«بسمه‌تعالی»

آموزش گام به گام

هک و ضدهک

نویسندگان:

STUART **MCCLURE**
JOEL **SCAMBRAY**
GEORGE **KURTZ**

مترجمان:

ابوالفضل طاهریان ریزی

بهمن اصغرزادهٔ امین

انتشارات طاهریان

سرشناسه: مکلور، استوارت
McCure, Stuart
عنوان و نام پدیدآور: آموزش گام به گام هک و ضدهک/نویسندگان استوارت مک‌کلور،جوئل اسکمبری، جورج کورتس;
مترجمان ابوالفضل طاهریان ریزی، بهمن اصغرزاده امین.
مشخصات نشر: تهران: طاهریان، ۱۳۸۸ .
مشخصات ظاهری: ۷۵۲ ص.جدول.
شابک: ۳-۷۳-۸٤۰٦-۹٦٤-۹۷۸
یادداشت: عنوان اصلی: Hacking exposed 6: network security secrets & solutions
موضوع: شبکه‌های کامپیوتری –اقدامات تأمینی
موضوع: تأمین خسارت
موضوع: حفاظت اطلاعات
شناسه افزوده: اسکمبری، جوئل
شناسه افزوده: Scambray, Joel
شناسه افزوده: کورتس، جورج
شناسه افزوده: Kurtz, George
شناسه افزوده: طاهریان ریزی، ابوالفضل، ۱۳۵۲ - مترجم
شناسه افزوده: اصغرزاده امین، بهمن، ۱۳٦۲- مترجم
رده بندی کنگره: ۱۳۸۸ ۸آ۷م/۵۹/۵۱۰۵ TK
رده بندی دیویی: ۰۰۵/۸
شماره کارشناسی ملی: ۱۹۵۱۸۳۷

انتشارات طاهریان

«آموزش گام به گام هک و ضد هک»

● **مترجمان**: ابوالفضل طاهریان ریزی، بهمن اصغرزادهٔ امین ● **ناشر**: انتشارات طاهریان
● **چاپ جلد**: چاپ ژیک ● **نوبت چاپ**: اول ● **سال چاپ**: ۱۳۸۹ ● **تیراژ**: ۲۱۰۰ جلد
● **لیتوگرافی**: باران ● **چاپ**: سپه ● **قیمت**: ۱۵۰۰۰۰ ریال ● **طرح جلد**: آرزو خسروپور
● **حروف‌چینی**: انتشارات طاهریان ● **شابک**: ۳-۷۳-۸۴۰۶-۹۶۴-۹۷۸

آدرس: میدان انقلاب، خیابان کارگر جنوبی، خیابان لبافی نژاد، پلاک ۲۶۶، طبقهٔ چهارم، واحد ۱۱
تلفن: ۶۶۴۹۲۷۳۳ تلفکس: ۶۶۹۷۴۱۵۲
www.Taherianpress.com

هرگونه چاپ و تکثیر از محتویات، طرح جلد و عنوان مجموعهٔ این کتاب بدون اجازهٔ کتبی ناشر ممنوع است و متخلفان به موجب قانون مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.

فهرست:

بخش اول: پوشش و استقرار

فصل ۱: ردنگاری

ردنگاری چیست؟ ۲۲
چرا ردنگاری لازم است؟ ۲۳
ردنگاری اینترنتی ۲۴
اطلاعات با دسترسی عمومی ۲۵
سازمان‌های مرتبط ۲۷
کارمندان: شماره تلفن‌ها، نام‌های تماس، آدرس‌های ایمیل، و جزییات شخصی ۲۸
رویدادهای جاری ۳۱
سیاست‌های حفاظتی یا امنیتی و جزییات تکنیکی نشانگر نوع مکانیسم امنیتی محل ۳۲
اطلاعات آرشیو شده ۳۳
موتورهای جستجو، Usenet، و رزومه‌ها ۳۴
دیگر اطلاعات جالب ۳۹
اقدامات متقابل امنیتی پایگاه داده عمومی ۳۹
اقدامات متقابل امنیت پایگاه داده عمومی ۴۹
انتقال‌های ناحیه [zone transfers] ۵۰
اقدامات متقابل امنیت DNS ۵۵
رهیابی [Tracerouting] ۵۶
اقدامات متقابل شناسایی مقدماتی شبکه ۶۰

فصل ۲: اسکن کردن

تشخیص اینکه آیا یک سیستم روشن است ۶۱
جاروهای ping شبکه ۶۲
اقدامات متقابل جاروهای Ping ۶۹
پرس‌وجوهای ICMP ۷۱
اقدامات متقابل پرس‌وجوی ICMP ۷۳
تشخیص دادن اینکه کدام سرویس‌ها در حال اجرا یا شنود هستند ۷۳
اسکن کردن درگاه ۷۳
انواع اسکن ۷۴
شناسایی سرویس‌های در حال اجرای TCP و UDP ۷۶
اسکنرهای درگاه مبتنی بر ویندوز ۸۳
تخریب اسکن کردن درگاه ۸۸
شناسایی سیستم عامل ۹۰
شناسایی سیستم عامل فعال ۹۰
انگشت نگاری پشته فعال ۹۱
اقدامات متقابل شناسایی سیستم عامل ۹۵
شناسایی سیستم عامل غیر فعال [passive] ۹۵
انگشت نگاری پشتهٔ غیرفعال ۹۶
امضاهای غیر فعال ۹۶
اقدامات متقابل شناسایی سیستم عامل غیرفعال ۹۸
ابزارهای همه کاره: ابزار خودکار اکتشاف ۹۸
اقدامات متقابل ابزارهای اکتشاف اتوماتیک ۱۰۰

فصل ۳: شالودهٔ هک کردن

قاپیدن علامت ابتدایی ۱۰۲
اصول ابتدایی قاپیدن علامت: telnet و netcat ۱۰۳
اقدامات متقابل قاپیدن علامت ۱۰۶
موردبندی سرویس‌های معمول شبکه ۱۰۶
مورد بندی FTP ، TCP 21 ..... ۱۰۶
اقدامات متقابل موردبندی FTP ۱۰۸
موردبندی Telnet، TCP 23 ..... ۱۰۸
موردبندی SMTP، TCP 25 ..... ۱۱۱
اقدامات متقابل موردبندی SMTP ۱۱۲
اقدامات متقابل موردبندی DNS ۱۱۶
موردبندی TFTP، UDP 69/TCP ۱۱۸
اقدامات متقابل موردبندی TFTP ۱۱۹
اقدامات متقابل Finger ۱۲۱
مورد بندی HTTP، TCP 80 ..... ۱۲۲
مورد بندی Microsoft RPC Endpoint Mapper(MSRPC)، TCP 135 ..... ۱۲۶
موردبندی سرویس نام NetBIOS، UDP 137 ..... ۱۲۹
اقدامات متقابل موردبندی سرویس‌های نام NetBIOS ۱۳۵
موردبندی جلسه [session] NetBIOS، 445/TCP 139 ..... ۱۳۶
موردبندی SMB از طریق TCP 139 (جلسه NetBIOS) و TCP 445 SMB (over raw) ۱۳۷
اقدامات متقابل جلسه پوچ SMB ۱۴۹
موردبندی SNMP، UDP 161 ..... ۱۵۶
موردبندی BGP، TCP 179 ..... ۱۶۳
اقدامات متقابل مورد بندی مسیریابی BGP ۱۶۶
مورد بندی LDAP اکتیو دایرکتوری ویندوز، UDP/TCP، 389 و ۳۲۶۸ ..... ۱۶۶
اقدامات متقابل موردبندی اکتیودایرکتوری ۱۶۹
مورد بندی Novell NetWare، TCP 524 و IPX ۱۷۱
اقدامات متقابل NetWare ۱۷۵
موردبندی RPC یونیکس، UDP/TCP، ۱۱۱و ۳۲۷۷۷ ..... ۱۷۶
اقدامات متقابل موردبندی RPC ۱۷۹
rwho (UDP 513) و rusers (برنامه RPC 100002) ۱۷۹
اقدامات متقابل rwhoو ruser ۱۸۰
موردبندی NIS، برنامه RPC 100004 ..... ۱۸۰
موردبندی سرویس SQL Resolution، UDP 1434 ..... ۱۸۱
اقدامات متقابل موردبندی نمونه SQL ۱۸۲
موردبندی OracleTNS، 2483/TCP 1521 ..... ۱۸۲
اقدامات متقابل مورد بندی Oracle TNS ۱۸۴
موردبندی NFS، TCP/UDP 2049 ..... ۱۸۵

بخش ۲: هک کردن سیستم

فصل ۴: هک کردن ویندوز

چه چیزی پوشش داده نمی‌شود ۱۹۸
حمله‌های اعتبار سنجی نشده ۱۹۸

حمله‌های کلاهبرداری اعتبار سنجی ۱۹۹
حدس زدن رمز عبور از راه دور ۱۹۹
استراق سمع در تبادل رمز عبور شبکه ۲۰۷
اقدامات متقابل ردیابی اعتبارسنجی ویندوز ۲۰۹
حمله‌های Middle–The–In–Man ۲۱۱
اقدامات متقابل MITM ۲۱۳
سوء استخراج‌های غیرمعتبر راه دور ۲۱۴
سوء استخراج‌های سرویس شبکه ۲۱۴
اقدامات متقابل سوء استخراج سرویس شبکه ۲۱۶
سو استخراج‌های برنامه‌های کاربر نهایی ۲۱۸
اقدامات متقابل برنامه کاربر نهایی ۲۱۹
سوء استخراج‌های درایور وسیله ۲۲۰
اقدامات متقابل سوء استخراج درایور ۲۲۱
حمله‌های معتبرشده ۲۲۲
تعدیل امتیاز ویژه [Privilege Escalation] ۲۲۲
جلوگیری از تعدیل امتیازات ویژه ۲۲۳
استخراج و کرک کردن رمزهای عبور ۲۲۴
قاپیدن رمزهای عبور هش شده ۲۲۴
اقدامات متقابل pwdump ۲۲۷
کرک کردن رمزهای عبور ۲۲۷
دامپینگ رمزهای عبور ذخیره شده [Dumping Cached Passwords] ۲۳۳
اقدامات متقابل کپی برداری ذخیره رمزعبور ۲۳۶
کنترل راه دور و درها ی پشتی [Back Doors] ۲۳۷
ابزارهای کنترل راه دور خط فرمان ۲۳۷
کنترل راه دور گرافیکی ۲۳۹
تغییر مسیر درگاه [Redirection] ۲۴۲
پاک کردن لوگ رویداد ۲۴۵
اقدامات متقابل ADS ۲۴۷
Rootkitها ۲۴۷
اقدامات متقابل عمومی‌برای آشکار سازی دارای اعتبار ۲۴۸
مدخل‌های رجیستری ۲۴۹
پردازش‌ها ۲۵۰
درگاه‌ها ۲۵۱
ویژگی‌های امنیتی ویندوز ۲۵۲
دیواره آتش ویندوز ۲۵۲
به روز رسانی‌های خودکار ۲۵۳
Security Policy و Group Polic ۲۵۵
Bitlocker و سیستم فایل رمزنگاری [the Encrypting File System] (EFS) ۲۵۶
با ویندوز ویستا، مایکروسافت رمزنگاری Bitlocker درایو ۲۵۸
اقدامات متقابل بوت سرد ۲۵۸
محافظت از منابع ویندوز ۲۵۹
سطوح جامعییت [Integrity Levels] ، UAC، و LoRIE ۲۶۰

ممانعت از اجرای داده [Data Execution Prevention] (DEP) ۲۶۲
مستحکم کردن سرویس ۲۶۳
ایزوله کردن جلسه ۲۶۶
بهبودهای مبتنی بر کامپایلر [based Enhancements–Compiler] ۲۶۷
Coda: وزنه امنیت ویندوز ۲۶۹

فصل ۵: هک کردن یونیکس

در طلب ریشه ۲۷۳
نگاشت آسیب پذیری ۲۷۴
دسترسی راه دور در برابر دسترسی محلی ۲۷۵
دسترسی راه دور ۲۷۶
حمله‌های force–Brute ۲۷۸
حمله‌های برپایه داده [Driven Attacks–Data] ۲۸۲
حمله‌های سرریز بافر ۲۸۲
اقدامات متقابل حمله سرریز بافر ۲۸۴
حمله‌های Format String ۲۸۸
اقدامات متقابل حمله‌های format string ۲۹۰
حمله‌های تایید اعتبار ورودی [Input Validation Attacks] ۲۹۱
حمله‌های سرریز عدد صحیح و علامت عدد صحیح ۲۹۳
اقدامات متقابل حمله سرریز عدد صحیح ۲۹۷
حمله‌های Dangling Pointer ۲۹۸
اقدامات متقابل Dangling Pointerها ۲۹۹
من پوشهٔ خودم را می‌خواهم ۳۰۰
telnet معکوس و کانال‌های پشتی ۳۰۱
اقدامات متقابل کانال پشتی ۳۰۴
انواع معمول حمله‌های راه دور ۳۰۵
اقدامات متقابل FTP ۳۰۶
اقدامات متقابل sendmail ۳۰۷
سرویس‌های Remote Procedure Call ۳۰۸
پروتکل مدیریت شبکه ساده [Simple Network Management Protocol] (SNMP) ۳۱۲
اقدامات متقابل SNMP ۳۱۳
اقدامات متقابل NFS ۳۲۰
ناامنی‌های X ۳۲۰
اقدامات متقابل X ۳۲۳
سیستم نام دامنه (DNS) ۳۲۳
مسمومیت ذخیره DNS [DNS Cache Poisoning] ۳۲۴
حمله‌های سرریز DNS TSIG ۳۲۶
نا امنی‌های SSH ۳۲۸
آسیب پذیری چالش–پاسخ OpenSSH ۳۲۹
اقدامات متقابل SSH ۳۳۰
حمله‌های سرریز بافر OpenSSL ۳۳۰
اقدامات متقابل OpenSSL ۳۳۲
حمله‌های Apache ۳۳۲

اقدامات متقابل Apache ۳۳۳
حمله‌های حالت بی قرار ۳۳۳
دسترسی محلی ۳۳۵
آسیب پذیری‌های ترکیب رمز عبور ۳۳۵
John the Ripper ۳۳۷
اقدامات متقابل ترکیب رمز عبور ۳۴۲
سرریز بافر محلی ۳۴۲
اقدامات متقابل سرریز بافر محلی ۳۴۳
اقدامات متقابل Symlink ۳۴۵
شرایط رقابت [Race Conditions] ۳۴۶
اقدامات متقابل اداره کردن سیگنال ۳۴۷
اصلاح فایل هسته [Core File Manipulation] ۳۴۷
اقدامات متقابل فایل هسته ۳۴۸
کتابخانه‌های مشترک ۳۴۸
اقدامات متقابل کتابخانه‌های مشترک ۳۴۹
رخنه‌های کرنل ۳۵۰
اقدامات متقابل رخنه‌های کرنل ۳۵۱
پیکربندی اشتباه سیستم ۳۵۱
مجوزهای فایل و دایرکتوری ۳۵۱
فایل‌های SUID Set user ID (SUID) and set group ID (SGID) kill files root ۳۵۲
اقدامات متقابل فایل‌های SUID ۳۵۴
اقدامات متقابل فایل‌های با قابلیت نوشتن جهانی ۳۵۶
بعد از هک کردن ریشه ۳۵۶
Rootkitها ۳۵۷
اسب‌های تروا ۳۵۷
اقدامات متقابل اسب تروا ۳۵۹
ردیاب‌ها [sniffers] ۳۶۱
ردیاب چیست؟ ۳۶۱
چگونه ردیاب‌های کار می‌کنند ۳۶۲
ردیاب‌های محبوب ۳۶۳
اقدامات متقابل ردیابی ۳۶۳
پاک کردن لوگ ۳۶۵
اقدامات متقابل پاک کردن لوگ ۳۷۱
Rootkitهای کرنل ۳۷۱
اقدامات متقابل rootkit کرنل ۳۷۴
بازیابی rootkit ۳۷۵
بخش ۳: شالودهٔ هک کردن
فصل ۶: هک کردن اتصال راه دور و VOIP
مهیا شده برای DIAL UP ۳۸۴
ردنگاری شماره تلفن ۳۸۴
اقدامات متقابل نشتی ۳۸۶
سخت افزار ۳۸۷

مسائل قانونی ۳۸۸
هزینه‌های جانبی ۳۸۹
نرم افزار ۳۸۹
ToneLoc ۳۹۱
فایل‌های batch در ToneLoc ۳۹۴
THC-Scan ۳۹۷
PhoneSweep ۴۰۱
تکنیک‌های سوء استخراج حامل ۴۰۴
اسکریپت‌نویسی BRUTE-FORCE– روش کار در منزل ۴۰۷
Low Hanging Fruit ۴۰۹
اعتبارسنجی تک، تلاش‌های نامحدود ۴۱۰
اعتبارسنجی تک، تلاش‌های محدود ۴۱۴
اعتبارسنجی دوتایی، تلاش‌های نامحدود ۴۱۶
اعتبارسنجی دوتایی، تلاش‌های محدود ۴۱۷
آخرین نکته درباره اسکریپت‌نویسی Force–Brute ۴۱۹
اقدامات متقابل امنیت Up–Dial ۴۱۹
هک کردن PBX ۴۲۱
Octel Voice Network Login ۴۲۲
Northern Telecom PBX/Williams ۴۲۳
Meridian Links ۴۲۴
System 75 /ATT Defi nity G ۴۲۵
PBX محافظت شده توسط Server/ACE ۴۲۶
هک کردن نامه صوتی [VOICEMAIL] ۴۲۷
هک کردن نامه صوتی با روش Brute-Foce ۴۲۷
اقدامات متقابل هک کردن brute-force نامه صوتی ۴۳۳
هک کردن شبکه خصوصی مجازی [VIRTUAL PRIVATE NETWORK] (VPN) ۴۳۳
شکستن PPTP مایکروسافت ۴۳۵
تعمیر کردن PPTP ۴۳۶
تحلیلی کارشناسانه بر IPSec: سبک و سنگین مردن توسط اسکینر و فرگوسن ۴۳۷
اصول IPSec VPN ها ۴۳۸
اعتبارسنجی و استقرار تونل در VPNهای IPSec ۴۳۹
هک کردن گوگل برای VPN ۴۳۹
اقدامات متقابل هک کردن گوگل برای VPN ۴۴۱
کاوش کردن سرورهای IPSec VPN ۴۴۲
اقدامات متقابل کاوش IPSec VPN ۴۴۳
حمله به IKE در حالت تهاجمی ۴۴۳
حمله‌های VICE OVER IP ۴۴۵
حمله به VoIP ۴۴۷
اسکن کردن SIP ۴۴۷
اقدامات متقابل اسکن کردن SIP ۴۴۸
غارت TFTP برای گنج‌های VoIP ۴۴۸
اقدامات متقابل غارت TTP ۴۴۹

موردبندی کاربران SIP ۴۵۰
موردبندی REGISTERکاربر در Asterisk ۴۵۰
موردبندی کاربر از طریق SIP EXpress RouterOPTIONS ۴۵۳
مورد بندی کاربر به طور خودکار ۴۵۶
اقدامات متقابل موردبندی SIP ۴۵۹
حمله‌های استراق سمع ۴۵۹
اقدامات متقابل استراق سمع ۴۶۴
طغیان‌های [Floods] SIP INIVTE ۴۶۵
اقدامات متقابل طغیان SIP INVITE ۴۶۶
فصل ۷: وسایل شبکه
اکتشاف ۴۷۰
شناسایی ۴۷۰
پروفایل کردن ۴۷۰
اقدامات متقابل dig ۴۷۲
traceroute ۴۷۲
اقدامات متقابل traceroute ۴۷۴
جستجوی IP ۴۷۴
جستجوی سیستم خودمختار [AUTONOMOUS SYSTEM LOOKUP] ۴۷۵
رهیابی طبیعی ۴۷۵
رهیابی با اطلاعات ASN ۴۷۶
نشان دادن ip bgp ۴۷۷
گروهای خبری عمومی ۴۷۸
اقدامات متقابل پروفایل کردن ۴۷۹
شناسایی سرویس ۴۷۹
nmap ۴۷۹
اقدامات متقابل شناسایی سرویس ۴۸۱
شناسایی سیستم عامل ۴۸۴
اقدامات متقابل شناسایی سیستم عامل ۴۸۵
قاپیدن علامت و مورد بندی Cisco ۴۸۵
اقدامات متقابل قاپیدن علامت و مورد بندی Cisco ۴۸۶
آسیب پذیری شبکه ۴۸۶
لایه ۱ از OSI ۴۸۷
لایه ۲ از OSI ۴۸۹
شناسایی رسانه لایه ۲ ..... ۴۸۹
ردیابی سوییچ ۴۹۰
تغییر مسیر ARP ۴۹۱
اقدامات متقابل ARP Redirect ۴۹۴
ردیابی سراسری ۴۹۵
اقدامات متقابل ردیابی انتشار سراسری ۵۰۱
پرش VLAN ۵۰۱
اقدامات متقابل پرش VLAN ۵۰۳
سوییت حمله پروتکل مسیریابی Internetwork (IRPAS) و پروتکل اکتشاف Cisco (CDP) ۵۰۴

اقدامات متقابل CDP ۵۰۵
حمله‌های پروتکلی درخت پوشا [Spanning Tree Protocol] (STP) ۵۰۶
اقدامات متقابل محاسبه مجدد STP ۵۰۶
حمله‌های پروتکل شاه سیم کردن VLAN (VTP) ۵۰۷
اقدامات متقابل VTP ۵۰۷
لایه ۳ از OSI ۵۰۷
پروتکل اینترنت نگارش ۴ (IPv4) ۵۰۷
پیش‌گویی عدد ترتیبی TCP ۵۰۸
IP نگارش ۶ یا آی پی: نسل بعد (IPng) ۵۰۸
اقدامات متقابل استراق سمع/ردیابی ۵۱۰
اقدامات متقابل dsniff ۵۱۳
اقدامات متقابل Ettercap ۵۱۴
پیکربندی‌های اشتباه ۵۱۴
خواندن/نوشتن MIB ۵۱۴
اقدامات متقابل برای نوشتن Net MIB برای Cisco ۵۱۸
رمزنگاری ضعیف Cisco ۵۱۸
دانلوهای TFTP ۵۲۰
اقدامات متقابل TFTP ۵۲۰
هک کردن پروتکل مسیریابی ۵۲۱
کلاهبرداری RIP ۵۲۱
پروتکل مسیریابی دروازه داخلی [Interior Gateway Routing Protocol] (IGRP) ۵۲۴
اول کوتاهترین مسیر باز [Open Shortest Path First] (OSPF) ۵۲۶
تزریق بسته BGP کلاهبرداری شده ۵۲۹
اقدامات متقابل حمله پروتکل مسیریابی ۵۳۳
هک کردن پروتکل مدیریت ۵۳۴
اداره تله و در خواست SNMP ۵۳۴
اقدامات متقابل اداره تله و درخواست SNMP ۵۳۴

فصل ۸: هک کردن بی‌سیم

ردنگاری بی سیم ۵۴۰
تجهیزات ۵۴۱
کارت‌ها ۵۴۱
آنتن‌ها ۵۴۳
نرم افزار حرکت جنگی ۵۴۵
NetStumbler ۵۴۹
اقدامات متقابل NetStumbler ۵۵۰
Kismet ۵۵۱
اقدامات متقابل Kismet ۵۵۳
نقشه برداری بی سیم ۵۵۳
StumbVerter ۵۵۳
GPSMap ۵۵۴
JiGLE ۵۵۶
اسکن کردن و موردبندی بی سیم ۵۵۷

منابع ربودن و تحلیل بسته ۵۵۹
پیکربندی کارت‌های بی سیم لینوکس به وضعیت بی قاعده ۵۶۰
Tcpdump ۵۶۲
Wireshark ۵۶۳
Airfart ۵۶۴
OmniPeek ۵۶۵
Wifi Scanner ۵۶۶
اقدامات متقابل و دفاع در برابر شناسایی شبکه‌ها بی سیم ۵۶۷
SSID ۵۶۸
Void11 ..... ۵۷۱
WPA/WEP ۵۷۲
به دست آوردن دسترسی (هک کردن 802.11) ۵۷۳
SSID ۵۷۳
WEP ۵۷۶
حمله‌های علیه الگویتم WEP ۵۷۶
ابزارهایی که از WEP سو استخراج می‌کند ۵۷۸
AirSnort ۵۷۸
اقدامات متقابل AirSnort ۵۷۹
DWEPCrack ۵۷۹
اقدامات متقابل DWEPCrack ۵۸۱
WEPAttack ۵۸۱
اقدامات متقابل WEPAttack ۵۸۲
اقدامات متقابل WEP ۵۸۲
اقدامات متقابل Anwrap ۵۸۴
Asleap ۵۸۴
اقدامات متقابل Asleap ۵۸۵
حمله علیه الگوریتم WPA ۵۸۶
عدم سرویس دهی ۵۸۷
ایمن کردن WPA ۵۸۷
منابع اضافی ۵۸۷
فصل ۹: هک کردن سخت افزار
دسترسی فیزیکی: ورود به داخل ۵۹۱
clone کردن کارت‌های دسترسی ۵۹۱
اقدامات متقابل clone کردن کارت دسترسی ۵۹۵
هک کردن وسایل ۵۹۶
دور زدن رمزعبور ATA ۵۹۶
اقدامات متقابل هک کردن ATA ۵۹۸
هک کردن USB U3 ..... ۵۹۸
اقدامات متقابل هک U3 ..... ۶۰۱
پیکربندی‌های پیش فرض ۶۰۱
خارج از جعبه ۶۰۱
رمزهای عبور استاندارد ۶۰۲

بلوتوث ۶۰۲
مهندسی معکوس سخت افزار ۶۰۳
نگاشت وسیله ۶۰۳
ردیابی داده‌های Bus ۶۰۴
معکوس کردن Firmware ۶۰۶
بخش ۴: هک کردن برنامه‌ها و داده‌ها
فصل ۱۰: هک کردن کد
تکنیک‌های سوء استخراج معمول ۶۱۸
سرریزهای بافر و رخنه‌های طراحی ۶۱۸
سریزهای بافر پشته ۶۱۹
اقدامات متقابل سریز باف پشته ۶۲۰
سرریزهای BSS/Heap/ داده ۶۲۲
اقدامات متقابل سرریز BSS/heap/ داده ۶۲۳
حمله‌های Format String ۶۲۳
اقدامات متقابل Format String ۶۲۴
خطاهای One-by-Off ۶۲۵
اقدامات متقابل One-by-Off ۶۲۵
حمله‌های تایید اعتبار ورودی ۶۲۶
حمله‌های قانونی سازی [Canonicalization] ۶۲۶
اقدامات متقابل قانونی سازی ۶۲۸
حمله‌های برنامه تحت وب و پایگاه داده ۶۲۹
اقدامات متقابل حمله برنامه تحت وب / پایگاه داده ۶۲۹
اقدامات متقابل معمول ۶۲۹
به نرمی‌صحبت کنید ۶۳۰
آن را به روش حکومتی کد کنید ۶۳۱
ذی‌حسابی ۶۳۲
مامور کردن یک رابط امنیتی در تیم توسعه ۶۳۲
آموزش ، آموزش، آموزش ۶۳۲
مدل سازی خطر ۶۳۳
چک لیست‌های کد ۶۳۴
آزمایش امنیت ۶۳۶
بررسی یا بازبینی امنیتی نهایی ۶۳۹
کنار هم قرار دادن ۶۴۰
تکنولوژی ۶۴۰
محیط‌های اجرا مدیریت شده ۶۴۱
کتابخانه‌های تایید اعتبار ورودی ۶۴۱
ارتقاء پلتفرم ۶۴۲
توصیه‌هایی برای خواندن بیشتر ۶۴۳
فصل ۱۱: هک کردن وب
هک کردن وب سرور ۶۴۵
فایل‌های مثال ۶۴۸
فاش شدن کد منبع ۶۴۸

حمله‌های قانونی سازی ۶۴۹
پسوندهای سرور ۶۵۰
سریزهای بافر ۶۵۳
اسکنرهای آسیب پذیری سرور وب ۶۵۵
هک کردن برنامه تحت وب ۶۵۶
پیدا کردن برنامه‌های آسیب‌پذیر با گوگل ۶۵۶
خزیدن در وب ۶۵۸
ابرازهای خزیدن وب ۶۵۹
ارزیابی برنامه تحت وب ۶۶۰
Plug-in های مرورگر ۶۶۱
سوییت‌های ابزار ۶۶۲
اسکنرهای امنیت برنامه تحت وب ۶۶۶
آسیب پذیری‌های برنامه‌های تحت وب معمول ۶۷۲
حمله‌های اسکریپت‌نویسی Site-Cross (XSS) ۶۷۳
اقدامات متقابل اسکریپت‌نویسی Site-Cross ۶۷۵
تزریق SQL ۶۷۶
اقدامات متقابل تزریق SQL ۶۷۹
جعل درخواست Site-Cross ۶۸۰
اقدامات متقابل جعل درخواست Cross_site ۶۸۱
تکه کردن پاسخ HTTP ۶۸۲
اقدامات متقابل تکه کردن پاسخ HTTP ۶۸۵
سوء استفاده از تگ‌های مخفی ۶۸۷
اقدامات متقابل تگ مخفی ۶۸۸
Includeهای سمت سرور (SSIها) ۶۸۸
اقدامات متقابل SSI ۶۸۹

فصل ۱۲: هک کردن کاربران وب

آسیب‌پذیری‌های کلاینت اینترنت ۶۹۲
تاریخی کوتاه از هک کردن کلاینت اینترنتی ۶۹۲
مایکروسافت اکتیو ایکس ۶۹۲
اقدامات متقابل سو استفاده از اکتیو ایکس ۶۹۴
جاوا ۶۹۵
اقدامات متقابل سو استفاده از جاوا ۶۹۶
جاوا اسکریپت و اسکریپت‌نویسی فعال [Active Scripting] ۶۹۶
اقدامات متقابل سوء استفاده از جاوا اسکریپت/اسکریپت‌نویسی فعال ۶۹۷
کوکی‌های ۶۹۷
اقدامات متقابل سو استفاده از کوکی ۶۹۸
اسکریپت‌نویسی Cross-Site (XSS) ۶۹۹
اقدامات متقابل XSS ۷۰۰
ناحیه ماشین محلی [Local Machine Zone] (LMZ) ۷۰۱
تگ IFRAME ۷۰۱
کنترل اکتیو ایکس HTML Help ۷۰۲
حمله‌های SSL ۷۰۲

حمله‌های Homograph ۷۰۴
اقدامات متقابل SSL ۷۰۴
Payloads and Drop Points ۷۰۶
هک کردن ایمیل ۷۰۶
فایل‌های ضمیمه ۷۰۷
MIME ۷۰۹
کرم‌های دفترچه آدرس ۷۱۰
اقدامات متقابل هک کردن ایمیل ۷۱۰
پیام رسان فوری ۷۱۲
سوء استخراج‌ها و اقدامات متقابل کلاینت اینترنتی مایکروسافت ۷۱۲
سرریز بافر پردازش کننده JPEG و GDI+ ۷۱۳
اقدامات متقابل سرریز بافرJPEG GDI+ ۷۱۵
قانونی سازی URP به طور نامناسب در IE ۷۱۶
اقدامات متقابل قانونی سازی URL به طور نامناسب در IE ۷۱۷
استثنای محلی HelpControl، HTML در IE ۷۱۸
اقدامات متقابل کنترل HTML Help در IE ۷۱۹
اقدامات متقابل عمومی‌سمت کلاینت مایکروسافت ۷۱۹
از کنترل‌های والدینی [Parental Controls] در ویندوز ویستا و ویندوز ۷ استفاده کنید ۷۲۱
خواندن ایمیل‌های به صورت متن ساده ۷۲۲
در اینترنت فریب نخورید ۷۲۳
چرا نباید از کلاینت‌های غیر مایکروسافت استفاده کرد؟ ۷۲۴
SOCIO– حمله‌های تکنیکی : ماهی‌گیری ودزدی شناسه ۷۲۵
تکنیک‌های ماهی‌گیری ۷۲۶
اقدامات متقابل ماهی‌گیری ۷۲۹
نرم افزار رنجش آور و فریبنده: Spyware، Adware و Spam ۷۳۰
تکنیک‌های جایگذاری معمول ۷۳۱
نقاط توسعه پذیر شروع خودکار ۷۳۱
الحاقات مرورگر وب ۷۳۲
مسدود کردن، شناسایی کردن، و پاک کردن نرم افزار رنجش آور و فریبنده ۷۳۳
MALWARE ۷۳۴
گونه‌های malware و تکنیک‌های معمول ۷۳۵
ویروس‌ها و زامبی‌ها ۷۳۵
Rootkitها و درهای پشتی ۷۳۷
Hacker Defender ۷۴۱
دیگر Rootkitهای معمول ۷۴۲
Botها و زامبی‌ها ۷۴۳
شناسایی و پاک کردن Malware ۷۴۵
عمل‌های بی درنگ ۷۴۵
پشتیان گیری، پهن کردن، و ساخت مجدد ۷۴۵
شناسایی و تمیزکاری ۷۵۶