

۱۴۱۹.۹۲
۹۵/۱۸

به نام خدا



مؤسسه فرهنگی علمی
دیبانگران تهران

مرجع آموزشی امنیت شبکه های کامپیوتری

مؤلفان:

حمید رضا قنبری

خانم حسنی احمدی پور

سجاد محمد زاده



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.

مرجع آمرزشی

امنیت شبکه های کامپیوتری

مؤلفان: حمیدرضا قنبری، نسیمی احمدی پور
سجاد محمدرده

ناشر: مؤسسه فرهنگی هنری دیباگران، تهران

حروفچینی و صفحه آرایی: شبنم دانش راده

طرح روی جلد: سحر نژاد محمدی

چاپ: دانشجو

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۵

تیراژ: ۱۵۰۰ جلد

قیمت: ۴۸۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۵۶۲-۶

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۰۲۲-۸۵۱۱۱۱-۶۶۴۱۰۰۴۶ کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: bookmarket@mftmail.com

فروش اینترنتی:

www.mftshop.com

www.mftbook.ir

نشانی اینستاگرام: [Dibagaran_publishing](https://www.instagram.com/Dibagaran_publishing)

نشانی تلگرام: [@mftbook](https://www.telegram.me/mftbook)

سرشناسه: قنبری، حمیدرضا، ۱۳۶۸-
عنوان و نام پدید آور: مرجع آموزشی امنیت شبکه های کامپیوتری/مؤلفان: حمیدرضا قنبری، نسیمی احمدی پور، سجاد محمد زاده.
مشخصات نشر: تهران- دیباگران تهران- ۱۳۹۵
مشخصات ظاهری: ۴۷۸ ص. مصور.
شابک: ۹۷۸-۶۰۰-۱۲۴-۵۶۲-۶
نوعیت فهرست نویسی: فیبا
یادداشت: کتابنامه: ص. ۴۷۸-۴۸۸.
موضوع: شبکه های کامپیوتری - تدابیر امنیتی
موضوع: computer networks-security measures
شناسه اثر: احمدی، نسیمی، ۱۳۶۹-
شناسه افزوده: زاده، سجاد، ۱۳۶۸-
رده بندی کنگره: ۳۹۵، م ۹/۱، ۵۱۰۵، ۲۴
رده بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۴۶۲۱۹۵۲

مقدمه: آشنایی با ساختار شبکه های کامپیوتری

۱۳	۱- معرفی شبکه های کامپیوتری
۱۴	۱-۱- تقسیم بندی بر اساس نوع وظایف
۱۷	۱-۲- تقسیم بندی بر اساس توپولوژی
۲۷	۱-۳- مبانی شبکه های بدون کابل
۳۲	۱-۴- سیستم عامل شبکه
۳۳	۱-۵- کلاسبیت ها و منابع
۳۴	۱-۶- پیکل
۳۶	۱-۷- محدود لایه های مختلف
۴۱	۱-۸- معرفی برخی اصطلاحات شبکه های کامپیوتری
۴۴	۲- آشنایی با سیستم های شبکه
۴۴	۲-۱- CABLING
۵۹	۲-۲- تولد مودم ها
۷۵	۲-۳- کارت شبکه
۸۲	۲-۴- روتر
۹۳	۲-۵- سوئیچ
۱۱۲	۲-۶- نصب و راه اندازی شبکه
۱۱۵	۲-۷- PDA
۱۲۸	۳- پروتکل های شبکه
۱۳۶	۳-۱- IP
۱۴۲	۳-۲- DNS
۱۵۹	۳-۳- DSL
۱۷۲	۳-۴- NAT
۱۸۴	۳-۵- شبکه های خصوصی مجازی
۱۹۶	۳-۶- WAP
۱۹۹	۳-۷- مانیتورینگ دسترسی در ویندوز XP
۲۰۳	۳-۸- شبکه نوری
۲۰۷	۴- فایروال
۲۰۸	۴-۱- فایروال چیست ؟

۲۱۲ ۴-۲- تهدیدات :

۲۱۳ ۴-۳- سرویس دهنده Proxy :

فصل اول: دیوارهای آتش در شبکه های محلی و سازمانی

۲۱۵ ۱- دیوارهای آتش شبکه :

۲۱۵ ۱-۱- مقدمه :

۲۱۶ ۲-۱- یک دیوار آتش چیست؟ :

۲۱۸ ۳-۱- دیوارهای آتش چه کاری انجام می دهند؟ :

۲۱۸ ۱-۳-۱- اثرات مثبت :

۲۲۰ ۲-۳-۱- اثرات منفی :

۲۲۱ ۴-۱- دیوارهای آتش چه کارهایی را نمی توانند انجام دهند؟ :

۲۲۳ ۵-۱- چگونه دیوارهای آتش عمل می کنند؟ :

۲۲۴ ۶-۱- انواع دیوارهای آتش :

۲۲۵ ۱-۶-۱- فیلتر کردن بسته (Packet Filtering) :

۲۳۲ ۲-۶-۱- بازرسی هوشمند بسته (Stateful Packet Inspection) :

۲۳۶ ۳-۶-۱- دروازه برنامه های کاربردی و پراکسیها :

۲۴۲ ۴-۶-۱- پراکسی های قابل تطبیق (Adaptive Proxies) :

۲۴۳ ۵-۶-۱- دروازه سطح مداری (Circuit - Level Gateway) :

۲۴۴ ۶-۶-۱- وانمود کننده ها (Impostors) :

۲۴۷ ۷-۱- جنبه های مهم دیوارهای آتش کارآمد :

۲۴۸ ۸-۱- معماری دیوار آتش (FIREWALL ARCHITECTURE) :

۲۴۹ ۱-۸-۱- مسیریاب فیلتر کننده بسته (Packet Filtering Router) :

۲۵۰ ۲-۸-۱- میزبان غربال شده یا میزبان سنگر :

۲۵۱ ۳-۸-۱- دروازه دو خانه ای (Dual - homed Gateway) :

۲۵۲ ۴-۸-۱- زیر شبکه غربال شده یا منطقه غیرنظامی :

۲۵۳ ۵-۸-۱- دستگاه دیوار آتش (Firewall Appliance) :

۲۵۴ ۹-۱- انتخاب و پیاده سازی یک راه حل دیوار آتش :

۲۵۴ ۱-۹-۱- آیا شما نیاز به یک دیوار آتش دارید؟ :

۲۵۵	۲-۹-۱ - دیوار آتش، چه چیزی را باید کنترل یا محافظت کند؟
۲۵۶	۳-۹-۱ - یک دیوار آتش، چه تأثیری روی سازمان، شبکه و کاربران شما خواهد گذاشت؟
۲۵۸	۱۰-۱ - سیاست امنیتی (SECURITY POLICY)
۲۵۹	۱-۱۰-۱ - موضوعات اجرایی (Administrative Issues)
۲۶۰	۲-۱۰-۱ - موضوعات فنی (Technical Issues)
۲۶۱	۱۱-۱ - نیازهای پیاده سازی
۲۶۱	۱-۱۱-۱ - نیازهای فنی
۲۶۲	۳-۱۱-۱ - معماری
۲۶۳	۱۲-۱ - نصب و راه اندازی
۲۶۴	۱۳-۱ - پیاده سازی و آزمایش
۲۶۴	۱-۱۳-۱ - آزمایش، آزمایش، آزمایش
۲۶۵	۱۴-۱ - خلاصه

فصل دوم: پیاده سازی دیوار آتش با استفاده از IPTABLES

۲۶۷	۱-۲ - مقدمه
۲۶۹	۲-۲ - واژگان علمی مربوط به فیلتر سازی بسته
۲۷۲	۳-۲ - انتخاب یک ماشین برای دیوار آتش
۲۷۳	۴-۲ - به کار بردن MASQUERADING و IP FORWARDING
۲۷۸	۵-۲ - حسابداری بسته (PACKET ACCOUNTING)
۲۷۸	۶-۲ - جداول و زنجیرها در یک دیوار آتش مبتنی بر لینوکس
۲۸۲	۷-۲ - قوانین (RULES)
۲۸۳	۸-۲ - تطبیق ها (MATCHES)
۲۸۴	۹-۲ - اهداف (TARGETS)
۲۸۶	۱۰-۲ - پیکربندی IPTABLES
۲۸۷	۱۱-۲ - استفاده از IPTABLES
۲۸۸	۱-۱۱-۲ - مشخصات فیلتر سازی (Filtering Specifications)
۲۹۲	۲-۱۱-۲ - تعمیم هایی برای iptables (تطبیق های جدید)
۳۰۴	۳-۱۱-۲ - مشخصات هدف (Target Specifications)
۳۰۷	۴-۱۱-۲ - عملیات روی یک زنجیر کامل
۳۱۰	۱۲-۲ - ترکیب NAT با فیلتر سازی بسته

۳۱۰..... ۱-۱۲-۲- ترجمه آدرس شبکه (NAT)

۳۱۲..... ۲-۱۲-۲- NAT مبدأ و Masquerading

۳۱۵..... ۳-۱۲-۲- NAT مقصد

۳۱۶..... ۱۳-۲- ذخیره نمودن و برگرداندن قوانین

فصل سوم: امنیت شبکه های دورن سازمانی

۳۱۹..... ۱-۳- مفاهیم امنیت شبکه های درون سازمانی و شبکه های WAN

۳۲۰..... ۲-۳- منابع شبکه

۳۲۱..... ۳-۳- حمله

۳۲۲..... ۴-۳- تحلیل خطر

۳۲۲..... ۵-۳- سیاست امنیتی

۳۲۳..... ۶-۳- طرح امنیت شبکه

۳۲۴..... ۷-۳- نواحی امنیتی

۳۲۴..... ۸-۳- توپولوژی شبکه

۳۲۵..... ۹-۳- محل های امن برای تجهیزات

۳۲۶..... ۱۰-۳- انتخاب لایه کانال ارتباطی امن

۳۲۷..... ۱۱-۳- منابع تغذیه

۳۲۸..... ۱۲-۳- عوامل محیطی

۳۲۸..... ۱۳-۳- قابلیت های امنیتی

۳۲۹..... ۱۴-۳- مشکلات اعمال ملزومات امنیتی

۳۲۹..... ۱-۱۴-۳- رویکردی عملی به امنیت شبکه لایه بندی شده

۳۳۰..... ۲-۱۴-۳- افزودن به ضریب عملکرد هرکرها

۳۳۱..... ۳-۱۴-۳- رویکردی عملی به امنیت شبکه لایه بندی شده (۲)

۳۳۶..... ۴-۱۴-۳- رویکردی عملی به امنیت شبکه لایه بندی شده

۳۳۹..... ۱۵-۳- پراکسی سرور

۳۴۰..... ۱-۱۵-۳- عملکردهایی که پراکسی سرور می تواند داشته باشد:

۳۴۱..... ۲-۱۵-۳- پیکربندی مرورگر

۳۴۲..... ۳-۱۵-۳- پراکسی چیست؟

۳۴۲..... ۴-۱۵-۳- پراکسی چه چیزی نیست؟

۳۴۴..... ۱۶-۳- STATEFULL PACKET خیلترهای

۳۴۴	۱۷-۳-پراکسی ها یا APPLICATION GATEWAYS
۳۴۵	۱-۱۷-۳-کاربرد پراکسی در امنیت شبکه
۳۴۶	۲-۱۷-۳-نوعی انواع پراکسی
۳۵۴	۱۸-۳-نتیجه گیری
۳۵۴	۱-۱۸-۳-مقایسه تشخیص نفوذ و پیش گیری از نفوذ
۳۵۵	۲-۱۸-۳-تشخیص نفوذ
۳۵۶	۳-۱۸-۳-پیش گیری از نفوذ
۳۵۷	۴-۱۸-۳-نتیجه نهایی
۳۵۸	۱۹-۳-روش های معمول حمله به کامپیوترها (۱)
۳۵۹	۱-۱۹-۳-برنامه های اسب تروا
۳۵۹	۲-۱۹-۳-درها و پشت برنامه های مدیریت از راه دور
۳۵۹	۳-۱۹-۳-عدم پذیرش ویس
۳۶۰	۴-۱۹-۳-وساطت برای حملات دیگر
۳۶۱	۵-۱۹-۳-اشتراک های ویندوزی حفاظت نشده
۳۶۱	۶-۱۹-۳-کدهای قابل انتقال (ActiveX و JavaScript و Java)
۳۶۳	۱۹-۳-روش های معمول حمله به کامپیوترها (۱)
۳۶۳	۷-۱۹-۳-اسکرپت های Cross-Site
۳۶۳	۸-۱۹-۳-ایمیل های جعلی
۳۶۵	۹-۱۹-۳-ویروس های داخل ایمیل
۳۶۵	۱۰-۱۹-۳-پسوند های مخفی فایل
۳۶۶	۱۱-۱۹-۳-سرویس گیرندگان چت
۳۶۷	۱۲-۱۹-۳-شنود بسته های اطلاعات
۳۶۸	۲۰-۳-کلیدها در رمزنگاری
۳۷۱	۱-۲۰-۳-رمزنگاری
۳۸۰	۲۱-۳-استاندارد های حفاظت از کلمه عبور
۳۸۱	۲۲-۳-ده نکته برای حفظ امنیت

فصل چهارم: شبکه های بی سیم و امنیت در آنها

۳۸۶	۱-۴- شبکه های بی سیم، کاربردها، مزایا و ابعاد
۳۸۸	۱-۱-۴- اساس شبکه های بی سیم
۳۸۸	۲-۱-۴- Wi - Fi حکومت عالی
۳۸۹	۳-۱-۴- 802.11a یک استاندارد نوپا
۳۹۰	۴-۱-۴- Blue tooth قطع کردن سیم ها
۳۹۲	۵-۱-۴- Blue tooth: استیانی خصوصی
۳۹۳	۶-۱-۴- به پیش رو داریم
۳۹۴	۷-۱-۴- منشا ذف امنیت در شبکه های بی سیم و خطرات معمولی
۳۹۶	۲-۴- شبکه های محلی بی سیم
۳۹۶	۱-۲-۴- پیشینه
۳۹۷	۲-۲-۴- معماری شبکه های محلی بی سیم
۳۹۹	۳-۴- عناصر فعال و سطح پوشش W/N
۳۹۹	۱-۳-۴- عناصر فعال شبکه های محلی بی سیم
۴۰۳	۴-۴- امنیت در شبکه های محلی براساس استاندارد 802.11
۴۰۴	۱-۴-۴- قابلیت ها و ابعاد امنیتی استاندارد 802.11
۴۰۶	۵-۴- سرویسهای امنیتی WEP- AUTHENTICATION
۴۰۶	۱-۵-۴- Authentication
۴۰۷	۲-۵-۴- Authentication بدون رمزنگاری
۴۰۸	۳-۵-۴- Authentication با رمزنگاری RC4
۴۰۹	۶-۴- سرویس های امنیتی INTEGRITY, 802.11B-PRIVACY
۴۰۹	۱-۶-۴- privacy
۴۱۱	۲-۶-۴- Integrity
۴۱۳	۷-۴- ضعف های اولیه امنیتی WEP
۴۱۴	۱-۷-۴- استفاده از کلیدهای ثابت WEP
۴۱۴	۲-۷-۴- Initialization vector
۴۱۵	۳-۷-۴- ضعف در الگوریتم

- ۴۱۵..... ۴-۷-۴ استفاده از CRC رمز نشده
- ۴۱۶..... ۸-۴ خطرها، حملات و ملزومات امنیتی
- ۴۱۷..... ۴-۸-۱ حملات غیرفعال
- ۴۱۷..... ۴-۸-۲ شنود
- ۴۱۷..... ۴-۸-۳ آنالیز ترافیک
- ۴۱۷..... ۴-۸-۴ حملات فعال
- ۴۱۹..... ۴-۹-۹ پیاده سازی شبکه بی سیم
- ۴۱۹..... ۴-۹-۱ دست به کار شوید
- ۴۲۰..... ۴-۹-۹ دست به کار شوید
- ۴۲۱..... ۴-۹-۹ راه اندازی یک شبکه بی سیم
- ۴۲۲..... ۴-۹-۴ دست را بالا بردن
- ۴۲۴..... ۴-۹-۵ محافظت از شبکه
- ۴۲۶..... ۴-۱۰-۱ معرفی WAP
- ۴۲۶..... ۴-۱۰-۱ WAP چیست؟
- ۴۲۸..... ۴-۱۰-۲ ایده WAP
- ۴۲۹..... ۴-۱۰-۳ معماری WAP
- ۴۳۰..... ۴-۱۰-۴ مدل WAP
- ۴۳۱..... ۴-۱۰-۵ WAP تا چه اندازه امن است؟
- ۴۳۲..... ۴-۱۱-۱ مفاهیم امنیت شبکه
- ۴۳۲..... ۴-۱۱-۱ منابع شبکه
- ۴۳۳..... ۴-۱۱-۲ حمله
- ۴۳۴..... ۴-۱۱-۳ تحلیل خطر
- ۴۳۵..... ۴-۱۱-۴ سیاست امنیتی
- ۴۳۶..... ۴-۱۱-۵ طرح امنیت شبکه
- ۴۳۷..... ۴-۱۱-۶ خواص امنیتی
- ۴۳۸..... ۴-۱۱-۷ مرکزی برای امنیت شبکه
- ۴۳۹..... ۴-۱۱-۸ چرا Service Directory

- ۴۴۱..... ۹-۱۱-۴-کتیو دایرکتوری چگونه کار می کند
- ۴۴۲..... ۱۰-۱۱-۴-مزایای اکتیو دایرکتوری
- ۴۴۴..... ۱۱-۱۱-۴-افزایش همکاری بین شبکه ها
- ۴۴۵..... ۱۲-۴-کنترل سازمانی
- ۴۴۵..... ۱۳-۴-کنترل فردی
- ۴۴۶..... ۱۴-۴-تقویت اینترنت ها
- ۴۴۷..... ۱۵-۴-وجود یک نظام قانونمند اینترنتی
- ۴۴۷..... ۱۶-۴-مار ۴ سرده فرهنگی برای آگاهی کاربران
- ۴۴۸..... ۱۷-۴-فایروالها
- ۴۵۰..... ۱۸-۴-سیاست گذاری ملی در بستر جهانی
- ۴۵۰..... ۱-۱۸-۴-الگوی آمریکایی
- ۴۵۱..... ۲-۱۸-۴-الگوی فلسطینی
- ۴۵۲..... ۳-۱۸-۴-الگوی چینی
- ۴۵۳..... ۴-۱۸-۴-الگوی کشورهای عربی حاشیه خلیج فارس
- ۴۵۵..... ۱۹-۴-اینترنت و امنیت فرهنگی ایران
- ۴۵۷..... ۱-۱۹-۴-معیارهای امنیت فرهنگی در سیاست گذار
- ۴۵۷..... ۲-۱۹-۴-مشکلات فعلی سیاست گذاری در امنیت فرهنگی و اینترنت
- ۴۵۹..... ۳-۱۹-۴-ملاحظات فرهنگی در سیاست گذاری
- ۴۶۰..... ۲۰-۴-جمع بندی
- ۴۶۲..... ۲۱-۴-امنیت تجهیزات شبکه
- ۴۶۳..... ۱-۲۱-۴-امنیت فیزیکی
- ۴۶۸..... ۲-۲۱-۴-امنیت منطقی
- ۴۷۶..... منابع
- ۴۷۷..... منابع لاتین

خط مشی کیفیت انتشارات مؤسسه فرهنگی دیباگران تهران در عرصه کتاب الکترونیک است که بتواند خواسته های 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 علم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم مؤثر واقع شویم.

گسترده‌گی علوم و تخصص‌های روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در طبع و نشر هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و معتبرترین 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 و خردی رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "آقایان محمد رضا قنبری- سجاد محمد زاده و سرکار خانم حسنی احمدی پور" و تلاش جمعی از همکاران انتشارات مبسّر 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 می‌نمایم 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 مولف

در این کتاب خواهید آموخت :

- آشنایی جامع با ساختار شبکه های کامپیوتری
- آشنایی با ساختار امنیت در شبکه های کامپیوتری
- آشنایی با راه های آتش در شبکه های کامپیوتری محلی و سازمانی
- پیاده سازی یو آر آی با استفاده از iptables
- امنیت در شبکه های درون زمانی
- شبکه های بی سیم و امنیت شبکه های بی سیم

بر خود وظیفه می دانیم از زحمات سرکار هم قریب باش (واحد تالیف و ترجمه انتشارات دیباگران تهران) و مدیریت محترم انتشارات دیباگران به پاس راه های بی شمار و کمک آن ها کمال تشکر و قدردانی را داشته باشیم .

کار حاضر بدون شک خالی از اشکال نیست، امید است از ارشاد و راهنمایی دیگران و اهل فن بی بهره نباشیم.

تالیف و ترجمه : حمیدرضا قنبری

حسنی احمدی پور

سجاد محمد زاده

با همکاری : گروه فنی و مهندسی ذوق