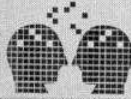


۱۳۵۰۱۹۹
کار و کتاب



کانون نشر علوم

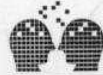
ٹینوکس، سیستم عامل نفوذگران

مؤلف:

مهندس مجید داوری دولت آبادی

ناشر:

کانون نشر علوم



ناشر علوم

www.nashreloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سرشناسه: داوری دولت‌آبادی، مجید، ۱۳۵۹-

عنوان و نام پدیدآور: لینوکس، سیستم‌عامل نفوذگران/ مؤلف مجید داوری دولت‌آبادی.

مشخصات نشر: تهران: کانون نشر علوم: انتشارات آترا، ۱۳۹۴.

مشخصات ظاهری: ۶۴۰ ص: مصور، جدول، نمودار.

شابک: ۹۷۸۹۶۴۳۷۱۱۷۶

وضعیت فهرست‌نویسی: فیا

موضوع: سیستم‌عامل لینوکس

نوع: سیستم‌های عامل (کامپیوتر)

رده‌بندی کنگره: ۱۳۹۳ ۱۹۴۵۲۸۲ س ۹۴۵/۷۶ QA ۷۶/۷۶

رده‌بندی دیویی: ۰۰۰۰۴۳۲

شماره ثبت‌نشان ملی: ۳۱۰۰۵

نام کتاب: لینوکس، سیستم‌عامل نفوذگران

ناشر: کانون نشر علوم

ناشر همکار: انتشارات آترا

مؤلف: مهندس مجید داوری دولت‌آبادی

ویراستار ادبی: کانون نشر علوم

صفحه‌آرا: فاطمه سلطان‌آبادی

طرح جلد: شیما نجفی

چاپ اول: بهار ۱۳۹۴

تیراژ: ۱۰۰۰

چاپ و صحافی: کانون نشر علوم

قیمت: ۴۰۰۰۰ تومان

شابک: ۹۷۸۹۶۴۳۷۱۱۷۶

مراکز پخش:

پخش علوم: خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد ۱

تلفن: ۶۶۹۶۱۵۶۸-۶۶۴۹۴۹۱۱

نشر و پخش آترا: میدان انقلاب، خیابان جمالزاده جنوبی، کوچه شهید آقاصوری، پلاک ۱۲

تلفن: ۶۶۹۲۲۰۸۲



ناشر سخن

به نام خداوند بخشنده و مهربان

گستره دانش بشری در برابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ همچنین که گفته «و ما عطا نکردیم به شما علم را جز اندکی» شاهی است بر ضعف معرفت انسانی نسبت به عظمت صمدانی. با این حال چه نیکو سفارش فرموده است خاتم انبیاء، حضرت محمد مصطفی (ص)، که «جوید علم را اگر چه به سرزمین چین». این توصیه، تمامی پیروان راستین دین حبیب اسلام را به فراگیری و اکتساب علوم و فنون مختلف در همه زمان‌ها و همه مکان‌ها فرا می‌خواند.

تلاش کانون نشر علوم، همواره معصرت به تولد آثار نایسته و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه مشکلات و دشواری‌های فراوانی حادث شده و خواهد شد. این امر تا حدی بسیار، تابعی از ماهیت رشته‌های فنی و مهندسی و معارف مربوط به آنهاست؛ چرا که این رشته‌ها به سرعت و بی‌وقفه در حال نو به نو شدن می‌باشند. این امر رسالت کانون نشر علوم را در نشر آثار مربوطه، اعم از تألیف یا ترجمه، خنجر تنگ می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از فافله عارم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی، در برابر شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند متّان در این مهم مساعدت فرماید.

پایان سخن اینکه، کانون نشر علوم دست یاری و همت تمامی مؤلفین و مترجمین علاقه‌مند در زمینه علوم فنی و مهندسی را به گرمی می‌فشارد و تمامی ایشان را خاضعانه و خاشعانه به همکاری فرا می‌خواند. همچنین این مجموعه از تمامی مخاطبین استدعا دارد که با نظرات صائب و راهگشای خود، در بهبود شکلی و محتوایی آثار منتشر شده مساعدت فرمایند؛ و صد البته که تمامی کاستی‌ها از این رهگذر تنها و تنها متوجه این مجموعه بوده و هست.

سید محمدحسین متّوری

کانون نشر علوم



مقدمه مؤلف

امروزه در دنیای هک و نفوذ، استفاده از سیستم‌عامل لینوکس امری بدیهی و ابزاری لازم و ضروری است. در واقع سیستم‌عامل لینوکس برای یک نفوذگر واقعی حکم عصای دست وی را دارد و نبود آن می‌تواند در روند عملیات نفوذ یا آزمایش نفوذ ایجاد اختلال کند. در این میان توزیع‌های لینوکس قدرتمندی نیز متخصص انجام عملیات آزمایش نفوذ و هک ارائه شده‌اند که در آن‌ها تمامی ابزارهایی که یک نفوذگر بخواهد متخصص درحین انجام عملیات به آن‌ها نیاز دارد، به‌طور پیش‌فرض بر روی این نوع توزیع‌ها نصب و راه‌اندازی شده است که می‌توان از آن‌ها استفاده کرد. سیستم‌عامل لینوکس چه از دیدگاه ابزارهای موجود برای نفوذ و بهره‌برداری در جهت حمله و چه از نظر کدنویسی بر این خصوص از توانایی بالایی برخوردار است. یک نفوذگر یا متخصص امنیت هر چقدر که آزمایشات خود را با سیستم‌عامل ویندوز انجام دهد، زمانی فرا می‌رسد که مجبور می‌شود تا از سیستم‌عامل لینوکس استفاده کند، زیرا ویندوز جوابگوی پیاده‌سازی تمامی آزمایشات در شاخه نفوذ نمی‌باشد.

"لینوکس، سیستم‌عامل نفوذگران"، کتابی است که سعی می‌کند کاربران و نفوذگران را با انواع روش‌های حمله و نفوذگری از طریق سیستم‌عامل لینوکس آشنا نماید. در این کتاب یک توزیع خاص سیستم‌عامل لینوکس مطرح نمی‌باشد. ابزارهای موجود در انواع توزیع‌های سیستم‌عامل لینوکس جهت امور امنیتی و نفوذگری استفاده شده است. کتاب مذکور به کاربران تازه کار لینوکس توصیه نمی‌شود و بایستی ابتدا از طریق یک کتاب پایه و مرجع اصول و روش کار، استفاده و کار با محیط سیستم‌عامل لینوکس فراگرفته شود. سپس جهت پیاده‌سازی امور نفوذگری و امنیتی به این کتاب مراجعه کرد. این کتاب برای کارشناسان، دانشجویان، متخصصان شبکه و امنیت شبکه بسیار مفید می‌باشد و از طریق آن می‌توانند با اصول روش‌های حمله و مقابله با آن از طریق مبداهای لینوکسی آشنا شوند و راهکارهای مقابله با آن را فراگیرند. این کتاب قصد دارد کارشناسان و متخصصان شبکه را با اصول و قواعد حملات بر علیه شبکه‌های کامپیوتری آشنا نماید. درحال حاضر نسخه‌های لاتینی که در این خصوص نوشته شده است به‌صورت پراکنده به بررسی حملات پرداخته است، اما این کتاب قصد دارد با یک انسجام کامل به حملاتی که توسط سیستم‌های عامل لینوکس بر علیه تمامی سیستم‌های عامل انجام می‌شود بپردازد، زیرا همان‌طور که می‌دانید سیستم‌عامل لینوکس از ابزارهای اساسی و پایه‌ای نفوذگران و هکرها برخوردار می‌باشد و یک هکر جهت انجام حملات هکری خود، شدیداً نیازمند این نوع سیستم‌عامل است. در این کتاب از تمامی منابع معتبر و پایه‌ای علم هک استفاده شده است که البته با تجزیهات ناچیز اینجانب آمیخته گردیده است تا کتابی جامع و مفید ایجاد شود.

اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به‌منظور افزایش آگاهی متخصصین، دانشجویان و مدیران شبکه در زمینه آزمایشات نفوذ،



قوانین هکریهای بااخلاق و نحوه استفاده از ابزارهای موجود در توزیع‌های قدرتمند لینوکس در حوزه نفوذ بودم تا آن‌ها را با اصول فنی آزمایشات نفوذ با کمک این توزیع‌ها آشنا و آگاه سازم و بتوان از آن در فرآیندها و پروژه‌های آزمایش نفوذ استفاده نمود (گرچه مدیران و متخصصین امنیت شبکه حکم اساتید اینجانب را دارند، اما به حکم وظیفه برخورد لازم دانستم که این آگاه‌سری را انجام دهم).

همان‌طور که گفته شد، شیرازه اصلی کتاب حاضر برگرفته از کتاب‌ها و منابع معتبر و استاندارد ساخته امنیت داده، اصول آزمایشات نفوذ، استانداردهای امنیت اطلاعات، نفوذگری (هک)، توزیع‌های استاندارد، آزمایش نفوذ و هک می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است. هدف کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش بام کجی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران مسئول انتقادات راهنمایی‌های دلسوزانه آن‌ها را به دیده منت پذیرا هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.zzn.com)

این کتاب صرفاً برای افزایش آگاهی‌ها و رشد علمی متخصصین کامپیوتر تألیف گردیده است. در نتیجه عواقب ناشی از هرگونه سوءاستفاده از مطالب این کتاب برعهده شخص خاطی بوده و مؤلف و انتشارات هیچ گونه مسئولیتی در این مورد برعهده نخواهند گرفت.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و آشنایان عزیز که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. برخورد لازم می‌دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانه ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. همچنین از جناب آقای سعید بیکی نیز کمال تشکر را دارم. اکثر مطالب فصل چهارم این کتاب برگرفته از ترجمه کتاب هنر اکسپلویت‌نویسی می‌باشد که توسط ایشان ترجمه شده است.

در پایان از مدیریت فرزانه انتشارات کانون نشر علوم جناب آقای مهندس سید محمدحسین منوری و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یارب بگشا گره ز کار من زار / رحمی که ز عقل عاجزم در همه کار

جز در گره تو کی بودم درگاهی / محروم ازین درم مکن یا غفار



فهرست مطالب

۱۵	فصل اول: لینوکس و توزیع‌های مختلف آن
۱۶	مقدمه
۱۶	مفاهیم پایه در لینوکس
۱۹	مفهوم توزیع در گنوالینوکس
۲۱	مفهوم توزیع‌های مبتنی بر دیسک‌های زنده
۲۲	توزیع‌های امنیتی و مخصوص نفوذ لینوکس
۲۷	فصل دوم: به سیری از لینوکس در حملات مبتنی بر شناسایی و جمع‌آوری اطلاعات
۲۹	معرفی ابزارهای Bil F جهت جمع‌آوری اطلاعات
۳۲	ابزار Whois به منظور جمع‌آوری اطلاعات
۳۳	تکنیک‌های پایهای برای شناسایی آدرس‌های IP و نام‌میزبان
۴۰	منظور از پروتکل RWHOIS
۴۰	بهره‌گیری از SNMP جهت جمع‌آوری اطلاعات
۴۴	ابزارهای WHOIS و dnsmap برای جمع‌آوری اطلاعات
۴۵	بهره‌گیری از SMTP جهت جمع‌آوری اطلاعات
۴۶	استفاده از NetBIOS جهت شناسایی و جمع‌آوری اطلاعات
۴۷	ایجاد نقشه شبکه به منظور جمع‌آوری اطلاعات
۵۳	انواع پوشش در شبکه
۵۴	بهره‌گیری از تکنیک‌ها برای شناسایی سیستم‌عامل سیستم هدف
۵۵	ابزار قدرتمند NMap
۶۵	بهره‌گیری از ابزار NetCat در عملیات پوشش پورت
۶۶	ابزار Unicornscan
۶۷	ابزار Amap
۶۷	ابزار nping
۶۸	ابزار Firewall برای شناسایی دیوارهای آتش مستقر در شبکه
۷۳	معرفی ابزارهای متداول دیگر در حوزه جمع‌آوری اطلاعات
۸۵	فصل سوم: حمله به مکانیزم‌های رمزنگاری و کلمات عبور با کمک لینوکس
۸۷	مفاهیم پایه‌ای در خصوص حملات برعلیه رمزعبور
۹۰	نمونه‌هایی از کدهای درهم شکستن کلمات عبور
۹۲	پیاده‌سازی حملات کلمات عبور با استفاده از پردازنده‌های کمکی
۹۴	استفاده از مکانیزم جدول رنگین‌کمانی (Rainbow Tables)
۹۵	ابزارهای درهم‌شکستن رمزها و کلمات عبور در لینوکس



۱۰۹	فصل چهارم: کدنویسی در لینوکس
۱۱۱	مفهوم Black Code
۱۱۱	مفهوم Exploit
۱۱۲	طبقه‌بندی کدهای Exploit
۱۱۲	مفهوم Shell Code
۱۱۴	اکسپلویت کردن برنامه
۱۱۵	تک کدهای کلی اکسپلویت
۱۱۶	سرریزهای باقی
۱۱۸	سرریزهای مبتنی بر حافظه
۱۲۳	اکسپلویت کردن بدون کد
۱۲۷	استفاده از محیط
۱۳۳	سرریزهای مبتنی بر Heap و PSS
۱۳۳	یک نمونه پایه از سرریز مبتنی بر Heap
۱۴۰	جای‌نویسی اشاره‌گرهای تابع
۱۴۹	نویسی Shellcode
۱۵۰	فراخوانی‌های سیستمی در لینوکس
۱۵۰	ابزار Dissembler
۱۶۳	فصل پنجم: استراق‌سمع از شبکه با کمک لینوکس
۱۶۴	مفهوم شنود یا استراق‌سمع
۱۶۷	معرفی ابزارهای Sniffer در لینوکس
۱۸۱	فصل ششم: پیاده‌سازی حملات مهندسی اجتماعی با کمک لینوکس
۱۸۳	منظور از مهندسی اجتماعی
۱۸۳	مهندسی اجتماعی معکوس
۱۸۴	بهره‌گیری از ابزارهای لینوکس در حملات مهندسی اجتماعی
۱۹۹	فصل هفتم: بررسی ابزارهای لینوکس جهت نفوذ به سرویس‌های وب و پست‌الکترونیکی
۲۰۰	معرفی حملات برعلیه سرور وب IIS
۲۰۱	معرفی حملات برعلیه سرور وب آپاچی
۲۰۲	معرفی حملات برعلیه برنامه‌های کاربردی تحت وب
۲۰۲	ابزارهای حمله و آزمایش نفوذ در سطح وب و پست‌الکترونیکی
۲۲۴	تجزیه و تحلیل برنامه‌های کاربردی وب (ابزارهای شناسایی CMSها)
۲۲۸	تجزیه و تحلیل برنامه‌های کاربردی وب (ابزارهای مخصوص Web Crawlers)



۲۳۳	تجزیه و تحلیل برنامه‌های کاربردی وب (ابزارهای تجزیه و تحلیل SSL)
۲۳۷	ابزارهای ارزیابی برنامه‌های کاربردی وب (ابزارهای شناسایی آسیب‌پذیری‌های مبتنی بر CMS)
۲۴۰	ابزارهای پراکسی برنامه‌های کاربردی وب
۲۴۰	ابزارهای ارزیابی کدباز وب
۲۴۳	ابزارهای بهره‌برداری از وب
۲۴۴	ابزارهای اسکن امنیتی
۲۴۵	ابزارهای تجزیه و تحلیل SMTP
۲۴۷	فصل هشتم: جعل هویت با کمک لینوکس
۲۴۸	سرقت هویت چیست؟
۲۴۸	انواع مکانیزم‌ها و حملات مبتنی بر جعل هویت
۲۶۶	استفاده از ابزارها جهت ریودن هویت
۲۷۵	فصل نهم: نفوذ به پایگاه‌های داده، در طریقه لینوکس
۲۷۶	ابزارهای نفوذ به پایگاه‌های داده
۳۰۵	معرفی سایر ابزارهای نفوذ به پایگاه‌های داده
۳۰۵	ابزارهای تجزیه و تحلیل، ارزیابی و بهره‌برداری از پایگاه‌های داده (تجزیه و تحلیل MS SQL)
۳۱۰	ابزارهای تجزیه و تحلیل، ارزیابی و بهره‌برداری از پایگاه‌های داده (تجزیه و تحلیل MySQL)
۳۱۱	ابزارهای تجزیه و تحلیل، ارزیابی و بهره‌برداری از پایگاه‌های داده (تجزیه و تحلیل Oracle)
۳۱۳	فصل دهم: حملات مبتنی بر سرریزی بافر با ابزارهای لینوکس
۳۱۴	بررسی مفهوم پشته
۳۱۴	بررسی مفهوم بافر
۳۱۵	بررسی مفهوم Heap
۳۱۵	بررسی مفهوم سرریزی بافر
۳۱۶	استفاده از ابزارها جهت پیاده‌سازی حملات سرریزی بافر
۳۲۴	بهره‌گیری از ابزار قدرتمند SET برای پیاده‌سازی حملات مبتنی بر سرریزی بافر
۳۲۵	ابزار JBroFuzz
۳۲۶	ابزارهای فازر شبکه (Network Fuzzers)
۳۲۷	ابزارهای مخصوص Fuzzers برنامه‌های کاربردی وب
۳۳۱	فصل یازدهم: ابزارها در لینوکس برای حمله به آسیب‌پذیری‌ها و عبور از نرم‌افزارهای امنیتی
۳۳۲	مفهوم آسیب‌پذیری و شماره‌گذاری آن‌ها
۳۳۳	پوشش‌گرهای آسیب‌پذیری
۳۳۴	مفهوم False Positive
۳۳۴	مفهوم Payload و انواع مازول‌های آن



۳۳۵	استفاده از ابزارها جهت بهره‌برداری از ضعف‌ها و آسیب‌پذیری‌ها
۳۳۵	ابزارهای مخصوص فاز شناسایی
۳۴۲	ابزارهای مخصوص فاز بهره‌برداری
۳۴۶	ابزارهای مشترک در فاز شناسایی و بهره‌برداری
۳۵۰	تکمیل‌بندی ابزارها براساس نوع آزمایش و حمله
۳۵۲	ابزارهای مورد استفاده در دو حوزه جعبه سیاه و سفید
۳۶۶	غشال کردن ضد ویروس از راه دور با کمک لینوکس
۳۶۸	غیرفعال کردن سرویس‌ها با کمک ابزار Veil
۳۷۱	تحلیل کد Hash md5، آماده با کمک ابزار Automater
۳۷۳	فصل دوازدهم: پیاده‌سازی حملات نوع DoS در لینوکس
۳۷۴	منظور از حملات انسداده سرویس یا پذیرش سرویس (DoS)
۳۷۵	مروری بر برخی حملات متداول DoS
۳۷۶	حملات انسداده سرویس توزیع‌شده DoS
۳۷۷	انواع حملات DDoS
۳۷۸	ابزارهای معروف جهت پیاده‌سازی حملات DoS و DDoS
۳۹۷	فصل سیزدهم: حمله به بستر مکانیزم VoIP از طریق لینوکس
۳۹۸	سیستم آزمایش نفوذ SIP
۴۰۰	تشخیص خودکار آسیب‌پذیری‌های VoIP مبتنی بر SIP
۴۰۲	آزمایش جعبه سیاه برای آزمایش کیفیت سرویس VoIP مبتنی بر SIP
۴۰۳	ارائه یک چارچوب آزمایش امنیت برای SIP
۴۰۴	ابزارهای مخصوص تجزیه و تحلیل VoIP
۴۰۴	ابزارهای تجزیه و تحلیل VoIP
۴۱۲	ابزارهای VoIP Fuzzers
۴۱۲	ابزارهای استراق‌سمع VoIP
۴۲۶	ابزارهای جعل VoIP
۴۲۹	حمله به مکانیزم VoIP با کمک ابزار Metasploit
۴۳۳	فصل چهاردهم: حمله به تجهیزات شبکه از طریق لینوکس
۴۳۴	معرفی برخی تجهیزات آسیب‌پذیر در شبکه‌های کامپیوتری
۴۳۵	ابزارهای لینوکس برای نفوذ به تجهیزات شبکه
۴۶۳	فصل پانزدهم: نفوذ به شبکه‌های بی‌سیم با کمک ابزارهای لینوکس
۴۶۴	کاربرد ابزار Ethereal در لینوکس



۴۶۹	استفاده از نقاط دسترسی جعلی
۴۷۹	نفوذ به شبکه‌های بی‌سیم برپایه WEP
۴۸۷	نفوذ به شبکه‌های بی‌سیم برپایه WPA و WPA2
۵۰۶	پایاده‌سازی مکانیزم DeAuth با استفاده از اسکریپت Airoscapy
۵۱۱	معرفی دیگر ابزارهای حملات بی‌سیم در لینوکس
۵۱۱	ابزار Aircrack-ng
۵۲۶	ابزار Kismet
۵۲۸	ابزار Wireshark
۵۲۹	ابزار macchanger
۵۲۹	ابزار Redfang 2.5
۵۳۰	ابزار THC-WarDrive
۵۳۰	ابزار PrismStumbler
۵۳۰	ابزار Mognet
۵۳۱	ابزار WaveStumbler
۵۳۱	ابزار AP Scanner
۵۳۱	ابزار netdiscover
۵۳۲	ابزار SSID Sniff
۵۳۲	ابزار Wavemon
۵۳۳	ابزار AirTraf
۵۳۵	ابزار AirMagnet
۵۳۵	ابزار Gpsmap-Expedia و Gpsmap/Kismap
۵۳۶	ابزار GpsDrive
۵۳۷	ابزار netxml2kml/Google Earth
۵۳۷	ابزار Wiffy
۵۳۸	ابزار Cowpatty
۵۴۱	ابزار AirSnort
۵۴۱	ابزار WifiScanner
۵۴۱	ابزار giskismet
۵۴۲	ابزار pcapdump
۵۴۳	ابزار ssidsniff
۵۴۴	ابزار fern-wifi-cracker
۵۴۴	ابزار freeradius-wpe



۵۴۴	ابزار gerix-wifi-cracker-ng
۵۴۵	ابزار freeradius-wpe setup
۵۴۵	ابزار horst
۵۴۵	ابزار pcapgetiv
۵۴۵	ابزار pyrit
۵۴۵	ابزار reaver
۵۴۶	ابزار weakivge
۵۴۷	ابزار wepckack
۵۴۷	ابزار wifi-money
۵۴۷	ابزار white
۵۴۷	ابزار AiRoPeek
۵۴۷	ابزار Sniffer Wireless
۵۴۷	ابزار mdk3

۵۵۱ فصل شانزدهم: نفوذ به شبکه‌های مبتنی بر Bluetooth در لینوکس

۵۵۲	مروری بر تهدیدات در بلوتوث
۵۵۴	ابزارهای متداول در حملات بر علیه بلوتوث
۵۵۴	ابزار heicool و fang
۵۵۸	ابزارهای مخصوص تجزیه و تحلیل Bluetooth
۵۶۰	ابزارهای بهره‌برداری از بلوتوث
۵۶۳	ابزار sdptool
۵۶۵	ابزار rfcommScan و carwhisperer (poc)
۵۶۶	ابزار ubertooth-lap
۵۶۷	ابزار Bluesnarfer
۵۶۷	ابزارهای blues-test-input و bluez-test-device, bluez-simple-agent

۵۶۹ فصل هفدهم: حمله به شبکه‌های RFID از طریق لینوکس

۵۷۰	تکنولوژی RFID
۵۷۰	تهدیدهای معروف RFID
۵۷۱	نرم‌افزارهای مشکل‌ساز RFID
۵۷۲	استثمارگران RFID
۵۷۲	کرم‌های RFID
۵۷۳	ویروس‌های RFID



۵۷۴	حملات امنیتی بر علیه RFID
۵۷۴	معماری لایه‌های اطلاعاتی پس‌زمینه
۵۷۵	چگونه یک ویروس RFID عمل می‌کند؟
۵۷۵	مواجهه با خود ارجاعی
۵۷۶	عوامل نفوذ
۵۷۹	بررسی مقاله است در RFID
۵۸۰	معرفی ابزارهای RFID
۵۸۰	ابزارهای RFIDIOACG
۵۸۰	ابزارهای شاخه RFIDIOtisch
۵۸۰	ابزارهای شاخه RFIDIOtisch
۵۸۰	بهره‌گیری از ابزار mifoc برای شناسایی گوریتم کلید متقارن
۵۸۷	فصل هجدهم: پیاده‌سازی حملات امنیتی سرویس‌های نام در لینوکس
۵۸۸	حملات مبتنی بر DNS
۵۸۸	حملات براساس سروریزی بافر در سرویس DNS
۵۸۸	حملات براساس افشاء اطلاعات در سرویس DNS
۵۸۹	حملات برپایه مسموم‌سازی حافظه نهان سرویس DNS
۵۹۳	حملات براساس نوع DoS بر علیه سرویس DNS
۵۹۴	حملات از نوع ارتباط‌رایی در DNS
۵۹۷	فصل نوزدهم: حملات مبتنی بر War Dialing در لینوکس
۵۹۸	انواع مکانیزم‌ها و حملات War Dialing
۵۹۹	بررسی ابزارهای حملات War Dialing
۶۰۱	ابزارهای تجزیه و تحلیل تلفنی
۶۰۲	ابزارهای بهره‌برداری از GSM
۶۰۳	فصل بیستم: نگهداری و پایداری نفوذ انجام شده توسط ابزارهای لینوکس
۶۰۴	ایجاد درپشتی در سیستم هدف به منظور اهداف بعدی
۶۰۵	اتصال از درون شبکه به سیستم نفوذگر برای مخفی ماندن
۶۰۶	یاکنزری رد پای حمله
۶۰۷	ابزارهای موجود در لینوکس برای نگهداری و پایداری نفوذ
۶۰۷	دره‌ی پستی سیستم عامل
۶۱۱	فصل بیست و یکم: ابزارهای پزشکی دیجیتال و گزارش گیری در لینوکس
۶۱۲	تهیه گزارش و قوانین آن در آزمایشات نفوذ



- ۶۱۳..... ابزارهای بررسی پزشکی دیجیتال و روال‌های گزارش‌گیری
- ۶۱۳..... ابزارهای پزشکی دیجیتال ضدویروس
- ۶۱۴..... ابزارهای ضد پزشکی دیجیتال
- ۶۱۴..... ابزارهای پزشکی دیجیتال
- ۶۱۷..... ابزارهای تجزیه و تحلیل پزشکی دیجیتال
- ۶۲۷..... ابزارهای حکاکای پزشکی دیجیتال
- ۶۲۲..... ابزارهای درهم‌سازی در پزشکی دیجیتال
- ۶۲۲..... ابزارهای تصحیح‌مندی پزشکی دیجیتال
- ۶۲۷..... بسته‌های افزایشی پزشکی دیجیتال
- ۶۳۸..... پزشکی دیجیتال شبکه
- ۶۴۰..... ابزارهای پزشکی دیجیتال گمنام
- ۶۴۱..... ابزارهای پزشکی قانونی PDF
- ۶۴۵..... ابزارهای پزشکی دیجیتال RAM
- ۶۴۶..... ابزارهای مخصوص مدیریت مدارهای دیجیتال
- ۶۴۷..... ابزارهای مخصوص جمع‌آوری و ضبط ر
- ۶۴۹..... منابع و مراجع