عنوان مقاله:
تشخیص نفوذ با استفاده از رویدادنگاری فراخوان های سیستمی در محیط مانیتور ماشین مجازی

محل انتشار:
هفتمین کنفرانس انجمن رمز ایران (سال: 1389)

تعداد صفحات اصل مقاله: 8

نویسندگان:
حامد نعمتی - *دانشگاه صنعتی مالک اشتر*

رضا عزمی - *دانشگاه الزهرا*

علیرضا قهرمانیان - *دانشگاه صنعتی مالک اشتر*

محمدتقی میرمحمدرضایی - *دانشگاه الزهرا*

خلاصه مقاله:
رویدادنگاری فراخوا نهای سیستمی به عنوان ابزاری متداول برای پیادهسازی مکانیز مهای امنیتی شناخته می شود. طی چند دهه اخیرراهکار های مختلفی برای تشخیص نفوذ براساس رویدا دنگاری فراخوان های سیستمی ارائه شده ولی همزمان با پیشرفت این مکانیزم ها،نفوذگران تلاش نمودند، شیوه رویدادنگاری فراخوان های سیستم ی را تغییر دهند تا بتوانند حضور خود در سیستم و نوع فعالیتی که انجام می دهند را مخفی نمایند. در این مقاله سعی بر آن است تا با معرفی یک معماری جدید مبتنی بر مانیتور ماشین مجازی (ناظر سیستم)، مکانیزمی جهت تضمین سلامت رویدادنگاری فراخوان های سیستم ی ارائه شود. در ادامه و با توجه به حجم فراوان داده های رویدادنگاری شده، طرحی براساس درخت هافمن برای تحلیل و فشرده سازی فایل رویدادنگاری ارائه م ی شود. در مرحله تشخیص نفوذ، با استفاده از شبکه بیزین ناهنجاری های داده های گردآوری شده، مشخص م یشود. برای ارزیابی معماری ارائه شده، نمونه اولیه ای مبتنی بر مانیتورماشین مجازی SCInterceptor پیادهسازی شده است.

کلمات کلیدی:
شخیص نفوذ، مانیتور ماشین مجازی، رویدادنگاری، فراخوانهای سیستمی ، درخت هافمن، دسته بندی کننده بیزین