

هکر قانون مند

تهیه و تألیف:

محمد حسین محمدی

سید یحیی مرادی

میلاد صیام پور

www.ketab.ir

سرشناسه	محمدی، محمدحسین، ۱۳۷۶-
عنوان و نام پدیدآور	Mohammadi, Mohammad Hossein هکر قانونمند/تهیه و تألیف محمدحسین محمدی ، سید یحیی مرادی ، میلاد صیامپور.
مشخصات نشر	تهران: آرنا، ۱۴۰۰.
مشخصات ظاهری	۲۷۱ص.
شابک	978-622-291-040-2
وضعیت فهرست نویسی	فیا
یادداشت	کتابنامه: ص. ۲۷۱.
موضوع	هکرها
موضوع	Hackers
موضوع	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	Computer networks -- Security measures
شناسه افزوده	مرادی، سیدیحیی، ۱۳۷۱ -
شناسه افزوده	Moradi, Seyed Yahya
شناسه افزوده	صیامپور، میلاد، ۱۳۷۵-
رده بندی کنگره	۶۶۸HM
رده بندی دیویی	N/۰۰۵
شماره کتابشناسی ملی	۷۶۵۱۹۳۹
اطلاعات رکورد کتابشناسی	فیا



عنوان	هکر قانون مند :
تهیه و تألیف	محمد حسین محمدی- سید یحیی مرادی- میلاد صیام پور :
ناشر	آرنا :
طرح جلد	محمد حسین محمدی :
چاپ	اول ۱۴۰۰ :
شمارگان	۵۰۰ نسخه : قیمت: ۹۰۰۰۰ تومان
شابک	۹۷۸-۶۲۲-۲۹۱-۰۴۰-۲ :

www.arnapub.com

مقدمه

یکی از معروف ترین و کاربردی ترین مدارک امنیت، مدرک CEH یا مدرک تخصصی هکرهاى قانونمند است. مدرک CEH، مدرکى امنیتی به منظور ارزیابی مهارت افراد در برقراری امنیت سیستمها و شبکه های سازمانی و نیز کمک به آنها جهت مقابله با حملات و نفوذهای هکرها است. در این دوره افراد با تکنیک ها و روش های هک و نیز چک لیست های امنیتی آشنا شده و قادر به بررسی وضعیت امنیتی سیستمها و شبکه ها خواهند بود تا نقاط ضعف آنها را شناسایی و برطرف سازند.

کتابی که پیش رو دارید ترجمه کتاب رسمی CEH و نیز اسلایدهای آموزشی مربوط به این مدرک، و نیز برخی از تجارب شخصی مؤلفان است. سعی شده است تا جاییکه امکان دارد متن کتاب روان باشد تا هدف اصلی آن که انتقال مطلب است، به درستی برآورده شود.

فهرست مطالب

۲۱	مقدمه ای بر هک قانون مند
۲۱	۱-۱- مقدمه
۲۱	۱-۲- واژگان فنی
۲۳	۱-۳- انواع مختلف تکنولوژی های هک
۲۴	۱-۴- پنج مرحله مختلف هک قانونمند
۲۴	۱-۴-۱- شناسایی پسیو و اکتیو
۲۵	۱-۴-۲- اسکین
۲۶	۱-۴-۳- ایجاد دسترسی
۲۶	۱-۴-۴- حفظ دسترسی
۲۶	۱-۴-۵- از بین بردن رد پا
۲۷	۱-۵- Hacktivism چیست؟
۲۷	۱-۶- انواع هکرها
۲۷	۱-۶-۱- کلاه سفید ها
۲۷	۱-۶-۲- کلاه سیاه ها
۲۷	۱-۶-۳- کلاه خاکستری ها
۲۸	۱-۷- هکرها ی قانونمند و cracker ها کیستند؟
۲۸	۱-۸- اهداف حمله کننده
۳۰	۱-۹- مثلث امنیت، عملکرد، و راحتی استفاده
۳۱	۱-۱۰- تحقیق آسیب پذیری چیست؟
۳۱	۱-۱۱- روش های اجرای هک قانونمند

۳۲	۱-۱۲- برنامه ارزیابی امنیتی
۳۲	۱-۱۳- انواع حملات قانونمند
۳۳	۱-۱۴- انواع تست
۳۳	۱-۱۵- تست بدون دانش (جعبه سیاه)
۳۴	۱-۱۶- تست با دانش کامل (جعبه سفید)
۳۴	۱-۱۷- تست با دانش جزئی (جعبه خاکستری)
۳۵	۱-۱۸- گزارش هک قانونمند

جمع آوری اطلاعات و مهندسی اجتماعی

۳۷	۲-۱- مقدمه
۳۷	۲-۲- Footprinting
۳۸	۲-۳- تعریف Footprinting
۳۹	۲-۴- متدلوژی های جمع آوری اطلاعات
۴۱	۲-۵- DNS Enumeration
۴۱	۲-۶- Nslookup و DNSstuff
۴۲	۲-۷- مفهوم Whois و ARIN Lookup
۴۳	۲-۸- تحلیل خروجی Whois
۴۵	۲-۹- پیدا کردن بازه آدرس های شبکه
۴۶	۲-۱۰- شناسایی انواع رکوردهای DNS
۴۶	۲-۱۱- نحوه کار traceroute در footprinting
۴۸	۲-۱۲- استفاده از Email Tracking
۴۸	۲-۱۳- نحوه کار Web Spider ها
۴۹	۲-۱۴- مراحل انجام Footprinting
۴۹	۲-۱۵- مهندسی اجتماعی
۴۹	۲-۱۶- مهندسی اجتماعی چیست؟
۵۰	۲-۱۷- انواع رایج حملات کدامند؟
۵۱	۲-۱۷-۱- مهندسی اجتماعی مبتنی بر انسان

۵۲	۲-۱۷-۲- مهندسی اجتماعی مبتنی بر کامپیوتر.....
۵۲	۲-۱۸- حملات داخلی.....
۵۲	۲-۱۹- حملات Phishing.....
۵۳	۲-۲۰- URL obfuscation.....
۵۴	۲-۲۱- پیشگیری از مهندسی اجتماعی.....

اسکن و Enumeration

۵۷	۳-۱- مقدمه.....
۵۷	۳-۲- اسکن.....
۵۷	۳-۳- اسکن پورت، اسکن شبکه، و اسکن آسیب پذیری.....
۵۹	۳-۴- متدلوژی اسکن.....
۵۹	۳-۵- تکنیکهای Ping Sweep.....
۶۰	۳-۶- تشخیص Ping Sweep ها.....
۶۰	۳-۷- اسکن پورت ها و شناسایی سرویس ها.....
۶۱	۳-۸- مقابله با اسکن پورت.....
۶۲	۳-۹- سوئیچ های دستور Nmap.....
۶۴	۳-۱۰- HPING2.....
۶۴	۳-۱۱- اسکن های FIN و Stealth SYN, XMAS, IDLE, NULL.....
۶۶	۳-۱۲- انواع flag های ارتباط TCP.....
۶۸	۳-۱۳- FloppyScan.....
۶۹	۳-۱۴- تکنیکهای War - Dialing.....
۷۰	۳-۱۵- تکنیکهای Banner Grabbing و شناسایی سیستم عامل.....
۷۱	۳-۱۶- رسم دیاگرام شبکه ای از دستگاههای آسیب پذیر.....
۷۲	۳-۱۷- چگونه از سرورهای پروکسی در انجام حمله استفاده می شوند؟.....
۷۳	۳-۱۸- ناشناس کننده ها چگونه کار می کنند؟.....
۷۳	۳-۱۹- تکنیکهای HTTP Tunneling.....
۷۴	۳-۲۰- ابزار Httpunnel برای ویندوز.....

۷۴	IP Spoofing	۳-۲۱- تکنیکهای
۷۵	Enumeration	۳-۲۲- Enumeration
۷۷	Null Session	۳-۲۳- مقابله با Null Session
۷۸	SNMP Enumeration چیست؟	۳-۲۴- SNMP Enumeration چیست؟
۷۹	SNMP enumeration	۳-۲۵- مقابله با SNMP enumeration
۸۱	enumeration در	۳-۲۶- چه مراحل در enumeration انجام می شوند؟

۸۳ هک سیستم

۸۳	مقدمه	۴-۱- مقدمه
۸۳	تکنیکهای شکستن	۴-۲- تکنیکهای شکستن پسورد
۸۵	ابزارهای هک	۴-۲-۱- ابزارهای هک
۸۵	LanManager Hash	۴-۳- LanManager Hash
۸۶	NTLM v2 و LM ، NTLM v1	۴-۴- مقایسه پروتکل های NTLM v1 و NTLM v2
۸۶	شکستن	۴-۵- شکستن پسوردهای ویندوز
۸۷	ابزارهای هک	۴-۵-۱- ابزارهای هک
۸۸	SMB Logon به	۴-۶- هدایت SMB Logon به حمله کننده
۸۸	ابزارهای هک	۴-۶-۱- ابزارهای هک
۸۹	SMB Relay MITM و	۴-۷- حملات SMB Relay MITM و مقابله با آن
۹۰	ابزارهای هک	۴-۷-۱- ابزارهای هک
۹۰	مقابله با	۴-۸- مقابله با شکستن پسورد
۹۱	ریازه زمانی	۴-۹- ریازه زمانی تغییر پسورد
۹۲	Event Viewer Log ها	۴-۱۰- بررسی Event Viewer Log ها
۹۲	انواع	۴-۱۱- انواع پسورد
۹۴	Passive Online	۴-۱۲- حملات Passive Online
۹۵	Active Online	۴-۱۳- حملات Active Online
۹۶	حدا	۴-۱۴- حدس پسورد به صورت اتوماتیک
۹۶	مقابله با	۴-۱۵- مقابله با حدس پسورد

۹۷	 حملات آفلاین	۴-۱۶
۹۸	 Pre-Computed Hashes	۴-۱۷
۹۸	 Nonelectronic حملات	۴-۱۸
۹۹	 spyware و keylogger تکنیکهای	۴-۱۹
۱۰۰	 ابزارهای هک	۴-۱۹-۱
۱۰۱	 دسترسی های ضروری	۴-۲۰
۱۰۱	 ابزارهای هک	۴-۲۰-۱
۱۰۲	 اجرای برنامه ها	۴-۲۱
۱۰۲	 ابزارهای هک	۴-۲۱-۱
۱۰۳	 Buffer Overflows	۴-۲۲
۱۰۳	 Rootkit ها	۴-۲۳
۱۰۴	 نصب Rootkit ها بر روی کامپیوترهای ویندوز ۲۰۰۰ و XP	۴-۲۴
۱۰۴	 rootkit ها	۴-۲۵
۱۰۵	 ابزارهای هک	۴-۲۵-۱
۱۰۵	 مخفی کردن فایل ها	۴-۲۶
۱۰۶	 NTFS File Streaming	۴-۲۷
۱۰۶	 ابزارهای هک	۴-۲۷-۱
۱۰۷	 NTFS Stream	۴-۲۸
۱۰۷	 ابزارهای هک	۴-۲۸-۱
۱۰۷	 Steganography تکنولوژی های	۴-۲۹
۱۰۷	 ابزارهای هک	۴-۲۹-۱
۱۰۹	 ابزارهای مقابله	۴-۲۹-۲
۱۰۹	 پاک کردن ردپاها و مدارک	۴-۳۰
۱۰۹	 Auditing غیر فعال کردن	۴-۳۱
۱۰۹	 ابزارهای هک	۴-۳۱-۱
۱۱۰	 Event Log پاک کردن	۴-۳۲

۱۱۰..... ۱-۳۲-۴- ابزارهای هک

۱۱۳ Trojan, Backdoor, Virus, Worm

۱۱۳..... ۱-۵- مقدمه

۱۱۳..... ۲-۵- تروجان ها و backdoorها

۱۱۴..... ۳-۵- تروجان چیست؟

۱۱۶..... ۴-۵- کانال های overt و covert چیست؟

۱۱۶..... ۱-۴-۵- ابزارهای هک

۱۱۶..... ۵-۵- انواع تروجان ها

۱۱۷..... ۶-۵- تروجان های Reverse-connecting چگونه کار میکنند؟

۱۱۸..... ۱-۶-۵- ابزارهای هک

۱۲۱..... ۷-۵- نحوه کار تروجان Netcat

۱۲۱..... ۱-۷-۵- نشانه های حمله تروجان چیست؟

۱۲۲..... ۸-۵- Wrapping چیست؟

۱۲۳..... ۱-۸-۵- ابزار های هک

۱۲۴..... ۹-۵- ابزارهای ساخت تروجان

۱۲۴..... ۱۰-۵- تکنیکهای مقابله با تروجان ها چیست؟

۱۲۵..... ۱۱-۵- تکنیکهای گریز از تروجان

۱۲۵..... ۱۲-۵- چگونه تروجان را شناسایی کنیم؟

۱۲۵..... ۱۳-۵- ابزارهای Port-Monitoring and Trojan-Detection

۱۲۶..... ۱۴-۵- بررسی سیستم فایل برای مقابله با تروجان

۱۲۷..... ۱۵-۵- ویروس ها و Wormها

۱۲۷..... ۱۶-۵- تفاوت بین ویروس و Worm

۱۳۰..... ۱۷-۵- انواع ویروس

۱۳۰..... ۱۸-۵- چگونه ویروس گسترش می یابد و سیستم را آلوده می کند

۱۳۲..... ۱۹-۵- ابزارهای ساخت تروجان

۱۳۲..... ۲۰-۵- تکنیکهای دور زدن آنتی ویروس

۱۳۲.....	۵-۲۱- روش های شناسایی ویروس.....
----------	----------------------------------

135 Sniffers

۱۳۵.....	۶-۱- مقدمه.....
۱۳۵.....	۶-۲- پروتکل های مستعد برای استراق سمع.....
۱۳۶.....	۶-۲-۱- ابزارهای هک.....
۱۳۷.....	۶-۳- استراق سمع اکتیو و پسیو.....
۱۳۸.....	۶-۳-۱- استراق سمع اکتیو.....
۱۳۹.....	۶-۳-۲- استراق سمع پسیو.....
۱۳۹.....	۶-۴- ARP Poisoning.....
۱۴۰.....	۶-۵- MAC Duplicating.....
۱۴۱.....	۶-۶- Capture کردن توسط Ethereal و نمایش فیلترها.....
۱۴۱.....	۶-۷- MAC Flooding.....
۱۴۲.....	۶-۸- DNS Poisoning.....
۱۴۳.....	۶-۹- Intranet DNS Spoofing.....
۱۴۴.....	۶-۱۰- Internet DNS Spoofing.....
۱۴۴.....	۶-۱۱- Proxy Server DNS Poisoning.....
۱۴۴.....	۶-۱۲- DNS Cache Poisoning.....
۱۴۵.....	۶-۱۲-۱- ابزارهای هک.....
۱۴۶.....	۶-۱۳- مقابله با استراق سمع.....
۱۴۷.....	۶-۱۳-۱- ابزارهای هک.....

149 Session Hijacking & Denial Service

۱۴۹.....	۷-۱- مقدمه.....
۱۵۰.....	۷-۲- Denial of Service.....
۱۵۰.....	۷-۳- انواع حملات DoS.....
۱۵۱.....	۷-۳-۱- ابزارهای هک.....

۱۵۲.....	۷-۴- نحوه کار حملات DDoS
۱۵۲.....	۷-۴-۱- ابزارهای هک
۱۵۵.....	۷-۵- دسته بندی حملات DDoS
۱۵۵.....	۷-۶- نحوه کار BOTها و BOTNETها
۱۵۷.....	۷-۷- حمله Smurf چیست؟
۱۵۸.....	۷-۸- SYN flooding چیست؟
۱۵۸.....	۷-۹- مقابله با DoS و DDoS
۱۵۹.....	۷-۹-۱- ابزارهای هک
۱۶۰.....	۷-۱۰- Session Flijackning
۱۶۰.....	۷-۱۱- Hijacking , Spoofing
۱۶۱.....	۷-۱۲- انواع Session hijacking
۱۶۲.....	۷-۱۳- مفاهیم TCP: دسته بکایی سه مرحله ای
۱۶۳.....	۷-۱۴- پیشگویی sequence
۱۶۵.....	۷-۱۵- چه مراحل در session hijacking انجام می شوند؟
۱۶۶.....	۷-۱۶- TCP/IP Hijacking
۱۶۷.....	۷-۱۷- RST Hijacking
۱۶۷.....	۷-۱۸- Blind Hijacking
۱۶۷.....	۷-۱۸-۱- ابزارهای هک
۱۶۸.....	۷-۱۹- session hijacking خطرات
۱۶۹.....	۷-۲۰- چگونگی پیشگیری از session hijacking

هک وب سرورها، آسیب پذیری برنامه های تحت وب، تکنیک های شکستن

پسوردهای مبتنی بر وب

۱۷۱.....	۸-۱- مقدمه
۱۷۱.....	۸-۲- هک وب سرورها
۱۷۲.....	۸-۳- انواع آسیب پذیری های وب سرور
۱۷۲.....	۸-۴- حملات به وب سرورها

۱۷۳.....	IIS Unicode Exploit - ۸-۹
۱۷۵.....	ابزارهای هک - ۸-۹-۱
۱۷۶.....	تکنیکهای مدیریت patchها - ۸-۱۰
۱۷۶.....	اسکنرهای آسیب پذیری - ۸-۱۱
۱۷۷.....	روش های امن سازی وب سرور - ۸-۱۲
۱۷۸.....	چک لیست محافظت از وب سرور - ۸-۱۳
۱۷۹.....	آسیب پذیری های برنامه های تحت وب - ۸-۱۴
۱۸۰.....	نحوه کار برنامه های وب - ۸-۱۵
۱۸۰.....	هدف از هک برنامه های تحت وب - ۸-۱۶
۱۸۰.....	آنانومی حمله - ۸-۱۷
۱۸۱.....	تهدیدات برنامه های وب - ۸-۱۸
۱۸۴.....	ابزارهای هک - ۸-۱۸-۱
۱۸۶.....	Google Hacking - ۸-۱۹
۱۸۶.....	تکنیکهای شکستن پسوردهای مبتنی بر وب - ۸-۲۰
۱۸۶.....	احراز هویت - ۸-۲۱
۱۸۶.....	انواع احراز هویت - ۸-۲۲
۱۸۸.....	شناسایی بر مبنای حالت هندسی دست - ۸-۲۳
۱۸۸.....	اسکن شبکه چشم - ۸-۲۴
۱۸۹.....	تشخیص چهره - ۸-۲۵
۱۸۹.....	پسورد - ۸-۲۶
۱۹۱.....	پسورد کرکر چیست؟ - ۸-۲۷
۱۹۲.....	پسورد کرکر چگونه کار می کند؟ - ۸-۲۸
۱۹۲.....	حملات برای شکستن پسورد: دسته بندی - ۸-۲۹
۱۹۲.....	ابزارهای هک - ۸-۲۹-۱