

هكر قانونمند جلد دوم

Certified Ethical
Hacker

www.ketab.ir

سرشناسه	حدادیان، امین، ۱۳۷۱ -
عنوان و نام پدیدآور	هکر قانونمند مبتنی بر EC-Council Certified Ethical Hacker v8.0 / امین حدادیان.
مشخصات نشر	اصفهان: نخبگان شریف، ۱۳۹۴
مشخصات ظاهری	ج۲: مصور(رنگی)، جدول(رنگی)، نمودار(رنگی).
شابک	ج۱: ۲-۰۰-۹۶۱۲۸-۹۶۰۰-۶۷۸-۹۷۸-۶۰۰-۹۶۱۲۸-۱-۹-۲: ج۲: ۲-۰۰-۹۶۱۲۸-۹۶۰۰-۶۷۸-۹۷۸-۶۰۰-۹۶۱۲۸-۱-۹-۲
نوع سند	فیبا
موضوع	آزمایش نفوذ (ایمن سازی کامپیوتر)
موضوع	کامپیوترها -- کنترل دستیابی
موضوع	شبکه های کامپیوتری -- تدابیر ایمنی
موضوع	هکرها
رده بندی کنگ	QAV۶/۹/ک۹ ج۳ ۱۳۹۴
رده بندی دیبی	۸/۵۰۰
شماره کتابشناسی ملی	۳۹۲۰۶۷۸



نشریات نخبگان شریف

عنوان اثر: هکر قانونمند جلد دوم

مؤلف: امین حدادیان

نوبت چاپ: اول

سال نشر: ۱۳۹۴

شمارگان: ۲۰۰۰ جلد

صفحه آرا: امین حدادیان

مسئول چاپ و نشر: مهندس محمدهادی احمدی

قیمت: ۲۵۰۰۰ تومان

ISBN: 978-600-96128-1-9

شابک: ۹۷۸-۶۰۰-۹۶۱۲۸-۱-۹-۲

شابک دوره: ۹۷۸-۶۰۰-۹۶۱۲۸-۸-۸-۲

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

اصفهان - خیابان میر - جنب پل هوایی - مجتمع تجاری پیکه - واحد شماره ۱۱

☎ ۰۳۱-۳۶۶۲۲۴۹۹

☎ ۰۳۱-۳۶۶۲۲۶۹۰

www.bamabashidlotfan.ir

☎ ۰۹۱۳ ۳۰ ۳۰۱۴۱

✉ ahmadi.mohamadhadi61@gmail.com

📍 @negin141

فهرست مطالب

۱.....	فصل یازدهم: هک وب سرور و برنامه های تحت وب
۶.....	Web Application چیست؟
۷.....	Web Application چگونه کار می کند
۸.....	پشته های آسیب پذیر یا Vulnerability Stack
۹.....	HTTP Response Splitting
۱۲.....	Web Cache Poisoning
۱۳.....	HTTP Response Hijacking
۱۴.....	SQL or RD, Brute force
۱۴.....	انواع آسیب پذیری های Web Application ها
۱۴.....	مسموم سازی کوکی
۱۴.....	Unvalidated Input
۱۴.....	Command Injection
۱۵.....	File Injection
۱۵.....	LDAP Injection
۱۶.....	SQL injection
۱۶.....	Cross-site Scripting (XSS)
۲۱.....	Parameter/Form Tampering
۲۲.....	Directory Traversal
۲۳.....	Security Misconfiguration
۲۴.....	Cross-Site Request Forgery (CSRF)
۲۴.....	Denial-of-Service (DoS)
۲۵.....	Buffer Overflow
۳۰.....	Cookie/Session Poisoning

۳۱.....	Session Fixation
۳۲.....	Improper Error Handling
۳۴.....	Insecure Cryptographic Storage
۳۴.....	Broken Authentication and Session Management
۳۴.....	Log Tampering
۳۴.....	Session Hijacking
۳۴.....	Cookie Tampering
۳۵.....	ابزارهای هک وب سرور
۳۷.....	اسکنرهای امنیت وب سایت
۳۸.....	تکنیک‌های مقابله با هک وب سرور
۳۹.....	تکنیک‌های مقابله با حملات SQL injection
۳۹.....	تکنیک‌های مقابله با حملات Command Injection
۴۰.....	تکنیک‌های مقابله با حملات XSS
۴۰.....	تکنیک‌های جلوگیری از حملات انکار سرویس
۴۰.....	توصیه‌های کلی برای جلوگیری از هک وب سرور
۴۲.....	نرم افزارهای مانیتورینگ سرور
۴۳.....	جمع بندی
۴۵.....	فصل دوازدهم حملات تزریق SQL
۴۷.....	متد HTTP POST Request چیست؟
۵۲.....	انواع SQL injection
۵۲.....	روش تست آسیب پذیری SQL injection بصورت دستی
۵۵.....	چگونه یک سایت آسیب پذیر به SQL پیدا کنیم؟
۵۶.....	روش استفاده از آسیب پذیری SQL injection به روش UNION
۵۶.....	مرحله اول: استخراج تعداد ستون‌های جدول جاری

مرحله دوم: پیدا کردن ستون آسیب پذیر	۵۷
مرحله سوم: استخراج ورژن دیتابیس	۵۸
مرحله چهارم: استخراج نام کاربر متصل به دیتابیس	۵۸
مرحله پنجم: استخراج نام دیتابیس جاری	۵۸
مرحله ششم: استخراج نام تمام دیتابیس های سیستم	۵۸
مرحله هفتم: استخراج نام تمام جدول های یک دیتابیس	۵۹
مرحله هشتم: استخراج نام تمام ستون های یک جدول	۶۱
مرحله نهم: استخراج اطلاعات موجود در یک جدول در یک دیتابیس	۶۲
تفاوت Double Query Error Based	۶۳
Blind SQL injection چیست؟	۶۴
استفاده از WAIT FOR DELAY برای تشخیص Blind SQL injection	۶۵
دور زدن سیستم احراز هویت و Login به پایت ها با SQLi	۶۹
تشخیص سطح دسترسی کاربر در SQL	۷۰
تشخیص ساختار دیتابیس	۷۰
پوشش ستون ها در دیتابیس	۷۱
طریقه ساختن حساب کاربری در DBMS	۷۲
یک تکنیک برای استخراج کلمات عبور در SQLi	۷۲
جدول های مهم در SQL	۷۳
استخراج SQL Server Hashes	۷۴
انتقال دیتابیس بر روی سیستم نفوذگر	۷۵
کار با عملگرهای سیستمی در SQL	۷۶
اکتشاف در شبکه از طریق SQLi	۷۸
ابزارهای پیاده سازی یک حمله SQLi	۷۹
چرا یک Web Application نسبت به SQLi آسیب پذیر است؟	۸۰

۸۱.....	استفاده از پارامترهای Type-Safe در برنامه نویسی برای جلوگیری از SQLi
۸۱.....	نرم افزارهای تشخیص حملات SQLi
۸۴.....	جمع بندی
۸۷.....	فصل سیزدهم تست نفوذ شبکه‌های بیسیم
۸۸.....	انواع شبکه‌های وایرلس
۸۹.....	استانداردهای شبکه‌های بیسیم
۹۲.....	Service Set Identifier (SSID) چیست؟
۹۳.....	مدهای احراز هویت Wi-Fi
۹۴.....	فرایند احراز هویت وای-فای با استفاده از یک سرور مرکزی
۹۵.....	واژه‌ها و اصطلاحات وایرلس
۹۶.....	انواع آنتنهای وایرلس
۹۷.....	انواع رمزنگاری وایرلس
۹۸.....	رمزنگاری WEP چیست؟
۹۹.....	نقش WEP در ارتباط وایرلس
۹۹.....	مهمترین دستاوردهای WEP
۹۹.....	WEP چگونه کار می‌کند؟
۱۰۰.....	WPA چیست؟
۱۰۱.....	WPA چگونه کار می‌کند؟
۱۰۲.....	نکته: کلید موقتی چیست؟
۱۰۳.....	WPA2 چیست؟
۱۰۳.....	WPA2 چگونه عمل می‌کند؟
۱۰۴.....	مقایسه پروتکل‌های WPA، WEP و WPA2
۱۰۵.....	نقص‌های WEP
۱۰۶.....	چگونه میتوان رمزنگاری WEP را رمزگشایی کرد؟

۱۰۷.....	TKIP
۱۰۸.....	AES
۱۰۸.....	تفاوت بین TKIP و AES در چیست ؟
۱۰۹.....	تهدیدات شبکه‌های وایرلس
۱۰۹.....	حملات کنترل دسترسی
۱۱۰.....	حملات یکپارچگی
۱۱۱.....	حملات مخرومانگی
۱۱۲.....	حملات دسترسی
۱۱۳.....	حملات احراز هویت
۱۱۴.....	روش هک وایرلس
۱۱۴.....	کشف وای-فای
۱۱۷.....	نقشه برداری GPS
۱۱۸.....	آنالیز ترافیک وایرلس
۱۱۹.....	Spectrum Analyses چیست ؟
۱۲۰.....	اجرای حمله وایرلس با استفاده از مجموعه Back-ng
۱۲۱.....	طریقه کشف نام SSIDهای مخفی
۱۲۱.....	طریقه اجرای یک حمله Fragmentation بر روی شبکه وایرلس
۱۲۲.....	طریقه اجرای یک حمله MAC Spoofing
۱۲۲.....	حملات DoS : Disassociation
۱۲۲.....	حملات DoS : Deauthentication
۱۲۳.....	حملات MITM
۱۲۴.....	حمله مسموم سازی ARP
۱۲۴.....	طریقه اجرای یک حمله Evil Twin یا Fake Hotspot
۱۲۵.....	کرک رمزگذاری وای-فای

- ۱۲۵..... نحوه کرک WEP با aircrack
- ۱۲۵..... نحوه کرک WPA-PSK با aircrack
- ۱۲۵..... ابزارهای کرک وایرلس
- ۱۲۶..... هک بلوتوث
- ۱۲۷..... چگونه یک قربانی را Bluejack کنیم؟
- ۱۲۸..... چگونه در برابر هک شدن بلوتوث ایمن شویم؟
- ۱۲۸..... ریفه مقابله با حملات وایرلس
- ۱۲۹..... Wi-Wi Security Addition Tool
- ۱۳۱..... جمع بندی
- ۱۳۵..... فصل چهاردهم هک موبایل
- ۱۳۷..... ریسک ها و آسیب پذیری های موبایل چه هستند؟
- ۱۳۹..... سیستم عامل Android
- ۱۴۱..... Root کردن اندروید یعنی چه؟
- ۱۴۱..... طریقه روت کردن گوشی اندرویدی
- ۱۴۲..... بررسی چند تروجان اندرویدی معروف
- ۱۴۴..... چگونه از گوشی اندرویدی خود محافظت کنیم؟
- ۱۴۶..... سیستم عامل iOS
- ۱۴۶..... Jailbreaking iOS
- ۱۴۷..... چگونه iOS خود را ایمن کنیم؟
- ۱۴۸..... Windows Phone OS
- ۱۴۹..... چگونه ویندوز فون خود را امن کنیم؟
- ۱۴۹..... سیستم عامل BlackBerry
- ۱۴۹..... تهدیدات BlackBerry
- ۱۵۲..... چگونه دستگاه بلکبری خود را ایمن کنیم؟

۱۵۲	MDM چیست؟
۱۵۳	سفارش‌های عمومی برای ایمن سازی دستگاه تلفن همراه
۱۵۴	جمع بندی
۱۵۹	فصل پانزدهم گریز IDS، Firewall و Honeypot
۱۶۰	نشانه‌ها و آثار نفوذ
۱۶۱	IDS چیست؟
۱۶۲	روش تشخیص نفوذ در IDS ها
۱۶۳	انواع سیستم های تشخیص نفوذ
۱۶۳	System Integrity Monitor (SIV) چیست؟
۱۶۴	Firewall
۱۶۵	ساختار Firewall
۱۶۶	انواع Firewall
۱۶۶	Packet Filters
۱۶۷	Circuit Level Gateways
۱۶۷	Application Level Gateways
۱۶۸	Stateful Multilayer Inspection Firewalls
۱۶۸	روش های شناسایی دیواره آتش
۱۶۸	Port Scanning
۱۶۸	Firewalking
۱۶۸	Banner Grabbing
۱۶۹	Honeypot
۱۷۰	انواع HoneyPot
۱۷۰	چگونه یک Honeypot را آماده سازی کنیم؟
۱۷۱	IDS Tool: Snort

۱۷۲.....	Snort چگونه کار می کند؟
۱۷۳.....	Snort رول های
۱۷۴.....	Rule Action
۱۷۴.....	IP Protocol
۱۷۵.....	Direction Operator
۱۷۵.....	IP Address
۱۷۵.....	Port Number
۱۷۵.....	تکنیک های IDS
۱۷۵.....	Insertion Attack
۱۷۶.....	Evasion Attack
۱۷۶.....	DoS Attack
۱۷۶.....	Obfuscation
۱۷۷.....	False Positive Generation
۱۷۷.....	درهم پیچیدن نشست یا Session Splicing
۱۷۷.....	تکنیک گریز کد کردن یا Unicode Evasion Technique
۱۷۸.....	حمله تکه تکه کردن یا Fragmentation Attack
۱۷۹.....	همپوشانی تکه ها یا Overlapping Fragments
۱۸۰.....	حمله زمان زنده بودن بسته یا Time-To-Live Attack
۱۸۱.....	Invalid RST Packets
۱۸۱.....	Urgency Flag
۱۸۲.....	شل کدهای چند ریختی یا Polymorphic Shellcode
۱۸۲.....	ASCII Shellcode
۱۸۲.....	حملات در لایه Application
۱۸۳.....	Desynchronization-Pre Connection SYN

۱۸۳.....	Desynchronization-Post Connection SYN
۱۸۳.....	رمزگذاری یا Encryption
۱۸۳.....	حمله سیل‌آسا یا Flooding
۱۸۴.....	تکنیک‌های گریز از Firewall
۱۸۴.....	IP Address Spoofing
۱۸۴.....	Source Routing
۱۸۵.....	Tiny Fragment
۱۸۵.....	دور زدن سایت‌ها - بلاک شده با استفاده از قراردادن آیپی سایت در URL
۱۸۵.....	دور زدن سایت‌ها - بلاک شده با استفاده از وب سایت‌های ناشناس کننده‌ی گشت و گذار
۱۸۶.....	دور زدن Firewall با استفاده از Proxy Server
۱۸۶.....	دور زدن Firewall با استفاده از ICMP Tunneling
۱۸۶.....	دور زدن Firewall با استفاده از ACK Tunneling
۱۸۶.....	دور زدن Firewall با استفاده از HTTP Tunneling
۱۸۶.....	دور زدن Firewall با استفاده از سیستم‌های تاراج
۱۸۷.....	دور زدن Firewall با استفاده از MITM
۱۸۸.....	ابزارهای گریز از Firewall
۱۸۹.....	طریقه دور زدن WAF در SQLi
۱۹۴.....	تکنیک‌های تشخیص Honeypot
۱۹۵.....	فصل شانزدهم Buffer Overflow
۱۹۸.....	چرا برنامه‌ها آسیب پذیری سرریز بافر دارند؟
۱۹۸.....	حافظه Stack چیست؟
۲۰۰.....	چند حالت نامطلوب پشته و صف
۲۰۰.....	سرریز بافر مبتنی بر پشته
۲۰۱.....	Heap چیست؟

۲۰۱		سرریز بافر مبتنی بر Heap
۲۰۲		Format String Problem
۲۰۲		درهم شکستن بسته
۲۰۳		مثال هایی از Buffer Overflow
۲۰۸		مراحل Buffer Overflow
۲۰۸		طریقه پیدا کردن آسیب پذیری Buffer Overflow
۲۰۹		انتهای یافتن آسیب پذیری سرریز بافر در برنامه های تحت وب
۲۱۱		Null byte چیست ؟
۲۱۱		چگونه Null byte ها را از بین ببریم ؟
۲۱۱		طریقه مقابله با سرریز بافر
۲۱۳		جمع بندی
۲۱۵		فصل هفدهم رمز نگاری
۲۱۶		انواع رمز گذاری
۲۱۷		شیوه های پایه رمز نگاری
۲۱۹		الگوریتم رمز نگاری DES
۲۲۰		استاندارد پیشرفته رمز نگاری یا AES
۲۲۰		تفاوت DES و AES چیست ؟
۲۲۱		استانداردهای رمز نگاری RC
۲۲۱		RC4
۲۲۲		RC5
۲۲۳		RC6
۲۲۳		امضای دیجیتال چیست ؟
۲۲۴		الگوریتم رمز نگاری RSA
۲۲۴		Hash چیست ؟

۲۲۵.....	MD5
۲۲۶.....	SHA
۲۲۶.....	SSH چیست؟
۲۲۷.....	ابزارهای رمزگذاری اطلاعات
۲۲۷.....	PKI چیست؟
۲۲۹.....	پروتکل امنیتی SSL چیست؟
۲۳۰.....	ملاحظات یک ارتباط مبتنی بر پروتکل امنیتی SSL
۲۳۰.....	مکانیزم‌ها، نشانه‌ها، هشده SSL
۲۳۰.....	اجزای پروتکل SSL
۲۳۱.....	الگوریتم‌های رمزگذاری پشته شده در SSL
۲۳۱.....	نحوه عملکرد داخلی پروتکل SSL
۲۳۴.....	پروتکل امنیتی TLS چیست؟
۲۳۵.....	رمزگذاری دیسک
۲۳۶.....	ابزارهای پنهان نگاری
۲۳۷.....	جمع بندی
۲۴۵.....	ضمائم
۲۴۶.....	ضمیمه ۱ : Server Security Checklist (2009 Standard)
۲۵۱.....	منابع

سخنی با خوانندگان

امروزه کمتر کسی را می‌توان یافت که اطلاعاتی برای ازدست رفتن نداشته باشد. همه ما در معرض ازدست رفتن اطلاعاتی هستیم که ممکن است به‌دست آوردن آنها دیگر امکان‌پذیر نباشد. از سوی دیگر نوع دیگری از دزدی و ناامنی در محیط‌های کاری رواج یافته است که ریشه در گسترش فناوری اطلاعات و ارتباطات و آسیب‌های همراه آن دارد. آن ناامنی، اطلاعاتی است که در گذشته‌های دور بارزترین مصداق آن دانستن جای کلید گاو صندوق بزرگانی بود که گنجینه‌های نهفته در آن داشتند، اما امروز همه افراد گنجینه‌های گوناگون را در اختیار دارند و معمولاً امکان دسترسی به آنها از سوی افراد مختلف امکان‌پذیر است. حوزه‌ای که آن بعد از زندگی را تحت پوشش قرار می‌دهد، امنیت فناوری اطلاعات است. بدون شک مهم‌ترین مقوله در امنیت فناوری اطلاعات آگاهی است، در صورتی که همه ما از جوانب مختلف امنیت اطلاعات و یا ناامنی اطلاعات آگاه باشیم، کمتر دچار ضرر و زیان می‌شویم. دردناک‌ترین بعد ناامنی اطلاعات زمانی است که اطلاعات دیده شده تنها اطلاعات فردی و شخصی نیست، بلکه مربوط به گروهی از افراد یک سازمان و حتی یک کشور است که امکان خرابکاری یا مقیاس بزرگتر را فراهم می‌کند. ساده‌ترین و موثرترین راه برای دستیابی به آگاهی، آموزش است. بنابراین آموزش امنیت اطلاعات یکی از مهم‌ترین مباحثی است که باید در سراسر فردی، سازمانی و ملی به آن پرداخته شود.

امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات است که باهدف تضمین استمرار فعالیت‌های کاری به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن بازدهی سرمایه‌گذاری‌ها و فرصت‌ها صورت می‌گیرد که طبق این دیدگاه امنیت اطلاعات تأثیر مثبتی بر روند سازمان دارد. از منظری دیگر امنیت فناوری اطلاعات کنترلی را به‌عنوان تداوم حفاظت از دارایی‌های سازمان از آسیب یا ازدست دادن معنا شده است. به عبارت دیگر امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای آن در بخش‌های غیر مجاز اشاره دارد که مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت و جاسوسی و خرابکاری است. امنیت اطلاعات تنها به تمامی سازمان‌ها را در سراسر دنیا به خود جلب کرده است. با توجه به این‌که اقتصاد و کسب و کار مدرن برای بقا بطور کامل به فناوری اطلاعات وابسته‌اند، نیاز به حفاظت از اطلاعات از قبل بیش‌تر می‌شود.

از آن‌جا که تقریباً همه جنبه‌های زندگی ما به وسیله ابزارها، روبه‌ها و تکنولوژی تحت کنترل قرار گرفته‌اند این موارد اهمیتی فزاینده یافته که اثرات گسترده فناوری الکترونیک نقاط ضعف و اجزای محرمات را نیز درک کرده است.

هر سازمان برای رسیدن به سطح قابل قبولی از امنیت بایستی تمام عوامل مؤثر در امنیت را در نظر بگیرد و لازم به ذکر است که عدم توجه مناسب به تمام عوامل در بیش‌تر مواقع سایر تمهیدات امنیتی را بی‌اثر می‌کند.

اولین قدم برای اینکه بتوان یک شبکه را امن کرد، شناخت انواع حملات و تهدیدها است. فراموش نکنید کسی در برقراری امنیت موفق تر است که خود مانند هکرها فکر کند.

منبع اصلی این کتاب، مجموعه کتب آموزشی CEH V8.0 است که که از سوی شرکت EC-Council به عنوان مرجع اصلی برای آزمون‌های بین المللی معرفی شده است. لذا این کتاب برای کسانی که تمایل دارند در آزمون بین المللی ۵۰-۳۱۲ شرکت EC-Council شرکت کنند مناسب خواهد بود. همچنین این کتاب برای خود خوانی (Self Study) مناسب است اما توصیه می‌شود در کنار کلاس‌های آموزشی از آن استفاده گردد.

از آنجایی که پیشنهاد دوره CEH، تسلط بر مبانی شبکه و نیز مبانی امنیت شبکه است، در تألیف این کتاب نیز فرض بر آن گرفته شده است که شما خواننده گرامی دوره‌های Network+ و Security+ شرکت EC-Council و دیدارهای معادل آنها در شرکت Cisco را گذرانده اید. به دلیل تخصصی بودن مطالب، در نگارش این کتاب تلاش شده است تا از ادبیاتی ساده، روان و قابل فهم استفاده شود. از آنجایی که برگرداندن بسیاری از اصطلاحات و مفاهیم انگلیسی هک و امنیت به معادل آنها در فارسی، معنا و مفهوم آنها را دچار دگرگونی می‌سازد، در اغلب موارد اصطلاحات انگلیسی به جای معادل (برگردان) فارسی آنها استفاده شده است؛ لذا خواننده این کتاب می‌بایست حتماً دوره Security+ را گذرانده باشد و یا به درک قابل قبولی از مفاهیم شبکه و امنیت و هک رسیده باشد. همچنین به دلیل فهم ساده‌تر برخی مطالب از طریق شکل‌ها، تلاش شده تا آنها را به صورت مصور توضیح داده و از آوردن توضیحات اضافی خودداری شود.

قابل ذکر است کلیه مطالب این کتاب صرفاً جنبه آموزشی دارد و مسئولیت هرگونه سوء استفاده از ابزارهای معرفی شده در آن، بر عهده شخص استفاده کننده می‌باشد.
بی‌صبرانه منتظر دریافت نظرات، پیشنهادات و انتقادات شما هستیم. در صورت یافتن هرگونه مشکل نگارشی و یا علمی لطفاً اینجانب را در جریان بگذارید.

e-mail: info@DE3.com
Web-site: www.DE3.ir
Cyber Security & Protection Services

و من آن توفیق