

هکر قانونمند

www.ketab.ir

مؤلف:

مادی علیرزاده

چشم‌دانش

سرشناسه: عابدزاده، هادی، ۱۳۷۴

عنوان و نام پدیدآور: هکر قانونمند/مؤلف هادی عابدزاده

مشخصات نشر: تهران: حریم دانش، ۱۳۹۵.

مشخصات ظاهری: ۲۶۴ ص. مقصور

شابک: ۹۷۸-۶۰۰-۸۲۹۷-۰۸-۶

وضعیت فهرست نویسی: فیا

موضوع: هک - شبکه‌های کامپیوتری - تدابیر ایمنی - ایمنی اطلاعات

موضوع: Computer security -- Security measures -- Computer networks -- Hackers

رده‌بندی کنگر: ۳۹۵/۷۰۸/۵۹/۵۱/۵ TK5۱۰۵

رده‌بندی دیویی: ۰۸۸

شماره کتابشناسی ملی: ۲۲۰۰۲۰۰۰

عنوان کتاب: هکر قانونمند

مؤلف: هادی عابدزاده

ناشر: حریم دانش

نوبت چاپ: اول ۱۳۹۵

قیمت: ۳۰۰,۰۰۰ ریال

تیراژ: ۱۰۰۰ جلد

شابک: ۹۷۸-۶۰۰-۸۲۹۷-۰۸-۶

کلیه حقوق چاپ و نشر برای انتشارات حریم دانش و مؤلف محفوظ می‌باشد.

مرکز پخش: میدان انقلاب، ضلع جنوب شرقی میدان انقلاب، پلاک ۱۱ جدید، کتابفروشی

گلریزان. تلفن: ۰۹۱۲۳۴۶۰۸۵۹ - ۶۶۹۷۶۲۳۰

جهت خرید این کتاب می‌توانید به سایت انتشارات (HarimeDanesh.ir) نیز مراجعه نمایید.

پیشگفتار

با توجه به رشد فراوان علم و فن آوری در دنیا، به نظر میرسد امنیت در سیستم های رایانه ای روز به روز برجسته تر می شود. در این میان، یکی از دغدغه های اساسی سازمان ها، ایمن سازی ساختار رایانه ای و امن کردن آنها در مقابل خطرات خارجی است. کتابی که پیش رو دارید حاصل تجربیات چندین ساله اینجانب است که سعی شده ارائه و انتقال مطالب با زبان و لحنی شفاف، ساد و صریح بیان شود. در این نوشتار با جدیدترین تکنولوژی ها در حوزه امن سازی شبکه های کامپیوتری آشنا خواهید شد و می توانید از این مطالب برای تست میزان امنیت سیستم های خود و در عین حال ایمن کردن آنها استفاده کنید.

ممکن است این کتاب دارای ایراد فنی یا نگارشی باشد. لذا از شما دانشجویان عزیز خواهشمندیم نظرات و پیشنهادات خود را با ما در میان بگذارید تا در ویرایش های آتی اصلاح گردد.

فهرست مطالب

۵	 پیشگفتار
۲۳	 مقدمه
۲۳	 هک به چه معناست؟
۲۳	 توضیح و تاریخچه هک
۲۵	 مدرک CEH چیست؟
۲۶	 برخی از مدارک شرکت EC-Council
۲۶	 آموزش تست نفوذ یا Penetration Testing؟
۲۶	 Ethical Hacking چیست؟
۲۷	 امتحانات بین المللی CEH v9
۲۷	 از دوره CEH چه چیزهایی یاد می گیریم؟
۲۷	 افراد خرابکار
۲۷	 هکر قانونمند
۲۸	 گزارش رخنه های امنیتی
۲۹	 فصل اول: مقدمه هک قانونمند
۳۰	 هکرها و کلاهپوشان
۳۰	 هکر کلاه سفید
۳۰	 هکر کلاه سیاه
۳۰	 هکر کلاه خاکستری
۳۱	 هکر اخلاقی
۳۱	 هکر نخبه
۳۱	 بچه اسکریپتی

۳۲		نوب
۳۲		هکر کلاه آبی
۳۲		هکتیویسم
۳۲		مراحل هک
۳۳		مهارت های یک هکر اخلاقی
۳۳		دانش پلتفرم ها
۳۳		دانش شبکه
۳۳		متخصصان کلاه سفید
۳۳		دانش فنی
۳۴		فعالیت های هکر قانونمند بعد از بستن قرارداد با سازمان
۳۴		انواع حملات قانونمند
۳۴		شبکه راه دور Remotly
۳۴		شبکه محلی
۳۴		مهندسی اجتماعی
۳۵		انواع تست نفوذ
۳۵		جعبه سیاه
۳۵		جعبه خاکسری
۳۵		جعبه سفید
۳۵		Vulnerability چیست؟
۳۶		Vulnerability ها را چگونه نام گذاری می کنند؟
۳۸		چرا سازمان ها درخواست Penetration Testing می دهند؟
۳۹		مثلث امنیت

۴۱	فصل دوم: روش‌های جمع آوری اطلاعات از هدف و شناسایی و دنبال کردن ردپاها
۴۲	Footprinting چیست؟
۴۳	اینترنت Footprinting
۴۳	بیرون کشیدن اطلاعات مفید سایت
۴۴	فوت پرینت با استفاده از موتورهای جست‌وجو
۴۴	DNS Footprinting
۴۵	Whois footprinting چیست؟
۴۶	DNSstuff و DNSLookup
۴۶	DnsLookup
۴۷	Network footprinting
۴۷	نحوه اسکن شبکه
۴۸	ابزارهای Traceroute
۴۸	WebSite Footprinting
۴۸	Email Footprinting
۴۹	کاربردها و نقش‌های Email Tracking
۴۹	Google Hacking شناسایی هدف توسط سرچ گوگل
۵۰	Dork چه دردی می‌خورد؟
۵۱	روش‌هایی جلوگیری از Footprinting
۵۲	فواید Footprint
۵۲	مراحل Footprinting
۵۳	فصل سوم: اسکن در سطح شبکه
۵۴	اسکن پورت
۵۵	Nmap چیست؟

۵۷	 اسکن شبکه
۵۷	 اسکن آسیب‌پذیری‌ها
۵۷	 ICMP های
۵۸	 مقابله با اسکن پورت
۵۹	 ۳ نمونه اسکن‌های آی‌پی پورت
۵۹	 تشخیص پینگ
۶۰	 علت استفاده از Proxy چیست؟
۶۱	 فصل چهارم: سرشماری سیستم‌های شبکه
۶۲	 روش‌های دست‌یابی به اطلاعات از طریق Enumerated
۶۳	 NetBIOS Enumeration
۶۴	 اقدامات برای جلوگیری از SNMP Enumeration
۶۵	 LDAP Enumeration
۶۵	 NTP Enumeration
۶۶	 SMTP Enumeration
۶۹	 SMB چیست؟
۷۱	 فصل پنجم: سیستم هکینگ
۷۲	 اهداف هک سیستم
۷۳	 شکستن پسورد (Password Cracking)
۷۳	 انواع پسوردها
۷۴	 تکنیک‌های شکستن پسورد
۷۴	 انواع حملات پسورد PassPassive Online Attack
۷۵	 Active Online Attack

۷۶		پسوردهای پیش فرض
۷۶		دزدیدن پسوردها به وسیله USB
۷۷		احراز هویت در ویندوز
۷۷		تکنیک Salting
۷۷		ابزارهای کرک پسورد
۷۸		Privilege Escalating
۷۸		ایجاد یک حساب کاربری مدیر به صورت مخفی
۷۸		ایجاد دسترسی در دامین
۷۹		فصل ششم: بدافزارها
۸۰		آسیب پذیری Back Door ادرستی چیست؟
۸۱		چگونه می توان از دستگاه خبر در باب Back Door ها محافظت نمود؟
۸۱		Server Hacking
۸۲		Client Hacking
۸۲		ویروس چیست؟
۸۲		اولین ویروس دنیا و ویروس نویس
۸۳		مراحل زندگی یک ویروس
۸۴		نشانه های حمله ویروس
۸۴		کامپیوتر چگونه توسط ویروس آلوده می شود؟
۸۵		انواع مختلف ویروس ها و نحوه آلودگی آن
۸۵		System Or Boot Sector Viruses
۸۵		Macro Viruses
۸۵		Cluster Viruses
۸۶		Stealt/Tunneling Viruses

۸۶	Encryption Viruses
۸۶	Polymorphic Code
۸۶	Worm
۸۷	تفاوت worm و ویروس
۸۷	مراحل تحلیل ویروس
۸۸	اقدامات متقابل در برابر ویروس و Worm
۸۸	مراحل تست نفوذ برای ویروس و Worm
۸۹	Spyware یا سوس افزار
۹۰	طریقه انتشار سوس افزارها
۹۰	یک جاسوس افزار چگونه کار می کند؟
۹۰	Desktop Spyware
۹۱	USB Spyware
۹۱	Print Spyware
۹۱	Rootkit
۹۱	Password Cracking
۹۲	Privilege Escalation
۹۳	FileStealer چیست؟
۹۳	Stealer یا سندر چیست؟
۹۴	RAT
۹۴	کیلاگر
۹۴	متاسیولیت چیست؟
۹۴	تروجان چیست؟
۹۵	تروجان کنترل دسترسی

۹۵	تروجان مخرب.....
۹۶	تروجان‌های پروکسی.....
۹۶	تروجان‌های FTP.....
۹۶	تروجان مخرب نرم‌افزارهای امنیتی.....
۹۶	اهداف تروجان‌ها.....
۹۷	ارسال ایمیل.....
۹۷	Botnet Trojan.....
۹۸	تروجان‌های چگونه شناسایی می‌شوند؟.....
۹۹	اقدامات پیشگیرانه در برابر تروجان.....
۹۹	تست نفوذ برای تروجان و backdoor.....
۱۰۱	فصل هفتم: حملات مرد میانی.....
۱۰۳	نرم‌افزار اول wireShark.....
۱۰۵	امکانات.....
۱۰۵	ابزار دوم Cain.....
۱۰۶	اهداف Sniffing.....
۱۰۶	ARP Poisoning.....
۱۰۶	Password Sniffing Tool.....
۱۰۷	نفوذگر چگونه با استفاده از Sniffer ها شبکه را هک می‌کند؟.....
۱۰۹	فصل هشتم: مهندسی اجتماعی.....
۱۱۰	مهندسی اجتماعی چیست؟.....
۱۱۰	انواع حمله‌های مهندسی اجتماعی.....
۱۱۱	مهندسی اجتماعی مبتنی بر انسان.....

۱۱۱	تقلید صدای یک کارمند یا یک کاربر مورد تایید
۱۱۱	وانمود کردن بعنوان یک شخص مهم
۱۱۲	استفاده از سوم شخص
۱۱۲	تماس پشتیبانی فنی
۱۱۲	مشاهده پسورد از روی دست
۱۱۲	استفاده از زباله دان
۱۱۳	مهندسی اجتماعی مبتنی بر کامپیوتر
۱۱۳	Insider Attacks حمله از داخل (حمله از سمت کارمندان خودی)
۱۱۴	Identity Theft سرقت هویت
۱۱۴	Fishing Attacks حملات فیشینگ
۱۱۴	Online Scams کلاهبرداری آنلاین
۱۱۵	گزارش سرور ایمیل
۱۱۵	URL Obfuscation مبهم کردن آدرس
۱۱۷	اقدام های متقابل در برابر مهندسی اجتماعی
۱۱۹	فصل نهم: حملات تکذیب پذیر و مختل کردن سیستم ها
۱۲۰	تفاوت داس و دیداس
۱۲۰	داس
۱۲۰	دیداس
۱۲۱	بررسی انواع حملات DOS
۱۲۱	حمله SYN flood
۱۲۲	حمله Reset یا RST
۱۲۳	حمله Land Attack
۱۲۴	حمله Smurf Attack

۱۲۵	Ping of death یا Ping Flood	حمله
۱۲۶	Teardrop	حملات
۱۲۶	DDoS	بررسی حملات عدم سرویس دهی توزیع شده
۱۲۸	Trinoo	حملات
۱۲۹	Kr TFN/TFN	حملات
۱۳۰	Stacheldraht	حملات
۱۳۱		فصل دهم: دیدن جلسات کاربری
۱۳۲	(Session) چیست؟	نشست
۱۳۲	(Session side jacking)	استراق سمع
۱۳۳		تثبیت نشست
۱۳۶		در پس زمینه، چه اتفاقی می افتد؟
۱۳۷	XSS	انواع آسیب پذیری
۱۳۷	Reflected(non-persistent)	
۱۳۸	Persistent(Stored)	
۱۳۹		فصل یازدهم: وب سرور هکینگ
۱۴۲		چند نمونه آسیب پذیری های تحت سرور:
۱۴۴	Shellshock	آسیب پذیری
۱۴۶	Glibc	چیست؟
۱۴۸		علت حمله به وب سرور چیست؟
۱۴۸		چرا به سرور نفوذ میکنند؟
۱۴۹		چطور از یک پشت بام به پشت بام دیگری برویم؟
۱۴۹		لوکال روت

۱۵۰	 چیست؟ Htaccess
۱۵۰	 چیست؟ Php.ini
۱۵۳	 فصل دوازدهم: وب اپلیکیشن هکینگ
۱۵۶	 آسیب پذیری وب چیست؟
۱۵۹	 فصل سیزدهم: حملات تزریق پایگاه داده
۱۶۰	 پایگاه داده چیست؟
۱۶۰	 فرمها و اعتبار آنها
۱۶۱	 بررسی اشتباه کاربرها و فرآر
۱۶۲	 تزریق SQL کور
۱۶۲	 تزریق SQL سطح دوم
۱۶۳	 نحوه جلوگیری از باگ SQL Injection
۱۶۴	 امنیت اضافی
۱۶۵	 فصل چهاردهم: شناسایی شبکه های بیسیم
۱۶۶	 اهمیت رمزنگاری ها در چیست؟
۱۶۷	 امنیت وای فای در گذشته
۱۶۷	 پروتکل چیست؟
۱۶۷	 پروتکل های
۱۷۰	 دسته بندی شبکه های بی سیم
۱۷۱	 دسته بندی شبکه های بی سیم از لحاظ گستردگی
۱۷۱	 الگوریتم های امنیتی وای فای
۱۷۱	 کلید های WPA ۲
۱۷۲	 WPA ۲ چگونه عمل میکند؟

۱۷۳	بروت فورس (Brute Force) چیست؟
۱۷۴	پروتکل WEP
۱۷۴	مشکلات امنیتی WEP شامل موارد زیر است:
۱۷۶	حمله های شناخته شده روی WEP
۱۷۶	نقص های WEP
۱۷۷	حمله های مردی در میانه
۱۷۷	بدافزار
۱۷۸	اسنیفینگ و ابزارهای
۱۷۸	جاسوسی به طریق نکران کدهای آسان است
۱۷۹	چگونه از خود محافظت کنیم؟
۱۸۰	به کمک سرویس VPN از خود محافظت کنید
۱۸۲	محرمانگی معادل سیمی (Wired Equivalent Privacy)
۱۸۲	دسترسی وای فای محافظت شده (Wi-Fi Protected Access)
۱۸۳	دسترسی وای فای محافظت شده ۲ (Wi-Fi Protected Access II)
۱۸۵	ابزارها
۱۸۵	Aircrack-ng
۱۸۵	Airdecap-ng
۱۸۶	Airmon-ng
۱۸۶	Airplay-ng
۱۸۶	Airodump-ng
۱۸۷	Airtun-ng
۱۸۷	Airolib-ng
۱۸۸	Packetforg-ng

۱۸۹	Airbase-ng
۱۹۰	Airdecloak-ng
۱۹۲	Airdriver-ng
۱۹۲	Airserv-ng
۱۹۳	Easside-ng
۱۹۴	Buddy-ng
۱۹۵	Tkipm-ng
۱۹۵	Wesside-ng
۱۹۷	فصل پانزدهم: حملات سرریز بافر
۱۹۸	بافر اورفلو
۲۰۰	انواع پشته از دید آدرس دهی در نظر
۲۰۱	انواع پشته از دید ماهیت
۲۰۲	انواع پشته از لحاظ استفاده از SP
۲۰۸	استاتیک
۲۰۸	دینامیک
۲۰۸	هیب (Heap) چیست؟
۲۰۹	انواع هیب
۲۰۹	آدرس بازگشت
۲۱۰	فرآیند؟
۲۱۲	سازماندهی فضای آدرس دهی توسط ویندوز
۲۱۳	خلاصه

۲۱۵	فصل شانزدهم: دیوار آتش، سیستم تشخیص نفوذ
۲۱۶	فایروال (Firewall) چیست؟
۲۱۷	فایروال چگونه کار می‌کند؟
۲۱۷	انواع فایروال:
۲۱۸	دیوار آتش لایه شبکه یا فیلتر بسته‌ها (Network layer or packet filters)
۲۱۸	فایروال لایه کاربرد (Application firewall)
۲۱۹	فایروال‌های پروکسی (Proxies)
۲۲۰	فایروال سخت‌افزاری و نرم‌افزاری:
۲۲۰	فایروال‌های نرم‌افزاری:
۲۲۱	فایروال‌های سخت‌افزاری:
۲۲۲	سیستم‌های تشخیص نفوذ:
۲۲۷	علائم نفوذ:
۲۲۹	موارد غیر معمول - علامت نفوذ:
۲۳۰	چه باید کرد؟
۲۳۱	ظرف عمل:
۲۳۵	معایب استفاده از Honeypot
۲۳۷	فصل هفدهم: رایانش ابری
۲۳۸	رایانش ابری چیست؟
۲۳۸	تعریف رایانش ابری:
۲۳۹	ویژگی‌های اساسی:
۲۴۰	شکل‌های ارائه:
۲۴۱	شکل‌های آماده‌سازی:
۲۴۲	امنیت:

- ۲۴۲ آینده ی این فناوری چیست؟
- ۲۴۴ آیا قابل اطمینان است؟
- ۲۴۵ فصل هجدهم: کریپتوگرافی یا رمزنگاری
- ۲۴۶ رمزنگاری چیست؟
- ۲۴۸ چرا رمزنگاری؟
- ۲۴۸ محرمانگی
- ۲۴۸ تمامیت
- ۲۴۹ تأیید هویت
- ۲۴۹ شیوه های پایه رمزنگاری
- ۲۵۱ رمزنگاری جایگزینی (substitution)
- ۲۵۵ سیستم های رمزنگاری با کلید عمومی
- ۲۵۷ حمله های فعال
- ۲۵۸ استگانوگرافی
- ۲۶۲ Steganography در ویدئو
- ۲۶۲ نتیجه گیری

مقدمه

هک به چه معناست؟

استفاده از مجموعه روش‌هایی جهت دسترسی، غیر مجاز روی سیستم‌ها هک نام دارد، که بسته به نقطه ضعف سیستم روش‌های هک متفاوت است و بدیهی است که به فردی که از این امکانات استفاده می‌کند هکر گفته می‌شود.

توضیح و تاریخچه هک

اولین هک کردن تاریخ (البته اون چیزی که در تاریخ ثبت شده و اگر نه هک قبل از اینها هم بوده) مربوط بوده به هک کردن تلفن و برقراری ارتباط با انگلیس بوده که مربوط است به یک دامپزشک ویتنامی که در سال ۱۹۷۱ با یکسری ابزار ساده و اولیه اقدام به برقراری تماس رایگان آن‌ها از راه دور می‌کرده و چون اینکار جواب می‌دهد خیلی از افراد این روش را یاد گرفته و انجام می‌دهند تا جایی که یک سال بعد استیو وزنیاک و استیو جابز (سازندگان شرکت اپل) که در آن زمان هم کلاسی بودن اقدام به ساخت و فروش این دستگاه برای تماس تلویزیونی رایگان می‌کنند. اما اولین هک و گروه هک کامپیوتری طبق مستندات تاریخی توسط باشگاه آشپز کامپیوتری (در سال ۱۹۷۸ و در آلمان به وجود می‌آید).

در سال ۱۹۸۴ با زیاد شدن هک و هکرها مجلس سنا قانون دستبرد و تقلب کامپیوتری را تصویب و بر طبق آن نفوذ غیر قانونی به سیستم‌های کامپیوتری یک جرم شناخته می‌شود. در سال ۱۹۸۸ کوین میتنیک بزرگترین هکری که دنیا، شروع به کنترل پیام‌های الکترونیکی MCI، مرکز محاسبات عددی مقام‌های رسمی امنیتی می‌کند و باعث خسارت ۴ میلیون دلاری

در آن زمان و دزدیدن یک ابر کامپیوتر و دستیابی به کدهای امنیتی آن از طریق کامپیوترهای دانشگاه لس آنجلس و انگلستان می‌شود. پلیس اینترپل پس از چند ماه تلاش بالاخره کوین را پیدا می‌کند، کوین حدود ۵ ماه را در زندان و ۶ ماه را هم در یک بخش بازپروری سپری می‌کند و حتی ۲ سال او را از دست زدن به کیبورد و موس قدغن می‌کنن.

هک قانونمند به چه معناست؟ شاید از خود پرسید که آیا هک هم می‌تواند قانونمند باشد؟ برای توضیح پاسخ یک جمله کافیست: برای اینکه بتوانید پلیس خوبی باشید باید راه‌های دزدی را یاد بگیرید. برای آنکه بتوانید از دارایی‌های اطلاعاتی خود حفاظت کنید باید راه‌های نفوذ به اطلاعات و دسترسی غیر مجاز به آن‌ها را یاد بگیرید و راهکارهای پیشگیرانه خود را در مقابل اینگونه حملات اعمال کنید. در کتاب هک قانونمند شما یاد می‌گیرید که چگونه هک کنید، اما آن را در راه صلح آمیز استفاده می‌کنید، ایرادش این است که شرکت‌ها یا سازمان‌هایی که داده‌های ارزشمند دارند به شما مبلغی را پرداخت خواهند کرد و طی قراردادی از شما می‌خواهند که به آن‌ها حمله هکری کنید و در انتها به آن‌ها نقاط ضعف امنیتی‌شان را متذکر شده و به آن‌ها راهکار تدافعی ارائه کنید.

در دوره هک قانونمند شما با ابزارهای هک آشنا خواهید شد و با آن‌ها کار خواهید کرد، در حقیقت این دوره مفاهیم پایه و اساسی امنیت تهاجمی و انواع حملات را به شما آموزش خواهد داد، شما در این دوره Toolkit یا جعبه ابزار خود را خواهید ساخت و برای اینکه بتوانید یک تست نفوذ سنج یا یک هکر قانونمند بهتر باشید باید دوره‌های پیشرفته‌تری را بگذرانید. CEH به شما آموزش نمی‌دهد که چگونه شبکه یا سیستم خود را ایمن کنید بلکه به شما نفوذ در سیستم و شبکه را آموزش خواهد داد.