سومین کنفرانس فناوری اطلاعات و دانش
۶ تا ۸ آذرماه ۱۳۸۶

تشخیص نفوذ در دسترسی‌های رمز شده با پروتکل SSH به سرویس‌دهنده‌های عمومی شبکه

وحید آقایی، فضل‌الله ادیب‌نیا و الهام حجتی

دانشگاه یزد و دانشگاه صنعتی امیرکبیر

E-mail: fadib@yazduni.ac.ir

چکیده – با فراگیر شدن ابزارهای کاربردی مختلف به عنوان سرویس‌دهنده‌های شبکه، حملات به آن‌ها مشکلاتی را ایجاد کرده است. سیستم‌های تشخیص نفوذ *(IDS)*، یک راه حل برای برخورد با چنین مشکلاتی است. اما این سیستم‌ها در مواجهه با دسترسی‌های رمزشده با پروتکل‌های رمزنگاری، به دلیل این که نمی‌توانند به محتویات بسته سرکشی کنند، توانایی عکس‌العمل مؤثر را ندارند. این مقاله، روشی نوین جهت تشخیص رفتارهای غیر معمول در دسترسی‌های رمزشده با پروتکل *SSH* به سرویس‌دهنده‌های عمومی شبکه مانند سرورهای *http*، سرورهای *ftp* و سرورهای پایگاه داده‌ها را ارائه می‌دهد. در این روش، ابتدا سیستم، اطلاعاتی شامل حجم داده انتقالی و فاصله زمانی بین پیام‌ها را از هر کاربر *SSH* استخراج می‌کند. در مرحله دوم، انواع فعالیت‌ها بر مبنای شباهت اطلاعات از یکدیگر تشخیص داده می‌شوند. در پایان، حملات با استفاده از قوانین تشخیص نفوذی که از فرکانس دسترسی‌ها و خصوصیات ترافیک *TCP* تولید شده است، کشف می‌شوند. این سیستم، اطلاعات محرمانه را استخراج نمی‌کند، چون تنها با استفاده از حجم داده انتقالی و فاصله زمانی بین پیام‌ها به تشخیص نفوذ می‌پردازد و قبل از شروع کار، به محاسبات زیادی که در روش‌های مرسوم تحلیل ترافیک رمزشده انجام می‌گیرد، نیاز ندارد. ما با پیاده‌سازی سیستم پیشنهادی خود بر روی نرم‌افزار تشخیص نفوذ *Snort* و با استفاده از مجموعه داده ارزیابی *DARPA*، نشان خواهیم داد که این سیستم توانایی تشخیص حملات را با دقت بالا دارا می‌باشد.

کلید واژه- *DARPA، Flooding، IDS، Snort، SSH*

۱- مقدمه

از زمانی که سرویس‌دهنده‌های عمومی شبکه رایج شدند، حملات بر علیه آن‌ها مشکلات زیادی را ایجاد کرده است. IDS (Intrusion Detection System) [۱]، یک راه حل جهت مواجهه با این حملات است. این سیستم، در کنار سرویس‌دهنده‌های عمومی شبکه قرار گرفته و فعالیت کاربران را با تحلیل پروتکل و تطبیق الگو، مشاهده می‌کند. به عبارت دیگر، سیستم‌های تشخیص نفوذ، Header و Payload پروتکل‌هایی مانند http، ftp و pop3 را از روی پیام‌های مشاهده شده، بازسازی می‌کنند و حملات را از مقایسه ترافیک با قوانین حملات، تشخیص می‌دهند. بنابراین، IDS باید تمام Payload پیام‌ها را مشاهده کند.

پروتکل‌هایی مانند SSH (Secure Shell) [۲]، جهت ایجاد راهی برای اطمینان از ارتباطات امن بر روی بسترهای ناامنی همچون اینترنت، پیشنهاد شده‌اند. این پروتکل، امکان تصدیق هویت کاربر و سرور و حفاظت از درستی و محرمانگی داده‌ها را ممکن می‌سازد. IDSهای مرسوم در مواجهه با ترافیک‌های رمزشده، یا اصلاً به آن‌ها توجه نکرده و بدون تحلیل، اجازه عبور می‌دهند که این روش دست نفوذگران به شبکه را باز می‌گذارد و یا اجازه عبور ترافیک‌های رمزشده را نمی‌دهند که این روش هم نمی‌تواند از مزایای رمزکردن ترافیک بهره‌مند شود. روش سوم [۳]، نیازمند به امانت گرفتن کلید اختصاصی توسط IDS است. به عبارت دیگر، این IDSها پس از آشکارسازی به مشاهده