بنام ایزد منان

نفوذگری
دروب
و
روشهای مقابله

www.ketab.ir

مؤلف:
مهندس مجید داوری دولت آبادی
عضو گروه امنیت GrayHat Hackers
Security Information Assets

داوری دولت آبادی، مجید، ۱۳۵۹ -
نفوذ گری دروب و روشهای مقابله/ مولف مجید داوری دولت آبادی.-- تهران : جهان نو، ۱۳۸۵ .
۶۰۸ ص.: مصور، جدول.
ISBN 964-8458-31-6
فهرست نویسی براساس اطلاعات فیپا.
۱. وب -- سایتها -- اقدامات تامینی. ۲. فکرها، الف. عنوان.
۷ن ۲د/ TK ۵۱-۵/۵۹ ۸/ ۰۰۵
کتابخانه ملی ایران ۸۵-۳۱۷۳م

نام کتاب	:	نفوذگری در وب و روشهای مقابله
مؤلف	:	مهندس مجید داوری دولت‌آبادی
ناشر	:	جهان نو
حروفنگاری	:	گروه هنری رُز ۶۶۴۹۶۲۸۵
لیتوگرافی	:	طیف‌نگار
چاپ	:	ظفر ـ دیبا
نوبت چاپ	:	اول ۱۳۸۵
تیراژ	:	۱۰۰۰
قیمت	:	۵۰۰۰۰ ریال

مراکز پخش:

نشر و پخش آیلار

انقلاب ـ خیابان شهید منیری جاوید (اردیبهشت) ـ چهارراه شهدای ژاندارمری ـ شماره ۲۲۳ (ساختمان دانشجو) طبقه اول تلفن ۶۶۴۰۱۲۵۵ دورنگار ۶۶۴۹۴۴۳۱

فروشگاه شماره ۱

انقلاب ـ روبروی دبیرخانه دانشگاه تهران ـ بازارچه کتاب، (کتاب آیلار) تلفن ۶۶۴۱۱۸۶۵

فروشگاه شماره ۲

کریمخان زند ـ مابین ایرانشهر و خردمند جنوبی ـ شماره ۱۴۴، تلفن: ۱ ـ ۸۸۳۱۹۷۴۰

شابک ۸ ـ ۳۰ ـ ۸۴۵۸ ـ ۹۶۴ ISBN: 964-8458-30-8

www.ketab.ir

فهرست مطالب

سخنی با خوانندگان ۱۸

فصل اوّل

مروری کلّی بر پروتکل HTTP و پورت ۸۰ ..... ۱۹

مقدمه ۲۰

مفهوم تور جهان گستر ۲۰

مفهوم URL ۲۱

مقدمه‌ای بر سیستم وب ۲۳

برنامه سمت سرویس دهنده وب ۲۴

پروتکل انتقال ابر متن: HTTP ۲۵

اطلاعات کلی و کلیدی در مورد URL ۲۹

کنکاش در ساختمان URL ۳۱

رمزنگاری URL ۳۳

مشخص کردن کاراکترهای مخصوص در یک رشته URL ۳۵

سوءاستفاده از روزهای URL ۳۶

آسیب پذیریهای Unicode ۳۶

آسیب پذیری رمزگشایی دوباره و یا رمزگشایی زاید ۳۷

مراجع این فصل ۳۸

فصل دوّم

مروری کلّی بر سرورهای معروف وب (IIS، Apache) ۳۹

سرور وب IIS ۴۰

سرویس دهندهٔ وب در NT: IIS 4.0 ..... ۴۱

ویژگیهای پیشرفتهٔ IIS5 ..... ۴۲

اطمینان بخشی و عملکرد در IIS ۴۲

ویژگیهای جدید در IIS5 ..... ۴۳

تهدیدهای وب با تکیه بر IIS ۴۶

برخی نقاط آسیب پذیر (حفره) در سرور وب IIS ۵۳

سیستم‌های عامل در معرض تهدید ۵۵

نحوه تشخیص آسیب پذیری سیستم ۵۵

نحوه حفاظت در مقابل نقطه آسیب پذیر ۵۵

روش مقابله ۵۶

Frontpage Server Extensions (FPSE) ۵۸

سرور وب Apache ۶۰

نصب سرویس‌دهنده Apache ۶۱

فایلهای حیاتی در پیکره بندی سرور وب Apache ۶۲

کنترل سرویس دهنده Apache ۶۳

فایل پیکربندی httpd.conf ۶۳

کنترل دسترسی‌ها در Apache ۶۷

Hosting Virtual در Apache ۶۹

فایل پیکربندی modules.conf ۷۰

www.ketab.ir

برخی نقاط آسیب پذیر (حفره) در سرور وب Apache ۷۰
سیستم‌های عامل در معرض تهدید ۷۱
نحوه حفاظت در مقابل نقطه آسیب پذیر ۷۱
امنیت در سرورهای وب ۷۴
امنیت در سرور وب IIS ۷۵
غیر فعال سازی WebDAV ۷۶
غیر فعال سازی سرویس DCOM ۷۶
حذف Application Sampleهای دیگر ۷۶
غیر فعال سازی Null NetBIOS ۷۶
غیر فعال سازی کامپوننت‌های COM ۷۷
حذف دایرکتوری مجازی IISADMPWD ۷۷
غیر فعال نمودن سرویس مسنجر ۷۷
پیکره بندی IIS با رعایت مسائل امنیتی ۷۷
معرفی برنامه Manager Service Internet(ISM) ۷۷
سرویس WWW ۷۸
روشهای تأیید اعتبار در سرورهای وب ۷۹
سرویس FTP ۸۰
Server Property Server Extensions ۸۱
تنظیمات پیشنهادی برای خصلت‌های اصلی WWW ۸۱
تنظیمات پیشنهادی برای خصلت‌های اصلی FTP ۸۲
تنظیمات پیشنهادی برای خصلت‌های اصلی Extensions Server ۸۲
امنیت در سرور وب Apache ۸۲
فرض‌های امنیتی سرور وب ۸۳
انتخاب سیستم عامل قبل از نصب سرور وب Apache ۸۳
ماژول‌های Apache ۸۳
کامپایل نمودن سرور Apache ۸۴
تنظیم نمودن سرور Apache ۸۷
روشهای پنهان سازی سرورهای وب ۹۰
Server Headerها همه چیز را می‌گویند ۹۱
استفاده از پسوند فایلها برای تشخیص سیستم عامل سرور وب ۹۱
استفاده از ASP Session ID Cookie برای تشخیص سیستم عامل سرور وب هدف ۹۱
استفاده از WebDAV برای تشخیص سیستم عامل سرور وب هدف ۹۲
بهره گیری از هدرهای مختلف برای تشخیص سیستم عامل سرور وب ۹۲
کسب اطلاعات مفید از Authentication Windows توسط نفوذگر ۹۲
شناسایی سرور وب هدف توسط پیام‌های پیش فرض ۹۲
بهره گیری از سرویسها برای شناسایی سرور وب هدف ۹۲
استفاده از ورودی‌های غیر مجاز برای کسب اطلاعات از سرور وب ۹۳
استفاده از پشته‌ها برای کشف نوع سیستم عامل سرور وب هدف ۹۳
بهره گیری از سایت Netcraft برای کسب اطلاعات از سرور وب هدف ۹۳
شناسایی سیستم عامل سرور وب هدف توسط پیش فرضهای TCP/IP ۹۳
مقایسه خدمات وب در سرورهای لینوکس و ویندوز ۹۴
مراجع این فصل ۹۵

فصل سوم
مروری کلّی بر برنامه‌های کاربردی تحت وب ۹۷
برنامه‌های کاربردی وب ۹۸
زبان نشانه گذاری ابر متن: HTML ۹۹

www.ketab.ir

تگ HTML ۱۰۰
شناسائی تگ‌های مهم در صفحات HTML ۱۰۱
تگ‌های مهم در مرورگر ۱۰۱
تکنولوژی‌ها و زبانهای، طراحی برنامه‌های کاربردی وب ۱۰۴
برنامه‌های CGI ۱۰۴
اسکریپت‌های ساده CGI ۱۰۷
امنیت و اسکریپت‌های CGI ۱۰۹
محل قرار گرفتن اسکریپت در سرور ۱۰۹
تفاوتهای GET و POST چیست؟ ۱۰۹
کنترل بیشتر با استفاده از " Non-Parsed Header Scripts ۱۱۰
زبان Perl ۱۱۰
خصوصیات Perl ۱۱۱
چگونه برنامه‌های نوشته شده به زبان Perl را اجرا کنیم ؟ ۱۱۲
پارامترهای خط فرمان برنامه Perl ۱۱۳
بررسی نکات مقدماتی در نوشتن اسکریپت Perl ۱۱۳
پلت فرمهای گسترده زبان Perl ۱۱۴
زبان جاوا اسکریپت ۱۱۴
تاریخچه جاوا اسکریپت ۱۱۴
ساختار جاوا اسکریپت ۱۱۵
تفاوتهای جاوا و جاوا اسکریپت ۱۱۵
تفاوت JavaScript و Jscript ۱۱۷
قابلیت JavaScript ۱۱۷
ابزارهای مورد نیاز برای نوشتن کد JavaScript ۱۱۸
زبان PHP ۱۱۸
قابلیتهای زبان PHP ۱۱۸
PHP چگونه کار می‌کند؟ ۱۱۹
PHP زبانی برای همه سیستم عامل‌ها ۱۲۰
نکاتی مفید در مورد تنظیم php.ini ۱۲۱
فایل پیکربندی PHP ۱۲۱
تابع ini_set ۱۲۶
تاریخچه کوتاهی از ActiveX ۱۲۷
نقاط ضعف و قوت ActiveX ۱۲۷
درک مفهوم جاوا و کنترل‌های ActiveX ۱۲۹
کنترل کردن ActiveXو برنامه‌های Java ۱۳۰
تغییر دادن درجه امنیت برنامه‌های ActiveX ۱۳۰
ActiveXو امنیت ۱۳۰
زبان ASP و ASP.NET ۱۳۱
ASP.NET چیست ؟ ۱۳۱
دات نت فریمورک ۱۳۱
تفاوت‌های ASP کلاسیک و ASP.NET ۱۳۲
امنیت در ASP.NET ۱۳۳
شناسائی و تائید کاربران در ASP.NET ۱۳۳
دستیابی از طریق کاربران ناشناس (Anonymous) درASP.NET ۱۳۳
دستیابی از طریق کاربران تائید شده در ASP.NET ۱۳۴
استفاده از Authentication در فایل‌های HTM و یا HTML ۱۳۴
اعمال محدودیت برای کاربران خاص در ASP.NET ۱۳۵
تائید کاربران بر اساس نوع وظیفه ۱۳۶

www.ketab.ir

استفاده از تنظیمات IIS به همراه Windows Authentication ۱۳۷
فعال نمودن Forms Authentication ۱۳۸
مقداردهی Mode Authentication در ASP.NET ۱۳۹
فعال نمودن روش Passport Authentication در ASP.NET ۱۴۱
تکنولوژی XML ۱۴۳
HTML SGML و XML ۱۴۳
مفاهیم اساسی XML ۱۴۳
استانداردهای خانواده بزرگ XML ۱۴۳
تعریف زبان‌های XML ۱۴۴
زبان‌های تعریف سبک XML ۱۴۵
سرویس‌های وب XML ۱۴۵
زبان ColdFusion ۱۴۶
مراجع این فصل ۱۴۷

فصل چهارم
مروری کلّی بر پایگاه‌های داده SQL Server و MySQL ۱۴۹
پایگاه داده ۱۵۰
پایگاه داده SQL Server ۱۵۱
امنیت در پایگاه‌های داده ۱۵۲
معماری امن شبکه با نگاه به پایگاه داده ۱۵۳
ارائه امن اطلاعات ۱۵۷
تولید اطلاعات به صورت استاتیک و مسائل امنیتی آن ۱۵۷
تولید اطلاعات به صورت دینامیک ۱۵۷
امنیت SQL Server 2000 ..... ۱۵۸
شناختن مدهای امنیت ۱۵۸
Authentication (تأیید اعتبار) ویندوز ۱۵۸
سطح امنیتی پایگاه داده ۱۵۹
Roles Database ۱۵۹
بررسی نقاط آسیب پذیر SQL Server و طریقه مقابله با آنها ۱۵۹
سیستم‌های عامل در معرض تهدید حفره‌های SQL Server ۱۶۲
نحوه تشخیص آسیب پذیری سیستم ۱۶۲
نحوه حفاظت در مقابل نقطه آسیب پذیر موجود در SQL Server ۱۶۲
پایگاه داده MySQL ۱۶۶
نصب و پیکربندی سرویس‌دهنده بانک اطلاعاتی MySQL ۱۶۶
نصب سرویس‌دهنده MySQL ۱۶۶
پیکربندی و مدیریت سرویس‌دهنده MySQL ۱۶۷
آشنایی بیشتر با کنسول MySQL ۱۶۸
مدیریت سرویس‌دهنده MySQL ۱۷۰
پشتیبان گیری از بانک‌های اطلاعاتی MySQL ۱۷۰
مراجع این فصل ۱۷۳

فصل پنجم
شناسایی مقدماتی شبکه هدف ۱۷۵
شناسایی مقدماتی ۱۷۶
جستجو در وب به دنبال اطلاعات و اخبار شبکهٔ هدف ۱۷۶
جستجو در سایتهای وب هدف (یک سازمان و یا موسسه) ۱۷۷
هنر استفاده از موتورهای جستجو در اینترنت ۱۷۷
بهره گیری از گروههای خبری Usenet ۱۷۸

www.ketab.ir

مقابله با شناسائی از طریق وب ۱۷۹
استفاده از بانک اطلاعاتی Whois در جهت شناسائی ۱۷۹
کسب اطلاعات در مورد نامهای حوزه با پسوند.net.com یا.org ۱۸۱
استفاده از سایت ARIN جهت تحقیق در مورد آدرس IP ۱۸۵
مقابله با جستجوی مخرّب از طریق Whois ۱۸۶
سیستم DNS ۱۸۷
تکنیکهای پرس و جو در سرویس دهنده‌های نام ۱۸۹
کسب اطلاعات از سرویس دهندهٔ DNS در راستای حمله ۱۹۰
مقابله با نشست اطلاعات حساس شبکه از طریق DNS ۱۹۳
ابزارهایی برای شناسایی مقدماتی شبکه هدف ۱۹۴
ابزار Sam Spade ۱۹۵
ابزار شناسائی شبکه مبتنی بر وب ۱۹۷
نقشه برداری از شبکه هدف ۱۹۸
Cheops: نرم افزار نقشه برداری از شبکه ۲۰۱
جلوگیری از نقشه برداری شبکه ۲۰۲
تعیین پورتهای باز بر روی سرور هدف ۲۰۳
پویش پورت با استفاده از نرم افزار Netcat (NC) ۲۰۵
جمع آوری اطلاعات کلی در مورد برنامه‌های کاربردی و پایگاه داده نصب شده در سرور وب ۲۰۶
پورت ۸۰ چیست ؟ ۲۰۷
برنامه‌های کاربردی مشتری و سرویس دهنده (Clients / Servers) ۲۱۰
arrow: HTTP:چیست ؟ ۲۱۰
arrow: resource:ها چیستند؟ ۲۱۰
arrow:: ساختار چگونگی انجام مذاکرات HTTP ۲۱۱
خطوط Header: ۲۱۳
جزئیات RFC 822در مورد خطوط Header: ۲۱۳
arrow: : الگوی انجام یک مبادله HTTP ۲۱۴
تجربه عملی با HTTP به وسیله Telnet: ۲۱۵
arrow:: روشهای دیگر HTTPمانند HEADو POST ۲۱۵
ارتباط مداوم و " : Header Connection: close" ۲۱۹
پاسخ " " 100 Continue ۲۱۹
قبول کردن URLمستقل ۲۲۰
ارتباط مداوم و استفاده از هدر" Connection: close" ۲۲۱
استفاده از عکس العمل" " 100 Continue ۲۲۱
پاسخگویی به درخواست‌های دارای If-Modified-Sinceو If-Unmodified-Since: ۲۲۲
پشتیبانی از دو روش GETو HEAD ۲۲۳
پشتیبانی کردن از درخواست‌های HTTP 1.0 ..... ۲۲۳
جستجو برای یافتن دیوارهای آتش و مسیریابها ۲۲۳
فیلترهای Stateful و هوشمند ۲۲۴
دیوار آتش مبتنی بر پراکسی (Proxy Based Firewall) ۲۲۵
بهترین پیشنهاد: استفادهٔ همزمان از هر دو نوع دیوار آتش ۲۲۵
Firewalk بر علیه Firewall ۲۲۶
مقابله با Firewalk ۲۲۹
مسیریابها (Routers) ۲۳۰
انواع مسیریابها ۲۳۰
مهمترین ویژگی‌های یک مسیریاب ۲۳۲
مسیریاب‌های سیسکو ۲۳۲
چرا مسیریاب‌های Cisco ؟ ۲۳۳

www.ketab.ir

چگونه می‌توان مسیریاب‌های Cisco را در داخل شبکه پیدا کرد؟ ۲۳۳
چگونه می‌توان به مسیریاب دسترسی پیدا کرد؟ ۲۳٤
چگونه مسیریاب را از شبکه خارج کنیم ؟ (Denial of Service) ۲۳٤
روش مقابله با نفوذ به مسیریابها ۲۳٤
برای اتصال به برنامه کاربردی و مرور صفحات وب از چه مرورگرهایی می‌توان بهره گرفت ؟ ۲۳٤
بررسی مرورگر Internet Explorer (IE) ۲۳۵
سیستم‌های عامل در معرض تهدید حفره‌های موجود در IE ۲۳۵
نحوه تشخیص آسیب پذیر ی سیستم ۲۳۵
نحوه حفاظت در مقابل نقاط آسیب پذیر مرورگر IE ۲۳٦
ایمن سازی IE ۲۳٦
عوامل تاثیر گذار در نحوه عملکرد ایمن مرورگر IE ۲۳۷
شکاف امنیتی تزریق کد به فریم در IE ۲٤۰
روش مقابله با شکاف امنیتی تزریق کد به فریم در IE ۲٤۱
بهبود قابلیت‌های امنیتی IE توسط Windows XP SP2 ..... ۲٤۱
مرورگرهای وب در لینوکس ۲٤۳
Konqueror مرورگری تنظیم پذیر ۲٤۳
FireFox مرورگری توسعه پذیر ۲٤۵
Epiphanyنماینده گنوم ۲٤۸
Dilloنماد کوچکی ۲٤۹
پیدا کردن نقاط آسیب پذیر سرورهای وب ۲۵۱
معرفی برخی از ابزارهای پویش و جستجوی نقاط آسیب پذیر ۲۵۲
مراجع این فصل ۲۵۳

فصل ششم

نفوذ در سرورهای وب تفسیر حملات (URL) ۲۵۵
حمله علیه وب سرور IIS ۲۵٦
حمله علیه مولفه‌های IIS ۲۵٦
حفره امنیتی افشاسازی منابع Translate: f ۲۵۷
روش مقابله با حفره امنیتی افشاسازی منابع Translate: f ۲۵۹
تزریق دستورات در پرس و جوهای پایگاه داده MDAC/RDS ۲۵۹
روش مقابله با تزریق دستورات در پرس و جوهای پایگاه داده MDAC/RDS ۲٦۰
حفره امنیتی Showcode.asp و Codebrws.asp ۲٦۱
روش مقابله با حفره امنیتی Showcode.asp و Codebrws.asp ۲٦۲
حفره امنیتی موجود در Null.htw ۲٦۲
حفره‌های امنیتی موجود در Webhits.dll و فایل‌های htw. ۲٦۳
روش مقابله با حفره‌ی امنیتی موجود در Webhits.dll و فایل‌های htw. ۲٦٤
حفره جریان داده متناوب (ASP Alternate Data Streams) ۲٦٤
روش مقابله با حفره جریان داده متناوب ۲٦۵
حفره امنیتی Bug DOT ASP ۲٦۵
روش مقابله حفره امنیتی ASP DOT Bug ۲٦٦
حفره امنیتی محدودسازی بافر ISM.DLL ۲٦٦
حفره‌های امنیتی موجود در IDA. و IDC. ۲٦۷
حفره امنیتی افشاسازی منابع در ISAPI DLL ۲٦۷
حفره امنیتی Adsamples در سایتهای با سرور NT ۲٦۸
راههای مقابله با حفره‌های امنیتی ISAPI DLL ۲٦۹
حمله علیه خود IIS ۲۷۳
پیمایش دایرکتوری IIS ۲۸۱

www.ketab.ir

دانلود کردن فایلها با استفاده TFTP ،FTP ،SMB ۲۸۲
استفاده از echo>file برای ایجاد کردن فایلها ۲۸۴
روش مقابله با آسیب پذیریهای موجود در پیمایش دایرکتوری IIS ۲۸۴
حفره امنیتی که باعث افشای آدرس IP داخلی IIS می‌شود ۲۸۶
روش مقابله با حفره امنیتی که باعث افشای آدرس IP داخلی IIS می‌شود ۲۸۶
حمله علیه وب سرور Apache ۲۸۷
لیست کردن دایرکتوریها بوسیله Slashهای طولانی ۲۸۷
روش مقابله با لیست کردن دایرکتوریها بوسیله Slashهای طولانی ۲۸۸
روش مقابله با Multiview ۲۸۹
تزریق mod_auth_sql ۲۸۹
نحوه تشخیص آسیب پذیریهای موجود در سرویس دهنده وب آپاچی ۲۸۹
روشهای کلی حفاظت از سرویس دهنده وب آپاچی ۲۸۹
مراجع این فصل ۲۹۳

فصل هفتم
پیمایش برنامه‌های کاربردی وب حملات صحت ورودی‌ها ۲۹۵
برنامه‌های کاربردی تحت وب ۲۹۶
باگها چه می‌توانند باشند؟ ۲۹۷
حملات Disclosure ۲۹۸
انواع Disclosureها ۲۹۸
حملات کسب آگاهی (Disclosure) چگونه صورت می‌گیرند؟ ۲۹۸
چگونه سرور خود را در برابر این حملات ایمن کنیم؟ ۲۹۹
حملات Exposure ۳۰۰
Exposure برای دریافت صفحات پویا ۳۰۰
حملات Exposureچگونه صورت می‌گیرند ؟ ۳۰۰
یک نفوذگر چگونه با استفاده از Exposureحمله می‌کند ؟ ۳۰۱
چگونه سایت خود را از این دسته حملات حفظ کنیم ؟ ۳۰۱
حمله تزریق اسکریپت ۳۰۲
حمله Cross-Sie-Scripting (CSS/XSS) ۳۰۴
به چه دلیل یک سایت نسبت به XSSآسیب پذیر است؟ ۳۰۶
حفره‌ای در برنامه تحت وب PHP-Fusion v5.01 ..... ۳۱۴
حفره‌ای در برنامه تحت وب PHPOpenChat v3.x ۳۱۵
حفره‌ای در برنامه تحت وب Chatness ۳۱۶
حفره‌ای در برنامه تحت وب YaBB ۳۱۷
حفره‌ای در برنامه تحت وب Ublog v1.0.4 ..... ۳۱۷
حفره امنیتی از نوع Cross-Site Scriptingدر برنامه Hosting Controller ۳۱۸
مقابله با حملات Cross-Site-Scripting (XSS/CSS) ۳۱۹
نفوذ از طریق حفره‌های موجود در CGI ۳۲۰
آسیب پذیری آزمون CGI ۳۲۰
عملکرد سیستم IDS در سطح کاربرد و روشهای فرار از آن ۳۲۱
حمله بر علیه IDS جهت کشف برنامه‌های CGI آسیب پذیر ۳۲۱
مکانیزمهای Whisker برای فریب دادن IDS ۳۲۲
نفوذ از طریق حفره‌های موجود در PHP ۳۲۵
نفوذ به سایت از طریق حفره امنیتی موجود در Phpnuke ۳۲۵
نفوذ به NewPHP با استفاده از SQL Injection ۳۳۲
بهره گیری از حفره‌ای مخرب در برنامه PHPRunner ۳۳۴
نفوذ به سرورهای لینوکس با استفاده از حفره Php Club ۳۳۵
بررسی حفره‌های خطرناک در سیستم‌های مدیریت محتوا ۳۳۶

www.ketab.ir

(RUNCMS , EXOOPS , CIAMOS) ۳۳۶
بهره گیری از حفره امنیتی Cpanel ۳۳۹
ایمن سازی PHP ۳۴۲
نفوذ به Forumها ۳۴۳
حفره امنیتی در ASPNuke ۳۴۴
نفوذ به برنامه کاربردی ASP با استفاده از حفره موجود در MSSQL ۳۴۵
بهره گیری از حفره‌های نرم افزار معروف ASP-Rider ۳۴۶
بهره گیری از قسمت نظردهی و ورودی ASP-Rider ۳۴۶
نفوذ به سیستم نظردهی ASP-Rider ۳۴۶
تخریب سیستم ASP-Rider ۳۴۷
بهره برداری از قسمت Admin Login در ASP-Rider ۳۴۷
روشهای مقابله با نفوذ در ASP.NET ۳۴۷
حفره‌های امنیتی موجود در Host Controller ۳۵۳
چگونگی اجرای فایلهای اجرایی از داخل صفحات HTML ۳۵۴
نفوذ به سیستم‌های کلاینت از طریق اسکریپت‌های تحت وب ۳۵۶
مراجع این فصل ۳۵۷

فصل هشتم

حمله به رویه‌های کسب مجوز حملات تزریق SQL ۳۵۹
حمله به برنامه‌های کاربردی وب بروش SQL Injection ۳۶۰
Query چیست؟ ۳۶۰
تزریق SQL در ASP بر اساس پایگاه داده SQL Server ۳۶۰
روش تشخیص آسیب پذیری SQL Injection در سایت‌ها و نحوه بهره برداری از آن ۳۶۵
بدست آوردن نام جدول و ستونهای موجود در پایگاه داده SQL ۳۶۷
استفاده از حمله Union در SQL برای کسب اطلاعات بیشتر از سرور ۳۶۸
بدست آوردن نام کاربری و کلمه عبور از جداول در پایگاه داده SQL ۳۷۰
تزریق SQL در PHP بر اساس پایگاه دادهMySQL ۳۷۴
بهره گیری از حفره SQL Injection در نرم افزار paFAQ 4 ..... ۳۷۷
روشهای مقابله در برابر حملات SQL Injection ۳۷۸
روش‌های کلی برای مقابله در برابر حملات SQL Injection ۳۷۸
اعتبار سازی ورودی‌ها ۳۷۹
مراجع این فصل ۳۸۱

فصل نهم

حمله به مکانیزم‌های احراز هویت «حمله به مشتری» ۳۸۳
مشخصهٔ نشست (Session ID) ۳۸۴
مدیریت وضعیتها؛ Cookies ۳۸۵
کوکی چیست؟ ۳۸۶
انواع کوکی ۳۸۶
چگونه می‌توان از وجود کوکیهای ماندگار روی سیستم مطلع شد؟ ۳۸۷
موارد استفاده کوکیها ۳۸۸
مزایا و معایب کوکیها از دید کاربران اینترنت ۳۸۹
مسائل امنیتی مربوط به کوکیها ۳۹۰
کار با کوکیها ۳۹۱
حملات بر علیه مشخصهٔ نشست یا Session ID ۳۹۱
حمله از نوع تعقیب نشستهای وب (Web Session Tracking) ۳۹۴
مقابله با حملات علیه Session ID ۳۹۶
ارتباط ربایی ۳۹۷

www.ketab.ir

ارتباط ربایی نوع اول ۳۹۸
ارتباط ربایی نوع دوم ۳۹۹
Phishing یا دزدی هویت ۳۹۹
Phishing چیست؟ ۳۹۹
Phishing چگونه کار می‌کند؟ ۴۰۰
پنج روش که به کاربر در محافظت از خودش در مقابل Phishing کمک می‌کند ۴۰۰
DomainKeys: اثبات هویت فرستنده‌ایمیل و حفاظت از آن ۴۰۲
استانداردسازی DomainKeys ۴۰۲
DomainKeys چگونه کار می‌کند؟ ۴۰۳
حملات Pharming ۴۰۴
حملات بر علیه کوکیها ۴۰۸
حمله به کوکیهای موقت (Persession Cookies) ۴۱۰
Cookie Snarfing ۴۱۲
Cookie Munching ۴۱۳
درو کردن حسابهای کاربری در وب (Account Harvesting) ۴۱۴
روش مبارزه با درو حسابهای کاربران وب ۴۱۵
مراجع این فصل ۴۱۵

فصل دهم

حمله به واسط مدیریت ۴۱۷
سیاست‌های دسترسی راه دور (Remote Access Policies) ۴۱۸
استفاده از Remote Access Policies ۴۱۸
اجزای یک Remote Access Policy ۴۱۸
ترتیب قرارگیری چندRemote Access Policy ۴۱۹
مدیریت سایتها از راه دور ۴۲۱
مدیریت سرور وب ۴۲۲
پورتهای مدیریت اختصاصی ۴۲۳
شبکه‌های مبتنی بر وب و مدیریت سیستم ۴۲۴
کلمات عبور پیش فرض ابزار CIM ۴۲۴
روش مقابله با کلمات عبور پیش فرض CIM ۴۲۵
دیگر محصولات مدیریت مبتنی بر وب ۴۲۶
مدیریت راه دور سیستم‌های لینوکس در حالت متنی (مدیریت از راه دور با استفاده از SSH) ۴۲۷
مراجع این فصل ۴۲۹

فصل یازدهم

حملات سرریزی پشته ـ بافر ۴۳۱
پشته چیست؟ ۴۳۲
بافر چیست؟ ۴۳۵
Heap چیست؟ ۴۳۵
سرریزی بافر چیست؟ ۴۳۶
انواع سرریزی بافر ۴۳۶
درهم شکستن وب سرور و برنامه‌های کاربردی آن از طریق سرریز کردن پشته ۴۳۶
پیدا کردن نقاط آسیب پذیر ۴۳۷
سازماندهی و آرایش بافر پیش از سرریزشدن ۴۳۸
مقابله ابتدایی با حمله به پشته از طریق سیستم IDS ۴۳۸
سرریز کردن بافر در سرور IIS (IIS Buffer Overflow) ۴۳۹
نفوذ به سرورهای IIS از طریق سرریز کردن بافر RPC ۴۴۰
سرریزی بافر در ISAPI.DLL ۴۴۴

www.ketab.ir

آسیب پذیری سرریز شدن بافر IIS Printer ٤٤٤
روش مقابله با سرریز شدن بافر IIS Printer ٤٤٨
سرریزی بافر در VSRAD، نرم افزار Frontpage Server Extensions ٤٤٨
روش مقابله با حفره موجود در VSRAD از نرم افزار FPSE ٤٤٩
سرریزی بافر در نرم افزار Compaq Insight Manager (CIM) ٤٥٠
روش مقابله با سرریزی بافر در نرم افزار CIM ٤٥١
حفره، چک نکردن بافر در ترکیب کننده‌های ویندوز (WebDAV) ٤٥١
روش مقابله با حفره چک نشدن بافر در ترکیب کننده‌های ویندوز (WebDAV) ٤٥٣
نفوذ به سرورهای وب از طریق سرریزی بافر، با استفاده از زبان اسکریپت Perl ٤٥٤
حفره سرریزی بافر در فایل PerlIIS.dll، نرم افزار ActivePerl ٤٥٧
روش مقابله با حفره سرریزی بافر در فایل PerlIIS.dll، نرم افزار ActivePerl ٤٥٧
سرریزی بافر سیستم کنترل از راه دور ColdFusion ٤٥٧
روش مقابله با سرریزی بافر سیستم کنترل از راه دور ColdFusion ٤٥٨
حفره‌ای در MS SQL با Service Patch 3 ..... ٤٥٨
روش مقابله با حفره موجود در MS SQL با Service Patch 3 ..... ٤٥٩
حفره سرریزی بافر در Microsoft Jet Database Engine ٤٦٠
سرریزی بافر در MySQL ٤٦١
سرریزی بافر، IFRAMEهای ناقص از راه دور در نرم افزار Internet Explorer ٤٦٢
روش مقابله با سرریزی بافر، IFRAMEهای ناقص در نرم افزار Internet Explorer ٤٦٢
سرریزی بافر مرورگر Opera در بارگذاری URLها ٤٦٣
سرریزی بافر از راه دور در نام حوزه مرورگرهای Mozilla/Netscape /Firefox ٤٦٤
روش مقابله با سرریزی بافر از راه دور در نام حوزه مرورگرهای Mozilla/Netscape/Firefox ٤٦٥
سرریزی بافر در تشکیلات Netscape ٤٦٥
روش مقابله با سرریزی بافر در تشکیلات Netscape ٤٦٦
سرریزی بافر در SmartDownload، مرورگر Netscape ٤٦٦
روش مقابله با سرریزی بافر در SmartDownload، نرم افزار Netscape ٤٦٧
سرریزی بافر در mod_ntlm، سرور آپاچی ٤٦٩
سرریزی بافر در Htdigest، سرور آپاچی ٤٧٠
مقابله با حملات مبتنی بر سرریزی پشته یا بافر ٤٧٠
مقابله در سطح مسئول سیستم و گروه امنیتی ٤٧٠
مقابله با سرریزشدن پشته در سطح برنامه نویسی ٤٧٢
مراجع این فصل ٤٧٣

فصل دوازدهم
حملات جعل آدرسهای وب و IP ۴۷۵
جملهٔ شماره سریال TCP/IP ٤٧٦
فریب دادن ماشینها از طریق ارسال دروغین پاسخهای DNS ٤٧٧
فریب دادن ماشینها با آدرسهای IP جعلی و دروغین(IP Spoofing) ٤٧٧
فریب ساده از طریق آدرسهای اشتباه IP ٤٧٨
فریب دادن یک ماشین با آدرسهای IP دروغین در محیط یونیکس ٤٧٨
فریب دادن یک ماشین با آدرسهای IP از طریق تکنیک Source Routing ٤٨٠
arrow:HTTP: چیست؟ ٤٨١
Referer URLها برای امنیت به کار می‌روند ٤٨٣
عبور کردن از روش امنیتی Referer ٤٨٣
جعل کردن آدرسهای درون صفحات وب ٤٨٤
روشهای مقابله در برابر جعل آدرسها ٤٨٤
جعل کردن وب ٤٨٥

www.ketab.ir

اثرات جعل کردن وب ۴۸۵
جعل کردن کل وب ۴۸۶
بازبینی فرمها و ارتباطات ایمن ۴۸۶
آغاز حمله جعل کردن وب ۴۸۶
مقابله با انواع فریبکاری متکی به آدرسهای IP جعلی ۴۸۸
راه حل‌هایی برای جلوگیری از حمله وب‌های جعلی ۴۸۹
مراجع این فصل ۴۸۹

فصل سیزدهم
حملات نوع DOS برای اخلال در سرویس‌دهی ۴۹۱
حملات DoS (عدم پذیرش سرویس) ۴۹۲
چگونگی عملکرد ویروس Blaster برای ایجاد یک حمله DOS ۴۹۳
حملات DoS علیه سرورهای وب ۴۹۶
متوقف کردن سرویس دهنده از درون ۴۹۷
روش مقابله با توقف سرویس دهنده‌ها ۴۹۸
حمله از نوع اشباع منابع سیستم ۴۹۸
روش پیشگیری از اشباع منابع سیستمی ۴۹۹
حملات DoS از بیرون ۴۹۹
حملهٔ نوع Land ۴۹۹
حملهٔ Latierra ۵۰۰
حملهٔ نوع Ping of Death ۵۰۰
حملهٔ نوع Jolt2 ..... ۵۰۰
حملهٔ نوع Teardrop ۵۰۰
حمله نوع Winnuke ۵۰۰
روش پیشگیری از حملات DoS از بیرون ۵۰۱
حمله DoS از نوع تلف کردن منابع سیستم (از راه دور) ۵۰۱
حمله نوع SYN Flood ۵۰۱
مقابله با حملات طغیان SYN (SYN Flood) ۵۰۳
حملهٔ نوع Smurf ۵۰۵
حملهٔ نوع Fraggle ۵۰۷
مقابله با حملات Smurf و Fraggle ۵۰۷
حملات DNS ۵۰۸
مقابله با حملات DNS ۵۰۸
آسیب پذیری از نوع عدم پذیرش سرویس در چند محصول عرضه شده TCP/IP و ICMP ۵۰۹
مقابله با حملات DoS در چند محصول عرضه شده TCP/IP و ICMP ۵۱۰
حملات DoS بر علیه سرور آپاچی ۵۱۰
حمله DoS بر علیه سرور وب HTTPD ۵۱۱
مقابله با حملات DoS برعلیه سرور وب HTTPD ۵۱۳
حملات DoS بر علیه Frontpage Server Extensions (FPSE) ۵۱۳
حملات DoS بر علیه برنامه‌های کاربردی تحت وب ۵۱۳
آسیب پذیری از نوع عدم پذیرش سرویس در نسخهٔ Iwebnegar 1.1 نرم افزار Iwebnegar ۵۱۳
مقابله با آسیب پذیری از نوع عدم پذیرش سرویس در نسخهٔ Iwebnegar 1.1 نرم افزارهای Iwebnegar ۵۱۵
خطای عدم سرویس دهی در Internet Explorer سیستم عامل Mac ۵۱۵
حملات توزیع شدهٔ DoS ۵۱۵
ماشینهای زامبی (Zombie) ۵۱۷
انواع حملات DDoS ۵۱۷
Trinoo ۵۱۷

www.ketab.ir

TFN/TFN2K ۵۱۸
Stacheldraht ۵۱۹
معرفی ابزارهای حملات DoS و DDoS ۵۲۰
مقابله با حملات DDoS ۵۲۰
سیاه چاله ۵۲۱
مسیریاب‌ها و دیوارهای آتش ۵۲۱
سیستم‌های کشف نفوذ (IDS) ۵۲۱
سرورها ۵۲۲
ابزار تخفیف DDoS ۵۲۲
پهنای باند زیاد ۵۲۲
چگونه از وقوع حملات DoS و یا DDoS آگاه شویم ؟ ۵۲۳
در صورت بروز یک تهاجم، چه عملیاتی را می‌بایست انجام داد ؟ ۵۲۳
مراجع این فصل ۵۲۳

ضمائم ۵۲۵
بررسی نرم افزار پویش نقاط آسیب پذیر شبکه: Retina ۵۲۶
اجزاء (Modules) ۵۲۷
Policy و تنظیم آن ۵۲۷
Force Scan ۵۲۸
Common Hacking Attack Methods (CHAM) ۵۲۸
تنظیم پورت‌ها ۵۲۸
Audits ۵۲۹
Reports ۵۳۰
Customize کردن نرم افزار Retina ۵۳۰
بررسی نرم افزار همه منظوره و قدرتمند شبکه: NetCat ۵۳۰
اتصال به یک پورت خاص و ایجاد حالت فال گوش ۵۳۱
انتقال فایل ۵۳۱
پویش پورتهای باز ۵۳۳
گرفتن اطلاعات از پورت خاص ۵۳۴
استفاده از NetCat برای برقراری ارتباط با یک پورت باز و ارسال داده ۵۳۵
جستجوی نقاط آسیب پذیر سرویس دهنده‌ها (پویش حفره) ۵۳۶
ایجاد رخنه‌های پنهان و اجرای پوستهٔ فرمان ۵۳۸
استفاده از NetCat برای ایجاد رخنه درون سیستم در حالت فعّال ۵۳۸
رله کردن ترافیک از طریق NetCat روی شبکه ۵۳۹
بررسی نرم افزار Nessus ۵۴۱
نصب نرم افزار Nessus در محیط لینوکس ۵۴۲
نکاتی راجع به Nessus ۵۴۷
بررسی نرم افزار Nmap ۵۴۸
تعیین پورتهای باز بر روی یک ماشین ۵۴۹
مکانیزمهای مختلف پویش پورت ۵۴۹
مکانیزم پویش مؤدبانه (Polite Scan) ۵۵۰
پویش مخفیانه: TCP SYN Scan ۵۵۰
پویش به روش نقص اصول پروتکل ۵۵۱
پویش به روش TCP ACK Scan ۵۵۲
پویش به روش FTP Bounce Scan ۵۵۳
بهره گیری از بسته‌های UDP ۵۵۳
عمل Ping بدون بهره گیری از ICMP ۵۵۴

www.ketab.ir

شناسائی برنامه‌های RPC نامطمئن (Remote Procedure Call) ۵۵٤
ردّ گم کردن ۵۵۵
تعیین سیستم عامل ماشین هدف با TCP Stack Fingerprinting ۵۵۵
زمانبندی صحیح و مناسب برای پویش پورتهای باز ۵۵٦
بررسی نرم افزار NMapWin ۵۵۸
بررسی ظاهر برنامه ۵۵۸
شروع کار با نرم افزار NMapWin ٥٦۰
بررسی برگه Scan از قسمت Folder Option ٥٦۰
بخش Scan Options: ٥٦۲
بررسی برگه Discover از قسمت Folder Option ٥٦۲
بررسی برگه Options از قسمت Folder Option ٥٦۳
بررسی برگه Timing از قسمت Folder Option ٥٦٥
بررسی برگه Files از قسمت Folder Option ٥٦۷
بررسی برگه Service از قسمت Folder Option ٥٦۸
بررسی برگه Win32 از قسمت Folder Option ٥٦۸
استفاده از NMapWin برای تعیین نوع سیستم عامل ٥٦۹
بررسی نرم افزار Venus ٥٦۹
Vulnerability Scanning ۵۷۰
Port Scanning ۵۷٥
IP Scanning ۵۷٥
DOS Attack ۵۷۸
مراجع این فصل ۵۷۹
ضمیمهٔ ب) شماره پورتهای معروف ۵۸۱

www.ketab.ir

سخنی با خوانندگان

امروزه تعداد سایتهای وب و برنامه‌های کاربردی آنها به سرعت در حال افزایش می‌باشد و شاید تا چند سال قبل هیچکس پیش بینی این وضعیت را نمی‌کرد. در حال حاضر تقریباً بسیاری از صنایع و حرفه‌ها از اینترنت و وب استفاده می‌کنند و خیلی از حرفه‌ها و صنایع نیز به وسیله وب ایجاد شده اند.

در این میان افرادی بسیار باهوش و تیزبین (نفوذگران)، با معلوماتی که شاید یک مهندس کامپیوتر و یا یک مدیر شبکه به ندرت با آنها آشنا باشد، نیز وجود دارند که همراه با پیشرفت علم کامپیوتر و حرفه‌ای تر شدن برنامه‌های کاربردی، آنان نیز پیشرفت فوق العاده‌ای دارند. امروزه محیط وب بستر مناسب و خوبی برای فعالیت و جولان نفوذگران بشمار می‌رود. البته نفوذگران هر چند در برخی موارد باعث بروز مشکلاتی می‌شوند امّا نمی‌توان از تلاش بعضی از آنها در گسترش و پیشرفت اینترنت و وب چشم پوشی نمود.

اینجانب به عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی به منظور افزایش آگاهی متخصصین، دانشجویان و مدیران شبکه در زمینه امنیت و شبکه بودم تا آنان را با اصول فنّی حملاتی که امنیت یک وب سایت و شبکه را تهدید می‌کند آشنا و آگاه سازم. (گرچه مدیران و متخصصین وب و امنیت شبکه حکم اساتید اینجانب را دارند امّا به حکم وظیفه برخود لازم دانستم که‌این آگاه سازی را انجام دهم.)

شالکهٔ کتاب حاضر برگرفته از کتابها و منابع معتبر و استاندارد شاخه نفوذگری (هک) و ضد هک بوده که با تجربیات اینجانب در امر شبکه و نفوذگری آمیخته شده است، که بفرم کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده است. همچنین با توجه به آشنایی با وضعیت امنیت اطلاعات و سایتهای وب در ایران، به مطالب برخی فصلها تعدادی نکات امنیتی نیز افزودم. پیشاپیش تمام کاستیهای آنرا می‌پذیرم و ضمن پوزش از اساتید، دانشجویان و مدیران عزیز، انتقادات و راهنماییهای دلسوزانه آنها را به دیده منّت پذیرا هستم.

(m_Davary@Parshack.zzn.com)

در این کتاب با توجه به مسائل امنیتی و نیز به دلیل حقیقی بودن تمام پویش‌ها، سعی شده است در مثالها از اسامی و آدرسهای فرضی استفاده گردد تا هم مثالها کاملاً واقعی و در عین حال مشکلات و خطراتی برای محتویات این آدرسها و سایتها ایجاد نشود. همچنین همانطور که اشاره شد این کتاب صرفاً برای افزایش آگاهی‌ها و رشد علمی متخصصین کامپیوتر تألیف گردیده است. در نتیجه عواقب ناشی از هر گونه سوء استفاده از مطالب این کتاب بر عهده شخص خاطی بوده و مؤلف و انتشارات هیچگونه مسئولیتی در این مورد بر عهده نخواهد گرفت.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام این کار ناچیز فشردند، تشکر می‌کنم. برخود لازم می‌دانم از زحمات بی دریغ مهندس محمد داوری دولت آبادی تشکر و قدردانی نمایم.

در پایان از مدیران فرزانه انتشارات اتحاد و ادبستان، آقایان اصغر سماک و حمید احمدی و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده اند صمیمانه قدردانی می‌نمایم.

آنان که خاک را بنظر کیمیا کنند
آیا بود که گوشهٔ چشمی بما کنند

(مجید داوری دولت آبادی – زمستان ۱۳۸۴)

www.ketab.ir