

۱۴۱۳/۷۰

مرجع کامل

انک و ضد انک

اخلاق

ترجمہ: محمد مختار



سرشناسه
عنوان و نام پدیدآور : مرجع کامل هک و ضد هک اخلاقی / مترجم:
Kevin, Beaver : بیور، کوین
مشخصات نشر : تهران: نبض دانش، ۱۳۹۵.
مشخصات ظاهری : ۴۳۴ صفحه مصور
شابک : ۹۷۸-۶۰۰-۷۷۰۳-۷۲-۴
وضعیت فهرست‌نویسی : فیپا
شناسه افزوده : محمدی، محمد، ۱۳۶۳ شهرپور - مترجم
موضوع : کامپیوترها -- ایمنی اطلاعات
رده بندی گ : ۱۳۹۵ ب ۹ ک ۹ / ۷۶ QA
رده بندی ی : ۰۰۵/۸
شماره کتابشاس ملی : ۴۲۴۹۱۵۱

این اثر مشمول قانون حمایت مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ است هر کس تمام یا قسمتی از این اثر را بدون اجازه ناشر، نشر یا پخش کند مورد پیگیری قانونی قرار خواهد گرفت.



نبض دانش

همراه: ۰۹۱۲۷۸۵۶۵۱۵

عنوان مرجع کامل هک و ضد هک اخلاقی
مترجم محمدی محمد
ناشر نبض دانش
سال چاپ ۱۳۹۵
نوبت چاپ اول
تیراژ ۲۰۰ نسخه
قیمت به همراه پکیج آموزشی ۲۸۵۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۷۷۰۳-۷۲-۴ ISBN: 978-600-7703-72-4

پست الکترونیکی: NabzeDanesh@gmail.com

فروشگاه اینترنتی: www.NabzeDanesh.ir

فصل ۱: آشنایی با هک اخلاقی.....	۲۱
۱-۱ توضیح واژگان فنی و تخصصی.....	۲۲
۲-۱ تعریف هکر.....	۲۳
۳-۱ تعریف کاربر بداندیش.....	۲۳
۴-۱ چرا و چگونه حمله کنندگان بداندیش باعث پیدایش هک‌های اخلاقی می‌شوند.....	۲۴
۵-۱ هک اخلاقی در مقایسه با بازرسی.....	۲۵
۶-۱ ملاقات مربوط به سیاست‌ها و برنامه‌ها.....	۲۵
۷-۱ مسائل مرتبط با به‌نابرت‌ها و تطبیق با قوانین.....	۲۶
۸-۱ درک لزوم هد کردن برنامه‌های خودتان.....	۲۶
۹-۱ درک خطراتی که سیستم‌ها با آن‌ها روبرو هستند.....	۲۸
۱۰-۱ حمله‌های غیراخلاق‌گرایانه.....	۲۹
۱۱-۱ حملاتی که به زیرساخت‌ها آسیب می‌رساند.....	۲۹
۱۲-۱ حملات مربوط به سیستم‌های عامل.....	۲۹
۱۲-۱ حمله به اپلیکیشن‌ها و دیگر حملات خاص.....	۳۰
۱۳-۱ پیروی از احکام هک اخلاقی.....	۳۰
۱۴-۱ اخلاقی کار کنید.....	۳۱
۱۵-۱ احترام به حریم خصوصی.....	۳۱
۱۶-۱ به سیستم‌هایتان آسیب نزنید.....	۳۲
۱۷-۱ استفاده از فرآیند هک اخلاقی.....	۳۲
۱۸-۱ فرمول‌بندی نقشه و برنامه‌ی خود.....	۳۳
۱۹-۱ انتخاب ابزارها.....	۳۵
۲۰-۱ اطمینان یابید که از ابزارهای مناسب برای این کار استفاده می‌کنید.....	۳۶
۲۱-۱ در ابزارهایی که برای هک اخلاقی به کار می‌برید به دنبال این ویژگی‌ها باشید.....	۳۷
۲۲-۱ اجرای برنامه.....	۳۷

- ۳۸..... ۱-۲۳) ارزیابی نتایج
- ۳۹..... ۱-۲۴) ادامه دادن
- ۴۰..... ۲) فصل ۲: رخنه به اندیشه‌ی هکرها
- ۴۱..... ۱-۲) چیزی که علیه‌ش برخاسته‌اید.....
- ۴۲..... ۲-۲) فکر کردن همچون افراد بد.....
- ۴۴..... ۳-۲) کسانی که به زور وارد سیستم‌های رایانه‌ای می‌شوند.....
- ۴۴..... ۲-۴) سطح مهارت هکرها.....
- ۴۶..... ۲-۵) تقسیم بندی هکرها براساس انگیزه‌ی هک.....
- ۴۹..... ۲-۶) هک به چه آثاری می‌انجامد؟.....
- ۵۰..... ۲-۷) برنامه‌ریزی و اجرای عملیات.....
- ۵۲..... ۲-۸) ناشناس باقی ماندن.....
- ۵۴..... ۳) فصل ۳: پایه‌ی ریزی برنامه‌ی هک.....
- ۵۵..... ۳-۱) آیا باید خود را بیمه کنید؟.....
- ۵۵..... ۳-۲) برقرار کردن اهداف.....
- ۵۶..... ۳-۳) هنگام تعریف اهداف هک اخلاقی‌تان کار را با پرسش‌های زیر آغاز کنید.....
- ۵۸..... ۳-۴) تعیین اینکه کدام سیستم را باید هک کنید.....
- ۵۸..... ۳-۵) اپلیکیشن‌هایی که می‌توانید تست نفوذ را بر روی آن‌ها انجام دهید.....
- ۵۹..... ۳-۶) تحلیل درختی حمله.....
- ۶۰..... ۳-۷) ایجاد استانداردهای آزمون‌گیری.....
- ۶۱..... ۳-۸) زمان‌بندی.....
- ۶۲..... ۳-۹) اجرای آزمون‌های خاص.....
- ۶۳..... ۳-۱۰) ارزیابی کورکورانه در برابر ارزیابی آگاهانه.....
- ۶۴..... ۳-۱۱) انتخاب محل.....
- ۶۴..... ۳-۱۲) واکنش به آسیب‌پذیری‌هایی که می‌یابید.....
- ۶۵..... ۳-۱۳) در نظر گرفتن چند فرض احمقانه.....

۶۵	انتخاب ابزارهای ارزیابی امنیتی..... (۳-۱۴)
۶۸	فصل ۴: اصول و قواعد هک..... (۴)
۶۹	۱-۴ آماده سازی صحنه برای آزمون.....
۷۱	۲-۴ دیدن آنچه دیگران می بینند.....
۷۲	۳-۴ گردآوری اطلاعات آشکار.....
۷۲	۴-۴ رسانه های اجتماعی.....
۷۲	۵-۴ جستجوی وب.....
۷۴	۶-۴ کپی کردن وب.....
۷۴	۷-۴ وب سایت ها.....
۷۴	۸-۴ نقشه بر روی از شبکه.....
۷۶	۹-۴ گروه های گوگل.....
۷۶	۱۰-۴ سیاست های حفظ ریم خصوصی.....
۷۷	۱۱-۴ اسکن کردن سیستم ها.....
۷۸	۱۲-۴ میزبان ها.....
۷۸	۱۳-۴ پورت های آزاد.....
۷۹	۱۴-۴ تعیین چیزی روی پورت های آزاد در حال اجرا.....
۷۹	۱۵-۴ مجوزهای لازم برای اشتراک گذاری های شبکه.....
۸۲	۱۶-۴ ارزیابی آسیب پذیری ها.....
۸۵	۱۷-۴ اجرای نفوذ به سیستم.....
۸۸	فصل پنجم: مهندسی اجتماعی..... (۵)
۸۹	۱-۵ معرفی مهندسی اجتماعی.....
۸۹	۲-۵ اینک چند مثال از مهندسی اجتماعی.....
۹۰	۳-۵ آغاز نخستین آزمون های مهندسی اجتماعی خود.....
۹۱	۴-۵ یک مطالعه ی موردی از مهندسی اجتماعی با آیرا وینکلر (IRA WINKLER).....
۹۲	۵-۴-۱ نتایج.....

- ۹۲..... (۲-۴-۵) چگونه می‌شد از این اتفاق جلوگیری کرد.....
- ۹۳..... (۵-۵) چرا حمله‌کنندگان از مهندسی اجتماعی استفاده می‌کنند.....
- ۹۴..... (۶-۵) درک مفاهیم.....
- ۹۵..... (۷-۵) انجام حمله‌های مهندسی اجتماعی.....
- ۹۶..... (۸-۵) جستجوی اطلاعات.....
- ۹۶..... (۹-۵) استفاده از اینترنت.....
- ۹۶..... (۱۰-۵) شبکه به درون مخزن زیاله.....
- ۹۷..... (۱۱-۵) شبکه‌های تلفنی.....
- ۹۸..... (۱۲-۵) ایمیل‌ها: دیشپ (PHISHING).....
- ۹۹..... (۱۳-۵) اعتماد سازی.....
- ۱۰۰..... (۱۴-۵) سوءاستفاده از رابطه.....
- ۱۰۰..... (۱-۱۴-۵) فریفتن با سخن و رفتار.....
- ۱۰۲..... (۱۵-۵) حتی متخصصان هم می‌توانند تحت مهندسی اجتماعی قرار بگیرند.....
- ۱۰۲..... (۱۶-۵) فریب از راه فن‌آوری.....
- ۱۰۴..... (۱۷-۵) اقدامات متقابل در برابر مهندسی اجتماعی.....
- ۱۰۴..... (۱-۱۷-۵) سیاست‌ها.....
- ۱۰۵..... (۲-۱۷-۵) هوشیاری و آموزش کاربر.....
- ۱۰۷..... (۱۸-۵) این شیوه‌ها می‌توانند محتوای آموزشهای معمول را تقویت کنند.....
- ۱۰۸..... (۶) فصل ۶: امنیت فیزیکی.....
- ۱۰۹..... (۱-۶) شناسایی آسیب‌پذیری‌های امنیت فیزیکی پایه.....
- ۱۱۰..... (۲-۶) یک پرسش و پاسخ درباره‌ی امنیت فیزیکی با جک وایلز (JACK WILES).....
- ۱۱۰..... (۳-۶) به نظر شما امنیت فیزیکی در رابطه با مسائل امنیتی.....
- ۱۱۱..... (۱-۳-۶) چگونه در هنگام انجام آزمون‌های "تیم سرخ" برای شرکتها می‌توانستید به درون بیشتر ساختمانها وارد شوید؟.....
- ۱۱۱..... (۲-۳-۶) با خودتان چه چیزهایی از ساختمان بیرون می‌آوردید؟.....
- ۱۱۲..... (۴-۶) مکانیابی دقیق آسیب‌پذیری‌های فیزیکی در دفتر خود.....

۱۱۲	نقاط حمله	(۱-۴-۶)
۱۱۳	اقدامات متقابل	(۲-۴-۶)
۱۱۳	خدمات عمومی	(۵-۶)
۱۱۴	نقاط حمله	(۱-۵-۶)
۱۱۴	اقدامات متقابل	(۲-۵-۶)
۱۱۵	چیدمان و کاربرد دفتر	(۶-۶)
۱۱۵	نقاط حمله	(۱-۶-۶)
۱۱۶	اقدامات متقابل	(۲-۶-۶)
۱۱۷	رایانه ها و اجزای شبکه	(۷-۶)
۱۱۷	نقاط حمله	(۱-۷-۶)
۱۱۸	هکرها چیستند؟ این اطلاعات دسترسی خواهند داشت؟	(۸-۶)
۱۲۰	اقدامات متقابل	(۱-۸-۶)
۱۲۱	فصل ۷: گذرواژه ها	(۷)
۱۲۲	شناخت آسیب پذیری های گذرواژه ها	(۱-۷)
۱۲۳	اینجا دو دسته بندی کلی آسیب پذیری های گذرواژه را بیان می کنیم	(۲-۷)
۱۲۳	آسیب پذیری های سازمانی گذرواژه ها	(۳-۷)
۱۲۴	وضعیت	(۱-۳-۷)
۱۲۵	نتیجه	(۲-۳-۷)
۱۲۶	آسیب پذیری های فنی گذرواژه	(۴-۷)
۱۲۶	شکستن گذرواژه ها	(۵-۷)
۱۲۷	روش قدیمی شکستن گذرواژه ها	(۶-۷)
۱۲۷	مهندسی اجتماعی	(۱-۶-۷)
۱۲۸	نگاه از پشت سر یا ورای شانه ها	(۲-۶-۷)
۱۲۹	استنباط	(۳-۶-۷)
۱۲۹	راستی آزمایی ضعیف	(۷-۷)

- ۱۳۰ (۱-۷-۷) دور زدن راستی آزمایی
- ۱۳۰ (۲-۷-۷) اقدامات متقابل
- ۱۳۰ (۸-۷) شکستن پسورد با ابزارهای فن آوری بالا
- ۱۳۴ (۹-۷) حملات لغت نامه ای
- ۱۳۵ (۱۰-۷) حمله های پر قدرت یا قدرت سخت (BRUTE-FORCE)
- ۱۳۶ (۱۱-۷) حمله های رنگین کمان
- ۱۳۷ (۱۲-۷) شکستن گذرواژه ی ویندوز با استفاده از PSDUMP3 و JOHN THE RIPPER
- ۱۳۹ (۱۳-۷) شکستن پسوردهای UNIX/LINUX با JOHN THE RIPPER
- ۱۴۰ (۱۴-۷) ساختن پسورد با اسناد
- ۱۴۱ (۱۵-۷) کرک کردن فایل های محافظت شده با پسورد
- ۱۴۲ (۱۶-۷) درک راه های دیدن شکستن پسورد
- ۱۴۳ (۱-۱۶-۷) ثبت ضربه کشید (ke stroke)
- ۱۴۳ (۲-۱۶-۷) ابزارهای ثبت
- ۱۴۴ (۱۷-۷) ذخیره سازی ضعیف پسورد
- ۱۴۴ (۱۸-۷) جستجو کردن
- ۱۴۵ (۱۹-۷) تحلیلگر شبکه
- ۱۴۷ (۲۰-۷) پسوردهای BIOS ضعیف
- ۱۴۹ (۲۱-۷) اقدامات متقابل کلی در برابر شکستن پسوردها
- ۱۴۹ (۲۲-۷) پسوردهای قوی
- ۱۵۰ (۲۳-۷) تهیه ی سیاست های درباره ی پسورد
- ۱۵۱ (۲۴-۷) درپیش گرفتن دیگر اقدامات متقابل
- ۱۵۳ (۲۵-۷) دیگر اقدامات متقابل برای حفاظت از پسورد به این قرارند
- ۱۵۳ (۲۶-۷) امن سازی سیستم های عامل
- ۱۵۷ (۸) فصل ۸: زیر ساخت شبکه
- ۱۵۸ (۱-۸) یک مطالعه موردی در هک زیر ساخت های شبکه با لورا چپل (LAURA CHAPPELL)

۱۵۹	وضعیت (۱-۱-۸)
۱۵۹	نتیجه (۲-۱-۸)
۱۶۰	شناخت آسیب‌پذیری‌های زیرساخت شبکه (۲-۸)
۱۶۰	هنگام بررسی امنیت زیرساخت شبکه‌ی شرکت خود باید به این موارد نگاهی بیندازید (۳-۸)
۱۶۱	انتخاب ابزار (۴-۸)
۱۶۲	اسکنرها (پایشگرها) و تحلیلگرها (۵-۸)
۱۶۲	ارزیابی آسیب‌پذیری (۶-۸)
۱۶۳	اسکن و کند و کاو در شبکه (۷-۸)
۱۶۳	اسکن پورت‌ها (پایش درگاه‌ها) (۸-۸)
۱۶۵	انجام رفته و پرسش پینگ (PING SWEEPING) (۹-۸)
۱۶۶	استفاده از ابزارهای اسکن پورت (۱۰-۸)
۱۶۷	NMAP (۱۱-۸)
۱۶۹	NETSCANTOOL PRO (۱۲-۸)
۱۷۰	اقدامات متقابل در برابر رفته و پرسش دادن پینگ و اسکن پورت (۱۳-۸)
۱۷۱	اسکن کردن SNMP (۱۴-۸)
۱۷۱	آسیب‌پذیری‌ها (۱-۱۴-۸)
۱۷۳	اقدامات متقابل بر ضد حمله‌های SNMP (۱۵-۸)
۱۷۴	تلنت (TELNET) (۱۶-۸)
۱۷۴	اقدامات متقابل بر ضد حمله‌های تصویر‌گیری از بتر (۱۷-۸)
۱۷۵	آزمودن فرمان‌ها یا قوانین دیواره‌ی آتش (FIREWALL RULES) (۱۸-۸)
۱۷۶	تحلیلگر دیواره‌ی آتش (ALGOSEC FIREWALL ANALYZER) (۱۹-۸)
۱۷۷	اقدامات متقابل در برابر آسیب‌پذیری‌های مجموعه قانون دیواره‌ی آتش (۱-۱۹-۸)
۱۷۸	تحلیل داده‌های شبکه (۲۰-۸)
۱۷۹	برنامه‌های تحلیلگر شبکه (۲۱-۸)
۱۸۴	اقدامات متقابل در برابر آسیب‌پذیری‌های پروتکل شبکه (۱-۲۱-۸)
۱۸۵	امنیت فیزیکی (۲۲-۸)

- ۱۸۵..... ۸-۲۳) آشکارسازی تحلیلگر شبکه
- ۱۸۵..... ۸-۲۴) حمله‌ی MAC-DADDY
- ۱۸۶..... ۸-۲۴-۱) استفاده از Cain & Abel برای مسموم سازی ARP
- ۱۸۷..... ۸-۲۴-۲) گام‌های زیر را به منظور استفاده از Cain & Abel انجام دهید
- ۱۸۹..... ۸-۲۵) کلک آدرس MAC
- ۱۸۹..... ۸-۲۵-۱) سیستم‌های مبتنی بر UNIX
- ۱۹۰..... ۸-۲۵-۲) Windows
- ۱۹۱..... ۸-۲۵-۲) اقدامات متقابل در برابر حمله‌های مسموم سازی ARP و جعل آدرس MAC
- ۱۹۲..... ۸-۲۶) آزمون حمله‌ها، عدم وجود خدمت (DENIAL OF SERVICE)
- ۱۹۲..... ۸-۲۶-۱) حمله‌ها، DOS
- ۱۹۲..... ۸-۲۶-۲) آنچه باید دوباره، باافزار پیشرفته بدانید
- ۱۹۳..... ۸-۲۶-۳) آزمون
- ۱۹۴..... ۸-۲۶-۴) اقدامات متقابل در برابر حمله‌ها، Dos
- ۱۹۶..... ۸-۲۶-۵) آشکارسازی ضعف‌های رایج در روتر، سویچ و دیوارهای آتش
- ۱۹۸..... ۸-۲۷) بنا کردن خطوط دفاعی کلی شبکه
- ۲۰۰..... ۹) فصل ۹: شبکه‌های محلی بی‌سیم یا WIRELESS LANS
- ۲۰۱..... ۹-۱) درک مفاهیم آسیب‌پذیری‌های شبکه‌ی بی‌سیم
- ۲۰۲..... ۹-۲) انتخاب ابزارها
- ۲۰۲..... ۹-۳) وضعیت
- ۲۰۳..... ۹-۴) برآیند
- ۲۰۵..... ۹-۵) کشف LAN‌های بی‌سیم
- ۲۰۵..... ۹-۵-۱) بررسی آگاهی دیگران از وجود شبکه‌ی شما
- ۲۰۷..... ۹-۶) اسکن کردن امواج رادیویی محلی خود
- ۲۰۸..... ۹-۷) کشف حمله‌های شبکه‌ی بی‌سیم و انجام اقدامات متقابل
- ۲۱۰..... ۹-۸) بلوتوث BLUETOOTH را فراموش نکنید

۲۱۱	۹-۹) ترافیک رمزدار (ENCRYPTED TRAFFIC)
۲۱۶	۹-۱۰) اقدامات متقابل در برابر حملات ترافیک رمزدار
۲۱۷	۹-۱۱) تنظیم محافظت شده‌ی وای فای یا Wi-Fi PROTECTED SETUP
۲۱۹	۹-۱۱-۱) اقدامات متقابل برضد مشکل PIN در WPS
۲۲۰	۹-۱۲) ابزارهای بی سیم غیرمجاز
۲۲۵	۹-۱۲-۱) اقدامات متقابل برضد ابزارهای بی سیم غیرمجاز
۲۲۶	۹-۱۳) کلک تغییر MAC (MAC SPOOFING)
۲۳۱	۹-۱۴) اقدامات متقابل برضد جعل MAC
۲۳۲	۹-۱۵) مشکلات امنیت فیزیکی
۲۳۲	۹-۱۶) اقدامات متقابل در برابر مشکلات امنیت فیزیکی
۲۳۲	۹-۱۷) ایستگاه‌های کاری بی سیم آسیب پذیر
۲۳۳	۹-۱۸) اقدامات متقابل در برابر ایستگاه‌های کاری بی سیم در معرض آسیب
۲۳۳	۹-۱۹) تنظیمات پیکربندی پیش فرض
۲۳۴	۹-۲۰) اقدامات متقابل در برابر سوء استفاده‌ها از تنظیمات پیکربندی پیش فرض
۲۳۵	۱۰) فصل ۱۰: ابزارهای موبایل
۲۳۶	۱۰-۱) برآورد آسیب پذیری‌های موبایل
۲۳۶	۱۰-۲) شکستن پسورد لپ تاپ‌ها
۲۳۶	۱۰-۳) انتخاب ابزارها
۲۴۱	۱۰-۴) مغالطه رمزگذاری کل دیسک
۲۴۲	۱۰-۴-۱) اقدامات متقابل
۲۴۳	۱۰-۵) کرک کردن تلفن‌ها و تبلت‌ها
۲۴۴	۱۰-۶) شکستن پسوردهای iOS
۲۴۹	۱۰-۷) اقدامات متقابل برضد شکستن پسورد
۲۵۲	۱۱) فصل ۱۱: ویندوز
۲۵۴	۱۱-۱) آشنایی با آسیب پذیری‌های ویندوز

۲۵۴	انتخاب ابزارها (۲-۱۱)
۲۵۵	ابزارهای رایگان مایکروسافت (۳-۱۱)
۲۵۶	ابزارهای ارزیابی همه در یکی یا همه کاره (ALL-IN-ONE) (۴-۱۱)
۲۵۶	ابزارهایی که کار مشخصی را انجام می دهند (TASK-SPECIFIC TOOLS) (۵-۱۱)
۲۵۷	گردآوری اطلاعات درباره ی آسیب پذیری های ویندوز خود (۶-۱۱)
۲۵۸	اسکن کردن سیستم (۱-۶-۱۱)
۲۵۸	تست کردن (۲-۶-۱۱)
۲۶۰	اقدامات متقابل در برابر اسکن کردن سیستم (۷-۱۱)
۲۶۰	BIOS (۱-۷-۱۱)
۲۶۱	هک ها (۸-۱۱)
۲۶۳	اقدامات متقابل برضد حملات ای NETBIOS (۹-۱۱)
۲۶۴	آشکارسازی نشست های خالی (NULL SESSION) (۱۰-۱۱)
۲۶۵	MAPPING (در انداختن یا بستن) (۱۱-۱۱)
۲۶۶	به دست آوردن اطلاعات (۱۲-۱۱)
۲۶۷	بیکربندی و اطلاعات کاربر (۱۳-۱۱)
۲۶۹	اقدامات متقابل برضد هک های نشست خالی (۱۴-۱۱)
۲۷۱	بررسی مجوزهای اشتراک (SHARE PERMISSIONS) (۱۵-۱۱)
۲۷۱	پیش فرض های ویندوز (۱-۱۵-۱۱)
۲۷۲	آزمون گیری (۱۶-۱۱)
۲۷۳	امنیت Windows 10 و Windows 10 (۱۷-۱۱)
۲۷۴	بهره گیری از وصله های ناموجود (missing patches) (۱-۱۷-۱۱)
۲۷۵	استفاده از METASPLOIT (۱۸-۱۱)
۲۸۲	اقدامات متقابل برضد بهره گیری ها از آسیب پذیری وصله ی ناموجود (۱۹-۱۱)
۲۸۳	اجرای اسکن های تأییدشده (AUTHENTICATED SCANS) (۲۰-۱۱)
۲۸۶	فصل ۱۲: لینوکس LINUX (۱۲)

۲۸۷	۱-۱۲) شناخت آسیب پذیری های لینوکس
۲۸۸	۲-۱۲) انتخاب ابزار
۲۸۹	۳-۱۲) گردآوری اطلاعات درباره ی آسیب پذیری های سیستم لینوکس
۲۸۹	۱-۳-۱۲) اسکن کردن سیستم
۲۹۴	۴-۱۲) اقدامات متقابل در برابر اسکن کردن سیستم
۲۹۴	۵-۱۲) یافتن سرویس های ناآمن و غیر ضروری
۲۹۴	۶-۱۲) جستجوها
۲۹۴	۷-۱۲) آسیب پذیری ها
۲۹۶	۸-۱۲) ابزارها
۲۹۸	۹-۱۲) اقدامات متقابل در برابر حمله به سرویس های غیر ضروری
۲۹۸	۱۰-۱۲) غیرفعال سازی سرویس های غیر ضروری
۳۰۰	۱۱-۱۲) امن سازی فایل های HOSTS و HOSTS.EQUIV
۳۰۱	۱۲-۱۲) هک هایی که با استفاده از فایل های RHOSTS و HOSTS.EQUIV انجام می شوند
۳۰۲	۱۳-۱۲) اقدامات متقابل در برابر حمله های فایل HOSTS.EQUIV و RHOSTS
۳۰۲	۱-۱۳-۱۲) غیرفعال سازی فرمان ها
۳۰۳	۲-۱۳-۱۲) مسدودسازی دسترسی
۳۰۳	۱۴-۱۲) ارزیابی امنیت NFS
۳۰۳	۱-۱۴-۱۲) هک های NFS
۳۰۴	۱۵-۱۲) اقدامات متقابل برضد حمله های NFS
۳۰۴	۱۶-۱۲) بررسی مجوزهای فایل (FILE PERMISSION)
۳۰۵	۱۷-۱۲) هک های مجوز فایل
۳۰۵	۱۸-۱۲) اقدامات متقابل در برابر حمله های مجوز فایل
۳۰۵	۱-۱۸-۱۲) آزمون گیری دستی (manual testing)
۳۰۶	۲-۱۸-۱۲) آزمون گیری خودکار (automated testing)
۳۰۶	۳-۱۸-۱۲) یافتن آسیب پذیری های سر ریز شدن بافر (buffer overflow)
۳۰۷	۴-۱۸-۱۲) اقدامات متقابل در برابر حمله های سرریزی بافر

- ۱۲-۱۹) بررسی امنیت فیزیکی ۳۰۷
- ۱۲-۱۹-۱) هک‌های امنیت فیزیکی ۳۰۷
- ۱۲-۱۹-۲) اقدامات متقابل در برابر حمله‌های امنیتی فیزیکی ۳۰۷
- ۱۲-۲۰) انجام آزمون‌های امنیتی کلی ۳۰۹
- ۱۲-۲۱) وصله زنی لینوکس (نصب وصله‌ها روی لینوکس) ۳۱۱
- ۱۲-۲۲) به‌روزرسانی توزیع یا قسم (DISTRIBUTION) ۳۱۱
- ۱۲-۲۳) مدیریت به‌روزرسانی چند-پلتفرم (MULTI-PLATFORM UPDATE MANAGER) ۳۱۲
- ۱۳) فصل ۱۳: سیستم‌های ارتباطی و پیام‌رسانی ۳۱۵
- ۱۳-۱) آشنایی با آسیب‌پذیری‌های سیستم‌های پیام‌رسان ۳۱۶
- ۱۳-۲) شناسایی و مقابله با حمله‌های ایمیلی ۳۱۷
- ۱۳-۳) بمب‌های ایمیلی ۳۱۷
- ۱۳-۴) پیوسته‌ها ۳۱۷
- ۱۳-۴-۱) حمله‌های با استفاده از سرورهای ایمیل ۳۱۷
- ۱۳-۴-۲) اقدامات متقابل در برابر حمله‌های پرست ایمیل ۳۱۸
- ۱۳-۴-۳) اتصال‌ها (connections) ۳۱۹
- ۱۳-۴-۴) اقدامات متقابل در برابر حمله‌های اتصال (connection attack) ۳۱۹
- ۱۳-۵) کنترل‌های خودکار امنیت ایمیل ۳۲۱
- ۱۳-۶) بنرها (BANNERS) ۳۲۱
- ۱۳-۶-۱) گردآوری اطلاعات ۳۲۱
- ۱۳-۷) اقدامات متقابل در برابر حمله‌های بنر ۳۲۳
- ۱۳-۸) حمله‌های SMTP ۳۲۳
- ۱۳-۸-۱) فهرست برداری از حساب کاربری (account enumeration) ۳۲۴
- ۱۳-۸-۲) حمله‌های با استفاده از فهرست برداری حساب‌های کاربری ۳۲۴
- ۱۳-۸-۳) اقدامات متقابل در برابر فهرست برداری از حساب‌های کاربری ۳۲۷
- ۱۳-۹) رله (RELAY) ۳۲۷

- ۳۲۷..... (automatic testing) آزمون گیری خودکار (۱-۹-۱۳)
- ۳۲۹..... آزمون گیری دستی (۲-۹-۱۳)
- ۳۳۱..... اقدامات متقابل در برابر حمله‌های رله‌ی SMTP (۱۰-۱۳)
- ۳۳۱..... افشای سرنویس ایمیل (E-MAIL HEADER DISCLOSURES) (۱۱-۱۳)
- ۳۳۱..... آزمون گیری (۱-۱۱-۱۳)
- ۳۳۲..... اقدامات متقابل در برابر افشا شدن سرنویس (۲-۱۱-۱۳)
- ۳۳۲..... ضبط ترافیک (CAPTURING TRAFFIC) (۱۲-۱۳)
- ۳۳۳..... به‌افزار (۱۳-۱۳)
- ۳۳۴..... روش‌های عالی عمومی برای به حداقل رسانی ریسک‌های امنیتی ایمیل (۱۴-۱۳)
- ۳۳۵..... ره‌آوردی از آزمون (۱۵-۱۳)
- ۳۳۶..... درک و استفاده از VOICE OVER IP (ارسال صدا روی اینترنت) (۱۶-۱۳)
- ۳۳۷..... آسیب‌پذیری‌های VoIP (۱-۱۶-۱۳)
- ۳۳۹..... انجام اسکن برای یافتن آسیب‌پذیری‌ها (۱۷-۱۳)
- ۳۴۲..... دریافت و ضبط ترافیک صدا (VOICE TRAFFIC) (۱۸-۱۳)
- ۳۴۴..... اقدامات متقابل در برابر آسیب‌پذیری‌های VoIP (۱۹-۱۳)
- ۳۴۶..... فصل ۱۴: وب‌سایت‌ها و اپلیکیشن‌ها (۱۴)
- ۳۴۷..... انتخاب ابزارهای اپلیکیشن وب (۱-۱۴)
- ۳۴۹..... مطالعه‌ی موردی از هک اپلیکیشن‌های وب با کیلب زیبا (CALL SIGN) (۲-۱۴)
- ۳۴۹..... وضعیت (۱-۲-۱۴)
- ۳۵۰..... نتیجه (۲-۲-۱۴)
- ۳۵۰..... جستجوی آسیب‌پذیری‌های وب (۳-۱۴)
- ۳۵۱..... پیمایش و گذر دایرکتوری (DIRECTORY TRAVERSAL) (۴-۱۴)
- ۳۵۱..... جستجوگرها (CRAWLERS) (۵-۱۴)
- ۳۵۲..... GOOGLE (۶-۱۴)
- ۳۵۳..... اقدامات متقابل در برابر بایش دایرکتوری (۷-۱۴)

۲۵۴	 (۸-۱۴) حمله‌های فیلتر کردن ورودی (INPUT-FILTERING)
۲۵۵	 (۹-۱۴) سرریز شدن بافر (BUFFER OVERFLOW)
۲۵۶	 (۱۰-۱۴) دست کاری URL
۲۵۷	 (۱۱-۱۴) دست کاری فیلد پنهان
۲۵۹	 (۱۲-۱۴) تزریق کد و تزریق SQL
۲۶۳	 (۱۳-۱۴) تزریق کد (CROSS-SITE SCRIPTING)
۲۶۵	 (۱۴-۱۴) داده‌ات متقابل در برابر حمله با داده‌های ورودی (INPUT ATTACK)
۲۶۷	 (۱۵-۱۴) حمله‌های اسکرپیت پیش فرض
۲۶۸	 (۱۶-۱۴) اقدامات متقابل در برابر حمله‌های اسکرپیت پیش فرض
۲۶۸	 (۱۷-۱۴) مکانیزم‌های غیر امن ورود به سیستم (UNSECURED LOGIN MECHANISMS)
۲۷۲	 (۱۸-۱۴) اقدامات متقابل برای سیستم‌های LOGIN نا امن
۲۷۳	 (۱۹-۱۴) هم کردن WEB 2.0
۲۷۴	 (۲۰-۱۴) انجام اسکن‌های کلی سیستم برای افتتاح سیب‌پذیری‌های اپلیکیشن وب
۲۷۴	 (۲۱-۱۴) به حداقل رسانی ریسک‌های امنیتی وب
۲۷۵	 (۲۲-۱۴) به کار بستن روش ایجاد امنیت توسط ابزار بازنسازی
۲۷۶	 (۲۳-۱۴) پیشنهاد کردن دیواره‌های آتش
۲۷۷	 (۲۴-۱۴) تحلیل کد منبع
۲۸۰	 (۱۵) فصل ۱۵: پایگاه‌های داده و سیستم‌های ذخیره‌سازی
۲۸۱	 (۱-۱۵) شیرجه زدن به درون پایگاه‌های داده
۲۸۱	 (۲-۱۵) انتخاب ابزار
۲۸۱	 (۳-۱۵) یافتن پایگاه‌های داده روی شبکه
۲۸۲	 (۴-۱۵) یک مطالعه‌ی موردی در هم پایگاه‌های داده با چپ اندروز (CHIP ANDREWS)
۲۸۳	 (۱-۴-۱۵) وضعیت
۲۸۳	 (۲-۴-۱۵) نتیجه
۲۸۵	 (۵-۱۵) شکستن پسوردهای پایگاه داده

۳۸۶	۱۵-۶) اسکن پایگاه‌های داده برای یافتن آسیب‌پذیری‌ها
۳۸۷	۱۵-۷) پیگیری روش‌هایی عالی برای به حداقل رسانی خطرهای امنیتی پایگاه داده
۳۸۸	۱۵-۸) سیستم‌های ذخیره‌سازی
۳۸۸	۱۵-۸-۱) انتخاب ابزارها
۳۸۹	۱۵-۹) یافتن سیستم‌های ذخیره‌سازی در شبکه
۳۸۹	۱۵-۱۰) یافتن متن‌های حساس در فایل‌های شبکه
۳۹۳	۱۵-۱۱) دنبال کردن روش‌هایی عالی برای به حداقل رسانی ریسک‌های امنیتی ذخیره‌سازی
۳۹۶	۱۶) فصل ۱۶: گزارش دهی نتایج و یافته‌ها
۳۹۷	۱۶-۱) گزینش وری نتایج
۳۹۸	۱۶-۲) اولویت‌بندی آسیب‌پذیری‌ها
۴۰۰	۱۶-۳) ایجاد گزارش‌ها
۴۰۲	۱۶-۴) فهرست موارد عملی در گزارش‌ها: گزارشی که باید شامل این‌ها باشد
۴۰۴	۱۷) فصل ۱۷: پوشاندن حفره‌های امنیتی
۴۰۵	۱۷-۱) تبدیل گزارش به اقدام
۴۰۶	۱۷-۲) نصب وصله‌ها برای محافظت
۴۰۷	۱۷-۳) مدیریت نصب وصله‌ها (PATCH)
۴۰۷	۱۷-۴) خودکار سازی نصب وصله‌ها
۴۰۸	۱۷-۴-۱) ابزارهای رایگان
۴۰۸	۱۷-۴-۲) مقاوم‌سازی سیستم‌ها
۴۰۹	۱۷-۵) ارزیابی زیرساخت‌های امنیتی
۴۱۲	۱۸) فصل ۱۸: مدیریت فرآیندهای امنیتی
۴۱۳	۱۸-۱) خودکار سازی فرآیندهای اخلاقی
۴۱۴	۱۸-۲) پایش استفاده‌های مخرب
۴۱۶	۱۸-۳) انجام هک اخلاقی با استفاده از منابع خارجی
۴۱۸	۱۸-۴) آیا به استخدام یک هکر اصلاح‌شده می‌اندیشید؟

- ۱۸-۵) القای تدریجی یک طرز فکر آگاه به امنیت ۴۱۹
- ۱۸-۶) پیش رفتن با دیگر اقدامات امنیتی ۴۲۰
- ۱۹) فصل ۱۹: ده نکته برای به دست آوردن موافقت مدیریت ۴۲۳
- ۱۹-۱) در پی یک متحد و یک پشتیبان باشید ۴۲۳
- ۱۹-۲) فواید کلی هک اخلاقی را بیان کنید ۴۲۴
- ۱۹-۳) در کسب و کار شرکت کنید ۴۲۵
- ۲۰) عمل ۱: دلایلی برای اثبات اینکه هک کردن تنها راه مؤثر برای آزمودن است ۴۲۸
- ۲۰-۱) هک اخلاقی مدیا، بازرسی ها و ارزیابی های امنیتی است ۴۲۸
- ۲۰-۲) مشتریان و کارکنان را متقاعد کنید، "سیستم های چقدر امن هستند؟" ۴۲۸
- ۲۱) فصل ۲۱: ده اشتباه رایج در هک ۴۳۱
- ۲۱-۱) دریافت نکردن تأیید پیش از شروع کار ۴۳۱
- ۲۱-۲) انجام دادن آزمون ها تنها برای یک بار ۴۳۲
- ۲۱-۳) نیازمندی های سیستم های درست ۴۳۳