

به نام خدا

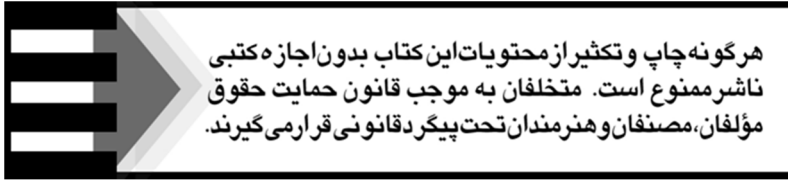


امنیت تجهیزات شبکه ای

سیسکو

مترجم:

مهندس حمید کریمخانی زندی



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: امنیت تجهیزات شبکه ای سیسکو

◀ عنوان اصلی : Securing CISCO Network Devices-student guide

◀ مترجم : مهندس حمید کریمخانی زندی

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرابی: شبینم هاشم زاده

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۳۹۷

◀ چاپ و صحافی: دانشجو

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۵۲۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۰۰-۱۲۴-۸۹۵-۵

◀ نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۰۴۶۴۱۰۰۶۶-۲۰۸۵۱۱۱

کد پستی: ۱۳۱۴۹۸۳۱۸۵

◀ فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

www.mftdibagaran.ir

◀ نشانی تلگرام: @mftbook لینک ربات دیباگران : @dibagarantehranbot

◀ اپتیکیشن دیباگران تهران را از سایت های اینترنتی دیباگران دریافت نمایید.

عنوان و نام پدیدآور: امنیت تجهیزات شبکه ای سیسکو/مترجم: حمید کریمخانی زندی.
مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۷
مشخصات ظاهری: ۴۱۰ ص: مصور، جدول، نمودار
شابک: ۹۷۸-۶۰۰-۱۲۴-۸۹۵-۵
وضعیت فهرست نویسی: فیبا
یادداشت: عنوان اصلی : securing CISCO network devices :student guide ۲۰۰۵
موضوع: سیستم عامل اینترنتی سیسکو
موضوع: Cisco ios
موضوع: شبکه های کامپیوتری-تدابیر ایمنی
موضوع: computer networks-security measures
موضوع: ارتباط بین شبکه ای
موضوع: internetworking(telecommunication)
شناسه افزوده: کریمخانی زندی، حمید، ۱۳۵۸- مترجم
رده بندی کنگره: ۱۳۹۷ الف ۸ /TK ۵۱۰۵/۵۴۳
رده بندی دیویی: ۰۰۴/۶۲
شماره کتابشناسی ملی: ۵۲۰۰۳۴۱

فهرست کتاب

۱۱.....	بخش اول
۱۱.....	معرفی مجموعه ی امنیتی سیسکو.....
۱۲.....	دیدگاه کلی.....
۱۲.....	اهداف.....
۱۴.....	معرفی مجموعه ی امنیتی سیسکو.....
۱۶.....	امنیت محیطی. محصولات و راه حل ها.....
۲۵.....	راهنمای کاربرد.....
۲۵.....	مهمترین نکات دیواره آتش IOS سیسکو.....
۳۱.....	ارتباط ایمن- راه حل های VPN ها.....
۳۵.....	ارتباط ایمن. متمرکز کننده سری VPN ۳۰۰۰ سیسکو.....
۴۳.....	ارتباط ایمن. مسیریاب های دارای توانایی VPN سیسکو.....
۴۹.....	ارتباط ایمن. جایگاه محصولات VPN
۵۰.....	راه حل های سیستم پیشگیری از تهاجم.....
۵۶.....	راه حل های سیستم پیشگیری از تهاجم شبکه - محیطهای سرویس دهنده ی IPS سیسکو.....
۶۰.....	راه حل های سیستم پیشگیری از تهاجم در میزبان.....
۶۷.....	راه حل های شناسایی. سرویس دهنده ی کنترل دسترسی امنیتی سیسکو.....
۷۱.....	کنترل پذیرش شبکه.....
۷۴.....	راه حل های مدیریت امنیتی- مرکز مدیریت امنیتی.....
۷۸.....	خلاصه.....

بخش دوم..... ۸۱

ایجاد شبکه های خود محافظ (دفاعی) سیسکو..... ۸۱

دیدگاه کلی..... ۸۲

اهداف..... ۸۲

تغییر تهدیدها و چالش ها..... ۸۴

ایجاد یک شبکه ی خود محافظ..... ۹۲

سیستم دفاعی در برابر تهدیدات انطباقی..... ۹۸

نرم افزار نسخه ی ۷ ابزار امنیتی PIX سیسکو..... ۱۰۲

ماژول های DDOS سیسکو..... ۱۰۸

MARS ایمن سیسکو و ارزیاب امنیتی..... ۱۱۲

ایمن سازی ساختار شبکه با ویژگی های امنیتی نرم افزار IOS سیسکو..... ۱۱۸

راه حل های امنیتی نقاط انتهایی شبکه خود محافظ..... ۱۲۳

محصولات امنیتی یکپارچه امنیتی سیسکو..... ۱۲۶

خلاصه..... ۱۲۹

بخش سوم..... ۱۳۱

ایمن سازی دسترسی اجرایی به مسیر یاب های سیسکو..... ۱۳۱

دیدگاه کلی..... ۱۳۲

اهداف..... ۱۳۲

پیکر بندی رمزهای عبور مسیر یاب..... ۱۳۳

تنظیم رمز عبور..... LINE-LEVEL AUXILIARY ۱۴۸

تعیین تعداد دفعات خطا در ورود به سیستم..... ۱۵۶

تنظیمات انقضاء زمانی..... ۱۵۸

پیکر بندی پیام های BANNER..... ۱۶۳

خلاصه..... ۱۶۶

بخش چهارم ۱۶۹

غیر فعال سازی رابط ها و سرویس های بدون استفاده مسیریاب های سیسکو ۱۶۹

دیدگاه کلی ۱۷۰

اهداف ۱۷۱

شبکه ایمن مسیریاب ها ۱۷۲

غیر فعال سازی رابط ها و سرویس های غیر ضروری ۱۷۷

غیر فعال سازی رابط ها و سرویس های غیر ضروری ۱۸۵

غیر فعال سازی و محدودیت سرویس های مدیریتی پیکربندی ۲۰۷

تضمین یکپارچگی مسیر ۲۱۴

غیر فعال سازی جستجو ها و اسکن ها ۲۱۸

تضمین امنیت دسترسی به ترمینال ۲۲۲

غیر فعال سازی **GRATUITOUS AND PROXY ARP** ۲۲۶

غیر فعال سازی هم پخش مستقیم **IP** ۲۳۰

خلاصه ۲۳۲

بخش پنجم ۲۳۳

پیشگیری از حملات و تهدیدات توسط لیست های دسترسی ۲۳۳

دیدگاه کلی ۲۳۴

اهداف ۲۳۴

لیست های دسترسی سیسکو ۲۳۶

اعمال لیست های دسترسی به رابط های مسیریاب ۲۴۶

استفاده از فیلتر کردن ترافیک با بکارگیری لیست های دسترسی ۲۵۲

فیلتر کردن ترافیک سرویس مسیریاب ۲۵۶

پیشگیری از تهدیدات از طریق فیلتر کردن ترافیک شبکه ۲۶۱

پیشگیری از حملات **DDos** از طریق لیست های کنترل دسترسی ۲۷۴

پیش بینی ها (احتیاط) ۲۹۱

خلاصه..... ۲۹۵

بخش ششم..... ۲۹۷

ایمن سازی سوئیچ های سیسکو..... ۲۹۷

دیدگاه کلی..... ۲۹۸

اهداف..... ۲۹۸

ایمن سازی دسترسی شبکه به لایه ۲..... ۳۰۲

محافظت از دسترسی اجرایی به سوئیچ ها..... ۳۰۳

محافظت از دسترسی به پورت مدیریت..... ۳۰۷

غیر فعال سازی رابط ها و سرویس های بدون استفاده ی شبکه..... ۳۰۹

حملات سرریز جدول CAM..... ۳۱۲

حملات جعل سازی آدرس MAC..... ۳۱۹

استفاده از پورت امنیتی در پیشگیری از حملات..... ۳۲۱

پیکربندی پورت امنیتی در سوئیچ سیسکو..... ۳۲۸

فعال سازی امنیت پورت با استفاده از دستورات سیستم عامل IOS سیسکو..... ۳۲۹

خلاصه..... ۳۳۷

بخش هفتم..... ۳۳۹

پیشگیری از حملات به لایه ۲..... ۳۳۹

دیدگاه کلی..... ۳۴۰

اهداف..... ۳۴۰

پیشگیری از حملات VLAN HOPPING..... ۳۴۱

جلوگیری از دستکاری پروتکل SPANNING-TREE..... ۳۴۸

ممانعت از ARP SPOOFING با DAI..... ۳۵۴

دفاع از VLAN های محرمانه..... ۳۵۸

بهترین روش های امنیتی لایه ۲..... ۳۶۵

۳۶۶.....خلاصه

۳۶۷.....بخش هشتم

۳۶۷.....استفاده از خصوصیات امنیتی سوئیچ

۳۶۸.....دیدگاه کلی

۳۶۹.....اهداف

۳۷۰.....خصوصیات امنیتی بکار رفته در سوئیچ های کاتالیست سیسکو

۳۷۳.....سرویس های شناسایی شبکه

۳۷۶.....لیست های کنترل دسترسی

۳۸۵.....پورت امنیتی

۳۸۷.....VLAN محرمانه

۳۸۹.....PRIVATE VLAN EDGE

۳۹۳.....محدودیت سرعت

۳۹۵.....تجزیه و تحلیل پورت سوئیچ شده برای پیشگیری از سیستم های نفوذ

۳۹۷.....رمز گذاری ترافیک مدیریت

۴۰۰.....فعالیت : مشکلات و راه حل آنها

۴۱۰.....خلاصه