۱۰ راه آسان برای مبارزه با هکرها

هکرها همیشه در پی شکار هستند؛ شکار ضعفهای موجود در یک سیستم.

از سوی دیگر همیشه راه هایی نیز برای بالا بردن ضریب ایمنی سیستم

وجود دارد. بنابراین آنچه از این نگرش تراوش می کند، این است که

هکرها به دنبال پیدا کردن حفره های جدید برای حمله هستند. آنها از

چه روشهایی بهره می گیرند تا به موفقیت برسند و نحوه ایمن کردن

سیستم چگونه است نیز دو روی یک سکه به شمار می آید. آنچه که این

مقاله به آن می پردازد، راه های آسان ایمن کردن یک سیستم براساس

حفره شناسی است که به طور خلاصه در ده مورد ارائه می شود:

۱- انجام تستهای اسکن :

هدف از این کار، روشن شدن سرحد تمام ورودی ها از اینترنت به شبکه داخلی یا بالعکس است.

راهبر یک سیستم با اسکن کردن دست کم ۲روز یک بار باید ورودی های سیستم های خود را به طور دقیق چک کند تا با آنالیز دقیق ، تغییرات خاص و غیرمنتظره را به عنوان یک علامت خطر در نظر گیرد. معمولا سازمان های بزرگ تا تعداد کاربران بالای ۱۰۰تا، به طور دقیق و منظم نمی توانند این وظیفه خطیر را انجام دهند، لذا بدل بسیار مناسب در این زمینه همانا فایروال است که با انتخاب مناسب یک فایروال خوب نرم افزاری و سخت افزاری توامان با یک آرشیتکت مناسب چاره ساز اساسی خواهد بود. معمولا برخی سرحدهای ورودی از اینترنت به شبکه داخلی از سوی راهبر، قابل کنترل نیست.

پس لزوم یافتن سرحدهای ناشناخته که منبع اصلی برای هکرها در جهت

نفوذ به شبکه قلمداد می شود، ضروری به نظر می رسد. اولین راه ایمن کردن شبکه ، شناسایی سرحدهای ورودی سیستم با اسکن ها و اسکنرهای مناسب است.

LANGuard و یا Angry Ipscanner برای سیستم های ویندوز و NMAP برای سیستم های عامل لینوکس و یونیکس قابل استناد است.

۲- انجام تستهای حمله و نفوذ:

تستهای حمله و نفوذ، راهی آسان با هدف یافتن سریع ورودی های نفوذپذیر در منظر یک شبکه داخلی است.

برای انجام این کار ۲نوع حمله و نفوذ را تدارک ببینید: حمله از روی LAN یا شبکه محلی خودتان یا حمله از بیرون از LAN مثلا از یک خط Dialup خانگی برای حمله به شبکه خودتان که برای این کار یک رایانه را از شبکه خارج کرده و بدون کارت شبکه و با مودم به اینترنت وصل شده و شروع به حمله کنید. نوع حملات در وهله اول پیدا کردن پورتهای قابل

نفوذ و بعد راه اندازی یک دیکشنری Attack روی Hyperterminal یا (Telnet در ویندوز) و یا با محیط Shell و Terminal در یونیکس و لینوکس برای خواندن کلمه عبور Root و... پس راه دوم و رمز موفقیت شما به عنوان راهبر سیستم ، این است که خودتان به خودتان حمله کنید و نقاط ضعف و قوت خود را بیابید. بدی سیستم های ویندوز این است که نمی توانید خودتان Patch یا پس دستوری برای آن بنویسید و تنها می توانید وجود حفره را گوشزد کنید و با دستکاری در رجیستری ویندوز با ترفندهای امنیتی مناسب در Regedt32 با حق رایت کامل جلوی آنها را بگیرید؛ اما اگر open source هستید براحتی با DeBugger یا سایر برنامه ها یک برنامه نویسی جالب روی شبکه انجام دهید تا سیستم خود را secure کنید. در ویندوز سطوح متفاوتی برای کاربران در client های آنها تعریف کرده ؛ اما همیشه راه ورودی خودتان به عنوان Admin سیستم را باز بگذارید. در ضمن نام کلمه Admin را در تمام سیستم عامل ها تغییر داده و کاربرتان را در حد یک Power user محدود کرده و اجازه دسترسی به فایل های شبکه را به وی بدهید تا ضریب ایمنی بالاتر رفته و درصد ورود ویروس و انواع حملات به زیر ۱۰درصد

از خارج و ۱۵درصد در داخل کاهش یابد.

۳- راه اندازی سیستم آگاه سازی کاربران :

این مبحث بیشتر به مهندسی اجتماعی در داخل یک شبکه و آگاه سازی کاربران از وجود حفره های موجود یا حفره های احتمالی مربوط است.

این نکته در عین پیش و پا افتاده بودنش بسیار حایز اهمیت است و برعکس آنچه فکر می شود باید به آن بها داد حتی اگر به قیمت تمسخر راهبر تمام شود. هیچ اشکالی ندارد تمام کاربران از کلمه های عبور سخت و بالای ۱۲حرف استفاده کنند. در کنار آن راه اندازی Policy برای تعویض هفتگی کلمه عبور از سوی کاربران و ایجاد قوانین سخت در این باره بسیار مفید خواهد بود. کاربرانی که از شبکه اخراج شده یا بیرون می روند بلافاصله باید account آنها برای همیشه نابود شود. وقتی با ویندوز کار می کنید و پس دستوری می آید، سعی کنید خودتان به عنوان راهبر روی تمام سیستم ها آن را نصب کنید؛ اما معمولا راهبران تنبل هستند و در عوض کردن کلمه عبور خود اهمال کاری می

کنند. به دلیل ورود تعداد بی شمار ویروس روی شبکه ها بخصوص اسبهای تراوا که از پورتهای ۳۳هزار و... استفاده می کنند، سعی کنید سیستم عامل ها را با وجود نصب ضدویروس هرازچندگاهی فرمت اساسی کرده و با چک کردن رایانه کاربران و کنترل برنامه های نصب شده از صحت سیستم آنها مطلع شوید. وجود یک سیستم مریض در شبکه به کل ماشین ها آسیب خواهد زد.

٤- پیکره بندی صحیح فایروال ها(دیواره آتش):

اگر برنامه های گران قیمت فایروال بخرید؛ اما آن را درست نصب نکنید براحتی راه نفوذ هکرها را آسان کرده اید. اگر در سازمان حساسی هستید، ابتدا به ساکن از فایروال های دست نویس موثقان خود استفاده کنید و اگر قادر به انجام این کار نیستید، فایروال را حتما با License بخرید و فکر نکنید که خرید یک سی دی به قیمت ناچیز واقعا همان فایروالی است که مد نظر آرشیتکتور شبکه است.

نه اصلا این طور نیست.

چرا که اسم و فایروال شما به هر حال به سرور مرکزی شرکت سازنده وصل می شود و وای به حالتان اگر شما سارق شناخته شوید. بنابراین بستگی به نوع سازمان و اهمیت آن به فایروال ها رسیدگی کنید و در وهله اول نوع پیکره بندی آن بسیار مهم است.

برای شبکه های بیزینس ترافیک خطوط بسیار مهم است و طراحی چندین Zone جدا و قرار دادن فایروال های مناسب بر سر راه هر Zone راه مناسبی است که می توان در نظر گرفت.

حتی ۲پورت ٤٤٠ برای SSL و یا ۸۰ برای ترافیک عادی نیز خطرآفرین است و چون باز بودن آنها برای نوع تبادل دیتا ضروری است باید با یک برنامه مناسب برای پرفورمنس شبکه به هر نوع ترافیک مصنوعی و غیرعادی شک کرده و سیستم ها را به دقت بررسی کنید. حتی وقتی تمام پورت ها را ببندید، مطمئن باشید که راه نفوذ هکر از همان پورت باز است و کافی است با یک اسب تراوا که روی پورت ۸۰ نیز کار می کند به جان سرور یا شبکه شما بیفتد، آن وقت همه چیز به ظاهر خوب است ، اما شبکه شما Zombie برای حملات قرار می گیرد، بدون آن که

متوجه باشید. همه چیز عادی است ، اما ترافیک شما به شدت بالاست.

این زنگ خطر کاملا جدی است که باید به آن توجه داشت.

یک پورت باز، یک در باز محسوب می شود و هر فایروال بسته به نوع آن تعاریف خاصی برای تنظیم در نظر گرفته است.

فایروال مانند روتر نیست ؛ بلکه توانایی تنظیم ترافیک و ورودی و خروجی دیتا را به شما نمایش می دهد. اگر روی یونیکس هستید حتما یک برنامه نویس شبکه استخدام کنید تا به وسیله او بتوانید هر روز حفره های جدید را بپوشانید و تنظیمات مناسب با کار کاربران ارائه دهید.

۵- اعمال سیاست های سخت برای کلمه های عبور:

از کاربران بخواهید اسم همسر، فرزند، تلفن خود یا شماره هویت ملی خود را به عنوان کلمه عبور انتخاب نکنند. از آنان بخواهید کلمه های عبور را بیشتر از ۱۲حرف انتخاب کنند. از آنها بخواهید پس از مرور اینترنت ، تمام پوشه های خود به عنوان History, cookie و... را پاک کنند. تمام کلمه های عبور Guest را در شبکه از میان ببرید. حتما کلمه های عبور برخی از اشخاص مهم در شبکه را نزد خود روی یک رایانه بدون اتصال به شبکه نگه دارید. سیستم روسای برتر خود را به اینترنت وصل نکنید. برای آنها یک رایانه با مودم بدون کارت شبکه در نظر بگیرید تا به بیرون وصل شوند (نه با رایانه خودشان ، بلکه یک رایانه بدون داشتن اطلاعات محرمانه). کلمه عبور account ناشناس روسای خود را هر روز عوض کنید و سعی کنید از یک جای بخصوص account نگیرید. اگر کار ضروری پیش آمد یک اتاق به عنوان کافی نت در سازمان خود راه بیندازید تا میزان ریسک به حداقل برسد. از کارتهای هوشمند به عنوان فاکتور اصلی authentication روی نوت بوک ها و سایر سیستم ها استفاده کنید. به کاربران خود بگویید هنگام عوض کردن کلمه عبور از همان کلمه سابق با حرف جدید در انتهای آن استفاده

نکنند. با رعایت این نکات بسیار ساده باور کنید ضریب ایمنی شما بسیار بالا می رود.

۶- از میان بردن همه Commentsها روی Source کدهای وب سایت:

Commentsها اغلب اوقات نقش پشت پرده application ها را بازی می کنند و هرگونه قصور و کوتاهی در نادیده گرفتن آنها باعث رسیدن یک جستجوگر حرفه ای به درون طراحی اصلی یک بانک اطلاعاتی ، یک شبکه و یا سیستم های حامی applicationها می شود. Commentsها، کدها و دستورهای اصلی برای نوشته شدن نام کاربر و کلمه عبور در برنامه های مختلف را در درون سمیکولون ها جای می دهد که با پاک کردن هر کامنتس در وب سایت می توان مانع رسیدن یک حمله کننده به source code شد و جلوی حملات احتمالی را گرفت.

هر کامنتسی باعث دسترسی یک کاربر از راه دور به سیستم می شود و کدهای آن وقتی در دسترس هکر قرار گیرد، وی براحتی با تکنیک های

exploit از آن سوءِاستفاده می کند و به قلب سیستم شما نفوذ می کند.

به عنوان مثال comment this is a یعنی آنچه بعد از نقطه ویرگول در یک برنامه جا می گیرد یک کامنتس به حساب می آید که همان پشت پرده یک خط برنامه با دستور اصلی است و می تواند در هر جای یک فایل هنگام نوشته شدن برنامه قرار گیرد. بنابراین یک راهبر حرفه ای برخوردار از وب سایت باید کامنتس ها را حذف کند تا کسی نتواند به سورس کدهای برنامه نوشته شده دسترسی پیدا کند.

۷- پاک کردن همه قراردادهای از پیش تعریف شده سیستم(Default):

اغلب اوقات Defualtها، انواع تستها و صفحات Sample یا صفحات نمونه (example) آسیب پذیر است و از سوی هکرها به عنوان راه ورود آسان بهره برداری می شود. انواع تستها می تواند مستقیما خود را به وب سرور و بانک اصلی آن رهنمون شود. exploitهای پیش پا افتاده بیشتر در این سطح ظاهر می شوند و کاربر با چندین بار امتحان یک حفره می تواند بدون اجازه وارد شود. این وارد شدن می تواند ورود به شبکه یا وب سرور را در بر گیرد. همین صفحات نمونه می تواند حمله

کننده را به سوی فایلهای کلمه عبور به صورت Text راهنمایی کند و کل امنیت سیستم را به خطر اندازد. یک exploit دیگر مانند Buffer-overflows نیز می تواند مسلسل وار دستورهای مخرب حمله کننده را روی سرور اجرا کند و کنترل سیستم را به دست هکر بسپارد.

۸- از کار انداختن همه سرویس های غیرضروری از همه ابزارهای موجود روی ماشین :

این نکته بسیار اهمیت دارد که راهبر، هر نوع سرویس غیرضروری را که روی ماشین استارت شده است ، متوقف کند و مانع ورود غیرقانونی هکرها شود. برخی سیستم ها براحتی با اسکن ساده سرویس های باز خود را نشان می دهند. مثلا اگر به اف.تی.پی نیازی نیست باید کاملا از کار بیفتد تا کسی از آن سوئ استفاده نکند.

برای مطمئن شدن حفره های موجود در سیستم می توانید به سراغ سایت http://www.esecurityonline.com/ بروید و ماشین خود را امتحان کنید تا به شما بگوید کجای سیستم نفوذپذیر است.

(**اگر سرورتان سری است ، نباید به این گونه سایتها وصل شوید، بلکه از مشاوره های حضوری و غیراینترنتی برخوردار شوید.**) بعضی

سرویس ها به طور خودکار روی سرور شما تنظیم شده و برخی نیز استارت خورده است.

با چک کردن کامل آن و مقایسه آن با کارهایی که وب سرورتان انجام می دهد، می توانید به سرویس های غیرضروری پی ببرید. به عنوان یک سیستم ساده باید Net Bios روی سیستم خود را از کار بیندازید تا کسی نتواند حتی روی LAN اطلاعات زیادی از شما به دست بیاورد

۹- ردیابی سیستم های مزاحم :

گاهی یکی از کاربران شما به مسائل هک علاقه دارد و خروارها فایل روی سیستم خود ذخیره می کند.

از آنجا که اغلب اوقات این کاربران صفرکیلومتر محسوب می شوند، ناخودآگاه یک اسب تروا را هم روی هارد خود نگه می دارد و بدون آن که این ویروس را خنثی کند، به عنوان یک دوست از روی درایو خود پذیرایی می کند، غافل از آن که این اسب خود میزبان یک هکر شده است ، بدون آن که کسی بفهمد. طور دیگر به قضیه بنگرید. شما یک سیستم ادیت متصل به وب سرور دارید. آیا این سیستم باید اینترنت را مرور کند؟ نه.

آیا کاربران سیستم باید روی ماشین خود خروارها آهنگ و موسیقی نگه دارد؟ نه.

آیا این کاربر متصل به وب سرور باید با همان ماشین ادیت چت کند؟ نه.

حتی کارت صدا هم روی این ماشین ادیت متصل به سرور حکم سم را دارد. کاربران مسوول و راهبران مسوولیت شناسی که این موضوع را درک می کنند سعی می کنند ضمن استفاده نکردن غیرضروری از ماشین از یک رایانه جانبی شخصی برای امورخصوصی خود استفاده کنند. دوباره تاکید می شود استفاده از کافی نت های سازمانی ، راه حل مناسبی برای این کاربران دیوانه مرور کردن اینترنت هنگام کار با ماشین ادیت متصل به وب سرور اصلی محسوب می شود. راهبر باید هر روز اطلاعات خود را به روز کند و با آگاهی از جدیدترین حفره ها خود را در یک مبارزه بی امان برای مقابله با هکرهای شناخته و ناشناخته صرف کند.

۱۰- خودروی خود را همیشه به دزدگیر مجهز می کنید که هنگام خطر با صدای هشداردهنده شما را از وجود یک مزاحم آگاه کند.

این نکته ما را به سوی هدفی مهمتر و امنیت فیزیکی سیستم ها رهنمود می کند. بنابراین امنیت فیزیکی و دسترسی افراد غیرمجاز به سیستم ها به طور حضوری نیز دلمشغولی دیگری است که باید به آن توجهات کافی مبذول شود. مثلا اسرار مهم غیر متصل به شبکه رایانه ای و ذخیره شده روی سی دی از دست هکرها در امان است ؛ اما از دست دزدان حرفه ای نه.

نصب تجهیزات تصویری و صوتی و ضبط تمام وقایع در اتاق سرور در سازمان های بزرگ ، اصلی انکارناپذیر است.

قرار دادن کلمه عبور و کارتهای هوشمند و بیومتریک برای تردد و نیز آن روی سکه ماجراست.

بسیاری از هکرها نتوانستند اسرار هسته ای امریکا در لس آلاموس را به دست آورند، اما یک سارق توانست تمام اطلاعات ذخیره شده روی سی دی را ببرد. بنابر این امنیت فیزیکی از اطلاعات رایانه ای نیز کمتر از امنیت غیرفیزیکی نیست.