

هكر قانونمند جلد اول

Certified Ethical
Hacker

www.ketab.ir

سرشناسه	حدادیان، امین، ۱۳۷۱ -
عنوان و نام پدیدآور	هکر قانونمند مبتنی بر EC-Council Certified Ethical Hacker
مشخصات نشر	۷۸.۰ / امین حدادیان.
مشخصات ظاهری	اصفهان: نخبگان شریف، ۱۳۹۴
شابک	ج۲: مصور(رنگی)، جدول(رنگی)، نمودار(رنگی).
وضعیت فهرست نویسی	ج۱: ۲-۹۶۱۲۸-۰۰-۶۰۰-۹۷۸-۰۰-۹۶۱۲۸-۱-۹-۲: ج۲: ۹۷۸-۶۰۰-۹۶۱۲۸-۰۰-۶۰۰-۹۷۸-۰۰-۹۶۱۲۸-۱-۹-۲
موضوع	فیبا
موضوع	آزمایش نفوذ (ایمن سازی کامپیوتر)
موضوع	کامپیوترها -- کنترل دستیابی
موضوع	شبکه های کامپیوتری -- تدابیر ایمنی
موضوع	هکرها
رده بندی کنگره	QAY۶/۹: ج۳ ۱۳۹۴
رده بندی دی	۸۵۰۰ :
شماره کتابخانه ملی	۳۹۲۰۶۷۸:



عنوان اثر: هکر قانونمند جلد اول

مؤلف: امین حدادیان

نوبت چاپ: اول

سال نشر: ۱۳۹۴

شمارگان: ۲۰۰۰ جلد

صفحه آرا: امین حدادیان

مسئول چاپ و نشر: مهندس محمدهادی خمای

قیمت: ۲۵۰۰۰ تومان

ISBN: 978-600-96128-0-2

شابک: ۲-۰-۹۶۱۲۸-۰۰-۶۰۰-۹۷۸

شابک دوره: ۸-۸-۹۶۱۲۸-۰۰-۶۰۰-۹۷۸

* 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 پگاه - واحد شماره ۱۱

☎ ۰۳۱-۳۶۶۲۲۴۹۹

☎ ۰۳۱-۳۶۶۲۲۶۹۰

www.bamabashidlotfan.ir

☎ ۰۹۱۳ ۳۰۳۰۱۴۱

✉ ahmadi.mohamadhadi61@gmail.com

⬇ @negin141

فهرست مطالب

- ۲..... فصل اول مقدمه‌ای بر هک قانونمند
- ۳..... CEH چیست؟
- ۴..... مقدمه بر هک قانونمند
- ۵..... اهداف هک چیست؟
- ۵..... انواع هکرها
- ۶..... تست نفوذ چیست؟
- ۶..... انواع تست
- ۷..... مراحل تست نفوذ
- ۹..... واژگان فنی
- ۱۲..... Exploit چیست؟
- ۱۳..... هک و فازهای پیاده سازی آن
- ۱۵..... انواع حملات
- ۱۷..... فصل دوم جمع‌آوری اطلاعات
- ۱۸..... Footprinting چیست؟
- ۱۸..... راهکارهای Footprinting
- ۱۹..... جمع‌آوری اطلاعات با استفاده از موتورهای جستجو
- ۱۹..... جمع‌آوری اطلاعات با استفاده از گوگل (Google Hacking)
- ۲۲..... جمع‌آوری اطلاعات در مورد اشخاص
- ۲۳..... ردیابی قربانی در شبکه‌های اجتماعی
- ۲۴..... جمع‌آوری اطلاعات با استفاده از وب سایت‌ها و Whois Lookup
- ۲۸..... جمع‌آوری اطلاعات با استفاده از ایمیل

۳۰	جمع‌آوری اطلاعات هوشمندی رقابتی
۳۰	جمع‌آوری اطلاعات با استفاده از DNS
۳۲	جمع‌آوری اطلاعات با استفاده از مهندسی اجتماعی
۳۲	ابزارهای جمع‌آوری اطلاعات در شبکه
۳۴	استفاده از دستور Whois
۳۵	استفاده از دستور Ping برای تعیین سیستم عامل مورد استفاده در هدف
۳۶	روش‌های جلوگیری از جمع‌آوری اطلاعات توسط هکرها
۳۷	فصل سوم اسکن شبکه
۳۸	اسکن شبکه (Network Scanning)
۴۴	پورت اسکن
۴۴	پرچم‌های بسته‌های TCP
۴۵	احراز هویت سه گانه در پروتکل TCP
۴۷	اسکن پورت‌های TCP
۴۹	انواع روش پورت اسکن
۴۹	UDP Scan
۴۹	Full Open Scan (TCP connect)
۵۰	Half-Open Scan (SYN Stealth Scan)
۵۰	FIN Scan
۵۰	ACK Flag Scanning
۵۱	Xmas Scan
۵۱	Null Scan
۵۲	IDLE Scan
۵۵	انجام اسکن به روش Idle
۵۶	طریقه پیدا کردن زامبی توسط nmap

۵۶	روش انجام Idle Scan در Hping
۵۸	تشخیص آسیب پذیری های موجود بر روی سیستم ها
۵۹	استفاده از Proxy برای مخفی ماندن هویت
۶۱	HTTP Tunneling
۶۱	IP Spoofing
۶۲	Enumeration
۶۳	Null Session چیست؟
۶۳	مقابله با Null Session
۶۴	SNMP Enumeration چیست؟
۶۵	مقابله با SNMP Enumeration
۶۶	جمع بندی
۶۷	فصل چهارم هک سیستم
۶۸	انواع حملات کلمه عبور
۷۰	دزدیدن کلمات عبور از طریق USB Drive
۷۱	کرک کردن رمز سیستم عامل ویندوز
۷۳	کرک رمز ویندوز با استفاده از فایل SAM
۷۹	حذف رمز ورود به ویندوز از طریق CMD
۷۹	هدایت SMB Logon به حمله کننده
۷۹	حملات SMB Relay MITM و مقابله با آن
۸۰	راهکارهای مقابله با Password Cracking
۸۱	افزایش سطح دسترسی
۸۲	اجرای نرم افزارها
۸۳	Keylogger ها
۸۵	Spyware

۸۵.....	روش‌های مقابله با Spyware و Keylogger
۸۶.....	مخفی کردن فایل‌ها با استفاده از Rootkit
۸۶.....	۳ گام برای تشخیص روتکیت:
۸۷.....	قرار دادن یک تروجان در فایل متنی
۸۸.....	Steganography چیست؟
۸۹.....	پاک کردن ردپا
۹۰.....	جمع بندی
۹۲.....	فصل پنجم: تروجان‌ها و Backdoor
۹۴.....	اهداف تروجان‌ها
۹۴.....	نشانه‌های حمله یک تروجان
۹۵.....	سیستم‌ها چگونه با تروجان‌ها برخورد می‌کنند
۹۶.....	استفاده از تکنیک بسته بندی کردن در تروجان‌ها
۹۷.....	تروجان چگونه گسترش می‌یابد؟
۹۸.....	تکنیک تروجان‌ها برای فرار از آنتی‌ویروس
۹۹.....	انواع تروجان
۹۹.....	تروجان‌های Command Shell
۹۹.....	تروجان‌های گرافیکی
۹۹.....	Document Trojans یا تروجان‌هایی که به مستندات متصل می‌شوند
۱۰۰.....	Emails Trojan یا تروجان‌های ایمیلی
۱۰۱.....	Defacement Trojans تروجان‌های تغییر ظاهر
۱۰۱.....	Botnet Trojans یا تروجان‌های بات‌نت
۱۰۱.....	Proxy Server Trojans یا تروجان‌های پروکسی سرور
۱۰۲.....	FTP Trojans
۱۰۲.....	VNC Trojans

۱۰۲.....	HTTP(S) Trojans
۱۰۳.....	SHTTTPD Trojan – HTTPS (SSL)
۱۰۴.....	ICMP Tunneling چیست ؟
۱۰۵.....	Remote Access Trojans چیست ؟
۱۰۵.....	Banking Trojan Analysis
۱۰۶.....	E-Banking Trojans چه هستند ؟
۱۰۸.....	M4st3r Trojan یا تروجانهای تخریب کننده
۱۰۸.....	Notification Trojans
۱۰۹.....	Data Hiding Trojans (Encrypted Trojans)
۱۰۹.....	تحلیل چند تروجان مخفی
۱۰۹.....	Flame
۱۰۹.....	Spyeye
۱۱۰.....	Zeroaccess
۱۱۰.....	OS X Trojan: Crisis
۱۱۲.....	طریقه تشخیص تروجان
۱۱۳.....	اسکن پورت ها
۱۱۵.....	اسکن پردازش ها
۱۱۵.....	اسکن کلیدهای مشکوک رجیستری
۱۱۵.....	اسکن برنامه‌های راه‌اندازی سخت افزارها (Device Drivers)
۱۱۶.....	اسکن سرویس‌های در حال اجرا
۱۱۶.....	اسکن برنامه‌های موجود در Startup سیستم
۱۱۷.....	اسکن فایل‌ها و پوشه‌های مشکوک در سیستم
۱۱۸.....	کنترل ارتباطات ورودی و خروجی سیستم
۱۱۹.....	اقدامات متقابل در برابر تروجان

۱۲۱	فصل ششم ویروس‌ها و کرم‌ها
۱۲۲	سیستم کاری ویروس : مرحله آلوده سازی
۱۲۳	سیستم کاری ویروس : مرحله حمله
۱۲۳	نشانه‌های ویروسی شدن سیستم
۱۲۴	تکنیک‌های رایج برای توزیع بدافزارها در سطح وب
۱۲۵	ویروس های گول زننده و آنتی‌ویروس‌های جعلی
۱۲۵	خلیا ویروس معروف Dnschanger
۱۲۶	تقسیم بندی ویروس‌ها بر لحاظ زمینه کاری
۱۲۸	انواع ویروس‌ها بر لحاظ روش آلوده سازی
۱۳۱	طریقه نوشتن یک ویروس ساده
۱۳۲	کرم‌های کامپیوتری (Computer Worm)
۱۳۲	تفاوت‌های کرم کامپیوتری با ویروس کامپیوتری
۱۳۳	تحلیل کرم معروف Stuxnet
۱۳۴	Sheep DIP چیست؟
۱۳۵	Antivirus چیست؟
۱۳۵	روش آنالیز بدافزار
۱۳۶	راه کارهای مقابله با ویروس‌ها و کرم‌ها
۱۳۹	فصل هفتم شنود در شبکه
۱۴۱	پروتکل‌های آسیب پذیر در مقابل شنود
۱۴۲	شنودگرهای سخت افزاری
۱۴۲	SPAN Port چیست؟
۱۴۳	حملات مربوط به مک آدرس (MAC Attacks)
۱۴۷	حملات MAC Flooding
۱۴۷	DHCP Attacks

۱۴۹.....	حملات قحطی DHCP یا (DHCP Starvation)
۱۵۰.....	حملات ARP Poisoning یا مسموم سازی ARP
۱۵۱.....	انواع حملات ARP Spoofing (ARP Poisoning)
۱۵۱.....	حمله ARP Spoofing بر روی رایانه
۱۵۲.....	حمله ARP Spoofing بر روی روتر یا سوئیچ
۱۵۳.....	حمله ARP Spoofing دوجانبه (بر روی سیستم کاربر و روتر)
۱۵۴.....	Spoofing Attack
۱۵۴.....	MAC Spoofing / Duplicating
۱۵۵.....	IP Spoofing چیست؟
۱۵۶.....	حملات مسموم سازی DNS (DNS Poisoning)
۱۵۷.....	Intranet DNS Spoofing (Local Network)
۱۵۸.....	Internet DNS Spoofing (Remote Network)
۱۵۸.....	Proxy Server DNS Poisoning
۱۵۹.....	DNS Cache Poisoning
۱۵۹.....	ابزارهای شنود اطلاعات
۱۶۴.....	روش‌های جلوگیری از حملات Sniffing
۱۶۴.....	تکنیک‌های تشخیص Sniffing در شبکه
۱۶۵.....	تکنیک Ping برای تشخیص شنود
۱۶۵.....	تکنیک ARP برای تشخیص شنود
۱۶۷.....	تکنیک DNS برای تشخیص شنود
۱۶۷.....	استفاده از nmap برای تشخیص شنودگر در شبکه
۱۶۹.....	جمع بندی
۱۷۳.....	فصل هشتم مهندسی اجتماعی
۱۷۵.....	Kevin David Mitnick کیست؟

۱۷۶	 مراحل انجام یک حمله مهندسی اجتماعی
۱۷۶	 انواع حمله‌های مهندسی اجتماعی
۱۷۶	 مهندسی اجتماعی مبتنی بر انسان
۱۷۷	 Impersonation جعل هویت یا
۱۷۸	 روش‌های فیزیکی
۱۷۸	 مهندسی اجتماعی معکوس
۱۷۹	 Identity Theft سرقت هویت
۱۷۹	 مهندسی اجتماعی مبتنی بر کامپیوتر
۱۸۰	 Phishing Attacks حملات فیشینگ
۱۸۰	 Spear Phishing فیشینگ هدفمند یا
۱۸۱	 طرز شناسایی ایمیل‌های فیشینگ
۱۸۱	 ابزارهای مقابله با فیشینگ
۱۸۱	 جعل هویت در شبکه‌های اجتماعی
۱۸۱	 مهندسی اجتماعی مبتنی بر تلفن همراه
۱۸۴	 Insider Attacks حمله از داخل (حمله از سمت کارمندان خودی)
۱۸۵	 نحوه پیشگیری از حملات مهندسی اجتماعی
۱۸۷	 جمع بندی
۱۸۹	 فصل نهم حملات انکار سرویس
۱۹۱	 تکنیک‌های پیاده سازی حملات DoS
۱۹۴	 Botnet چیست؟
۱۹۵	 معرفی چند تروجان باتنت
۱۹۶	 ابزارهای پیاده سازی یک حمله DoS
۱۹۹	 اجرای یک حمله DoS با استفاده از Ping
۱۹۹	 اجرای یک حمله DoS با استفاده از nmap

۱۹۹.....	اجرای یک حمله DoS با استفاده از hping3
۱۹۹.....	اقدامات متقابل در زمان وقوع یک حمله DoS
۲۰۰.....	تکنیک‌های شناسایی و مقابله با عوامل اجرایی یک DoS
۲۰۱.....	نرم افزارهای مقابله با DoS
۲۰۲.....	روش‌های جلوگیری از وقوع DoS
۲۰۴.....	تکنیک‌های مقابله با Botnet
۲۰۵.....	جمع‌بندی
۲۰۷.....	فصل دهم ربات‌نشست
۲۰۸.....	چرا دزدی نشست خطا نیست؟
۲۰۸.....	چرا دزدی نشست بسیار ساده است؟
۲۰۹.....	تکنیک‌های پیدا کردن شماره نشست
۲۰۹.....	استفاده از حملات Brute Force برای پیدا کردن شناسه نشست
۲۱۰.....	حمله ارجاع هدرهای HTTP یا HTTP Referrer Attack چیست؟
۲۱۱.....	مقایسه حملات Spoofing و Hijacking
۲۱۲.....	فرایند اجرای Session Hijacking
۲۱۳.....	انواع دزدی نشست
۲۱۳.....	انواع Session Hijacking در مدل OSI
۲۱۴.....	Application Level Session Hijacking
۲۱۴.....	شنود Session
۲۱۵.....	پیش‌بینی Session Token
۲۱۶.....	حملات Man-In-The-Middle
۲۱۶.....	حملات Man-In-The-Browser
۲۱۸.....	حملات Client-Side (کدهای آلوده جاوا اسکریپت، XSS، تروجان و ...)
۲۱۸.....	Network Level Session Hijacking

۲۲۲.....	TCP/IP Hijacking
۲۲۳.....	RST Hijacking
۲۲۳.....	Blind Hijacking
۲۲۴.....	MITM:Packet Sniffer
۲۲۴.....	UDP Hijacking
۲۲۴.....	معرفی و شرح Cookie hijacking و راه‌های مقابله با آن
۲۲۴.....	چیست؟ Cookie hijacking
۲۲۵.....	روش‌های Cookie Hijacking
۲۲۶.....	راه‌های جلوگیری و مقابله با Cookie hijacking
۲۲۷.....	ابزارهای پیاده‌سازی یک حمله Session Hijacking
۲۲۹.....	دفاع در برابر سرقت نشست (Session Hijacking)
۲۳۰.....	چیست؟ IPSec
۲۳۲.....	معماری IPSec
۲۳۳.....	احراز هویت و محرمانگی در IPSec
۲۳۴.....	عناصر تشکیل دهنده IPSec
۲۳۴.....	پیاده‌سازی IPSec
۲۳۶.....	جمع‌بندی
۲۳۹.....	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 بازرترین مصداق آن دانستن جای کد گاو صندوق بزرگانی بود که گنجینه‌های نهفته در آن داشتند، اما امروز همه افراد گنجینه‌های گوناگون را اختیار دارند و معمولاً امکان دسترسی به آنها از سوی افراد مختلف امکان‌پذیر است. حوزه‌ای که این 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 ناامنی‌های اطلاعات آگاه باشیم، کمتر دچار ضرر و زیان می‌شویم. دردناک‌ترین بعد ناامنی اطلاعات زمانی است که اطلاعات را ندیده‌اند 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 سطح فردی، سازمانی و ملی به آن پرداخته شود.

امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طرف 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 برای تضمین باووم حفاظت از دارایی‌های سازمان از آسیب یا ازدست دادن معنا شده است. به عبارت دیگر امنیت اطلاعات حفاظت از اطلاعات و به حداقل رساندن خطر افشای آن در بخش‌های غیر مجاز اشاره دارد که معمولاً از ابزارها برای جلوگیری از سرقت، حمله، جنایت و جاسوسی و خرابکاری است. امنیت اطلاعات توجه حامی 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، رویه‌ها و تکنولوژی تحت کنترل قرار گرفته‌اند این موارد اهمیتی فزاینده یافته که اثرات گسترده فناوری الکترونیک نقاط ضعف و اجزای محرومانه 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 متناسب به تمام عوامل در بیش‌تر مواقع سایر تمهیدات امنیتی را بی‌اثر می‌کند.

منبع اصلی این کتاب، مجموعه کتب آموزشی CEH V8.0 است که از سوی شرکت EC-Council به عنوان مرجع اصلی برای آزمون‌های بین‌المللی معرفی شده است. لذا این کتاب برلی کسانی که تمایل دارند در آزمون بین‌المللی 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 پیشنیاز 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 یا دوره‌های 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 سیارات از اصطلاحات و مفاهیم انگلیسی هک و امنیت به معادل آنها در فارسی، معنا و مفهوم آنها را دچار دگرگونی می‌ساخت، 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، امنیت و هک رسیده باشد. همچنین به دلیل فهم ساده‌تر برخی مطالب از طریق شکل‌ها، تلاش شده تا آنها را بصورت مصور توضیح داده و از آوردن توضیحات اضافی خودداری شود.

قابل ذکر است کلیه مطالب این کتاب صرفاً به 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 عزیزان هستیم. در صورت یافتن هرگونه مشکل نگارشی و یا علمی لطفاً اینجانب را در جریان بگذارید.

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

ومن الله التوفیق