

امنیت شبکه‌های میکروتیک



مهندس علیرضا فخرریمیمی

MTCNA , MTCRE , MikroTik Certified Consultant

مهندس الهام فخرریمیمی

MTCNA

ویراستار : مهندس امیر حسین جابری

MikroTik Certified Trainer / MTCWE / MTCRE / MTCNA



نشرگستر

با نامش ، یادش و به امید پشتوانه الطاف بیکران خداوندی‌اش

سرشناسه	: فخر رحیمی، علیرضا، ۱۳۶۲ -
عنوان و نام پدیدآور	: امنیت در میکروتیک/علیرضا فخر رحیمی ، الهام فخر رحیمی ؛ ویراستار امیرحسین جابری.
مشخصات نشر	: تهران : نشر گستر، ۱۳۹۰.
مشخصات ظاهری	: ۱۰۴ ص.
شابک	: 9786005883381 ریل : ۳۵۰۰۰
وضعیت فهرست نویسی	: فیبا
موضوع	: سیستم عمل اینترنتی میکروتیک
موضوع	: مسیریابها (شبکه کامپیوتری)
موضوع	: ارتباط بین شبکه‌ای
موضوع	: ارتباطات بی‌سیم
شناسه افزوده	: فخر رحیمی، الهام، ۱۳۶۲ -
رده بندی کنگره	: ۱۳۹۰ الف ۳/ن ۵۴۳/TK۵۱۰۵
رده بندی دهیوی	: ۰۴۴
شماره کتابشناسی ملی	: ۲۵۸۶۰۰۵



نشر گستر

نام کتاب : امنیت شبکه‌های میکروتیک

نویسندگان : علیرضا فخر رحیمی - الهام فخر رحیمی

نوبت چاپ : اول

تاریخ چاپ : ۱۳۹۰

تیراژ : ۱۰۰۰ جلد

قیمت : ۳۵۰۰ تومان

چاپ : پژمان

ناشر : انتشارات نشر گستر (۳-۱۵۶۱-۶۶۵۹)

بخش : persianmikrotik.ir و کتابفروشی اینترنتی فردا (۰۹۳۵۶۰۹۹۹۰۹)

فهرست مطالب

۱۱.....	پیش درآمد
۱۳.....	آشنایی با نمادهای کتاب
۱۵.....	بخش اول: مقدمه در مورد امنیت
۱۷.....	مبانی امنیتی و حملات
۱۸.....	مراحل هک
۱۸.....	شناسایی :
۱۸.....	مرحله دوم : پویش
۱۹.....	مرحله سوم : ایجاد دسترسی
۱۹.....	مرحله چهارم : حفظ دسترسی
۱۹.....	مرحله پنجم : از بین بردن ردپا
۱۹.....	اهداف حمله کننده ها
۲۰.....	امنیت ، عملکرد و سهولت استفاده
۲۱.....	جستجوی اطلاعات در اینترنت
۲۴.....	آشنایی با حملات DOS
۲۴.....	DoS چیست ؟
۲۵.....	چگونه از وقوع حملات DoS و یا DDoS آگاه شویم ؟
۲۵.....	در صورت بروز یک تهاجم ، چه عملیاتی را می بایست انجام داد ؟
۲۵.....	بررسی یک حمله DOS
۲۵.....	معرفی ابزارهای D.O.S
۲۶.....	آشنایی با Brute Force
۲۸.....	آشنایی با دیواره آتش
۲۸.....	روال کاری دیواره آتش
۲۹.....	آشنایی با دیواره آتش میکروتیک
۳۰.....	بررسی ارتباطات عبوری میکروتیک chain = forward
۳۰.....	بررسی ارتباطات ورودی chain= input
۳۱.....	گام اول : ایجاد یک قانون برای پذیرش ارتباطات از همان نشانی
۳۱.....	گام دوم : ایجاد یک قانون برای مسدود نمودن دسترسی هر نشانی IP دیگر
۳۲.....	لیست آدرس
۳۳.....	استفاده از لیست آدرس ها در دیواره آتش
۳۳.....	استفاده از لیست آدرس ها در میکروتیک
۳۴.....	بررسی chain=Forward

۳۶	ایجاد Log از برخی ارتباطات
۳۷	ارتباطات در میکروتیک
۳۸	Connection stat
۳۹	بخش دوم: امنیت در عمل
۴۱	تعیین مشخصه میکروتیک
۴۲	اطلاعات حاصل از winbox loader
۴۴	نصب آخرین نسخه Mikrotik Router OS
۴۶	حذف سرویس‌های غیر ضروری
۴۶	حذف بسته‌های نرم افزاری غیر ضروری
۴۷	کاربران و گذرواژه
۴۷	انتخاب کلمه عبور ایمن برای مدیر شبکه
۴۸	ایجاد کاربر Fail-Safe
۴۹	افزودن کاربر خاص
۵۰	ثبت وقایع
۵۳	مشاهده log
۵۴	نصب و پیکربندی Syslog Server
۵۷	مسدود نمودن ترافیک DHCP در شبکه
۵۸	ایمن سازی شبکه از طریق بکارگیری جدول ARP
۶۰	الزام کاربران به استفاده از DNS خاص
۶۱	محافظت در برابر حملات DoS
۶۲	گامهای رفع مشکل
۶۲	راهکارها
۶۲	محافظت
۶۴	اجازه برقراری ارتباط Telnet فقط به یک IPV6
۶۴	مشاهده گراف ها
۶۶	بررسی پهنای باند
۶۷	گزینه Hide Passwrod
۶۹	بخش سوم: امنیت کاربران
۷۱	ایجاد کاربران
۷۲	ایجاد گروههای کاربری خاص
۷۳	مسدود نمودن دسترسی کاربران از نشانی‌های متفرقه
۷۳	دسترسی از طریق Radius Server
۷۴	مشاهده کاربران در حال ارتباط با میکروتیک
۷۴	فعال یا غیرفعال نمودن سرویس‌ها بدون تغییر در بسته‌های نرم‌افزاری
۷۵	محدود نمودن ساعت دسترسی کاربران
۷۶	مسدود نمودن ارتباطات همه پختی
۷۷	امنیت کاربران Hotspot
۷۷	ایجاد پروفایل امنیتی خاص برای کاربران
۷۸	ایجاد کاربر خاص
۷۸	محدودیت کاربران

۷۹.....	مشاهده سیستم‌های مرتبط
۸۰.....	کاربرد IP bonding
۸۱.....	مسدود نمودن یا باز نمودن سایت‌های خاص برای کاربران
۸۲.....	بررسی سیستم‌های استفاده کننده از سرویس Hotspot در زمان مشخص
۸۳.....	محدودیت دسترسی کاربران به سایت‌ها یا نوع خاصی از فایل‌ها
۸۳.....	تنظیمات لازم برای ارسال بسته‌ها به پورت ۸۰۸۰
۸۳.....	تنظیمات web proxy
۸۵.....	انتقال همه سایت‌های درخواستی کاربر به یک وبسایت
۸۶.....	بررسی وضعیت Proxy
۸۷.....	مشاهده ارتباط serverها و Clientها
۸۸.....	مشاهده ارتباطات یک نشانی داخلی شبکه
۸۹.....	دسترسی مستقیم به یک سایت بدون اعمال قانون‌های Web proxy
۸۹.....	انسداد دسترسی به سایت‌های با نشانی خاص
۹۰.....	دسترسی به فقط یک وبسایت
۹۱.....	ثبت ارتباط به یک سایت
۹۲.....	لیست دسترسی
۹۳.....	افزودن ارتباطات به telnet و یمن ارتباطها
۹۵.....	Port Knocking
۹۶.....	ایجاد Certificate
۹۷.....	Import certificates
۹۸.....	امنیت در شبکه‌های بی سیم میکروتیک
۹۹.....	مسدود نمودن ارتباط مستقیم بین کاربران
۹۹.....	نکات امنیتی برای یک میکروتیک AP
۱۰۱.....	Connect list
۱۰۲.....	امنیت در میکروتیک‌های بی سیم
۱۰۲.....	ایجاد یک پروفایل امنیتی خاص

ای پادشاه خوبان داد از غم تنهایی
دایم گل این بیان شاداب نمی باشد
دیشب بخود ز قفس با باد همی کردم
صد باد مباری بجا با سلسله می رفته
شبان و مجرعی دور از تو چنانم کرد
یارب که شاید نیست این نکته که در عالم
ساقی چمن گل را می روی تو نیست
ای در تو ام در مان در بستر ناکامی
در دایره قسمت ما قطع یکیم
کفر خود و رای خود در عالم زندگی نیست
زین دایره سینا غمین بگرم می د
حافظ شب جبران شد بوی خوش و دل شاد

دل بی تو به جان آمد وقت است که باز آیی
در یاب نسیمان را در وقت توانایی
کتمان غلی بجه ز زمین بخت سودایی
این است تربیت ای دل تابا و پیمایی
کز دست بخوابد شد پایاب سلیبایی
رخسار و یکس خود آن شاد بهر جای
ششاد و خرامان کن تا باغ یارایی
وی یا تو ام مونس در کوشش تنهایی
لفت آنچه تو اندیشی کم آنچه تو فرمایی
کفر است در این نه بختی و خود را می
تا گل کنم این شغل در سا فرمایی
شادیت مبارک باد ای عاشق شیدایی

پیش در آمد

زمانی که صرف این کتاب و کتابهای قبلی در مورد میکروتیک شده بود می توانست به سادگی روزمرگی هایمان هدر رود ، اما تلنگر عزیزی که ما را به دانستن قدر زمان راهنمایی کرد ، انگیزه اصلی این کتاب شده که امیدواریم مفید باشد ، تقدیم لحظه لحظه ثانیه هایی که صرف نگارش این صفحات شده اند به وجود گرانسنگ آن عزیز اندک تشکری است که می توان از ایشان داشت.

از ابتدا در نظر داشتیم گام به گام با خوانندگان عزیز همراه باشیم ، تا بحال راه اندازی شبکه های میکروتیک و پیکربندی مسیر یاب های میکروتیک را با یکدیگر مرور کردیم ، گام بعدی پیاده سازی راهکارهایی برای ایمن سازی شبکه است . در این کتاب در سه بخش مباحث را با هم به صورت کاربردی پیاده سازی می کنیم .

لازم است این نکته را همواره مد نظر داشته باشیم که هر راهکاری ، هر الگویی و هر ترفندی ، هر چه قدر که موثر و دقیق باشد تنها شما را به امنیت ۹۹٪ می رساند! پس بدانید صرف پیکربندی یک سرویس دهنده تضمینی برای عدم نفوذ نخواهد شد . این نکته که امنیت ۱۰۰٪ دست نایافتنی است ، باعث پایش دائمی شبکه توسط مدیر شبکه و تغییرات پیوسته پیکربندی با توجه به شرایط خواهد شد .

تقدیم این کتاب به پدر و مادر عزیزمان و ویدای عزیز شاید سیاسی هر چند اندک از دریای بیکرانه تلاشهای بی پایانشان باشد که امیدوارم پذیرای این هدیه ناچیزمان باشند.

علیرضا فخررحیمی

MTCNA # 1109NA183

MTCRE# 1112RE018

Mikrotik Certified Consultant

Security + #6339 /A/330/2795

Security in Computers and Internet #

252059

الهام فخررحیمی

MTCNA# 1112NA091