عنوان مقاله:

بهره گیری از Port-Knocking بعنوان اولین لایه دفاعی در استراتژی دفاع در عمق با استفاده ترکیبی از ویژگی های پروتکل کنترل پیامهای اینترنتی، آدرس اینترنتی و تونل زنی

محل انتشار:

فصلنامه پدافند الکترونیکی و سایبری, دوره 2, شماره 4 (سال: 1393)

تعداد صفحات اصل مقاله: 17

نویسندگان:

مهران پوروهاب - *دانشگاه گیلان*

رضا ابراهیمی آتانی - *دانشگاه گیلان*

خلاصه مقاله:

شبکه های کامپیوتری همواره مستعد مبتلا شدن به انواع حملات بوده و این حملات به طور معمول شامل حملات شناسایی، دست یابی و از کار انداختن خدمات هستند. در حملات از نوع شناسایی، مهاجمین اقدام به جمع آوری اطلاعات و شناسایی خدمات در حال اجرا در جهت نیل به آسیب رسانی، دست یابی و یا از کار انداختن خدمات هستند. در واقع، خوراک حملات دست یابی و از کار انداختن خدمات از طریق حملات شناسایی فراهم می شود. Port-Knocking(PKn) یک روش منحصر بفرد برای جلوگیری از کشف و بهره برداری از خدمات آسیب پذیر توسط مهاجمین بوده و در واقع هدف آن مخفی نگه داشتن خدمات از دید نفوذگران و عدم کارآیی حملات شناسایی است، در حالی که کاربران تصدیق شده اجازه دسترسی به این خدمات نامرئی را دارند. در این مقاله روش جدیدی با هدف ایجاد سادگی و استفاده از ابزارهای موجود در اغلب سیستم عامل ها به منظور حذف برنامه های خاص و پیچیده جهت اجرای فرآیند PKn و باز کردن پورت ها در هر زمان و هر کجا معرفی گردیده است. از اهداف دیگر این روش، ایجاد پیچیدگی بیشتر در عملیات Knock با بکارگیری از ویژگی های خاص پروتکل ICMP و استفاده همزمان از مرورگرهای اینترنتی جهت کاهش کارآیی حملات Replay و از بین بردن مخاطرات ناشی از حملات DoS با مخفی نگه داشتن خدمات است. جهت اطمینان از کارآیی و قابلیت های ارائه شده، این روش با موفقیت بر روی سیستم عامل RouterOS میکروتیک پیاده سازی و اجرا گردیده است.

کلمات کلیدی:

امنیت شبکه, امنیت خدمات, امنیت پورت, احراز هویت, پورت-ناکینگ