بسم الله الرحمن الرحیم

آشنایی با اسکنرهای آسیب پذیری
Vulnerability Scanners

هر روزه در نرم افزارهای گوناگون مشکلات برنامه نویسی زیادی پیدا می شود که به این مشکلات Bug می گویند.این Bug ها یا توسط گروه های تست که وابسته به شرکت مشخصی هستند که برنامه ای را تولید می کند پیدا شده و ترمیم می شوند و یا بیشتر مواقع توسط گروه های Bug Finder که از هکرهای برنامه نویس تشکیل شده است ، پیدا می شوند.اگر این باگ ها توسط گروه هکرها پیدا شود ، به سرعت به سایت هایی که آسیب پذیری های مختلف را همراه با گزارش کامل نحوه ی پیداکردن آسیب پذیری و دلیل ایجاد آن و نرم افزاری که آسیب پذیری در آن پیدا شده است ، گزارش داده می شود و به این ترتیب اکثر هکرها از این موضوع با خبر می شوند.به این آسیب پذیری هاVulnerability می گویند.از برخی از این آسیب پذیری ها می توان سوء استفاده کرد و به همین دلیل از امنیت کامپیوترها و شبکه های کامپیوتری کاسته می شود و می تواند عواقب جبران نا پذیری مانند حمله ی کرم ها و ویروس ها از طریق آسیب پذیری موجود بر روی سیستم را به دنبال داشته باشد.به همین دلیل شرکت های امنیتی نرم افزارهایی را جهت پیدا کردن این آسیب پذیری ها بر روی کامپیوترها نوشته اند که به آن ها Vulnerability Scanner یا اسکنر آسیب پذیری می گویند.این برنامه ها کمک بسیار شایانی در بالا بردن سطح امنیتی کامپیوترها می کند.

طی سال های اخیر، چندین آسیب پذیری های امنیتی در سیستم عامل های مختلف حتی لینوکس پیدا شده است که ویروس نویسان زیادی از این آسیب پذیری ها استفاده کرده و اقدام به نوشتن ویروس کرده اند. در شبکه های کامپیوتری وجود کوچک ترین حفره ای چه در Server و یا چه در Client بسیار خطرناک است زیرا با آلوده شدن یک سیستم و مقاوم نبودن سیستم های دیگر ، بسیار آسا کل شبکه آلوده شده و خسارت های زیادی را به بار می آورد. از همین رو وجود چنین اسکنرهایی برای کشف حفره های امنیت بسیار ضروری است.سیستم عامل لینوکس یک سیستم کاملا امن تر از سیستم عامل ویندوز می باشد به شرطی که آسیب پذیری خاصی نداشته باشد.اغلب موارد امنیتی گزارش شده در لینوکس که می توان از آن ها سوء استفاده کرد ، به صورت محلی یا Local بوده و قابلیت استفاده از یک کامپیوتر دیگر برای حمله به دیگری را ندارد و تنها در هنگام استفاده از این آسیب پذیری ها به هکر دسترسی سطح ریشه و یا root را می دهد که حساب مدیر و مهم ترین حساب در لینوکس می باشد.اما بعضی از برنامه های تحت لینوکس مانند برنامه های FTP و یا Conference دارای نواقصی می باشند که اگر هکری از این آسیب پذیری ها استفاده کند و وارد سیستم شود و حساب سطح ریشه را نداشته باشد ، می تواند با استفاده از آسیب پذیری محلی برای گرفتن سطح ریشه و حساب root استفاده کند.مانند آسیب پذیری جدیدی در سیستم Mambo که یکی از برنامه های وب تحت لینوکس می باشد علاوه بر هکرها ویروسی نیز برای سوء استفاده از این آسیب پذیری منتشر شده است.

تکلیف سیستم عامل ویندوز نیزمشخص است! در تمامی برنامه های اصلی مرتبط با سیستم عامل مانند برنامه های کار با اینترنت و مرورگرها ، برنامه های استفاده از سخت افزارها ، برنامه های کنترل سیستم عامل و تعدادی از برنامه های آفیس و حتی ویژوال استودیو نیز آسیب پذیری های مختلفی کشف شده است.مساله ی واقعا بحث برانگیز بر سر امنیت ویندوز ، پیدا شدن اولین آسیب پذیری امنیتی در Internet Explorer تنها 15 دقیقه بعد از پخش این برنامه بود که همه را به شگفتی واداشت.

اسکنرهای امنیتی می توانند تمامی آسیب پذیری های گفته شده به جز آسیب پذیری های مربوط به مرورگرهای وب را کشف کنند.این نکته را نیز لازم است یادآوری کنیم که اسکنرهای امنیتی هیچ وقت جایگزین یک هکر حرفه ای برای سنجیدن میزان امنیت حاضر بر روی شبکه یا یک سیستم نمی شود.

نحوه ی کار اسکنرهای آسیب پذیری :
در مجموع اسکنرهای آسیب پذیری ، ابزار خودکاری هستند که برای اسکن میزبانان (Host) و شبکه ها جهت پیدا کردن نقطه ضعف های امنیتی و آسیب پذیری های مشخص به کار می روند.برخی از این ابزار فروشی هستند و در سایت های شرکت های تولید کننده یافت می شوند.همچنین برخی رایگان هستند و قابلیت دانلود رایگان را دارند.
اسکنر Network Associates Cyber Cop و اسکنر Internet Security Scanner (ISS) ، از اسکنرهای مهم تجاری محسوب می شوند.این ابزار اساسا یک سری از بررسی های خودکار را در برابر هدف اجرا می کنند.هر اسکنر دارای بانک اطلاعاتی مختص به خو است که به منظور بررسی هدف برای تعیین آسیب پذیری ها از آن استفاده می کند.
اسکنرهای امنیتی به دو دسته ی کلی تقسیم می شوند :

1. اسکنرهایی که به طور کلی با بانک اطلاعاتی کامل برای پیدا کردن تمامی آسیب پذیری ها تا تاریخ معینی استفاده می شوند
2. اسکنرهایی که فقط برای یافتن یک آسیب پذیری به کار می روند

دسته ی اول اسکنرهایی هستند که دارای بانک اطلاعاتی راجع به آسیب پذیری هایی هستند که تاریخ معینی در بانک اطلاعاتی آنان گنجانده شده است
دسته ی دوم اسکنرهایی هستند که تنها یک آسیب پذیری مشخص و بسیار خطرناک را پیدا می کنند.به عنوان مثال شرکت .eeye Digital Security Inc پس از پیدا شدن آسیب پذیری های Dcom و Plug and Play اسکنرهای مخصوص این آسیب پذیری ها منتشر کرد تا متخصصان امنیت شبکه بتوانند کامپیوتر های آسیب پذیر را یافته و آن آسیب پذیری آن ها را اصلاح کنند تا از ورود هکرها و ویروس ها به وسیله ی این دو باگ به کامپیوتر کاربران جلوگیری کنند.
برخی دیگر از اسکنرها به دنبال آسیب پذیری های برنامه های تحت وب و پورتال ها مانند PHP Nuke می پردازند که تعداد آن ها کم است.این نوع اسکنرها به دنبال آدرس های URL مشخصی در سایت هدف می گردند و یا کدهایی را همراه با برخی آدرس ها در سایت هدف اجرا می کنند که غالبا این دستورات مربوط به حملات SQL Injection و یا XSS و برخی از آسیب پذیری های CGI می باشند.Wishker یک از اسکنرهای CGI است که به دنبال آسیب پذیری های موجود در برنامه های قابل اجرا تحت وب که با زبان CGI یا Common Gateway Interface نوشته شده اند می پردازد.
در صورتی که آسیب پذیری ای در بانک اطلاعاتی اسکنر نباشد ، اسکنر قادر به یافتن آن آسیب پذیری نیست به همین دلیل باید بانک اطلاعاتی اسکنرها هر چند هفته یک بار و یا ماهانه ((بسته به نوع کار استفاده کننده)) به روز رسانی یا Update شود.موضوع به روز بودن بانک اطلاعاتی یکی از نکات بسیار مهم برای متخصصان امنیت شبکه و همچنین هکرها برای یافتن آسیب پذیری های جدید است.
نحوه ی کار اسکنرها بسیار آسان است به این صورت که :

1. پس از دریافت آدرس آی پی قربانی یا URL آن به آن وصل شده و شروع به گشتن پورت های باز می کند
2. نوع پورت را که برای چه سرویسی است بر اساس اطلاعات پایگاه داده مشخص می کند
3. اگر به سرویس خاصی تعلق داشت به اسکن آن می پردازد تا از آن آسیب پذیری ای پیدا کند به این ترتیب که مانند یک مهاجم کدها و دستورات آسیب پذیری معینی را اجرا کرده و منتظر جواب می ماند که اگر کد عمل کرد و شماره ی پورت ، نام سرویس که پورت ارایه می کند ، نام نرم افزاری که پورت به واسطه ی آن باز شده و نسخه ی ویرایش آن را در صفحه ی اصلی اسکنر می نویسد در غیر این صورت تنها نشماره ی پروت و نام سرویس آن را می نویسد و در برخی موارد که شماره ی پورت باز با هیچ یک از شماره پورت های موجود در بانک اطلاعاتی متطابقت نداشته باشد بسته به اسکنر پیغامی مبنی بر "نا مشخص بودن پورت" داده می شود.

و در مورد اسکنرهای برنامه های تحت وب:

1. URL قربانی را دریافت کرده و به دایرکتوری اصلی سایت که حاوی آدرس تمامی صفحات و حتی خود صفحات است وصل می شود
2. به دنبال نام و آدرس صفحاتی که ممکن است آسیب پذیری هایی در آن ها موجود باشد می گردد ((بر اساس بانک اطلاعاتی خود))
3. کدها را بر روی صفحاتی که پیدا کرده است ، اجرا می کند.

اسکنرهای Host-Based و Network-Based:

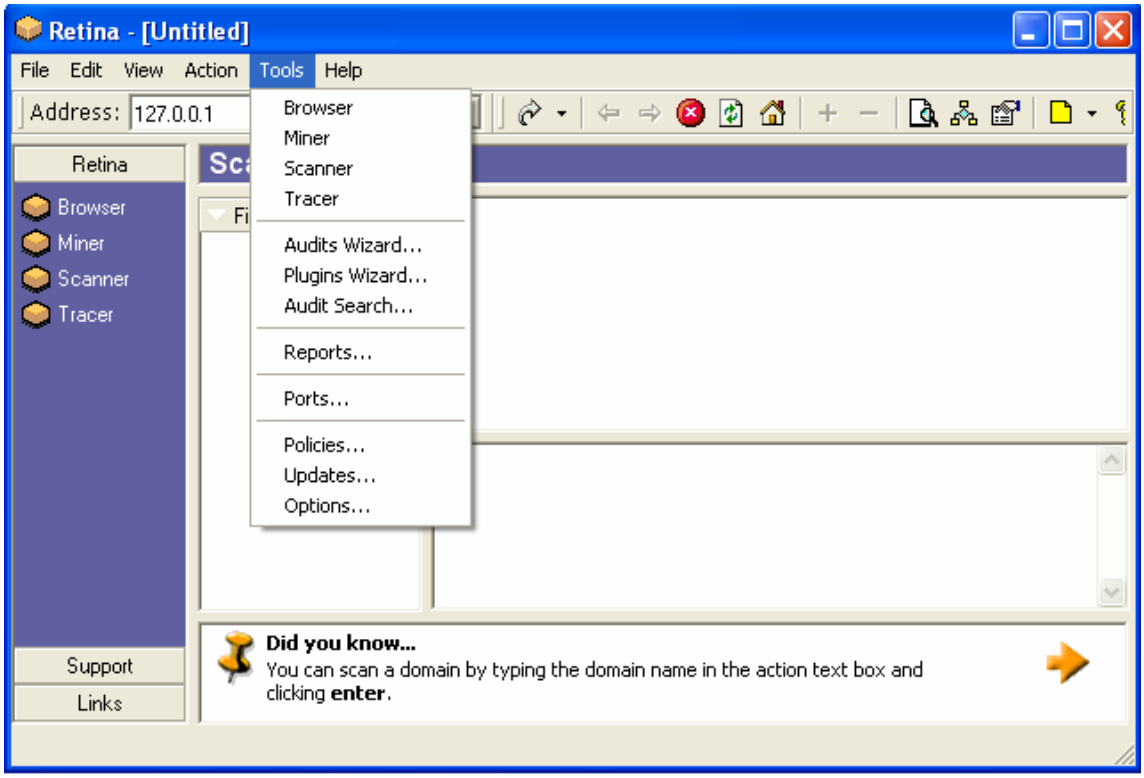
دو نوع اسکنر خودکار با نام های host-based و network-based موجود می باشند.اسکنرهای network-based از یک سیستم مبدا به سمت یک سیستم مقصد به جستجوی آسیب پذیری ها می پردازند.این اسکنرها از سیستم راه دوری مانند یک سیستم Laptop بدون این که در شبکه عضو باشند ، کار خود را آغاز می کنند درست مانند یک هکربرای یافتن آسیب پذیری جهت نفوذ به سیستم هدف.برعکس اسکنر host-based به میزبان از سیستم مبدا به سیستم مقصد به جستجوی آسیب پذیری می پردازند.این نوع اسکنرها به نصب نمایندگی نرم افزار در سرویس دهنده نیاز دارند. این نمایندگی پس از این که آسیب پذیری های یافت شده را دسته بندی کرد ، آن ها را به ایستگاه مدیریتی گزارش می کند.اسکنرهای network-based در جستجوی آسیب پذیری های که می توان به صورت راه دور و یا Remote از آن ها استفاده کرد هستند.مانند آسیب پذیری های IIS ، Buffer Overflow ، DoS و همچنین مجوزهای ضعیف SSL و مجوزهای دیگر ، عدم داشتن رمز عبور برای یک حساب مدیریتی و یا معمولی ، پیدا کردن یک رمز عبور ضعیف و در نهایت سرویس دهنده هایی با تنظیمات امنیتی غلط.البته هنگام به کارگیری این اسکنرها باید نهایت دقت را داشته باشید.اسکنرهای network-based قابلیت تست حملات DoS را دارا می باشند و اگر به طور غلط تنظیم شوند می توانند یک حمله ی واقعی را بر روی سیستم مورد اسکن پیاده سازی نمایند.به همین دلیل یک آزماش کننده بی تجربه با دستکاری اسکنر می تواند صدمات جبران ناپذیری را به بار آورد.اسکنرهای host-based به نمایندگی در سیستم هدف نیاز دارند تا بتوانند آسیب پذیری ها را در آن پیدا کنند.یک مزیت این نوع اسکنرها این است که به عنوان مثال در یک شبکه که 1 سرور و 4 سرویس گیرنده وجود دارد ، مدیر شبکه می تواند اسکنر اصلی را بر روی سرور نصب کند و نمایندگی ها را در سیستم های سرویس گیرنده و سپس در هر زمان می توان سیستم ها را اسکن کرد.شکل 1 نمونه ای از کار یک اسکنر host-based را نشان می دهد.البته این کار بازهم نیاز به تنظیمات خاصی دارد و به عنوان مثال اگراسکنر در سیستم هدف به طور دقیق پیکربندی نشود و یا این که فایروال و مجوزهای امنیتی آن را به عنوان یک عامل غیر مجاز شناسایی کنند ، اسکن بی نتیجه خواهد بود.اما هرگز کار این اسکنرها با کار اسکنرهای network-based اشتباه نگیرید.

False Positive چیست؟

گاهی یک اسکنر آسیب پذیری هایی را در یک سیستم پیدا می کند که همچین آسیب پذیری در آن سیستم نیست.به این خطا False Positive می گویند که ممکن است در هر اسکن یک یا دو مورد مشاهده شود.

نحوه ی کار با اسکنرهای آسیب پذیری :

هر اسکنر به طور جداگانه ای برای انجام اسکن تنظیم شده اند.اما پیکر بندی آن ها برای انجام یک اسکن تقریبا شبیه دیگری است.به عنوان مثال همه ی اسکنرهای آسیب پذیری در منوی Tools خود مواردی که در عکس می بینید را دارند :



البته این نکته را یادآوری می کنم آموزش کامل یک اسکنر آسیب پذیری زمان زیادی را می طلب و در غالب یک مقاله نمی گنجد.امیدوارم مطالب گفته شده باعث افزایش اطلاعات شما شده باشد.

لینک دانلود برخی از اسکنرهای معتبر :

Retina Network Security Scanner از شرکت eeye Digital Security:

http://www.eeye.com/html/products/retina/index.html

X-Scan از X-Focus :((حجم: 3 مگابایت))

http://www.xfocus.org/programs/200507/18.html

GFI LANguard Network Security Scanner از GFI :((حجم: 15.9 مگابایت))

http://software.gfi.com/languardnss7.exe

Shadow Security Scanner از Safety-lab :((حجم: 9.6 مگابایت))

http://mirror1.safety-lab.com/SSS.exe

لینک دانلود کرک این اسکنرها را می توانید با مراجعه به وبلاگ www.siahacker.blogfa.com پیدا کنید.

Copyright© by Siahacker
2005 – 2006 All right Reserved
Email:Siahacker@gmail.com