عنوان مقاله:
روش پیشنهادی تشخیص رفتار غیر عادی شبکه بااستفاده از سیستم تشخیص نفوذSnort

محل انتشار:
دومین کنفرانس بین المللی فناوری اطلاعات و دانش (سال: 1384)

تعداد صفحات اصل مقاله: 8

نویسندگان:
علیرضا هدایتی - *کارشناسی ارشد معماری کامپیوتر، دانشگاه صنعتی مالک اشتر - مجتمع دانشگ*

حسین حسین شیرازی - *دکتری کامپیوتر – عضو هیات علمی دانشگاه صنعتی مالک اشتر، دانشگاه صنع*

احمد خادم زاده - *دکتری مخابرات – عضو هیات علمی مرکز تحقیقات مخابرات، مرکز تحقیقات مخا*

خلاصه مقاله:
به منظور شناسایی و تشخیص نفوذ در شبکههای کامپیوتری تاکنون سیستمهای متعددی ساخته شده است . یکی ازرایج ترین سیستمهای تشخیص نفوذ ، سیستم تشخیص نفوذ Snort میباشد . Snort یک سیستم تشخیص نفوذ مبتنی بر شبکه است که براساس مکانیزم تشخیص سوءاستفاده و با استفاده از یک سری قوانین، رخداد نفوذها را بصورت بلادرنگ تشخیص داده و ثبت میکند . در این مقاله روشی ارائه میگردد که در آن سیستم تشخیص نفوذ Snort بابکارگیری ابزارپویشگرامنیتی Nmap نسبت به ایجاد پایگاه دانشی از رفتار عادی شبکه اقدام می نماید . بدین ترتیب Snort قادر خواهد بود در موقع بروز تغییرات وحملات جدید ، رفتار غیر عادی شبکه و حملاتی که قوانین مشخصی ندارندرا شناسایی واعلام نماید .

کلمات کلیدی:
نفوذ - سیستم تشخیص نفوذ - روشهای تشخیص نفوذ -Snort- پایگاه دانش

لینک ثابت مقاله در پایگاه سیویلیکا: