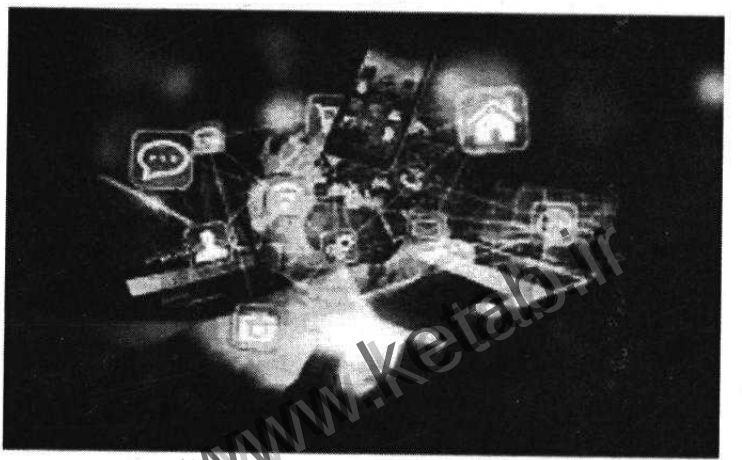
اصول و مبانی امنیت در شبکه های رایانه ای



نویسندگان

محمدحسین روزبهانی

رضا اقدامی کلید بری

جواد خباز

سرشناسه : روزبهانی، محمدحسین، ۱۳۷۸-
عنوان و نام پدیدآور : اصول و مبانی امنیت در شبکه‌های رایانه‌ای/ نویسندگان محمدحسین روزبهانی، رضا اقدامی‌کلید بری، جواد خباز.
مشخصات نشر : تهران: نشر بهداد، ۱۴۰۱.
مشخصات ظاهری : ۱۶۴ ص.: مصور(رنگی)، جدول.
شابک : ۱۵۰۰۰۰۰ ریال :978-600-8203-69-8
وضعیت فهرست نویسی : فیپا
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
Computer networks -- Security measures
کامپیوترها -- ایمنی اطلاعات
Computer security
شناسه افزوده : اقدامی کلیدبری، رضا، ۱۳۶۸-
شناسه افزوده : خباز، جواد، ۱۳۵۳-
رده بندی کنگره : TK۵۱۰۵/ ۵۹
رده بندی دیویی : ۰۰۵/ ۸
شماره کتابشناسی ملی : ۸۸۵۵۵۶۴
اطلاعات رکورد کتابشناسی : فیپا

عنوان کتاب: اصول و مبانی امنیت در شبکه های رایانه ای
مولفان : محمدحسین روزبهانی - رضا اقدامی کلیدبری - جواد خباز
ناشر: انتشارات بهداد
قطع و تیراژ: وزیری / ۱۰۰ جلد
قیمت: ۱۵۰/۰۰۰ تومان
تعداد صفحات : ۱۷۸
چاپخانه : دیانا
صحافی : دیانا
نوبت چاپ: اول
سال چاپ: ۱۴۰۱
شابک: ۹۷۸-۶۰۰-۸۲۰۳-۶۹-۸

چکیده

هدف از ارائه ی این کتاب معرفی اصول و مبانی امنیت در شبکه های کامپیوتری می باشد .در ابتدا به تعاریف و مفاهیم امنیت در شبکه می پردازیم .

در مبحث امنیت شبکه ،منابع شبکه وانواع حملات ،تحلیل خطر ،سیاست های امنیتی ،طرح امنیت شبکه و نواحی امنیتی به تفضیل مورد تحلیل و بررسی قرار می گیرد .

برای حفظ امنیت شبکه نیاز است تا مراحل اولیه ایجاد امنیت و سیتم های عامل و برنامه کاربردی مناسب لحاظ شود .در ادامه به انواع حملات در شبکه های رایانه ای پرداخته ایم و برای افزایش امنیت در سطح شبکه به AUDITING ، کامپیوترهای بدون دیسک ،به رمز در آوردن داده ها و محافظت در برابر ویروس پرداخته ایم .

و اما روشهای تامین امنیت در شبکه که عبارتند از : دفاع در عمق ،فایروال و پراکسی که به طور کامل تشریح شده است .و در ادامه سطوح امنیت شبکه ، تهدیدات علیه امنیت شبکه ، امنیت شبکه لایه بندی شده، ابزارها و الگوهای امنیت شبکه ،مراحل ایمن سازی شبکه ، راهکارهای امنیتی شبکه ،مکانیزم های امنیتی و الگوریتم جهت تهیه الگوی امنیت شبکه توضیح داده شده است .

واژه‌های کلیدی

امنیت ،حملات ، شبکه ، فایروال ، پراکسی ، الگو

فهرست مطالب

مقدمه ۱

فصل اول ۱

تعاریف و مفاهیم امنیت در شبکه ۱

۱) تعاریف امنیت شبکه : ۲

۲) مفاهیم امنیت شبکه ۲

امنیت شبکه یاNetwork Security ۲

۲-۱) منابع شبکه ۳

۲-۲) حمله ۳

۲-۳) تحلیل خطر ۴

۲-۴) سیاست امنیتی ۵

۲-۵) طرح امنیت شبکه ۵

۲-۶) نواحی امنیتی ۶

فصل دوم ۹

انواع حملات در شبکه های رایانه ای ۹

۱)مفاهیم حملات در شبکه های کامپیوتری ۱۰

۲) وظیفه یک سرویس دهنده ۱۱

۳) سرویس های حیاتی و موردنیاز ۱۳

۴) مشخص نمودن پروتکل های مورد نیاز ۱۴

۵) مزایای غیرفعال نمودن پروتکل ها و سرویس های غیرضروری ۱۵

۶)انواع حملات (Attacks) ۱۷

۶-۱) حملات از نوع DoS ۱۸

۶-۲) حملات از نوع DDoS (distributed denial-of-service) ۱۹

چگونه از وقوع حملات DoS و یا DDoS آگاه شویم ؟ ۱۹
در صورت بروز یک تهاجم ، چه عملیاتی را می بایست انجام داد ؟ ۲۰
۶-۱-۱) Smurf/smurfing : ۲۰
Fraggle (6-1-2 ..... ۲۱
Ping flood (6-1-3 ..... ۲۱
SYN flood(6-1-4 ..... ۲۱
Land (6-1-5 ..... ۲۲
Teardrop(6-1-6 ..... ۲۲
Bonk (6-1-7 ..... ۲۲
Boink(6-1-8 ..... ۲۳
۶-۳) حملات از نوع Back door ۲۴
Back Orifice(6-3-1 ..... ۲۵
NetBus(6-3-2 ..... ۲۵
Sub7) SubSeven(6-3-3 ..... ۲۶
VNC) Virtual Network Computing (6-3-4 ..... ۲۶
PCAnywhere(6-3-5 ..... ۲۶
Terminal(6-3-6 Services ۲۷
جدول۱-۲. مقایسه تهدیدات امنیتی در لایه های چهارگانه TCP/IP ۲۸
جدول۲-۲. اهداف امنیتی در منابع شبکه ۲۹
packet sniffing(7 چیست ؟ ۳۰
۷-۱) نحوه کار packet sniffing ۳۱
۷-۲) روش های تشخیص packet sniffing در شبکه ۳۲
۷-۳) بررسی سرویس دهنده DNS : ۳۲

۴-۷) اندازه گیری زمان پاسخ ماشین های مشکوک : ۳۳
۵-۷) استفاده از ابزارهای مختص AntiSniff ۳۴
فصل سوم : ۳۵
افزایش امنیت در شبکه ۳۵
۱) علل بالا بردن ضریب امنیت در شبکه : ۳۶
۳) راه‌های بالابردن امنیت در شبکه ۳۷
۱-۳) آموزش ۳۷
۲-۳) تعیین سطوح امنیت ۳۷
۳-۳) تنظیم سیاست‌ها ۳۸
۴-۳) به رسمیت شناختن یا Authentication ۳۸
۵-۳) امنیت فیزیکی تجهیزات ۳۸
۶-۳) امنیت بخشیدن به کابل ۳۹
۴) مدل‌های امنیتی ۴۰
۱-۴) منابع اشتراکی محافظت شده توسط کلمات عبور ۴۰
۲-۴) مجوزهای دسترسی (Access Permissions) ۴۱
۵) امنیت منابع ۴۲
۶) روش‌های دیگر برای امنیت بیشتر ۴۳
Auditing(6-1 ۴۳
۲-۶) کامپیوترهای بدون دیسک ۴۴
۳-۶) به رمز درآوردن داده‌ها ۴۵
۴-۶) محافظت در برابر ویروس ۴۶
فصل چهارم : ۴۷
انواع جرایم اینترنتی وعلل بروز مشکلات امنیتی ۴۷

امنیت و مدل TCP/IP: ۴۸
۱-۱) لایه فیزیکی : ۴۸
۱-۲) لایه شبکه : ۴۹
۱-۳) لایه حمل : ۵۰
۱-۴) لایه کاربرد : ۵۰
۲) جرائم رایانه‌ای و اینترنتی ۵۲
۲-۱)پیدایش جرایم رایانه‌ای ۵۳
۲-۲) قضیه رویس: ۵۳
۲-۳)تعریف جرم رایانه‌ای ۵۴
۲-۴) طبقه‌بندی جرایم رایانه‌ای ۵۵
۳-۴) علل بروز مشکلات امنیتی ۶۱
۳-۴-۱) ضعف فناوری ۶۲
۳-۴-۲) ضعف پیکربندی ۶۴
۳-۴-۳) ضعف سیاست ها ۶۸
فصل پنجم: ۷۱
روشهای تامین امنیت در شبکه ۷۱
۵-۱)اصول اولیه استراتژی دفاع در عمق ۷۲
۱-۵-۱) دفاع در عمق چیست ؟ ۷۲
۱-۲-۱) انسان ۷۳
۲-۲-۱) فناوری ۷۳
۳-۲-۱) عملیات ۷۴
۳-۱) استراتژی دفاع در عمق : محدوده حفاظتی ۷۵
۴-۱) استراتژی دفاع در عمق : ابزارها و مکانیزم ها ۷۶

۵-۱) استراتژی دفاع در عمق : پیاده سازی ۷۷
۶-۱) جمع بندی ۷۸
۲) فایروال ۷۸
۱-۲) ایجاد یک منطقه استحفاظی (security perimeter) ۷۹
۲-۲) شبکه های perimeter ۸۰
۳-۲) فایروال ها : یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات ۸۳
۴-۲) فیلترینگ پورت ها ۸۴
۵-۲) ناحیه غیرنظامی (Demilitarized Zone) ۸۶
۶-۲) فورواردینگ پورت ها ۸۷
۷-۲) توپولوژی های فایروال ۸۹
عملکردهایی که پراکسی سرور می‌تواند داشته باشد ۹۹
۱-۳) پیکربندی مرورگر ۱۰۲
۲-۳) پراکسی چیست؟ ۱۰۲
۳-۳) پراکسی چه چیزی نیست؟ ۱۰۲
۴-۳) پراکسی با Packet filter تفاوت دارد ۱۰۳
۵-۳) پراکسی با Stateful packet filter تفاوت دارد ۱۰۴
۶-۳) پراکسی ها یا Application Gateways ۱۰۵
۷-۳) برخی انواع پراکسی ۱۰۷
SMTP Proxy ۱۰۸
HTTP Proxy(3-7-1 ..... ۱۱۰
FTP Proxy(3-7-2 ..... ۱۱۲
DNS Proxy(3-7-3 ..... ۱۱۴
۴-۷-۳) نتیجه گیری ۱۱۵

مقدمه

چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه‌ها مشخص می‌گردد. اگر امنیت شبکه برقرار نگردد، مزیتهای فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی هستند. همچنین دستکاری اطلاعات- به عنوان زیربنای فکری ملت‌ها توسط گروههای سازماندهی شده بین‌المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود.

برای کشور ما که بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکتهای خارجی تهیه می‌شود، بیم نفوذ از طریق راههای مخفی وجود دارد. در آینده که بانکها و بسیاری از نهادها و دستگاههای دیگر از طریق شبکهٔ به فعالیت می‌پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه بصورت مسئله‌ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایتهای ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟ نکته جالب اینکه بزرگترین شرکت تولید نرم‌افزارهای امنیت شبکه، شرکت چک پوینت است که شعبهٔ اصلی آن در اسرائیل می‌باشد. مسأله امنیت شبکهٔ برای کشورها، مسأله‌ای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژیها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، پس می‌بایست

محققین کشـــور این مهم را بـدســـت بگیرنـد و در آن فعـالیـت نمـاینـد. امروزه اینترنت آنقدر قابل دســترس شـــده که هرکس بدون توجه به محل زندگی، ملیت، شـغل و زمان میتواند به آن راه یابد و از آن بهره ببرد. همین سـهولت دسـترسـی آن را در معرض خطراتی چون گم شـدن، ربوده شـدن، مخدوش شـدن یا سـوءاسـتفاده از اطلاعات موجود در آن قرار می‌دهد. اگر اطلاعات روی کاغذ چاپ شـــده بود و در قفســـه‌ای از اتاقهای محفوظ اداره مربوطه نگهداری می‌شد، برای دسـترسـی به آنها افراد غیرمجاز می‌بایسـت از حصارهای مختلف عبور می‌کردند، اما اکنون چند اشاره به کلیدهای رایانه‌ای برای این منظور کافی است.