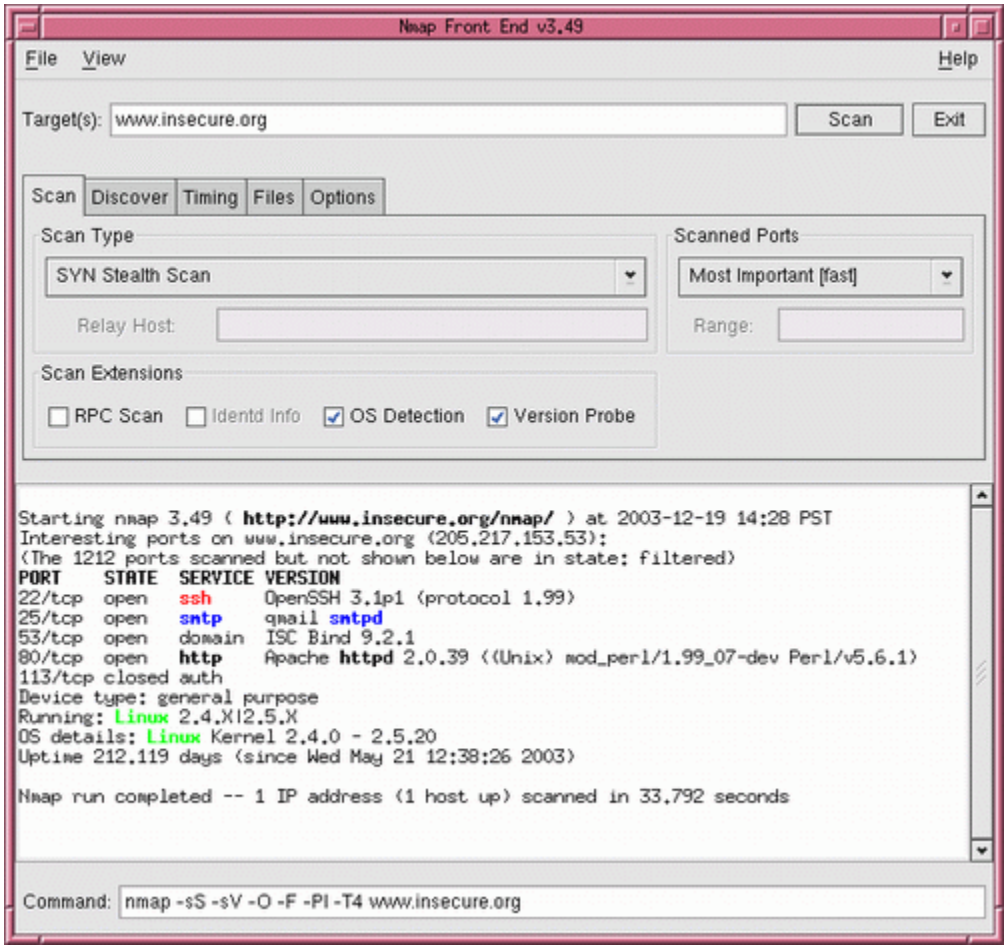
روش های آنالیز کردن امنیت سرورها و کلاینت

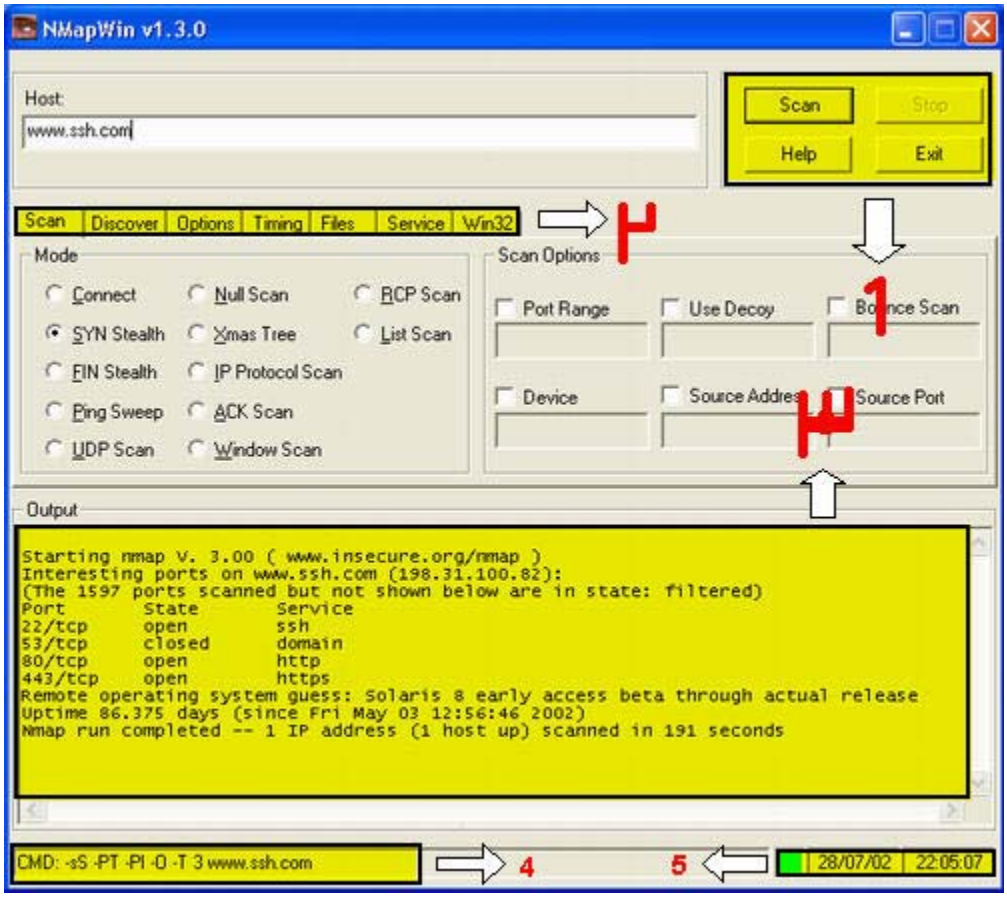
نـــوع مقاله : امنیت شبکه
سطح مقاله : مبتدی - مـــتـــــوسط
کـــــاربران : مـدیران امنیتـي

سلام دوستان، در این درس قصد داریم شما را با روش های آنالیز کردن امنیت سیستم ها آشنا کنیم و در کنار آن موثرترین پورت اسکنر را به شما معرفی کنیم. همانطور که می دانید و در مقالات گذشته گفته شد یکی از ابتدایی ترین کارهایی که یک هکر برای هک کردن یک سرور یا کلاینت انجام می دهد پیدا کردن آدرس های IP آن کامپیوتر مورد نظر و سپس اسکن کردن آن IP برای پیدا کردن درگاه ها و پورت های باز روی آن کامپوتر است، برای پیدا کردن IP روشهای مختلفی وجود دارد، از ساده ترین راه که تایپ کردن آدرس یک سایت درInternet Explorer و دیدن آیپی درstatus bar در هنگام لود شدن سایت گرفته تا Whois گرفتن از یک Domain و گرفتن IP و اطلاعاتی در مورد سرور و شخص ثبت کننده Domain است، البته این روشها برای گرفتن IP سرور بکار می رود و برای بدست آوردن IP یک سیستم کلاینت از روشهای مختلفی از جمله استفاده از فرمان Netstat -NA & Netstat و استفاده از ابزارهای Monitoring مثل ProPort و ... استفاده می شود که که در درس های گذشته این روش ها را توضیح دادیم و تصور من 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 IP ها است بروید، برای این منظور هکرها از قابلیت Scaning استفاده می کنند که خود به 3 بخش عمده IP و Port و Vulnerability اسکنینگ تقسیم می شود که هر کدام تعریف خاص خودش را دارد، فقط برای آشنایی شما عرض کنم که IP Scaning برای مشخص شدن آیپی های فعال در تعداد زیادی IP که متعلق به یک ISP هستند استفاده می شود که این راه برای هک کردن کلاینت ها بکار برده می شود و پورت اسکنینگ زمانی استفاده می شود 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 با استفاده از حفره های آسیب پذیر سرویس های نصب شده بر روی کامپیوتر به سیستم قربانی و یا سرور وصل شویم. پورت ها درگاه های کامپیوتر هستند و بدون باز بودن آنها ارتباطی بین دو سیستم برقرار نمی شود. با نصب سرویس ها و برنامه های مختلف پورت ها باز می شوند و باز بودن یک پورت بدون هیچ دلیلی در یک سیستم معنایی ندارد. برای انجام پویش از یک سیستم ابزارهای اسکنینگ زیادی وجود دارد ، چون هم هکرهای حرفه ای و هم هکرای آماتور برای رسیدن به اهدافشان از این برنامه ها استفاده می کنند و این مختص قشر خاصی از هکرها نیست ولی اکثر پورت اسکنرها بر پایه سیستم عامل های مبتنی بر یونیکس مثل لینوکس نوشته شده اند ولی بعضی از آنها نسخه ای هم برای ویندوز دارند. حتی مدیران شبکه ها نیز برای سرورهای خود از امکان اسکنینگ استفاده می کنند تا شبکه خود را از نظر امنیت مورد ارزیابی قرار دهند که برای این عزیزان در مقالات بعدی اسکنرهای آسیب پذیری متعددی را که به Vulnerability Scanner معروف هستند معرفی خواهیم کرد. در این مقاله به شما یکی از بهترین و قویترین ابزار پویش پورت را معرفی می کنیم، Nmap بهترین پورت اسکنر رایگان است که امکانات زیادی را برای هکرها و یا مدیران امنیت سرورها فراهم کرده است، Nmap توسط Fyoder نوشته شده و توسط هکرهایی که با لینوکس کار می کنند استفاده می شود. اگر شما نیز مثل تمام هکرهای حرفه ای از سیستم عامل های لینوکس استفاده می کنید 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 افرادی که با ویندوز کار می کنند استفاده می شود که هم اکنون نسخه اصلی این برنامه با نام NmapWin v1.3.1 در اختیار علاقه مندانی که با ویندوز کار می کنند قرار داره شده که شما نیز می توانید این نسخه از Nmap را که حدود 5 مگابایت حجم دارد را از این سایت دریافت و استفاده کنید :
http://download.insecure.org/nmap/dist/nmapwin_1.3.1.exe
البته این نکته را در نظر بگیرید که از NmapWin فقط در ویندوز NT,2000,XP می توان استفاده کرد و نسخه ای از این برنامه برای ویندوزهای دیگر نوشته نشده است. تصور می کنم اکثر دوستانی که این مقاله را مطالعه می کنند از ویندوز استفاده می کنند. به همین دلیل طرز کار با NmapWin را برای شما توضیح می دهیم، خود Nmap بیشتر از خط فرمان استفاده می کند ولی یک GUI خوب هم برای این برنامه ساخته شده است که به آن Nmap frontend می گویند. این رابط گرافیکی کار با Nmap ای که تحت لینوکس است را ساده تر کرده است که در عکس بالا مشخص است. البته NmapWin این دو را با هم ادغام کرده و یک نسخه گرافیکی برای ویندوز محسوب می شود. Nmap نسبت به نسخه گرافیکی آن کاملتر و دارای دستورات بیشتری است که حتی با استفاده از آن ممکن است یک سیستم بوسیله بسته های زیادی که از طرف اسکنر به سمت آن برای مشخص شدن پورت های باز ارسال می شود Flood و Crash کند.
NmapWin را از سایتی که داده ام دانلود و سپس install 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 توضیح می دهم. وقتی برنامه را باز می کنید در قسمت بالای برنامه گزینه Host را می بینید که شما در این قسمت باید آیپی ماشین هدف را بدهید که هم می تواند یک آیپی متعلق به یک کلاینت و یا تعداد زیادی آیپی متعلق به یک ISP و یا چندین سرور باشد، اگر می خواهید تعدادی آیپی برای اسکن شدن به برنامه بدهید چندین راه وجود دارد، برای مثال می توانید یک Range آیپی را به این صورت بدهید 217.218.*.* که به این صورت تمام آیپی هایی که با 217.218 شروع می شود توسط برنامه اسکن می شود و یا مثلاً اگر Range را به این صورت 217.218.12.102-125بدهید تعداد آیپی هایی که بین 2 عدد آخر وجود دارد اسکن می شود و در مورد هر آیپی در صورت فعال بودن و تنظیم صحیح برنامه اطلاعات زیادی در اختیار شما قرار داده می شود و اگر هم قصد دارید پورتهای یک سیستم کلاینت را اسکن کنید آیپی آن را در همان قسمت Host وارد می کنید. در سمت راست برنامه در کنار گزینه 4Host گزینه دیگر وجود دارد که هر کدام کار خاصی انجام می دهند (شماره 1) گزینه Scan برای شروع کار برنامه بکار می رود البته بعد از دادن آیپی های هدف و تنظیم برنامه ، گزینه Stopهمانطور که از اسم آن مشخص است برای متوقف کردن عملیات اسکنینگ بکار می رود. گزینه Help نیز برای کمک به کاربر و آشنا کردن کاربران با این اسکنر و Exit هم که برای خارج شدن از برنامه است.



بخش اصلی برنامه قسمت option folder می باشد و تمام تنظیمات برنامه در این قسمت انجام می گیرد که خود چند قسمت اصلی و فرعی دارد مثل Win32, Discover, Scan... درباره تک تک این گزینه ها در ادامه مقاله توضیح می دهیم (شماره 2) قسمت دیگر برنامه Outputاست که در این صفحه خاکستری رنگ نتایج اسکن در مورد یک یا چند IP نشان داده می شود و اطلاعات ارزشمندی درباره آیپی هایی که در قسمت Host وارد کردید در این صفحه بدست می آورید (شماره 3) 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 ، این فرمان ها را برای تنظیم بدهید (شماره 4) در سمت راست Status bar نیز دکمه سبز رنگی است که این دکمه وقتی کار برنامه متوقف باشد سبز است و وقتی برنامه فعال و در حال اسکن کردن باشد به رنگ قرمز در می آید 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 دوباره برنامه را تنظیم کنید (شماره 5) با فهرست های اصلی NmapWin آشنا شدید و اکنون توضیح در مورد هر کدام از گزینه های Option Folder:

بخش Scan:

این قسمت مهمترین قسمت برنامه NmapWin است که خود به 2 بخش Modeو Scan Optionتقسیم 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/IPداریم مثل پروتکل کنترل انتقال (TCP)و یا پروتکل UDPو یا پروتکل اینترنت یا همان پروتکل IP و همچنین پروتکل پیام کنترل اینترنت (ICMP)و دراین قسمت و قسمت Discoverاز برنامه نیز شما می توانید اسکن های مختلفی درهر کدام از این پروتکل ها داشته باشید. در کل کاری که پورت اسکنرها انجام می دهند این است که بسته هایی به سمت سیستم هدف که همان IP داده شده به برنامه است و تمام پورت های آن می فرستند و امتحان می کنند تا مشخص شود چه پورت هایی بر روی آن سیستم باز هستند و اطلاعات بدست آمده را در اختیار کاربر برنامه پویشگر قرار می دهند. در پورت اسکنرهای قوی نوع بسته هایی که فرستاده می شوند را می شود انتخاب کرد که NmapWinدر قسمت Option Folderو قسمت Scanو گزینه Mode این امکان را در اختیار شما قرار داده است.

گزینه Connect: قبل از توضیح درباره این نوع اسکن باید ذکر کنم که در توضیحات ، من از اصطلاحات رایج TCP/IP استفاده کرده ام و این مطالب برای کسانی قابل درک است که آشنایی قبلی با TCP و پروتکل های آن داشته باشند که در مقالات گذشته در مورد شبکه ها و پروتکل های آن مطالبی را ارائه داده ایم. گزینه Connectیک نوع اسکن و پویش از نوع TCP است که سعی می کند تا handshake سه طرفهTCP را با هر پورت هدف روی سیستمی که اسکن می شود را کامل کند ، برای اینکه این موضوع را کامل درک کنید که پویش از نوع TCP Connectبه چه صورت است handshake سه طرفه را بیشتر برای کسانی که این مسائل را نمی دانند توضیح می دهیم. برای انجام handshakeسه طرفه در ابتدا کامپیوتر ما که یک کلاینت است به سمت سرور یک بسته SYNمی فرستد که یک درخواست برای اتصال است. در مرحله بعد اگر سرور این درخواست را قبول کند برای سیستم ما یک بسته SYN/ACKارسال می کند و سپس در مرحله 3 کامپیوتر ما یک بسته ACK برای سرور می فرستد و ارتباط بین دو کامپیوتر و شبکه برقرار می شود. تمام اتصال های مجاز TCPمثل FTP, Http, Telnetو ... بوسیله همین handshakeسه طرفه و راهی که در بالا ذکر شد ارتباط برقرار کرده و به همدیگر وصل می شوند. ولی احتمال کمی وجود دارد که اسکن از طریقه گزینه Connectباعث Crash شدن سیستم قربانی بشود. این نکته قابل ذکر است که استفاده از این نوع پویش کمی برای هکر خطرناک است چون اگر پورت باز باشد سیستم هکر 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 IP هکر در log فایلهای سرور ثبت شود و اگر پورت بسته باشد هیچ بسته SYN-ACKتوسط سرور برگردانده نمی شود و یا یک بسته RESET فرستاده می شود و این پاسخها به معنی این است که پورت بسته می باشد، در هر صورت اسکن از طریقه گزینه Connectاطلاعاتی از شما را در log فایل ثبت می کند و هکرهای حرفه ای کمتر از این گزینه برای اسکن استفاده می کنند و اکثر آنها سعی می کنند از اسکنینگ مخفی تری استفاده کنند تا ردپایی از خود در سرور قربانی خود برجای نگذارند.

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 ، دلیل آن هم این است که اسکن TCP SYN فقط بسته SYNاولیه را به سمت پورت هدف می فرستد و منتظر جواب SYN-ACKمی ماند تا بفهمد که پورت باز است یا خیر، اگر پورت باز باشد و سیستم قربانی بسته SYN-ACK را برای سیستم ما ارسال کند برنامه Nmapو این گزینه سریع یک بسته Resetبرای 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 ACKنمی فرستد ، بنابراین مرحله 3 در این نوع اسکن بکار گرفته نمی شود، اگر از طرف سرور یک بسته SYN/ACKبرای ما فرستاده شود به این معنی است که آن پورت باز است و اگر یک بسته Resetیا RST/ACKبرسد یعنی آن پورت می باشد. بنابراین این نوع اسکن هویت هکر را پنهان می کند. البته اگر سرور برای ثبت وقایع از برنامه های خاص خود و برای کنترل بسته ها از روترها و فایروالها استفاده کند تا حدودی امکان اسکن کامل و دقیق سیستم از هکرها گرفته می شود. امکان دیگر پویش از طریقه SYNسرعت این نوع اسکنینگ است چون دو سوم Handshake را انجام می دهد و به همین دلیل از نوع اسکن Connect سریعتر به نتیجه می رسد زیرا دیگر بسته ACKرا به سمت سیستم قربانی ارسال نمی کند و آخرین نکته این نوع اسکن در این است که اگر یک حمله هماهنگ به سمت سرور با این نوع پویش و فرستادن بسته های SYNبشود ممکن است (بستگی به قدرت آن سرور و هماهنگ بودن هکرها) سرور قربانی Downشود، پس با نصب IDSو فایروال های سخت افزاری و با بستن پورت های نامشخص و بی استفاده راه مقابله با هکرها را پیش بگیرید.

گزینه های Fin Stealth ,Xmas Tree ,Null Scan: این نوع پویشها برای سیستمهای ویندوز مثل 2000 ، 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 ,FINوارد شوند چه زمانی باید Resetفرستاد پیروی نمی کنند، برای مثال کاری که گزینه FIN Stealth انجام می دهد به این صورت است که یک بسته FIN به هر پورت می فرستد که اگر در پاسخ بسته Resetنشان داده شود به معنی بسته بودن پورت است و اگر پاسخی دریافت نشود این نتیجه گرفته می شود که ممکن است پورت باز باشد ولی در کل این 3 گزینه برای اسکن کردن کلاینت ها و سرورهایی که ازسیسنم عامل هایی غیر از ویندوز استفاده می کنند بکار می رود و خیلی هم سودمند است .

گزینه Ping Sweep: این نوع اسکن نیز آیپی های فعال در یک شبکه را پیدا می کند و می توان گفت که این گزینه همان کار IP اسکنینگ ها را انجام می دهد و برای این کار برنامه NmapWinیک بسته درخواست ICMP Echoرا به تمام آن IP ها ارسال می کند تا مشخص شود که کدام سیستم ها در آن لحظه فعال هستند، در هر صورت از این گزینه نیز می توانید برای پیدا کردن آیپی های فعال در یک ISPاستفاده کنید و سپس به وسیله توضیحاتی که داده شد هر کدام از آن IP ها را برای پیدا کردن پورتهای باز پویش کنید.

گزینه UDP Scan: این گزینه برای اسکن کردن پورتهای UDPبکار می رود و برای اینکار یک بسته UDP به پورتهای سیستم هدف می فرستد تا متوجه شود که آیا پورت های UDPدر آن سیستم باز است یا خیر. پروتکل UDPپروتکل قابل اطمینانی نیست و بر عکس TCPقابلیت Handshake سه طرفه را ندارد ولی برای سرویسهایی مثل Real Playerو برنامه هایی که به تبادل آهنگ و فایل های تصویری و صوتی در شبکه می پردازند و به سرعت بیشتر از امنیت احتیاج دارند این پروتکل انتخاب اول است. برای کسانی که قصد دارند پورتهای UDPیک سیستم را برای امتحان امنیت سرویس های نصب شده بر روی کامپیوتر که از پورت های UDPاستفاده می کنند، این گزینه مفید است.

گزینه IP Protocol Scan & ACK Scan: این گزینه برای اسکنینگ آیپی ها و مشخص کردن آیپی های فعال و دادن اطلاعاتی در مورد هر IP بکار می رود که تقریباً این گزینه همان کار گزینه ping Sweepرا انجام می دهد ولی گزینه Ack Scan 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 اتصالهای برقرار شده می دهد و نتایج بدست آمده اطلاعات ارزشمندی را در اختیار هکر قرار می دهد از جمله لیستی از پورتهایی که به اتصالهای برقرار شده اجازه ورود به شبکه را می دهند که در نهایت به آنها کمک می کند تا روترها و فایروالهای یک سرور را پیدا کنند.

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

گزینه RCP Scan & List Scan: اسکن از نوع لیست اسکن تقریباً همان کار اسکن ping Sweepرا انجام می دهد ولی بصورت مخفیانه تر و شما می توانید با استفاده از این قابلیت یک اسکن Nmap TCPرا از یک

سرور FTPکه خود نیز خبر ندارد عبور بدهید تا مبدأ حمله را مخفی کنید ولی اسکن از طریقه RCPیکی از کاملترین نوع اسکنینگ است و سرویسهای RPCرا اسکن می کند و برای فرستادن دستورهایش از تمام پورتهای TCPو UDPباز در سیستم قربانی استفاده کرده و در نهایت می فهمد که آیا یک برنامه RPCدر حال گوش دادن به پورت است یا خیر. در هر صورت این نوع اسکن برای هکرهای حرفه ای خیلی مفید است، برای کسانی که کاملاً با برنامه های RPCآشنایی دارند و با این نوع اسکن می شود از نقطه ضعفهای امنیتی این برنامه ها اطلاع پیدا کرد و سپس از طریقه این حفره های امنیتی به یک سرور نفوذ کرد.
این تمام گزینه ها و انواع اسکن ها در برنامه NmapWinو در قسمت Modeدر قسمت اسکن بود ولی در بخش اسکن یک گزینه دیگر به اسم Scan Optionهم وجود دارد که 6 گزینه دارد که فقط اولین گزینه آن برای ما کارایی دارد و مورد استفاده قرار می گیرد.
بخش اسکن Optionو گزینه Port Range: شما با انتخاب کردن این گزینه و فعال کردن آن می توانید Range پورتهایی که مایل هستید در آن سیستم اسکن بشود را بدهید تا پورتهای باز در آن سیستم و در آن Range پورت را به شما نشان بدهد و اگر این قسمت را شما خالی بگذارید در آن سیستم هایی که در Hostآیپی های آنها 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 Range مثل 80 - 2000 بدهید تمام پورتهایی که بین این 2 رنج هستند اسکن خواهد شد. پورتهای مبدأ 25 یا 80 انتخاب خوبی برای شماره پورت ابتدایی بشمار می روند زیرا پورتهای وب سرور و سرویس SMTPمیل سرور هستند و ترافیک حاصل از اسکن ، سرور را گمراه می کنند و سرور گمان می کند که این ترافیک از یک وب سرور که از httpاستفاده می کند می آید.
بخش Discover:
این بخش نیز یکی دیگر از قسمتهای Option Folder برنامه NmapWin است که خود 4 گزینه دارد و در مورد هر کدام توضیح می دهیم.
گزینه TCP Ping: این گزینه از برنامه برای پینگ در TCPبکار می رود و با فرستادن پینگ که به آن پیام ICMP Echo هم می گویند برای آیپی 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 2 پروتکل TCPو ICMPبکار 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: برای پینگ کردن سیستمها در پروتکل کنترل پیام اینترنت(ICMP) می توان از این گزینه استفاده کرد و فقط مخصوص این پروتکل است.
گزینه Don't Ping: با فعال کردن این گزینه برنامه هیچ نوع پینگی انجام نمی دهد و 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 هکر اهمیت بیشتری داشته باشد ، این گزینه از آیپی های مبدأ برای اسکن استفاده می کند و به وسیله روشهایی آیپی هکر و 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 Nullصورت 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 Connectاسکن کنیم و می توان گفت این گزینه مکمل اسکن Connect بشمار می رود و با انتخاب این گزینه بهمراه پویش اسکن اطلاعات ارزشمندی می شود از یک سرور بدست آورد.
گزینه Resolve All: از این گزینه نیز شما می توانید برای پیدا کردن (domain name server)DNSها در سیستم ها و آیپی های داده شده به برنامه استفاده کنید ، البته این گزینه بر روی تمام آیپی های داده شده به برنامه عمل Reverse Whois را انجام می دهد و برای آن فرقی نمی کند آن IP فعال است یا Downزیرا از همه آنها Whois می گیرد. این گزینه نیز برای پیدا کردن سرورها و DNS ها خیلی مفید است.

گزینه Don't Resolve: این گزینه عمل Reverse Whois را روی هیچ سیستمی انجام نمی دهد 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 آدرس IP 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 می زند.
گزینه Random Host: این گزینه نیز به آیپی های داده شده در قسمت Host برنامه توجه نمی کند و آیپی هایی را بصورت اتفاقی انتخاب می کند و سپس اسکن می کند.
قسمت Debugو گزینه Debug: این گزینه اولین گزینه قسمت Debug است که در قسمت Option قرار دارد که برای دیباگ کردن بکار می رود و با انتخاب این گزینه نتایج دیباگ را شما می توانید در قسمت Outputبرنامه ببینید .
گزینه Very verbose & Verbose : این دو گزینه نیز جزئیات و مراحل اسکن و دیباگ را نشان می دهند که من پیشنهاد می کنم اگر قصد استفاده از گزینه دیباگ را دارید به عنوان مکمل این اسکن از گزینه Very verboseاستفاده کنید چون این گزینه نسبت به گزینه verboseکارایی بیشتری دارد و مراحل اسکن و دیباگ را دقیقتر نشان می دهد .

بخش Timing:

این بخش خود دارای 2 قسمت است که در ابتدا قسمت Throttleتوضیح می دهیم:
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 به خاطر بسته های زیادی که به سمت آن فرستاده می شود هنگ و Crashکند. این قسمت از برنامه Nmapبرای تنظیم سرعت اسکن بکار می رود که گزینه Normalبهترین انتخاب برای این کار است و اگر سیستم شما ضعیف بود و در حال اسکن با این سرعت هنگ کرد از گزینه Politeاستفاده کنید که سرعت کمتری دارد و هر بسته را تقریباً در 0/4ثانیه برای سیستمهای قربانی می فرستد و 2 گزینه آخر سرعت اسکن را خیلی زیاد می کند و بیشتر برای زمانی مفید 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 می دهد ، 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 2 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 forceرا انجام می دهد و برای سریعتر کردن کار اسکن می شود از این قسمت استفاده کرد که در این حالت ورودی از یک فایلی 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 Outputنشان داده می شود را در یک فایل با فرمتهای مختلف ذخیره کنید تا بتوانید از روی فرصت پورتها و حفره های باز روی آن سیستم را مورد بررسی قرار دهید، با انتخاب گزینه نرمال نتایج بدست آمده

بصورت Logفایل و txt. ذخیره می شود و شما می توانید فرمتهای دیگری مثل XML و یا Grep را انتخاب کنید.

بخش Service:

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

بخش Win32:

این بخش نیز که قسمت آخر برنامه NmapWin است برای تنظیم بهتر برنامه در ویندوزهای XP و 2000 می باشد که خود 2 قسمت دارد که ما گزینه های قسمت اول را توضیح می دهیم ، 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 متوجه شده اید که همراه آن pcap هم نصب می شود که برای ویندوزهای 2000 , xpنوشته 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 Socketغیر 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 2000 و XP استفاده می کند.

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

گزینه NT4Route: این قسمت نیز برای کاربران سیستم NT 4.0است که از این نسخه NmapWinدر ویندوز خود استفاده می کنند و با انتخاب این گزینه در صورت استفاده از ویندوز NTمی توان 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 NmapWinاست که کار آن استفاده از تکنیک Trace Routeبرای پیدا کردن روترها و gatewayهای یک سرور است. با انتخاب این گزینه برنامه برای هر آیپی عمل Traceرا 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 اسکن خود استفاده کنید.

دوستان این تمام گزینه های اسکنر NmapWin بود که برای شما آنها را شرح دادیم، 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 پورت های باز آن امتحان کنید تا از میزان امنیت سرور خود و یا کامپیوترهای دیگر مطلع شوید و توسط راه هایی که در مقالات بعدی تیم آشیانه ارائه می شود این حفره های آسیب پذیر را از بین ببرید تا سیستمی همیشه ایمن داشته باشید. امیدواریم از خواندن این مقاله لذت برده باشید و از این اطلاعات در راه های درست و ایمن کردن سرورها استفاده کنید.

نویسنده مقاله: بهروز کمالیان

http://www.ashiyane.ir