عنوان مقاله:
به کار گیری سیستم های پاسخ به نفوذ خودکار در سیستمهای امنیتی

محل انتشار:
اولین کنفرانس ملی رویکردهای نو در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:
نادر حسین پور صفاریان - *دانشجوی کارشناسی ارشد*

احمد اکبری - *استاد راهنما*

خلاصه مقاله:
برای جلوگیری از نفوذهای بسیار سریع و پیچیده ، استفاده از مکانیزمهای تشخیص نفوذ قدرتمند، به تنهایی کافی نیستند، بلکه باید از سیستمهای پاسخ به نفوذ کارآمد جهت جلوگیری از پیشرفت نفوذ و کاهش/ حذف تاثیرهای مخرب در کوتاه ترین زمان استفاده نمود. در حال حاضر علیرغم فعالیتهای نسبتا خوبی که در تولید تجهیزات امنیتی شده است ، در دسترس بود پاسخ هایمتفاوت و متنوع بسته به سطح و پیچیدگی حملات و اعمال به موقع پاسخ متناسب یا وجود ندارد یا اگر وجود دارد بهینه نبوده و به خوبی بهره برداری نمی شود. هدف اصلی این مستند، ارائه طبقه بندی کلی سیستمها پاسخ به نفوذ و بررسی ویژگیهای اصلی یه سیستم پاسخ به نفوذ خودکار مطلوب بوده و در ادامه نحوه پیاده سازی و کیفیت پیاده سازی این ویژگیها در یک نمونه تجاری موفق(سیسکو) بیان می شود. در پایان شرایط لازم برای پیاده سازی هر چه بهتر این نوع سیستمها بیان می گردد.

کلمات کلیدی:
پاسخ به نفوذ خودکار، پاسخ تطبیقی، پاسخ پیشقدم، پاسخ حساس به هزینه، مدیریت و تحلیل ریسک، پاسخ مبتنی بر شبکه، پاسخ مبتنی برکلاینت