Anthem writeup

Nmap

```
nmap -Pn -sC -sV 10.10.101.185 -oA nmap
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-02 16:15 CDT
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.56% done; ETC: 16:17 (0:00:01 remaining)
Nmap scan report for 10.10.101.185
Host is up (0.13s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| 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: 2021-10-02T21:16:41+00:00
| ssl-cert: Subject: commonName=WIN-LU09299160F
| Not valid before: 2021-10-01T21:10:55
|_Not valid after:  2022-04-02T21:10:55
|_ssl-date: 2021-10-02T21:17:49+00:00; +20s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 19s, deviation: 0s, median: 19s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.21 seconds
```

Website analysis

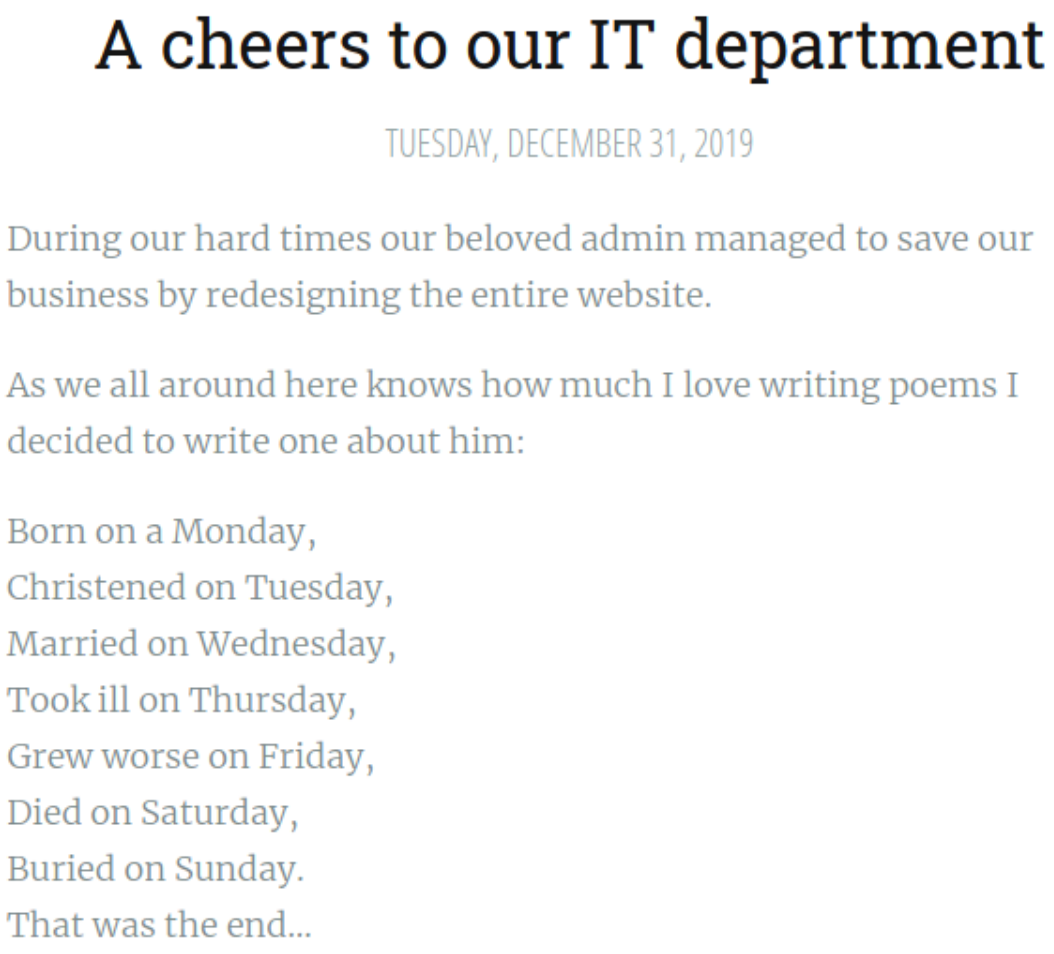
We discover a potential password within Robots.txt

```
UmbracoIsTheBest!

# Use for all search robots
User-agent: *

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

CMS is umbraco

http://10.10.101.185/umbraco/#/login

Read the poem and notice the author is James Orchard Halliwell



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...

He is famous for nuersy rymes. The name of the poem leads us to the admin login.

Solomon Grundy (nursery rhyme)

From Wikipedia, the free encyclopedia

Not to be confused with Salmagundi or Solomon Gundy.

"**Solomon Grundy**" is an English nursery rhyme. It has a Roud Folk Song Index number of 19299.[1]

We can find the email naming convention Jane Doe's author page

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

Our login to umbranco will be SG@anthem.com:UmbracoIsTheBest!

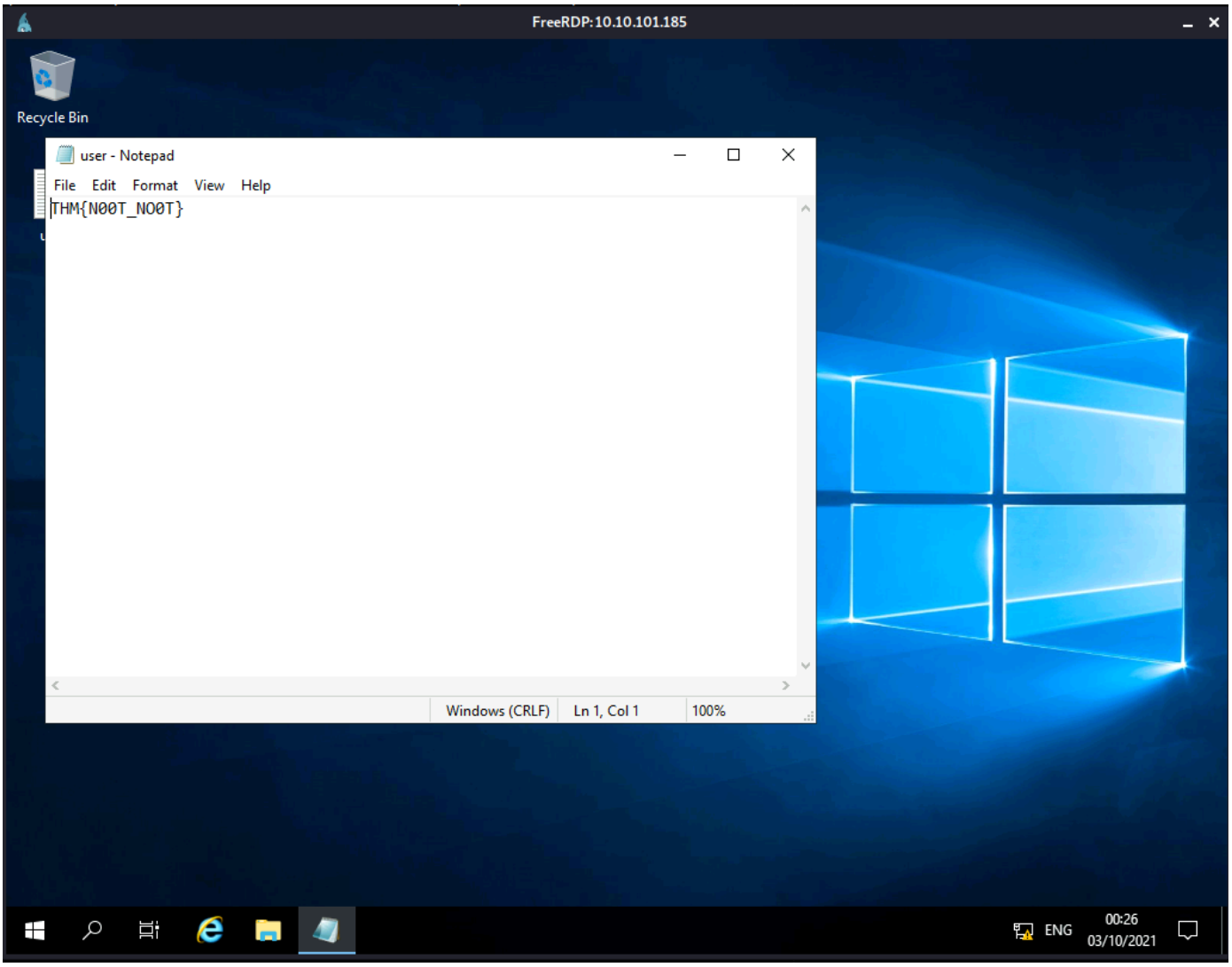
Foothold

Umbraco version 7.15.4

I coulden't find away to gain RCE through the CMS so lets try RDP.

After trying a few naming convetions, I was able to login with SD:UmbracoIsTheBest!

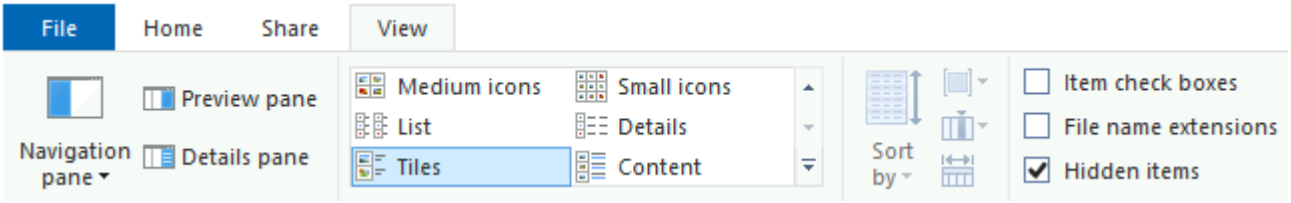
```
xfreerdp /u:sd /p:UmbracoIsTheBest! /cert:ignore /v:10.10.101.185
```



Priv esc

We have limited files we have read acess to.

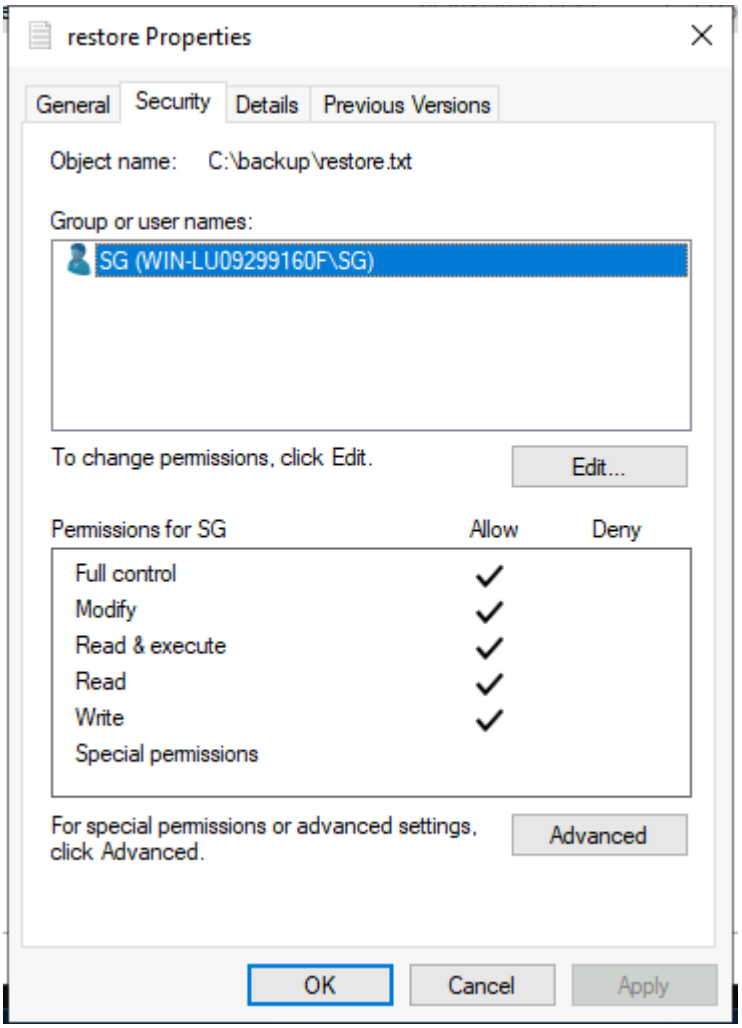
Turn on hidden files in file explorer.



We find a backup file within the root of the C drive.

We cannot read it but if we check its permissions, the SG user is the onwner of the file.

Select properties on the file and then click edit. Give the SG user full control of the file.



Now we can read the admin passowrd "ChangeMeBaby1MoreTime"

Run cmd or powershell as the administrator and enter the password.

You should now have an admin shell.