سلسله مقالات امنیت

چرا لینوکس از ویندوز امن‌تر است؟

ویروس

نویسنده: محمد تشکری

بهمن‌ماه ۱۳۸۶

مقدمه

در چند ساله اخیر یکی از مباحث داغ پیرامون مقایسات بین سیستمهای عامل[1] لینوکس-[2] و ویندوز[3]،بحث امنیت بوده است. کارشناسان از دیدگاهها مختلف به این موضوع پرداخته اند و هریک در مورد این مبحث نظریاتی داده اند. کاربران عادی نیز صرفنظر از دیدگاه کارشناسی، مباحثی را پذیرفته اند که با تصورات آنها - که اغلب غیر کارشناسانه نیز هست - بیشتر سازگاری داشته باشد.
هدف از این مقاله که گردآوری شده نظرات کارشناسان و کاربران در شبکه اینترنت بوده و از انجمنهای گفتگو گرفته تا مقالات تخصصی را شامل می‌شود، ارائه دیدگاهی است که خوانندگان بتوانند بر اساس استدلال منطقی، نسبت به میزان امنیت این دو سیستم عامل قضاوت نمایند.
در هر کدام از سلسله مقالات «چرا لینوکس از ویندوز امن تر است؟» به یکی از معیارهای امنیت در سیستم عامل پرداخته می شود. در این مقاله سعی بر ارائه مطالبی در خصوص ویروسهای کامپیوتری داریم.

ویروس کامپیوتری[4] چیست؟

همانگونه که از نامش پیداست و همگان میدانند، ویروس کامپیوتری یک برنامه مخرب است (البته شاید هم غیر مخرب!) که دو خاصیت اساسی دارد:

الف- بطور خودکار و بدون اجازه و خواست کاربر اجرا می‌شود
ب- بطور خودکار و بدون اجازه و خواست کاربر تکثیر می‌شود

یک ویروس کامپیوتری برای انجام دو مأموریت فوق احتیاج به یک بستر دارد. این بستر غالبا در پرونده های اجرائی[5] سیستمهای عامل برای ویروسها فراهم می‌شود. که ممکن است از طریق پرونده های آلوده، رایانامه[6] آلوده یا طرق دیگر وارد سیستم شود.
نگاهی دقیقتر به مراحل اجرای یک پرونده اجرائی در سیستم عامل می‌اندازیم. این کار در سه مرحله کلی صورت می‌گیرد:

مرحله ۱: سیستم عامل در ابتدا نوع پرونده‌ی مورد نظر را از نظر اجرائی بودن بررسی می‌کند.
مرحله ۲: مجوزهای اجرا[7]ی پرونده توسط کاربر، بوسیله سیستم بررسی می شود.
مرحله ۳: در صورت اجرائی بودن پرونده و داشتن مجوز اجرا توسط کاربر، فرآیند اجرای آنرا به انجام می رساند.

حال ببینیم هر یک از سیستمهای عامل لینوکس و ویندوز چگونه مراحل فوق را به انجام می رسانند:

الف - ویندوز:

مرحله ۱: نحوه شناسائی پرونده های اجرائی در ویندوز، «پسوند»[8] آنهاست. یعنی ویندوز یک پرونده را که پسوند exe یا com یا bat داشته باشد اجرائی فرض کرده و در صورتی که exe یا com باشد آنرا بصورت دودوئی(binary) و اگر bat باشد آنرا

1 Operating Systems
2 GNU/Linux
3 Microsoft Windows
4 Computer Viruses
5 Executable Files
6 eMail
7 Execute Permission
8 Extension

بصورت فرمانهای اجرائی اعلان دستور[1] سیستم، اجرا می نماید.

مرحله ۲: در حالت پیش فرض همه پرونده ها برای همه کاربران در ویندوز مجوز اجرا دارند. البته این موضوع به نوع سیستم پرونده[2] نیز وابسته است و در صورتی که شما از سیستم پرونده امن ویندوز(مانند NTFS) استفاده نکنید اصلا هیچ نوع مجوزی وجود ندارد که بررسی شود!!! یعنی همه مجازند هرکاری بکنند![3]

مرحله ۳: اگر یک پرونده از دو مرحله فوق رد شود و به این مرحله برسد، حال تمام سیستم اعم از سخت افزار، نرم افزار، سرویسها و ... در اختیار او خواهند بود تا اجرا شده و خدمات مورد نیاز کاربر را ارائه نماید. در واقع ویندوز از اینجا به بعد هرچه برنامه اجرائی بخواهد در اختیارش قرار میدهد. به این دلیل است که بعضی پرونده ها و برنامه های غیر مخرب نیز بعد از اجرا ممکن است عملکرد سیستم را متوقف[4] نمایند. البته در نسخه های جدید ویندوز (از 2000 به بعد) یک برنامه امنیتی در سیستم عامل و در لایه Application آن، قرار داده شده که از خرابکاری پرونده های اصلی سیستم عامل جلوگیری بعمل آورد. اما اکثر مواقع این برنامه امنیتی در محافظت از سیستم پرونده ناموفق عمل نموده است.

نتیجه: شما میتوانید هر پرونده ای را در سیستم عامل ویندوز بعنوان اجرائی به آن معرفی کنید!!![5] بنابراین حتی در بعضی موارد لازم نیست در آن پرونده ویروسی وجود داشته باشد، اجرای کدهای نامفهوم برای سیستم در بسیاری موارد موجب مضرات فراوان می شود که ساده ترین آنها توقف عملکرد سیستم یا همان «هنگ کردن» معروف است.

ب- لینوکس:

مرحله ۱: لینوکس پرونده های اجرائی را از روی سرنام[6] داخل پرونده ها شناسائی میکند که قابل تغییر توسط کاربر نیستند[7]. در واقع داشتن یا نداشتن پسوند هیچ تغییری در رفتار لینوکس برای یک پرونده اجرائی نخواهد داشت. چرا که یک پرونده اجرائی در لینوکس حتماً اجرائی است حتی اگر پسوند آن jpg یا wav باشد!

مرحله ۲: مجوز اجرا برای کاربر از مهمترین بخشهای یک پرونده در لینوکس است. بعبارت دیگر یک پرونده اگر هم از نظر سرنامهایش اجرائی باشد، مجوز اجرا توسط آن کاربر خاص باید وجود داشته باشد تا پرونده اجرا شود. در حالت پیش فرض مجوز اجرا فقط برای پرونده های خاص و فقط برای مالک آن پرونده - که آنرا ایجاد نموده - وجود دارد. همچنین در هنگام نسخه برداری از پرونده ها مجوزهای اجرا حذف می گردند.

مرحله ۳: حالا نوبت اجرای پرونده است. در صورتی که پرونده قابل اجرا باشد و مجوز کافی برای اجرای آن توسط کاربر وجود داشته باشد، سیستم عامل تمام امکانات سیستم مانند سخت افزار، نرم افزار و سرویسها و ... را که آن کاربر مجوز دسترسی به آنها را دارد در اختیار پرونده می گذارد که خدمات مورد نیاز را به کاربر ارائه نماید.

توضیح تکمیلی: در سیستم عامل لینوکس همه چیز بصورت پرونده دیده میشود و توسط یک ساختار یکپارچه پرونده[8] کنترل می‌گردد. به این صورت که اطلاعات مربوط به پروسه‌های[9] سیستم در مسیری بعنوان proc/ و پرونده های رابط سخت‌افزارهای[10]

---

1 Command Prompt
2 File System
3 این در نسخه های پائینتر ویندوز مانند ۹۵و ۹۶و ۹۷و ۹۸و ME صدق میکند و در صورت استفاده از سیستم پرونده FAT32 در نسخه های بالاتر
4 HANG
5 کافیست پرونده را تغییر نام داده و پسوندش را عوض کنید
6 header
7 با کوچکترین تغییر، پرونده دیگر اجرائی نخواهد بود.
8 File Hierarchy System
9 Process
10 Devices

سیستم در مسیری بعنوان dev/ نگهداری شده و برای همه آنها حق دسترسی[1] تعریف می شود. محتویات این پوشه ها در زمان راه اندازی سیستم بصورت پویا[2] ایجاد شده و در زمان خاموش شدن سیستم از بین می روند.

نتیجه : یک برنامه اجرائی امکان اجرا و همچنین تکثیر خودکار در سیستم عامل لینوکس را نخواهد داشت.

نگاهی گذرا به ساختار داخلی سیستمهای عامل ویندوز و لینوکس:

ویندوز: یک سیستم عامل تک کاربره[3] است! بله درست متوجه شدید سیستم عامل ویندوز یک سیستم عامل با طراحی تک کاربره و چند وظیفه‌ای[4] است که کاربران مختلف را بصورت وظایف مختلف سیستم عامل مدیریت میکند. بنابراین، کاربران بعنوان وظایف سیستم عامل شناسائی شده و به آنها مانند دیگر وظایف (فقط با تقدم[5] بیشتر) پرداخته می‌شود. به همین دلیل است که با ورود کاربران مختلف به یک سیستم، بار بسیار زیادی به آن سیستم وارد می‌آید و سیستم بطور چشمگیری کند می‌شود.
از سوی دیگر ویندوز یک سیستم عامل طراحی شده بر پایه Micro Kernel است. (البته به گفته مقامات و کارشناسان مایکروسافت) معنی این ساختار این است که همه آنچه در سیستم است در خارج از هسته[6] سیستم عامل رخ می دهد و هسته فقط پیامهای مربوط به بخشهای مختلف را به موقع به بخش دیگر می‌رساند. اگر واقعا اینطور باشد میزان توقف سیستم عامل و از کار افتادن سرویسها و خدمات تقریبا به صفر میرسد، اما در عمل آنچه می بینیم یک رابط گرافیکی سنگین است که جزء لاینفک ویندوز بوده و بار زیادی را به سیستم تحمیل میکند و در صورتی که کاربر نخواهد از محیط گرافیکی استفاده کند، خوب هیچ چاره ای ندارد، باید استفاده کند!

1 Permission
2 Dynamic
3 Single User
4 Multi Tasking
5 Priority
6 Kernel

لینوکس: لینوکس یک سیستم عامل چند کاربره[1] و چند وظیفه ای بوده و از ابتدا به این صورت طراحی شده است. این بدین معنی است که سیستم عامل برای هر کاربر به محض ورود به سیستم یک نشست[2] جدید ایجاد مینماید و همه نیازمندیهای کاربر در قالب آن نشست برآورده می شود. حال اگر در اثر اجرای دستور یا برنامه‌ای مخرب، مشکلی ایجاد شود، خوب! هیچ جای نگرانی نیست. فقط نشست و پرونده های مربوط به آن کاربر دچار مشکل شده و آسیب می بیند و به محیط کاربران دیگر و همچنین پرونده های سیستم هیچگونه آسیبی نمی رسد. (البته اگر این کاربر «مدیر»[3] نباشد)

نکته دیگر اینکه طراحی لینوکس بر پایه Monolitic Kernel است. این بدین معنی است که برخی از نیازهای سیستم عامل می تواند در هسته گنجانده شود و بصورت یکپارچه کنترل و هدایت شود. این گونه است که می توان کلیه نیازها را در زمان درخواست و احتیاج واقعی کاربر، فعال نموده وبرای آن، منابع[4] اختصاص داد و یا برخی نیازهای ثابت را درون هسته گنجاند تا سیستم از سرعت و عملکرد بهتری برخوردار شود. لینوکس به دلیل نوع طراحی هسته و سیستم پرونده‌اش رفتاری همانند یونیکس[5] را انجام می‌دهد.

اما مبحث آخر، برخی می‌گویند «*چون لینوکس به اندازه زیاد استفاده نمی شود هنوز برای آن ویروس نوشته نشده است*»!!! نظر این افراد را به برخی آمارهای جهانی که به راحتی از طریق اینترنت قابل دسترس می باشند جلب می نمایم:

- پایداری[6] و قابلیت اطمینان[7] این سیستم عامل به حدی است که بیش از ۷۰ درصد سرویس دهنده‌های جهان بر روی آن کار میکنند (www.netcraft.com)
- دلایل فوق و همچنین سرعت و انعطاف پذیری لینوکس باعث شده است تا بیش از ۷۵ درصد از برترین سوپرکامپیوترهای جهان از این سیستم عامل استفاده نمایند.(www.top500.org)
- ۹۰ ٪ کاربران خانگی از ویندوز استفاده میکنند.

آیا کسانی که ویروس می نویسند خرابکاری بر روی ایستگاه کاری یک کاربر که در خانه خود نشسته است را به خرابکاری بر روی سرویس دهنده هزاران کاربر ترجیح میدهند؟!!

مسلم است که جواب منفی است. اما نوشتن ویروس برای ویندوز بسیار آسان و دست یافتنی بوده و در مقابل ویروس نویسی برای سیستمهای مانند یونیکس (مثل لینوکس) اگر ناممکن نباشد بسیار بسیار مشکل و دردسر ساز خواهد بود.

در نهایت با پیدا شدن یک حفره امنیتی در سیستم عامل متن باز[8] لینوکس، بیش از ۴۰۰ هزار برنامه نویس سراسر جهان در کمتر از یک ساعت آن مشکل را بر طرف مینمایند(والبته در بیشتر موارد به دلیل باز بودن کد، قبل از انتشار حفره امنیتی و آسیب رسیدن به سیستمهای عملیاتی این کار انجام می شود) در صورتیکه حفره هائی در سیستم عامل ویندوز موجود است که پس از گذشت چندصد روز هنوز مایکروسافت اقدام به رفع آن نکرده است.

باید به این نکته نیز توجه داشت که همیشه در ویندوز ابتدا فاجعه اتفاق می افتد و بعد وصله امنیتی - پس از مدتها - به دست کاربر می‌رسد، اما در لینوکس بیش از ۹۵٪ موارد قبل از رخ دادن فاجعه، مشکل توسط برنامه نویسان سراسر جهان - که تعدادشان ۱۰ برابر

---

1 Multi User
2 Session
3 root
4 resource
5 UNIX Like
6 Stability
7 Reliability
8 Open Source

تعداد کل کارکنان شرکت مایکروسافت است! - برطرف می‌شود.