

تحلیل حملات مرد میانی در شبکه‌های بی‌سیم

مجید عبقری - حمید انیسی

www.ketab.ir

سرشناسه	:	انیسی، حمید، ۱۳۷۴-
عنوان و نام پدیدآور	:	تحلیل حملات مرد میانی در شبکه‌های بی سیم / حمید انیسی، مجید عبقری.
مشخصات نشر	:	تهران: نشر زهره، ۱۳۹۸.
مشخصات ظاهری	:	۱۲۲ ص.
شابک	:	۹۷۸-۹۶۴-۲۹۸۱-۸۰-۹
وضعیت فهرست نویسی	:	فیبا
موضوع	:	شبکه‌های محلی بی سیم - تدابیر ایمنی.
موضوع	:	Wireless LANs -- Security measures
موضوع	:	ارتباطات بی سیم - تدابیر ایمنی
موضوع	:	Wireless communication systems -- Security measures
موضوع	:	کامپیوترها - ایمنی اطلاعات
موضوع	:	Computer security
شناسه افزوده	:	عبقری، مجید، ۱۳۷۳-
رده بندی کنگره	:	۷۸/TK۵۱۰۵
رده بندی دیویی	:	۸۷۰۰
شماره کتابشناسی ملی	:	۵۷۵۹۴

تحلیل حملات مرد میانی در شبکه‌های بی سیم

مجید عبقری - انیسی



ناشر: زهره

صفحه آرا: معین دلاوری

نوبت چاپ: اول - ۱۳۹۸

شمارگان: ۱۰۰۰ جلد

شابک: ۹۷۸-۹۶۴-۲۹۸۱-۸۰-۹

قیمت: ۲۵۰۰۰ تومان



کلیه حقوق چاپ و نشر مخصوص و محفوظ ناشر است

تهران خیابان انقلاب خیابان وصال شیرازی کوچه ماهان پلاک ۴ زنگ اول

۶۶۴۹۸۴۵۹-۰۹۳-۲۴۳۴۳۴۱

فهرست مطالب

۹	مقدمه
۱۱	فصل اول: تأمین امنیت شبکه‌های بی‌سیم
۱۳	۱-۱- مقدمه فصل اول
۱۳	۱-۲- تأمین امنیت در شبکه‌های بی‌سیم
۱۴	۱-۳- منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول
۱۴	۱-۴- شبکه‌های محلی بی‌سیم
۱۵	۱-۵- امنیت در شبکه‌های محلی بر اساس استاندارد ۸۰۲.۱۱
۱۶	۱-۶- احراز هویت
۱۶	۱-۷- محرمانگی
۱۶	۱-۸- تمامیت
۱۷	۱-۹- سرویس‌های امنیتی
۱۷	۱-۱۰- احراز هویت
۱۷	۱-۱۱- احراز هویت بدون رمزنگاری
۱۸	۱-۱۲- احراز هویت با رمزنگاری RC4
۱۹	۱-۱۳- سرویس‌های امنیتی
۱۹	۱-۱۴- محرمانگی
۲۰	۱-۱۵- تمامیت
۲۱	۱-۱۶- ضعف‌های اولیه امنیتی WEP
۲۲	۱-۱۷- استفاده از کلیدهای ثابت WEP
۲۳	۱-۱۸- ضعف در الگوریتم
۲۳	۱-۱۹- استفاده از CRC رمز نشده
۲۴	۱-۲۰- خطرهای حملات امنیتی
۲۴	۱-۲۱- حملات غیرفعال
۲۴	۱-۲۲- شنود
۲۴	۱-۲۳- آنالیز ترافیک

۲۵	 ۲۴-۱ حملات فعال
۲۵	 ۲۵-۱ تغییر هویت
۲۵	 ۲۶-۱ پاسخ‌های جعلی
۲۵	 ۲۷-۱ ده نکته اساسی در امنیت شبکه‌های WI-FI
۳۱	فصل دوم: بررسی انواع حملات مرد میانی در شبکه‌های بی‌سیم
۳۳	 ۱-۲ مقدمه
۳۵	 ۲-۲ انواع حملات در شبکه‌های کامپیوتری
۳۶	 ۳-۲ انواع حملات مرد میانی
۳۷	 ۴-۲ مهندسی اجتماعی
۴۱	 ۱-۴-۲ مراحل مهندسی اجتماعی
۴۲	 ۵-۲ آلودگی حافظه پنهان ARP
۴۲	 ۶-۲ ارتباطات عادی حافظه پنهان ARP
۴۴	 ۷-۲ آلودگی‌های حافظه پنهان
۴۵	 ۸-۲ حمله فیشینگ
۴۶	 ۱-۸-۲ روش‌های مختلف فیشینگ
۴۸	 ۹-۲ حمله جعل DNS
۴۹	 ۱-۹-۲ Spoofing
۵۰	 ۲-۹-۲ روش‌های حمله جعل DNS
۵۲	 ۱۰-۲ پروتکل HTTPS
۵۲	 ۱-۱۰-۲ SSL و عملکرد آن
۵۳	 ۱۰-۲-۲ شیوه رمزنگاری اطلاعات در SSL
۵۴	 ۳-۱۰-۲ تهیه گواهی SSL
۵۴	 ۲-۱۰-۴ حمله علیه HTTPS
۵۵	 ۵-۱۰-۲ آسیب‌پذیری‌های SSL
۵۹	 Hijacking-۱۱-۲
۵۹	 ۱۲-۲ بررسی حملات سرقت نشست
۶۱	 ۱-۱۲-۲ مدیریت نشست
۶۲	 ۲-۱۲-۲ حمله بر علیه مکانیزم‌های مدیریت نشست

۶۲	 ۱-۲-۱۲-۲ سرقت جلسه
۶۳	 ۲-۲-۱۲-۲ پیش‌بینی جلسه
۶۴	 ۳-۲-۱۲-۲ شنود جلسه
۶۴	 ۳-۱۲-۲ حمله جست‌وجوی فراگیر
۶۴	 ۴-۱۲-۲ قرارگیری در معرض جلسه
۶۵	 ۵-۱۲-۲ حمله تزریق کد
۶۶	 ۶-۱۲-۲ حمله تثبیت جلسه
۶۹	فصل سوم: پیاده‌سازی انواع حملات مرد میانی در شبکه‌های بی‌سیم
۷۱	 ۱-۳ مقدمه
۷۱	 ۲-۳ پیاده‌سازی حمله آلودگی باغچه پنهان
۷۸	 ۳-۳ پیاده‌سازی یک حمله شنود
۸۲	 ۴-۳ پیاده‌سازی حمله جعل DNS
۹۱	 ۵-۳ پیاده‌سازی حمله به HTTPS
۹۶	 ۶-۳ پیاده‌سازی حمله ربودن جلسه
۱۰۱	فصل چهارم: بررسی روش‌های مقابله با انواع حملات مرد میانی در شبکه‌های بی‌سیم
۱۰۳	 ۱-۴ مقدمه
۱۰۵	 ۲-۴ دفاع در برابر آلودگی حافظه نهان ARP
۱۰۵	 ۳-۴ استاتیک کردن حافظه نهان ARP
۱۰۶	 ۴-۴ ایمن‌سازی شبکه
۱۰۷	 ۱-۴-۴ ایمن‌سازی سوئیچ‌های شرکت سیسکو در مقابل آلودگی حافظه نهان
۱۰۸	 ۱-۴-۴-۱ حمله DHCP Spoofing و نحوی مقابله با آن در سوئیچ‌های سیسکو (DHCP Snooping)
۱۰۹	 ۲-۴-۴ حمله آلودگی حافظه نهان و نحوی مقابله با آن
۱۱۰	 ۵-۴ نظارت بر ترافیک حافظه نهان با برنامه‌های دیگر
۱۱۰	 ۶-۴ روش‌های مقابله با حمله جعل DNS
۱۱۴	 ۱-۶-۴ فرمان‌ها و ابزارهای کنترل و بررسی DNS
۱۱۴	 ۷-۴ پروتکل HTTPS
۱۱۵	 ۸-۴ دفاع در برابر ارتباط رایبی SSL
۱۱۵	 ۱-۸-۴ اطمینان حاصل نمایید که ارتباطات امن از طریق HTTPS انجام می‌شود

- ۴-۸-۲- بردارهای شناخته شده حملات را بلوکه کنید..... ۱۱۶
- ۴-۸-۳- انجام کارهای بانکداری آنلاین در منزل..... ۱۱۶
- ۴-۸-۴- امن سازی ماشین های شبکه داخلی..... ۱۱۷
- ۴-۸-۵- استفاده از نرم افزارهای آنتی ویروس و فایروال های قدرتمند..... ۱۱۷
- ۴-۹-۱- روش های مقابله علیه مکانیزم های مدیریت نشست..... ۱۱۷
- ۴-۹-۱- استفاده از کوکی برای نگهداری مقادیر نشست..... ۱۱۸
- ۴-۹-۲- عدم استفاده از SID های انتخابی کاربران..... ۱۱۸
- ۴-۹-۳- تولید یک SID جدید توسط سیستم پس از ورود کاربر به سیستم..... ۱۱۹
- ۴-۹-۴- تعیین طول عمر یا یک وقفه برای نشست ها..... ۱۱۹
- ۴-۹-۵- فراهم نمودن مکان Logout و از بین بردن نشست ها..... ۱۱۹
- ۴-۹-۶- استفاده از بیلد HTTP Referrer برای تشخیص چند مشتری که در حال مرور کردن با یک SID یکسان هستند..... ۱۱۹
- ۴-۹-۷- فعال سازی فیلد امنیت رپو با کوکی ها..... ۱۲۰
- ۴-۱۰- جلوگیری از حملات سرقت جلسه در P2IP..... ۱۲۰
- منابع و مآخذ..... ۱۲۲

مقدمه

حمله مرد میانی یکی از انواع حملات سایبری است که یک فرد مخرب خود را بین یک مکالمه دو طرفه قرار می‌دهد و هویت هر دو طرف را جعل می‌کند و به اطلاعاتی که دو طرف قصد ارسال به یکدیگر دارند، دسترسی می‌یابد. حمله مرد میانی به مخرب اجازه قصد ارتباط، ارسال و دریافت داده مربوط به اشخاص دیگر را می‌دهد و حتی می‌تواند جلوی ارسال اولیه آن‌ها را بگیرد بدون این‌که حتی طرفین متوجه شوند تا زمانی که خیلی دیر شده است.

معروف‌ترین حالت مرد میانی شامل یک هکر است که از روتر بی‌سیم به عنوان یک مکانیزم برای قطع کردن ارتباط دوحانبه استفاده می‌کند. این کار می‌تواند با قرار دادن یک روتر مخرب به عنوان یک روتر امن یا سه استفاده از نقص‌های موجود در یک روتر امن برای قطع ارتباط بین کاربران انجام شود.

در این کتاب حملات مرد میانی در ارتباط با شبکه‌های بی‌سیم و روش‌های مقابله با آن‌ها را بررسی و سپس پیاده‌سازی کردیم و نشر دادیم در ارتباطات واقعی حملات می‌تواند در بسیاری از اوقات به وسیله اطلاعات مناسب کشف شود. معروف‌ترین حملات از طریق آلودگی حافظه نهان، جعل دی‌ان‌اس، سرقت جلسه و حمله به SSL اتفاق می‌افتند.