نفوذگری در شبکه

O احسان ملکیان، نفوذگری در شبکه و روش‌های مقابله، تهران: نص، چاپ اول: ۱۳۸۱، ۵۹۱ صفحه، وزیری، شمیز

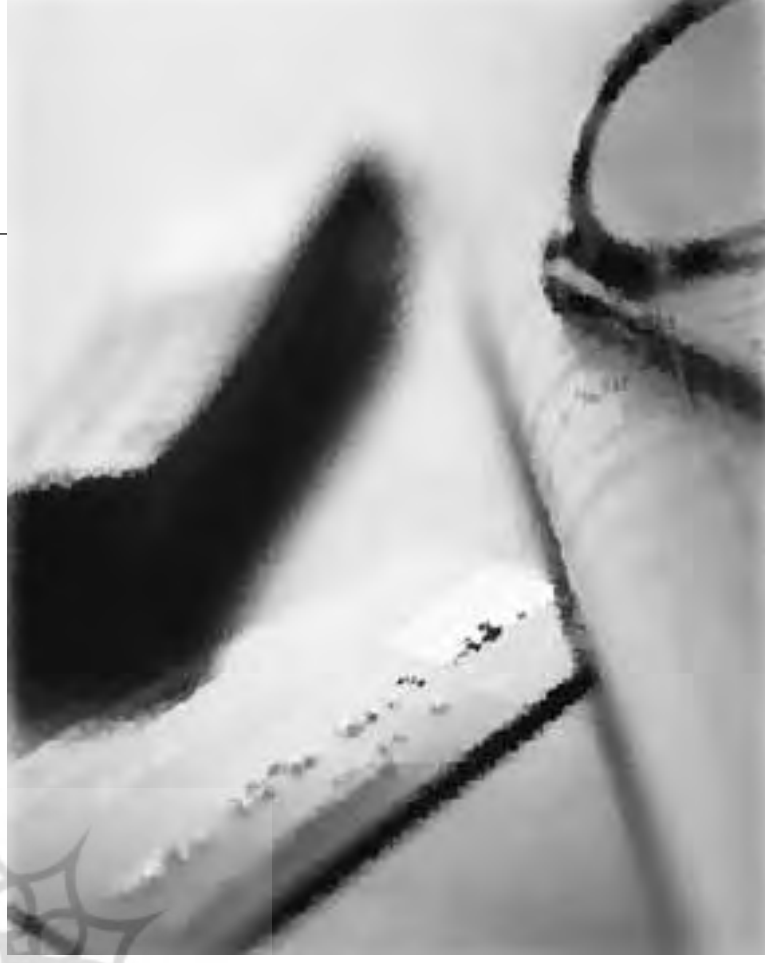
O مهندس محمدهادی معرفت

هنگامی که وارد اینترنت می‌شوید، با میلیون‌ها کاربر گمنام ارتباط برقرار می‌کنید. تا زمانی که کامپیوتر خود را به یک شبکه پهناور (همچون اینترنت) پیوند می‌دهید، هارد (Disk Drive Hard) خود را بستری مناسب برای ورود مزاحمان و یا جاسوسان قرار داده‌اید. این مزاحمان کامپیوترها را به ویروس‌ها و کرم‌ها (worns) آلوده و سعی در از بین بردن اطلاعات و خراب کردن هارد دیسک‌ها دارند، همچنین نظاره‌گر کاربران بوده تا با چک کردن نامه‌ها (mail-e)، سایت‌های مورد علاقه و... شخصیت آنها را ارزیابی کنند. متأسفانه پی بردن به اطلاعات شخصی استفاده‌کنندگان از اینترنت بسیار ساده است. همچنین به آسانی می‌توان از کارت اعتباری افراد برای خرید کردن استفاده کرد.

مؤلف این کتاب را با نگاهی به کتاب Counter Hack اثر Ed Skoudis تألیف نموده است. اولین بار واژهٔ نفوذگر (Hacker) در دهه شصت میلادی در دانشگاه MIT به وجود آمد. اصلاً نفوذگر کسی است که از سرکشی به فایل‌ها و برنامه‌های قابل نفوذ و سیستم‌های محرمانه لذت می‌برد و تنها قصد آن شکست توانایی‌های محاسباتی ماشین در مقابل هوش آدمی است. در اواخر دههٔ هشتاد جنبش نفوذگری (Hacktivism) در شبکه به سوی فعالیت‌های ضدامنیتی گرایش پیدا کرد.

این کتاب در ۱۲ فصل به بررسی انواع حملات و رخنه‌ها در شبکه و سیستم‌های امنیتی شبکه می‌پردازد.

در فصل اول کتاب که با عنوان پیشگفتار نامیده شده است. ضمن معرفی پیشینه جنبش نفوذگری، به بررسی انواع و اقسام هکرها پرداخته است و این گروه‌ها عبارتنداز: ۱) نفوذگران کلاه سفید (white hat Hacker)که از نوع نفوذگران خوب می‌باشند. یک کلاه سفید باعث سازندگی و پویایی سیستم‌ها می‌گردد و معایب آنها را به مدیران مربوطه گوشزد می‌نماید. ۲) نفوذگران کلاه سیاه (Black Hat Hacker). معروف به نفوذگران خرابکار و بد می‌باشند. این‌گونه نفوذگران معمولاً در سیستمی که بدان نفوذ کرده‌اند از خود اثری باقی می‌گذارند و عاشق دستبرد زدن به فایل‌ها و



تاریخ نشان می‌دهد که تمام سیستم‌های عامل با هر قابلیت و عظمتی، سرشار از نقاط آسیب‌پذیر بوده‌اند. درحالی که این سیستم عامل‌ها فقط برای مقابله با مشکلات عادی آمادگی دارند، در صورت وجود یک اشکال عمده ممکن است که حتی سیستم مختل گردد. این جاست که هوش و ذکاوت یک نفوذگر و داشتن یکسری از اطلاعات و تبحر در برنامه‌نویسی می‌تواند عامل مهمی برای رسیدن به هدف اصلی یعنی از بین بردن و مختل کردن سیستم عامل باشد

اطلاعات شخصی مردمان هستند. ۳) نفوذگران کلاه خاکستری (Gray Hat Hacker). نفوذگران کمی خوب و اندکی مخرب هستند. ۴) نفوذگران کلاه صورتی (Pink Hat Hacker). نفوذگران لوس، بی‌مزه و بی‌خاصیت. بی‌طور کل هر نوعی از نفوذگر را می‌توان به عنوان یک دشمن خارجی برای شبکه محسوب کرد. بدین معنا که معمولاً از بیرون شبکه اقدام به نفوذ و حمله می‌نمایند. علاوه بر این یک شبکه ممکن است دشمنان داخلی هم داشته باشد (یعنی افرادی که دسترسی مستقیم به شبکه دارند) این افراد ممکن است از کارمندان و مشتریان ناراضی، پیمانکاران و یا شرکای تجاری شبکه که انگیزه‌ای به جز سود جویی نداشته باشند، تشکیل شده باشد.

برخی از انگیزه‌ها و اندیشه‌های یک نفوذگر عبارتنداز: اهداف سیاسی و دولتی، آزاررسانی و کسب شهرت، جاسوسی و کسب اطلاع از وضعیت نظامی یک کشور. البته امروزه نفوذگران را از لحاظ مهارت و توانایی می‌توان به چندین گروه متفاوت طبقه‌بندی نمود گروه اول که معروف به کودک هستند، معمولاً افرادی بی‌تجربه هستند که می‌خواهند با استفاده از ابزارهای نفوذگری عرض اندامی بنمایند گروه دوم افرادی با سطح معلومات متوسط را شامل می‌شود که اطلاعاتی از اصول فنی اینترنت و سرویس‌دهنده‌های وب دارند و سعی در پیدا کردن نقاط ضعف شبکه‌ها را دارند. گروه سوم را به نام نفوذگران خبره و هوشمند می‌شناسیم که بدون هیچگونه هیاهویی با خلق ابزار و یا تکنیک جدید مدت‌های مدیدی سیطره کاملی بر شبکه دارند و هرگز ردپایی از خود برجای نمی‌گذارند. درانتهای این فصل نیز به روش راه‌اندازی یک آزمایشگاه برای آشنایی با ابزارهای حمله و نفوذ هکرها پرداخته است.

فصل دوم یک مرور اجمالی بر مفاهیم TCP/IP (Protocol Transmission Control Protocol / Internet) دارد که پیش نیاز فهم مکانیزم‌های مختلف حمله و دفاع محسوب می‌شود. TCP/IP قراردادی است که برای ایجاد ارتباط بین کامپیوترها نوشته شده است. این قرارداد در سیستم UNIX (یونیکس) قرار دارد و استاندار برای انتقال اطلاعات در شبکه‌ها از جمله پشته اینترنت است. در این فصل برای تعمیق دانش پایه از تکنولوژی شبکه به دو موضوع متفاوت مدل TCP/IP و پشته پروتکل‌های TCP/IP پرداخته است. به دلیل اینکه طراحی شبکه‌ها سلیقه‌ای و پیچیده نشود سازمان جهانی استاندارد ISO (Intenational standard Organization) یک مدل هفت لایه‌ای برای شبکه ارائه کرد به گونه‌ای که وظایف و خدمات شبکه در هفت لایه مجزا تعریف و ارائه می‌شود این مدل هفت لایه‌ای OSI[1] نام دارد. این مدل ارتباطات کامپیوتر به کامپیوتر را به هفت لایه، جدا می‌کند. هریک از لایه‌ها براساس استانداردهایی بنا می‌شود که در لایه‌های زیر آن قرارداد. به طوری که پایین‌ترین لایه از لایه‌های هفت گانه فقط با ارتباط‌های سخت‌افزاری سروکار دارد، بالاترین لایه با تعامل‌های نرم‌افزاری در سطح برنامه کاربردی سروکار دارد. این لایه‌ها عبارتنداز: ۱ـ لایه فیزیکی (Physical Layer) ۲ـ لایه پیوند داده‌ها (Layer Data Link) ۳ـ لایه شبکه (Network Layer) ۴ـ لایه انتقال (Layer Transport) ۵ـ لایه جلسه (Session Layer) ۶ـ لایه نمایش (ارائه) (Presentiation Layer) ۷ـ لایه کاربرد (layer Application)

زیر بنای اینترنت ساختار چهارلایه‌ای TCP/IP است. حملات نفوذگران در یکی از این چهار لایه صورت می‌گیرد. این چهار لایه تلفیقی از هفت لایه OSI می‌باشد. بنابراین ماهیت و مکانیزم‌های

حمله و همچنین ابزار و هدف حمله، وابسته به لایه‌ای است که مورد حمله قرار می‌گیرد. کلیدی‌ترین پروتکلی که در این فصل به تفصیل مورد بررسی قرار می‌گیرد، پروتکل IP (Internet Protocol) نام دارد. برخی از پروتکل‌های مهم که یک سری وظایف جانبی دارند و در این فصل بررسی شده‌اند عبارتنداز: ARP (Address Resolution Protocol)، UDP (User Datagram Protocol) در انتهای این فصل به معرفی دیواره آتش (Firewall) پرداخته می‌شود. دیواره آتش سیستمی است که در بین کاربران شبکه محلی و شبکه اینترنت قرار می‌گیرد و ضمن نظارت بر دسترسی‌ها، در تمام سطوح ورود و خروج اطلاعات نظارت کامل دارد.

فصل سوم به بررسی ویژگی‌های کلی سیستم عامل یونیکس (UNIX) و گونه‌های سازگار با آن اختصاص دارد. این سیستم عامل به دلیل سابقه‌ای که دارد حملات متنوع و پیچیده‌ای بر علیه آن شکل گرفته است. ولی با این حال می‌توان گفت که بخش بسیار بزرگی از ساختار شبکهٔ اینترنت شامل سرویس‌دهنده‌ها، ایستگاه‌های کاری (workstation) و ماشین‌های نهایی (Host) به نحوی از یونیکس استفاده می‌کنند.

در سیستم عامل یونیکس هرچیزی به صورت یک فایل تلقی و مدل می‌شود به صورتی که این سیستم عامل برای خود یک فرهنگ و ادبیات ویژه وضع کرده است. یونیکس از ساختار پیمانه‌ای (ماجولار) استفاده کرده است.

به گونه‌ای که در پایین‌ترین سطح یک هسته با بستر سخت‌افزار درگیر است و تمام برنامه‌ها به صورت هویتی مستقل حول هسته شکل می‌گیرد. در ادامه این فصل با پروسه‌های مهم و نحوه کارکرد آنها آشنا خواهید شد.

در فصل چهارم به بررسی مشخصات کلی سیستم عامل ویندوز (نسخه NT ,۲۰۰۰) پرداخته شده است. بدون داشتن مطالعه عمیق و اصولی پیرامون مفاهیم این فصل، حمله و روش‌های دفاعی سازگار نخواهد بود. این سیستم عامل تاکنون بیشترین حملات موفق برعلیه آن انجام شده است. لذا آسیب‌پذیرترین سیتم عامل شناخته شده است. این فصل نسخه‌های کلی سیستم عامل ویندوز را از دیدگاه امنیت بررسی می‌کند. معماری NT شامل دو بخش حالت کاربر (User mode) و حالت هسته (kernel Mode) می‌باشد. این دو حالت به تفصیل مورد بررسی قرار گرفته است. NT برای ایجاد امنیت در سطح شبکه و نظارت بر دسترسی‌های آن تمهیداتی را اندیشیده است. این موارد را می‌توانید در بخش مبحث تعیین مجوز برای منابع اشتراکی در شبکه بیابید. در انتهای این فصل سیستم عامل ویندوز ۲۰۰۰ و ویژگی‌های جدید این سیستم عامل را که به نحوی به امنیت سیستم مربوط می‌شود به طور مختصر مورد بررسی قرار خواهد داد.

پس از مباحث معمول و مقدماتی هسته اصلی کتاب آغاز می‌شود. اکثر حملات در پنج مرحله متفاوت طرح‌ریزی و انجام می‌شود. این فصل‌ها در عنوان پنج گام از فصل پنجم تا یازدهم این کتاب بررسی و تشریح شده‌اند.

فصل پنجم: نحوه شناسایی مقدماتی شبکه مقصد را برای نفوذگر تعریف می‌کند. نفوذگران باتجربه و ماهر برای شناسایی مشخصات فنی و عمومی شبکه هدف، وقت بسیاری را می‌گذارند. این مشخصات و یا اطلاعات به صورت غیرمحرمانه در شبکه منتشر شده است. بدست آوردن اطلاعات عمومی برای شناسایی مقدماتی شبکه هدف کار چندان مشکلی نیست ولی اصول و راهکارهای ویژه‌ای دارد. در ادامه این فصل بعد از آشنایی با راه‌های شناسایی مقدماتی، راه‌های پیشگیری از دسترسی نفوذگر به اطلاعات حساس، معرفی خواهد شد. روش‌های شناخته شده برای شناسایی مقدماتی هدف که در این فصل به تفصیل مورد بررسی قرار گرفته‌اند عبارتنداز:

۱) شناسایی به روش مهندسی اجتماعی و روش‌های روان‌شناختی، گرفتن اطلاعات از راه‌های‌استفاده از تلفن به عنوان پیشابانان فنی شبکه و یا عنوان‌های مدیریتی دیگر ۲) آشغال گردی و روش‌های دفاعی جست‌وجو در میان کاغذهای باطله و دستنوشته‌های معدوم شده، چنین روشی معمولاً برای شرکت‌های بزرگ ملی و دولتی کارساز است ۳) جست‌وجو در وب و استفاده از موتورهای جست‌وجو در اینترنت ۴) استفاده از Usenet.

گروه‌های خبری Usenet فضای خوبی جهت بیرون کشیدن اطلاعات حساس در مورد شبکه هدف برای نفوذگر می‌باشد ۵) بانک‌های اطلاعاتی whois: مکان خوبی برای استخراج نام‌های حوزه (Domain) و IP شرکت‌ها و اشخاص می‌باشد ۶) استفاده از سایت ARIN جهت تحقیق در مورد آدرس IP در این سایت شما می‌توانید بفهمید که مثلاً یک آدرس IP متعلق به چه شرکت یا سازمانی است.

در انتهای این فصل ابزارهایی برای شناسایی شبکه مبتنی بر وب را معرفی و بررسی می‌کند.

در فصل ششم به بررسی گام دوم یعنی پویش و جست‌وجو در شبکه به دنبال رخنهٔ نفوذ پرداخته می‌شود. در گام اول نفوذگر مقداری اطلاعات در مورد شبکه هدف به دست آورده است که این اطلاعات شامل موارد زیر است: آدرس IP شبکه هدف، آدرس حوزه شبکه هدف و تعدادی از شماره تلفن‌های دسترسی به شبکه و یک سرویس اطلاعات پیرامون خدمات شبکه هدف.

مودم یکی از متداول‌ترین ابزاری است که نفوذگر برای رسیدن به شبکه از آن استفاده می‌کند. نفوذگر با استفاده از یک سری شماره تلفن‌های احتمالی به دنبال تشخیص یک سیگنال حامل (Carrier) مربوط به مودم می‌گردد و این کار از طریق نرم افزارهای

خاص حمله به مودم‌ها مانند THC-Scan قابل انجام است.

مرحله بعد برای یک نفوذگر ترسیم توپولوژی مربوط به شبکه هدف است. با استفاده از ابزارهای پویش در شبکه، نفوذگر می‌تواند ماشین‌های سرویس‌دهندهٔ مختلف را از قبیل FTP, web Proxy, تشخیص بدهد. بعد از تشخیص توپولوژی تقریبی شبکه نفوذگر می‌تواند با استفاده از عمل پویش پورت (Port Scan) فهرست مشخصی از شماره پورت‌ها را بررسی نماید و از باز یا بسته بودن آن آگاه شود. البته پویش پورت مکانیزم‌های مختلفی دارد که به تفصیل در این بخش کتاب مورد بررسی قرار گرفته‌اند. به غیر از جست‌وجوی پورت‌های باز روی ماشین و دستیابی به آنها نفوذگر تمایل دارد سیستم عامل نصب شده روی شبکه هدف را تشخیص بدهد و میزان آسیب‌پذیری آن با شبکه را باتوجه به نوع سیستم عامل تخمین بزند و با توجه به نوع سیستم عامل نوع حمله خود را طراحی و اجرا کند.

یکی از ابزارهای بسیار بدیع که می‌تواند در خدمت نفوذگر قرار بگیرد استفاده از نرم‌افزاری به نام Firewall است. دیواره آتش یا فیلتر تنها ابزاری است که جلوی تاخت و تازهای نفوذگران را در شبکه می‌گیرد. Firewall سعی می‌کند تا متوجه شود چه شماره پورت‌هایی از طریق دیواره آتش بازمانده است و قواعد فیلترینگ دیواره آتش شبکه بااستفاده از این ابزار استخراج می‌شود. نحوه استفاده از این ابزار و راه‌های مقابله با آن یکی از موضوع‌های مطرح شده در این فصل می‌باشد.

کشف مزاحمت (IDS) برنامه‌ای است که با تحلیل ترافیک شبکه بااستفاده از تحلیل داده‌ها وتقاضاها سعی در شناسایی فعالیت‌های نفوذگر دارد: در صورت مشاهده خطر، به مانند یک آژیر دزدگیر، مسئولان شبکه را متوجه ترافیک‌های مجازی کرده و حضور نفوذگران در شبکه را نشان می‌دهد. عملکرد سیستم IDS آخرین مبحث مطرح شده در این فصل می‌باشد.

فصل هفتم به بررسی گام سوم یعنی نفوذ از طریق رخنه در سیستم عامل یا برنامه‌های کاربردی می‌پردازد.

تاریخ نشان می‌دهد که تمام سیستم‌های عامل با هر قابلیت و عظمتی، سرشار از نقاط آسیب‌پذیر بوده‌اند. درحالی که این سیستم عامل‌ها فقط برای مقابله با مشکلات عادی آمادگی دارند، در صورت وجود یک اشکال عمده ممکن است که حتی سیستم مختل گردد. این جاست که هوش و ذکاوت یک نفوذگر و داشتن یکسری از اطلاعات و تبحر در برنامه‌نویسی می‌تواند عامل مهمی برای رسیدن به هدف اصلی یعنی از بین بردن و مختل کردن سیستم عامل باشد. یکی از راههای شکستن برنامه‌های کاربردی از طریق سرریز کردن پشته است.[۲] نفوذگر پروسه‌هایی را که به نحوی از پشته یا بافر استفاده کرده‌اند ولی برای سرریز شدن آن فکری نکرده‌اند،کشف می‌کند و آنها را مورد هدف قرار می‌دهد. گونه بسیار پیچیده وخطرناکی از حمله به پشته آن است که نفوذگر بتواند پشته را به نحوی سرازیر کند که پس از سرریز شدن کنترل اجرای آن برنامه پروسه را در دست بگیرد. برای آشنایی با اصول این حملات و فراگیری راههای پیشگیری و مقابله با آنها به مبحث آن در این فصل مراجعه نمایید.

به غیر از آسیب‌پذیری برنامه‌ها و پروسه‌ها در مقابل سرریز شدن پشته، یکی از مهمترین عامل‌های نگرانی شکاف‌های ناشی از ضعف برنامه‌نویسی (Bugs) است. یک برنامه ممکن است در شرایط عادی سال‌ها به درستی کار کند و باگ‌های آن کشف نشود. در حالی که نفوذگر ممکن است ماه‌ها به دنبال همین اشکالات باشد. در اکثر سیستم‌های کامپیوتری موجود در سازمان‌ها یکی از روش‌های تأمین امنیت از داده‌های محرمانه و حساس، استفاده از کلمات عبور است. حدس زدن کلمات عبور به روش‌های سعی و خطا توسط ابزارهای خودکار فرآیندچندان سختی نیست و یک نفوذگر تازه‌کار هم می‌تواند آنها را به کار گیرد. L ø fphtcrack یکی از قوی‌ترین و قدرتمندترین ابزار شکستن کلمه عبور محسوب می‌شود و یک نرم‌افزار ساده، زیبا و سریع است که مخصوص ماشین‌هایی با سیستم عامل‌های Windows ۲۰۰۰ NT است. راه استفاده از این نرم‌افزار و روش‌های مقابله با ابزارهای شکننده کلمه عبور از مباحث مطرح شده در این فصل می‌باشد.

فصل هشتم دنبالهٔ گام سوم و به مبحث نفوذ از طریق استراق سمع در سطح لایه شبکه می‌رسیم. حمله در سطح لایه شبکه گاهی بسیار مخرب و خطرناک‌تر از حملات در لایه‌های بالاتر است. sniffer برنامه‌ای است که نفوذگر با استفاده از ترافیک جاری بر روی شبکه محلی استراق سمع کرده و بخش‌های مفید آن را در اختیار نفوذگر قرار می‌دهد. این حمله یکی از خطرناک‌ترین حملات غیرفعال (Passive) محسوب می‌شود و به سادگی قابل کشف نیست. اطلاعاتی که یک Sniffer سرقت می‌کند امنیت تک تک ماشین‌های یک شبکه محلی را به خطر می‌اندازد. ابزارهای دیگری که برای استراق سمع عنوان شده‌اند، عبارتنداز: ابزار Snort، ابزار Sniffit، ابزار Dsniff

حمله مخرب دیگری که در این بخش مورد بررسی قرار می‌گیرد. «ربودن یک نشست» (Session Hijacking) می‌باشد. در این نوع حمله نفوذگر به ناگاه خود را به جای کاربر وانمود کرده و ضمن آنکه نشست قبلی را ادامه می‌دهد کاربر اصلی را با قطع ارتباط مواجه می‌کند در هنگام این قطع ارتباط، نشست قبلی او توسط نفوذگر دزدیده شده است. ابزار Hunt یکی از ابزارهای ربودن نشست است که در این فصل مورد بررسی قرار گرفته است.

یکی از مباحث انتهایی این فصل استفاده از ابزار NetCat و روش‌های مقابله با این ابزار است. این نرم‌افزار قادر است هرگونه داده‌ای را بر روی هر پورت TCP یا UDP مبادله نماید.

فصل نهم: آخرین مرحله از گام سوم یعنی اخلال در سرویس‌دهی بااستفاده از حملات Dos را بررسی می‌کند. براساس این حمله نفوذگر تلاش می‌کند به یکی از روش‌های علمی / عملی،

مانع از سرویس‌دهی یک سرویس‌دهنده در شبکه شود. حمله Dos می‌تواند حالت خفته و هدایت شده از قبل داشته باشد. در این فصل نیز انواع حملات Dos نیز توضیح داده شده است.

فصل دهم: این فصل به بررسی گام چهارم یعنی سیطره بر شبکه توسط نفوذگر بعد از رخنه در شبکه هدف می‌پردازد. بعد از اینکه نفوذگر توانست به شبکه نفوذ کند باید نفوذ خود را حفظ کند. برای رسیدن به چنین هدفی نفوذگر از نرم‌افزارهای آلوده و مخربی مثل اسب‌های تروا (Trojan Horses)، درهای پشتی (Backdoors) استفاده می‌کند که این نرم‌افزارها به عنوان یک ستون پنجم تحت فرمان نفوذگر عمل می‌کند. این فصل به بررسی این نرم‌افزارها و راه‌های پیشگیری و مقابله با این نرم‌افزارها می‌پردازد.

فصل یازدهم: گام پنجم یعنی ردگم کردن و مخفی ماندن است. اکثر نفوذگران حملات پیچیده خود را به گونه‌ای طراحی می‌کنند که نه تنها هیچ اثری از خود بر جای نمی‌گذارند بلکه برای مدت‌های بسیار طولانی مخفی وآرام می‌ماند و نفوذگر می‌تواند یک دستبرد طولانی مدت را انجام دهد که معمولاً خسارات جبران‌ناپذیری به جا خواهد گذاشت. این فصل به بررسی راهکارهایی می‌پردازد که نفوذگر حمله خود را مخی نگاه می‌دارد و با این کار تسلط و سیطره خود را بر یک سیستم یا شبکه بلندمدت و طولانی نماید. قربانیان این حملات بیشتر ادارات دولتی، شرکت‌های تجارتی دانشگاه‌ها و محیط‌های نظامی بوده‌اند.

یکی از راه‌هایی که در این فصل به بررسی آن پرداخته شده است این است که نفوذگر پس از اولین نفوذ برای از بین بردن ردپاهای خود به بخش ثبت رخدادها (Event Logs) رجوع کرده و رکوردهای ثبت شده از تلاش‌های مکرر وناقص برای ورود به سیستم و تعداد رکوردهای ثبت شده از خطاهای متوالی و مشابه را از بین می‌برد. البته این روش برای نفوذگران حرفه‌ای مرسوم نیست. چرا که آنان به جای حذف فایل‌ها، فایل‌های (Event Logs) را تغییر می‌دهند. مؤثرترین حمله بر علیه فایل‌های ثبت رخداد، استفاده از ابزارهایی است که قادرند فایل‌های ثبت رخدادها را (EVT.) نسخه‌برداری کنند و در حافظه بار کنند. یکی دیگر از راه‌های مخفی ماندن اثر ردپاهای نفوذگران مخفی کردن شاخه‌های ایجاد شده توسط نفوذگر روی ماشین قربانی می‌باشد چرا که حضور یک فایل مشکوک بر روی سیستم فایل ماشین قربانی به سادگی کشف شده و با آن مبارزه خواهد شد. راه دیگر از بین بردن رد پای نفوذگر، رخنه از طریق کانال‌های پنهان (Covert channel) است که منظور مکانیزم‌های ارتباط مخفیانه و نهانی نفوذگر با قربانی است. کانال‌های پنهان مکانیزم‌های پنهان‌سازی ترافیک داده‌ها بین نفوذگر و قربانی است به گونه‌ای که حتی‌الامکان کشف نشود و رمزنگاری فقط به عنوان بخش کوچکی از این مکانیزم‌ها مطرح است. راه‌های مهم ایجاد کردن کانال‌های پنهان از طریق زیر است: ۱) استفاده از روش Loki ۲) ایجاد کانال‌های پنهان از طریق HTTP ۳) از طریق Telnet.

فصل دوازدهم: به تشریح و کالبدشکافی سه نوع حمله پرداخته و راه‌های غلبه بر مشکلات امنیتی مطرح شده در این سه نمایشنامه را بررسی می‌نماید.

این کتاب دارای چهار ضمیمه است که در ضمیمه الف به بررسی اسب تروای Bo۲k پرداخته است. ضمیمهٔ ب نحوهٔ کار با یکی از قوی‌ترین دیواره آتش شخصی یعنی Zone Alarm را آموزش می‌دهد. ضمیمه ج استانداردهای رمزنگاری و راه‌های رمزنگاری و احراز هویت را بررسی می‌کند. ضمیمه د فهرست محتویات CD جنبی کتاب است.

یکی از جنبه‌هایی که باعث شده این کتاب برتر از کتاب‌های مشابه نمود کند این است که مطالب مطرح شده در این کتاب درعین جامعیت، با زبانی ساده‌تر و عملیاتی‌تر بیان شده است. در حالی که در ترجمه‌های اخیر کتاب‌های Hacker اشتباهات فاحش مترجمان آن باعث دور شدن مطلب از منظور اصلی بحث شده است.

به علاوه CD جانبی که همراه این کتاب عرضه شده است، حاوی قطعات ویدیو و مقالات مختلف و چند کتاب الکترونیکی خوب مرتبط با موضوع‌های بحث شده در مورد کتاب است که می‌تواند مکمل بسیار خوبی برای این کتاب باشد در CD تمام ابزارهای استفاده شده در این کتاب (حدود صدوشصت ابزار) وجود دارد.

هرگز نباید نفوذگران را با هر انگیزه و اندیشه‌ای دست کم گرفت. اکثر این جماعت افرادی هستند با ضریب هوشی، قدرت تصمیم‌گیری و سرعت انتقال بالا؛ همچنین تحصیلکرده، کنجکاو، فعال و بی‌قرار!

کدام یک از این خصوصیات را کامپیوتر دارد تا بتوان به آن اطمینان کرد.

پی‌نوشت‌ها :

1- open system interconnection

۲- پشته یک نوع ساختمان داده است که آیتم‌های داده در آن ذخیره می‌شود.