

به نام خدا



هکر قانونمند باشیم

بر اساس استاندارد

CHE

مؤلفان

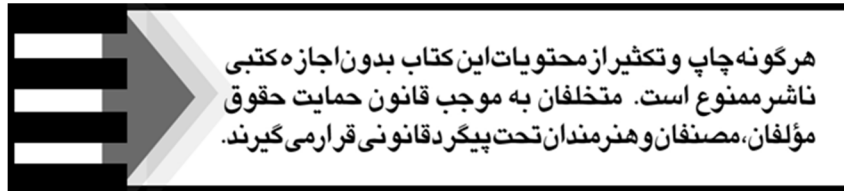
مهندس سعید حق گو

مهندس معصومه خورشیدوند

مهندس حمیدرضا قنبری

محمد مهدی ذوالفقاری

با همکاری گروه فنی و مهندسی ذوق



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

◀ عنوان کتاب: **هکر قانونمند باشیم**

براساس استاندارد CHE

◀ مولفان: مهندس سعید حق گو

مهندس معصومه خورشیدوند

مهندس حمیدرضا قنبری

محمد مهدی ذوالفقاری

با همکاری گروه فنی و مهندسی ذوق

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرای: شبیم هاشم زاده

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۳۹۶

◀ چاپ و صحافی: دانشجو

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۳۷۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۰۰-۱۲۴-۸۴۹-۸

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۰۴۶۶۴۱۰۰-۲۲۰۸۵۱۱۱

کد پستی: ۱۳۱۴۹۸۳۱۸۵

فروشگاههای اینترنتی:

www.mftbook.ir

www.mftdibagaran.ir

نشانی تلگرام: @mftbook لینک ربات تلگرام دیباگران: @dibagaranetehranbot

عنوان و نام پدیدآور: هکر قانونمند باشیم براساس

استاندارد CHE / مولفان: سعید حق گودیگران

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۶

مشخصات ظاهری: ۳۳۶ ص: مصور.

شابک: ۹۷۸-۶۰۰-۱۲۴-۸۴۹-۸

وضعیت فهرست نویسی: فیبا

یادداشت: مولفان: سعید حق گو، معصومه خورشیدوند، حمیدرضا

قنبری، مهدی ذوالفقاری، با همکاری گروه فنی و مهندسی ذوق

موضوع: هکرها

موضوع: Hckers

موضوع: مهندسی اجتماعی

موضوع: social engineering

موضوع: شبکه های کامپیوتری-تدابیر ایمنی

موضوع: computer networks-security measures

موضوع: کامپیوترها-ایمنی اطلاعات

موضوع: computer security

شناسه افزوده: حق گو، سعید، ۱۳۵۰- مترجم

رده بندی کنگره: ۱۳۹۶ ۵۸ ۶۶۸/ HM

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۵۱۱۱۴۸۶

فهرست مطالب

فصل اول.....	۱۹
مقدمه ای بر هک قانونمند.....	۱۹
مقدمه	۲۰
واژگان فنی	۲۰
انواع مختلف تکنولوژی های هک.....	۲۲
مرحله مختلف هک قانونمند.....	۲۴
HACKTIVISIM چیست ؟.....	۲۸
انواع هکرها.....	۲۸
هکهای قانونمند و CRACKER ها کیستند؟.....	۲۹
اهداف حمله کننده ها.....	۳۰
مثبت امنیت ، عملکرد، و راحتی استفاده	۳۲
تحقیق آسیب پذیری چیست ؟.....	۳۳
روش های اجرای هک قانونمند.....	۳۴
برنامه ارزیابی امنیتی	۳۵
انواع حملات قانونمند.....	۳۵
انواع تست	۳۷
تست بدون دانش (جعبه سیاه).....	۳۷
تست با دانش کامل (جعبه سفید).....	۳۸
تست با دانش جزئی (جعبه خاکستری).....	۳۸
گزارش هک قانونمند.....	۳۹

فصل دوم.....	۴۱
جمع آوری اطلاعات و مهندسی اجتماعی.....	۴۱
مقدمه.....	۴۲
FOOTPRINTING.....	۴۲
تعریف FOOTPRINTING.....	۴۳
متدلوژیهای جمع آوری اطلاعات.....	۴۴
DNS ENUMERATION.....	۴۶
NSLOOKUP و DNSSTUFF.....	۴۶
مفهوم WHOIS و ARIN LOOKUP.....	۴۷
تحلیل خروجی WHOIS.....	۴۹
پیدا کردن بازه آدرس های شبکه.....	۵۲
شناسایی انواع مختلف رکوردهای DNS.....	۵۳
نحوه کار TRACEROUTE در FOOTPRINTING.....	۵۴
استفاده از EMAIL TRACKING.....	۵۵
نحوه کار WEB SPIDER ها.....	۵۶
مراحل انجام FOOTPRINTING.....	۵۷
مهندسی اجتماعی.....	۵۸
مهندسی اجتماعی چیست ؟.....	۵۸
انواع رایج حملات کدامند؟.....	۵۹
مهندسی اجتماعی مبتنی بر انسان.....	۵۹
مهندسی اجتماعی مبتنی بر کامپیوتر.....	۶۱
حملات داخلی.....	۶۱
حملات PHISHING.....	۶۱
URL OBFUSCATION.....	۶۳
پیشگیری از مهندسی اجتماعی.....	۶۳

فصل سوم..... ۶۵

اسکن و ENUMERATION..... ۶۵

۶۶	مقدمه
۶۶	اسکن
۶۶	اسکن پورت، اسکن شبکه ، و اسکن آسیب پذیری
۶۸	متدلوژی اسکن
۶۸	تکنیک های PING SWEEP
۶۹	تشخیص PING SWEEP ها
۷۰	اسکن پورتهای و شناسایی سرویس ها
۷۰	مقابله با اسکن پورت
۷۱	سوئیچ های دستور NMAP
۷۴	HPING2
۷۵	اسکن های SYN, STEALTH, XMAS, NULL, IDLE, و FIN
۷۶	انواع FLAG های ارتباط TCP
۷۹	ابزارهای هک
۸۰	تکنیک های WAR-DIALING
۸۱	ابزارهای هک
۸۱	تکنیک های BANNER GRABBING و شناسایی سیستم عامل
۸۳	رسم دیاگرام شبکه ای از دستگاههای آسیب پذیر
۸۴	چگونه از سرورهای پروکسی در انجام حمله استفاده می شوند؟
۸۵	ناشناس کننده ها چگونه کار می کنند؟
۸۶	تکنیک های HTTP TUNNELING
۸۶	ابزار HTTP TUNNEL برای ویندوز
۸۷	تکنیکهای IP SPOOFING
۸۸	ENUMERATION
۸۹	NULL SESSION
۹۱	مقابله با NULL SESSION
۹۳	چيست SNMP ENUMERATION؟

۹۴.....	مقابله با SNMP ENUMERATION
۹۴.....	انتقال DNS ZONE در ویندوز ۲۰۰۰

۹۷ فصل چهارم

۹۷ هک سیستم

۹۸.....	مقدمه
۹۸.....	تکنیک های شکستن پسورد
۱۰۰.....	ابزارهای هک
۱۰۱.....	LANMANAGER HASH
۱۰۲.....	شکستن پسوردهای ویندوز ۲۰۰۰
۱۰۲.....	ابزارهای هک
۱۰۳.....	هدایت SMB LOGON به حمله کننده
۱۰۴.....	ابزارهای هک
۱۰۴.....	حملات SMB RELAY MITM و مقابله با آن
۱۰۵.....	ابزارهای هک
۱۰۵.....	مقابله با شکستن پسورد
۱۰۷.....	بازه زمانی تغییر پسورد
۱۰۷.....	بررسی EVENT VIEWER LOG ها
۱۰۸.....	انواع پسورد
۱۱۰.....	حملات PASSIVE ONLINE
۱۱۱.....	حملات ACTIVE ONLINE
۱۱۲.....	حدس پسورد به صورت اتوماتیک
۱۱۳.....	مقابله با حدس پسورد
۱۱۳.....	حملات آفلاین
۱۱۵.....	PRE-COMPUTED HASHES
۱۱۵.....	حملات NONELECTRONIC
۱۱۷.....	تکنیک های KEYLOGGER ها و SPYWARE

۱۱۷	ابزارهای هک
۱۱۹	دسترسی های ضروری
۱۱۹	ابزارهای هک
۱۲۰	اجرای برنامه ها
۱۲۰	ابزارهای هک
۱۲۱	BUFFER OVERFLOWS
۱۲۱	ROOTKIT ها
۱۲۲	نصب ROOTKIT ها بر روی کامپیوترهای ویندوز ۲۰۰۰ و XP
۱۲۳	مقابله با ROOTKIT ها
۱۲۳	ابزارهای هک
۱۲۳	مخفی کردن فایل ها
۱۲۴	NTFS FILE STREAMING
۱۲۵	ابزارهای هک
۱۲۵	مقابله با NTFS STREAM
۱۲۵	ابزارهای هک
۱۲۶	تکنولوژی های STEGANOGRAPHY
۱۲۶	ابزارهای هک
۱۲۸	ابزارهای مقابله
۱۲۸	پاک کردن ردپاها و مدارک
۱۲۸	غیر فعال کردن AUDITING
۱۲۹	ابزارهای هک
۱۲۹	پاک کردن EVENT LOG
۱۳۰	ابزارهای هک

۱۳۱ فصل پنجم

۱۳۱ TROJAN, BACKDOOR, VIRUS, WORM

۱۳۲	مقدمه
۱۳۲	تروجان ها و BACKDOOR ها

۱۳۴	تروجان چیست؟
۱۳۵	کانالهای OVERT و COVERT چیست؟
۱۳۶	ابزارهای هک
۱۳۶	انواع تروجان ها
۱۳۷	تروجانهای REVERSE-CONNECTING چگونه کار می کنند؟
۱۳۷	ابزارهای هک
۱۴۱	نحوه کار تروجان NETCAT
۱۴۱	نشانه های حمله تروجان چیست ؟
۱۴۲	WRAPPING چیست؟
۱۴۳	ابزارهای هک
۱۴۴	ابزارهای ساخت تروجان
۱۴۴	تکنیک های مقابله با تروجانها چیست ؟
۱۴۵	تکنیکهای گریز از تروجان
۱۴۶	چگونه تروجان را شناسایی کنیم؟
۱۴۶	ابزارهای PORT-MONITORING AND TROJAN-DETECTION
۱۴۷	بررسی سیستم فایل برای مقابله با تروجان
۱۴۹	ویروس ها و WORMها
۱۴۹	تفاوت بین ویروس و WORM
۱۵۱	انواع ویروس
۱۵۴	ابزارهای ساخت تروجان
۱۵۵	تکنیک های دور زدن آنتی ویروس
۱۵۵	روشهای شناسایی ویروس

۱۵۷ فصل ششم

۱۵۷ SNIFFER ها

۱۵۸	مقدمه
۱۵۸	پروتکل های مستعد برای استراق سمع
۱۵۹	ابزارهای هک

۱۶۰		استراق سمع اکتیو و پسیو
۱۶۱		استراق سمع اکتیو
۱۶۲		استراق سمع پسیو
۱۶۲		ARP POISONING
۱۶۴		MAC DUPLICATING
۱۶۵		CAPTURE کردن توسط ETHEREAL و نمایش فیلترها
۱۶۵		MAC FLOODING
۱۶۶		DNS POISONING
۱۶۸		INTRANET DNS SPOOFING
۱۶۹		INTERNET DNS SPOOFING
۱۷۰		PROXY SERVER DNS POISONING
۱۷۱		DNS CACHE POISONING
۱۷۱		ابزارهای هک
۱۷۳		مقابله با استراق سمع
۱۷۴		ابزارهای هک

۱۷۵ فصل هفتم

۱۷۵ SESSION HIJACKING و DENIAL OF SERVICE

۱۷۶		مقدمه
۱۷۷		DENIAL OF SERVICE
۱۷۷		انواع حملات DoS
۱۷۸		ابزارهای هک
۱۸۰		نحوه کار حملات DDOS
۱۸۱		ابزارهای هک
۱۸۳		دسته بندی حملات DDOS
۱۸۴		حمله SMURF چیست ؟
۱۸۵		SYN FLOODING چیست ؟
۱۸۶		مقابله با DoS و DDOS

۱۸۷	ابزارهای هک
۱۸۸	SESSION HIJACKING
۱۸۸	HIJACKING و SPOOFING
۱۹۲	مفاهیم TCP
۱۹۳	پیشگویی SEQUENCE
۱۹۶	SESSION HIJACKING سطوح
۱۹۶	TCP/IP HIJACKING
۱۹۷	RST HIJACKING
۱۹۸	BLIND HIJACKING
۱۹۹	ابزارهای هک
۲۰۰	SESSION HIJACKING خطرات
۲۰۰	SESSION HIJACKING از پیشگیری

فصل هشتم ۲۰۳

هک وب سرورها، آسیب پذیری برنامه های تحت وب، و تکنیک های شکستن پسوردهای مبتنی بر وب... ۲۰۳

۲۰۴	مقدمه
۲۰۴	هک وب سرورها
۲۰۵	انواع آسیب پذیریهای وب سرور
۲۰۵	حملات به وب سرورها
۲۰۶	IIS UNICODE EXPLOIT
۲۰۸	ابزارهای هک
۲۰۹	تکنیک های مدیریت PATCHها
۲۱۰	اسکنرهای آسیب پذیری
۲۱۱	روش های امن سازی وب سرور
۲۱۲	چک لیست محافظت از وب سرور
۲۱۳	SCRIPT MAPPING
۲۱۴	ISAPI FILTERS
۲۱۴	فایل ها و دایرکتوریها

۲۱۴.....	IIS METABASE
۲۱۵.....	آسیب پذیریهای برنامه های تحت وب
۲۱۵.....	نحوه کار برنامه های وب
۲۱۶.....	هدف از هک برنامه های تحت وب
۲۱۶.....	آنا تومی حمله
۲۱۷.....	تهدیدات برنامه های وب
۲۲۱.....	ابزارهای هک
۲۲۲.....	GOOGLE HACKING
۲۲۳.....	تکنیک های شکستن پسوردهای مبتنی بر وب
۲۲۳.....	انواع احراز هویت
۲۲۷.....	پسورد
۲۲۹.....	مثال هایی از پسوردهای بد
۲۲۹.....	پسورد کرکر چیست ؟
۲۳۰.....	پسورد کرکر چگونه کار می کند؟
۲۳۱.....	حملات برای شکستن پسورد
۲۳۱.....	ابزارهای هک

۲۳۵.....فصل نهم

۲۳۵.....SQL INJECTION و BUFFER OVERFLOW

۲۳۶.....	مقدمه
۲۳۶.....	SQL INJECTION چیست ؟
۲۳۷.....	مراحل انجام SQL INJECTION
۲۳۹.....	آسیب پذیری های SQL SERVER
۲۴۲.....	BLIND SQL INJECTION
۲۴۳.....	مقابله با SQL INJECTION
۲۴۵.....	انواع BUFFER OVERFLOW و روشهای شناسایی
۲۴۵.....	پشته (STACK)
۲۴۶.....	HEAP

۲۴۷		سرریزی بافر مبتنی بر پشته (STACK-BASED BUFFER OVERFLOW)
۲۴۹		سرریزی بافر مبتنی بر HEAP (HEAP-BASED OVERFLOW)
۲۵۰		روش شناسایی BUFFER OVERFLOW در برنامه
۲۵۰		تکنیکهای تغییر BUFFER OVERFLOW
۲۵۱		روشهای جلوگیری از BUFFER OVERFLOW

فصل دهم ۲۵۳

هک شبکه های وایرلس ۲۵۳

۲۵۴		مقدمه
۲۵۵		استانداردهای وایرلس
۲۵۵		مفاهیم وایرلس
۲۵۶		مکانیزم های احراز هویت WEP و WPA، و تکنیکهای شکستن آنها
۲۵۹		اصطلاحات هک شبکه وایرلس
۲۶۰		ابزارهای هک
۲۶۰		استراق سمع کننده های وایرلس و قرار دادن SSID ها و MAC SPOOFING
۲۶۱		تغییر دستی MAC ADDRESS در ویندوز XP
۲۶۲		ابزارهای هک
۲۶۲		ROGUE ACCESS POINT (تقلبی)
۲۶۳		ابزارهای هک
۲۶۳		تکنیک های هک شبکه وایرلس
۲۶۴		مراحل هک شبکه های وایرلس
۲۶۵		روشهایی شناسایی شبکه های وایرلس
۲۶۶		ابزارهای هک
۲۶۶		روشهای امن سازی شبکه های وایرلس

فصل یازدهم..... ۲۶۹

امنیت فیزیکی ۲۶۹

۲۷۰	 مقدمه
۲۷۰	 رویدادهای نقض امنیت فیزیکی
۲۷۲	 امنیت فیزیکی
۲۷۳	 ضرورت امنیت فیزیکی چیست؟
۲۷۴	 ضرورت امنیت فیزیکی
۲۷۵	 چک لیست امنیت فیزیکی
۲۸۰	 برخی از ابزارهای امنیت فیزیکی

فصل دوازدهم..... ۲۸۳

هک لینوکس ۲۸۳

۲۸۴	 مقدمه
۲۸۴	 اساس لینوکس
۲۸۶	 دستورات پایه لینوکس
۲۸۸	 دایرکتوریهای لینوکس
۲۸۹	 نحوه کامپایل کرنل لینوکس
۲۹۱	 دستورات کامپایل GCC
۲۹۲	 نحوه نصب ماژولهای کرنل لینوکس
۲۹۲	 آسیب پذیری های لینوکس
۲۹۳	 ZLIB
۲۹۳	 ابزارهای هک
۲۹۴	 روشهای امن سازی لینوکس
۲۹۶	 فایروال در لینوکس (IPTABLE)
۲۹۶	 ابزارهای لینوکس

فصل سیزدهم ۲۹۹

گریز از IDS ها، HONEYPOT ها و فایروال ها ۲۹۹

۳۰۰	 مقدمه
۳۰۰	 انواع سیستم های تشخیص نفوذ و تکنیکهای گریز
۳۰۲	 مکان IDS در شبکه
۳۰۴	 گریز از IDS
۳۰۴	 ابزارهای هک
۳۰۵	 فایروال
۳۰۶	 انواع فایروال
۳۰۹	 ابزارهای هک
۳۰۹	 ابزارهای تست
۳۱۰	 HONEYPOT
۳۱۱	 انواع مختلف HONEYPOT
۳۱۲	 مزایای HONEYPOT
۳۱۲	 محل قرار گیری HONEYPOT در شبکه
۳۱۳	 ابزارها
۳۱۴	 OPEN SOURCE های HONEYPOT
۳۱۵	 HONEYPOT فیزیکی و مجازی
۳۱۵	 ابزارهای هک

فصل چهاردهم ۳۱۷

رمزنگاری ۳۱۷

۳۱۸	 مقدمه
۳۱۸	 تکنیکهای رمزنگاری و رمزگذاری
۳۲۰	 نحوه تولید کلیدهای عمومی و خصوصی
۳۲۰	 نگاهی به الگوریتم های MD۵، SHA، RC۴، و BLOWFISH

ابزارها..... ۳۲۳

ابزارهای هک..... ۳۲۴

فصل پانزدهم..... ۳۲۵

روشهای تست نفوذ..... ۳۲۵

مقدمه..... ۳۲۶

ارزیابی های امنیتی..... ۳۲۶

روشهای تست نفوذ..... ۳۲۷

مراحل تست نفوذ..... ۳۲۸

چارچوب قانونی تست نفوذ..... ۳۳۳

ابزارهای خودکار تست نفوذ..... ۳۳۳

موارد قابل ارائه در تست نفوذ..... ۳۳۵

خط‌مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند خواسته‌هایی به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "سرکار خانم معصومه خورشید وند-جناب آقایان سعید حق گو-حمیدرضا قنبری-محمد مهدی ذوالفقاری و با همکاری گروه فنی و مهندسی ذوق" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
Publishing@mftmail.com

مقدمه مولفان

هوالحکیم

آنچه در کتاب هکر قانونمند باشیم ، براساس استاندارد CHE ، می خوانید، نگاهی است با رویکردهای آموزشی ، بر تمام جنبه های نفوذ و پیشگیری از نفوذ.امید است مطالعه این کتاب گامی کوچک در ارتقای سطح دانش مخاطبین گرامی به همراه داشته باشد .

زمستان ۱۳۹۶

گروه مولفان