

عنوان مقاله:

کشف سناریوهای نفوذ به شبکه های کامپیوتری با استفاده از بررسی کننده مدل SPIN

محل انتشار:

سومین کنفرانس انجمن رمز ایران (سال: 1384)

تعداد صفحات اصل مقاله: 12

نویسندگان:

مهدی آبادی - دانشکده فنی و مهندسی دانشگاه تربیت مدرس

سعید جلیلی - دانشکده فنی و مهندسی دانشگاه تربیت مدرس

خلاصه مقاله:

هر سناریوی نفوذ یک توالی از سوء استفاده های قابل اجرا توسط نفوذی است که با یک هدف خاص مانند دستیابی به پایگاه داده ها، جلوگیری از سرویس و غیره انجام می شود. در این مقاله، چگونگی استفاده از شیوه بررسی مدل LTL برای کشف خودکار سناریوهای نفوذ به شبکه های کامپیوتری نشان داده می شود. بدین منظور، فرض می شود که در شبکه مورد نظر یک سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) وجود دارد و نفوذی قصد دارد با انجام یک توالی از سوء استفاده ها و بدون این که NIDS هشدار را اعلام کند به هدف خود برسد. برای کشف سناریوی نفوذ، ابتدا اجزاء شبکه با استفاده از زبان مدل سازی PROMELA توصیف می شوند. سپس، مشخصه ای که نقیض هدف نفوذی را توصیف می کند، در منطق زمانی LTL بیان می شود. در نهایت، به کمک بررسی کننده مدل SPIN که یک بررسی کننده مدل LTL است، هر گونه تخطی از مشخصه فوق (به عبارت دیگر سناریوی نفوذ) بدست آورده می شود. همچنین، الگوریتمی ارائه می شود که با استفاده از آن میتوان از روی سناریوی نفوذ کشف شده سناریوی نفوذ حداقل را بدست آورد.

کلمات کلیدی:

سناریوی نفوذ، بررسی مدل، واریسی خودکار، منطق زمانی LTL

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/32561>

