سومین کنفرانس فناوری اطلاعات و دانش
۶ تا ۸ آذرماه ۱۳۸۶
کنفرانس بین المللی فناوری اطلاعات و دانش IKT 2007
دانشگاه فردوسی مشهد

یک شیوه تشخیص ناهنجاری ترکیبی مبتنی بر میانگین- واریانس و چندمتغیری براساس ترافیک ARP در شبکه‌های سازمانی

یاسر یاسمی، سعادت پورمظفری و سیاوش خرسندی

ایران، تهران، دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر و فناوری اطلاعات

yasami, saadat, khorsand@cic.aut.ac.ir

چکیده - با گسترش روزافزون شبکه‌های کامپیوتری و استفاده از آن، مسائل امنیتی در این ارتباطات در سالهای اخیر اهمیت ویژه‌ای یافته است. بزرگترین خطر امنیتی که اینترنت در حال حاضر با آن مواجه است، انتشار سریع نرم‌افزارهای بدخواه اینترنتی است. طرحهای مبتنی بر امضا غالباً در تشخیص نرم‌افزارهای بدخواه یک روزه ناتوان بوده و با توجه به اینکه نوعاً نیازمند دخالت انسانی برای فرموله کردن امضاهای حملات جدید هستند، توانایی آنها برای برهمکنش سریع با تهدیدات جدید محدود است. ما در این مقاله یک تکنیک تشخیص ناهنجاری بر اساس ترافیک ARP ، برای حفاظت از شبکه‌های محلی داخلی در برابر آلودگی به نرم‌افزارهای بدخواهی که در ایجاد ناهنجاری در ترافیک شبکه نقش دارند، معرفی می‌کنیم. با توجه به این که ترافیک همه‌پخشی ARP سربار سوئیچینگ و مصرف پهنای باند اضافی بر شبکه های محلی تحمیل می‌کند، این تکنیک با تشخیص رفتارهای ناهنجار در شبکه، علاوه بر ارزش امنیتی که دارد، در بالا بردن کارایی شبکه نیز می‌تواند مفید باشد. الگوریتم پیشنهادی از این نظر که ترکیبی از دو شیوه مبتنی بر میانگین- واریانس و چندمتغیری را به کار می‌گیرد، بدیع بوده و نتایج آزمایشات انجام شده نشان می‌دهد که کارایی به مراتب بالاتری نسبت به هریک از شیوه‌های مذکور به تنهایی دارد.

کلید واژه- سیستمهای تشخیص ناهنجاری (ADS)، ARP (Address Resolution Protocol)، نرم‌افزارهای بدخواه.

۱- مقدمه

شبکه های کامپیوتری و استفاده از آن در سالهای اخیر گسترش بسیار زیادی یافته است. کاربردهای گسترده از این صنعت در زمینه‌های مختلف ملاحظات امنیتی آن را نیز از اهمیت ویژه ای برخوردار ساخته است. نرم‌افزارهای بدخواه و کرمهای اسکن‌کننده به سرعت در حال فراگیر شدن هستند. علیرغم برخی تلاشهایی که برای ارائه الگوریتمهای مبتنی بر امضا صورت گرفته [۱]، توانایی این روشها در تشخیص کرمهای نوظهور محدود می‌باشد. نرم‌افزارهای بدخواه می‌توانند از تکنیکهای ضدتشخیص متنوعی نظیر رفتارهای پویا، ماجولاریتی ابزارهای حمله [۵] و ... بهره ببرند. متأسفانه، حتی بهترین حالت امنیت شبکه ممکن است به خاطر آسیب‌پذیریهای جدیداً کشف شده، کاربران بی‌توجه و پیکربندیهای ناصحیح سیستم دچار آسیب گردد. مسلماً در چنین شرایط مسابقه‌ای برد با نویسنگان این نرم‌افزارهای بدخواه است. پدافندگرهای شبکه باید تمامی راههای نفوذ به شبکه را مسدود نمایند به طوریکه تنها یک راه برای نفوذ حمله‌کنندگان به شبکه وجود داشته باشد.

میزبانهای آلوده به نرم‌افزارهای بدخواه در شبکه باید به سرعت شناسایی گردند تا از انتشار آنها جلوگیری شود. این