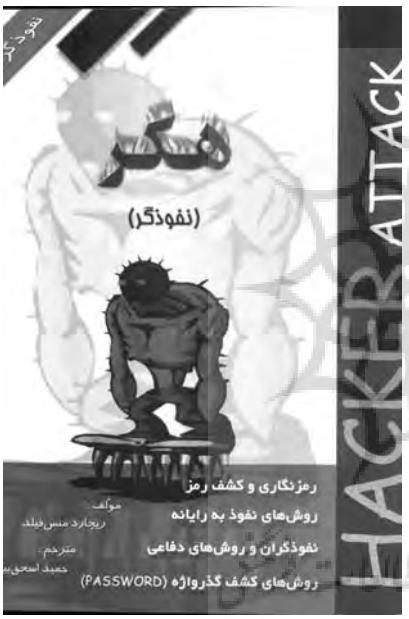
نقد و بررسی

نفوذگران در کمین اند

O مهندس محمدهادی معرفت

Oریچارد منس فیلد، هکر (نفوذگر)، مترجم: حمید اسحق بیگی،تهران: اسحاق، چاپ اول، ۱۳۸۱وزیزی، شمیز



آیا تا به حال کامپیوتر شما مورد حمله نفوذگران واقع شده است؟

آیا کامپیوتر شما، حتی وقتی خاموش است از حملهٔ نفوذگران در امان است؟

آیا تا به حال با دریافت یک فایل، سیستم کامپیوتر شما مختل شده است؟

آیا تا به حال استفادهٔ غیرمعقول از اتصال اینترنت شما شده است؟

و آیا...

معمولاً با خواندن این‌گونه سؤالها و خبر حملهٔ نفوذگران به سیستمهای کامپیوتری نگران از دست دادن موقعیت شغلی و کاری خود می‌شوید. راستی، نفوذگران چه کسانی هستند؟

هکر (hacher) یا نفوذگر کسی است که از تخصص کامپیوتری خود برای کارهای ممنوع استفاده می‌کند. چنین کسی بدون مجوز وارد سیستمهای کامپیوتری می‌شود و برنامه‌ها و داده‌ها را زیر و رو می‌کند.

کراکر (Cracker) شخصی است که با عبور از معیارهای امنیتی یک سیستم کامپیوتری به طور غیرمجاز به آن سیستم دسترسی پیدا می‌کند. هدف این اشخاص، بیشتر کسب غیرقانونی اطلاعات از یک سیستم کامپیوتری یا استفاده از منابع آن سیستم است.

اعمال مجرمانهٔ این افراد که مواردی نظیر تخریب منابع اطلاعاتی، تقلبهای مالی، نفوذ به سازمانها و دسترسی به اطلاعات محرمانهٔ آنها، انتشار اطلاعات سری و پخش شایعات مخرب، سرقت و سوءاستفاده از اطلاعات شخصی افراد و غیره را شامل می‌شود، تاکنون آسیبها و خسارات جبران‌ناپذیری برجای گذاشته است.

برای مقابله و پیشگیری از سرقت و دسترسی منابع اطلاعاتی موجود در شبکه‌ها و کامپیوترها لازم است شناخت دقیقی از روشهای نفوذ به رایانه‌ها داشته باشیم و راههای مقابله با نفوذ را فرابگیریم. کتاب هکر (نفوذگر) از تألیفات ریچارد منس فیلد (Richard Mansfield) در بیست و چهار فصل پیوسته این راهکارها را معرفی می‌کند.

دو فصل ابتدایی این کتاب به بحث خطرات موجود در اینترنت و بررسی تاریخ هکرها می‌پردازد... با بررسی تاریخچهٔ نفوذگران درمی‌یابیم که اولین نفوذگران، نفوذگران

راههای مقابله با نفوذگران از مباحث عمدهٔ کتاب است که نویسنده به طور مفصل بدان پرداخته است. اعتماد به افراد ناشناس، همواره مخاطراتی به همراه داشته است. بسیاری از کاربران زمان زیادی را در اتاقهای گفت و گو می‌گذرانند و در قالبهای مختلفی به ارتباط با افراد می‌پردازند. این درحالی است که آنها طرف مقابل را صرفاً براساس اطلاعاتی که خود شخـــص ارائه داده است، می‌شنـــاسند. ایـن ساده‌تـــریـن و متداولترین راه فریب افراد، برای پی بردن به اسرار یا اطلاعات شخصی یا اجرای اعمال خرابکارانه بر روی کامپیوترهای آنهاست

کامپیوتر شما برای کارهای مخفیانه و غیرمجاز استفاده کنند بدون آن که شما متوجه شوید.

یکی از مهمترین بحث‌های این کتاب راههای رمزنگاری و روشها و استانداردهای کشف رمز است که در فصول ۱۲ تا ۱۵ این کتاب به بررسی آن پرداخته می‌شود.

اولین چیزی که در هر نفوذی مطرح است، نفوذ به داخل سیستم موردنظر است. این کار اغلب شامل به دست آوردن کلمهٔ رمز ورود (Password) است. در بیشتر شبکه‌های رایانه‌ای و تعداد زیادی از پایگاهها وب برای ورود، به کلمهٔ رمز ورود احتیاج است. یکی از این راهها استفاده از برنامه‌های force Brute است. با این نوع برنامه‌ها نفوذگران می‌توانند یک ویروس را به شبکه‌ای ارسال کنند و با آن کلمهٔ رمز را به دست آورند. برای نفوذ به بیشتر سیستمهای رایانه‌ای به دو دادهٔ مهم احتیاج است: یکی کلمهٔ رمز ورود (Password) و دیگری نام کاربری (User name) که هر دوی آنها را ویروسها می‌توانند به دست آورند. یکی دیگر از روشهای نفوذگران که کتاب بدان پرداخته است، روش عیب‌یابی برنامه توسط برنامه‌نویس است. نفوذگران برنامه‌نویس و دیگر برنامه‌نویسان یک راه مخفی موسوم به Backdoor ایجاد می‌کنند که این راه، راه ورود به سیستمی است که برنامهٔ آن را نوشته‌اند.

برنامه‌نویسان اغلب راههای ورودی مخفی را در جایی از برنامه قرار می‌دهند که دسترسی به آنها به صورت قانونی امکان‌پذیر باشد؛ مانند بخشی که برای دادن سرویسهای فنی به سیستم یا برنامهٔ کاربردی به کار می‌رود. یک در مخفی یا پشتی مانند یک راه مخفی است که می‌توان به داخل آن وارد شد. برنامه‌نویسان راه ورود از طریق این راههای مخفی را می‌دانند؛ اما دیگران نمی‌دانند که درهای مخفی در آن قسمت وجود دارد.

در برابر نفوذگرانی که سعی در نفوذ به داخل سیستمی را دارند، مدیر سیستمی وجود دارد که سعی می‌کند در برابر آنها حفاظ یا دیواری محکم ایجاد کند. حفاظ آهنی یا دیوارهٔ آتش (Firewall) اسامی عمومی نرم‌افزار و سخت‌افزارهایی است که برای به دام انداختن نفوذگران کاربرد دارد. این نرم‌افزارها یا سخت‌افزارها فعالیتهای نفوذگران را تا حدودی کنترل می‌کنند و نتیجه را در داخل یک فایل ذخیره می‌کنند. حفاظ آهنی سیستم عامل را شبیه‌سازی می‌کند و دسترسی به منابع را به صورت‌های مختلف محدود می‌سازد.

بیشتر نفوذگران برای اطمینان یافتن از تواناییهای خود سیستمهای امنیتی را از بین می‌برند. آنها پس از وارد شدن به یک سیستم، فقط به نظارهٔ داده‌ها و گشت و گذار در آنها بسنده نمی‌کنند؛ زیرا بعضاً اطلاعاتی وجود دارند که رایگان نیستند و این نفوذگران را کلافه می‌کند. آنها علاوه بر استفاده از این نوع اطلاعات، می‌خواهند یک آزمون مهارت نیز به عمل آورند. امروزه نفوذگران به صورتهای گوناگونی به اطلاعات شخصی افراد از طریق اینترنت دسترسی پیدا می‌کنند، ازجمله دسترسی به فایلهای ردپا (Cookie).

راههای مقابله با نفوذگران از مباحث عمدهٔ کتاب است که نویسنده به طور مفصل بدان پرداخته است. اعتماد به افراد ناشناس، همواره مخاطراتی به همراه داشته است. بسیاری از کاربران زمان زیادی را در اتاقهای گفت و گو می‌گذرانند و در قالبهای مختلفی به ارتباط با افراد می‌پردازند. این درحالی است که آنها طرف مقابل را صرفاً براساس اطلاعاتی که خود شخـــص ارائه داده است، می‌شنـــاسند. ایـن ساده‌تـــریـن و متداولترین راه فریب افراد، برای پی بردن به اسرار یا اطلاعات شخصی یا اجرای اعمال خرابکارانه بر روی کامپیوترهای آنهاست. برای گریز از چنین آسیبهایی لازم است کاربران نکات مهمی را مدنظر داشته باشند و سعی در رعایت آنها کنند. این نکات عبارت است از: عدم اجرای فایلهای ضمیمه درون نامه‌های ناشناس، استفاده از آخرین نرم‌افزارهای ضد ویروس و استفاده نکردن از کلمات کلیدی نظیر شماره کارت اعتباری و غیره بر روی کامپیوترهایی که مورد اطمینان نیستند. امروزه افراد سودجو با نصب نرم‌افزارهایی که قادر به ضبط و ذخیرهٔ اطلاعات صفحهٔ کلید هستند، به سادگی از اطلاعات شخصی

کتاب هکر (نفوذگر)، به بررسی و تجزیه و تحلیل روشهای نفوذ کردن و نیز مقابله با آن در سیستم‌های رایانه‌های می‌پردازد. یک هکر همیشه دوست دارد از همه چیز سردربیاورد تا بتواند به لایه‌های امنیتی نفوذ کند. یا این که همه چیز را دربارهٔ شبکه و سیستمهای رایانه‌ای بداند

و محرمانهٔ کاربران مطلع می‌شوند. به همین منظور، اطلاعات مهم و کلیدی را فقط به کامپیوترهای مطمئن وارد کنید.

البته درخصوص کارتهای اعتباری، استفاده از صفحات SSL رواج یافته است.

استفاده از فیلترهای مناسب توسط ISP نقش شایان توجهی در جلوگیری از دسترسی کاربران به سایتهای غیرمجاز و غیرقانونی دارد. تجربه نشان داده است که این کار در درازمدت تأثیر بسزایی در پیشگیری از جرایم به دنبال خواهد داشت.

یکی دیگر از راههای جلوگیری از نفوذ که نویسنده بدان توجه داشته است استفاده از Passwordهایی است که حدس زدن آن مشکل و ترکیبی از حروف و اعداد باشد و هر ازگاهی تغییر یابد.

یک ISP ایده‌آل می‌تواند با نصب حفاظ آهنی و ضدویروسهای مناسب از انتشار ویروسها به کامپیوتر کاربران جلوگیری کند. بنابراین، همیشه از جدیدترین نرم‌افزارهای ضدویروس استفاده کنید. یکی از راههای کنترل رایانه‌ها و شبکه‌ها این است که از یک برنامهٔ امنیتی برای کنترل Cookie که اطلاعات را به سایتهای وب بازمی‌گردانند، استفاده کنید.

برای سایت‌های وب و برنامه‌های کاربردی مختلف از کلمات عبور متفاوت استفاده کنید تا کشف آنها برای نفوذگران مشکل باشد.

اگر از DSL یا مودم کابلی، برای اتصال به اینترنت استفاده می‌کنید، یک نرم‌افزار حفاظ آهنی یا دیوارهٔ آتش (Firewall) مناسب برای کنترل ترافیک شبکه و کامپیوتر خود نصب کنید.

فصل هفدهم این کتاب به بررسی راههای امنیت در ویندوز خصوصاً ویندوز نسخهٔ ۲۰۰۰ می‌پردازد. یکی از بهترین راههای حفاظت، تهیهٔ نسخهٔ پشتیبان از داده‌هاست. باید به خاطر داشته باشید که حتی قوی‌ترین نرم‌افزارهای ضدویروس نیز نمی‌توانند شما را در همه حال از ویروسها محافظت کنند. برای جلوگیری از این فاجعه باید از فایلهای داده‌ای به طور منظم و مرتب نسخهٔ پشتیبان تهیه کرد. به این‌ترتیب در جریان حملهٔ ویروس، داده‌های شما از بین نمی‌رود.

بخش سوم و آخر این کتاب به معرفی ویروس‌ها و کرمها و شبه‌ویروسها می‌پردازد در فصل بیست کتاب ابتدا به تاریخچه ویروسهای رایانه‌ای و کرمها می‌پردازد. فصل بیست و دوم به یکی از ویروسهای ویرانگر رایانه‌ها به نام ملیسا که در ۲۶ مارس سال ۱۹۹۹ توسط یکی از کاربران شرکت AOL (American On line) به وسیلهٔ پیام پست الکترونیکی به یک گروه خبری ارسال شد و بعدها باعث آلوده شدن سرویس‌گر (Server)های شرکت‌های بزرگی چون اینتل و مایکروسافت و... گردید، می‌پردازد. و به تفصیل به چگونگی فعالیت ملیسا می‌پردازد. در انتهای بخش ۴ نیز راههای مقابله با ویرس‌ها بررسی شده است.

در سال ۱۳۸۱ توسط انتشارات سیمین‌دخت و به دست توانای دو تن از مترجمین در حوزهٔ کامپیوتر یعنی محمودرضا ذوقی و حمیدرضا ذوقی کتاب حاضر ترجمه و به چاپ رسید. در بررسی اجمالی و دقیق این کتاب که توسط آقایان ذوقی ترجمه شده است در مقایسه با کتاب حاضر می‌توان به سادگی و روانی ترجمه آقایان ذوقی اشاره نمود.

یکی از موارد قابل توجه و تعمق در ترجمه کتاب توسط حمیداسحق بیگی در مورد تاریخچه شیوع ویروس ملیسا است در صفحهٔ ۲۱۰ کتاب می‌خوانیم «در ۲۶ مارس سال ۱۹۹۹، این ویروس توسط شخصی که دارای کارگزار اینترنت آمریکا آن لاین بود...» در صورتی که این ویروس توسط یکی از کاربران AOL شیوع پیدا کرده بود.

وجود کلمات و عبارات ثقیل کتاب چاپ شده توسط نشر اسحاق و بعضاً ایرادهای (ضعف‌های) موجود در ترجمه محوریت این کتاب را تغییر داده است و باعث شده است که خوانندگان دچار گمراهی شوند.

آخرین نکته مورد توجه این است که بدانید نفوذگران در کمین‌اند. بنابراین، همیشه با چشمان باز و مسلح در اینترنت قدم بگذارید.