سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
یک سیستم تشخیص نفوذ چند لایه با رویکرد ترکیبی

محل انتشار:
پانزدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1397)

تعداد صفحات اصل مقاله: 6

نویسندگان:
مجید آمره ای - *دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران*

اکرم بیگی - *دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران*

خلاصه مقاله:
سیستم های تشخیص نفوذ ابزاری مفید برای تامین امنیت شبکه های رایانه ای در مقابل نفوذگر ها هستند. این سیستم ها از روش های تشخیص نفوذ مبتنی بر امضاء یا مبتنی بر ناهنجاری و یا ترکیبی از آنها استفاده می کنند. در سیستم های تشخیص نفوذ مبتنی بر امضاء از روش تطبیق داده ها با نمونه های موجود یا ایجاد قوانین استفاده می شود . همچنین در سیستم های تشخیص نفوذ مبتنی برناهنجاری می توان از خوشه بندی برای شناسایی نفوذهای ناشناخته و از طبقه بندی برای شناسایی نفوذهای شناخته شده و تفکیک آنها از فعالیت های نرمال استفاده کرد. در این مقاله سیستم تشخیص نفوذی با سه لایه تشخیص پیشنهاد داده ایم که از هر دو روش مبتنی بر امضاء و مبتنی بر ناهنجاری استفاده می کند. لایه اول با استفاده از قوانین ابتکاری برخی از نفوذها را که بسیار مشابه نمونه های نرمال هستند را تشخیص می دهد. لایه دوم با استفاده از خوشه بندی نمونه های ورودی که به مرکز خوشه ناهنجار نزدیکتر از مرکزخوشه نرمال است را به عنوان نفوذ تشخیص میدهد. دو مرکز خوشه توسط الگوریتم ژنتیک محاسبه می شود. لایه سوم نیز بااستفاده از یک طبقه بند جنگل تصادفی نفوذها را تشخیص می دهید. آزمایش های انجام شده بر روی مجموعه داده NSL-KDD ومقایسه با نتایج منتشر شده اخیری که از این مجموعه داده استفاده کرده اند، موثر بودن سیستم تشخیص نفوذ پیشنهادی را بخوبینشان می دهد.

کلمات کلیدی:
سیستم تشخیص نفوذ، تشخیص نفوذ مبتنی بر امضاء، تشخیص نفوذ مبتنی بر ناهنجاری، خوشه بندی، طبقه بندی، قوانین ابتکاری

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/781762