Introducción A NetBIOS

NetBIOS es un protocolo de red que viene habilitado de forma predeterminada en Windows. Básicamente lo que permite NetBIOS es que las aplicaciones se comuniquen con la red. Un equipo en una red local se comunica con otro a través de una conexión utilizando lo que se conoce como datagramas NetBIOS. Su función es establecer la sesión y mantener las conexiones. NetBIOS es un protocolo de capa de sesión, lo que significa que proporciona servicios para la capa de presentación y la capa de aplicación. NetBIOS se utiliza para proporcionar nombres de host y servicios a otras aplicaciones en una red. También se utiliza para compartir archivos e impresoras en una red local. Sin embargo, NetBIOS es un protocolo antiguo y obsoleto, y puede tener vulnerabilidades que son aprovechadas por los piratas informáticos para llevar a cabo diferentes métodos de ataques. Es posible desactivar NetBIOS en Windows siguiendo unos sencillos pasos.

NetBIOS (Network Basic Input/Output System) es un protocolo de red utilizado principalmente en sistemas operativos de Microsoft para proporcionar servicios de red en una red local. Fue desarrollado en la década de 1980 y, aunque ha sido en gran medida reemplazado por tecnologías más modernas, todavía juega un papel en ciertos entornos.

Aquí tienes una descripción detallada de NetBIOS:

1. Función Principal:

NetBIOS se diseñó originalmente para proporcionar una capa de abstracción sobre la comunicación entre dispositivos en una red local. Permite a los dispositivos descubrirse mutuamente y compartir recursos, como impresoras y archivos.

2. Nombres NetBIOS:

Uno de los conceptos fundamentales en NetBIOS es el sistema de nombres. Cada dispositivo en una red NetBIOS tiene un nombre de 16 caracteres que lo identifica. Estos nombres son utilizados para identificar recursos y para comunicarse entre dispositivos.

3. Resolución de Nombres:

Para que los dispositivos puedan comunicarse entre sí, necesitan saber la dirección IP correspondiente al nombre NetBIOS. El proceso de traducir un nombre NetBIOS a una dirección IP se llama resolución de nombres. NetBIOS proporciona dos métodos principales para resolver nombres:

- **Broadcast:** En una red local pequeña, un dispositivo puede enviar una transmisión de difusión preguntando por una dirección IP asociada a un nombre NetBIOS específico. Sin embargo, esto puede generar tráfico innecesario en redes más grandes.
- **WINS (Windows Internet Name Service):** WINS es un servicio centralizado que mantiene una base de datos de nombres NetBIOS y sus direcciones IP correspondientes. Los dispositivos pueden consultar el servidor WINS para obtener la dirección IP de un nombre NetBIOS.

4. Sesiones y Comunicación:
NetBIOS también maneja la creación y el cierre de sesiones entre dispositivos. Una sesión NetBIOS permite que dos dispositivos se comuniquen de manera confiable y bidireccional. Los datos enviados a través de una sesión NetBIOS están garantizados de llegar en el mismo orden en que se enviaron.
5. Puertos NetBIOS:
NetBIOS utiliza una serie de puertos para diferentes tipos de servicios. Por ejemplo:
- **Puerto 137:** Para el servicio de resolución de nombres NetBIOS (NBNS).
- **Puerto 138:** Para el servicio de datagramas NetBIOS (NBDGM), que maneja la comunicación sin conexión.
- **Puerto 139:** Para el servicio de sesión NetBIOS (NBSS), que maneja la comunicación orientada a la conexión.
6. Seguridad y Limitaciones:
NetBIOS fue desarrollado en una época en la que la seguridad en la red no era una preocupación tan importante como en la actualidad. Por lo tanto, NetBIOS carece de muchas características de seguridad modernas y puede ser vulnerable a ataques. Por esta razón, se recomienda encarecidamente su uso solo en redes seguras y protegidas.
En resumen, NetBIOS es un protocolo de red obsoleto pero que aún puede encontrarse en entornos de red heredados o en configuraciones específicas. Aunque ha sido en gran parte reemplazado por tecnologías más seguras y eficientes, como TCP/IP y DNS, es importante comprender NetBIOS para trabajar con sistemas y redes más antiguos.

Nota Importante Sobre El Laboratorio

En este problema de hacking que vamos a ver hoy, vamos a utilizar el laboratorio que se describió en el post anterior:
https://juanjosevivas.es/escaneo-de-redes-usando-metasploit/
Os remito a este post para las instrucciones sobre el laboratorio que estamos usando desde ahora y que vamos a usar en este problema que vamos a resolver.
Pero, tenemos o puede que no, un pequeño problema. Este laboratorio tiene 6 máquinas. Dos de ellas son:

- Windows 11
- Windows Server 2022

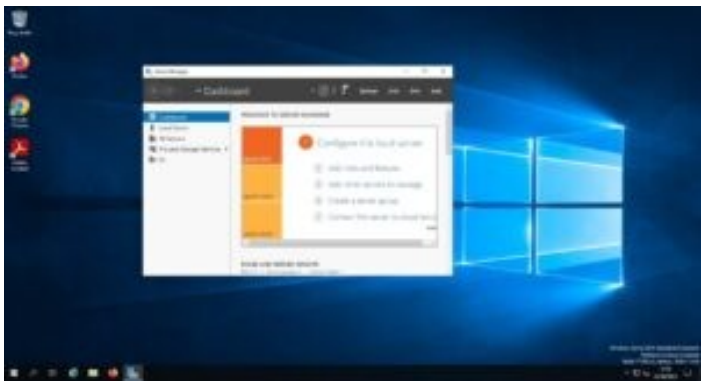
Estas máquinas no van a funcionar en un PC anfitrión que sea viejo, por muchas capacidades de memoria o procesador que tenga ese PC. y es que la arquitectura de los nuevos sistemas operativos de Windows, por motivos de seguridad, no aceptan procesadores antiguos y el sistema operativo no arranca.
Y a pesar de que son máquinas virtualizadas, detectan el procesador antiguo del PC anfitrión y no se ejecutan.
De modo que si al arrancar, por ejemplo Windows 11, que vamos a usar en este problema, aparece un mensaje de error tipo "pantalla azul", es que el PC anfitrión que estás utilizando no vale. Necesitas otro mas moderno.

Dicho esto procedamos a plantear el laboratorio que vamos a hacer.

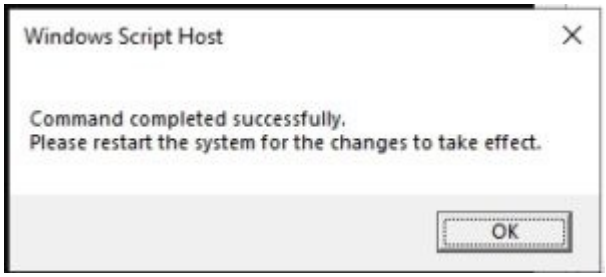
Recopilación De Información Usando NetBIOS

NetBIOS significa Sistema básico de entrada y salida de red. Windows usa NetBIOS para compartir archivos e impresoras. Un nombre NetBIOS es un nombre de computadora único asignado a sistemas Windows, que comprende una cadena ASCII de 16 caracteres que identifica el dispositivo de red a través de TCP/IP. Los primeros
15 caracteres son para el nombre del dispositivo y el último caracter se reserva para el tipo de servicio del dispositivo.
El servicio NetBlOS es un objetivo fácil, ya que es fácil de explotar y se ejecuta en sistemas Windows incluso cuando no está en uso. La enumeración de NetBIOS permite a los atacantes leer o escribir en un sistema informático (dependiendo de la disponibilidad de acciones) o lanzar un ataque DoS.
nbtstat es una herramienta de red que se utiliza para verificar las conexiones TCP/IP en ejecución. nbtstat enumera todas las conexiones de red que se utilizan en el sistema operativo Windows. Esta herramienta está preinstalada en Windows, no necesita utilizar ningún software externo para ejecutar nbtstat. Puede mostrar estadísticas del protocolo NetBIOS a través de TCP/IP (NetBT), tablas de nombres NetBIOS para el equipo local y equipos remotos, y la caché de nombres NetBIOS. Este comando también permite actualizar la caché de nombres NetBIOS y los nombres registrados con el Servicio de nombres Internet de Windows (WINS). Si se usa sin parámetros, este comando muestra información de la Ayuda. Este comando solo está disponible si el protocolo de Internet (TCP/IP) está instalado como componente en las propiedades de un adaptador de red en conexiones de red.
Usaremos la máquina Windows Server contra la Windows 11
Como password para esas máquinas usaremos: Pa$$w0rd, o sea cambiando las 2 s por $ y la o por un cero (0). Esta es la password que usaremos para las máquinas Windows.

Y entramos en Windows Server 2019



Fijaros que en la esquina inferior derecha aparece un mensaje donde dice que la licencia ha expirado. Existe un procedimiento para rearmar una licencia de Windows y estirar así su uso gratuito. Este procedimiento se explica en uno de mis posts. Este:
https://juanjosevivas.es/rearmado-de-licencias-windows-10/
Y asi procedemos al rearmado de la licencia.



Y con esto tendríamos rearmada la licencia para 90 días mas. Reiniciamos la máquina.
Bien pues ya tenemos arrancadas las máquinas Windows Server 2019 y Windows 11. Sabemos que las direcciones IP son:

- Windows 11 -> 10.10.1.11
- Windows Server 2019 -> 10.10.1.19

Para el primer ejercicio, en el cual vamos a usar nbstat, vamos a entrar en las máquinas Windows 11 y Windows Server 2019.

Hay que tener en cuenta que NetBIOS es un protocolo obsoleto, pero que hay que conocer. En los PCs modernos viene desactivado y tendremos que activarlo.
Haga clic derecho en Conexión de área local y seleccione Propiedades. Haga clic en Protocolo de Internet (TCP/IP) y seleccione Propiedades. Haga clic en Avanzado > WINS. En el área de configuración de NetBIOS, asegúrese de que Predeterminado o Habilitar NetBIOS sobre TCP/IP estén seleccionados.
NetBIOS sobre TCP/IP (NBT, o a veces NetBT) es un protocolo de red que permite que las aplicaciones informáticas heredadas que dependen de la API de NetBIOS se utilicen en redes TCP/IP modernas. … Algunas aplicaciones aún usan NetBIOS y no escalan bien en las redes actuales de cientos de computadoras cuando NetBIOS se ejecuta sobre NBF.

En Windows Server 2019 abrimos una ventana de comandos como administrador. O sea buscamos el icono de la ventana de comandos, lo sacamos al escritorio, botón derecho, ejecutar como administrador. Lo cuento telegráficamente porque entiendo que esas cosas sabéis hacerlas.
Y desde esa ventana de comandos tecleamos:
nbtstat -a 10.10.1.11

```
C:\Users\Administrator>nbtstat -a 10.10.1.11
Ethernet0:
Node IpAddress: [10.10.1.19] Scope Id: []
NetBIOS Remote Machine Name Table
Name Type Status
---------------------------------------------
WINDOWS11 <00> UNIQUE Registered
WORKGROUP <00> GROUP Registered
WINDOWS11 <20> UNIQUE Registered
```

WORKGROUP <1E> GROUP Registered
WORKGROUP <1D> UNIQUE Registered
 ☻__MSBROWSE__☻<01> GROUP Registered
MAC Address = 00-0C-29-0A-D2-2A
Y ahora tecleamos:
nbtstat -c
Y nos devuelve el nombre de la máquina remota almacenada en la caché:
Ethernet0:
Node IpAddress: [10.10.1.19] Scope Id: []
NetBIOS Remote Cache Name Table
Name Type Host Address Life [sec]

WINDOWS11 <20> UNIQUE 10.10.1.11 437

Comando Net Use

Ahora vamos a ver el comendo net use
net use es un comando de la línea de comandos de Windows que se utiliza para conectarse, eliminar y configurar conexiones a recursos compartidos, como unidades mapeadas y impresoras de red. Es uno de los muchos comandos `net` como `net send`, `net time`, `net user`, `net view`, etc. Este comando está disponible desde el símbolo del sistema en Windows 11, Windows 10, Windows 8, Windows 7, Windows Vista y Windows XP, y en versiones anteriores de Windows y en sistemas operativos de servidor de Windows. La sintaxis general del comando es la siguiente:
net use [{ devicename | * }] [\\\\computername\\sharename [\\volume] [{ password | * }]] [/user: [domainname\\] username] [/user: [dotteddomainname\\] username] [/user: [username@dotteddomainname] [/home { devicename | * } [{ password | * }]] [/persistent: { yes | no }] [/smartcard] [/savecred] [/delete] [/help] [/?]
Bien, pues simplemente desde un terminal de cualquiera de los windows que tenemos abiertos, tecleamos:
net use
Y nos saldrá un mensaje diciendo que no hay ninguna entrada.
Si desde Windows 11 por ejemplo tecleamos:
net view
PS C:\Users\Admin> net view
Server Name Remark

\\LAPTOP-LBJPLKJ
\\SERVER2019
\\WINDOWS11
The command completed successfully.
Es decir, nos devuelve las máquinas que hay ahora mismo en la red. Ha acertado porque están los dos Windows que hemos arrancado y la máquina anfitriona.

Y así podríamos poner infinidad de ejemplos. Yo recomiendo para estudiar este tipo de comandos, cogerse un buen manual, con una configuración determinada de máquinas abiertas y empezar a probar todos los comandos posibles y añadir esta utilidad al arsenal que debemos conocer.

NetBIOS Enumerator

NetBIOS Enumerator es una herramienta de enumeración que se utiliza para trabajar con algunos protocolos como SMB. Los atacantes utilizan NetBIOS Enumerator para enumerar detalles como el nombre de NetBIOS, los nombres de usuario, los nombres de dominio y las direcciones MAC en un rango de IP determinado. NetBIOS Enumerator también puede ser utilizado para escanear puertos.

NetBIOS Enumerator se utiliza para escanear y enumerar información sobre dispositivos y recursos en una red que utiliza el protocolo NetBIOS y otros. Esta herramienta se utiliza para obtener información sobre nombres de máquinas, direcciones IP asociadas, nombres de grupos de trabajo y recursos compartidos en la red que utilizan NetBIOS para la comunicación.

Sin embargo, es importante tener en cuenta que el uso de herramientas de enumeración de NetBIOS en redes ajenas sin autorización puede ser considerado un intento de intrusión o un comportamiento malicioso. Por lo tanto, siempre se debe utilizar este tipo de herramientas de manera ética y responsable, siguiendo las políticas de seguridad y autorización de la red en la que se está trabajando.

Bien, y una vez que ya sabemos lo que es NetBIOS Enumerator, vamos a instalar la aplicación en nuestras máquinas Windows a ver como funciona.

Porque esto es una aplicación Windows. No es una utilidad de línea de comandos.

Dicha aplicación Windows puede conseguirse en:

https://nbtenum.sourceforge.net/

Arrancamos la máquina Windows Server 2022. La password es Pa$$w0rd como las otras. Ahora tendremos tres máquinas arrancadas.

En la máquina Windows 11 abrimos un navegador cualquiera y navegamos a:

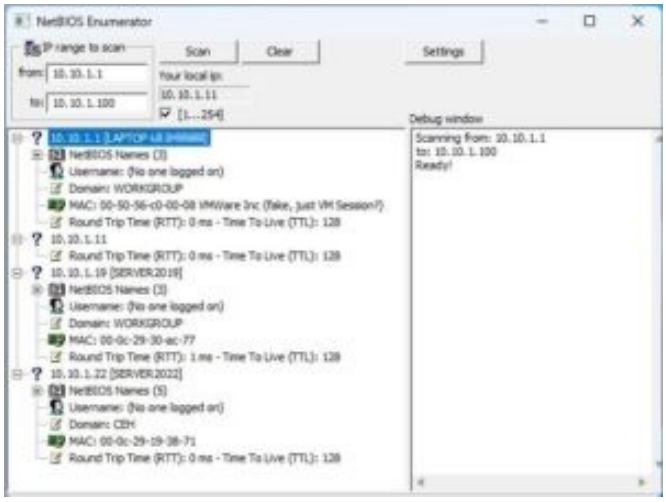
https://nbtenum.sourceforge.net/

Y descargamos la aplicación que viene dentro de un archivo zip. Dicho archivo tiene una carpeta que descomprimimos en el desktop de Windows 11.

procedemos a ejecutar la aplicación que hay dentro de la carpeta:

NetBIOS Enumerater

Y marcamos como rango de IPs a escanear desde 10.10.1.1 a 10.10.1.100 y el resultado es:



Fijaros que detecta 4 equipos en la red,
10.10.1.1 -> El PC anfitrión
10.10.1.11 -> Windows 11
10.10.1.19 -> Windows Server 2019
10.10.1.22 -> Windows Server 2022
Y además nos da un puñado de información sobre cada equipo.

Enumeración Utilizando NSE Scripting

NSE (Nmap Scripting Engine) Script se refiere a una característica dentro de la popular herramienta de escaneo de red llamada Nmap. Nmap es utilizado para descubrir hosts y servicios en una red, creando un mapa de la topología y los recursos disponibles. El NSE Scripting Engine es una parte integral de Nmap que permite a los usuarios ejecutar scripts personalizados para realizar tareas específicas durante el escaneo de red.
Los scripts NSE están escritos en lenguaje de programación Lua y son utilizados para automatizar y ampliar las capacidades de Nmap. Estos scripts pueden realizar diversas funciones, como:
1. **Detección de vulnerabilidades:** Algunos scripts NSE se utilizan para buscar y detectar posibles vulnerabilidades en los servicios y sistemas que se están escaneando.
2. **Enumeración de información:** Los scripts pueden recopilar información detallada sobre servicios, nombres de dominio, versiones de software, etc.
3. **Interacción con servicios:** Los scripts pueden simular interacciones con servicios y protocolos específicos para evaluar su comportamiento y configuración.
4. **Realización de tareas específicas:** Los scripts NSE pueden realizar tareas como la búsqueda de cámaras IP en la red, la búsqueda de dispositivos con vulnerabilidades conocidas o incluso la recopilación de información de configuración de routers.
La comunidad de Nmap ha desarrollado y compartido una amplia gama de scripts NSE que abarcan diferentes áreas y tipos de tareas. Estos scripts pueden ser muy útiles para los administradores de red, profesionales de seguridad y cualquier persona que necesite realizar análisis y evaluación de redes.

Es importante destacar que el uso de scripts NSE también debe llevarse a cabo de manera ética y cumpliendo todas las leyes y regulaciones aplicables. El escaneo de redes sin autorización puede ser considerado ilegal o irresponsable, por lo que siempre se debe utilizar NSE y herramientas similares con cuidado y en entornos donde tengas permiso para hacerlo.
Estos Scripts de Nmap están desarrollados en un lenguaje llamado Lúa.
Bien, ahora que sabemos lo que es NSE Scripting, vamos a probarlo. Cerramos las máquinas Windows 11 y Windows Server 2019, dejamos abierto Windows Server 2022 y abrimos nuestra máquina de ataque Parrot Security, que ya sabéis que su contraseña es toor.
Vamos a hacer algo parecido a lo de antes, pero usando Nmap con NSE Scripting. Es decir vamos a enumerar recursos de una red utilizando el protocolo NetBIOS.
Abrimos un terminal en Parrot Security y tecleamos:
sudo su

```
nmap -sV -v --script nbstat.nse 10.10.1.22
```

El resultado del escaneo puede tardar, pero como veremos es bastante cómodo y da un resultado mas exhaustivo usar estos scripts.
El resultado es muy extenso y no lo voy a poner aquí. Pero podéis ver la carpeta donde están todos los scripts que vienen por defecto con la instalación de Nmap en Parrot Security.
En Parrot Security, abrimos el administrador de archivos y navegamos hacia:
/usr/share/nmap/scripts
Y buscamos:
nbstat.nse
Lo abrimos con pluma y ahí podemos ver el Script escrito en Lúa.
Pues esto como todo, al final consiste en hacerse con una buena documentación y aprenderse estas utilidades como si fueran el Padre Nuestro.