



اولین همایش ملی فناوری در مهندسی کاربردی باشگاه پژوهشگران جوان و نخبگان دانشگاه آزاد اسلامی (NCTAE2016)
واحد تهران غرب، 21 بهمن ماه 1395

بررسی و مقایسه روش های تشخیص نفوذ در شبکه های کامپیوتری

معصومه لطیف^{1*}، زهره باطنی²

¹ دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد تهران مرکزی masomeh13latif@gmail.com

² استادیار دانشگاه آزاد اسلامی واحد تهران مرکزی zbateni@hotmail.com

چکیده

با رشد روز افزون فناوری اطلاعات و استفاده گسترده از شبکه های کامپیوتری، امنیت شبکه به عنوان یکی از مباحث بسیار مهم و چالش برانگیز این حوزه مطرح است. نفوذ در شبکه های کامپیوتری با انگیزه های مختلف مالی، سیاسی، نظامی و یا برای نشان دادن ضعف امنیتی موجود در برنامه های کاربردی، ضعف امنیتی در طراحی شبکه و پروتکل های آن صورت می گیرد. سیستم های تشخیص نفوذ ابزارهای امنیتی هستند که برای تامین امنیت ارتباطات در سیستم های اطلاعاتی مورد استفاده قرار می گیرند. سیستم های تشخیص نفوذ بر اساس روش مورد استفاده برای تشخیص نفوذ به دو دسته مبتنی برامضا و مبتنی بر ناهنجاری تقسیم می شوند. روش مبتنی بر امضا بر اساس الگوهای نفوذ از پیش ساخته شده است و تشخیص دهنده دارای پایگاه داده ای از الگوهای حمله است. در روش مبتنی بر ناهنجاری رویدادهای مشاهده شده با فعالیت های نرمال مقایسه می شود. برای تشخیص ناهنجاری باید الگوهای خاصی را پیدا کرد و رفتارهایی که از الگو پیروی می کنند نرمال و رویدادهای انحرافی به عنوان ناهنجاری تشخیص داده می شوند. سیستم های تشخیص نفوذ از لحاظ معماری به سه دسته مبتنی بر میزبان، مبتنی بر شبکه و توزیع شده تقسیم تقسیم می شوند. در این مقاله روش ها تشخیص نفوذ و نیز معماری سیستم های تشخیص نفوذ مورد بررسی و ارزیابی قرار می گیرد.

کلمات کلیدی: تشخیص نفوذ، تشخیص مبتنی بر ناهنجاری، معماری سیستم های تشخیص نفوذ، امنیت شبکه، تشخیص مبتنی بر امضاء

1. مقدمه

با افزایش روز افزون حملات به شبکه های کامپیوتری از یک سو و وابستگی بسیار زیاد فعالیت های حوزه های مختلف صنعتی، بازرگانی، نظامی، پزشکی و آموزشی به سرویس هایی که توسط شبکه های کامپیوتری ارائه می شود، تلاش برای جلوگیری و کشف و نفوذ در شبکه ها امری بسیار ضروری است. تشخیص نفوذ عبارت است از فرآیند شناسایی و پاسخ به فعالیت های مخرب که به شکل هدفمند منابع شبکه را مورد حمله قرار می دهد. از این رو وجود سیستم های تشخیص نفوذ کارآمد برای تامین امنیت شبکه از اهمیت بسیار زیادی برخوردار است.