عنوان مقاله:
پیاده سازی نرم افزاری جهت تشخیص حمله ARP Spoofing در سیستم عامل ویندوز

محل انتشار:
دومین کنفرانس ملی دانش و فناوری علوم مهندسی ایران (سال: 1397)

تعداد صفحات اصل مقاله: 10

نویسندگان:
محمد نقدی - *دانشجوی کارشناسی ارشد نرم افزار، دانشگاه آزاد اسلامی واحد همدان ، گروه کامپیوتر ، همدان ، ایران*

محمد مهدی شیرمحمدی - *استادیار گروه کامپیوتر، دانشگاه آزاد اسلامی واحد همدان ، گروه کامپیوتر ، همدان ، ایران*

خلاصه مقاله:
هدف از این تحقیق پیادهسازی یک نرم افزار سیستم عامل ویندوز، برای تشخیص حمله ARP Spoofing در یک شبکه LAN است. این حمله که از نوع MITM یا حمله مرد میانی است امکان تغییر/حذف/ یا ویرایش بسته های IP را قبل از رسیدن به قربانی فراهم می کند. ایده اصلی که پشت حمله MITM است، نفوذ به ارتباطات موجود بین نقاط پایانی (میزبان ها) در شبکه محلی و تغییر محتویات یا تزریق اطلاعات غلط می باشد. برای دریافت بسته ها و تشخیص حمله در این نرم افزار، از کتابخانه PCap.NET که نسخه تحت ویندوز WinPCap است استفاده کرده ایم. روش تشخیص حمله ARP Spoofing در این نرم افزار به این صورت است که ابتدا همه بسته های از نوع ARP Replay ذخیره شده و سپس با بررسی و مقایسه این بسته ها، رایانه مهاجم که آدرس MAC خود را با آدرس IP رایانه قربانی یا سرور پیوند داده، مشخص خواهد شد. در واقع، تشخیص حمله در این نرم افزار، با مقایسه بسته هایی که آدرس MAC یکسان و آدرس IP متفاوت دارند، انجام می گیرد. در نهایت با استفاده از نرم افزار Network Spoofer در یک شبکه LAN و روی یکی از کلاینتهای موبایل با سیستم عامل اندروید، اقدام به ایجاد حمله و جعل جدول ARP نمودیم. با اجرای نرم افزار بر روی یکی از کلاینت های شبکه، حمله به درستی تشخیص و آدرس IP و MAC مهاجم و قربانی به کاربر اطلاع داده شد.

کلمات کلیدی:
ARP spoofing, ARP Poisoning, MITM، حمله مرد میانی، WinPCap, PCap.NET