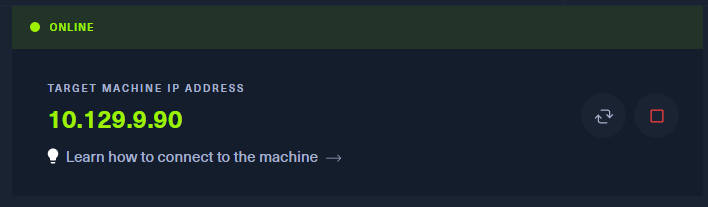
ANALISIS MAQUINA VIRTUAL DANCING

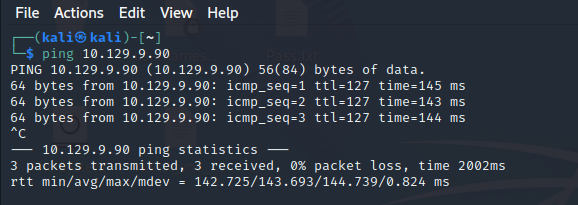
Dificultad: Fácil

Etiqueta: Enumeración, Penetración, SMB

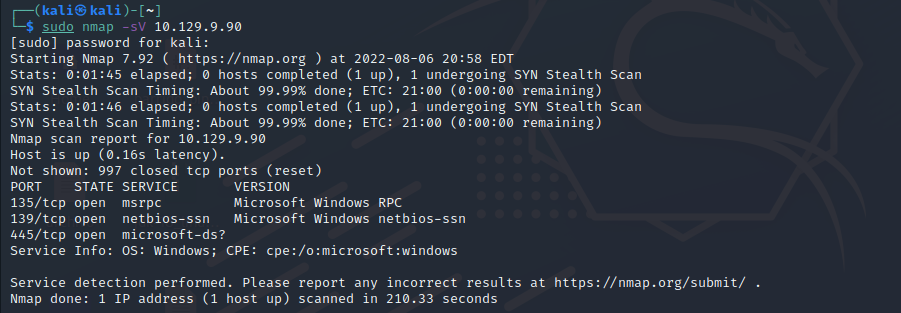
IP Maquina



Realizamos ping para ver si tenemos conexión



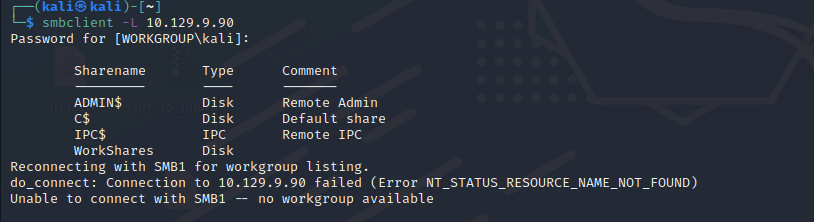
Escaneamos para ver los puertos y servicios



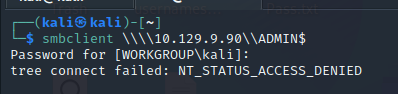
Encontramos 3 puertos abiertos y entre ellos el 445 que es un SMB lo que significa que tenemos un recurso compartido activo que podríamos explorar. Piense en este recurso compartido como una carpeta a la que se puede acceder a través de Internet. Para hacerlo, necesitaremos tener instalados los servicios y scripts apropiados.

Smbclient intentará conectarse al host remoto y verificará si se requiere alguna autenticación. Si la hay, le pedirá una contraseña para su nombre de usuario local. Deberíamos tomar nota de esto. Si no especificamos un nombre de usuario específico para smbclient al intentar conectarse al host remoto, solo usará el nombre de usuario de su máquina local. Ese es con el que actualmente está conectado a su máquina virtual. Esto se debe a que la autenticación SMB siempre requiere un nombre de usuario, por lo que al no darle uno explícitamente para intentar iniciar sesión, solo tendrá que pasar su nombre de usuario local actual para evitar generar un error con el protocolo.

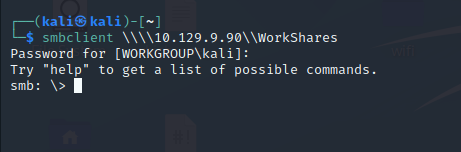
Colocamos en la terminal smbclient -L $ip\_maquina para listar nombres de usuario y dejamos en blanco la contraseña



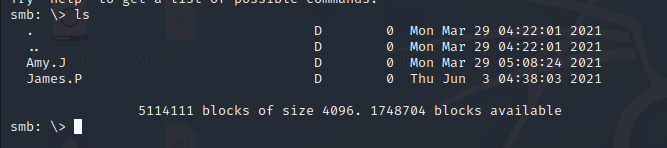
Tenemos probar con cada nombre de usuario para la conexión



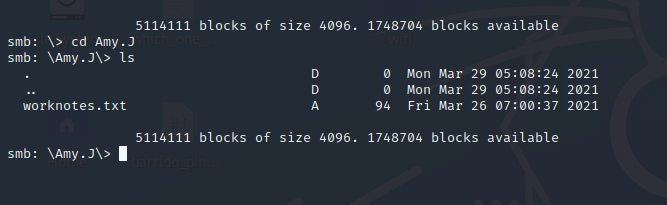
Nos salió error al igual con C$ y IPC$ con el que nos funciono fue con WorkShares$



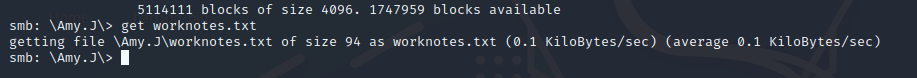
Con ls podemos listar los archivos

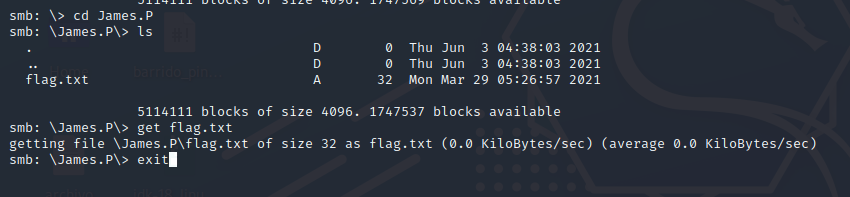


Y encontramos dos directorios mas Amy.J y James.P vemos que contiene cada uno

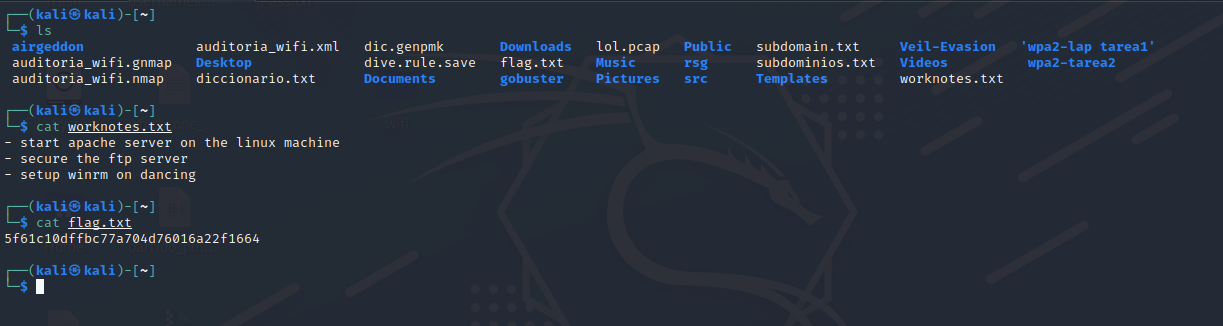


En Amy encontramos un archivo worknotes.txt lo cual descargaremos con get worknotes.txt





Y en James.P encontramos el archivo que mas nos interesa flag.txt, salimos con exit y buscamos con ls los archivos descargados y los leemos usamando el comando cat



Bandera: 5f61c10dffbc77a704d76016a22f1664