

۱۳۹۵/۲/۲۹



کتاب نشر علوم

هکرهای قانونمند (CEH)

مؤلف:

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

ناشر:

کانون نشر علوم



ناشر علم

www.nashreoloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سرشناسه: داوری دولت آبادی، مجید، ۱۳۵۹-

عنوان و نام پدیدآور: هک‌های قانونمند (CEH) / مؤلف مجید داوری دولت آبادی.

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

مشخصات ظاهری: ۲۴۸ص: مصور، جدول، نمودار.

شابک: ۹۷۸۶۰۰۶۲۶۵۲۱۶

وضعیت فهرست‌نویسی: قیفا

با است: واژه‌نامه.

موضوع: هک‌ها

موضوع: شبکه‌های کامپیوتری--تدابیر ایمنی

موضوع: مپیوترها--اطلاعات

رده‌بندی کنگره: ۸۱۲ ۸۱۲۵/۵/۵۹ TK۵۱۰

رده‌بندی: ۵/۸

شماره کتابشناسی: ۳۶۴ ۹۸۵

نام کتاب: هک‌های قانونمند (CEH)

ناشر: انتشارات آترا

ناشر همکار: کانون نشر علوم

مؤلف: مهندس مجید داوری دولت آبادی

ویراستار ادبی: کانون نشر علوم

صفحه آرا: فاطمه آدیگوزل‌پور اردبیلی

طرح جلد: فاطمه ایرانی

چاپ اول: زمستان ۱۳۹۳

تیراژ: ۱۰۰۰

چاپ و صحافی: زندگی

قیمت: ۱۸۰۰۰ تومان

شابک: ۹۷۸۶۰۰۶۲۶۵۲۱۶

مراکز پخش:

نشر و پخش آترا: میدان انقلاب، خیابان جمالزاده جنوبی، کوچه شهید آقاصبوری، پلاک ۲

تلفن: ۶۶۹۲۲۰۸۲

خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد ۱

تلفن: ۶۶۹۶۱۵۶۸-۶۶۴۹۴۹۱۱



سخن ناشر

به نام خداوند بخشنده و مهربان

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

تلاش کانون نشر علوم، همواره معطوف به تولید آثار پژوهشی 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، خطم برآورده می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علوم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی، به نفع و سود 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 منوّر

کانون نشر علوم



مقدمه مؤلف

امروزه در دنیای شبکه‌های کامپیوتری و اینترنت، امنیت اطلاعات از جایگاه ویژه‌ای برخوردار است و اگر هر سازمانی و کاربری به آن توجه لازم را نداشته باشد، هر لحظه ممکن است صدمات جبران‌ناپذیری به منابع مالی و اطلاعاتی سازمان خود وارد کند. در حال حاضر تقریباً تمامی صنایع و حرفه‌ها به نوعی نیازمند امنیت اطلاعات و ایجاد مکانیزم‌هایی جهت محرمانگی آنها هستند. در حال حاضر اکثر سازمان‌ها و شرکت‌ها تاحدی به مقوله امنیت اطلاعات و شبکه‌های کامپیوتری پرداخته‌اند، اما نکته قابل توجه این است که مبحث امنیت، موضوعی نیست که با کمی محافظت و استفاده از برخی تجهیزات امنیتی بتوان آن را به‌طور کامل پیاده‌سازی کرد. زیرا امنیت کاملاً نسبی است و هر روز به ساختارهای آن اضافه می‌شود. متأسفانه برخی مدیران متوجهان شبکه، اطلاعات کافی در خصوص امن‌سازی شبکه‌ها ندارند و با دید کاملاً ابتدایی با آن برخورد می‌کنند. همین موضوع باعث می‌شود تا تمامی طراحی‌ها و پیاده‌سازی‌های آن‌ها در سطح شبکه، برنامه‌نویسی بدون در نظر گرفتن اصول و استانداردهای امنیتی صورت گیرد. به تفسیر خیلی ساده ممکن است در یک لحظه تمامی اطلاعات حساس و مهم آن‌ها تحت تأثیر مهاجمان و نرم‌افزارهای مخرب قرار گرفته و هرچه را که در طول سالیان طولانی به‌دست آورده‌اند، به یک‌باره از دست بدهند. امروزه محیط شبکه‌ها بستر مناسب و خوبی برای فعالیت و جولان نفوذگران به‌شمار می‌رود.

هدف از تألیف این کتاب در مرحله اول آشنایی بیشتر کارشناسان و متخصصان با انواع حملات و آزمایشات شاخه نفوذگری است تا آن‌ها هرچه بیشتر با اصول حملات آشنا شوند. در مرحله بعدی این کتاب قصد دارد متخصصان را با اصول و قواعد آزمایشات نفوذ و قوانین هک‌های با اخلاق آشنا نماید. در واقع روند فصل‌های این کتاب به کارشناسان و متخصصان می‌آموزد که چگونه یک آزمایش نفوذ (Penetration Test) کامل را بر روی هدف برنامه‌ریزی شده خود انجام دهند و در پایان یک گزارش کامل از آن ارائه نمایند و بتوان در مراحل بعدی جهت امن‌سازی از آن گزارشات استفاده نمود و درنهایت گزارشات مذکور را برای اهداف بعدی بایگانی نمود. یک متخصص امنیت شبکه و اطلاعات بایستی با تمامی این اصول (قوانین آزمایشات نفوذ و ساختارها و قوانین هک‌های با اخلاق) آشنا باشد و از آن‌ها در جهت امن‌سازی هرچه بیشتر بسترهای کامپیوتری و شبکه‌ای خود استفاده نماید.



در واقع این کتاب براساس دوره هکرهای قانونمند (CEH) نوشته شده است و می‌تواند به‌عنوان مرجع برای این دوره مورد استفاده قرار گیرد.

اینجانب به عنوان 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 و قوانین هکرهای بااخلاق بودم تا آن‌ها را با اصول فنی آزمایشات نفوذ آشنا آگاه سازم و بتوان از آن در دوره‌های امنیت اطلاعات و شبکه مانند CEH استفاده نمود (گرچه مدیران و متخصصین امنیت شبکه حکم اساتید اینجانب را دارند، اما به حکم وظیفه برخورد لازم هست به این آگاه سازی را انجام دهم).

شیرازه اصلی کتاب حاضر برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه امنیت داده، اصول آزمایشات نفوذ، استانداردها، امنیت اطلاعات، نفوذگری (هک)، ضدهک و دوره استاندارد CEH می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به‌فرم کاملاً آزاد از مطالب و تجربیات منوری، و دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه را با دیدم منت پذیرا هستم.

(m_Davari@TOP-co.ir)

(m_Davary@Parshack.ir)

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیز که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. برخورد لازم می‌دانم این 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.

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

در دیده من گرد تمنا مگذار

بارب در دل به غیر خود جا مگذار

رحمی رحمی مرا به من وا مگذار

گفتم گفتم ز من نمی‌آید هیچ



فهرست مطالب

۱۹	فصل اول: مروری بر هک اخلاقی گرا
۲۲	اصطلاحات ضروری
۲۲	اجزای امنیت اطلاعات (مثلث امنیتی)
۲۳	صحت و عدم انکار
۲۳	چالش های امنیتی
۲۴	تأثیرات هک و نفوذ به یک سیستم
۲۴	تأثیرات هک بر تجارت و آسیب و کار
۲۴	هکر کیست؟
۲۵	انواع هکرها و کلاس بندی آنها
۲۶	مراحل نفوذ به یک سیستم
۲۷	انواع حمله به یک سیستم کامپیوتری
۲۸	هکر اخلاقی کیست و لزوم وجودش چیست؟
۲۹	گستره و محدودیت های هک اخلاقی
۲۹	هکر اخلاقی چه کارهایی انجام می دهد؟
۲۹	مهارت های یک هکر اخلاقی
۲۹	منابع به دست آوردن آسیب پذیری ها
۳۰	معرفی سایت های منبع در زمینه معرفی آسیب پذیری های جدید
۳۰	آزمایش نفوذپذیری
۳۴	جرا آزمایش نفوذپذیری
۳۵	فصل دوم: شناسایی و جمع آوری اطلاعات
۳۶	اصطلاحات جمع آوری اطلاعات
۳۷	اهداف Footprinting
۳۷	نهیذیدات Footprinting
۳۷	روش های Footprinting
۴۶	ابزارهای تکمیلی جهت انجام عملیات Footprinting
۴۶	مقایله ب مکتبیرم جمع آوری (Footprinting)
۴۶	آزمایش نفوذ Footprinting
۴۹	فصل سوم: پوشش شبکه ها
۴۹	روش های شناسایی پوشش
۶۲	مفهوم مخفی سازها (Anonymizers)
۶۴	تکنیک IP Spoofing
۶۴	آزمایش نفوذ
۶۵	فصل چهارم: استخراج اطلاعات
۶۵	تکنیک های استخراج اطلاعات (Enumeration)
۶۵	استخراج اطلاعات از Netbios
۶۶	استخراج اطلاعات از SNMP



۶۷	استخراج اطلاعات از یونیکس و لینوکس
۶۸	استخراج اطلاعات از LDAP
۶۸	استخراج اطلاعات از NTP
۶۹	استخراج اطلاعات از SMTP
۷۰	استخراج اطلاعات از DNS Zone Transfer
۷۰	طریقه جلوگیری از مکانیزم‌های استخراج اطلاعات
۷۲	بایست نفوذ درخصوص استخراج اطلاعات
۷۲	نصل: جیم: نفوذ به سیستم هدف
۷۲	الف: هک سیستم
۷۵	تکنیک‌های هک سیستم: شکستن کلمات عبور
۷۵	انواع حملات بر علیه کلمات عبور (Password Attack)
۸۰	کلمات عبور پیچیده تر
۸۰	رمز بودن کلمات عبور: ورمیل US
۸۰	مفهوم مرکز توزیع کلید (KDC)
۸۱	تکنیک Salting
۸۱	ابزارهای درهم شکستن کلمه عبور
۸۱	چگونگی غیرفعال کردن LM Hash
۸۲	روش‌های مقابله با کشف و درهم شکسته شدن کلمات عبور
۸۲	نرم افزارهای بالا بردن سطح دسترسی
۸۲	چگونگی دفاع در برابر بالا بردن دسترسی
۸۳	مفهوم Keylogger
۸۵	معرفی انواع Keyloggerها
۸۵	جاسوس افزار (Spyware)
۸۵	طریقه انتشار جاسوس افزارها
۸۵	یک جاسوس افزار چه کارهایی را انجام می دهد؟
۸۶	انواع جاسوس افزارها
۸۸	چگونگی مقابله با Keyloggerها
۸۹	ابزارهای ضد Keylogger
۸۹	چگونگی مقابله با جاسوس افزارها
۹۰	انواع Rootkit
۹۱	Rootkit ای به نام FU
۹۱	انواع شناسایی Rootkit
۹۱	نحوه مقابله با Rootkit
۹۱	ضد Rootkitها
۹۲	خاصیت NTFS Stream
۹۲	نحوه ایجاد یک NTFS Stream
۹۳	راه‌های مقابله با خاصیت NTFS Stream
۹۳	مفهوم پنهان نگاری (Steganography)



۹۳	تکنیک‌های پنهان‌نگاری (Steganography)
۹۴	انواع پنهان‌نگاری
۹۵	مفهوم Steganalysis
۹۵	چالش‌های پیش‌روی Steganalysis
۹۶	مراحل آزمایش نفوذ در خصوص نفوذ به سیستم هدف
۹۹	فصل ششم: اسب‌های تروا و درهای پشتی
۹۹	اسب‌تروا (تروجان) چیست؟
۱۰۰	مفهوم کانال‌های (vert & covert)
۱۰۰	اهداف اسب‌تروا (تروجان)
۱۰۰	سازندگان تروجان به دنبال چه چیزی هستند؟
۱۰۰	نشانه‌های مورد حمله قرار گرفتن توسط تروجان
۱۰۱	پورت‌های معروف و مشترک اسب‌تروا شده در تروجان‌ها
۱۰۱	چگونگی الوده شدن یک سیستم با تروجان
۱۰۲	مفهوم لفافه‌بندی شده (Wrappers)
۱۰۲	راه‌های مختلف قرار دادن تروجان در یک سیستم
۱۰۳	تکنیک‌های دور زدن ضد ویروس
۱۰۳	انواع اسب‌های تروا
۱۰۹	انواع آگاهی‌رسانی
۱۰۹	اسب‌های تروا چگونه شناسایی می‌شوند؟
۱۱۰	پوشش برای شناسایی پروسیس‌های مشکوک
۱۱۰	پوشش برای شناسایی ورودی‌های مشکوک رجیتری
۱۱۱	پوشش برای شناسایی درایورهای مشکوک
۱۱۱	پوشش برای شناسایی سرویس‌های مشکوک ویندوز
۱۱۱	پوشش برای شناسایی برنامه‌های مشکوک در Startup
۱۱۲	پوشش برای شناسایی فایل‌ها و پوشه‌های مشکوک
۱۱۲	پوشش برای شناسایی فعالیت‌های مشکوک شبکه
۱۱۲	اقدامات پیشگیرانه در مقابل تروجان
۱۱۳	اقدامات پیشگیرانه در مقابل در پشتی (Backdoor)
۱۱۳	مجموعه ساخت اسب‌تروا
۱۱۳	نرم‌افزارهای ضد تروجان
۱۱۳	آزمایش نفوذ برای اسب‌های تروا و درهای پشتی
۱۱۴	مراحل آزمایش نفوذ
۱۱۴	مکانیزم ICMP Tunneling

۱۱۵	فصل هفتم: ویروس‌ها و کرم‌ها
۱۱۵	معرفی ویروس
۱۱۵	مراحل زندگی ویروس
۱۱۶	کار کردن ویروس‌ها: فاز الودگی
۱۱۶	فاز حمله



۱۱۶	چرا افراد ویروس‌های کامپیوتری ایجاد می‌کنند
۱۱۶	نشانه‌های حمله ویروس
۱۱۷	یک کامپیوتر چگونه توسط ویروس آلوده می‌شود؟
۱۱۷	ویروس Hoaxes
۱۱۷	تجزیه و تحلیل ویروس W32/Sality.AA
۱۱۹	تجزیه و تحلیل ویروس W32/Virut
۱۱۹	روش آلوده‌سازی ویروس W32/Virut
۱۱۹	تجزیه و تحلیل ویروس Kelz
۱۲۰	انواع مختلف ویروس‌ها و نحوه آلودگی آن
۱۲۴	ایجاد یک ویروس کوچک
۱۲۴	کرم‌های اینترنتی (Worm)
۱۲۴	تفاوت کرم اینترنتی و ویروس
۱۲۵	تجزیه و تحلیل برش کرم‌های اینترنتی معروف
۱۲۶	مفهوم Trojan Dip Computer
۱۲۷	ایجاد یک تحلیل‌گر ویروس
۱۲۷	مراحل تحلیل ویروس و دیگر بدافزارها
۱۲۸	اقدامات متقابل در برابر ویروس و کرم
۱۲۸	مراحل آزمایش نفوذ برای ویروس و کرم
۱۲۹	فصل هشتم: ابزارهای استراق سمع
۱۲۹	مکانیزم استراق سمع (Wiretapping)
۱۲۹	انواع استراق سمع
۱۲۹	اهداف و تهدیدات Sniffing
۱۳۰	یک ابزار استراق سمع (Sniffer) چگونه کار می‌کند؟
۱۳۱	انواع روش‌های استراق سمع
۱۳۱	تکنیک‌های استراق سمع فعال
۱۳۲	پروتنکل‌های آسیب‌پذیر در حملات استراق سمع
۱۳۲	سخت‌افزار تحلیل‌گر پروتنکل
۱۳۳	مفهوم پورت Span
۱۳۳	حملات نوع MAC Flooding
۱۳۳	MAC Flooding با استفاده از نرم‌افزار macof
۱۳۴	نحوه مقابله با حملات مبتنی بر MAC
۱۳۴	حملات مبتنی بر DHCP
۱۳۵	حملات نوع DHCP Starvation
۱۳۶	حمله سرور Rogue DHCP
۱۳۶	حملات نوع ARP Poisoning
۱۳۷	تهدیدات حمله ARP Poisoning
۱۳۷	نحوه مقابله با حملات ARP Poisoning
۱۳۸	مفهوم MAC Spoofing/Duplication



۱۳۸	تکنیک‌های DNS Poisoning
۱۳۸	مفهوم Intranet DNS Spoofing
۱۳۸	مفهوم Proxy Server DNS Spoofing
۱۳۹	DNS Cache Spoofing چیست؟
۱۳۹	نحوه مقابله با حملات نوع DNS Spoofing
۱۴۰	ابزارهای مخصوص استراق‌سمع (Sniffing)
۱۴۰	افزونه‌های Vreshark
۱۴۰	ابزارهای مخصوص شنکارسازی
۱۴۱	نقوذگر چگونه با استفاده از Snifferها شبکه را هک می‌کند؟
۱۴۱	نحوه مقابله با استراق‌سمع (Sniffing)
۱۴۲	طریقه شناسایی Sniffing
۱۴۲	ابزارهای تشخیص حالت بی‌سیم
۱۴۳	فصل نهم: مهندسی اجتماعی
۱۴۳	مهندسی اجتماعی چیست؟
۱۴۳	رفتارهای آسیب‌پذیر برای حمله
۱۴۳	فاکتورهای ایجاد یک شرکت آسیب‌پذیر برای حمله
۱۴۳	تأثیرات مهندسی اجتماعی
۱۴۴	علامت‌های خطرناک یک حمله
۱۴۴	مراحل یک حمله مهندسی اجتماعی
۱۴۴	ضربات و خسارات مهندسی اجتماعی به سازمان
۱۴۴	روش‌های نفوذ بر اساس تکنیک‌های مهندسی اجتماعی
۱۴۵	اهداف عمومی برای مهندسی اجتماعی
۱۴۵	انواع مهندسی اجتماعی
۱۴۶	انواع مهندسی اجتماعی مبتنی بر انسان
۱۴۶	مهندسی اجتماعی مبتنی بر کامپیوتر
۱۴۶	مفهوم Phishing
۱۴۷	مهندسی اجتماعی از طریق پیامک
۱۴۷	مهندسی اجتماعی توسط ارسال پیامک جعلی برای شوند پیامک دیگران
۱۴۷	حمله کارمندان داخلی
۱۴۷	روش‌های جلوگیری از تهدیدات کارمندان داخلی
۱۴۸	مهندسی اجتماعی به وسیله تقلید شخصیت در شبکه‌های اجتماعی
۱۴۸	خطرات شبکه‌های اجتماعی بر شبکه‌های شرکت
۱۴۸	اقدامات متقابل در مهندسی اجتماعی
۱۴۹	چگونگی شناسایی Phishing در نامه‌الکترونیکی
۱۴۹	اقدامات متقابل در خصوص سرقت هویت
۱۵۰	آزمایش نفوذ با مهندسی اجتماعی
۱۵۰	مهارت‌های یک آزمایش‌کننده نفوذ
۱۵۰	مراحل آزمایش نفوذ



۱۵۱	فصل دهم: حملات بر پایه عدم سرویس‌دهی
۱۵۱	حملات عدم سرویس‌دهی چیست؟
۱۵۱	حملات توزیع شده عدم سرویس‌دهی چیست؟
۱۵۲	علائم و نشانه‌های حملات نوع DoS
۱۵۲	مجرمان اینترنتی
۱۵۲	مفهوم پرس‌وجوهای گپ در اینترنت (ICQ)
۱۵۲	مفهوم گپ نه اینترنت (IRC)
۱۵۳	تکنیک‌های حملات نوع DoS
۱۵۵	بوم Botnet
۱۵۵	تکنیک‌های انتشار Botnet
۱۵۶	حملات DoS بر علیه Visa, MasterCard و Swiss Banks
۱۵۷	تکنیک‌های تشخیص حملات DoS
۱۵۷	تجزیه و تحلیل Webnet
۱۵۷	تشخیص‌های پی در پی - تیرات‌های
۱۵۷	استراتژی‌های متقابل
۱۵۸	اقدامات متقابل در مورد حملات DoS
۱۵۹	تکنیک‌های دفاعی و مقابله با Botnet‌ها
۱۶۰	اقدامات حفاظتی و پیشگیرانه در مقابل حملات DoS و DDoS
۱۶۱	محافظت در مقابل حملات DoS و DDoS در سطح ISP
۱۶۱	محافظت در مقابل حملات نوع DDoS به صورت پیشرفته
۱۶۱	ابزارهای محافظت در مقابل حملات نوع DoS/DDoS
۱۶۱	آزمایش نفوذ در خصوص حملات DoS
۱۶۵	فصل یازدهم: ربودن نشست‌ها
۱۶۵	مفهوم ربودن نشست
۱۶۵	خطرات ناشی از ربودن نشست
۱۶۵	چرا عملیات ربودن نشست‌ها معمولاً موفقیت‌آمیز است؟
۱۶۶	تکنیک‌های کلیدی ربودن نشست
۱۶۶	حملات مبتنی بر ورود به‌زور در ربودن نشست
۱۶۷	حمله جعل (Spoofing) در مقابل ربودن (Hijacking)
۱۶۷	مراحل کلی ربودن نشست
۱۶۷	انواع مبتنی بر حملات ربودن نشست
۱۶۷	ربودن نشست در مدل OSI
۱۶۸	ربودن نشست در سطح لایه کاربرد
۱۶۸	تسراق‌سمع نشست‌ها
۱۶۸	رمزهای نشست قابل پیش‌بینی
۱۶۹	حملات مبتنی بر Man-in-the-Middle
۱۶۹	حملات نوع Man-in-the-Browser
۱۷۰	حملات سمت کلاینت



۱۷۰	حملات مبتنی بر Cross-site Script
۱۷۰	نشت ثابت
۱۷۰	ربودن نشست در سطح شبکه
۱۷۱	بهره‌برداری از دست‌نکاتی سمرجله‌ای در TCP/IP
۱۷۱	پیش‌بینی ترتیب شماره
۱۷۱	ربودن نشست در TCP/IP
۱۷۲	سکانیزم IP Spoofing بهره‌گیری مسیریابی براساس مبداء بسته‌ها
۱۷۲	ربودن نشست براساس RST
۱۷۳	ربودن نشست در توران
۱۷۴	استفاده از استراق‌بص در حملات Man-in-the-Middle
۱۷۴	ربودن نشست UDP
۱۷۴	ابزارهای مخصوص ربودن نشست
۱۷۴	اقدامات متقابل کلی جهت جلوگیری از حملات ربودن نشست
۱۷۵	محافظت در مقابل ربودن نشست
۱۷۵	توصیه‌هایی جهت پیش‌گیری از ربودن نشست‌ها به مجموعه‌های وب
۱۷۵	توصیه‌هایی جهت پیش‌گیری از ربودن نشست‌ها به کاربران
۱۷۵	دفاع در مقابل حملات مبتنی بر ربودن نشست
۱۷۶	بازسازی و اصلاح حملات ربودن نشست
۱۷۶	استفاده از ساختار IPsec
۱۷۷	احراز هویت و محرمانگی در IPsec
۱۷۷	ترکیبات IPsec
۱۷۸	آزمایش نفوذ در خصوص ربودن نشست
۱۸۱	فصل دوازدهم: نفوذ به سرورهای وب
۱۸۱	معماری سرورهای وب کدباز و IIS
۱۸۱	تغییر صفحه اصلی سایت وب
۱۸۲	چرا سرورهای وب معمولاً در معرض خطر قرار می‌گیرند؟
۱۸۳	تأثیرات حملات بر علیه سرورهای وب
۱۸۳	پیگردینی نادرست سرورهای وب
۱۸۴	حملات نوع Directory Traversal
۱۸۵	حمله تکنه‌سازی پاسخ HTTP
۱۸۵	حمله مسموم‌سازی حافظه Cache سرور وب
۱۸۵	حمله ربودن پاسخ‌دهی HTTP
۱۸۶	حمله ورود به‌زور به SSH
۱۸۶	حمله نوع Man-in-the-Middle
۱۸۶	درهم شکستن کلمات عبور سرور وب
۱۸۷	تکنیک‌های درهم شکستن کلمات عبور سرور وب
۱۸۷	حملات بر علیه برنامه‌های کاربردی وب
۱۸۸	مداخله حملات مبتنی بر سرور وب
۱۸۹	استفاده از ابزارهای نفوذ به سرور وب



ناشر علوم

www.nashreloom.com

بیشکام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

۱۹۲	اقدامات متقابل: وصله‌های امنیتی و به‌روزرسانی
۱۹۳	اقدامات متقابل: پروتکل‌ها
۱۹۳	اقدامات متقابل: حساب‌های کاربری
۱۹۳	اقدامات متقابل: فایل‌ها و دایرکتوری‌ها
۱۹۴	چگونگی دفاع در مقابل حملات بر علیه سرور وب
۱۹۵	چگونگی مقابله با حملات بر علیه سرورهای وب
۱۹۶	چگونگی دفاع در برابر جداکننده پاسخ HTTP و مسموم‌سازی Cache وب
۱۹۶	مفهوم سله‌های امنیتی و Hotfix‌ها
۱۹۷	من در از مدیریت وصله‌ها
۱۹۷	شناسایی منابع: ب. برای به‌روزرسانی و وصله‌ها
۱۹۷	نصب وصله‌های امنیتی
۱۹۷	پایه‌سازی رتبه وصله‌های امنیتی و به‌روزرسانی‌ها
۱۹۸	ابزارهای مخصوص مدیریت وصله‌ها
۱۹۸	ابزارهای امنیتی برنامه‌های کاربردی
۱۹۹	آزمایش نفوذ در خصوص سرور وب
۲۰۳	فصل سیزدهم: نفوذ به برنامه‌های کاربردی وب
۲۰۳	مفاهیم برنامه‌های کاربردی تحت وب
۲۰۴	ترکیبات برنامه‌های کاربردی تحت وب
۲۰۵	برنامه‌های کاربردی Web 2.0
۲۰۶	آسیب‌پذیری پشته
۲۰۶	بردار حملات وب
۲۰۷	تهدیدات برنامه‌های کاربردی وب
۲۱۸	علم اصول نفوذ به برنامه‌های کاربردی وب
۲۲۶	ابزارهای مخصوص نفوذ به برنامه‌های کاربردی وب
۲۲۶	اقدامات متقابل در خصوص حملات به برنامه‌های کاربردی وب
۲۳۱	ابزارهای امنیتی مخصوص برنامه‌های کاربردی وب
۲۳۲	آزمایش نفوذ در خصوص برنامه‌های کاربردی وب
۲۴۵	فصل چهاردهم: حملات تزریق کد SQL
۲۴۵	مفاهیم کلی در تزریق کد SQL
۲۵۱	آزمایش تزریق کد SQL
۲۵۳	انواع حملات مبتنی بر تزریق SQL
۲۵۵	تزریق کد SQL به صورت کورکورانه
۲۵۶	متمدولوی تزریق کد SQL
۲۵۶	حملات تزریق کد SQL پیشرفته
۲۶۰	ابزارهای مخصوص تزریق کد SQL
۲۶۱	تکنیک‌ها و روش‌های گریز
۲۶۲	اقدامات متقابل در خصوص حملات تزریق کد SQL
۲۶۳	ابزارهای تشخیص حملات تزریق کد SQL



۲۶۵	فصل یازدهم: نفوذ به شبکه های بی سیم
۲۶۵	مفاهیم پایه ای در شبکه های بی سیم
۲۶۶	استانداردهای شبکه های بی سیم
۲۶۶	مفهوم SSID
۲۶۷	روش های احراز هویت Wi-Fi
۲۶۷	فرآیند احراز هویت Wi-Fi با استفاده از سرور احراز هویت مرکزی
۲۶۷	اصطلاحات شبکه های بی سیم
۲۶۸	مفهوم Chalking شبکه های Wi-Fi
۲۶۹	انواع آنتن ها در شبکه های بی سیم
۲۶۹	انواع رمزنگاری در شبکه های بی سیم
۲۷۰	رمزنگاری WEP
۲۷۱	رمزنگاری WPA چیست؟
۲۷۲	مفهوم کلیدهای زمانی
۲۷۳	رمزنگاری WPA2 چیست و چگونه کار می کند
۲۷۴	موضوعات مربوط به رمزنگاری WEP
۲۷۵	ضعف های موجود در IV
۲۷۵	طریقه درهم شکستن رمزنگاری WEP
۲۷۵	طریقه درهم شکستن رمزنگاری WPA/WPA2
۲۷۶	دفاع در مقابل درهم شکستن رمزنگاری WPA
۲۷۶	تهدیدات شبکه های بی سیم
۲۸۰	متدولوژی نفوذ به شبکه های بی سیم
۲۸۹	ابزارهای نفوذ به شبکه های بی سیم
۲۹۰	نفوذ به شبکه های مبتنی بر بلوتوث
۲۹۲	تهدیدات بلوتوث
۲۹۲	انجام عملیات BlueJack بر علیه یک سیستم
۲۹۳	اقدامات متقابل بر علیه حملات بلوتوث
۲۹۳	طریقه تشخیص و مسدود کردن نقطه دسترسی بی حفاظ
۲۹۴	دفاع در مقابل حملات بر علیه شبکه های بی سیم
۲۹۵	ابزارهای امنیتی در شبکه های بی سیم
۲۹۶	آزمایش نفوذ در خصوص شبکه های Wi-Fi
۲۹۶	چرچوب آزمایش نفوذ در شبکه های بی سیم
۲۹۸	آزمایش نفوذ شبکه های بی سیم رمز شده در حالت LEAP
۲۹۹	آزمایش نفوذ شبکه های بی سیم رمز شده در حالت WPA/WPA2
۳۰۰	آزمایش نفوذ شبکه های بی سیم رمز شده در حالت WEP
۳۰۱	آزمایش نفوذ شبکه های بی سیم رمز نشده
۳۰۳	فصل شانزدهم: فرار از سیستم های تشخیص نفوذ، دیوارهای آتش و Honeypot
۳۰۳	مفاهیم IDS، دیوار آتش و Honeypot
۳۰۳	سیستم های تشخیص نفوذ و محل استقرار آن ها



www.nashreloom.com

www.nashreloom.com

پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

۳۰۴	راههای تشخیص نفوذ
۳۰۴	انواع سیستم‌های تشخیص نفوذ
۳۰۵	نشانه‌های عمومی از نفوذ
۳۰۶	دیوارهای آتش
۳۰۶	معماری به‌کار رفته در دیوارهای آتش
۳۰۷	منظور از ناحیه DMZ
۳۰۷	نوع دیوار آتش
۳۰۸	شناسایی دیوار آتش از دیدگاه پوشش پورت
۳۰۸	شناسایی دیوار آتش از دیدگاه مکانیزم Firewalking
۳۰۹	شناسایی در اسکن از دیدگاه Banner Grabbing
۳۰۹	منظور از سیستم‌های Honeypot
۳۱۰	طریقه پیاده‌سازی یک Honeypot
۳۱۰	سیستم IDS، دیوار آتش و Honeypot
۳۱۳	فرار از سیستم IDS
۳۲۱	فرار از دیوارهای آتش
۳۲۴	فرار از سیستم‌های Honeypot
۳۲۴	ابزارهای مخصوص فرار از سیستم‌های امنیتی
۳۲۵	اقدامات متقابل درخصوص فرار از سیستم‌های امنیتی
۳۲۵	آزمایش نفوذ درخصوص دیوار آتش، IDS و سیستم‌های Honeypot
۳۳۱	فصل هفدهم: سرریزی بافر
۳۳۱	مفاهیم کلی در سرریزی بافر
۳۳۱	چرا برنامه‌های کاربردی آسیب‌پذیر هستند؟
۳۳۱	مفهوم پشته
۳۳۲	سرریزی بافر مبتنی بر پشته
۳۳۲	مفهوم Heap
۳۳۳	سرریزی بافر مبتنی بر Heap
۳۳۳	عملیات‌های پشته
۳۳۴	مفهوم Shellcode
۳۳۴	مفهوم NOPها
۳۳۴	متدولوژی سرریزی بافر
۳۳۵	مراحل پیاده‌سازی سرریزی بافر
۳۳۵	حمله به یک برنامه واقعی
۳۳۵	درهم شکستن پشته
۳۳۵	تشخیص سرریزی بافر
۳۳۶	ابزار سرریزی بافر (BOU)
۳۳۷	آزمایش شرایط سرریزی بافر (Heap (heap.exe
۳۳۷	مراحل آزمایش سرریزی بافر با کمک ابزار اشکال‌یاب OllyDbg
۳۳۸	آزمایش برای شرایط غائب رشته یا استفاده از IDA Pro



۳۳۸	ابزارهای تشخیص سرریزی بافر
۳۳۸	اقدامات متقابل در خصوص سرریزی بافر
۳۳۹	جلوگیری از اجرای داده (DEP)
۳۳۹	مفهوم EMEIT
۳۴۰	ابزارهای امنیتی در سرریزی بافر
۳۴۰	آزمایش نفوذ در خصوص سرریزی بافر
۳۴۳	فصل هجدهم: رمزنگاری
۳۴۳	مفاهیم رمزنگار
۳۴۳	انواع رمزنگاری
۳۴۳	الگوریتم‌های رمزنگاری
۳۴۴	الگوریتم رمزنگاری AES
۳۴۴	الگوریتم رمزنگاری DES
۳۴۴	الگوریتم رمزنگاری RC4, RC5 و RC6
۳۴۴	DSA و طرح‌های امضای مرتبط
۳۴۵	الگوریتم RSA
۳۴۵	نواع خلاصه پیام (Hash یک‌طرفه)
۳۴۵	تابع خلاصه پیام (MD5)
۳۴۵	الگوریتم Secure Hashing (SHA)
۳۴۵	مفهوم SSH
۳۴۶	ابزارهای رمزنگاری
۳۴۶	زیرساخت کلید عمومی (PKI)
۳۴۶	رمزنگاری پست‌الکترونیکی
۳۴۷	رمزنگاری دیسک
۳۴۷	حملات مبتنی بر رمزنگاری
۳۴۸	مندوب‌نوی شکستن کد
۳۴۸	حملات مبتنی بر ورود به‌زور
۳۴۸	حمله علاقات و بررسی در میانه راه در طرح‌های امضای دیجیتال
۳۴۹	ابزارهای رمزنگاری
۳۵۱	فصل نوزدهم: آزمایش نفوذ
۳۵۱	مفاهیم کلی در آزمایش نفوذ
۳۵۱	ارزیابی‌های امنیتی
۳۵۱	ارزیابی آسیب‌پذیری‌ها
۳۵۲	محدودیت‌های ارزیابی آسیب‌پذیری
۳۵۲	مفهوم آزمایش نفوذ
۳۵۲	چرا 'آزمایش نفوذ'؟
۳۵۳	آنچه باید مورد آزمایش قرار گیرد؟
۳۵۳	چد چیزی باعث می‌شود یک آزمایش نفوذ خوب 'بجام شود'؟



www.nashreeloom.com

www.nashreeloom.com

بینش‌نگار در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

۳۵۳	آزمایش نفوذ بر روی ROI
۳۵۳	نقاط مورد آزمایش
۳۵۴	مکان‌های آزمایش
۳۵۴	انواع آزمایشات نفوذ
۳۵۵	تکنیک‌های آزمایش نفوذ
۳۵۶	انواع آزمایش نفوذ
۳۵۸	تأثیرات آزمایش نفوذ قابل انتقال
۳۵۹	مسیر آزمایش نفوذ
۳۶۰	ارزایی امنیت: راه‌های کاربردی
۳۶۰	آزمایش نامه‌های کاربردی وب
۳۶۱	ارزیابی امنیتی شبکه
۳۶۱	ارزیابی دسترسی به راه دور و بی‌سیم
۳۶۱	ارزیابی امنیتی تلفنی
۳۶۲	مهندسی اجتماعی
۳۶۲	آزمایش تجهیزات فیلترگذاری شبکه
۳۶۲	شبیه‌سازی حملات DDoS
۳۶۲	برون‌پاری آزمایش نفوذ سرویس‌ها
۳۶۳	ابزارهای آزمایش نفوذ

۳۶۵ منابع و مراجع