ایجاد سیستم عامل امن ملی برای مراکز حساس کشور

محمدرضا هژیرپسند
محقق و مشاور امنیت نرم افزار
مدیر گروه برنامه نویسی و وب مجتمع فنی تهران (مرکزی گیلان)
mH_p0rtal@yahoo.com

چکیده

استفاده از سیستم عامل های غیر خریداری شده که دارای مشکلات بروز رسانی میباشند نقطه ضعف بسیار بزرگی میباشد که به نفوذگران خارجی اجازه میدهد تا به سیستم های دولتی و مراکز حساس نفوذ پیدا کنند . ایجاد و راه اندازی یک سیستم عامل امن برای مراکز حساس میتواند بهترین راه کار برای جلوگیری از این نوع حملات باشد. نرم افزارهای پیش نهادی در این مقاله هر کدام به طور واقعی نوشته شده است و مرحله تست خود را گذرانده است.

کلمات کلیدی

Operation System – Linux – Secure OS – File System checking – OS Level Network Monitor – Anti Malware

۱ –مقدمه

با گسترش روز افزون حملات و ویروس ها برای جمع اوری اطلاعات و یا تخریت اطلاعات فضای سایبری کشور نیاز به ارایه راه کار های امنیتی و پیاده سازی آنها میباشد. با مروری بر ویروس های stuxnet - duqu و flame و دیگر ویروس های که شاید به طور محسوس تر به کار خود ادامه میدهند و همچنین نفوذ به وب سایت ها دولتی کشور , وجود فایروال ها و یا آنتی ویروس ها میتواند تا حدی در مقابل این حملات ایستادگی کنند. برای طراحی چنین حملاتی افراد با شبیه سازی حملات بر روی سیستم هایی که دارای همان ویژگی ها هستند میتوانند با یافتن و یا استفاده از حفره های امنیتی که پچ نشده اند و یا حفره های Zero – Day که به معنی حفره های انتشار نشده میباشد , به تولید ورم ها و بد افزار های خاص بپردازند. ویروس stuxnet که برای تخریب تجهیزات هسته ای ایران و چند کشور دیگر ساخته شده بود از یک حفره 0-day که در نرم افزار WinCC/SCADA میباشد استفاده میکرد. همچنین در این ویروس یک root kit که برای ارسال اطلاعات به وب سرور های خارج از کشور نیز پیش بینی شده بود . ویروس duqu نیز که به عقیده بسیاری وابسته به ویروس stuxnet میباشد اما نحوه کارکردش کمی متفاوت میباشد. این ویروس به منظور جمع آوری اطلاعات و ارسال آن که از طریق استفاده از یک حفره منتشر نشده در Microsoft word ساخته شده است.

در جدیدترین کشفیات , بد افزاری به نام flame که به گفته محققین یکی از پیشرفته ترین و پیچیده ترین بد افزار های موجود میباشد نیز در شبکه کشور کشف شد. این بد افزار که به صورت یک روبات عمل میکند توانایی دریافت دستور خودکشی میباشد که میتواند تمامی آثار خود را از سیستم قربانی پاک کند. پس از بررسی چندین بد افزار میتوان به نبود سیستم های جلوگیرنده و مانیتورینگ بومی اشاره کرد . سیستم های امنیتی موجود همگی از یک روال برای چک کردن و شناسایی نرم افزار های مخرب استفاده میکنند و این خود باعث میشود ویروس نویسان با استفاده از دانش قبلی نسبت به موانع راه خود به راحتی آنها را پیش رو

بگذارند. از این رو ساخت و توسعه ی سیستم های امنیتی و جمع اوری آنها در یک سیستم عامل که به صورت یک پارچه به محافظت از اطلاعات بپردازند امنیت سیستم را بسیار بیشتر از وجود یک آنتی ویروس و یا فایر وال غیر بومی تظمین میکنند.

1-2 چک کردن نواحی مختلف توسط File System Monitoring

در اکثر نفوذ هایی که به یک وب سرور میشود و یا در آلوده سازی های که معمولا توسط یک ویروس انجام میشود یک فایل و یا چندین فایل ساخته و یا در سیستم ویرایش میشود.چک کردن این کار در ویندوز و یا در سیستم عامل های یونیکسی توسط نرم افزاری که نوشته شده است به نام دیده بان انجام میشود. به طور مثال اگر یک سرور وب در یک سازمان به کار خود بپردازد و ویروسی به آن سرور نفوذ کند و بتواند تمامی نود های شبکه را آلوده سازد میتواند توسط این روش به راحتی شناسایی و جلوی آن گرفته شود.و یا اگر یک وب سایتی مورد نفوذ قرار گیرد اما به نحوی باشد که ظاهر سایت تغییری نکند و هدف این باشد که کاربران و یا مدیران سایت با مراجعه به صفحه خاصی و یا دانلود فایل به خصوصی دچار بدافزاری گردند همچنین این نیز قابل شناسایی میباشد.در سیستم عامل پس از تغییر یک فایل به صورت سیگنال نوع تغییر و دیگر موارد به بخش های مورد نیاز ارسال میشود. مانند عکس زیر :

یک فایل پس از تغییر date modified آن تغییر خواهد کرد که تمامی تغییرات قابل مانیتورینگ میباشد. از کارهایی که میتواند این نرم افزار در یک سیستم عامل انجام دهد میتوان به صورت اجمالی به موارد زیر اشاره کرد :

- جلوگیری از ساخت - تغییر نام و تعییر محتوای فایل
- مانیتورینگ هدفمند روی یک یا چند مسیر
- پنهان شدن و کار کردن نرم افزار در سطح سیستم عامل
- مانیتورینگ مسیر های مختلف رجیستری
- مانیتورینگ قوی برای جلوگیری از اجرا شدن فایل های اجرایی
- اسکن سرور برای شناسایی سورس کد های مخرب و قابل نفوذ
- مستند سازی بر اساس لاگ فایل ویندوز
- مستند سازی بر اساس نوع دیتابیس مورد نیاز
- مستند سازی بر اساس فایل های xml

از این رو بسیاری از کارهایی که یک فایروال یا آنتی ویروس قادر به تشخیص آن نیستند این نرم افزار میتواند به خوبی تشخیص داده و به مقابله با آنها بپردازد.

۲-۲ مانیتورینگ اتصالات از درون سیستم عامل به شبکه های بیرونی

یکی از مهمترین بخش هایی که در ویروس ها میباشد این است که اطلاعات را به نحوی به محیط بیرون سیستم عامل ارسال نمیاد و یا توسط برنامه هایی Backdoors به فرد نفوذ گر یک دسترسی راه دور دهند تا بتوانند سطح دسترسی خودشان را در سیستم عامل بالا ببرند . مانیتورینگ قوی نیازمند است تا برنامه هایی که تلاش به وصل شدن به دنیای اینترنت از داخل سیستم عامل دارند را بتوان شناسایی و با اجازه نرم افزار باشد. آنتی ویروس ها اقلب به انجام این کار روی آورده اند اما انها به راحتی دور میخورند . روش هایی مانند باز کردن یک مرورگر به صورت مخفی که وظیفه ارسال اطلاعات را دارد و یا inject کردن خودشان به پروسه هایی از ویندوز که دسترسی به اینترنت دارند میتواند بسیار متداول باشد . اما با نرم افزار های low level میتوان چک کرد که ایا مرورگر توسط کاربر باز شده است و یا یک domain از یک application . در حالت هایی که یک برنامه خود را inject مینماید هم مانیتورینگ تمامی ارسالی های یک پروسس که دسترسی به اینترنت دارد میتواند راه حل خوبی باشد.در نرم افزار طراحی شده برای سیستم عامل های ویندوزی و یونیکسی میتوان این موارد را مشاهده کرد :

- مستند سازی تمامی وب سایت های ویزیت شدن در سیستم عامل از طریق هر گونه برنامه در تمامی حالات
- مسدود سازی وصل شدن به پروتکل های مختلف و یا سرور های IRC و .... که در ویروس های امده به ایران مشاهده شده است
- مستند سازی اطلاعات برنامه های نصب شده و یا اجرا شده
- گزارش نفوذ و یا ورود به کامپیوتر های مختلف در شبکه به کامپیوتر سرور
- پیغام دادن در صورت افلاین شدن یک کلاینت
- اسکن کردن پورت های باز کلاینت ها و سرور – محدود سازی برنامه ها برای استفاده از پورت های tcp upd
- مسدود سازی کارت شبکه کلاینت در صورت رویت حملات احتمالی
- ایجاد یک برنامه داخلی برای ارسال اطلاعات به صورت رمز شده و کاملا ایمن
- چک کردن کلاینت ها برای جلوگیری از الوده شدن به بد افزار ها
- چک کردن سیستم سرور – نواحی حساس برای اسکن بر اساس signature برای پیدا کردن بد افزار ها
- دسته بندی گزارشات بر اساس روز ماه سال

۲-۳ بررسی حملات تحت وب – تشخیص و جلوگیری از ان

یکی دیگر از مسایلی که در دنیای سرور های تحت وب میباشد حملات تحت وب میباشد که میتواند بسیار خطرناک باشند و دسترسی کاربر را از یک سطح دسترسی پایین به سطح دسترسی root برسانند . به طور مثال وب سایت وب سرور Apache با حمله به ظاهر ساده Xss هک شد و دسترسی هکرها را به روت رسانده بود . در این موارد حملاتی مانند Sql injection – Blind Sql injection – Xss – csrf و دیگر حملات موجود را میتوان از طریق استفاده استفاده از نرم افزار نوشته شده که میتواند به صورت plug in نیز اضافه گردد استفاده کرد. در مرحله ویرایش یک وب سرور قوی نیاز میباشد . وب سرور پیشنهادی میتواند وب سرور Ngix باشد که با کمی تغییر در ساختار آن میتواند اولین گام در برقراری امنیت باشد . Ngix یک وب سرور بسیار قدرتمند با کارایی بالا که میتواند در فشار ترافیکی بالا به خوبی دوام بیاورد و از نظر حفره های کشف شده نسبت به وب سرور های معروفی که در ایران استفاده میشوند apache – iis بسیار ایمن تر میباشد. پس از ویرایش وب سرور به اجرای برنامه و هماهنگ سازی آن با وب سرور میتوان پرداخت . این نرم افزار با انالیز درخواست های کاربران میتواند به وجود کارکتر های غیر مجار پی ببرد . با جلوگیری این حملات و ارسال ای پی های افراد نفوذ گر به فایروال میتوان به جلوگیری از این گونه حملات پرداخت . همچنین جلوگیری از Brute force کردن پسورد های سرویس های مهم و حساس مانند SSH

FTP – HTTP forms – با مشاهده لاگ های مورد نظر و طبق سیاست از پیش تعریف شده میتواند بسیار در جلوگیری از اولین قدم نفوذگران کارامد باشد.

۲-۴ مانیتورینگ حملات و برنامه های سیستمی

در این بخش که معمولا وظیفه یک برنامه مانند انتی ویروس میباشد ,حملاتی از قبیل Buffer overflow و یا Format string را باید به دقت مانیتور کرد. در شرایطی که یک سیستم عامل شروع به کار میکند هکر ها به پیدا کردن حفره در آن از طریق ارسال داده های که باعث اختلال در برنامه های سیستمی شود میپردازند . از این رو با فرض بر اینکه تمامی موانع امنیتی ایجاد شده توسط فرد هکر یکی پس از دیگری Bypass شود میتوان در این مرحله نیز رخ دادن چنین حملاتی را تشخیص داد. همانند برنامه stack guard یا exeshield میتوان برنامه های بومی نوشت که به این گونه حملات حساس باشند تا نفوذگر نتواند با یک حمله stack overflow یک پروسس سیستمی به بالا بردن دسترسی خود بپردازد.
همچنین تمامی توابعی که در سیستم میتواند توسط برنامه هایی مانند Keylogger و یا information gathering انجام دهد میتوانند مورد مانیتورنیگ قرار گیرد تا از اجرای برنامه های جاسوسی جلوگیری شود.
این نوع جلوگیری میتواند درصد زیادی کمک به مقابله با ورم ها و ویروس ها کند.

۳- جمع بندی

با افزایش روز افزون خطرات سایبری و دخیل شدن دنیای کامپیوتر در زندگی امنیت یکی از اصلی ترین رکنی مباشد که باید در این فضا مورد توجه قرار گیرد. با آنالیز روش های مختلف هکینگ و سناریوهای مختلف میتوان به یک شواهد مشابهی رسید .این شواهد گویای این است که هکر ها با دانش قبلی به نفوذ میپردازند و از تجهیزات و موانع امنیتی اطلاع دارند. ویرایش یک سیستم عامل متن باز برای استفاده مراکز مهم میتواند اصلی ترین بخش آن سازمان را از نفوذ ویروس ها و یا افرادی که میخواهند به آن بخش راه پیدا کنند , در امان بدارد.