

ParsBook.Org

پارس بوک، بزرگترین کتابخانه الکترونیکی فارسی زبان

ParsBook.Org



The Best Persian Book library

معرفی برنامه Nmap Scanner

یکی از ابتدایی ترین کارهایی که یک هکر برای هک کردن یک سرور یا کلاینت انجام می دهد پیدا کردن آیپی های آن کامپیوتر مورد نظر و سپس اسکن کردن آن آیپی برای پیدا کردن درگاه ها و پورت های باز روی آن سرور یا کلاینت است ، برای پیدا کردن آیپی روشهای مختلفی وجود دارد ، از ساده ترین راه که تایپ کردن آدرس یک سایت در Internet Explorer و دیدن آیپی در status bar در هنگام لود شدن سایت گرفته تا Whois گرفتن از یک Domain و گرفتن آیپی و اطلاعاتی در مورد سرور و شخص ثبت کننده Domain هست، البته این روشها برای گرفتن آیپی سرور بکار میرود و برای گرفتن آیپی از یک کلاینت روشهای مختلفی از جمله استفاده از فرمان Netstat -NA & Netstat و استفاده از ابزارهای Monitoring و ... بکار برده میشود ولی فرض ما در این مقاله بر این است که شما تمامی این راه ها و روشها را می دانید و حالا می خواهید به مرحله بعدی که اسکن کردن این آیپی ها است بروید ، خب برای این منظور هکرها از قابلیت **Scanning** استفاده میکنند ، که خود به 2 بخش عمده آیپی و پورت اسکنینگ تقسیم میشود که هر کدام تعریف خاص خودش را دارد ، فقط برای آشنایی شما عرض کنم که آیپی اسکنینگ برای مشخص شدن آیپی های فعال در تعداد زیادی آیپی که متعلق به یک ISP هستند استفاده می شود که این راه برای هک کردن کلاینت ها بکار برده میشود و پورت اسکنینگ زمانی استفاده میشود که ما آیپی هایی را مشخص کردیم و حالا می خواهیم پورتهای باز روی آن سیستم را پیدا کنیم و از طریق آن پورتهای باز به سیستم قربانی و یا سرور وصل بشویم که البته خود پورت اسکنینگ نیز چند قسمت دارد که در ادامه مقاله توضیح میدهم . خب برای انجام این کارها ابزارهای اسکنینگ زیادی وجود دارد ، چون هم هکهای حرفه ای و هم هکرای آماتور برای رسیدن به اهدافشان از این برنامه ها استفاده میکنند و این مختص قشر خاصی از هکرها نیست ولی اکثر پورت اسکنرها بر پایه سیستم عامل های مبتنی بر یونیکس مثل لینوکس ساخته شدند ولی بعضی از آنها نسخه ای هم برای ویندوز دارند ، این مقدمه را برای این گفتم که به شما بهترین و قویترین ابزار پویس پورت را

معرفی کنم ، **Nmap** بهترین پورت اسکنر رایگان است که تمام هکرهاى حرفه ای را به سمت خودش کشیده است ، Nmap توسط Fyoder نوشته شده و توسط هکرهایی که با لینوکس کار میکنند استفاده میشود و امکانات زیادی در اختیار هکر قرار میدهد . اگه شما نیز مثل تمام هکرهاى حرفه ای از سیستم عامل های لینوکس استفاده میکنید می توانید Nmap را از این سایت دریافت و استفاده کنید :

http://www.insecure.org/Nmap/nmap_download.html

ولی اگر هنوز با ویندوز کار می کنید باز هم نگران چیزی نباشید چون تیم eEye یک نسخه از این برنامه را بصورت ویندوز در آورده و این نسخه نیز توسط هکرهایی که با ویندوز کار میکنند استفاده می شود که هم اکنون نسخه کامل شده این برنامه با نام **NmapWin v1.3.0** در اختیار هکرهایی که با ویندوز کار می کنند قرار داده شده که شما نیز می توانید این نسخه از Nmap را که حدود ۶ مگابایت حجم دارد را از این سایت دریافت و استفاده کنید :

<http://www.sourceforge.net/projects/nmapwin>

ولی قبلش این نکته را در نظر بگیرید که از NmapWin فقط در ویندوز NT,2000,XP می شود استفاده کرد و نسخه ای از این برنامه برای ویندوزهای دیگر نوشت نشده است . خب من هم چون می دانم اکثر دوستانی که این مقاله را دارند می خوانند از ویندوز استفاده می کنند طرز کار با NmapWin را برایتان توضیح می دهم ، خود Nmap بیشتر از خط فرمان استفاده میکند ولی یک GUI خوب هم برای این برنامه ساخته شده است که به آن Nmap front end می گویند و کار با Nmap ای که تحت لینوکس است را ساده تر کرده که البته NmapWin این دو را با هم ادغام کرده و یک نسخه گرافیکی برای ویندوز حساب می شود ، البته Nmap نسبت به نسخه گرافیکی آن کاملتر و بهتر است و گزینه های بیشتری دارد که حتی می شود یک سیستم را بوسیله فرستادن بسته های زیاد Flood کرد و موجب Crash شدن سیستم قربانی شد ولی با NmapWin نیز میشود این کارها را بصورت کمی محدودتر انجام داد . خب NmapWin را از سایتی که داده ام دانلود و سپس instal کنید و حالا آماده برای آشنا شدن با برنامه و گزینه های آن باشید .

هنگامی که برنامه NmapWin را باز می کنید با گزینه های زیادی مواجه می شوید که من از همان قسمت بالا که به اصطلاح Network Section برنامه می گویند شروع می کنم به توضیح دادن . وقتی برنامه را باز می کنید در قسمت بالای برنامه گزینه Host را می بینید که شما در

این قسمت باید آپی ماشین هدفان را بدهید که هم می تواند یک آپی متعلق به یک کلاینت باشد و هم می تواند تعداد زیادی آپی متعلق به یک ISP و یا چندین سرور باشد ، اگر می خواهید تعدادی آپی برای اسکن شدن به برنامه بدهید چندین راه وجود دارد ، برای مثال می توانید یک رنج آپی را به این صورت بدهید *.218.217 که به این صورت تمام آپی هایی که با 217.218 شروع می شود توسط برنامه اسکن می شود و یا مثلاً اگر رنج را به این صورت 125-102.12.218.217 بدهید تعداد آپی هایی که بین 2 عدد آخر وجود دارد اسکن می شود و در مورد هر آپی در صورت فعال بودن و تنظیم صحیح برنامه اطلاعات زیادی در اختیار شما قرار داده می شود و اگر هم می خواهید پورتهای یک سیستم کلاینت را اسکن کنید آپی آن را در همان قسمت Host وارد می کنید . در سمت راست برنامه در کنار گزینه Host ۲ گزینه دیگر وجود دارد که هر کدام کار خاصی انجام می دهند گزینه اسکن برای شروع کار برنامه بکار می رود البته بعد از دادن آپی های هدف و تنظیم برنامه ، گزینه Stop همانطور که از اسم آن مشخص است برای متوقف کردن عملیات اسکنینگ بکار میرود و این زمانی بکار میرود که شما از اسکنینگ یک آپی منصرف شدید و می خواهید آپی های دیگری را تست کنید . گزینه Help هم که برای کمک به کاربر و آشنا کردن کاربران با این اسکنر بکار میرود و Exit هم که برای خارج شدن از برنامه است .

خب حالا می رسیم به قسمت اصلی برنامه که همان قسمت option folder برنامه حساب می شود و تمام تنظیمات برنامه در این قسمت انجام می گیرد و این قسمت خودش چند قسمت اصلی و فرعی دارد مثل Win32 ,Discover ,Scan ، ... درباره تک تک این گزینه ها در ادامه مقاله برایتان توضیح میدهم ، قسمت دیگر برنامه Output است که در این صفحه خاکستری رنگ نتایج اسکن در مورد یک یا چند آپی نشان داده می شود و اطلاعات ارزشمندی درباره آپی هایی که در قسمت Host وارد کردید در این صفحه نشان داده می شود و در پایین ترین قسمت برنامه Status Bar قرار گرفته است که در سمت چپ آن به شما فرمان هایی نشان داده می شود که شما در هنگام تنظیم برنامه در قسمت option Folder بکار می برید و این فرمان ها برای کسانی مفید است که با برنامه اصلی Nmap که تحت لینوکس است و ظاهر گرافیکی ندارد کار می کنند و باید به جای انتخاب گزینه ها و تنظیم آن این فرمان ها را برای تنظیم بدهید و در سمت راست Status bar شما دکمه سبزی را در آنجا می بینید که این دکمه وقتی کار برنامه متوقف باشد سبز است و وقتی برنامه فعال و در حال اسکن کردن باشد به رنگ قرمز است که در این حالت شما نمی توانید برنامه را تنظیم کنید و

باید منتظر باشید تا عملیات اسکنینگ به پایان برسد و دکمه سبز بشود و سپس شما دوباره برنامه را تنظیم کنید . خب فعلاً با فهرست های اصلی NmapWin آشنا شدید و حالا توضیح در مورد هر کدام از گزینه های Option Folder:

بخش Scan:

این قسمت مهمترین قسمت برنامه NmapWin است که خود به ۲ بخش Mode و Scan Option تقسیم شده است ، ما در قسمت Mode نوع پویش و حالت اسکنینگ را مشخص می کنیم چون همانطور که می دانید ما چند نوع پروتکل در TCP/IP داریم مثل پروتکل کنترل انتقال (TCP) و یا پروتکل UDP و یا پروتکل اینترنت یا همان پروتکل آیپی و همچنین پروتکل پیام کنترل اینترنت (ICMP) و در این قسمت و قسمت Discover از برنامه نیز شما می توانید اسکن های مختلفی در هر کدام از این پروتکل ها داشته باشید . در کل کاری که پورت اسکنرها انجام می دهند اینه که بسته هایی به سمت سیستم هدف که همان آیپی داده شده به برنامه است و تمام پورت های آن می فرستند و امتحان می کنند تا بفهمند چه پورت هایی روی آن سیستم باز هستند و اطلاعات بدست آمده را در اختیار هکر قرار می دهند . در پورت اسکنرهای قوی نوع بسته هایی که فرستاده می شوند را می شود انتخاب کرد که NmapWin در قسمت Option Folder و قسمت Scan و گزینه Mode این امکان را در اختیار شما قرار داده است .

گزینه Connect: قبل از توضیح درباره این نوع اسکن باید عرض کنم که در توضیحات ، من از اصطلاحات رایج TCP/IP استفاده می کنم و اگر بخوام در مورد هر اصطلاح توضیح بدهم از بحثمان در این مقاله دور می شویم و مقاله خیلی طولانی می شود پس لازمه درک این توضیحات آشنایی قبلی شما با TCP و پروتکل های آن است . خب گزینه Connect یک نوع اسکن و پویش از نوع TCP است که سعی می کند تا handshake سه طرفه TCP را با هر پورت هدف روی سیستمی که اسکن می شود را کامل کند ، برای اینکه این موضوع را خوب درک کنید و بفهمید اسکن از نوع TCP Connect به چه صورت است handshake سه طرفه را بیشتر برای کسانی که این مسائل را نمی دانند توضیح میدهم . برای انجام handshake سه طرفه در ابتدا کامپیوتر ما که یک کلاینت است به سمت سرور یک بسته SYN می فرستد که یک درخواست برای اتصال است بعد اگر سرور این درخواست را قبول کند برای سیستم ما یک بسته SYN/ACK ارسال می کند و بعد در مرحله ۲ کامپیوتر ما یک بسته ACK برای سرور می فرستد ، این را هم باید بگویم که تمام اتصالات مجاز TCP مثل FTP , Http , Telnet و ... بوسیله

همین handshake سه طرفه و راهی که در بالا ذکر شد ارتباط برقرار می کنند و به هم دیگر وصل می شوند . ولی احتمال کمی وجود دارد که اسکن از طریق گزینه Connect باعث Crash شدن سیستم قربانی بشود . در ضمن استفاده از این نوع اسکنر کمی خطرناک است چون اگر پورت باز باشد سیستم شما handshake سه طرفه را با یک ACK تمام می کند و بعد با استفاده از بسته های FIN اتصال را قطع می کند که این کار باعث می شود آیبی هکر در log فایل های سرور ثبت بشود و اگر هم که پورت بسته باشد هیچ بسته SYN-ACK توسط سرور برگردانده نمی شود و یا یک بسته RESET فرستاده می شود و این پاسخها به معنی این است که پورت بسته است ، در هر صورت اسکن از طریق گزینه Connect اطلاعاتی از شما را در log فایل ثبت می کند و هکرهاى حرفه ای کمتر از این گزینه برای اسکن استفاده می کنند و بیشتر سعی می کنند از اسکنینگ مخفی تری استفاده کنند.

گزینه SYN Stealth: این نوع اسکن که به آن پورت اسکن TCP SYN هم می گویند پیش فرض اسکنینگ ها در برنامه NmapWin می باشد که چند ویژگی نسبت به گزینه Connect دارد ، اول اینکه این نوع اسکن مخفی تر از پویش Connect است ، دلیلش هم این است که اسکن TCP SYN فقط بسته SYN اولیه را به سمت پورت هدف می فرستد و منتظر جواب SYN-ACK می ماند تا بفهمد که پورت باز است یا نه ، اگر پورت باز باشد و سیستم قربانی بسته SYN-ACK برای سیستم ما بفرستد برنامه Nmap و این گزینه سریع یک بسته Reset برای سیستم قربانی می فرستد تا قبل از اینکه اتصال کامل شود آن را قطع کند پس در این صورت دیگر کامپیوتر ما برای سرور بسته ACK نمی فرستد ، پس مرحله ۲ کلاً در این نوع اسکن بکار گرفته نمی شود ، اگر از طرف سرور یک بسته SYN/ACK برای ما فرستاده بشود یعنی آن پورت باز است و اگر یک بسته Reset یا RST/ACK برسد یعنی آن پورت بسته است . پس همانطور که ملاحظه کردید این نوع اسکن هویت هکر را پنهان میکند . البته اگر سرور برای ثبت وقایع و بسته ها از روترها و فایروالها استفاده کند بوسیله روشهایی می شود به آدرس آیبی هکر در هنگام اسکنینگ از این روش نیز دست یافت . مزیت دیگر اسکن از طریق SYN سرعت این نوع اسکنینگ است چون دو سوم Handshake را انجام میدهد و به همین دلیل از نوع اسکن Connect سریعتر به نتیجه میرسد چون دیگه بسته ACK به سمت سیستم قربانی نمی فرستد و آخرین نکته و ویژگی این نوع اسکن اینه که میشود اگر یک حمله هماهنگ به سمت سرور با این نوع اسکن و فرستادن بسته های SYN بشود به احتمال زیاد (بستگی به قدرت آن سرور و

هماهنگ بودن هکرها) آن سرور Down می شود دیگه چه برسد به کلاینت ها و سیستمهای ضعیف.

گزینه های Null Scan ,Xmas Tree ,Fin Stealth: این نوع پویشها و اسکنها برای سیستمهای ویندوز مثل ۲۰۰۰ ، 9x نوشته نشده است و برای این سیستمها کار نمی کنند چون سیستمهای ویندوز از RFCها در مورد اینکه اگر بسته های Null ,Xmas Tree ,FIN وارد شوند چه زمانی باید Reset فرستاد پیروی نمی کنند ، برای مثال کاری که گزینه FIN Stealth میکند به این صورت است که یک بسته FIN به هر پورت می فرستد که اگر در پاسخ بسته Reset نشان داده بشود یعنی اینکه پورت بسته است و اگر پاسخی دریافت نشود یعنی اینکه ممکن است پورت باز باشد ولی در کل این ۳ گزینه برای اسکن کردن کلاینت ها و سرورهای که از سیستم عامل هایی غیر از ویندوز استفاده میکنند بکار میرود و خیلی هم سودمند است .

گزینه Ping Sweep: این نوع اسکن نیز آبیی های فعال در یک شبکه و در آن رنج آبیی داده شده را پیدا می کند و می شود گفت که این گزینه همان کار آبیی اسکنینگ ها را انجام می دهد و برای این کار برنامه NmapWin یک بسته درخواست ICMP Echo را به تمام آن آبیی ها می فرستد تا مشخص شود که کدام سیستم ها در آن لحظه فعال هستند ، در هر صورت از این گزینه نیز می توانید برای پیدا کردن آبیی های فعال در یک ISP استفاده کنید و سپس به وسیله توضیحاتی که داده شد هر کدام از آن آبیی ها را برای پیدا کردن پورتهای باز اسکن کنید .

گزینه UDP Scan: همانطور که از اسمش پیداست این گزینه برای اسکن کردن پورتهای UDP بکار میرود و برای اینکار یک بسته UDP به پورتهای سیستم هدف می فرستد تا بفهمد آیا پورت UDP در آن سیستم باز است یا خیر ، چون کلاً پروتکل UDP زیاد قابل اطمینان نیست و برعکس TCP قابلیت Handshake سه طرفه را ندارد زیاد روی نتیجه بدست آمده توسط این گزینه نیز نمی شود اعتماد کرد ولی باز هم برای اهداف خاصی این گزینه مفید است و برای کسانی که قصد دارند توسط پورتهای UDP به سیستم قربانی وصل شوند این گزینه خوبی است .

گزینه IP Protocol Scan & ACK Scan: خب گزینه اسکن پروتکل آبیی همانطور که از اسمش مشخص است برای اسکنینگ آبیی ها و مشخص کردن آبیی های فعال و دادن اطلاعاتی در مورد هر آبیی بکار میرود که تقریباً این گزینه همان کار گزینه ping Sweep را انجام میدهد ولی گزینه Ack Scan که بیشتر برای تشخیص فایروالها استفاده می شود و طرز کار آن به این

صورت است که یک بسته با کد بیت ACK را به تمام پورتهای موجود در سیستم قربانی می فرستد و امکان فیلتر کردن بسته ها را در اتصالاتی برقرار شده میدهد و نتایج بدست آمده اطلاعات ارزشمندی را در اختیار هکر قرار میدهد از جمله لیستی از پورتهایی که به اتصالاتی برقرار شده اجازه ورود به شبکه را میدهند که در نهایت به شما کمک می کند تا روترها و فایروالهای یک سرور را پیدا کنید .

گزینه Window Scan : این نوع اسکن تقریباً مثل اسکن ACK است ولی برای فهمیدن باز یا بسته بودن پورت روی چندین سیستم عامل ، روی اندازه TCP و بندوز تمرکز می کند و کلاً این نوع اسکن کاملتر از پویش ACK است .

گزینه RCP Scan & List Scan : اسکن از نوع لیست اسکن تقریباً همان کار اسکن ping Sweep را انجام میدهد ولی بصورت مخفیانه تر و شما می توانید با استفاده از این قابلیت یک اسکن Nmap TCP را از یک سرور FTP که خودش هم خبر ندارد عبور بدهید تا مبدأ حمله را مخفی کنید ولی اسکن از طریق RCP یکی از کاملترین نوع اسکنینگ و سرویسهای RPC را اسکن میکند و برای فرستادن دستورهایش از تمام پورتهای TCP و UDP باز در سیستم قربانی استفاده میکند و در نهایت می فهمد که آیا یک برنامه RPC در حال گوش دادن به پورت است یا خیر . در هر صورت این نوع اسکن برای هکهای حرفه ای خیلی مفید است ، برای کسانی که کاملاً با برنامه های RPC آشنایی دارند و با این نوع اسکن می شود از نقطه ضعفهای امنیتی این برنامه ها اطلاع پیدا کرد و سپس از طریق این حفره های امنیتی به یک سرور نفوذ کرد .

خب این تمام گزینه ها و انواع اسکن ها در برنامه NmapWin و در قسمت Mode در قسمت اسکن بود ولی در بخش اسکن یک گزینه دیگر به اسم Scan Option هم وجود دارد که ۶ گزینه دارد که فقط اولین گزینه آن برای ما کارایی دارد و مورد استفاده قرار می گیرد .

بخش اسکن Option و گزینه Port Range : شما با انتخاب کردن این گزینه و فعال کردن آن می توانید رنج پورتهایی که مایلید در آن سیستم اسکن بشود را بدهید تا پورتهای باز در آن سیستم و در آن رنج پورت را به شما نشان بدهد و اگر این قسمت را شما خالی بزارید در آن سیستم هایی که در Host آبی هایشان را نوشتید تمام پورتها اسکن می شود و اگر فقط یک شماره پورت در این قسمت بدهید فقط آن پورت در آن سیستم اسکن خواهد شد و اگر هم یک رنج مثل ۸۰ - ۲۰۰۰ بدهید تمام پورتهایی که بین این ۲ رنج هستند اسکن خواهد شد . پورتهای مبدأ ۲۵ یا ۸۰ انتخاب خوبی برای شماره پورت ابتدایی بشمار می روند چون پورتهای وب سرور و

میل سرور هستند و ترافیک حاصل از اسکن سیستم سرور را گمراه می کنند و آن فکر میکند که این ترافیک از یک وب سرور که از http استفاده می کند می آید و استفاده از این گزینه ها نیز به شما کمک خواهد کرد .

بخش Discover:

این بخش نیز یکی دیگر از قسمتهای Option Folder برنامه NmapWin است که خود ۴ گزینه دارد و در مورد هر کدام برایتان توضیح میدهم .

گزینه TCP Ping: این گزینه از برنامه برای پینگ در TCP بکار می رود و با فرستادن پینگ که به آن پیام ICMP Echo هم می گویند برای آیی ها و سیستمهای مشخص شده در برنامه می فهمد که کدام یک از آن سیستمها فعال هستند و بعد از این کار شما می توانید پورتهای آن سیستمهای فعال را اسکن کنید .

گزینه TCP+ICMP: این گزینه که پیش فرض قسمت Discover هم است برای پینگ کردن سیستمها در هر ۲ پروتکل TCP و ICMP بکار می رود و در بخش Discover از همه بهتر و مفیدتر است و برای بررسی فایروالهای سرورها نیز می شود از این گزینه استفاده کرد .

گزینه ICMP Ping: این گزینه نیز همانطور که از اسمش پیداست برای پینگ کردن سیستمها در پروتکل کنترل پیام اینترنت (ICMP) بکار می رود و فقط مخصوص این پروتکل است .

گزینه Don't Ping: با فعال کردن این گزینه برنامه هیچ نوع پینگی انجام نمی دهد و کلاً بخش Discover از اسکن برنامه حذف و غیر فعال می شود .

بخش Options:

گزینه Fragmentation: این گزینه زمانی برای ما مفید است که مخفی اسکن کردن ما از نتیجه اسکن برای ما اهمیت بیشتری داشته باشد ، این گزینه از آیی های مبدأ برای اسکن استفاده میکند و به وسیله روشهایی آیی هکر و کلاً هر اطلاعاتی راجع به شخص اسکن کننده را پنهان می کند و بیشتر این گزینه زمانی مفید است که اسکنی از نوع SYN FIN-Xmas و یا Null صورت بگیرد ولی در هر صورت با انتخاب این گزینه کمی از کارایی برنامه و نتیجه پایانی اسکن کم می شود .

گزینه Get Identd Info: این گزینه نیز برای زمانی مفید است که بخواهیم سیستمی را از نوع پویش Connect اسکن کنیم و می شود گفت این گزینه مکمل اسکن Connect بشمار می رود و با انتخاب این گزینه به همراه پویش اسکن اطلاعات ارزشمندی می شود از یک سرور بدست

آورد .

گزینه Resolve All: از این گزینه نیز شما می توانید برای پیدا کردن DNS(domain name server) در سیستم ها و آپی های داده شده به برنامه استفاده کنید ، البته این گزینه بر روی تمام آپی های داده شده به برنامه عمل Reverse Whois را انجام می دهد و برایش فرقی نمی کند آن آپی فعال است یا Down و از همه Whois می گیرد و این گزینه نیز برای پیدا کردن سرورها و DNS ها خیلی مفید است .

گزینه Don't Resolve: این گزینه نیز همانطور که از اسمش مشخص است عمل Reverse Whois را روی هیچ کدام از سیستم ها انجام نمی دهد و از هیچ آپی Resolve نمی گیرد و بیشتر برای زمانی مفید است که شما برای اسکنی که می خواهید انجام دهید احتیاج به سرعت دارید که در این صورت می توانید از این گزینه استفاده کنید .

گزینه Fast Scan: این گزینه نیز احتیاج به توضیح ندارد و مشخص است که با انتخاب این گزینه سرعت اسکن بیشتر می شود ولی وقتی که سرعت بیشتر باشد نتیجه اسکن ضعیف تر از حالت عادی اسکن می شود ولی اگر شما به سرعت احتیاج دارید می توانید از این گزینه استفاده کنید .

گزینه OS Detection: این گزینه که گزینه پیش فرض قسمت Option هم است یکی از مهمترین گزینه های برنامه می باشد که کار آن حدس زدن و فهمیدن سیستم عامل سیستم در حال اسکن است ولی شاید برای شما جالب باشد که چطوری برنامه NmapWin و این گزینه می تواند نوع سیستم عامل را فقط با دانستن آپی آن حدس بزند ، برای این کار Nmap از یک تکنیک به نام کپی برداری از پشته TCP/IP استفاده می کند و با کمک گرفتن از RFC ها بسته هایی را به پورتهای مختلفی روی سیستم هدف می فرستد و چگونگی تغییر شماره سریال در بسته SYN-ACK را بررسی می کند و در نهایت نوع سیستم عامل را حدس میزند .

گزینه Random Host: این گزینه نیز به آپی های داده شده در قسمت Host برنامه توجه نمی کند و آپی هایی را بصورت اتفاقی انتخاب می کند و سپس اسکن میکند .

قسمت Debug و گزینه Debug: این گزینه اولین گزینه قسمت Debug است که در قسمت Option قرار دارد که برای دیباگ کردن بکار میرود و با انتخاب این گزینه نتایج دیباگ را شما می توانید در قسمت Output برنامه ببینید .

گزینه Very verbose & Verbose : این دو گزینه نیز جزئیات و مراحل اسکن و دیباگ را نشان

میدهند که من پیشنهاد می کنم اگر قصد استفاده از گزینه دیباگ را دارید به عنوان مکمل این اسکن از گزینه Very verbose استفاده کنید چون این گزینه نسبت به گزینه verbose کارایی بیشتری دارد و مراحل اسکن و دیباگ را دقیقتر نشان می دهد .

بخش Timing:

این بخش خود دارای ۲ قسمت است که اول قسمت Throttle را برایتان توضیح می دهم :
هکرها با توجه به نوع اسکن و زمانی که دارند سرعت های اسکن مختلفی را انتخاب می کنند که بستگی به سرعت و قدرت سیستم قربانی هم دارد ، برای مثال اگر سرعت سیستم قربانی کند باشد و ما یک نوع اسکن سریع را انتخاب کنیم ممکن است بعضی از پورتهای باز را از دست بدهیم و یا ممکن است آن سیستم بخاطر بسته های زیادی که برایش فرستاده می شود هنگ و Crash کند . این قسمت از برنامه Nmap برای تنظیم سرعت اسکن بکار می رود که گزینه Normal بهترین انتخاب برای این کار است و اگر سیستم شما ضعیف بود و در حال اسکن با این سرعت هنگ کرد از گزینه Polite استفاده کنید که سرعت کمتری دارد و هر بسته را تقریباً در 0/4 ثانیه برای سیستمهای قربانی می فرستد و ۲ گزینه آخر سرعت اسکن را خیلی زیاد می کند و بیشتر برای زمانی خوب هستند که شما وقت کمی برای اسکن دارید و احتیاج به سرعت دارید ولی این نکته را در نظر بگیرید که با سرعت بالا اسکن کردن ضریب اشتباه را بالا می برد و ممکن است بعضی از پورتهای باز مشخص نشود پس بهترین انتخاب گزینه نرمال است که پیش فرض برنامه نیز همین گزینه است .

قسمت Timeouts: این قسمت نیز بیشتر برای زمان بندی هر اسکن و پویش بکار می رود و قابلیت سفارشی کردن زمان اسکن را به شما میدهد ، برای مثال با انتخاب گزینه Host Timeout (ms) و فعال کردن آن شما می توانید زمانی را تعیین کنید که برای هر اسکن صرف بشود و گزینه های دیگر نیز تقریباً به همین منظور هستند و برای زمانبندی انواع اسکن بکار می روند .

بخش Files:

این بخش نیز خود ۲ قسمت دارد که بیشتر برای ذخیره کردن نتایج اسکن بکار می رود .
قسمت Input File: این قسمت تقریباً کاره یک passlist در برنامه های کراکر و brute force را انجام می دهد و برای سریعتر کردن کار اسکن می شود از این قسمت استفاده کرد که در این حالت ورودی از یک فایل که ما انتخاب کرده ایم خوانده می شود .

قسمت Output: با انتخاب این گزینه و فعال کردن این قسمت شما می توانید نتایج بدست آمده از اسکن را که در Output نشان داده می شود را در یک فایل با فرمت های مختلف ذخیره کنید تا بتوانید از روی فرصت پورته ها و حفره های باز روی آن سیستم را مورد بررسی قرار دهید ، با انتخاب گزینه نرمال نتایج بدست آمده بصورت Log فایل و .txt ذخیره می شود و شما می توانید فرمت های دیگری مثل XML و یا Grep را انتخاب کنید .

بخش Service:

این قسمت هم برای سفارشی کردن زمان و روز اسکن آپی های مشخص بکار می رود و برای مثال می شود یک آپی را در این قسمت ثبت کرد و یک روز را مشخص کرد و برنامه در صورت انتخاب گزینه AutoStart در آن روز مشخص خود به خود آن آپی و سیستم را اسکن می کند و حتی شما می توانید دقیقه و ثانیه شروع عملیات اسکن را در این قسمت مشخص کنید و در کل از این قسمت برای سفارشی کردن زمان و روز اسکن استفاده می شود .

بخش Win32:

این بخش نیز که قسمت آخر برنامه NmapWin است برای تنظیم بهتر برنامه در ویندوزهای XP و ۲۰۰۰ می باشد که خود ۲ قسمت دارد که من گزینه های قسمت اول را برایتان توضیح می دهم ، چون قسمت Commands برای کسانی مفید است که با Nmap تحت لینوکس کار کردند و با خط فرمان آن آشنایی دارند ، پس بحث ما روی قسمت اول است .

گزینه No Pcap: وقتی که شما برنامه NmapWin را بر روی سیستم خود نصب می کنید ، اگر دقت کرده باشید می بینید که همراه آن pcap هم نصب می شود که برای ویندوزهای xp , 2000 نوشته شده است و در این ویندوزها می توانید به عنوان مکمل Nmap کارهای پویش را انجام دهید ، با انتخاب این گزینه ، برنامه دیگر از pcap استفاده نمی کند و pcap غیر فعال می شود و اگر این گزینه را انتخاب کنیم برنامه بجای pcap از Raw Socket به صورت پیش فرض استفاده می کند و از آن کمک می گیرد .

گزینه No Raw Socket: اگر این گزینه انتخاب شود Raw Socket غیر فعال می شود و توسط برنامه ، دیگر استفاده نمی شود و اگر گزینه No Pcap انتخاب نشده باشد برنامه از pcap به عنوان مکمل و البته در ویندوزهای ۲۰۰۰ و XP استفاده می کند.

گزینه Force Raw Socket: اگر این گزینه را شما انتخاب کنید دیگر pcap غیر فعال می شود و فقط Raw Socket توسط برنامه استفاده می شود .

گزینه NT4Route: این گزینه نیز برای کاربران سیستم 4.0 NT است که از این نسخه NmapWin در ویندوز خود استفاده می کنند و با انتخاب این گزینه در صورت استفاده از ویندوز NT می شود اطلاعات ارزشمندی در مورد انواع فایروالهای روی سرورها و کلاینت ها بدست آورد .

گزینه Win Trace: این گزینه نیز یکی از بهترین گزینه های برنامه NmapWin است که کار آن استفاده از تکنیک Trace Route برای پیدا کردن روترها و gateway های یک سرور است و با انتخاب این گزینه برنامه برای هر آیی عمل Trace را انجام می دهد و اطلاعات ارزشمندی درباره هر سیستم در اختیار شما قرار می دهد و البته این گزینه کمی از سرعت اسکن را می گیرد ولی به نظر من ارزش این را دارد و شما نیز سعی کنید از این گزینه به عنوان مکمل برنامه و اسکنتان استفاده کنید .

خب دوستان این تمام گزینه های اسکنر NmapWin بود که من سعی کردم شما را با طرز کار هر یک از گزینه ها آشنا کنم ، شما با فهمیدن کار هر یک از این گزینه ها و استفاده درست از آنها می توانید بهترین پویش را از یک سرور انجام دهید و اطلاعات زیادی از یک سرور بدست آورید و سپس راه های مختلف نفوذ به یک سرور را با استفاده از این اطلاعات امتحان کنید تا به هدف اصلی خود که همانا نفوذ کامل به آن سرور است برسید ، امیدوارم از خواندن این مقاله لذت برده باشید و از این اطلاعات در راه های درست و ایمن کردن سرورها استفاده کنید .

ParsBook.Org

پارس بوک، بزرگترین کتابخانه الکترونیکی فارسی زبان

ParsBook.Org



The Best Persian Book Library