عنوان مقاله:
تکنولوژی های سیستم های تشخیص نفوذ و ویژگی های ابزار تشخیص نفوذ ایده آل

محل انتشار:
چهارمین کنفرانس بین المللی یافته های نوین علوم و تکنولوژی (سال: 1396)

تعداد صفحات اصل مقاله: 9

نویسندگان:
فایزه بارانی - *دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد بیرجند*

مصطفی سبزه کار - *دانشجوی دکتری مهندسی کامپیوتر دانشگاه فردوسی مشهد*

خلاصه مقاله:
برای ایجاد امنیت کامل در یک سیستم کامپیوتری، علاوه بر دیواره های آتش و دیگر تجهیزات جلوگیری از نفوذ، سیستمهای دیگری به نام سیستم های تشخیص نفوذ (IDS1) مورد نیاز می باشند تا بتوانند در صورتی که نفوذگر از دیواره ی آتش، آنتی ویروس و دیگرتجهیزات امنیتی عبور کرد و وارد سیستم شد، آن را تشخیص داده و چاره ای برای مقابله با آن بیاندیشند. هدف یک سیستم تشخیص نفوذ جلوگیری از حمله نیست و تنها کشف و احتمالا شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه های کامپیوتری و اعلام آن به مدیر سیستم است. عموما سیستم های تشخیص نفوذ در کنار دیواره های آتش و به صورت مکمل امنیتی برای آن ها مورد استفاده قرار می گیرند. سیستم های تشخیص نفوذ به صورت سیستم های نرم افزاری و سخت افزاری ایجاد شده و هر کدام مزایا و معایب خاص خود را دارند. سرعت و دقت از مزایای سیستم های سخت افزاری است و عدم شکست امنیتی آن ها توسط نفوذگران، قابلیت دیگر این گونه سیستم ها می باشد. در این مقاله ما ابتدا تعریفی از سیستمهای تشخیص نفوذ ارایه خواهیم کرد و سپس اجزای این سیستمها را شرح خواهیم داد. در ادامه ویژگی یک IDS ایدهال را بیان خواهیم کرد.

کلمات کلیدی:
تشخیص نفود, اجزای سیستم تشخیص نفوذ, IDS