



نفوذپذیری در شبکه و روش‌های مقابله

ترجمه: محسن مصطفی جوکار

سرشناسه	:	دهانجانی‌نیتش Nitesh.Dhanjani
عنوان و نام پدیدآور	:	نفوذپذیری در شبکه و روش‌های مقابله / [نیتش دهانجانی]: ترجمه محسن مصطفی‌جوکار.
مشخصات نشر	:	تهران: انتشارات فراهوش: آریاپارس، آریاپژوه، ۱۳۹۱.
مشخصات ظاهری	:	۲۸۸ ص: مصور.
شابک	:	۹۷۸-۹۶۴-۷۲۲۹-۸۶-۹
وضعیت فهرست نویسی	:	فیا
یادداشت	:	عنوان اصلی: portable reference Linux and UNIX security.
موضوع	:	سیستم عامل لینوکس
موضوع	:	یونیکس (فایل کامپیوتر)
موضوع	:	کامپیوترها — ایمنی اطلاعات
شناسه افزوده	:	مصطفی جوکار، محسن، مترجم
رده بندی کنگره	:	۷۱/۹۴ / ۱۳۹۱
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۳۷۱۸۷۲۷



<http://www.Farahoush.com>



نام کتاب: نفوذپذیری در شبکه و روش‌های مقابله

ترجمه: محسن مصطفی جوکار

ناشر: انتشارات فراهوش (زوبا سابق)

تکثیر تمام یا قسمتی از اثر بدون مجوز
کتبی ناشر ممنوع است و متخلفان به
موجب قانون حمایت حقوق مؤلفان،
مستفان و هنرمندان تحت پیگرد قانونی
قرار خواهند گرفت

نوبت چاپ: اول

سال چاپ: ۱۳۹۱

تعداد صفحات: ۲۸۸

تیراژ: ۱۰۰۰ نسخه

قیمت: ۱۱۰۰۰ تومان

شابک: ۹۷۸-۹۶۴-۷۲۲۹-۸۶-۹

ISBN: 978-964-7229-86-9

مرکز بخش:

بخش کتاب پَر پرواز:

تلفن: ۸۸۹۷۵۵۳۳

تلفن: ۸۸۹۷۵۵۳۳

فهرست مطالب

عنوان	صفحه
تقویدپذیری در شبکه	۱
و روش‌های مقابل	۱
ترجمه: محسن مصطفی جوکار	۱
فهرست مطالب	۳
مقدمه	۲۱
دستورهای عمومی	۲۳
آدرس IP	۳۱
نمادگذاری دهدهی	۳۱
کلاس‌ها:	۳۱
Class A	۳۱
Class B	۳۱
Class C	۳۲
Class D	۳۲
Class E	۳۳
Subnet Masks	۳۳
(CIDR) CLASSLESS INTER-DOMAIN ROUTING	۳۳
PREFIX/mask	۳۳
Loopback	۳۳
آدرس‌های خصوصی	۳۴
هدر IP (پروتکل اینترنت)	۳۴
هدر TCP (پروتکل کنترل انتقال)	۳۵
هدر UDP (پروتکل داده‌های کاربر)	۳۵
منابع اینترنتی	۳۶
ابزارهای هک	۳۶
منابع تحت وب	۴۰

۴۱.....	لیست‌های پستی
۴۲.....	کنفرانس‌ها و رویدادها
۴۲.....	دستورات مفید NETCAT
۴۴.....	جدول اسکی
۵۰.....	کدهای HTTP
۵۲.....	فایل‌های مهم
۵۵.....	بخش اول
۵۵.....	تکنیک‌های هک و دفاع
۵۷.....	فصل اول
۵۸.....	موتورهای جستجو
۵۸.....	جستجوی مطالب کاری ارسال شده برای نقاط ضعف کاری
۵۸.....	جستجوی EDGAR
۵۹.....	به دنبال اطلاعات حساس در فایل‌های SNA
۶۰.....	جستجو برای آمار وب سرور
۶۰.....	ردیابی منابع داده ای محافظت شده
۶۱.....	به دنبال اطلاعات حساس از طریق فایل‌های بک‌آپ
۶۱.....	جستجوی آرشیو USENET برای کمپوهای اجرایی
۶۲.....	دفاع در برابر در معرض قرار گرفتن موتور جستجو
۶۲.....	شرکت‌های ثبت دامنه
۶۳.....	پرس و جوی سوابق ثبت دامنه با نام دامنه
۶۴.....	جستجوی ثوابق ثبت دامنه به وسیله پیشوند دامنه
۶۶.....	پرس و جوی رکوردهای شرکت ثبت دامنه به وسیله هندل کردن آنها
۶۷.....	پرس و جوی رکوردهای شرکت ثبت دامنه از طریق ایمیل
۶۷.....	جلوگیری از مواجه شدن با رکوردهای شرکت ثبت دامنه
۶۷.....	ثبت اینترنت منطقه ای
۶۷.....	جستجوی رکوردهای RIR به وسیله پیشوند شرکت
۶۸.....	جستجوی رکوردهای RIR به وسیله یک آدرس IP یا بلاک شبکه
۷۰.....	پرس و جوی رکوردهای RIR به وسیله اجرا کردن آن
۷۱.....	پرس و جوی رکوردهای RIR به وسیله ایمیل
۷۱.....	جلوگیری از مواجه شدن با رکوردهای RIR

۷۱.....	DNS REVERSE-LOOKUPS
۷۱.....	انجام یک DNS REVERSE-LOOKUPS
۷۲.....	جلوگیری از مواجه شدن با DNS REVERSE-LOOKUP
۷۲.....	MAIL EXCHANGE
۷۳.....	ZONE TRANSFERS
۷۳.....	انجام ZONE TRANSFERS با استفاده از دستور HOST
۷۵.....	جلوگیری از نفوذ ZONE TRANSFER
۷۵.....	TRACEROUTE
۷۵.....	انجام TRACEROUTE
۷۶.....	جلوگیری از ورود درخواستهای TRACEROUTE
۷۶.....	خلاصه
۷۷.....	فصل ۲
۷۷.....	پویش و شناسایی
۷۸.....	PING کردن
۷۹.....	PING کردن میزبان با استفاده از ابزار PING
۷۹.....	PING SWEEPING
۷۹.....	استفاده از NMAP برای انجام PING SWEEP
۸۰.....	بلاک کردن ICMP
۸۰.....	PING کردن TCP
۸۰.....	استفاده از NMAP برای انجام TCP PING
۸۱.....	جلوگیری از پویش TCP PING
۸۱.....	پویش پورت
۸۱.....	اتصال TCP
۸۲.....	استفاده از NMAP برای انجام پویش پورت از نوع اتصال TCP
۸۲.....	پویش FTP BOUNCE
۸۲.....	TCP SYN/HALF-OPEN
۸۳.....	پویش SYN
۸۳.....	پویش پورت منبع
۸۴.....	FIN
۸۴.....	پویش FIN

۸۴.....	IDENT معکوس
۸۴.....	پویش IDENT معکوس
۸۵.....	XMAS
۸۵.....	پویش XMAS
۸۵.....	NULL
۸۶.....	پویش NULL
۸۶.....	RPC
۸۶.....	پویش RPC
۸۷.....	پروتکل IP
۸۷.....	پویش پروتکل IP
۸۷.....	ACK
۸۸.....	پویش ACK
۸۸.....	WINDOW
۸۸.....	پویش WINDOW
۸۸.....	UDP
۸۸.....	پویش پورت UDP
۸۸.....	نقاع در برابر پویش پورت
۸۹.....	انگشت نگاری
۸۹.....	انگشت نگاری سیستم عامل با استفاده XPROBE2
۹۱.....	استفاده از NMAP برای انجام انگشت نگاری سیستم عامل
۹۲.....	خلاصه
۹۳.....	فصل سوم
۹۳.....	در این فصل:
۹۴.....	شمارش سرویس‌های راه دور
۹۴.....	شناسایی سرویس‌های از راه دور با استفاده از AMAP
۹۵.....	متوقف کردن و مسدود کردن سرویس‌های غیر ضروری
۹۵.....	FTP (پروتکل انتقال فایل): 21 (TCP)
۹۵.....	به دست آوردن پتر از سرور FTP
۹۶.....	تغییر دادن پتر مربوط به سرور FTP
۹۶.....	SSH (شیل امن): 22 (TCP)

۹۶.....	به دست آوردن بئر از SSH سرور
۹۶.....	تغییر دادن اطلاعات نسخه SSH
۹۷.....	به دست آوردن بئر از سرور TELNET
۹۷.....	تغییر بئر مربوط به سرور TELNET
۹۸.....	SMTP (پروتکل انتقال ساده ایمیل): 25 (TCP)
۹۸.....	گرفتن بئر مربوط به سرور SMTP
۹۸.....	تغییر بئر مربوط به سرور SMTP
۹۸.....	شمارش کاربران به وسیله EXPN و VRFY
۹۹.....	خاموش کردن EXPN و VRFY
۹۹.....	DNS (سیستم نام دانه): 53 (TCP/UDP)
۹۹.....	به دست آوردن اطلاعات مربوط به نسخه BIND
۱۰۰.....	پیکربندی BIND برای نمایش ندادن اطلاعات مربوط به نسخه
۱۰۰.....	(FINGER: 79 (TCP
۱۰۰.....	شمارش کاربران از راه دور به وسیله استفاده از دستور FINGER
۱۰۱.....	غیرفعال کردن FINGER
۱۰۲.....	HTTP (پروتکل انتقال ابر متن): 80 (TCP)
۱۰۳.....	تغییر بئر مربوط به سرور HTTP
۱۰۳.....	POP3 (پروتکل اداره پست ۳): 110 (TCP)
۱۰۴.....	به دست آوردن بئر از سرور POP3
۱۰۴.....	تغییر دادن بئر مربوط به سرور POP3
۱۰۴.....	TCP (PORTMAPPER: 111)
۱۰۴.....	پرس و جوی PORTMAPPER برای سرویس‌های RPC
۱۰۶.....	غیرفعال کردن سرویس‌های PORTMAPPER و RPC
۱۰۶.....	NNTP (پروتکل انتقال خبر در شبکه): 119 (TCP)
۱۰۶.....	به دست آوردن بئر از سرور NNTP
۱۰۶.....	تغییر بئر مربوط به سرور NNTP
۱۰۷.....	TCP AND UDP (SAMBA: 137 TO 139)
۱۰۷.....	تغییر دادن اطلاعات مربوط به نسخه سرور SAMBA
۱۰۸.....	IMAP2/IMAP4 (پروتکل دسترسی به پیام 2/4): 143 (TCP)
۱۰۸.....	تغییر بئر مربوط به سرور NNTP

تغییر دادن پتر مربوط به سرور IMAP	۱۰۸
SNMP (پروتکل ساده مدیریت شبکه): 161, 162 (UDP)	۱۰۸
شمارش SNMP	۱۰۸
جلوگیری از شمارش SNMP	۱۰۹
HTTPS (پروتکل امن انتقال ابر متن): 443 (TCP)	۱۰۹
به دست آوردن پتر از سرور HTTPS	۱۱۰
تغییر پتر مربوط به سرور HTTPS	۱۱۰
NNTPS (پروتکل امن انتقال خبر در شبکه): 563 (TCP)	۱۱۰
گرفتن پتر از سرور NNTPS	۱۱۰
تغییر پتر مربوط به سرور NNTPS	۱۱۱
IMAPS (پروتکل امن دسترسی به پیام در اینترنت): 993 (TCP)	۱۱۱
گرفتن پتر از سرور IMAPS	۱۱۱
تغییر پتر مربوط به سرور IMAPS	۱۱۱
POP3S (پروتکل امن اداره پست ۳): 995 (TCP)	۱۱۱
به دست آوردن پتر از سرور POP3S	۱۱۲
تغییر پتر مربوط به سرور POP3S	۱۱۲
شمارش اطلاعات مربوط به نسخه MySQL	۱۱۲
فقط امکان اجازه به ارتباط محلی را بدهید	۱۱۲
خودکار سازی گرفتن پتر	۱۱۳
خلاصه	۱۱۵
فصل چهارم	۱۱۷
در این فصل:	۱۱۷
سرویس‌های راه دور	۱۱۸
تاکتیک‌های نفوذ	۱۱۸
BRUTE-FORCING	۱۱۸
نفاع‌های متداول در برابر حملات BRUTE-FORCE	۱۱۹
بو کشیدن	۱۱۹
اقدامات متقابل با بو کشیدن	۱۲۰
MAN-IN-THE-MIDDLE	۱۲۱
جلوگیری از حمله MAN-IN-THE-MIDDLE	۱۲۱

۱۲۱		پیکربندی نادرست
۱۲۲		بازرسی و پیکربندی استوار میزبان
۱۲۲		دفاع‌های متداول علیه آسیب پذیری نرم‌افزار
۱۲۳		آسیب پذیری‌های سرویس از راه دور
۱۲۳		شناخت سرویس‌های در حال اجرا بر روی پورتهای غیر استاندارد
۱۲۴		مسدود و متوقف کردن سرویس‌های غیرضروری
۱۲۴		FTP (پروتکل انتقال فایل): 21 (FTP)
۱۲۴		BRUTE-FORCING
۱۲۴		BRUTE-FORCE کردن FTP
۱۲۵		جلوگیری از BRUTE-FORCE کردن FTP
۱۲۵		بو کشیدن
۱۲۵		بو کشیدن تصدیق FTP
۱۲۵		از پروتکل‌های امن استفاده کنید
۱۲۶		BOUNCE ATTACKS
۱۲۶		جلوگیری از حملات BOUNCE
۱۲۶		سرقت اتصال
۱۲۷		جلوگیری از اتصال به حملات سرقت
۱۲۷		آسیب پذیری نرم‌افزار
۱۲۸		LONG PATH OVERFLOW VULNERABILITY
۱۲۸		SSH (SECURE SHELL): 22 (TCP)
۱۲۸		BRUTE-FORCING
۱۲۸		BRUTE-FORCE SSH
۱۲۹		SSH BRUTE-FORCING از
۱۲۹		حمله SSH MAN-IN-THE-MIDDLE
۱۲۹		ETTERCAP و SSHMITM
۱۲۹		جلوگیری از حملات MAN-IN-THE-MIDDLE در برابر SSH
۱۲۹		آسیب پذیری نرم‌افزار
۱۲۹		چالش سرریز بافر OPENSSH
۱۳۰		TCP (TELNET: 23)
۱۳۰		BRUTE-FORCING

۱۳۰	 TELNET کردن BRUTE-FORCE
۱۳۰	 TELNET کردن BRUTE-FORCE از جلوگیری
۱۳۰	 TCP ربودن
۱۳۱	 TELNET ربودن جلسات
۱۳۲	 SSH استفاده از
۱۳۲	 بو کشیدن
۱۳۲	 بو کشیدن احراز هویت TELNET
۱۳۳	 از TELNET استفاده نکنید
۱۳۳	 آسیب پذیری نرم افزار
۱۳۳	 SMTP (پروتکل ساده انتقال پست الکترونیکی): 25 (TCP)
۱۳۳	 بو کشیدن ترافیک SMTP
۱۳۴	 رمزگذاری پست‌های الکترونیکی
۱۳۴	 آسیب پذیری نرم افزار
۱۳۴	 آسیب پذیری سر ریز بافر SENDMAIL در پردازش هدر
۱۳۵	 آسیب پذیری SENDMAIL MIME
۱۳۵	 سرریز بافر HELO در SENDMAIL
۱۳۵	 آسیب پذیری سرریز بافر در رکورد SENDMAIL DNS MAP TXT
۱۳۵	 DNS (سیستم نام دامنه): 53 (TCP و UDP)
۱۳۶	 حقه بازی
۱۳۶	 جعل کردن پاسخ‌های DNS
۱۳۷	 آسیب پذیری نرم افزار
۱۳۷	 آسیب پذیری DOS و سرریز بافر BIND NXT
۱۳۷	 TFTP (پروتکل انتقال فایل بی اهمیت): 69 (UDP)
۱۳۷	 بو کشیدن
۱۳۷	 بو کشیدن داده‌های TFTP
۱۳۸	 از پروتکل‌های امن استفاده کنید
۱۳۹	 پیکربندی اشتباه TFTP
۱۳۹	 به دست آوردن فایل‌های بحرانی سیستم
۱۳۹	 تنظیم دایرکتوری ریشه TFTP
۱۳۹	 HTTP (پروتکل انتقال ابر متن): 80 (TCP)

۱۳۹	 BRUTE-FORCING
۱۴۰	 BRUTE-FORCE کردن هویت HTTP
۱۴۰	 جلودگیری از BRUTE-FORCE کردن HTTP
۱۴۰	 بو کشیدن
۱۴۰	 بو کشیدن URLها
۱۴۱	 بو کشیدن اطلاعات HTTP
۱۴۳	 بو کشیدن هویت HTTP
۱۴۳	 استفاده از HTTPS
۱۴۳	 پیکربندی اشتباه HTTP
۱۴۳	 فهرست کردن خودکار
۱۴۴	 خاموش کردن فهرست گیری
۱۴۴	 به دست آوردن کد منبع، تنظیمات، آمار و منابع کلمه عبور
۱۴۴	 منابع حیاتی را به خدمت نگیرید
۱۴۵	 آسیب پذیری برنامه‌های کاربردی تحت وب
۱۴۵	 بهره برداری از ورودی نامناسب
۱۴۶	 جلودگیری از آسیب پذیری اعتبار سنجی ورودی
۱۴۶	 ربودن جلسه
۱۴۶	 جلودگیری از ربودن جلسه
۱۴۷	 پنهان کردن عناصر HTML
۱۴۷	 به عناصر پنهان HTML اعتماد نکنید
۱۴۷	 توضیحات کد منبع
۱۴۸	 بررسی توضیحات برای کد منبع
۱۴۸	 آسیب پذیری وب سرور
۱۴۸	 آسیب پذیری تکه جابجایی وب سایت و سرور آپاچی
۱۴۸	 POP2 (پروتکل اداره پست شماره ۲): 109 (TCP)
۱۴۸	 BRUTE-FORCE کردن
۱۴۸	 بو کشیدن
۱۴۹	 بو کشیدن ترافیک POP2
۱۴۹	 تونل کردن ترافیک POP2 از طریق SSH
۱۴۹	 POP3 (پروتکل اداره پست شماره ۳): ۱۱۰ (TCP)

۱۴۹		BRUTE-FORCE کردن
۱۴۹		POP3 کردن BRUTE-FORCE
۱۴۹		جولوگیری از BRUTE-FORCE کردن POP3
۱۵۰		بو کشیدن
۱۵۰		بو کشیدن کلمه‌های عبور POP3
۱۵۰		تونل کردن ترافیک POP3 از طریق SSH
۱۵۰		TCP (PORTMAPPER: 111)
۱۵۱		پیکربندی اشتباه
۱۵۱		پرس و جو از راه دور برای فایل‌های به اشتراک گذاشته شده NFS
۱۵۱		بلوک و استوار کردن NFS
۱۵۱		آسیب پذیری نرم افزار
۱۵۲		NNTP (پروتکل انتقال اخبار در شبکه): 119 (TCP)
۱۵۲		BRUTE-FORCE کردن
۱۵۲		NNTP کردن BRUTE-FORCE
۱۵۲		جولوگیری از BRUTE-FORCE کردن NNTP
۱۵۲		بو کشیدن
۱۵۲		بو کشیدن اطلاعات احراز هویت NNTP
۱۵۲		تونل کردن NNTP از طریق SSH
۱۵۴		BRUTE-FORCE کردن
۱۵۴		SAMBA کردن BRUTE-FORCE
۱۵۴		جولوگیری از BRUTE-FORCE کردن SAMBA
۱۵۴		بو کشیدن
۱۵۴		به دست آوردن کلمه عبور HASH شده SAMBA
۱۵۵		تونل و ایمن کردن ترافیک SAMBA
۱۵۵		پیکربندی نادرست SAMBA
۱۵۵		شمارش و نصب کردن فایل‌های به اشتراک گذاشته SAMBA از راه دور
۱۵۶		بلاک کردن و تونل کردن ترافیک SAMBA
۱۵۶		IMAP2/IMAP4 (پروتکل دسترسی به پیام‌های اینترنتی 2/4): 143 (TCP)
۱۵۶		BRUTE-FORCE کردن
۱۵۶		جولوگیری از BRUTE-FORCE کردن IMAP

۱۵۶	بو کشیدن
۱۵۶	بو کشیدن ترافیک IMAP
۱۵۷	جایگزینی امن
۱۵۷	HTTPS (پروتکل امن انتقال ابرمتن): 443 (TCP)
۱۵۷	آسیب پذیری نرم افزار
۱۵۷	سرریز بافر در OPENSSL SSLV2
۱۵۷	TCP (REXEC: 512)
۱۵۸	TCP (RLOGIN: 513)
۱۵۸	BRUTE-FORCE کردن
۱۵۸	بو کشیدن
۱۵۸	پیکربندی اشتباه RLOGIN
۱۵۸	پیکربندی اشتباه RHOSTS
۱۵۹	غیر فعال کردن RLOGIN و در نظر گرفتن جایگزین برای آن
۱۵۹	TCP (RSH: 514)
۱۵۹	NNTPS (پروتکل امن انتقال خبر در شبکه): 563 (TCP)
۱۵۹	IMAPS (پروتکل امن دسترسی به پیام در اینترنت): 993 (TCP)
۱۶۰	POP3S (پروتکل امن اداره پست ۳): 995 (TCP)
۱۶۰	(NFS: 2049 (TCP AND UDP)
۱۶۰	TCP (MySQL: 3306)
۱۶۰	BRUTE-FORCE کردن
۱۶۰	BRUTE-FORCE کردن MySQL
۱۶۱	جلوگیری از BRUTE-FORCE کردن MySQL
۱۶۱	بو کشیدن
۱۶۲	بو کشیدن ترافیک MySQL
۱۶۲	بلاک کردن و استوار کردن MySQL
۱۶۲	VNC (شبکه مجازی محاسبه): 5800, +5900 (TCP)
۱۶۲	BRUTE-FORCE کردن
۱۶۲	BRUTE-FORCE کردن VNC
۱۶۳	جلوگیری از BRUTE-FORCE کردن VNC
۱۶۳	بو کشیدن

۱۶۳	بو کشیدن و کرک کردن کلمه عبور VNC
۱۶۴	تونل کردن ترافیک VNC به صورت امن از طریق SSH
۱۶۴	پیگر بندی اشتباه VNC
۱۶۴	آسیب پذیری نرم افزار
۱۶۵	TCP (X: 6000 TO 6063)
۱۶۵	پیگر بندی اشتباه X
۱۶۵	سوء استفاده از پیگر بندی نادرست سرور X
۱۶۷	متوقف کردن تونل زدن X
۱۶۷	TCP 8000+ (WEB PROXIES)
۱۶۷	پیگر بندی اشتباه وب پروکسی ها
۱۶۸	حملات پروکسی
۱۶۸	حملات معکوس پروکسی
۱۶۸	متوقف کردن ارتباطات ورودی
۱۶۸	آسیب پذیری برنامه های کاربردی
۱۶۹	NFS ناقص و آسیب پذیری سرریز بافر در TCPDUMP
۱۶۹	آسیب پذیری سرریز صحت در NETSCAPE/MOZILLA POP3 MAIL
۱۶۹	آسیب پذیری از راه دور پشته در BITCHX
۱۶۹	آسیب پذیری سرریز بافر در پیام طولانی PGP4PINE
۱۷۰	جלוگیری از سوء استفاده از آسیب پذیری برنامه
۱۷۰	NESSUS
۱۷۱	به دست آوردن SHELL
۱۷۱	استفاده از NETCAT به منظور به دست آوردن یک SHELL از راه دور
۱۷۲	استفاده از XTERM برای به دست آوردن یک SHELL از راه دور
۱۷۲	جلوگیری از حملات به دست آوردن SHELL از راه دور
۱۷۳	تغییر مسیر پورت
۱۷۳	تغییر مسیر محلی پورت
۱۷۴	تغییر مسیر پورت از راه دور
۱۷۴	سخت کردن قوانین دیوار آتش
۱۷۴	کرک کردن ETC/SHADOW/
۱۷۵	استفاده از JOHN برای کرک کردن ETC/SHADOW/

از کلمات عبور قوی استفاده کنید	۱۷۵
خلاصه	۱۷۵
فصل پنجم	۱۷۷
تشدید امتیاز	۱۷۷
در این فصل:	۱۷۷
بهره برداری از اعتماد محلی	۱۷۸
پیدا کردن گروه مالک فایل ها	۱۷۸
پیدا کردن فایل های WORLD-READABLE و WORLD-WRITABLE	۱۷۹
اطمینان حاصل کردن از مجوزهای مناسب	۱۸۰
بهره برداری از " " در PATH برای قرار دادن Trojan ها	۱۸۰
" " را در PATH قرار ندهید	۱۸۱
آسیب پذیری نرم افزار	۱۸۱
معایب هسته	۱۸۱
بهره برداری از PTRACE	۱۸۱
به روزرسانی یا وصله کردن هسته	۱۸۲
اعتبار سنجی ورودی نامناسب	۱۸۲
لینکها نمادین	۱۸۲
CORE DUMPS	۱۸۲
آسیب پذیری بازایی فایل SHADOW مربوط به SOLARIS FTP CORE DUMP	۱۸۴
نصب فوری وصله های نرم افزار	۱۸۴
پیکربندی اشتباه	۱۸۵
خلاصه	۱۸۵
فصل ششم	۱۸۷
پنهان کردن	۱۸۷
در این فصل:	۱۸۷
پاک کردن LOG ها	۱۸۸
تاریخچه SHELL	۱۸۸
غیر فعال کردن تاریخچه SHELL	۱۸۹
فعال کردن سیستم حساسی و ورود به سیستم	۱۸۹
پاک کردن VAR/	۱۸۹

درهای پشتی.....	۱۹۰
نصب یک سرویس SHELL از راه دور.....	۱۹۰
جلوگیری از نصب سرویس SHELL از راه دور.....	۱۹۱
SHELL ها، SETUID و SETGID متعلق به ROOT هستند.....	۱۹۱
UID مربوط به حساب کاربری محلی را به 0 تغییر دهید.....	۱۹۲
اختصاص دادن 0 UID به یک کاربر محلی.....	۱۹۲
حسابرسی ETC/PASSWD/.....	۱۹۲
RHOSTS.....	۱۹۲
سوء استفاده از RHOSTS به منظور حصول اطمینان از دسترسی مداوم به ROOT.....	۱۹۲
بررسی RHOSTS و SSH را در نظر داشته باشید.....	۱۹۳
کلیدهای معتبر سازی SSH.....	۱۹۳
مکانیزم سوء استفاده از کلید معتبر SSH برای اطمینان از ادامه دسترسی ROOT.....	۱۹۳
به ROOT اجازه ورود از طریق SSH را ندهید.....	۱۹۴
LOKI2.....	۱۹۴
استوار کردن قوانین دیوار آتش.....	۱۹۴
TROJAN ها.....	۱۹۴
دستورات تروجانی متداول.....	۱۹۴
شناسایی TROJAN ها.....	۱۹۵
ROOTKIT ها.....	۱۹۵
ADORE.....	۱۹۵
LRK (LINUX ROOTKIT).....	۱۹۵
TORNKIT.....	۱۹۶
KNARK.....	۱۹۶
شناسایی ROOTKIT ها.....	۱۹۶
خلاصه.....	۱۹۶
بخش دوم.....	۱۹۷
امن کردن میزبان.....	۱۹۷
فصل هفتم.....	۱۹۹
تنظیمات پیش فرض و سرویس‌ها.....	۱۹۹
در این فصل:.....	۱۹۹

۲۰۰	تنظیم سیاست‌های کلمه عبور
۲۰۰	حذف و یا غیرفعال کردن حساب‌های کاربری غیر ضروری
۲۰۰	حذف کردن " " از متغیر PATH
۲۰۱	بررسی کردن محتویات ETC/HOSTS. EQUIV/
۲۰۱	بررسی کردن فایل. RHOSTS
۲۰۱	غیرفعال کردن روش پشته
۲۰۱	استفاده از TCP WRAPPER
۲۰۲	استوار کردن تنظیمات INETD و XINETD
۲۰۲	غیرفعال کردن سرویس‌های غیر ضروری
۲۰۳	اطمینان حاصل کنید که ورود به سیستم روشن است.
۲۰۳	استوار کردن سرویس‌های از راه دور
۲۰۴	SSH
۲۰۵	PROTOCOL 2
۲۰۵	PERMITROOTLOGIN NO
۲۰۶	(BIND) DNS
۲۰۷	(APACHE) HTTP AND HTTPS
۲۰۹	SAMBA
۲۰۹	NFS
۲۱۰	خلاصه
۲۱۱	فصل هشتم
۲۱۱	کاربر و امتیازات سیستم فایل
۲۱۱	در این فصل:
۲۱۲	شدیدا باید کنترل شود
۲۱۲	مجوزهای فایل: خودآموز سریع
۲۱۳	فایل‌های WORLD-READABLE
۲۱۴	فایل‌های WORLD-WRITABLE
۲۱۴	فایل‌های متعلق به BIN و SYS
۲۱۴	مقدار UMASK
۲۱۵	فایل‌های مهم
۲۱۸	فایل‌های داخل /DEV

۲۱۸	پارتیشن‌های دیسک
۲۱۹	فایل‌های SETUID و SETGID
۲۱۹	پیاده‌سازی گروه‌های چرخشی
۲۱۹	SUDO
۲۲۰	خلاصه
۲۲۱	فصل نهم
۲۲۱	ورود به سیستم و وصله کردن
۲۲۱	در این فصل:
۲۲۲	ورود به سیستم
۲۲۲	فایل‌های LOG
۲۲۳	VAR/ADM/LOGINLOG
۲۲۳	VAR/ADM/SULOG
۲۲۳	VAR/LOG/CRON
۲۲۴	چرخه ورود به سیستم
۲۲۵	فضای خالی در VAR/
۲۲۵	وصله کردن
۲۲۶	خلاصه
۲۲۷	بخش ۴
۲۲۷	موضوع ویژه
۲۲۹	فصل دهم
۲۲۹	NESSUS ATTACK SCRIPTING LANGUAGE
۲۲۹	(NASL)
۲۲۹	در این فصل:
۲۳۰	اجرای اسکریپت‌های NASL از طریق خط فرمان
۲۳۰	نوشتن PLUG-IN‌های NESSUS با استفاده از NASL
۲۳۰	یک مثال از آسیب پذیری
۲۳۱	PLUG-IN
۲۳۴	اجرای یک PLUG-IN
۲۳۵	خلاصه
۲۳۷	فصل یازدهم

۲۳۷	هک کردن شبکه بی سیم
۲۳۷	در این فصل:
۲۳۸	معرفی WEP
۲۳۹	آنتن‌ها
۲۳۹	هدایتی
۲۳۹	آنتن‌های گیرنده یا فرستنده امواج در جهت مناسب
۲۴۰	ابزارهای محبوب
۲۴۰	AIRSNORT
۲۴۱	KISMET
۲۴۱	FATA-JACK
۲۴۲	امن کردن شبکه‌های بی سیم
۲۴۲	۱- فرض کنید که شبکه امن نیست
۲۴۲	۲- تشویق به منظور ابزارهایی که از رمزنگاری استفاده می‌کنند
۲۴۲	۳- به نقاط دسترسی برای اداره شبکه بی سیم اجازه ندهید
۲۴۳	۴- ESSID پیش فرض را تغییر داده و broadcast را غیرفعال کنید
۲۴۳	۵- فیلتر کردن آدرس MAC
۲۴۳	خلاصه
۲۴۵	فصل نوزدهم
۲۴۵	هک کردن با
۲۴۵	SHARP ZAIRUS PDA
۲۴۵	در این فصل:
۲۴۶	KISMET
۲۴۷	WELLENREITER
۲۴۸	BING
۲۴۹	OPENS5H
۲۴۹	HPING2
۲۵۰	VNC SERVER
۲۵۱	KEYPEBBLE VNC VIEWER
۲۵۲	SMBMOUNT
۲۵۲	TCPDUMP

۲۵۳	 WGET
۲۵۳	 ZETHEREAL
۲۵۳	 ZNESSUS
۲۵۴	 MTR
۲۵۴	 DIG
۲۵۵	 PERL
۲۵۵	 ZAUROS منابع آنلاین برای
۲۵۵	 خلاصه
۲۵۷	 دستورالعمل پیشرفته گوگل
۲۵۷	 (GOOGLE DORK)

مقدمه

این کتاب به شما آموزش می‌دهد که یک هکر عیناً به چه صورتی فکر می‌کند، بنابراین شما می‌توانید از سیستم لینوکس یا یونیکس خود در مقابل آن‌ها محافظت کنید. این کاملاً ساده است و راه دیگری برای آموزش شما در مورد جلوگیری از در خطر افتادن سیستم شما وجود ندارد. برای جلوگیری از حملات پیچیده‌تر هکرها شما نیاز به درک فرایندها، تکنیک‌ها و تاکتیک‌ها دارید. ماهیت قدرتمند سیستم عامل‌های یونیکس و لینوکس، یک شمشیر دو لبه بودن آن‌ها است. در اغلب موارد، کد منبع هست سیستم عامل به صورت رایگان در دسترس است، و یک مدیر شبکه می‌تواند درون سیستم عامل را با توجه به نیاز خود تغییر دهد. اما این طبیعت قدرتمند و انعطاف پذیر یونیکس و لینوکس، شامل مقدار زیادی پیچیدگی است که احتمال اینکه سیستم به راحتی در معرض خطر بیافتد را افزایش می‌دهد. لازم به ذکر است امروزه توزیع‌های مختلفی از یونیکس و لینوکس در دسترس است. هر توزیع به همراه مجموعه‌ای از سیاست‌های امنیتی و تنظیمات مربوط به خودش می‌آید. برای مثال برخی از توزیع‌ها، مجموعه‌ای از سرویس‌های کنترل از راه دور را خاموش کرده‌اند، در صورتیکه توزیع‌های دیگر تمام سرویس‌های موجود را که ممکن است توسط ضعیف‌ترین سیاست‌ها پیکربندی شوند، روشن گذاشته‌اند. هکرها از پیچیدگی‌های مدیریتی میزبان‌های یونیکس و لینوکس آگاه هستند و دقیقاً هکرها می‌دانند چگونه از آن‌ها سوء استفاده کنند. این کتاب شما را با جزئیات تاکتیک‌های فریبنده هکرها آشنا می‌کند و به شما آموزش می‌دهد که چگونه در برابر آن‌ها از خود دفاع کنید. هدف از این کتاب نمایش تاکتیک‌هایی است که توسط هکرها امروزه مورد استفاده قرار می‌گیرند، به طوری که شما محافظت از خود در برابر آن‌ها را یاد می‌گیرید. هنگامی که شما درک می‌کنید چگونه یک هکر فکر می‌کند و از چه روش‌های مختلفی برای شکستن سیستم استفاده می‌کند، این به نفع شماست.