مهندسی نفوذ

- پیاده‌سازی روش‌های موثر نفوذ به شبکه‌های کامپیوتری
- همراه با ارائه راهکارهایی برای مقابله با آنها

مهندس علیرضا رنجبر

زیرنظر:
مهندس وحید جمشیدی گوهرریزی
عضو هیئت علمی دانشگاه شهید باهنر کرمان

نوپردازان

سرشناسه : رنجبر، علیرضا، ۱۳۶۷.
عنوان و نام‌پدیدآور : مهندسی نفوذ: پیاده‌سازی روش‌های مؤثر نفوذ به شبکه‌های کامپیوتری، همراه با ارائه راهکارهایی برای مقابله با آنها/ علیرضا رنجبر؛ زیر نظر وحید جمشیدی گوهریزی
مشخصات نشر : تهران: نوپردازان، ۱۳۹۱.
مشخصات ظاهری : پانزده، ۱۹۲ ص.: جدول، نمودار.
شابک : 978-964-975-175-7
وضعیت فهرست‌نویسی : فیپا
یادداشت : کتابنامه: ص. ۱۶۷-۱۷۰.
یادداشت : نمایه.
موضوع : شبکه‌های کامپیوتری -- اقدامات تامینی
موضوع : حفاظت اطلاعات
شناسه افزوده : جمشیدی گوهریزی، وحید، ناظر
رده‌بندی کنگره : ۱۳۹۱ ۹م۸۵ر/TK۵۱۰۵/۵۹
رده‌بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۲۷۲۷۱۴۹

مهندسی نفوذ

تالیف	علیرضا رنجبر
ناشر	نوپردازان
قطع	وزیری
نوبت چاپ	اول
تاریخ	زمستان ۱۳۹۲
تیراژ	۱۵۰۰
صفحات	۱۹۲
شابک	۹۷۸-۹۶۴-۹۷۵-۱۷۵-۷
لیتوگرافی	نورنگ ۷۷۵۲۹۳۶۳-۷۷۵۳۱۰۲۷
چاپ‌وصحافی	طرفه ۵۵۲۶۹۲۸۷-۸

۹۰۰۰ تومان

کتابیران: تهران، میدان انقلاب، ابتدای خیابان آزادی، خیابان دکتر قریب، بعد از فرصت شیرازی، پلاک ۷، تلفن: ۱۸ - ۶۶۵۶۶۵۰۹
نوپردازان: تهران، خیابان لبافی‌نژاد، بین اردیبهشت و فروردین، پلاک ۲۲۸
تلفن: ۶۶۴۱۴۴۷۴ - ۶۶۴۱۴۵۱۵ - ۶۶۴۱۱۱۷۲ - ۶۶۴۹۴۴۰۹

سخنی با مخاطب

امنیت در همه زمان‌ها یکی از مسائل مهم در طراحی شبکه‌ها محسوب می‌شود به‌طوری که هر بخش یا سازمان نیاز اساسی به ایجاد امنیت در شبکه خود را دارد. اما همان‌طور که می‌دانیم امنیت یک سیستم مجزا و آماده نیست که آن را خریداری و نصب کنیم، امنیت باید با توجه به نیاز و طراحی شبکه ایجاد شود و مجموعه‌ای از تکنولوژی‌ها و راهکارهاست. بنابراین امنیت یک شبکه باید مهندسی و برنامه‌ریزی شود و با توجه به نیاز و نوع آن شبکه موارد امنیتی خاص برای آن لحاظ شود.

هنگامی‌که از مسئول شبکه یک سازمان درباره امن بودن شبکه‌اش سؤال می‌شود، اغلب می‌گوید: «ما اتصال شبکه خود را با اینترنت قطع کرده‌ایم پس شبکه ما امن است» و این دقیقاً همان زمانی است که حملات بر روی شبکه اهمیت بسیاری پیدا خواهند کرد زیرا بزرگترین خطری که شبکه فعلی را تهدید می‌کند، می‌تواند یکی از سیستم‌های داخل همان شبکه باشد. به‌عبارت دیگر یکی از کارمندان همان شرکت ممکن است خواسته یا ناخواسته شرایطی را فراهم آورد تا هکر به داخل شبکه (با اتصال اینترنت و یا بدون اتصال به آن) نفوذ کند و در هنگامی‌که شبکه از سوی مسئول آن امن تلقی می‌شود بیشترین خسارت را به آن وارد کند. حتی ممکن است یکی از کارمندان همان شرکت به هر دلیلی (دشمنی‌های شخصی و یا حتی سرگرمی) قصد حمله به سایر کارمندان درون آن شبکه را داشته باشد.

این کتاب به بررسی مهم‌ترین حملات بر روی شبکه‌های کامپیوتری می‌پردازد و دلیل انتخاب این حملات از بین صدها حمله گستردگی موضوعی و اهمیت آنها است. به این صورت که با طرح هر یک از این حملات موضوعات بسیاری در بحث امنیت را می‌توان بیان کرد. در هر فصل بعد از بیان کامل و اجرای هر یک از حملات روش‌های دفاع در برابر آنها نیز شرح داده می‌شود تا با توجه به نوع حمله روش دفاع مناسب با شبکه خود را انتخاب کنید.

اما آنچه در این کتاب خواهید آموخت تنها روش‌های پیشگیری نیست بلکه عمده بحث بر روی پیاده‌سازی حملات و چگونگی اجرای عملی آنها است و دلیل این روش آموزش این است که در صورتی‌که شما نتوانید به‌عنوان یک هکر به شبکه خود نفوذ کنید نمی‌توانید از نقاط ضعف شبکه خود اطلاع یابید. به‌عبارت دیگر قبل از آنکه شما یک کارشناس حرفه‌ای امنیت شوید بایستی بتوانید نقاط ضعف شبکه را بشناسید و این امر محقق نمی‌شود مگر آنکه شما به‌صورت عملی در شبکه و شرایط آن حضور یابید و با اجرای روش‌های نفوذ متفاوت سعی در به‌دست آوردن نقاط ضعف شبکه خود را کنید.

این حالت را با جنگ‌های واقعی مقایسه کنید. در یک جنگ که به‌صورت فیزیکی اجرا می‌شود همواره نمی‌توان از یک روش دفاعی برای مقابله با آن استفاده کرد زیرا نحوه اجرای حملات از جانب دشمن تغییر می‌کند و برای آنکه شما بتوانید در برابر دشمن خود دفاع کنید باید نحوه اجرای حمله او را بدانید. به‌عبارت

دیگر باید دشمن خود را بشناسید و حالتی مشابه با این در بحث امنیت وجود دارد. اجرای یک روش دفاعی در تمامی زمان‌ها مؤثر نخواهد بود و روش‌های دفاعی بسته به نوع حمله باید ایجاد شوند.

بزرگترین مشکلاتی که در رابطه با آموزش حملات وجود دارد و اغلب افراد به دلیل همین مشکلات از آموختن آنها منصرف می‌شوند نبود محیط مناسب برای اجرا و آموختن آنها و همچنین نبود کتابی که این حملات را به‌صورت عملی نشان دهد، است. ایجاد یک شبکه برای هر فرد اغلب پرهزینه است و همچنین نمی‌تواند شبکه‌ای را پیدا کند تا به‌صورت تمام وقت در اختیار او باشد. بنابراین در این کتاب روشی آموزش داده خواهد شد تا با اختیار داشتن تنها یک کامپیوتر محیطی همانند محیط واقعی را برای خود ایجاد کنید. دقت داشته باشید روشی که در این کتاب آموزش داده خواهد شد یک روش شبیه‌سازی نیست، بلکه به نوعی تقلید از واقعیت و پیاده‌سازی شرایط واقعی یکسری سیستم بر روی یک سیستم منفرد است و تمامی نرم‌افزارها در محیط واقعی(بر روی سیستم عامل‌ها) پیاده‌سازی و اجرا می‌شوند. (البته شاید کمی گیج شده باشید اما با مطالعه فصل اول- مجازی‌سازی چگونگی پیاده‌سازی این روش به شما نشان داده خواهد شد).

به یاد داشته باشید که در هک کردن و یادگیری روش‌های آن مهم‌ترین نکته‌ای که باید مدنظر داشت صبور بودن است و لازمه یک هکر و یک کارشناس امنیت خوب صبر و حوصله داشتن است. معمولاً هکرها برای نفوذ به سیستم‌ها شاید ماه‌ها در حال بررسی راه‌های ورود به آن شبکه هستند پس سعی نکنید که هک کردن را یک روزه!! یاد بگیرید.

در اینجا وقت آن است تا از اساتید ارجمند که اینجانب را در تألیف کتاب همراهی نمودند قدردانی کنم. در ابتدا از استاد وحید جمشیدی که سهم به‌سزایی در طراحی و بازبینی این اثر داشتند و بدون همکاری ایشان تألیف این کتاب ممکن نبود، تشکر می‌کنم. از دکتر شاپور گهوارهٔ - ناشر محترم نوپردازان که کتاب را به چاپ رسانده‌اند و همچنین از مهندس محمد خراد رستمی که کمال همکاری را با اینجانب انجام دادند تشکر و قدردانی می‌کنم. در پایان از مخاطبان، دانشجویان و اساتید محترم درخواست داریم تا نقطه نظرات خود درباره موضوعات کتاب را با ما در میان بگذارند تا این اثر در چاپ‌های بعدی با کیفیت بهتر در اختیار مخاطبان قرار گیرد.

امید است تا با ارائه این اثر سهمی هرچند کوچک در تعالی ایران اسلامی داشته باشیم.

alireza.ranjbar12@gmail.com
vjamshidi@uk.ac.ir

طبقه‌بندی فصول کتاب

مطالب کتاب در هر فصل در ۴ بخش طبقه‌بندی شده‌اند که این بخش‌ها عبارتند از:

پیشگفتار به‌صورت مختصر حمله موردنظر را تعریف می‌کنیم و شما را با موضوع کلی کاری که می‌خواهیم انجام دهیم، آشنا می‌کنیم.

تئوری حملات، حملات از لحاظ تئوری بیان و تمامی جزئیاتی که در رابطه با آن حمله نیاز است را تعریف می‌کنیم. در این بخش حملات با استفاده از اشکال و بیان تعریف‌ها، توضیح داده می‌شوند.

اجرای حملات در عمل حمله مورد نظر به‌صورت مرحله به مرحله و کاملاً عملی به مخاطب نشان داده می‌شود و با قرار دادن نتایج به‌دست آمده شما را به‌گونه‌ای هدایت می‌کنیم تا بتوانید با استفاده از این مراحل آن حمله را پیاده‌سازی کند.

دفاع در برابر حملات اکثر روش‌های دفاعی که برای مقابله با آن حمله می‌توانیم استفاده کنیم را بیان کرده‌ایم و هر کدام را مفصلاً شرح داده‌ایم که شما بعد از یادگیری حمله و آشنایی با چگونگی اجرای آن در بخش قبل با استفاده از این راهکارها می‌توانید راه‌حل دفاعی مناسب شبکه خود را انتخاب و بر روی آن پیاده‌سازی کنید.

فصل‌بندی کتاب به‌صورت زیر است:

در **فصل اول** به مجازی‌سازی و ایجاد یک شبکه برای تست کردن سایر حملات پرداخته‌ایم و به‌صورت کامل جزئیات آن را بیان کرده‌ایم.

در **فصل دوم** به یکی از موفق‌ترین حملات در تمامی زمان‌ها یعنی حملات MITM پرداخته‌ایم. مبنای این نوع حملات سرقت اطلاعات مهم کاربران است.

در **فصل سوم** به حملات DoS در شبکه پرداخته‌ایم که در این نوع حملات هکر با ایجاد سربار اضافی بر روی اجزاء شبکه (منابع شبکه) سعی در مختل کردن آن بخش را دارد.

در **فصل چهارم** چگونگی اجرای حملات بر روی درخت پوشا یا STP را نشان داده‌ایم و بیان کرده‌ایم که چگونه در زمانی‌که یک طراح شبکه با استفاده از درخت پوشا قصد بالا بردن کارایی شبکه را دارد، موجبات یکی از خطرناک‌ترین حملات شبکه را فراهم کرده است.

در **فصل پنجم** به حملات بر روی پروتکل‌های تونل‌زنی پرداخته‌ایم و نشان داده‌ایم که هنگامی‌که یک کاربر قوانین شبکه را با پروتکل‌های تونل‌زنی نقض می‌کند خود و شبکه را با چه خطراتی رو به رو می‌کند.

ضمیمه «الف» در این ضمیمه به‌صورت مختصر حملات Wardialing را بررسی کرده‌ایم. در این حملات هکر از طریق یک شماره‌گیری ساده به مودم کامپیوتر میزبان متصل می‌شود و با کشف پسورد کامپیوتر میزبان به‌راحتی به آن نفوذ می‌کند.

ضمیمه «ب» در این فصل نرم‌افزارهایی را که در کتاب در طی سایر فصل‌ها استفاده کرده‌ایم، برای راحتی مخاطبان توضیح داده‌ایم.

ضمیمه «پ» در این ضمیمه مخاطب با راه‌اندازی اولیه و اجرای دستورات پایه برای کار با روترها و سوئیچ‌های سیسکو در نرم‌افزار GNS3 آشنا شده است.

فهرست مطالب

فصل ۱ مجازی سازی ۱

فصل ۲ حملات Man-in-the-Middle ۱۹

فصل ۲ حملات جلوگیری از ارائه سرویس ۶۵

فصل ۵ حملات بر روی پروتکل‌های تونل‌زنی ۱۱۷