DC03

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Reconocimiento

Vamos a empezar como siempre con un escaneo de puertos con nmap, con la herramienta autonmap.

Texto

Descripción generada automáticamente

Tras realizar enumeración en todos los puertos, no encontré nada, enumerando rpcclient, ldap, smb.  
Lo siguiente que probé es un ataque smb relay, aunque me di cuenta tarde de que las firmas SMB estaban activas, pero obtuve una grata sorpresa. Mas adelanté vi que fue un Evenenamiento LLMNR.

Para ello utilizé la herramienta responder

Imagen de la pantalla de un video juego

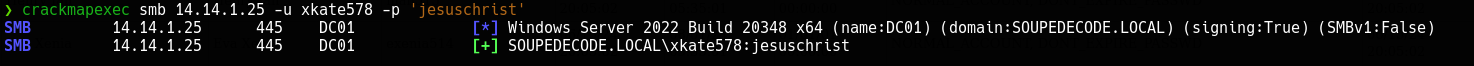
Descripción generada automáticamente con confianza baja

Tenemos un hash ntlmv2 para el usuario xkate578, nos lo guardamos y vemos si lo podemos crakear con john.

Texto

Descripción generada automáticamente

Ya tenemos unas credenciales. Para comprobar si son válidas los podemos probar con crackmapexec



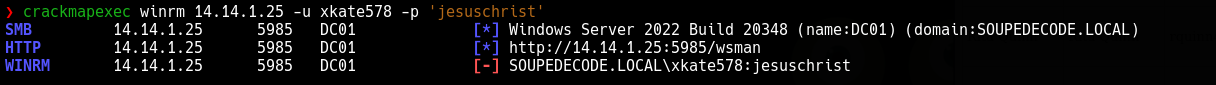
Como podemos ver, son correctas.

Tambien con cme podemos enumerar carpetas compartidas, y vemos una interesante, share.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Aquí tenemos ya la flag de user, al ver esta flag voy a comprobar si este usuario se puede conectar de forma remota con winrm, pero no hay suerte, por lo que toca escalar privilegios.

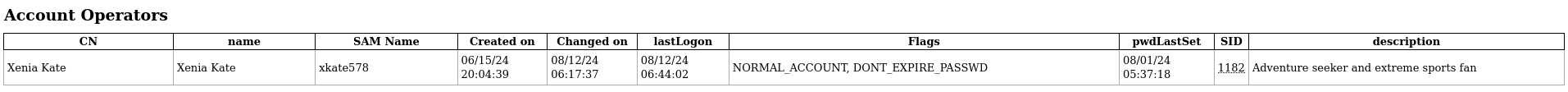


Al tener unas credenciales validas y poder enumerar todos los usuarios del dominio, pruebo tambien si hay usuarios vulnerables a ataque ASREPRoast o Kerberoast, pero no hay ninguno.   
Lo siguiente ejecutamos ldapdomaindump, para asi tambien enumerar grupos, equipos… y ver toda la información con una estructura y visualmente mejor.

Texto

Descripción generada automáticamente

Aquí ya podemos ver cosas interesantes, como que nuestro usuario pertenece al grupo de “Account Operators”

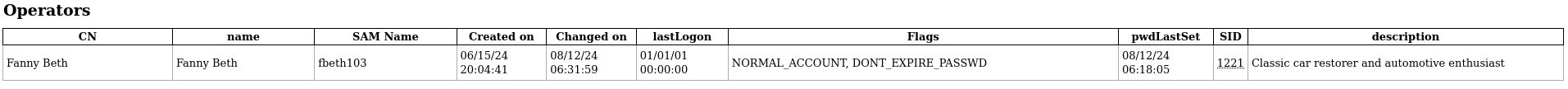


Si buscamos info sobre este grupo encontramos lo siguiente:  
El grupo Account Operators concede privilegios limitados de creación de cuentas a un usuario. Los miembros de este grupo pueden crear y modificar la mayoría de los tipos de cuentas, incluidas las cuentas para los usuarios, los grupos locales y los grupos globales. Los miembros del grupo pueden iniciar sesión localmente en controladores de dominio.

Los miembros del grupo NO pueden administrar la cuenta de usuario Administrador, las cuentas de usuario de los administradores, o los grupos Administradores, Operadores de servidor, Operadores de cuenta, Operadores de copia de seguridad u Operadores de impresión. Los miembros de este grupo no pueden modificar los derechos de usuario.

Sabiendo esto, vemos otro grupo bastante interesante, Operators, que este a su vez forma parte del grupo Admins del Dominio, por lo que si hay algún usuario que pertenezca a este grupo de Operators, podremos cambiarle la contraseña y por consiguiente conseguir unas credenciales de Admins del dominio.

En el grupo Operators solo tiene un usuario, fbeth103



Vamos a ver si podemos forzarle un cambio de contraseña a este usuario a través de rpcclient.

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

Vemos que funciona y además, al pertenecer al grupo de domain admins vemos el Pwn3d! de cme, lo que significa que tenemos acceso total al domino.

Lo siguiente que haremos es dumpear todo el NTDS, NTDS es una tecnología de directorio de Microsoft que se utiliza para almacenar información sobre los recursos de red y servicios de una organización. NTDS proporciona la capacidad de administrar todos los recursos de red a través de una sola plataforma y cuenta con la capacidad de gestionar la autenticación, autorización y acceso a los recursos de red.

En resumen, que podemos obtener todas las credenciales del dominio.

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Con esta información nos podemos conectar con winrm, realizando un pass the hash con el usuario Administrator y su hash NTLMv1

Texto

Descripción generada automáticamente

Pwned!