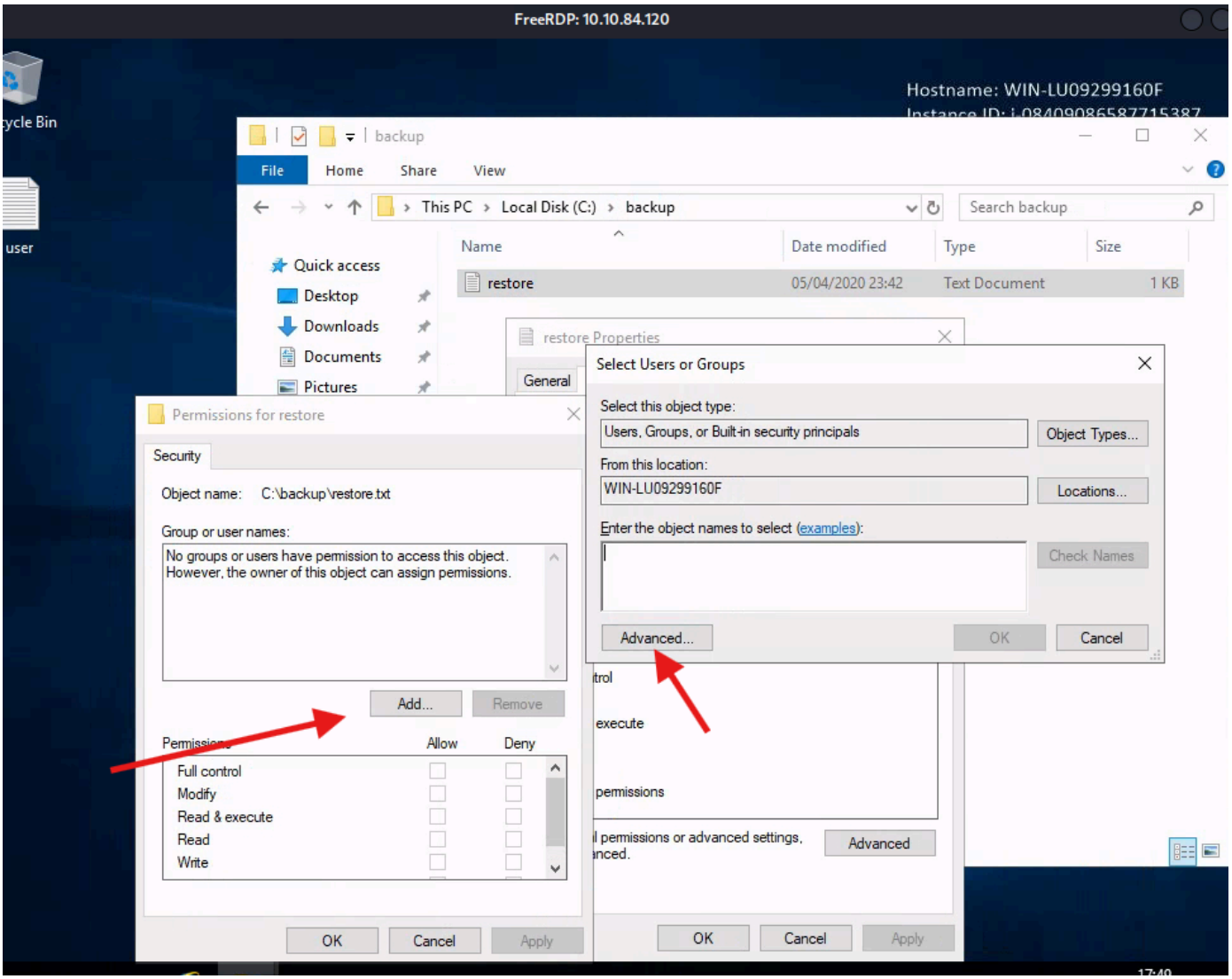



Hostname: WIN-LU09299160F
Local Disk (C:)
File
Home
Share
View
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
backup
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Shared Folders (\\vr
Network
Name
Date modified
Type
Size
backup 05/04/2020 23:42 File folder
inetpub 05/04/2020 11:27 File folder
PerfLog 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
Date created: 05/04/2020 23:41
Size: 21 bytes
Files: restore
8 items
1 item selected

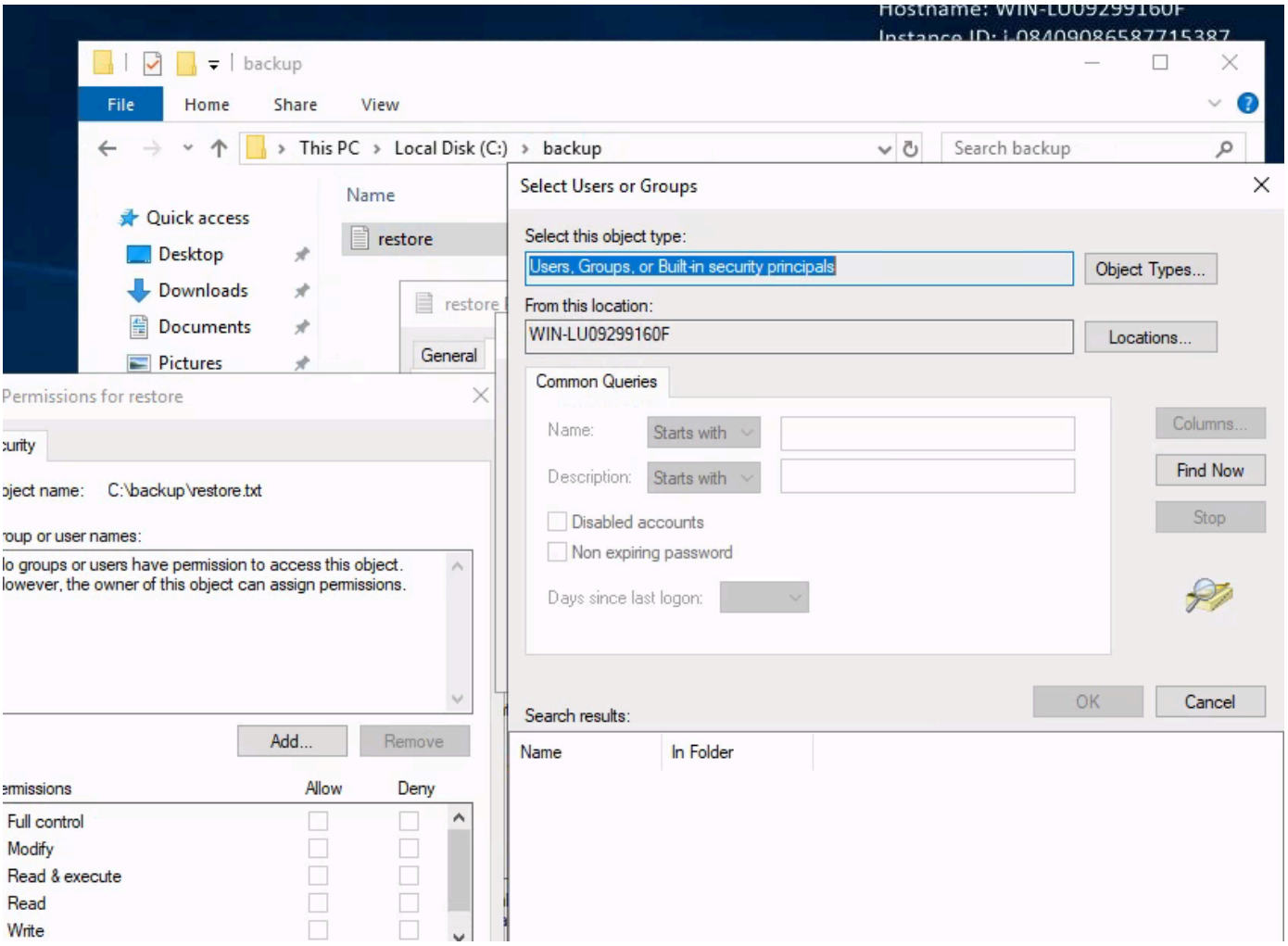


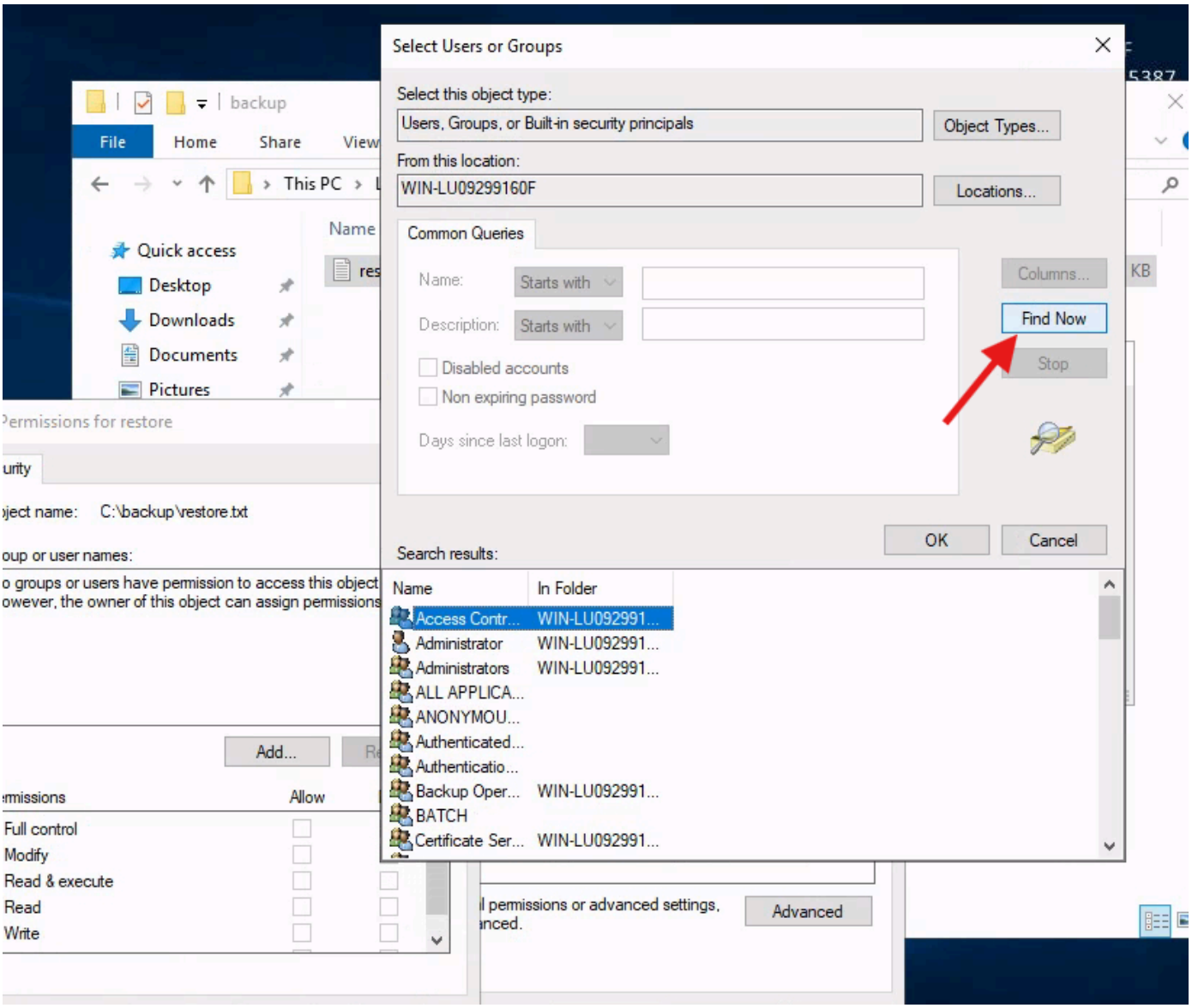
we got permission issue

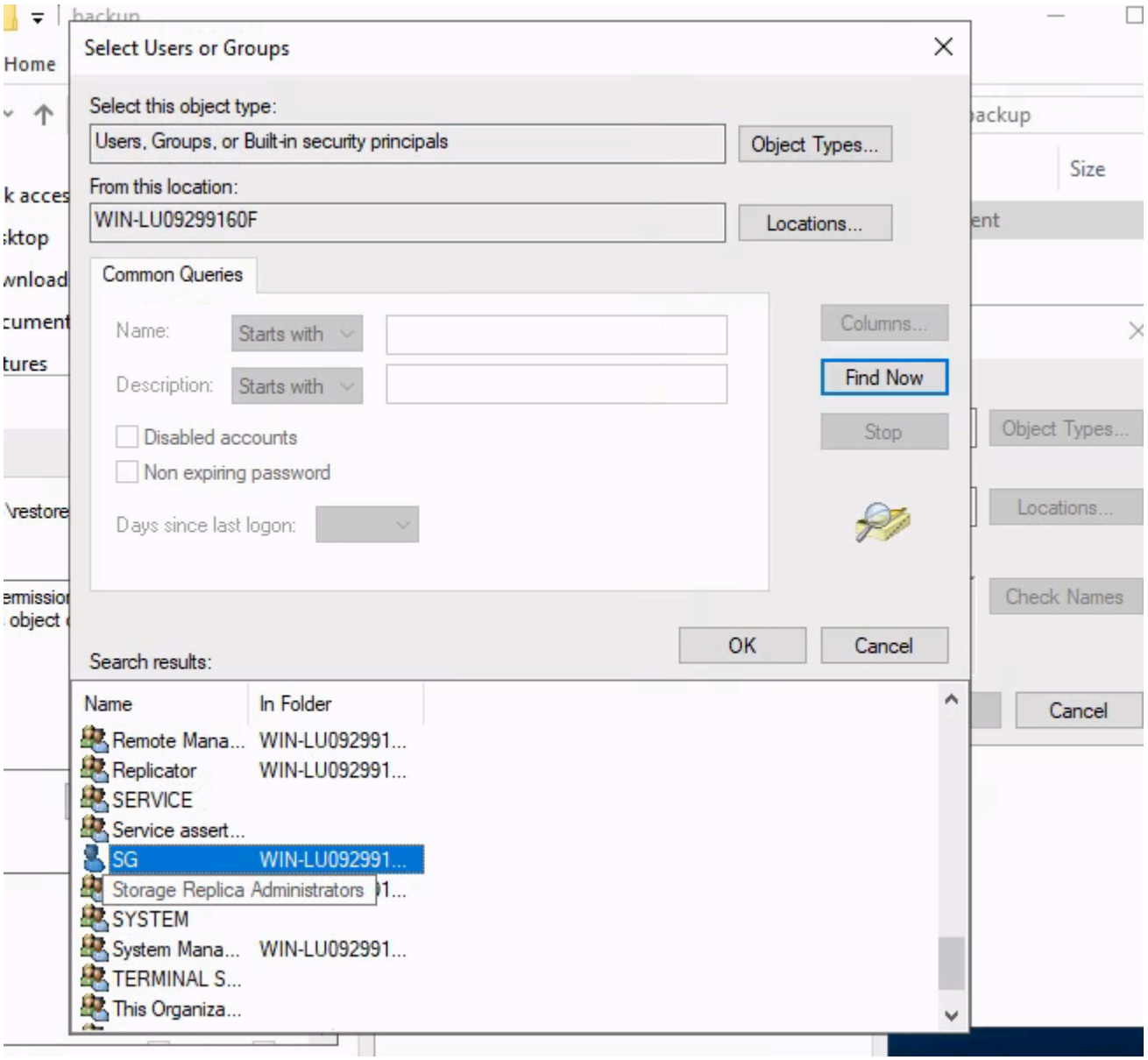

Hostname: WIN-LU09299160F
backup
File
Home
Share
View
This PC › Local Disk (C:) › backup
Search backup
Quick access
Desktop
Downloads
Documents
Name
Date modified
Type
Size
restore
05/04/2020 23:42
Text Document
Untitled - Notepad
File Edit Format View Help
Notepad
C:\backup\restore.txt
You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.
OK



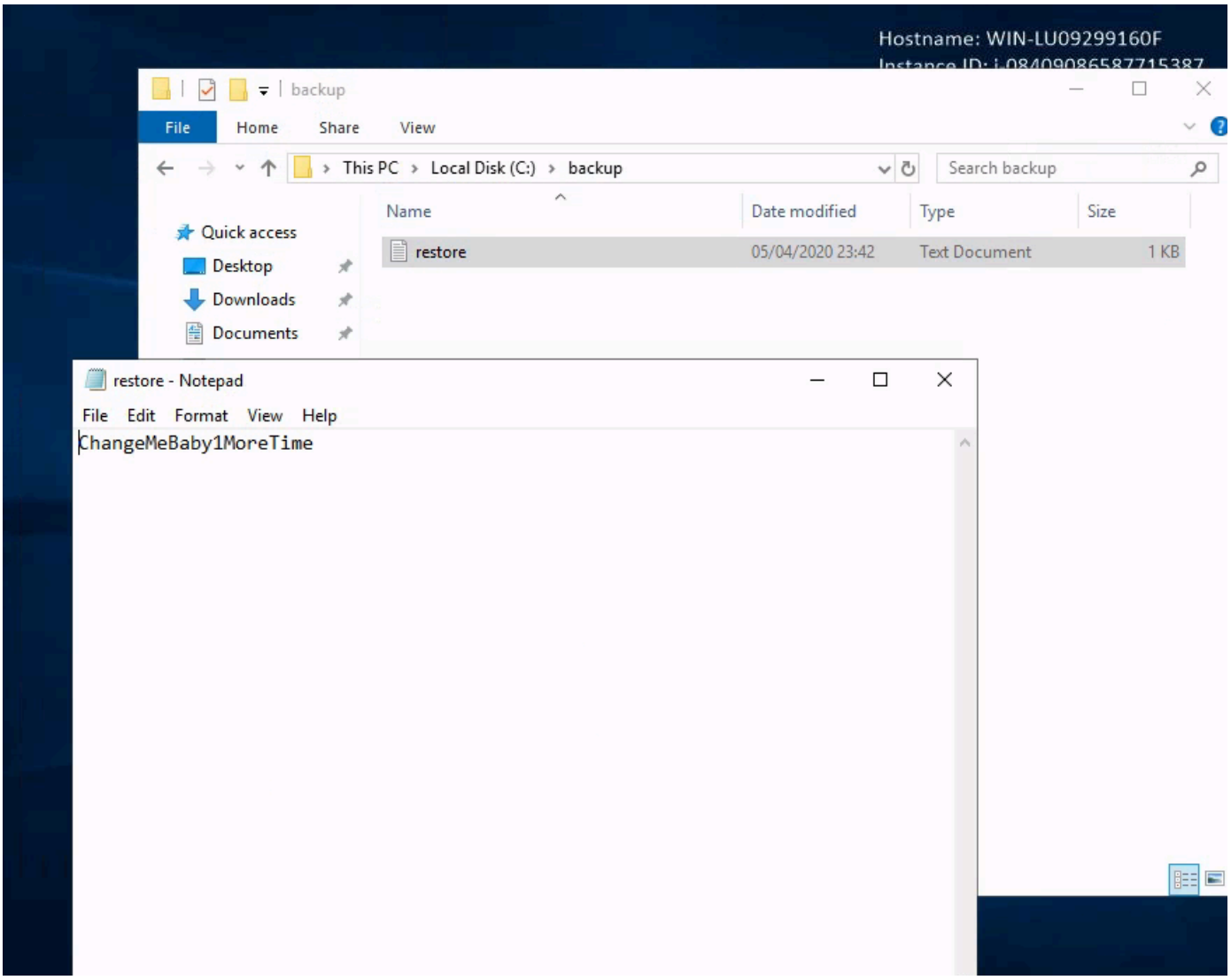
We need to add our user to this list. We can find our user by clicking ‘Advanced’.


Hostname: WIN-LU09299160F
backup
File
Home
Share
View
This PC
Local Disk (C:)
backup
Search backup
Quick access
Desktop
Downloads
Documents
Pictures
Name
restore
General
Permissions for restore
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.
Add...
Remove
Permissions
Allow
Deny
Full control
Modify
Read & execute
Read
Write
Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
WIN-LU09299160F
Locations...
Common Queries
Name:
Starts with
Description:
Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name
In Folder


Select Users or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
WIN-LU09299160F
Locations...
Common Queries
Name: Starts with
Description: Starts with
Disabled accounts
Non expiring password
Days since last logon:
Columns...
Find Now
Stop
OK
Cancel
Search results:
Name
In Folder
Access Contr... WIN-LU092991...
Administrator WIN-LU092991...
Administrators WIN-LU092991...
ALL APPLICA...
ANONYMOU...
Authenticated...
Authenticatio...
Backup Oper... WIN-LU092991...
BATCH
Certificate Ser... WIN-LU092991...
backup
File
Home
Share
View
This PC
Quick access
Desktop
Downloads
Documents
Pictures
Permissions for restore
C:\backup\restore.txt
Add...
Allow
Full control
Modify
Read & execute
Read
Write
Advanced



Make sure you click apply!

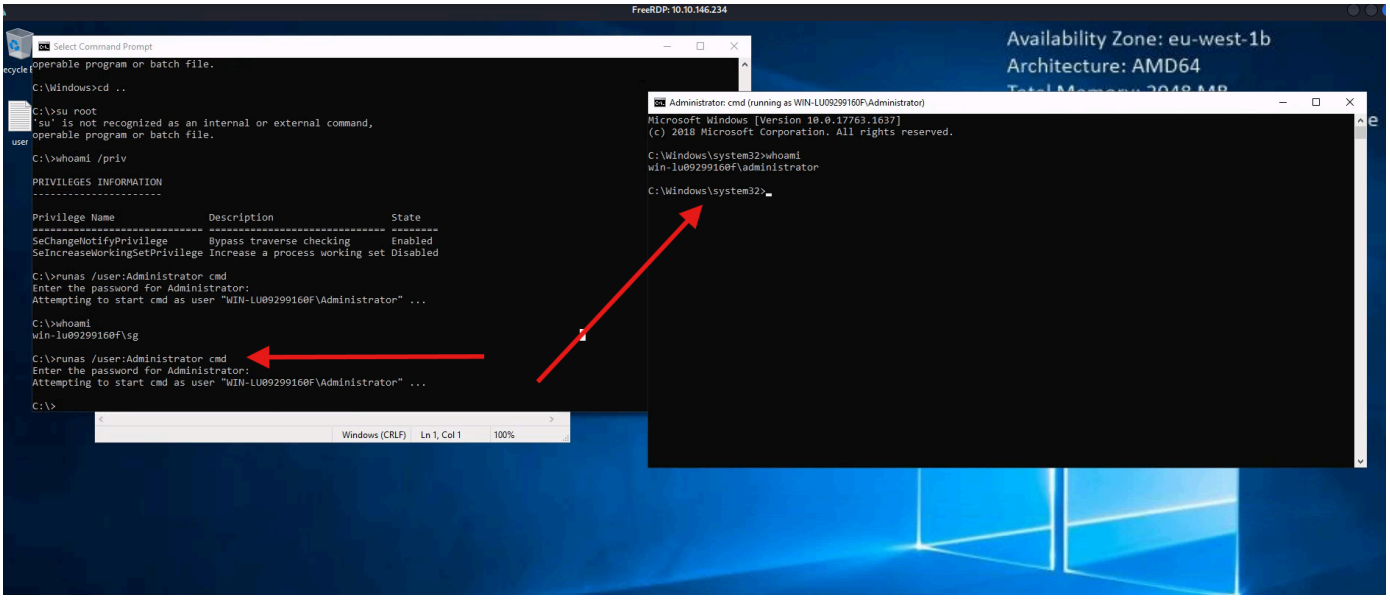


Escalate your privileges to root, what is the contents of root.txt?

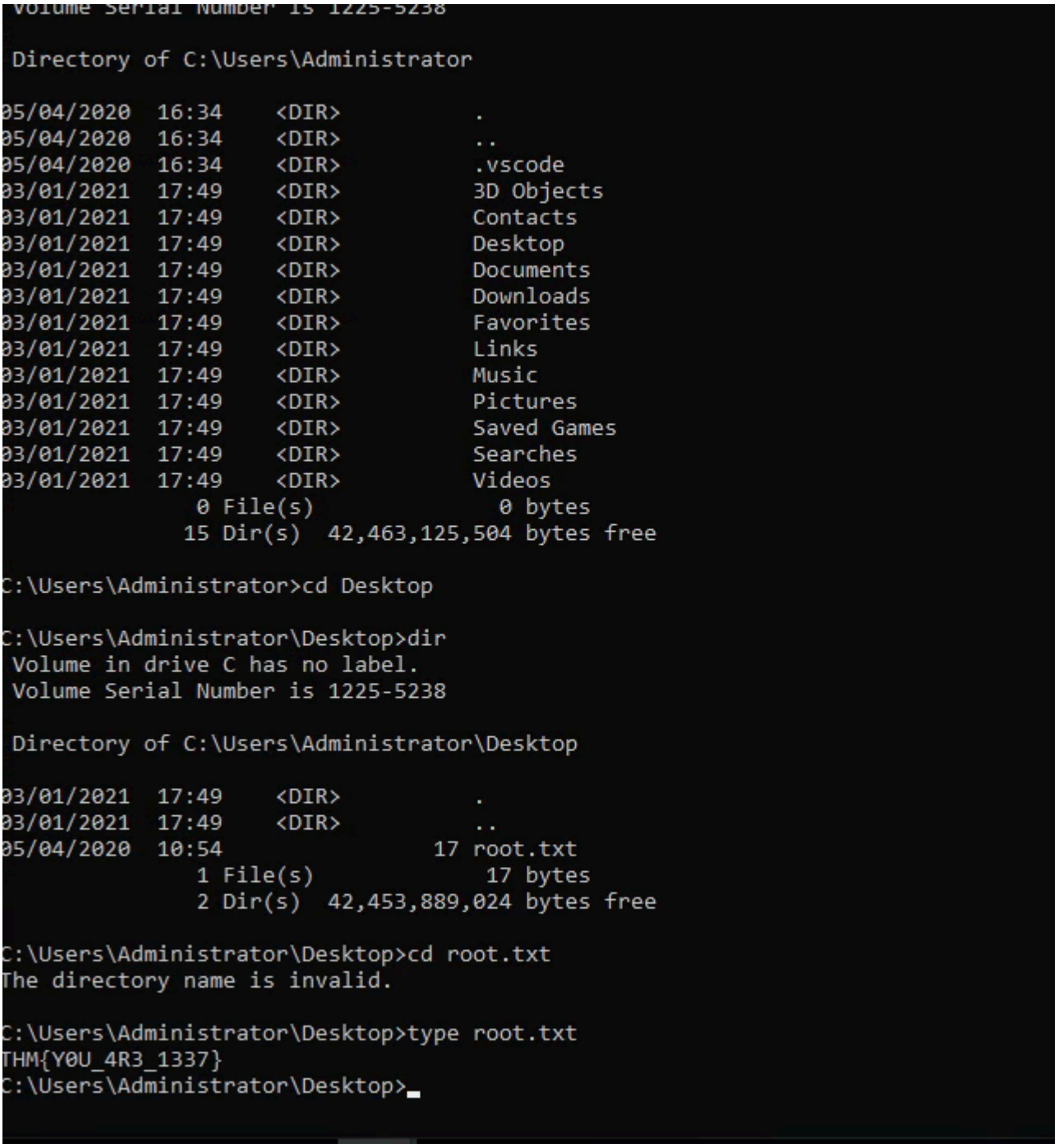
```
Select Command Prompt
C:\Users\SG>cd /.

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.

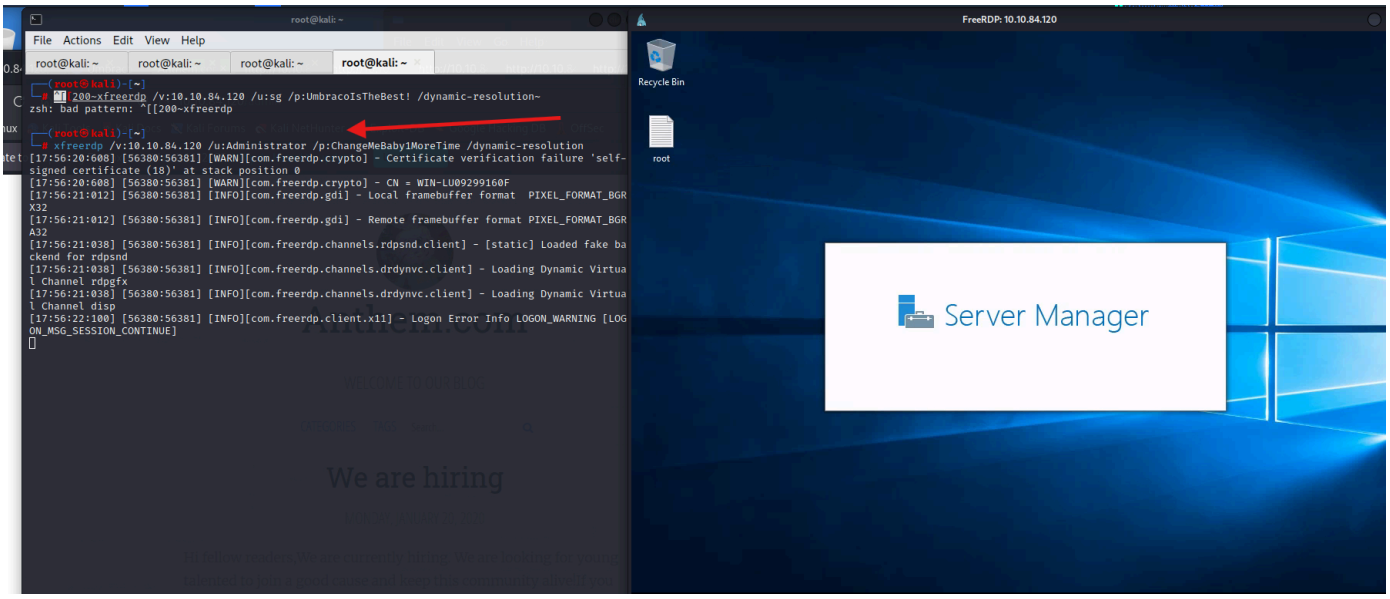
runas /user:Administrator cmd

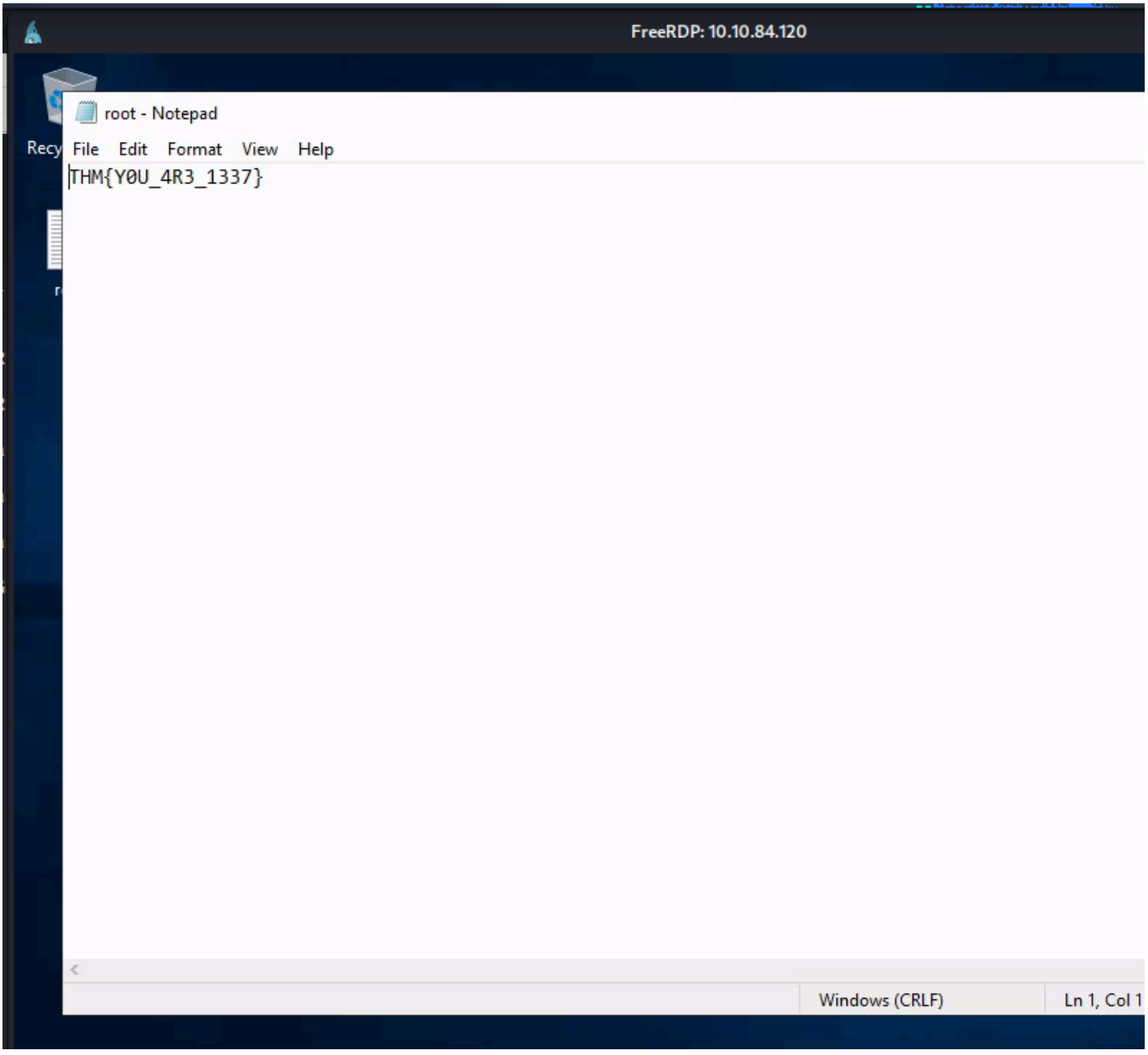


```
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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
```



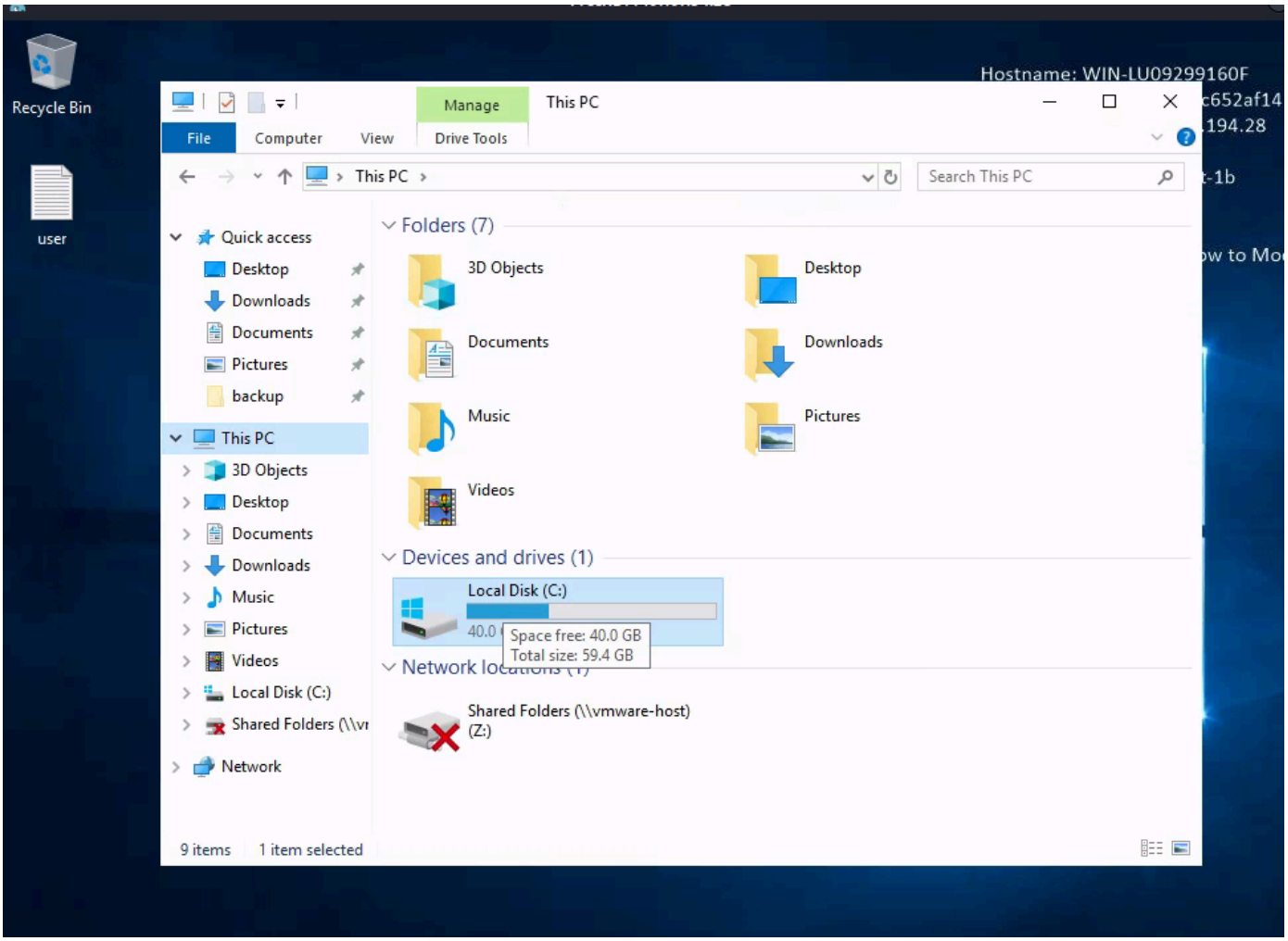
Second way All I'm going to do is relog in as Administrator.


root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
(root㉿kali)-[~]
[200~xfreerdp /v:10.10.84.120 /u:sg /p:UmbracoIsTheBest! /dynamic-resolution~
zsh: bad pattern: ^[[200~xfreerdp
(root㉿kali)-[~]
xfreerdp /v:10.10.84.120 /u:Administrator /p:ChangeMeBaby1MoreTime /dynamic-resolution
[17:56:20:608] [56380:56381] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[17:56:20:608] [56380:56381] [WARN][com.freerdp.crypto] - CN = WIN-LU09299160F
[17:56:21:012] [56380:56381] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[17:56:21:012] [56380:56381] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[17:56:21:038] [56380:56381] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[17:56:21:038] [56380:56381] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[17:56:21:038] [56380:56381] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel disp
[17:56:22:100] [56380:56381] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_WARNING [LOGON_MSG_SESSION_CONTINUE]
FreeRDP: 10.10.84.120
Recycle Bin
root
Server Manager

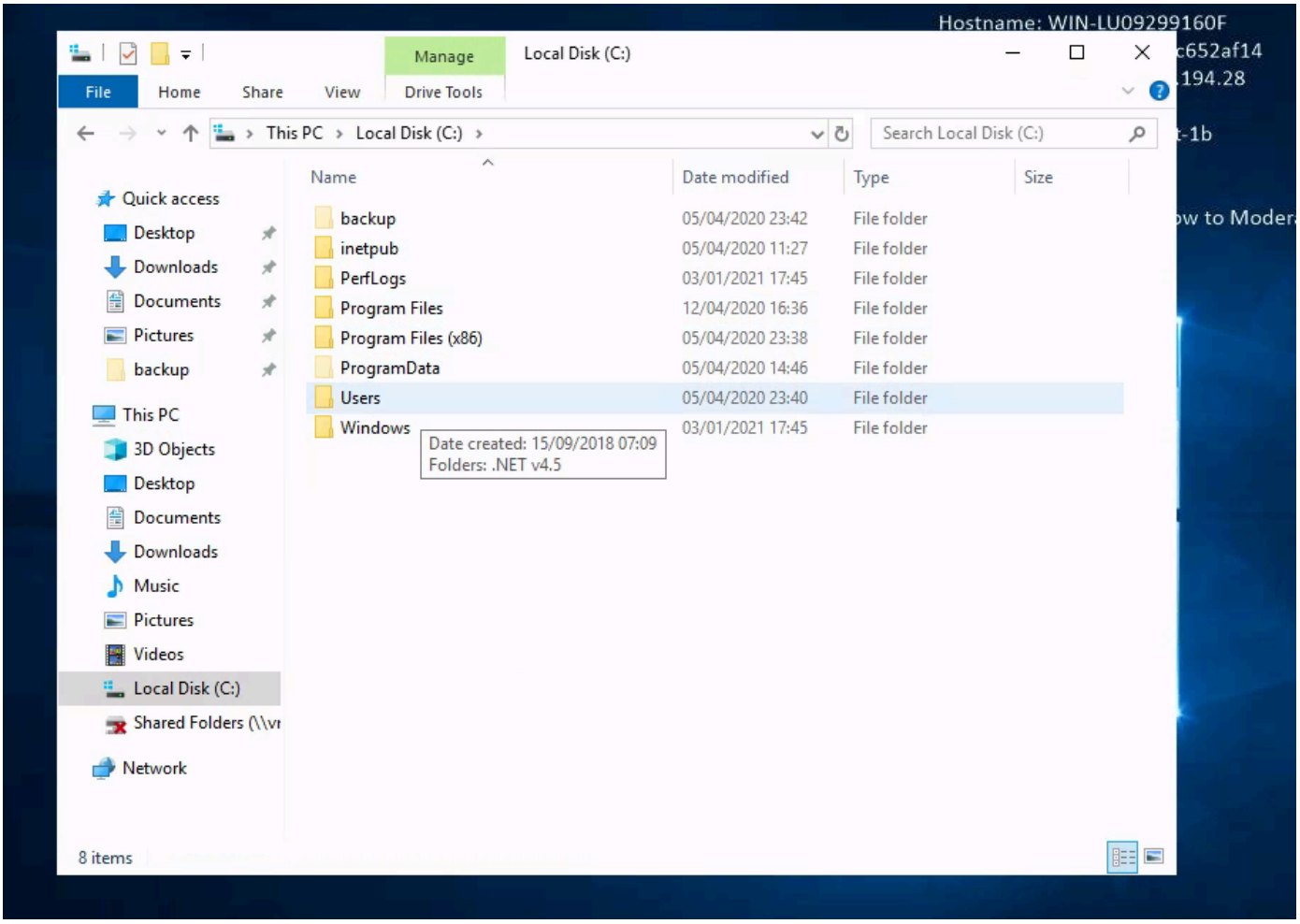

FreeRDP: 10.10.84.120
root - Notepad
File Edit Format View Help
THM{Y0U_4R3_1337}
Windows (CRLF)
Ln 1, Col 1

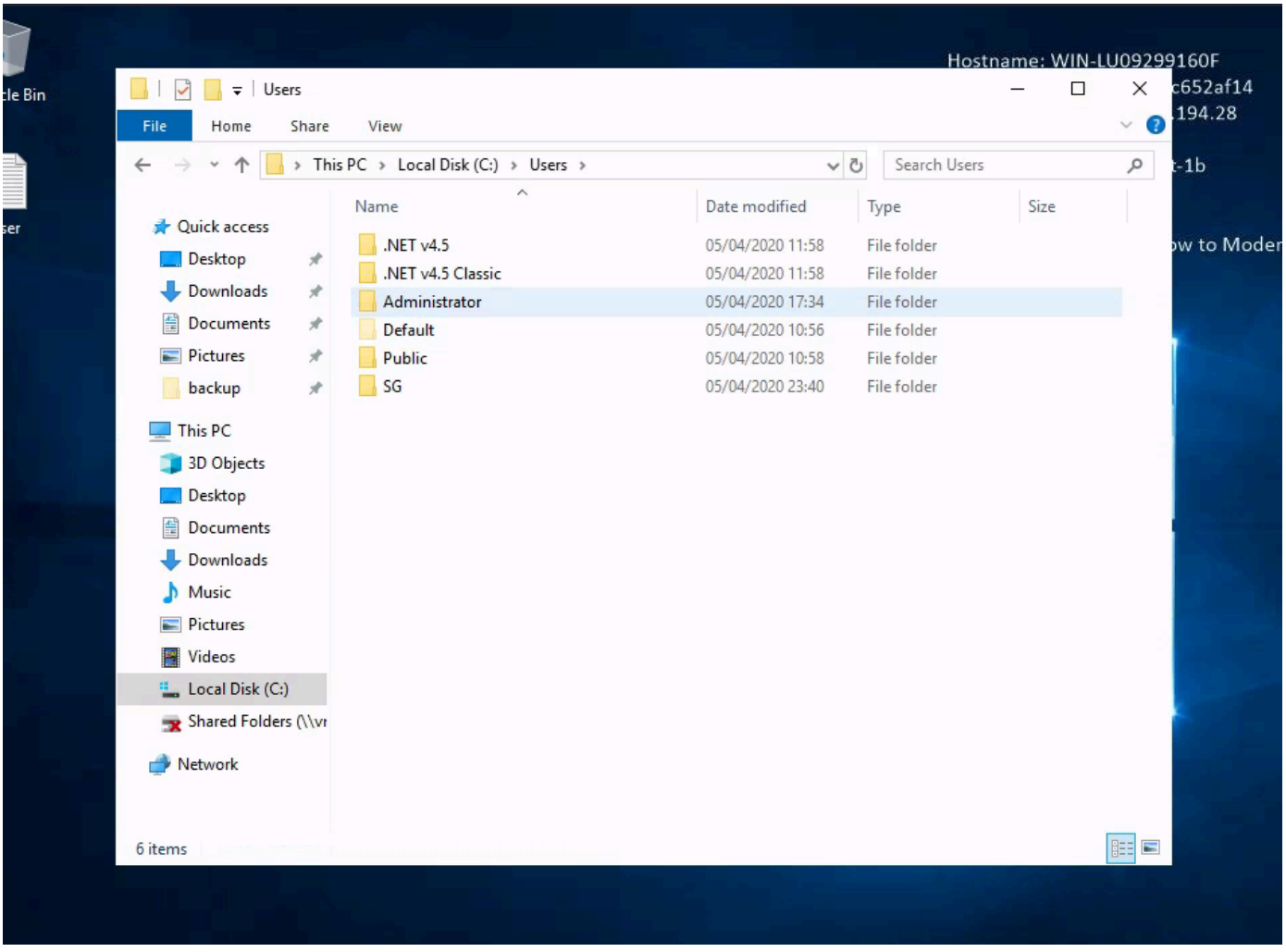
Third Way

From SG machine

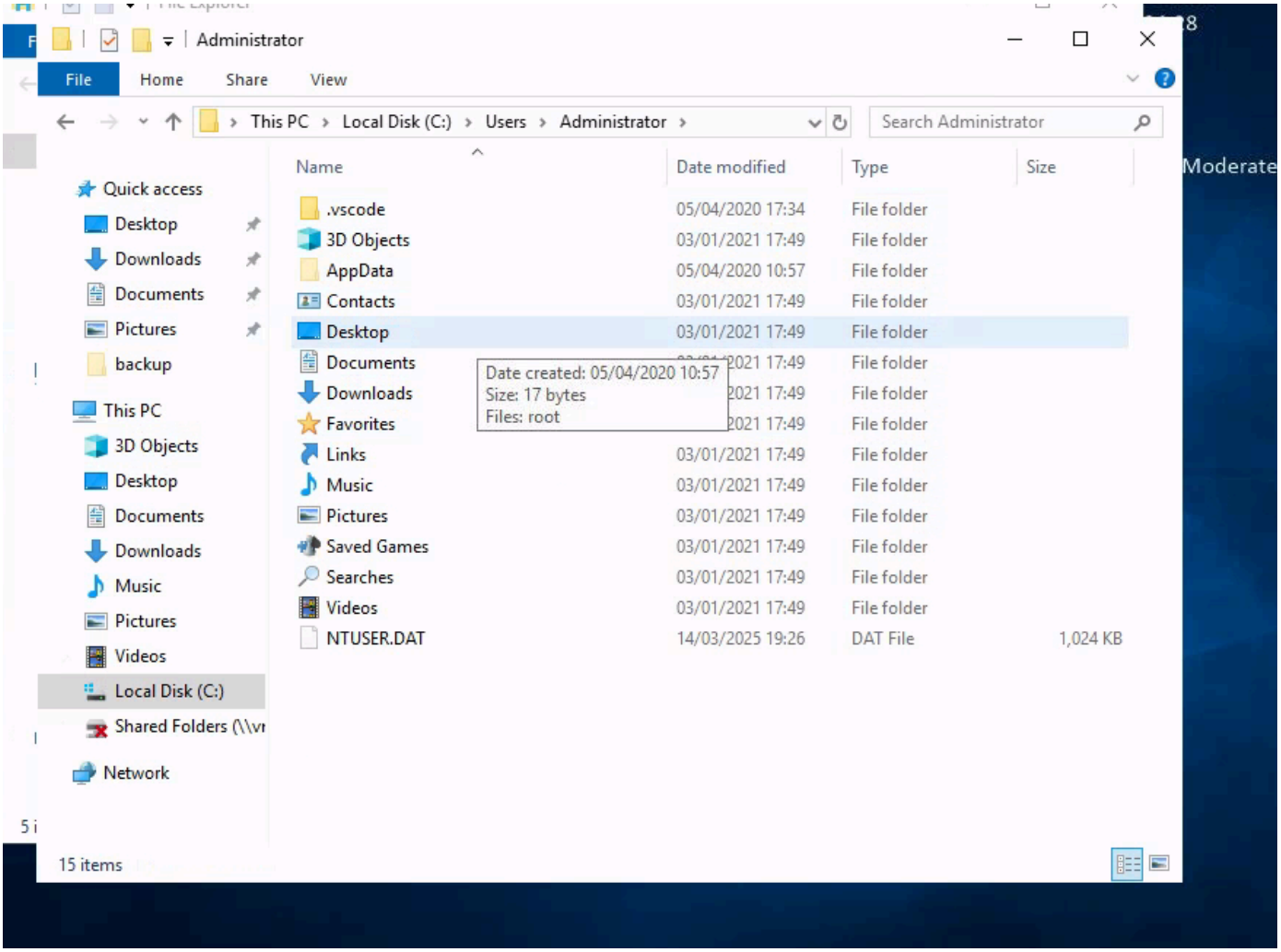


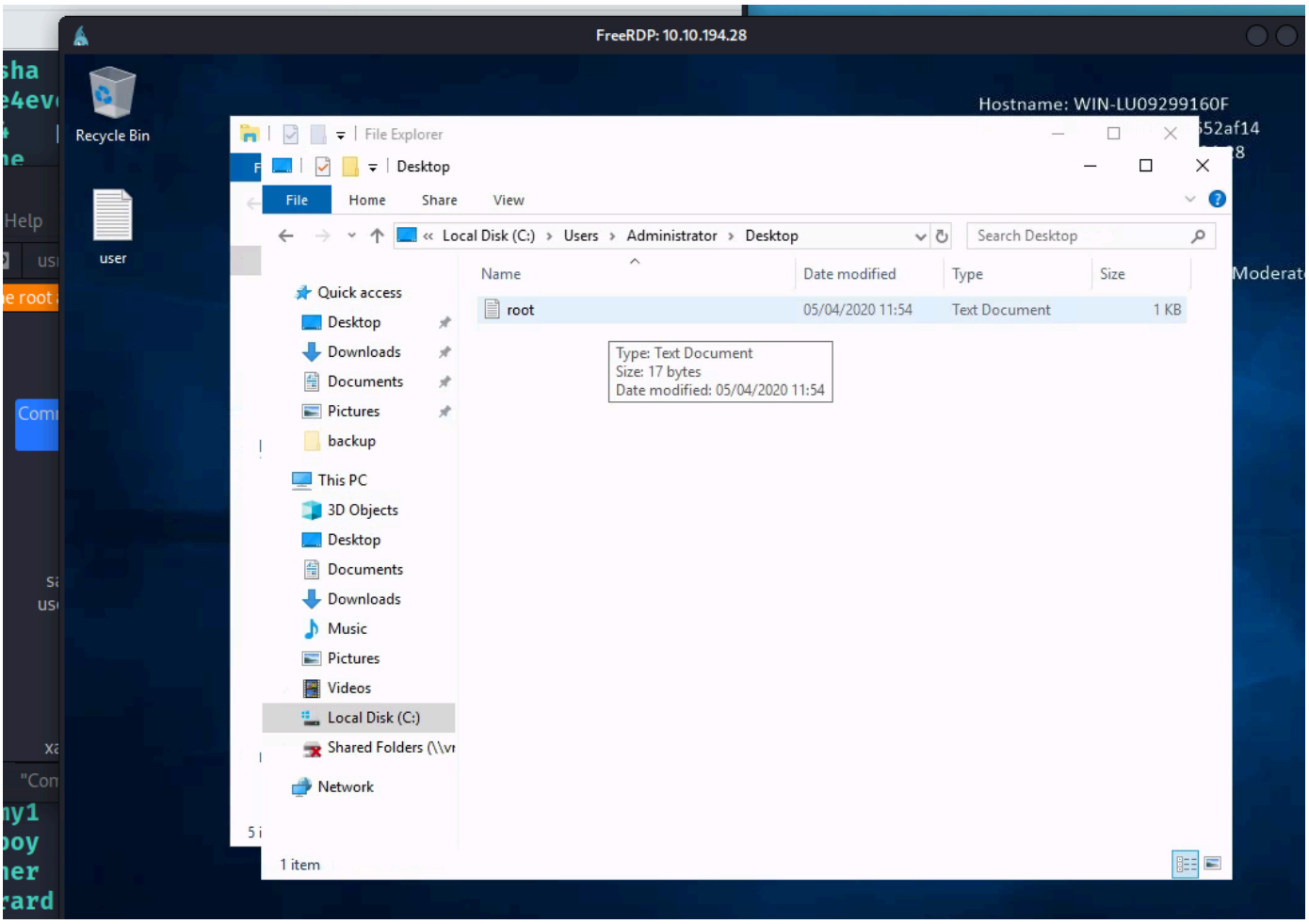
.


Hostname: WIN-LU09299160F
Manage
Local Disk (C:)
File
Home
Share
View
Drive Tools
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
backup
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Shared Folders (\\vr
Network
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
Date created: 15/09/2018 07:09
Folders: .NET v4.5
8 items


Hostname: WIN-LU09299160F
Users
File
Home
Share
View
This PC › Local Disk (C:) › Users ›
Search Users
Quick access
Desktop
Downloads
Documents
Pictures
backup
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Shared Folders (\\vr
Network
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 05/04/2020 17:34 File folder
Default 05/04/2020 10:56 File folder
Public 05/04/2020 10:58 File folder
SG 05/04/2020 23:40 File folder
6 items

and login with password




FreeRDP: 10.10.194.28
Hostname: WIN-LU09299160F
Recycle Bin
user
File Explorer
Desktop
File
Home
Share
View
Local Disk (C:) › Users › Administrator › Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
backup
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Shared Folders (\\vr
Network
Name
Date modified
Type
Size
root
05/04/2020 11:54
Text Document
1 KB
Type: Text Document
Size: 17 bytes
Date modified: 05/04/2020 11:54
1 item