بخشی از ترجمه مقاله

عنوان فارسی مقاله :

سیستم تشخیص نفوذ شبکه با استفاده از طبقه بندي رفتار حمله

عنوان انگلیسی مقاله :

Network Intrusion Detection System Using Attack Behavior Classification

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل

با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

V. CONCLUSIONS

Intrusion detection is an important issue that has received a lot of attention in computer networks. This paper uses TDDNN neural network to recognize the temporal behavior of network attacks. Our system captures packets in real time using a packet capture engine that presents the packets to a preprocessing stage using two pipes. The preprocessing stage extracts the relevant features for port scan and host sweep attacks, stores the features in a tapped line of a TDNN, and produces outputs that represent possible attack behaviors in a pre-specified number of packets. These outputs are used by the pattern recognition neural networks to recognize the attacks, which are classified, by the classifier network to generate attack alerts.

DARPA data sets are used to evaluate the systems in terms of recognition capability and throughput. Test results show that our system detects all types of attacks much faster than rule-based systems such as SNORT.

5 . نتيجه گيري

تشخيص نفوذ مسئله ي مهمی است که توجه زيادي را در شبکه هاي کامپيوتري به خود جلب کرده است. اين مقاله از شبکه‌ي عصبي TDDNN براي تشخيص رفتار زماني حملات شبکه استفاده مي‌کند. سيستم ما بسته‌ها را به صورت بلادرنگ و با استفاده از يك موتور دريافت بسته دريافت مي‌کند که بسته ها را با استفاده از دو لوله به يك مرحله‌ي پيش پردازش ارائه مي‌دهد. مرحله‌ي پيش پردازش، ويژگي هاي مربوطه را براي حملات اسکن پورت و پاکسازي ميزبان استخراج مي‌کند، ويژگي ها را در يك خط شنود يك TDNN ذخيره مي کند و خروجي هايي را توليد مي کند که بيانگر رفتارهاي احتمالي حمله در تعداد از پيش‌تعيين‌شده‌اي از بسته ها هستند. اين خروجي‌ها توسط شبکه هاي عصبي تشخيص الگو براي تشخيص حملات مورد استفاده قرار مي گيرند، که توسط شبکه‌ي طبقه‌بندي‌کننده طبقه‌بندي مي شوند تا هشدارهاي حمله را توليد نمايند.

از مجموعه داده‌هاي DARPA براي ارزيابي سيستم‌ها از نظر راندمان و قابليت تشخيص استفاده مي‌گردد. نتايج تست نشان مي‌دهند که سيستم ما تمام انواع حملات را بسيار سريع‌تر از سيستم‌هاي مبتني بر قانون مثل SNORT تشخيص مي‌دهد.