

به نام خدا

۱۵۸ ۲۹۲۴
۱۵۸ ۲۹۲۴



مک قانونمند باشیم

بر اساس استاندارد

CHE

مؤلفان

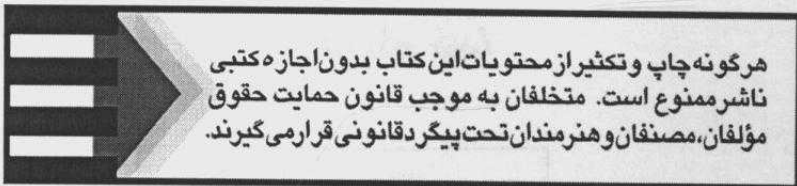
مهندس سعید حق گو

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: مهناز 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: شبینم 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: ۶۶۴۱۰۰۴-۰۸۵۱۱۱۱۱۲۲

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 گو دیباگران

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۶

مشخصات ظاهری: ۲۳۶ 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

رصوع: 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 ۱۲۰۰۰-مترجم

رده بندی کنگره: ۸ ۱۳۹۶ HM

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۵۱۱۱۴۸۶

فهرست مطالب

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

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

۶۵.....	فصل سوم.....
۶۵.....	اسکن و ENUMERATION.....
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 پورت ها و شناسایی سرویس ها.....
۷۰.....	مقابله با اسکن.....
۷۱.....	سوئیچ های دد تور NM.....
۷۴.....	HPING2.....
۷۵.....	اسکن های FIN، IDLE.NULL.XMAS.SYN و STEALTH.....
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.....
۸۳.....	رسم دیاگرام شبکه ای از دستگاه های 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.....	تکنیک های 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	LANMAN USER HASH
۱۰۲	شکستن پسوردهای ویندوز ۲۰۰۰
۱۰۲	ابزارهای هک
۱۰۳	هدایت SMB LOGON با حمله کنت
۱۰۴	ابزارهای هک
۱۰۴	حملات SMB RELAY MITM و مانع شدن
۱۰۵	ابزارهای هک
۱۰۵	مقابله با شکستن پسورد
۱۰۷	بازه زمانی تغییر پسورد
۱۰۷	بررسی EVENT VIEWER LOGها
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 KEYLOGGERها 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 ETHERREAL 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.....	سطوح SESSION HIJACKING
۱۹۶.....	TCP/IP HIJACKING
۱۹۷.....	RST HIJACKING
۱۹۸.....	BLIND HIJACKING
۱۹۹.....	ابزارها - هک
۲۰۰.....	SESSION HIJACKING خطرات
۲۰۰.....	چگونگی پیشگیری از SESSION HIJACKING

۲۰۳..... فصل هشتم

هک وب سرورها، آسیب پذیری برنامه های 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.....	اسکریپت های 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	آناتومی حمله
۲۱۷	تهدیدات برنامه های وب
۲۲۱	ابزارهای هک
۲۲۲	GOOGLE HACKING
۲۲۳	تکنیک های شکستن پسوردهای مبتنی بر وب
۲۲۳	انواع اجرار همت
۲۲۷	پسورد
۲۲۹	مثال هایی از پسوردهای
۲۲۹	پسورد کرکر چیست؟
۲۳۰	پسورد کرکر چگونه کار میکند؟
۲۳۱	حملات برای شکستن پسورد
۲۳۱	ابزارهای هک

۲۳۵ فصل نهم

۲۳۵ BUFFER OVERFLOW و SQL INJECTION

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 WPA و WPA2 و تکنیکهای شکستن آنها.....
۲۵۹.....	اصطلاحات هک شبکه وایرلس.....
۲۶۰.....	ابزارهای هک.....
۲۶۰.....	استراق سمع کننده های وایرلس و فرستادن SSID ها 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

مقدمه..... ۲۷۰

رویدادهای نقض امنیت فیزیکی..... ۲۷۰

امنیت فیزیکی..... ۲۷۲

ضرورت امنیت فیزیکی چیست؟..... ۲۷۳

ضرورت امنیت فیزیکی..... ۲۷۴

چک لیست امنیت فیزیکی..... ۲۷۵

برخی از ابزارهای امنیت فیزیکی..... ۲۸۰

فصل دوازدهم..... ۲۸۳

هک لینوکس..... ۲۸۳

مقدمه..... ۲۸۴

اساس لینوکس..... ۲۸۴

دستورات پایه لینوکس..... ۲۸۶

دایرکتوریهای لینوکس..... ۲۸۸

نحوه کامپایل کرنل لینوکس..... ۲۸۹

دستورات کامپایل GCC..... ۲۹۱

نحوه نصب ماژولهای کرنل لینوکس..... ۲۹۲

آسیب پذیری های لینوکس..... ۲۹۲

ZLIB..... ۲۹۳

ابزارهای هک..... ۲۹۳

روشهای امن سازی لینوکس..... ۲۹۴

فایروال در لینوکس (IPTABLE)..... ۲۹۶

ابزارهای لینوکس..... ۲۹۶

فصل سیزدهم ۲۹۹

گزیز از IDS ها، HONEYPOT ها و فایروال ها ۲۹۹

مقدمه ۳۰۰

انواع سیستم های تشخیص نفوذ و تکنیکهای گزیز ۳۰۰

مکان IDS در شبکه ۳۰۲

گزیز از IDS ۳۰۴

ابزارهای هک ۳۰۴

فایروال ۳۰۵

انواع فایروال ۳۰۶

ابزارهای هک ۳۰۹

ابزارهای تست ۳۰۹

HONEYPOT ۳۱۰

انواع مختلف HONEYPOT ۳۱۱

مزایای HONEYPOT ۳۱۲

محل قرار گیری HONEYPOT در شبکه ۳۱۲

ابزارها ۳۱۳

HONEYPOT های OPEN SOURCE ۳۱۴

HONEYPOT فیزیکی و مجازی ۳۱۵

ابزارهای هک ۳۱۵

فصل چهاردهم ۳۱۷

رمزنگاری ۳۱۷

مقدمه ۳۱۸

تکنیکهای رمزنگاری و رمزگذاری ۳۱۸

نحوه تولید کلیدهای عمومی و خصوصی ۳۲۰

نگاهی به الگوریتم های MD۵، SHA، RC۴، ARC۵ و BLOWFISH ۳۲۰

۳۲۳.....ابزارها

۳۲۴.....ابزارهای هک

۳۲۵.....فصل پانزدهم

۳۲۵.....روشهای تست نفوذ

۳۲۶.....مقدمه

۳۲۶.....ارزیابی های امنیتی

۳۲۷.....روشهای تست نفوذ

۳۲۸.....مراحل تست نفوذ

۳۳۳.....چارچوب قانونی تست نفوذ

۳۳۳.....ابزارهای خودکار تست نفوذ

۳۳۵.....موارد قابل ارائه در تست نفوذ

هوالحکیم

آنچه در کتاب هکر قلمبند 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 به جهت در تقای سطح دانش مخاطبین گرامی به همراه داشته باشد .

زمستان ۱۳۹۶

گروه مولفان