

فهرست

صفحه

هفت

عنوان

پیشگفتار

فصل اول – مقدمه

۱

۱-۱- سیاست امنیتی

۱

۲

۱-۱-۱- مدل‌های عمومی اعتماد

۳

۱-۱-۲- افراد مرتبط با سیاست امنیتی

۳

۱-۱-۳- طراحی سیاست امنیتی

۴

۱-۱-۴- نیازمندیهای اولیه یک سیاست

۵

۱-۱-۵- ساختار سیاست امنیتی شبکه

۵

۱-۱-۶- مثال ۱: سیاست استفاده مقبول از تجهیزات کامپیوتری

۸

۱-۱-۷- مثال ۲: سیاست امنیتی مسیر یاب

۹

۱-۲- حملات شبکه‌ای

۹

۱-۲-۱- از کار انداختن سرویس

۱۱	Spoofing - ۱-۲-۲
۱۱	Buffer Overflow - ۱-۲-۳
۱۲	Sniffing - ۱-۲-۵
۱۲	Brute force cracking - ۱-۲-۶
۱۲	Port Scanning - ۱-۲-۷
۱۳	Back Orifice - ۱-۲-۴
۱۴	۱-۳- شبکه‌های بی‌سیم
۱۴	۱-۳-۱- مقدمه
۱۴	۱-۳-۲- انواع شبکه‌های بی‌سیم
۱۶	۱-۳-۳- استانداردهای بی‌سیم
۱۷	۱-۳-۴- امنیت، مخاطرات امنیتی و تهدیدهای تکنولوژی بی‌سیم

فصل دوم - امنیت مسیریاب

۲۱	۲-۱- هدف مسیریاب
۲۲	۲-۲- روش کار و معماری
۲۳	۲-۲-۱- انواع مسیریاب در شبکه
۲۵	۲-۲-۲- مدیریت مسیریاب
۲۶	۲-۳-۱- مکانیزم دسترسی به مسیریاب برای مدیریت آن
۲۶	۲-۳-۲- به‌روز نگه داشتن مسیریاب
۲۸	۲-۳-۳- گزارش‌گیری
۲۸	۲-۴- سیاست امنیتی برای مسیریاب
۲۸	۲-۴-۱- لایه‌های امنیتی مسیریاب
۲۹	۲-۴-۲- نکات سیاست امنیتی هر لایه
۳۰	۲-۵- امنیت دسترسی به مسیریاب
۳۰	۲-۵-۱- دسترسی فیزیکی

۳۱	۲-۵-۲- نحوه پیکربندی مسیریاب Cisco و اجرای دستورات
۳۲	۲-۵-۳- فهرست دسترسی
۳۷	۲-۵-۴- مدیریت رمز عبور
۳۹	۲-۵-۵- کنترل دسترسی به خطوط کنترل
۴۲	۲-۶- سرویس‌ها و امنیت آنها
۴۳	۲-۶-۱- CDP
۴۳	۲-۶-۲- سرویس HTTP و پیکربندی با استفاده از آن
۴۴	۲-۶-۳- SNMP
۴۵	۲-۶-۴- BOOTP Server
۴۵	۲-۶-۵- راه‌اندازی از روی شبکه
۴۵	۲-۶-۶- NTP
۴۶	۲-۶-۷- جلوگیری از IP‌های غیر معتبری مبتنی بر FC1918
۴۸	۲-۶-۸- سرویس‌دهنده‌های TCP و UDP
۴۸	۲-۶-۹- سرویس Finger
۴۸	۲-۶-۱۰- IP Unreachable
۵۰	۲-۶-۱۱- ICMP Redirect Messages
۵۰	۲-۶-۱۲- Directed Broadcasts
۵۱	۲-۶-۱۳- Proxy ARP
۵۲	۲-۶-۱۴- IP Source Routing
۵۴	۲-۶-۱۵- TCP Intercept
۵۴	۲-۷- امنیت مسیریابی و پروتکل‌های مسیریابی
۵۴	۲-۷-۱- پروتکل و روش‌های مسیریابی
۵۷	۲-۷-۲- استفاده از مسیریابی سیاه چال
۵۷	۲-۷-۳- Unicast Reverse-Path Forwarding Verification
۵۸	۲-۷-۴- CAR

۵۹	۲-۸- سرویس‌های پیشرفته کنترل دسترسی
۵۹	۲-۸-۱- احراز هویت
۵۳	۲-۸-۲- واگذاری اختیار
۶۲	۲-۸-۳- حسابداری
۶۳	۲-۹- آزمایش امنیت مسیرباب
۶۳	۲-۹-۱- آزمایش کارکرد صحیح
۶۴	۲-۹-۲- ابزار RAT
۶۵	۲-۹-۳- Solarwinds
۶۵	۲-۱۰- آزمایشگاه امنیت مسیرباب
۶۵	۲-۱۰-۱- مثال اول
۷۱	۲-۱۰-۲- مثال دوم

فصل سوم – دیوار آتش

۸۷	۳-۱- انواع دیوار آتش
۸۷	۳-۱-۱- فیلتر بسته
۹۳	۳-۱-۲- دیوار آتش سطح مدار
۹۵	۳-۱-۳- دیوار آتش سطح کاربرد
۹۷	۳-۱-۴- Stateful Inspection دیوار آتش
۱۰۰	۳-۲- معماری دیوار آتش
۱۰۰	۳-۲-۱- Screening Router معماری
۱۰۱	۳-۲-۲- Dual-Homed Host معماری
۱۰۲	۳-۲-۳- Screened Host معماری
۱۰۳	۳-۲-۴- Screened Subnet معماری
۱۰۴	۳-۳- ویژگی دیگر دیوارهای آتش
۱۰۴	۳-۳-۱- شناسایی هویت و بررسی اختیارات

۱۰۴	۳-۳-۲ NAT (Network Address Translation)
۱۰۹	۳-۳-۳ تعدیل بار سرویس دهنده‌ها
۱۱۰	۳-۳-۴ کنترل و نظارت بر ترافیک شبکه
۱۱۱	۳-۳-۵ تشخیص ویروس
۱۱۲	۳-۳-۶ قابلیت استفاده
۱۱۳	۳-۳-۷ VPN
۱۱۶	۳-۴ بررسی محصولات دیوار آتش
۱۱۷	۳-۴-۱ Checkpoint دیوار آتش
۱۳۱	۳-۴-۲ Cisco Secure PIX Firewall
۱۳۴	۳-۴-۳ دیوار آتش لینوکس
۱۳۸	۳-۴-۴ SonicWALL دیوار آتش
۱۴۱	۳-۴-۵ Astaro Security Linux
۱۴۱	۳-۴-۶ FirewallAnalyzer
۱۴۳	۳-۵ یک Checklist عمومی برای دیوارهای آتش

فصل چهارم – سیستم شناسایی نفوذ و نفوذگر

۱۴۹	۴-۱ پیش زمینه امنیت کامپیوتر و شبکه
۱۵۰	۴-۱-۱ امنیت کامپیوتر و شبکه و جایگاه سیستم تشخیص نفوذ
۱۵۰	۴-۱-۲ تهدیدها و خطرهای
۱۵۱	۴-۱-۳ آسیب پذیری
۱۵۲	۴-۱-۴ حملات
۱۵۲	۴-۲ پیش زمینه‌ای در مورد تشخیص نفوذ
۱۵۳	۴-۲-۱ IDS واژگان اساسی
۱۵۴	۴-۲-۲ یک مدل برای IDS
۱۵۶	۴-۲-۳ طبقه‌بندی IDSها

۱۶۰	۴-۳- سیستم‌های تشخیص نفوذ امروزی
۱۶۰	Audit Source Location - ۴-۳-۱
۱۶۷	Detection Methods - ۴-۳-۲
۱۷۱	Behavior on Detection - ۴-۳-۳
۱۷۴	۴-۴- معرفی برخی محصولات IDS
۱۷۵	Symantec ManHunt - ۴-۴-۱
۱۸۰	McAfee IntruShield - ۴-۴-۲
۱۸۵	Snort - ۴-۴-۳
۱۸۹	Honeypot - ۴-۵
۱۹۰	Honeypot انواع - ۴-۵-۱
۱۹۱	Honeyd - ۴-۵-۲
۱۹۲	Honeynets - ۴-۵-۳
۱۹۳	۴-۵-۴- مزایای Honeypot در محافظت از شبکه
۱۹۴	Specter - ۴-۵-۵
۱۹۶	Symantec Decoy Server - ۴-۵-۶

منابع

۱۹۷	۵-۱- منابع امنیت مسیریاب
۱۹۷	۵-۲- منابع امنیت دیوار آتش
۱۹۸	۵-۳- منابع IDS
۲۰۰	

پیشگفتار

با توسعه فناوری اطلاعات و پیاده‌سازی سیستم‌های اطلاعاتی در سراسر دنیا، تأمین امنیت آن به‌عنوان دغدغه‌ای مهم در مجامع علمی، دولتی و خصوصی مطرح شده است. از آنجا که شبکه به‌عنوان بستری اساسی برای انتقال اطلاعات به حالتی فراگیر نزدیک می‌شود، حفظ امنیت در انتقال اطلاعات و عدم نفوذپذیری از طریق شبکه، به‌عنوان حالت خاصی از امنیت اطلاعات، نیاز به بررسی بسیار دارد و البته کارهای ارزشمندی هم در این زمینه انجام گرفته و محصولات مختلفی ارائه شده است. آشنایی مدیران سازمان‌ها، مراکز دولتی، نظامی، تجاری و هر جایی که امنیت اطلاعات برای آنها مطرح است، با مبانی امنیت شبکه، مخاطرات امنیتی، راه‌حل‌ها و نحوه سیاست‌گذاری صحیح برای این موضوع، امری اجتناب‌ناپذیر محسوب می‌شود. اگر همچنین مدیران شبکه، به مسایل امنیتی شبکه خود آگاه نباشند، ممکن است به صورت‌های مختلفی مورد حمله افراد نفوذگر قرار گیرند.

این کتاب سعی دارد با ارائه مفاهیم بنیادی امنیت شبکه، مدیران سطح بالا را با مسایل مطرح در امنیت شبکه آشنا سازد تا بدین‌وسیله قادر به وضع سیاست‌های خاص برای حفظ امنیت اطلاعات و به‌طور خاص امنیت شبکه، شناسایی افراد خاطی و برخورد با آنها باشند. همچنین، در سطحی پیشرفته‌تر و البته نه صرفاً تکنیکی،

مسئولین شبکه‌های شرکت‌ها و سازمان‌ها را با امنیت شبکه و تجهیزات آن، مخاطرات امنیتی، راه‌حل‌ها و سایر مسائل مربوط به امنیت یک شبکه در مقابله با نفوذگران داخلی و خارجی آشنا می‌گرداند. گفتنی است که مطالعه کامل این کتاب نیاز به آشنایی با مفاهیم شبکه و دانستن اطلاعات پایه‌ای در زمینه امنیت شبکه دارد. در این کتاب، منظور از “شبکه داخلی”، شبکه (محلی) مورد اعتماد ماست که در مقابل عبارت “شبکه خارجی” که قابل اعتماد نیست به کار می‌رود.

فصل اول این کتاب، به معرفی مسایل عمومی امنیت شبکه، شامل وضع سیاست امنیتی، حملات شبکه‌ای و آشنایی مختصری با شبکه‌های بی‌سیم و امنیت آن (از آن جهت که جامعیت این مستند، حفظ شود) می‌پردازد. در فصل دوم، معرفی مسیر یاب، مخاطرات امنیتی و مسائل مربوط به بالا بردن سطح امنیتی مسیر یاب و با استفاده از آن، بهبود امنیت شبکه داخلی خود (با تأکید بر مسیر یاب‌های سیسکو) در رأس مطالب قرار دارد. فصل سوم، بحثی کلی و جامع در مورد دروازه‌های امنیتی و دیوار آتش، انواع آن، معماری‌ها، سرویس‌های پیش‌رفته امنیتی ارائه شده در دیوار آتش و معرفی چند محصول را در این زمینه شامل می‌شود. در نهایت در فصل چهارم، سیستم‌های شناسایی نفوذ و نفوذگر موسوم به IDS¹ را مورد بحث قرار خواهیم داد که معرفی نفوذ و نفوذگر، سیستم‌های شناسایی نفوذ، انواع آن، سیستم‌های فریب و به دام انداختن نفوذگر و معرفی چندین محصول موجود در بازار امروز دنیا در این زمینه، رئوس مطالب را تشکیل می‌دهد.

¹. Intrusion Detection System