

نفوذ به شبکه‌های اد هاک

مؤلفان:

سجاد علی محمدی

وحید سجادی اصیل



انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

۱۴۰۴

سرشناسه	: علی محمدی، سجاد، ۱۳۶۳
عنوان و نام پدیدآور	: نفوذ به شبکه‌های اد هاگ/ سجاد علی محمدی، وحید سجادی اصلیل.
مشخصات نشر	: تهران: ارتش جمهوری اسلامی ایران، دانشگاه فرماندهی و ستاد، انتشارات دافوس، ۱۴۰۳.
مشخصات ظاهری	: ۱۶۷ ص: مصور، جدول.
شابک	: ۹۷۸-۶۲۲-۵۱۰۷-۰۸-۳
وضعیت فهرست نویسی	: قیپا
یادداشت	: کتابنامه: ص. ۱۶۷-۱۴۶.
موضوع	: شبکه‌های موردی (Computer networks) Ad hoc networks ارتباطات بی‌سیم Wireless communication systems شبکه‌های محلی بی‌سیم Wireless LANs شبکه‌های موردی - تدابیر ایمنی Ad hoc networks (Computer networks) -- Security measures
شناسه افزوده	: سجادی، وحید، ۱۳۵۸
شناسه افزوده	: دانشگاه فرماندهی و ستاد آجا، انتشارات دافوس
شماره کتابشناسی ملی	: ۹۹۸۸۶۶۹
اطلاعات رکورد	: قیپا
کتابشناسی	

عنوان: نفوذ به شبکه‌های اد هاگ

مؤلفان: سجاد علی محمدی و وحید سجادی اصلیل

طراح جلد: علیرضا اکبرپور

صفحه‌آرایی: امیرحسین رضایی

ناشر: دافوس

شمارگان: ۱۰۰۰

تعداد صفحه: ۱۶۷ ص

نوبت چاپ: چاپ اول

تاریخ انتشار: ۱۴۰۴

چاپ و صحافی: مدیریت چاپ، انتشارات و فصلنامه دانشگاه فرماندهی و ستاد آجا

قیمت: ۱.۹۰۰.۰۰۰ ریال

نشانی: تهران، میدان پاستور، خیابان دانشگاه جنگ، دانشگاه فرماندهی و ستاد، انتشارات دافوس

تلفن: ۰۲۱-۶۶۴۷۰۴۸۶، ۰۲۱-۶۶۴۱۴۱۹۱

مسئولیت صحت مطالب بر عهده مؤلفان می‌باشد.

کلیه حقوق برای دافوس آجا محفوظ است. (نقل مطالب با ذکر مأخذ بلامانع است).

فهرست مطالب

۱۵	فصل اول: مبانی شبکه‌های اد هاك
۱۶	مقدمه
۱۷	معرفی شبکه اد هاك
۱۷	تاریخچه شبکه اد هاك
۱۹	معرفی و نمای کلی شبکه‌های اد_هاك
۲۳	انواع مختلف شبکه‌های بی سیم موزدی
۲۴	تفاوت بین شبکه‌های سلولی و شبکه‌های اد هاك
۲۵	ویژگی شبکه‌های اد_هاك
۲۷	کاربردهای شبکه‌های اد هاك
۳۱	فصل دوم: تهدیدات شبکه‌های اد هاك
۳۲	مقدمه
۳۲	ویژگی‌ها، محدودیت‌ها
۳۲	ویژگی‌های شبکه‌های اد_هاك
۳۳	محدودیت‌های شبکه‌های اد_هاك
۳۴	چالش‌ها، مزایا و معایب شبکه‌های اد_هاك
۳۴	چالش‌های پیاده‌سازی شبکه‌های اد_هاك
۳۶	چالش‌های امنیتی در شبکه‌های اد_هاك بی سیم
۳۸	مزایای شبکه‌های اد_هاك
۳۸	معایب شبکه‌های اد_هاك
۳۹	استانداردهای شبکه‌های اد_هاك

۴۱	طبقه‌بندی حملات امنیتی کلاسیک به شبکه‌های اد_هاک
۴۲	حملات غیرفعال
۴۲	حملات فعال
۴۲	حملات خارجی
۴۳	حملات داخلی
۴۳	زنجیره کشتار سایبری
۴۶	میتراک
۴۹	فصل سوم: حملات علیه دسترس‌پذیری
۵۰	مقدمه
۵۰	شیوه‌های اختلال در دسترس‌پذیری با استفاده از حملات کلاسیک
۵۰	حملات فعال
۵۱	حمله سیل
۵۲	حمله حفره خاکستری
۵۳	پارازیت
۵۶	حمله سیاه‌چاله
۵۸	حمله سیل
۵۸	سیل سلام
۶۱	حملات سیل و عدم همگام‌سازی
۶۲	حمله سیل آسای همگام‌سازی
۶۲	حمله عجولانه
۶۳	حمله انکار سرویس
۶۴	ربودن جلسه

۶۵		حمله جعل سیستم موقعیت یاب جهانی
۶۶		حمله جعل لینک
۶۶		تکرار حمله جعل
۶۷		حمله باج خواهی
۶۷		حمله بیزانسی
۶۸		سرریز جدول مسیریابی
۶۹		حمله فرسودگی
۶۹		برخورد
۷۰		حمله ناعادلانه
۷۱		حملات غیرفعال
۷۱		حمله عروس دریایی
۷۲		شیوه های اخلاص در دسترس پذیری با استفاده از حملات میتراتک
۷۲		حذف دسترسی به حساب (ID: T1640)
۷۳		فیشینگ (ID: T1660)
۷۴		انکار سرویس شبکه (ID: T1464)
۷۵		ربودن منابع (ID: T1496)
۷۵		شیوه های اخلاص در دسترس پذیری با استفاده از حملات زنجیره کشتار سایبری
۷۵		تسلیمات (تسلیم سازی)
۷۶		باج افزار مبتنی بر اسکرپت
۷۶		متنوع کردن الگوهای دسترسی به فایل
۷۷		تکنیک های فرار
۷۷		تحویل

۷۷	حمله سیل
۷۸	ایرپون
۷۹	فرمان و کنترل
۷۹	ابزار فایل ۲ ایر
۷۹	استفاده از بات نت
۸۰	اقدامات بر روی هدف
۸۱	دسترسی به شبکه
۸۱	حمله افشای مکان
۸۳	فصل چهارم: حملات علیه محرمانگی
۸۴	مقدمه
۸۴	شیوه‌های نفوذ در حوزه محرمانگی با استفاده از حملات کلاسیک
۸۴	حملات فعال
۸۴	جعل هویت
۸۵	حمله کرم چاله
۸۶	حمله ثبت ساختگی
۸۶	حمله بد رله تبانی
۸۶	حملات غیر فعال
۸۷	تجزیه و تحلیل ترافیک
۸۸	استراق سمع
۸۹	اسکن فعال (ID: T1595)
۹۰	سازش بی سیم (ID: T0860)
۹۰	پیوند مخرب (ID: T1204.001)

۹۱	شناسایی
۹۱	استراق سمع
۹۱	اسکن پورت
۹۲	استثمار
۹۲	مسمومیت حافظه پنهان خدمات نام دامنه
۹۲	فرمان و کنترل
۹۲	استفاده از الگوریتم تولید دامنه
۹۳	فصل پنجم: حملات علیه یکپارچگی خدمات
۹۴	مقدمه
۹۵	شیوه‌های نفوذ در حوزه یکپارچگی با استفاده از حملات کلاسیک
۹۵	حملات فعال
۹۵	حملات تغییر
۹۶	حمله سیل
۹۶	تزریق کد آلوده
۹۷	تزریق/تکثیر/اساخت/تغییر بسته
۹۹	حمله بالماسکه کردن
۹۹	برخورد لایه لینک
۹۹	تکرار گره
۱۰۰	حملات علیه مسیریابی
۱۰۰	حمله مردمیانی
۱۰۰	جعل هویت کاربر
۱۰۱	فرسودگی لایه پیوند

- شکنجه محرومیت از خواب..... ۱۰۱
- حملات مستقیم به اطلاعات مسیریابی..... ۱۰۱
- ارسال انتخابی..... ۱۰۲
- حمله مسمومیت حافظه پنهان مسیریابی..... ۱۰۳
- محرومیت از خواب..... ۱۰۳
- افشای موقعیت مکانی..... ۱۰۴
- حمله زمان‌بندی..... ۱۰۴
- حملات غیرفعال..... ۱۰۴
- حملات چندلایه..... ۱۰۴
- حملات جعل هویت..... ۱۰۴
- حملات مردمیانی..... ۱۰۵
- شیوه‌های نفوذ در حوزه یکپارچگی با استفاده از حملات میتراتک..... ۱۰۸
- تزریق محتوا (ID: T1659)..... ۱۰۸
- حمله مرد میانی (ID: T1638)..... ۱۰۹
- مترجم فرمان و اسکرپت (ID: T1623)..... ۱۱۰
- شیوه‌های نفوذ در حوزه یکپارچگی با استفاده از حملات زنجیره کشتار سایبری..... ۱۱۱
- تسلیمات (تسلیم سازی)..... ۱۱۱
- تنوع محموله تحویل..... ۱۱۱
- حمله سیل احراز هویت..... ۱۱۱
- تحویل..... ۱۱۲
- استثمار..... ۱۱۲
- مسمومیت حافظه پنهان خدمات نام دامنه..... ۱۱۲

نصب.....	۱۱۳
کنترل از راه دور دسکتاپ.....	۱۱۳
فصل ششم: نگاهی جامع به تهدیدات و حملات امنیتی شبکه‌های اد هاگ.....	۱۱۵
مقدمه.....	۱۱۶
شیوه‌های نفوذ به شبکه‌های اد هاگ در حوزه اختلال در دسترس‌پذیری.....	۱۱۶
مؤلفه کلاسیک فعال.....	۱۱۷
مؤلفه کلاسیک غیر فعال.....	۱۱۸
مؤلفه میتر اتک.....	۱۱۸
شیوه‌های نفوذ به شبکه‌های اد هاگ در حوزه محرمانگی.....	۱۲۰
مؤلفه کلاسیک فعال.....	۱۲۰
مؤلفه کلاسیک غیر فعال.....	۱۲۱
مؤلفه میتر اتک.....	۱۲۱
شیوه‌های نفوذ به شبکه‌های اد هاگ در حوزه یکپارچگی.....	۱۲۴
مؤلفه کلاسیک فعال.....	۱۲۴
مؤلفه کلاسیک غیر فعال.....	۱۲۵
مؤلفه میتر اتک.....	۱۲۶
شیوه‌های نفوذ به شبکه‌های اد هاگ از طریق زنجیره کشتار سایبری.....	۱۲۸
مرحله اول: شناسایی.....	۱۲۸
مرحله دوم: تسلیح‌سازی.....	۱۲۸
مرحله سوم: تحویل.....	۱۲۹
مرحله چهارم: بهره‌برداری.....	۱۲۹
مرحله پنجم: نصب.....	۱۲۹

مرحله ششم: فرماندهی و کنترل ۱۳۰

مرحله هفتم: اقدام ۱۳۰

فصل هفتم: واژه‌ها و اصطلاحات ۱۳۳

واژه‌ها ۱۳۴

اصطلاحات و تعاریف ۱۴۱

منابع و مراجع ۱۴۵

www.ketab.ir

در دنیای امروز که تکنولوژی به سرعت در حال پیشرفت است، اهمیت شبکه‌های اد هاک به طور فزاینده‌ای مورد توجه محققان، مهندسان و علاقه‌مندان به فناوری اطلاعات قرار گرفته است. این نوع شبکه‌ها که با قابلیت‌های خاص خود، فضای وسیعی از کاربردها را شامل می‌شوند، در زمینه‌های مختلفی از جمله نظامی، امداد و نجات، اینترنت اشیاء و ارتباطات بی‌سیم، نقشی اساسی و حیاتی ایفا می‌کنند. با این حال، به دلیل ماهیت خاص و غیرمتمرکز این شبکه‌ها، چالش‌های امنیتی متعددی نیز در راستای حفاظت از داده‌ها و اطمینان از دسترسی و یکپارچگی اطلاعات در آن‌ها وجود دارد.

کتاب حاضر با هدف بررسی جامع و دقیق مبانی، چالش‌ها و روندهای آینده شبکه‌های اد هاک به نگارش درآمده است. در فصل نخست، مطالبی به معرفی شبکه‌های اد هاک، تاریخچه و انواع مختلف آن اختصاص یافته است. در این بخش، روند تکاملی این شبکه‌ها و تفاوت‌های اساسی آن‌ها با شبکه‌های سلولی به طرز واضحی بیان می‌شود. همچنین، ویژگی‌های کلیدی شبکه‌های اد هاک و کاربردهای متعدد آن‌ها در دنیای واقعی مورد بررسی قرار می‌گیرد.

فصل دوم به موضوع امنیت در شبکه‌های اد هاک پرداخته و ویژگی‌ها و محدودیت‌های این نوع شبکه‌ها را به تفصیل بررسی می‌کند. در این فصل، چالش‌های امنیتی و مزایا و معایب مرتبط با شبکه‌های اد هاک نیز مورد بحث و بررسی قرار می‌گیرد. شناخت دقیق از استانداردها و طبقه‌بندی حملات امنیتی، به خوانندگان این کتاب این امکان را می‌دهد تا با تهدیدات موجود آشنایی بیشتری پیدا کنند.

فصول سوم تا پنجم به ترتیب به حملات علیه دسترس‌پذیری، محرمانگی و یکپارچگی خدمات اختصاص یافته است. هر فصل به شیوه‌هایی که منجر به نفوذ در این حوزه‌ها می‌شود، می‌پردازد و با ارائه مثال‌های کلاسیک و پیشرفته، خوانندگان را با تهدیدات واقعی و روش‌های مقابله با آن‌ها آشنا می‌سازد.

در فصل ششم، سیستم‌های تشخیص نفوذ به عنوان ابزاری کارآمد برای مانیتورینگ و شناسایی تهدیدات در حال حاضر و آینده مورد بررسی قرار می‌گیرد. در این بخش، نکات کلیدی در خصوص نحوه عملکرد این سیستم‌ها و تکنیک‌های مورد استفاده برای شناسایی حملات به تصویر کشیده می‌شود.

سرانجام، در فصل هفتم روندهای آینده شبکه‌های اد هاگ تحلیل می‌گردد. با توجه به تحولات فوری در عرصه فناوری اطلاعات و تهدیدات نوظهور، شناخت روندهای آینده می‌تواند به محققان و متخصصان کمک کند تا خود را برای چالش‌های جدید آماده سازند و به بهبود امنیت شبکه‌های اد هاگ پردازند.

این کتاب به عنوان یک منبع جامع، قصد دارد تا به پژوهشگران، دانشجویان و تمامی علاقه‌مندان به حوزه فناوری اطلاعات، یک بینش عمیق درباره شبکه‌های اد هاگ و چالش‌های امنیتی آن ارائه دهد. امید است که خوانندگان با آگاهی بهتری نسبت به اهمیت این شبکه‌ها و چالش‌های آن‌ها مجهز شده و در تحقیق و توسعه فناوری‌های مرتبط پیشگام باشند.

با امید به این که این اثر، گامی مؤثر در راستای بهبود درک، واکنش و پیشرفت در مفهوم شبکه‌های اد هاگ و امنیت آن‌ها باشد، از شما دعوت می‌شود که به مطالعه فصول این کتاب پردازید