

۹۸۸۹۴۷
۹۴۱ ۱۱/۹

به نام آن که جان را فکرت آموخت

امنیت و نفوذپذیری در شبکه‌های کامپیوتری

مرحان

سید مهدی عمادی

شهره لیثی بهرمایی



سرشناسه	عنوان و نام پدیدآور
شناسه نشر	موضوع
موضوعات ظاهری	موضوع
شابک	وضعیت فهرست‌نویسی
موضوع	موضوع
موضوع	موضوع
شناسه افزوده	شناسه افزوده
شناسه افزوده	رده بندی کنگره
رده بندی کنگره	رده بندی دیویی
رده بندی دیویی	شماره کتابشناسی ملی
شماره کتابشناسی ملی	

امنیت و نفوذپذیری در شبکه‌های کامپیوتری



مولفان	سید مهدی - عمادی استرآبادی - شهره لیثی بهرمانی
مدیر تولید	سید مهدی - عمادی استرآبادی - شهره لیثی بهرمانی
حروفچینی و صفحه‌آرایی	ابن فضل لیثی بهرمانی
نوبت چاپ	اول ۳۹۴
تیراژ	۵۰۰
قیمت	۲۰۰۰۰ ریال
شابک	۹۷۸-۶۰۰-۱۶۰-۲۲۲-۱

فروشگاه : تهران - خیابان انقلاب - بین خیابان فروردین و منیری جاوید - روبروی دبیرخانه شهید آیت‌الله آران - کتابفروشی فلاح
تلفن: ۶۶۴۱۰۳۵۴
دفتر انتشارات : تهران - خیابان انقلاب - خیابان اردیبهشت - بین باقی‌نژاد و جمهوری - ساختمان ۱۰
تلفن: ۶۶۴۸۲۲۲۱ - ۶۶۴۸۱۰۹۶ - ۶۶۴۶۵۸۳۱

ایمیل و وب‌سایت: www.fadakbook.ir - info@fadakbook.ir

کلیه حقوق و حق چاپ متن و عنوان کتاب که به ثبت رسیده است؛ مطابق با قانون حقوق مولفان و مصنفان مصوب ۱۳۴۸ محفوظ و متعلق به انتشارات فدک ایستایس می‌باشد. هر گونه برداشت، تکثیر، کپی‌برداری به هر شکل (چاپ، فتوکپی، انتشار الکترونیکی) بدون اجازه کتبی از انتشارات فدک ایستایس ممنوع بوده و متخلفین تحت پیگرد قانونی قرار خواهند گرفت.

معاونت حقوقی
انتشارات فدک ایستایس

امروزه توجه بیشتر سازمان‌ها و بنگاه‌های اقتصادی معطوف به شبکه محلی و رایانه‌های شخصی متصل به آن می‌باشد. گرچه شبکه‌های ارتباطی می‌توانند اشکال مختلفی به خود بگیرند و تعداد و تنوع آنها هم روز به روز بیشتر می‌شود، اما استفاده از این شبکه‌ها بدون توجه به مقوله امنیت ارتباطی، سلب اعتماد همگانی از فناوری اطلاعات را در بر خواهد داشت که خسارت ناشی از این بی‌اعتمادی برای سازمان‌ها بسیار قابل توجه است.

در این راستا این کتاب مقدمه‌ای بر امنیت شبکه داخلی است که مخاطب آن به‌طور عمده مدیران و اجرایی سازمان‌ها می‌باشند. هدف آن بوده است که مفاهیم اساسی امنیت در این حوزه و روش‌های متداول نفوذ به شبکه‌های رایانه‌ای معرفی شوند و بنابراین از توسعه و تفصیل مطالب پرهیز گردیده است. با این وجود برخی از بخش‌های کتاب برای کارشناسان فنی و راهبران شبکه‌های داخلی مفید خواهد بود.

شاید وقتی در ارتباطات رایانه‌ای بوجود آمد و شبکه‌های کامپیوتری پدید آمد هیچکس تصور نمی‌کرد که امنیت به مهم‌ترین بخش آن تبدیل خواهد شد، به‌طوری که امروزه امنیت شبکه جزء مهم‌ترین و کاربردی‌ترین تخصص‌ها در بخش فناوری اطلاعات گردیده است. به همین دلیل مطالعه و آموزش در زمینه امنیت شامل مباحث بسیار گسترده‌ای است و فراتر از سطح این مجموعه آموزشی است. آنچه که در این کتاب ارائه شده، یک سری مباحث اصلی امنیت شبکه است و بیشتر برای آشنایی شما با مسئله امنیت و شیوه‌های ایجاد امنیت و شناخت تهدیدهای امنیتی رایج است. شما می‌توانید این تخصص را با گرفتن مدارکی همچون CEH، CISSP، Security+ کسب کنید.

نکته دیگری که می‌خواهیم به آن اشاره کنیم این است که زمانی که شما قدم به عرصه امنیت شبکه می‌گذارید هیچ پایانی برای کسب دانش شما وجود نخواهد داشت. درست زمانی که فکر می‌کنید همه دانش لازم برای امنیت شبکه را بدست آورده‌اید، به سبب ساریوها تغییر می‌کند و یکسری روش‌های جدید نفوذ و حمله کشف می‌شود. برخی هکرها با صرفه‌گیری باگ‌های جدیدی را کشف می‌کنند و راه نفوذ دیگری را پیدا می‌کنند. پس به یاد داشته باشید که امنیت شبکه مسئله بسیار مهمی است و دانش آن روز به روز دستخوش تغییر و پیشرفت می‌شود.

سید مهدی عمادی استرآبادی

شهره لیثی بهرمانی

پاییز ۱۳۹۴

پیشگفتار

این کتاب به منظور تدریس مبحث تئوری نابجایی طی یک ترم تحصیلی در سطح پیشرفته نگارش یافته و باقیه استفاده به عنوان مرجع اصلی در دانشگاه‌هایی نظیر Northwestern را دارا می‌باشد. مطالعه کاربرد نابجایی‌ها به منزله پیش‌زمینه‌آشنایی با مباحث تئوری‌های کارسختی، خزش، اصطکاک داخلی و... جهت توجیه پدیده‌های حساس به ساختار کریستالی قلمداد می‌شود. تدریس کامل مباحث تئوری نابجایی پایه و کاربردی طی یک ترم تحصیلی دشوار بوده و طی این زمان تنها معرفی سطحی هر دو مبحث امکان‌پذیر است. به همین دلیل در این کتاب تنها مبانی تئوری بررسی می‌گردد. این کار باعث می‌شود تا جزییات مبانی تئوری نابجایی به طور کامل بررسی گردیده و دانشجویان مهارت لازم در زمینه را به دست آورند.

از آن‌جا که دانشجویان فنی و مهندسی اغلب مباحث ریاضی، تحلیل بردار و ترمودینامیک مقدماتی را گذرانده‌اند، در کل کتاب فرض بر این است که دانشجو با این مطالب آشنایی کافی دارد. برای مطالعه کتاب آگاهی در دیگر زمینه‌های تخصصی ضروری نیست. به طور نمونه پیش از تعیین حوزه تنش و کرنش نابجایی‌ها، تئوری الاستیسیته مورد بررسی قرار گرفته زیرا دانشجویان آشنایی کمی با این مبحث دارند.

در انتهای هر فصل مسائل متعددی گنجانده شده و به دانشجویان توصیه می‌گردد که تا حد امکان بر روی آن‌ها کار کنند. درک کامل تئوری نابجایی تنها از طریق تکرار حل مسائل حاصل می‌شود. در انتها صمیمانه از زحمات پروفیسور W. J. McG. Tegart برای راهنمایی‌ها و تصحیح کتاب قدردانی می‌گردد.

سید مهدی عمادی استرآبادی

شهره لیثی بهرمانی

باییز ۱۳۹۴

فهرست مطالب

فصل ۱ مقدمات شبکه ۱

- ۱.۱ مقدمه ۲
- ۱.۲ مراحل ایجاد امنیت در شبکه ۲
- ۳.۱ واژگان فنی ۶
- ۴.۱ انواع مختلف تکنولوژی‌های هک ۷
- ۵.۱ مراحل هک ۸
- ۶.۱ مراحل هک ۹
- ۷.۱ انواع هکرها ۱۰
- ۸.۱ cracker کیستند؟ ۱۱
- ۹.۱ انواع حملات هکرها ۱۲
- ۱۰.۱ موارد مورد نیاز هکر ۱۳
- ۱۱.۱ نکاتی لازم در مورد پروکل TCP ۱۵
- ۱۲.۱ آشنایی با تست نفوذپذیری ۱۶
- ۱.۱۲.۱ گام‌های ابتدایی برای تست امنیت ۱۶
- ۲.۱۲.۱ طبقه‌بندی و اهداف تست نفوذپذیری ۱۷
- ۳.۱۲.۱ اهداف تست نفوذپذیری ۱۸
- ۴.۱۲.۱ محدودیت‌های تست نفوذپذیری ۱۸
- ۵.۱۲.۱ طبقه‌بندی تست نفوذپذیری ۱۹
- ۱۳.۱ نیازمندی‌های متداول ۲۰
- ۱.۱۳.۱ نیازمندی‌های سازمانی ۲۰
- ۲.۱۳.۱ نیازمندی‌های پرسنلی ۲۱
- ۳.۱۳.۱ نیازمندی‌های تکنیکی ۲۱
- ۱۴.۱ مراحل تست نفوذپذیری ۲۱
- ۱۵.۱ راه‌های نفوذ ۲۲
- ۱.۱۵.۱ جعل اطلاعات ۲۲
- ۲.۱۵.۱ استراق سمع داده‌ها ۲۵

۲۶	Ping of death	حمله	۳.۱۵.۱
۲۶	Jolt 2	حمله نوع	۴.۱۵.۱
۲۶	Smurf	حمله نوع	۵.۱۵.۱
۲۹		اهداف حمله کننده ها	۱۶.۱
۳۰	CIA	مثلت	۱۷.۱
۳۱		تحقیق آسیب پذیری چیست؟	۱۸.۱
۳۲		روش های اجرای هک قانونمند	۱۹.۱
۳۲		برنامه ارزیابی امنیتی	۲۰.۱
۳۲		انواع حملات قانونمند	۲۱.۱
۳۳		انواع تست	۲۲.۱
۳۵		گزارش هک قانونمند	۲۳.۱

فصل ۲ جمع آور، اطلاعات و مهندسی اجتماعی ۳۵

۳۸		مقدمه	۱.۲
۳۹	Footprinting		۲.۲
۳۹		متدلوژی های جمع رری اطلاعات	۳.۲
۴۰	DNS Enumeration		۴.۲
۴۱	DNSstuf و Nslookup		۵.۲
۴۱	ARIN Lookup و Whois	مفهوم	۶.۲
۴۳	Whois	تحلیل خروجی	۷.۲
۴۵		پیدا کردن بازه آدرس های شبکه	۸.۲
۴۵	DNS	شناسایی انواع مختلف رکوردهای	۹.۲
۴۵	footprinting در traceroute	نحوه کار	۱۰.۲
۴۶	Email Tracking	استفاده از	۱۱.۲
۴۷	Web Spider	نحوه کار	۱۲.۲
۴۷	Footprinting	مراحل انجام	۱۳.۲
۴۸		مهندسی اجتماعی	۱۴.۲
۴۸		انواع رایج حملات	۱۵.۲
۴۹		مهندسی اجتماعی مبتنی بر انسان	۱۶.۲
۵۰		مهندسی اجتماعی مبتنی بر کامپیوتر	۱۷.۲
۵۰		حملات داخلی	۱.۱۷.۲
۵۰	Phishing	حملات	۲.۱۷.۲
۵۱		پیشگیری از مهندسی اجتماعی	۱۸.۲

فصل ۳ اسکن و Enumeration ۵۳

۱.۳	مقدمه ۵۴
۲.۳	اسکن ۵۴
۳.۳	متدلوژی اسکن ۵۵
۴.۳	تکنیک‌های ping sweep ۵۶
۵.۳	تشخیص Ping Sweep ها ۵۶
۶.۳	اسکن پورت‌ها و شناسایی سرویس‌ها ۵۶
۷.۳	مقابله با اسکن پورت ۵۷
۸.۳	سوئیچ‌های دستور Nmap ۵۷
۱۸.۳	اسکن‌های SYN, Stealth, XMAS, NULL, IDLE و FIN ۶۰
۹.۳	انواع flag‌های ارتباط TCP ۶۱
۱۰.۳	Net tools suite pack ۶۲
۲۰.۳	Floris Scan ۶۲
۱۰.۳	تکنیک‌های War-Dialing ۶۴
۱۱.۳	تکنیک‌های Banner Grabbing و شناسایی سیستم‌عامل ۶۴
۱۲.۳	رسم دیاگرام شبکه‌های دستگاه‌های آسیب‌پذیر ۶۶
۱۳.۳	چگونه از سرورهای پروکسی برای انجام حمله استفاده می‌شوند؟ ۶۶
۱۴.۳	ناشناس‌کننده‌ها چگونه کار می‌کنند؟ ۶۷
۱۵.۳	HTTP tunneling ۶۸
۱۱۵.۳	تکنیک‌های HTTP Tunneling ۶۸
۲۱۵.۳	ابزار Httpunnel برای ویندوز ۶۸
۱۶.۳	تکنیک‌های IP Spoofing ۶۹
۱۱۶.۳	Enumeration ۷۰
۲۱۶.۳	Null Session ۷۲
۳۱۶.۳	انتقال DNS Zone در ویندوز ۲۰۰۰ ۷۳

فصل ۴ هک سیستم ۷۵

۱.۴	مقدمه ۷۶
۲.۴	تکنیک‌های شکستن پسورد ۷۶
۱.۲.۴	LanManager Hash ۷۷
۲.۲.۴	شکستن پسوردهای ویندوز ۲۰۰۰ ۷۸
۳.۲.۴	هدایت SMB Logon به حمله کننده ۷۹
۴.۲.۴	حملات SMB Relay MITM و مقابله با آن ۸۰

۳.۴	مقابله با شکستن پسورد ۸۱
۱.۳.۴	بازه زمانی تغییر پسورد ۸۲
۲.۳.۴	بررسی Event Viewer Log ها ۸۲
۴.۴	انواع پسورد ۸۳
۵.۴	حملات Passive Online ۸۴
۶.۴	حملات Active Online ۸۴
۷.۴	حدس پسورد به صورت اتوماتیک ۸۵
۸.۴	مقابله با حدس پسورد ۸۶
۹.۴	حملات آفلاین ۸۶
۱۰.۴	Pre-Computed Hashes ۸۷
۱۱.۴	حملات Nonelectronic ۸۷
۱۲.۴	تکنیک‌های keylogger ها و spyware ۸۸
۱۳.۴	دسترسی‌های ضروری ۸۹
۱۴.۴	اجرای برنامه ۹۰
۱۵.۴	Buffer Overflows ۹۱
۱۶.۴	rootkit ها ۹۱
۱.۱۶.۴	نصب rootkit ها بر روی کامپیوترهای ویندوز ۲۰۰۰ و XP ۹۲
۲.۱۶.۴	مقابله با rootkit ها ۹۲
۱۷.۴	مخفی کردن فایل‌ها ۹۳
۱.۱۷.۴	NTFS File Streaming ۹۳
۲.۱۷.۴	مقابله با NTFS Stream ۹۴
۳.۱۷.۴	تکنولوژی‌های Steganography ۹۴
۴.۱۷.۴	ابزارهای مقابله ۹۶
۱۸.۴	پاک کردن ردپاها و مدارک ۹۶
۱۹.۴	غیر فعال کردن Auditing ۹۶
۲۰.۴	پاک کردن Event Log ۹۷

فصل ۵ بدافزارها ۹۹

۱.۵	مقدمه ۱۰۰
۲.۵	بدافزار چیست؟ ۱۰۰
۳.۵	نگاهی گذرا به سرگذشت بدافزارها ۱۰۱
۴.۵	انواع بدافزار ۱۰۲
۱.۴.۵	کرم (Worm) ۱۰۲
۲.۴.۵	ویروس (Virus) ۱۰۳

۳.۴.۵	اسب تروا (Trojan Horse) ۱۱۰
۴.۴.۵	در پشتی (Backdoor/Trapdoor) ۱۲۴
۵.۴.۵	روتکیت (Rootkit) ۱۲۵
۶.۴.۵	نرم افزار جاسوسی (Spyware) ۱۳۰
۷.۴.۵	ابزار نفوذ (Hack Tool) ۱۳۲
۸.۴.۵	تبلیغات ناخواسته (Adware) ۱۳۲
۹.۴.۵	ترساندن Scareware ۱۳۳
۱۰.۴.۵	Logic Bomb یا بمب منطقی ۱۳۴
۵.۵	روش های مقابله با بدافزارها ۱۳۵
۶.۵	حذف بدافزارها ۱۳۸

فصل ۶ Snifferها ۱۴۱

۱.۶	مقدمه ۱۴۱
۲.۶	پرو کل ها - مستعد برای استراق سمع ۱۴۲
۳.۶	اسنیفر پیست ۱۴۴
۴.۶	استراق سمع اکتیو و پسیو ۱۴۴
۱.۴.۶	استراق سمع اکتیو ۱۴۵
۲.۴.۶	استراق سمع پسیو ۱۴۵
۵.۶	رمز گذاری ۱۴۶
۱.۵.۶	رمز گذاری در سطح ارتباط ۱۴۶
۲.۵.۶	رمز گذاری در دو انتها ۱۴۶
۳.۵.۶	رمز گذاری در سطح برنامه ۱۴۷
۶.۶	ARP Poisoning ۱۴۸
۷.۶	MAC Duplicating ۱۴۹
۸.۶	MAC Flooding ۱۵۰
۹.۶	DNS Poisoning ۱۵۲
۱۰.۶	Intranet DNS Spoofing ۱۵۲
۱۱.۶	Proxy Server DNS Poisoning ۱۵۴
۱۲.۶	NS Cache Poisoning ۱۵۴
۱۳.۶	مقابله با استراق سمع ۱۵۶
۱۴.۶	شبکه کوچک ۱۵۷

۱.۷	مقدمه ۱۶۰
۲.۷	Denial of Service ۱۶۰
۳.۷	انواع حملات DoS ۱۶۰
۴.۷	نحوه کار حملات DDoS ۱۶۲
۵.۷	دسته‌بندی حملات DDoS ۱۶۵
۶.۷	نحوه کار BOTها و BOTNETها ۱۶۶
۷.۷	حمله smurf چیست؟ ۱۶۷
۸.۷	SYN flooding چیست؟ ۱۶۸
۹.۷	مقابله با DoS و DDoS ۱۶۸
۱۰.۷	Session Hijacking ۱۷۰
۱۱.۷	Hijacking و Spoofing ۱۷۰
۱۲.۷	انواع session hijacking ۱۷۱
۱.۱۲.۷	Active Session Hijacking ۱۷۱
۲.۱۲.۷	Passive Session Hijacking ۱۷۲
۱۳.۷	مفاهیم TCP: دست تکن سه مرحله‌ای ۱۷۲
۱۴.۷	پیشگویی sequence ۱۷۳
۱۵.۷	چه مراحل در session hijacking انجام می‌شوند؟ ۱۷۴
۱۶.۷	سطوح session hijacking ۱۷۵
۱۷.۷	TCP/IP Hijacking ۱۷۵
۱۸.۷	RST Hijacking ۱۷۶
۱۹.۷	Blind Hijacking ۱۷۶
۲۰.۷	خطرات session hijacking ۱۷۷
۲۱.۷	چگونگی پیشگیری از session hijacking ۱۷۷

هک وب سرورها، آسیب‌پذیری برنامه‌های تحت وب و تکنیک‌های

شکستن پسوردهای مبتنی بر وب ۱۷۹

۱.۸	مقدمه ۱۸۰
۲.۸	هک وب سرورها ۱۸۰
۳.۸	انواع آسیب‌پذیری‌های وب سرور ۱۸۰
۴.۸	حملات به وب سرورها ۱۸۱
۵.۸	IIS Unicode Exploit ۱۸۱
۶.۸	تکنیک‌های مدیریت patchها ۱۸۵

اسکنرهای آسیب‌پذیری	۱۸۶	۷.۸
روش‌های امن‌سازی وب سرور	۱۸۶	۸.۸
چک لیست محافظت از وب سرور	۱۸۷	۹.۸
آسیب‌پذیری‌های برنامه‌های تحت وب	۱۸۸	۱۰.۸
نحوه کار برنامه‌های وب	۱۸۸	۱۱.۸
هدف از هک برنامه‌های تحت وب	۱۸۹	۱۲.۸
آناتومی حمله	۱۸۹	۱۳.۸
تهدیدات برنامه‌های وب	۱۹۰	۱۴.۸
Google Hacking	۱۹۴	۱۵.۸
تکنیک‌های شکستن پسوردهای مبتنی بر وب	۱۹۴	۱۶.۸
احراز هویت	۱۹۵	۱۷.۸
انواع احراز هویت	۱۹۵	۱۸.۸
شناسایی بر مبنای حالت هندسی دست	۱۹۶	۱.۱۸.۸
اسکن شبکه	۱۹۷	۲.۱۸.۸
تشخیص بهره	۱۹۸	۳.۱۸.۸
پسورد	۱۹۸	۴.۱۸.۸

۲۰.۳ Buffer Overflow و SQL Injection

فصل ۹

مقدمه	۲۰۴	۱.۹
SQL Injection چیست؟	۲۰۴	۲.۹
مراحل انجام SQL injection	۲۰۵	۳.۹
آسیب‌پذیری‌های SQL Server	۲۰۶	۴.۹
Blind SQL Injection	۲۰۸	۵.۹
مقابله با SQL Injection	۲۰۸	۶.۹
چرا برنامه‌ها آسیب‌پذیرند؟	۲۰۹	۷.۹
انواع Buffer Overflow و روش‌های شناسایی	۲۱۰	۸.۹
پشته (Stack)	۲۱۰	۹.۹
Heap	۲۱۱	۱۰.۹
سرریزی بافر مبتنی بر پشته (stack-based buffer overflow)	۲۱۲	۱۱.۹
انواع Buffer Overflow و روش‌های شناسایی	۲۱۲	۱.۱۱.۹
سرریزی بافر مبتنی بر heap (heap-based overflow)	۲۱۳	۲.۱۱.۹
روش شناسایی buffer overflow در برنامه	۲۱۴	۳.۱۱.۹
تکنیک‌های تغییر buffer overflow	۲۱۵	۴.۱۱.۹
روش‌های جلوگیری از buffer overflow	۲۱۵	۵.۱۱.۹

فصل ۱۰ شبکه‌های وایرلس ۲۱۷

مقدمه	۲۱۸	۱.۱۰
استانداردهای وایرلس	۲۱۸	۲.۱۰
مفاهیم وایرلس	۲۱۸	۳.۱۰
مکانیزم‌های احراز هویت WEP و WPA و تکنیک‌های شکستن آن‌ها	۲۱۹	۴.۱۰
اصطلاحات هک شبکه وایرلس	۲۲۱	۵.۱۰
استراق سمع کننده‌های وایرلس و قرار دادن SSID ها و MAC spoofing	۲۲۳	۶.۱۰
تغییر دستی MAC Address در ویندوز XP	۲۲۳	۷.۱۰
Rogue Access Point (تقلبی)	۲۲۴	۸.۱۰
تکنیک‌های هک شبکه وایرلس	۲۲۵	۹.۱۰
مراحل هک شبکه‌های وایرلس	۲۲۵	۱۰.۱۰
روش‌هایی شناسایی شبکه‌های وایرلس	۲۲۷	۱۱.۱۰
روش‌های شناسایی شبکه‌های وایرلس	۲۲۷	۱۲.۱۰

فصل ۱۱ امنیت فیزیکی ۲۲۹

مقدمه	۲۳۰	۱.۱۱
رویدادهای نقض امنیت فیزیکی	۲۳۰	۲.۱۱
امنیت فیزیکی	۲۳۱	۳.۱۱
ضرورت امنیت فیزیکی چیست؟	۲۳۱	۱.۳.۱۱
چه کسی مسئول امنیت فیزیکی است؟	۲۳۲	۲.۳.۱۱
عواملی که امنیت فیزیکی را تحت تأثیر قرار می‌دهد	۲۳۳	۳.۳.۱۱
چک لیست امنیت فیزیکی	۲۳۳	۴.۳.۱۱
برخی از ابزارهای امنیت فیزیکی	۲۳۷	۵.۳.۱۱

فصل ۱۲ هک لینوکس ۲۴۱

سیستم‌عامل چیست؟	۲۴۲	۱.۱۲
مفهوم نرم‌افزارهای open source	۲۴۲	۲.۱۲
مفهوم مجوز GPL	۲۴۲	۳.۱۲
سیستم‌عامل لینوکس	۲۴۳	۴.۱۲
اساس لینوکس	۲۴۳	۵.۱۲
تعریف GNU	۲۴۳	۶.۱۲
Kernel چیست؟	۲۴۴	۷.۱۲
قابلیت‌های لینوکس	۲۴۴	۸.۱۲

۹.۱۲	سیستم پرونده‌ها در لینوکس	۲۴۵
۱۰.۱۲	دستورات پایه لینوکس	۲۴۶
۱.۱۰.۱۲	فایل‌ها و دایرکتوری‌ها	۲۴۶
۲.۱۰.۱۲	دایرکتوری‌های لینوکس	۲۴۷
۱۱.۱۲	نحوه کامپایل کرنل لینوکس	۲۴۷
۱۲.۱۲	دستورات کامپایل GCC	۲۴۹
۱۳.۱۲	نحوه نصب ماژول‌های کرنل لینوکس	۲۴۹
۱۴.۱۲	آسیب‌پذیری‌های لینوکس	۲۴۹
۱۵.۱۲	روش‌های امن‌سازی لینوکس	۲۵۱
۱۶.۱۲	فایروال در لینوکس (IPTable)	۲۵۲
۱۷.۱۲	ابزارهای لینوکس	۲۵۲

فصل ۱۳ گریز از IDS ها، honeypot ها و فایروال‌ها ۲۵۳

۱.۱۳	مقدمه	۲۵۴
۲.۱۳	انواع سیستم‌های تشخیص نفوذ و تکنیک‌های گریز	۲۵۴
۳.۱۳	گریز از IDS	۲۵۷
۴.۱۳	فایروال	۲۵۷
۵.۱۳	کارهایی که فایروال انجام می‌دهد	۲۵۸
۶.۱۳	انواع فایروال	۲۵۸
۷.۱۳	ابزارهای تست	۲۶۰
۸.۱۳	Honeypot	۲۶۱
۱.۸.۱۳	انواع مختلف honeypot	۲۶۱
۲.۸.۱۳	مزایای honeypot	۲۶۱
۳.۸.۱۳	محل قرارگیری honeypot در شبکه	۲۶۲
۴.۸.۱۳	ابزارها	۲۶۳
۵.۸.۱۳	Honeypot های تجاری	۲۶۳
۶.۸.۱۳	Honeypot های open source	۲۶۳
۷.۸.۱۳	Honeypot فیزیکی و مجازی	۲۶۴

فصل ۱۴ رمزنگاری ۲۶۵

۱.۱۴	مقدمه	۲۶۶
۲.۱۴	تکنیک‌های رمزنگاری و رمزگذاری	۲۶۶
۳.۱۴	نحوه تولید کلیدهای عمومی و خصوصی	۲۶۷

نگاهی به الگوریتم‌های RC4, RC5, Blowfish و MD5.SHA	۲۶۷	۴.۱۴
SSH	۲۶۸	۵.۱۴
ابزارها	۲۶۹	۶.۱۴

فصل ۱۵ روش‌های تست نفوذ ۲۷۱

مقدمه	۲۷۲	۱.۱۵
ارزیابی‌های امنیتی	۲۷۲	۲.۱۵
روش‌های تست نفوذ	۲۷۲	۳.۱۵
مراحل تست نفوذ	۲۷۳	۴.۱۵
چارچوب قانونی تست نفوذ	۲۷۶	۵.۱۵
انواع خودکار تست نفوذ	۲۷۶	۶.۱۵
موارد قابل ارائه در تست نفوذ	۲۷۷	۷.۱۵

فصل ۱۶ حذف پسورد ۲۷۹

استخراج و کرک رمزهای عبور	۲۸۰	۱.۱۶
حساب‌های کاربردی و کلمات عبور	۲۸۰	۲.۱۶
گروه‌های کاربری	۲۸۱	۳.۱۶
گروه‌های موجود در یک شبکه	۲۸۲	۴.۱۶
ورود به حساب کاربری Administrator	۲۸۳	۵.۱۶
هدف اصلی نفوذگر	۲۸۴	۶.۱۶
اطلاعات کلی	۲۸۴	۷.۱۶
روش مقابله	۲۸۴	۸.۱۶
استفاده از فرامین و ابزارهای خود ویندوز	۲۸۵	۹.۱۶
User Accounts (Control Userpasswords2)	۲۸۵	۱۰.۱۶
(Iusrmgr.msc) Local Users And Groups	۲۸۶	۱۱.۱۶
Net User Command	۲۸۶	۱۲.۱۶
روش مقابله در جلوگیری از استفاده از این فرامین و ابزارها	۲۸۸	۱۳.۱۶
ایجاد دیسکت حذف‌کننده‌ی پسورد	۲۸۸	۱۴.۱۶
پسورد گذاری کامل syskey و حساب‌های کاربری	۲۹۵	۱۵.۱۶
حذف Syskey و پسورد حساب Administrator	۲۹۶	۱۶.۱۶
روش کار	۲۹۶	۱۷.۱۶
روش مقابله	۲۹۶	۱۸.۱۶
حذف پسورد در Welcome Screen	۲۹۷	۱۹.۱۶

۱۵.۱۶ نحوه‌ی Reset کردن پسورد با استفاده از ابزارهای مختلف موجود در اینترنت ۳۰۳

۱.۱۵.۱۶ ابزار Active@ password Changer ۳۰۴

۲.۱۵.۱۶ نحوه‌ی عوض کردن و یا حذف کردن پسوردهای ویندوز با استفاده از Ubuntu live CD ۳۰۷

۳.۱۵.۱۶ حذف یا تغییر پسوردهای ویندوز با استفاده از برنامه Chntpw در Ubuntu ۳۱۲

۴.۱۵.۱۶ با استفاده از ابزار NTPswd ۳۱۷

۵.۱۵.۱۶ PC Login Now ۳۲۵

۶.۱۵.۱۶ Windows Login Password Professional ۳۳۰

۱۶.۱۶ نحوه حذف پسورد برنامه‌ها ۳۳۴

۱.۱۶.۱۶ نحوه حذف پسورد برنامه Access Administrator ۳۳۴

۱.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Click And Lock1 ۳۳۴

۱.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Program Protector ۳۳۴

۴.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Ashampoo Magical Security ۳۳۴

۵.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Anfibia Deskman ۳۳۴

۶.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Access ۳۳۵

۷.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Private Encryption ۳۳۵

۸.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه XP Smoker ۳۳۵

۹.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Lock My Pc ۳۳۵

۱۰.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه PC Security Toolbar ۳۳۵

۱۱.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه st Security Agent1 ۳۳۶

۱۲.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Pc Security ۳۳۶

۱۳.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Secure Browser ۳۳۶

۱۴.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Secure Browser ۳۳۶

۱۵.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Password Door ۳۳۶

۱۶.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه FolderMage Pro ۳۳۷

۱۷.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Stealth Encrypto ۳۳۷

۱۸.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Private Desktop ۳۳۷

۱۹.۱۶.۱۶ نحوه‌ی حذف پسورد آنتی‌ویروس nod32 ۳۳۷

۲۰.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه USB Disk Security ۳۳۷

۲۱.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Hide My Folders ۳۳۸

۲۲.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Private Pix ۳۳۸

۲۳.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Clear Lock ۳۳۸

۲۴.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Security Administrator ۳۳۸

۲۵.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه Anti porn ۳۳۸

۲۶.۱۶.۱۶ نحوه‌ی حذف پسورد برنامه FolderGuard ۳۳۸

۳۴۰	مقدمه	۱.۱۷
۳۴۰	طریقه‌ی نصب در لینوکس کلاه قرمز	۲.۱۷
۳۴۵	ngrep	۳.۱۷
۳۴۷	استفاده از نرم‌افزار ngrep در ویندوز	۱.۳.۱۷
۳۴۹	tcpdump	۴.۱۷
۳۵۰	بررسی چند دستور دیگر در اسنiffer tcp dump	۱.۴.۱۷
۳۵۱	windump	۵.۱۷
۳۵۲	Sniffing with snort	۶.۱۷
۳۵۳	تست برنامه snort	۱.۶.۱۷
۳۵۴	یک اسنiffer تجاری	۷.۱۷
۳۵۵	رمزگذاری در دو انتها	۸.۱۷
۳۵۶	رمزگذاری و سنجش برنامه	۹.۱۷

۳۵۸	مقدمه	۱.۱۸
۳۵۸	نصب	۲.۱۸
۳۵۹	استفاده	۳.۱۸
۳۵۹	رابط کنسول	۴.۱۸
۳۶۷	رابط وب	۵.۱۸
۳۶۸	محیط‌ها و متغیرهای متاسپلویت	۶.۱۸
۳۶۹	محیط سراسری	۷.۱۸
۳۷۰	محیط موقت	۸.۱۸
۳۷۰	تنظیمات پیشرفته محیط	۱.۸.۱۸
۳۷۱	ارتقا و افزودن اکسپلویت و پیلود جدید	۹.۱۸