

مهندسی نفوذ

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

مهندس علیرضا رنجبر

زیر نظر:

مهندس وحید جمشیدی گوه‌ریزی

عضو هیئت علمی دانشگاه شهید باهنر کرمان



نور دانا

[illegible]

سرشناسه : رنجبر، علیرضا، ۱۳۶۷.
عنوان و نام پدیدآور : مهندسی نفوذ: پداده سازی روش های مؤثر نفوذ به شبکه های 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.

شایک : 978-964-975-175-7 :

وضعیت فهرست نویسی : فیفا

یادداشت : کتابنامه، ص. ۱۶۷-۱۷۰.

یادداشت : نمایه.

موضوع  شبکه‌های کامپیوتری -- اقدامات تأمینی

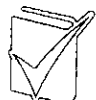
موضوع : حفاظت اطلاعات :

شناسه افزوده : جمشیدی، گهریزی، وحید، ناظر

ردمندی، کنگره : ۱۳۹۱م ۸۵/۵/۵۹ TK51

۰۰۵/۸ : رده بندی ديوي

شماره کتابشناسی، هلد : ۲۷۲۷۱۴۹



نویسندگان

مفتی محمد رفیع

قَالَ

علیرضا رنجبر

ناشر

نوپردازان

قَطْع

وزیری

نوبت چاپ

اول

تاریخ

زمستان ۱۳۹۲

تیراڑ

10..

صفحات

192

شایک

9VA-9FF-9VD-1VD-V

لیتوگرافی

نورنگ

YV02936F-YV031.2V

جواب و صحافی

طرفه

DDYF92AV-A

کتابخانه: تهران، میدان انقلاب، ابتدای خیابان آزادی، خیابان دکتر قریب، بعد از فرصت شیرازی،

بلاک ۷، تلفن: ۶۶۵۶۶۵۰۹ - ۱۸

نویز دازان: تهران، خیابان لیاقی نژاد، بین اردیبهشت و فروردین، پلاک ۲۳۸

تلفن: ۶۶۴۹۴۴.۹ - ۶۶۴۱۱۱۷۳ - ۶۶۴۱۳۵۱۵ - ۶۶۴۱۴۴۷۴

WWW.Ketabiran.ir

فروش اینترنتی

سخنی با مخاطب

امنیت در همه زمان‌ها یکی از مسائل مهم در طراحی شبکه‌ها محسوب می‌شود به طوری که هر بخش یا سازمان نیاز اساسی به ایجاد امنیت در شبکه خود را دارد. اما همان طور 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 بررسی شود و با توجه به نیاز و نوع آن شبکه موارد امنیتی خاص برای آن لحاظ شود. هنگامی که 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. به عبارت 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 هنگامی که 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 صورتی که شما نتوانید به عنوان یک هکر به شبکه خود نفوذ کنید نمی‌توانید از نقاط ضعف شبکه خود اطلاع یابید. به عبارت 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 به صورت عملی در شبکه و شرایط آن حضور یابید و با اجرای روش‌های نفوذ متفاوت سعی در به دست آوردن نقاط ضعف شبکه خود را کنید.

این حالت را با جنگ‌های واقعی مقایسه کنید. در یک جنگ که به صورت 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. به عبارت

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 به صورت عملی نشان دهد، است. ایجاد یک شبکه برای هر فرد اغلب پرهزینه است و همچنین نمی‌تواند شبکه‌ای را پیدا کند تا به صورت 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 گهواره - ناشر محترم نوپردازان که کتاب را به چاپ رسانده‌اند و همچنین از مهندس محمد حواد 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 به صورت مختصر حمله مورد نظر را تعریف می‌کنیم و شمارا 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 به صورت مرحله به مرحله و کاملاً عملی به مخاطب نشان داده می‌شود و با قرار دادن نتایج به دست آمده شما را به گونه‌ای هدایت می‌کنیم تا بتوانید با استفاده از این مراحل آن حمله را پیاده‌سازی کنید.

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 راه حل دفاعی مناسب شبکه خود را انتخاب و بر روی آن پیاده‌سازی کنید.

فصل‌بندی کتاب به صورت زیر است:

در فصل اول به مجازی‌سازی و ایجاد یک شبکه برای تست کردن سایر حملات پرداخته‌ایم و به صورت 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 سرشار 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 زمانی که 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 هنگامی که 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 به صورت مختصر حملات Wardialing را بررسی کرده ایم. در این حملات هکر از طریق یک شماره گیری ساده به مودم کامپیوتر میزبان متصل می شود و با کشف پسورد کامپیوتر میزبان به راحتی به آن نفوذ می کند.

ضمیمه «ب» در این فصل نرم افزارهایی را که در کتاب در طی سایر فصل ها استفاده کرده ایم، برای راحتی مخاطبان توضیح داده ایم.

ضمیمه «پ» در این ضمیمه مخاطب با راه اندازی اولیه و اجرای دستورات پایه برای کار با روترها و سوئیچ های سیسکو در نرم افزار GNS3 آشنا شده است.

فهرست مطالب

فصل ۱ مجازی سازی ۱

۲	VirtualBox
۵	GNS3
۱۰	تنظیمات کامپیوتر و کانکشن‌ها
۱۲	ساخت کانکشن در Windows XP Loopback

فصل ۲ حملات Man-in-the-Middle ۱۹

۱۹	پیشگفتار
۱۹	چگونگی اجرای حملات MITM
۲۱	• ربودن و دیدن (Sniffing) ترافیک شبکه
۲۱	• حملات اجرای دوباره
۲۲	• تغییر مسیر در پروتکل ICMP
۲۲	• Denial of Service
۲۲	نرم‌افزارهایی برای اجرای حملات MITM
۲۲	انواع حملات MITM
۲۲	• آلوده کردن حافظه ARP
۲۳	تئوری حملات آلوده کردن جداول ARP
۲۳	اجرای حملات آلوده کردن جداول ARP در عمل
۲۸	• حملات Man in the Middle بر روی SSL
۲۹	پروتکل SSL
۳۰	اجرای پروتکل SSL
۳۱	بررسی مشکلات پروتکل SSL
۳۱	۱. شناسایی گواهینامه
۳۲	۲. ارتباط HTTPS از طریق HTTP انجام می‌شود
۳۳	تئوری حملات MITM بر روی SSL
۳۳	۱. نوع اول حملات
۳۴	۲. نوع دوم حملات
۳۵	بررسی و مقایسه دو نوع حملات

۳۶	اجرای عملی روش دوم
۴۱	• حملات جعل DNS یا DNS Spoofing
۴۲	تئوری حملات
۴۳	اجرای حملات DNS Spoofing در عمل
۴۷	روش‌های دفاع در برابر حملات Man In The Middle
۴۷	• شناختن حملات MITM
۴۷	• روش دفاع کامل
۴۸	• زیر ساخت کلیدهای عمومی
۴۹	رمزنگاری کلید پنهان
۴۹	رمزنگاری کلید عمومی
۵۰	عملیات درهم سازی
۵۱	امضاهای دیجیتالی
۵۱	زیر ساخت کلیدهای عمومی (PKI)
۵۲	مرجع گواهینامه
۵۶	گواهینامه‌ها
۵۷	مرجع ثبت‌کننده
۵۷	مراحل اجرای PKI
۶۰	• امنیت پورت
۶۱	• گواهینامه EVSSL
۶۳	• استفاده از پروتکل‌های رمز شده
۶۳	• شناسایی سطح پایین

فصل ۳ حملات جلوگیری از ارائه سرویس ۶۵

۶۵	پیشگفتار
۶۷	سریازگیری
۶۷	نصب
۶۷	کنترل
۶۸	خودکارسازی
۶۹	انتشار
۷۰	تئوری حملات DDoS
۷۱	• پخش سیل آسا Ping
۷۲	• حملات تقویت DNS
۷۳	• حملات DDoS بر مبنای سرویس

۷۴	خطرناک حملات DoS
۷۵	پیاده‌سازی حملات DDoS در عمل
۷۶	• ساخت Botnet ها
۸۰	• انتشار Botnet ها
۸۰	• ارتباط با Botnet ها
۸۰	دفاع در برابر حملات DoS
۸۱	• توصیه‌های کلی
۸۲	• استراتژی
۸۳	• تنظیمات شبکه
۸۴	• تجهیزات DDoS
۸۵	• سیستم‌های IDS/IPS
۸۷	• Honeypot
۸۷	• واکنش نشان دادن نسبت به حملات DDoS
۸۸	• افزایش ظرفیت و ظرفیت انطباقی

فصل ۴ حملات بر روی درخت پوشا ۸۹

۸۹	پیشگفتار
۸۹	مشکل حلقه در شبکه‌ها
۹۱	پروتکل Spanning Tree (STP) چیست؟
۹۵	چگونگی اجرای حملات بر روی درخت پوشا
۹۶	دریافت ترافیک BPDU
۹۶	• Tcpdump
۹۷	• Wireshark
۹۸	تئوری حملات
۹۸	• انتخاب شدن به عنوان پل ریشه
۹۹	• اجرای حملات DoS بر روی درخت پوشا
۱۰۰	• اجرای حملات MITM بر روی درخت پوشا
۱۰۳	اجرای عملی حملات بر روی درخت پوشا
۱۰۳	• تغییر و جعل کردن فریم‌های BPDU
۱۰۵	• کشف شبکه
۱۰۸	• اجرای عملی حمله
۱۱۰	دفاع در برابر حملات بر روی درخت پوشا

- غیرفعال کردن STP ۱۱۱
- محافظ ریشه و محافظ BPDU ۱۱۴

فصل ۵ حملات بر روی پروتکل‌های تونل‌زنی ۱۱۷

- پیشگفتار ۱۱۷
- چگونگی اجرای پروتکل‌های تونل‌زنی ۱۱۸
- مثالی از اجرای عملی پروتکل تونل‌زنی برای گذشتن از Firewall ۱۱۹
- ایجاد یک کانال عبور با پروتکل SSH ۱۱۹
- Proxy ها چه هستند؟ ۱۲۱
- اجرای پروتکل SSH در عمل ۱۲۳
- استفاده از تونل ایجاد شده ۱۲۷
- استفاده از تونل در نرم‌افزار uTorrent ۱۲۷
- استفاده از تونل در مرورگر Firefox ۱۲۸
- اطمینان استفاده از تونل در نرم‌افزارها ۱۲۸
- تونل‌زنی DNS ۱۲۸
- مشکلات استفاده از تونل با SSH ۱۳۰
- تونل‌زنی SSH بر روی HTTPS ۱۳۱
- تونل‌زنی SSH بر روی HTTP ۱۳۱
- شبکه‌های TOR ۱۳۱
- مسیریابی پیازی ۱۳۱
- شبکه TOR (The Second-Generation Onion Router) ۱۳۲
- ناشناس ماندن فرستنده ۱۳۲
- ناشناس ماندن گیرنده ۱۳۳
- ناشناس ماندن مسیر ارتباطی ۱۳۳
- خطرات استفاده از پروتکل‌های تونل‌زنی ۱۳۴
- اجرای عملی حملات بر روی پروتکل‌های تونل‌زنی ۱۳۵
- دفاع در برابر حملات بر روی پروتکل‌های تونل‌زنی ۱۴۰
- پیشگیری استفاده از پروتکل‌های تونل‌زنی ۱۴۱
- کشف پروتکل‌های تونل‌زنی ۱۴۲

۱۴۳	 Wardialing چیست؟
۱۴۳	 تاریخچه
۱۴۴	 چرا Wardialing؟
۱۴۵	 انواع سیستم‌های Dial-Up که نیاز به امنیت و حفاظت دارند
۱۴۵	 • مودم‌ها - مدیریت از راه دور و نرم‌افزارهایی که این ارتباط را ایجاد می‌کنند
۱۴۵	 • سرورهای دسترسی از راه دور با استفاده از Dial-Up
۱۴۵	 • روترها و سوئیچ‌هایی که دارای مودم می‌باشند
۱۴۶	 • مودم‌هایی که به زیرساخت‌های حیاتی شبکه متصل هستند
۱۴۶	 • دسترسی به PBX ها از طریق Dial up
۱۴۶	 • هک کردن مودم‌ها و PBX ها - تکنیک‌ها و روند اجرای آن
۱۴۶	 • دسترسی به هدف
۱۴۷	 • با استفاده از نرم‌افزارهای Wardialing وضعیت تمام خطوط آن شرکت را مشخص کنید
۱۴۷	 • نتایج به دست آمده از Wardialer ها را بررسی کنید و سعی کنید
۱۴۷	 سیستم مورد نظر را از طریق Banner ها شناسایی کنید
۱۴۸	 • در صورت نیاز، خط‌هایی که مشغول بودند یا به علت انتظار زیاد نادیده گرفته شده‌اند را دوباره شماره‌گیری کنید
۱۴۸	 • با استفاده از تکنیک‌های پیشرفته سعی کنید به هدف نفوذ کنید
۱۴۹	 • کنترل دستگاهی که به آن نفوذ کرده‌اید را به دست بگیرید
۱۴۹	 نرم‌افزارهای مورد استفاده در اجرای حملات Wardialing
۱۴۹	 روش‌های ایجاد امنیت در برابر حملات Wardialing

ضمیمه «ب» توضیح نرم‌افزارهای استفاده شده در کتاب ۱۵۱

۱۵۱	 لینوکس BackTrack
۱۵۳	 FileZilla

ضمیمه «پ» دستورات اولیه برای راه‌اندازی روتر و سوئیچ سیسکو در GNS3 ۱۵۹

۱۶۷ مراجع و منابع

۱۷۱ فهرست نمایه