NetBios چیست؟

سلام دوستان ، در این مقاله میخوام راجع به NetBios با شما صحبت کنم و شمارا با طرز کار کردن با این برنامه خدماتی ویندوز آشنا کنم ، قبل از شروع مقاله لازم به ذکر هست که نیمی از مطالب این مقاله توسط من و نیمی دیگرش توسط آقای Atlantis گفته شده که جزو بحثهای گذشته گروه هکران البرز بوده که من به فارسی براتون مینویسم .

NetBiosچیه ؟ نت بیوس یا Network Basic Input/Onput System یک برنامه خدماتی هست که در ویندوز وجود داره و مایکروسافت اونو قرار داده که کامپیوترها در یک شبکه بتونند یک سری امکانات را با هم شریک بشن مثل فایلها و پرینتر که در این بین فایلها مورد علاقه نفوذگران هستن .

البته در مورد مفاهیم تخصصی تر درباره این ۲ سرویس یعنی NetBiosو NetBeui باید بگم که اصول کار اینها به مدل مرجع ۷ لایه TCP/IPبرمیگرده و اینکه هر کدام به کدام لایه مربوط میشه و به چه صورت وظیفش را انجام میده که البته NetBeuiچون وابسته به لایه هفتم هست و اگرچه از نظر سرعت انتقال اطلاعات ، سرعت بالایی داره ولی از نظر آدرس دهی بسیار ضعیف و امروزه در شبکه های TCP/IPاستفاده نمیشه و کاربرد آن به شبکه های Lanمحدود شده ، اما نت بیوس در شبکه های TCP/IPاستفاده میشه .

کلاً ویندوز دارای ۳ پیمان و پروتکل اصلی هست که ارتباط بین سیستمها را آسان میکنه که این ۳ شامل :

۱- پیمان IPX/SPX: این پیمان مجموعه ای از دو پیمان هست که ارتباط شبکه ای بین کلاینت و سرور شبکه های تحت سیستم عامل ناول نت را برقرار میکنه .

۲- پیمان NetBEUI: این به معنی NetBios Extanded User INterface (رابط پیشرفته نت با بیوس کاربری) که در اصل NetBEUIیک بخش اضافه شده به NetBiosهست که بعنوان یک برنامه کمکی ارتباط را در شبکه های محلی آسان میکنه ، NetBEUIدر اصل توسط IBMطراحی شد ولی توسط مایکروسافت در ویندوز 9xو NTبکار رفت .

۳-پیمان TCP/IP: این پیمان که خیلی هم معروف هست را میشه در شبکه های محلی و گسترده (Wans)به همان خوبیه ارتباطات اصلی از طریقه اتصالهای اینترنت بکار برد، TCPقسمتی هست که پیمان شمارا به قسمتهای کوچکتر که بسته ها هستن تقسیم میکنه .

بعد برنامه TCPتمام بسته های مربوط به یک پیام را در مقصد دریافت کرده و آنرا بصورت اولین پیام تبدیل میکنه ، اما آیپی قسمتی هست که کار آدرس دهی میکنه و اطمینان میده که هر کدام از بسته ها به سیستم مربوطه هدایت میشه ، همچنین پیمانهای دیگری هم مثل FTP(File Transfer Protocol) و یا HTTP(hyper text transfer protocol)& ... هست که توضیح درباره هر کدام از اینها یک مقاله جداگانه میشه و ما را از بحثمان دور میکنه .

اینها دارای لایه های مختلفی هستن که میتونه باهم ارتباط برقرار کنه و اینجاست که یک هکر میتونه به داخل سیستم شما نفوذ کنه ولی میتونین با قطع این ارتباط این اجازه را به اونها ندین ، برای مثال اجازه به اشتراک گذاری فایلهارا ندین و همچنین نباید هیچ پورت یا درگاه بازی که مخصوص یک تروجن یا Backdoorباشه در سیستمتان باز باشه که اگر غیر از این باشه هکر کارای بیشتری میتونه در هارد

شما انجام بده .

برای اینکه اشتراک گذاری فایلها را غیر فعال کنید در ویندوز 9xبه این مسیر برین :

start ->Setting->Control panel->Network و بعد در صفحه Configurationاز dialog box تیک گزینه "i want to be able to give others accessto my files" را حذف و غیرفعال کنید .

پورت ۱۳۹ پورت مربوط به اشتراک گذاری فایل و پرینتر که همان پورت مخصوص نت بیوس و هر کسی که گزینه مربوط به اشتراک فایلها و پرینتر را در قسمت Networkسیستم انتخاب کرده باید بدونه که سیستمش در خطر نفوذ هکرها قرار داره و هر کسی از روی اینترنت میتونه به یک سیستم با این پورت باز وصلشه و این کار بوسیله یک اسکن ساده میتونه انجام شه که همان طور که ملاحظه کردین من در مورد پورت اسکنر Nmapهم براتون توضیح دادم ، ولی اگر دیدین در یک سیستم پورت ۱۳۹ بازه ادامه کار به چند مورد بستگی داره ، که یکی از شرایط آن ، اینه که باید شخص مورد نظر منابع سیستمش را به اشتراک گذاشته باشه .

برای مثال یک پوشه یا درایو را shareکرده باشه تا شما بتونین وارد آنهاشین و مثلا اگر Level دسترسی را Read Only قرار داده باشه شما فقط میتونین اطلاعات را از سیستم هدف بگیرین و یا اگر Full Access باشه که در این صورت میشه فایل آپلود کرد و یا اطلاعات و پوشه ها را حذف کرد که در این مرحله هست که یک هکر میتونه یک تروجن در سیستم قربانی و Startupآن آپلود کنه و یک BackDoor یا در پشتی در سیستم هدف ایجاد کنه و به وسیله آن به سیستم با امکانات بیشتری نسبت به نت بیوس وصلشه .

خب حالا شروع میکنیم به توضیح و استفاده از نت بیوس ، شما احتیاج به برنامه کمکی ندارید و تمام امکانات لازم در خود ویندوز وجود داره ، هر چند استفاده از برنامه هایی مثل Netbruteخیلی میتونه به شما کمک کنه که شما میتونین از این سایت http://www.rawlogic.com/netbrute آنرا دانلود کنین ، کمترین کاری که این برنامه میکنه مشخص میکنه که در کدام سیستمها قابلیت اشتراک فایلها فعال هست و وقت شما را با وصل شدن و امتحان کرده تمام آیپیها نمیگیره و در وقت شما بسیار صرفه جویی میشه .

البته بهتره در Port Setting برنامه Time out = 300را به مابین ۱۰۰۰۰ - ۱۵۰۰۰ تغییر بدین تا پویش دقیقتری انجام بشه ، ولی هدف ما از این مقاله کار با این ابزارها نیست و هدف آشنا کردن شما با نت بیوس و ظرز کار با نت بیوس ولی بدون این برنامه ها نیز میتونین به هدفتون برسین .

کار هک با این برنامه خدماتی ویندوز یعنی همان نت بیوس به ۵ مرحله تقسیم میشه که سرفصل آنها به این ترتیب هست :

۱- بررسی کردن این نکته که آیپی یا Hostدر نت بیوس فعال شده یا نه .

۲- گذاشتن آیپی یا Host در فایل Host.

۳- پیدا کردن کامپیوتر آماده برای به اشتراک گذاری فایلها .

۴- اگر فایلها با پسورد محافظت میشن پیدا کردن پسورد آن .

۵- در اختیار گرفتن منابع و فایلهای کامپیوتر هدف .

و حالا توضیح و شرح مراحل بالا :

۱- قبل از این که سعی کنیم از نت بیوس استفاده کنیم باید آنرا فعال کنیم و همچنین Sharing باید فعال

باشه و انتخاب شده باشه البته این تکته مهم و امنیتی را در نظر داشته باشین که وقتی شما این امکان را در سیستمتان فعال کنید ، امکان این هست که افراد دیگری نیز در آن لحظه به سیستم شما وصل بشن ، آزمایش این روش یک نوع ریسک از طرف شماست ولی در حالت معمولی حتما این امکان اشتراک فایلها را غیر فعال کنید تا کسی اجازه نداشته باشه به اطلاعات شما در هاردتان از طریقه نت بیوس دسترسی داشته باشه و اگر میخواین از این روش استفاده دایمی بکنید حتما از نظر دفاعی در سطح بالایی قرار بگیرین تا بتونید ارتباطاتتان را تحت کنترل داشته باشین .

اکنون ما باید بفهمیم که در کامپیوتر و سیستم هدف نت بیوس فعال هست یا نه ، چون اگر در هر ۲ کامپیوتر یعنی در کامپیوتر خود و سیستم هدف این سرویس فعال نباشه امکان دسترسی وجود نداره ، برای اینکار ویندوز یک برنامه داره به اسم NBTSTAT.exe این فایل در ویندوز 9xو Meدر پوشه ویندوز و در ویندوز 2000/XPدر پوشه Winnt\System32قرار داره و این فایل فقط از طریقه MS-Dos Promptقابل اجرا هست ، بنابراین MS-DOSرا باز کنید و تایپ کنید :

"NBTSTAT" بدون هیچ دستور و فرمان دیگری ، خروجی اطلاعاتی در مورد این برنامه به شما میده ، اما وقتی که ما قصد داشته باشیم از آن برای دسترسی به یک کامپیوتر دیگر استفاده کنیم از این برنامه به این شکل و این دستور استفاده می کنیم NBTSTAT -A <IP Address> اگر جواب این دستور " Host Not Found" بود به این معنی هست که در سیستم هدف نت بیوس فعال نیست و امکان دسترسی وجود نداره ولی اگر لیستی شامل Nameو Typeو Statusمثل شکل زیر برگردانده شد ، یعنی سیستم هدف آماده برای وصل شدن هست :

C:\>Windows\NBTSTAT -A 213.29.86.155

NetBios Remote Machine Name Table

Name	Type	Status
ONE	<00> UNIQUE	Registered
123	<00> GROUP	Registered
ONE	<03> UNIQUE	Registered
ONE	<20> UNIQUE	Registered
123	<1E> GROUP	Registered
....	....	....

این اطلاعات برای ما مشخص میکنن که چه سرویس هایی در اختیار ما قرار داره که توضیح راجب هر سرویس و امکانات آن بسیار مفصل هست ، اما <20> و نام جلوی آن (ONE)برای ما مهم است چون به ما اطلاع میده که قابلیت اشتراک فایل فعال و در دسترسی ما هست .

۲- حالا ما باید آیپی و sharenameیا همان اسمی که مقابل <20>قرار گرفته را در فایل HOSTSقرار بدیم ، این فایل در این مسیرها قرار داره :

win9x/ME :\Windows

win2000/XP :\Windows\system32\drivers\etc

اگر فایل HOSTSدر سیستم شما موجود نبود به آسانی با یک Editorآنرا بسازین و در شاخه و پوشه ذکر شده قرار بدین ، اما دقت کنین که این فایل نباید پسوند txt.داشته باشد ، فقط "HOSTS" بدون هیچ حرف اضافه تری . برای قرار دادن آیپی و Sharename از یک ویرایشگر معمولی مثل Notepadاستفاده کنید و بعد فایل را Saveکنید .

۳- برای برقراری اتصال به سیستم مورد نظر ، بسته به سیستم عاملی که استفاده میکنید به شکل زیر عمل

کنید :

win9x/ME/2000 : برینStart>Search>Find Computer

WinXP : برین start > Search File or Floder > Computer or People

اکنون آیپی کامپیوتر هدف را وارد کنید و Findرا کلیک کنید و صبر کنید تا اتصال برقرار بشه ، حالا شما در پنجره زیری باید آیپی سیستم هدف را ببینید و یک Locationو یک Comment. با کلیک کردن به روی آیپی وارد ریشه C:\در سیستم هدف خواهید شد ، اگر پنجره ظاهر شد و از شما پسورد خواست ، این به این معنی هست که در سیستم هدف یک ابزار دفاعی قرار گرفته به اسم Password Protectedو شما میتونین از برنامه ای به اسم pqwak برای شکستن این پسورد استفاده کنید که این کار را به روش Brute Forceانجام میده که قاعدتا کمی وقت گیر هست .

اما در اکثر مواقع شما با این مشکل برخورد نمیکنید ، حالا شما به هارد سیستم مورد نظر دسترسی دارین ، البته کار در این حالت کمی کند انجام میشه که این هم بخاطر الگوریتم شبکه هست ، خب شما اکنون میتونین یک سری کارها را در سیستم قربانی انجام بدین که البته بستگی به سطح اختیارات شما در آن سیستم داره ، مراحل ۴ و ۵ را هم در طی مراحل ۳ توضیح دادم ، این مطلبم اشاره کنم که هر دو پروتکل TCPو UDP از نت بیوس پشتیبانی میکنن .

در هر صورت اگر میخواهین از این روش هک کنید در ابتدا باید صبر و تحمل زیادی داشته باشین و بعد پشتکار خوبی داشته باشین ، و بعد با خواندن این مقاله با این برنامه خدماتی کار کنین e6_ اگر هم مشکلی در این زمینه براتون پیس آمد ما در گروه هکران البرز در خدمت شما دوستان عزیز هستیم .

http://groups.yahoo.com/group/hackeraneAlborz
/http://www.hackeranealborz.com
/http://hackeranealborz.persianblog.com

برگرفته از سایت برنامه نویس

www.PishgamSoft.com

محمد سیستم