عنوان مقاله:
مروری بر تاریخچه و تکنیک های پاسخ به نفوذ

محل انتشار:
همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1393)

تعداد صفحات اصل مقاله: 13

نویسندگان:
حامد زمانیان هوچ - *دانشجوی کارشناسی ارشد فناوری اطلاعات گرایش شبکه موسسه آموزش عالی روزبهان ساری*

قاسم نوری - *دانشجوی کارشناسی ارشد فناوری اطلاعات گرایش شبکه موسسه آموزش عالی روزبهان ساری*

خلاصه مقاله:
برای ایجاد امنیت کامل در یک سیستم کامپیوتری، علاوه بر دیواره های آتش و دیگر تجهیزات جلوگیری از نفوذ، سیستم هایدیگری به نام سیستم های تشخیص و پاسخ به نفوذ مورد نیاز می باشند تا بتوانند در صورتی که نفوذگر از دیواره ی آتش، آنتیویروس و دیگرتجهیزات امنیتی عبور کرد و وارد سیستم شد، آن را تشخیص داده و چاره ای برای مقابله با آن بیندیشند.در این مقاله ما به صورت کلی به تاریخچه و نحوه پیدایش سیستم های تشخیص نفوذ و سیستم های پاسخ به نفوذ می پردازیم،همچنین تفاوت بین این سیستم هارا بیان می کنیم در ادامه یک طبقه بندی برای سیستم های پاسخ به نفوذ ارائه می کنیم. وسپس رویکردها و تکنیک های پاسخ به نفوذ را بررسی می کنیم و در آخر چالش های پیش رو را مطرح می کنیم.

کلمات کلیدی:
امنیت ، سیستم های تشخیص نفوذ ، سیستم های پاسخ به نفوذ، نفوذ، امنیت، تکنیک