عنوان مقاله:
ارائه روشی برای بهبود سیستم تشخیص نفوذ snort در تشخیص رفتار غیرعادی شبکه با استفاده از پایگاه دانش

محل انتشار:
دهمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1383)

تعداد صفحات اصل مقاله: 11

نویسندگان:
علیرضا هدایتی - *دانشگاه صنعتی مالک اشتر*

حسین شیرازی - *دانشگاه صنعتی مالک اشتر*

احمد خادم زاده

خلاصه مقاله:
به منظور شناسایی و تشخیص نفوذ در شبکه های کامپیوتری تاکنون سیستمهای متعددی ساخته شده است یکی از رایج ترین سیستمهای تشخیص نفوذ سیستم تشخیص نفوذ snort می باشد Snort یک سیستم تشخیص نفوذ مبتنی بر شبکه است که طبق مکانیزم تشخیص سواستفاده و با استفاده از یک سری قوانین رخداد نفوذها را به صورت بلادرنگ تشخیص داده و ثبت می کند دراین مقاله روشی ارائه می گردد که در آن سیستم تشخیص نفوذ snort با بکارگیری ابزار پویشگر امنیتی Nmap نسبت به ایجاد پایگاه دانشی از رفتار عادی شبکه اقدام می نماید. بدین ترتیب snort قادر خواهدبود که در مواقع بروز تغییرات و حملات جدید رفتار غیرعادی شبکه و حملاتی که قوانین مشخصی ندارند را شناسایی و اعلام نماید.

کلمات کلیدی:
نفوذ، سیستم تشخیص نفوذ، روشهای تشخیص نفوذ، snort، پایگاه دانش