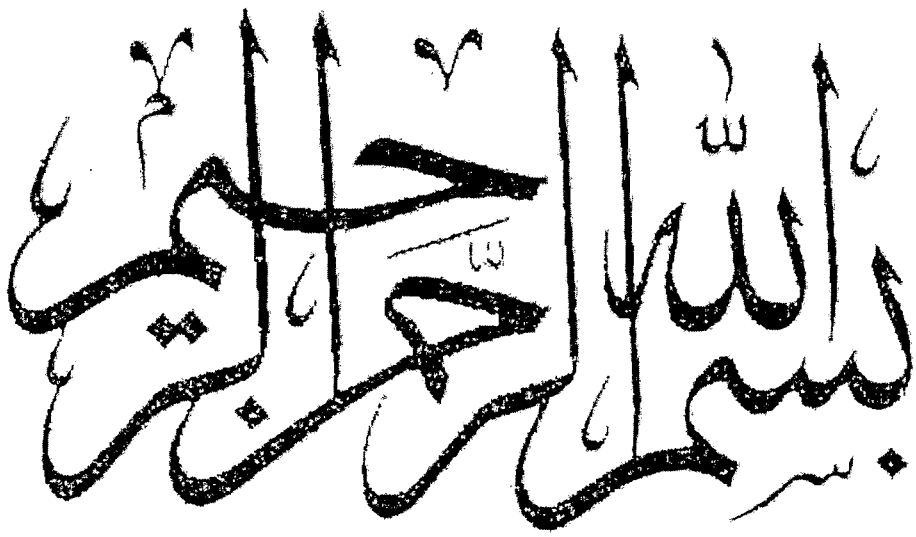

دانشکده مهندسی برق و کامپیوتر
گروه مهندسی کامپیوتر

پایان نامه
برای دریافت درجه کارشناسی ارشد
مهندسی فناوری اطلاعات – شبکه‌های کامپیوتری

بررسی روش‌های تشخیص نفوذ در ترافیک رمزشده

استاد راهنما: دکتر فضل‌الله ادیب‌نیا

اساتید مشاور: دکتر محمد حسن شیرعلی شهرضا و دکتر محمد قاسم‌زاده

پژوهش و نگارش: وحید آقایی

شهریورماه ۱۳۸۷

تقدیم به

مادر مهربان و دلسوز و پدر صبورم که در دنیا بهتر از آن دو پیدا نکردم

و همسر فریبا

و دوست که هر چه بر سر ما می‌رود، محبت اوست

و تمام آن‌هایی که دوستشان داریم و نمی‌دانند چقدر

و تمام آن‌هایی که دوستمان دارند و نمی‌دانیم چقدر

پروردگارا! برایم سرنوشتی خیر بنویس، تقدیری مبارک، تا زود نخواهم آن چه را تو دیر می‌خواهی.

خداوند مهربان را سپاسگزارم که توانستم یکی دیگر از مقاطع علم‌آموزی را پشت سر بگذارم، بر خود لازم می‌دانم از اساتید بزرگوارم جناب آقای دکتر ادیب‌نیا، جناب آقای دکتر قاسم‌زاده و جناب آقای دکتر شیرعلی که توفیق استفاده از راهنمائی‌های مدبرانه و دلسوزانه آنان را برای انجام این پژوهش داشتم و کلیه عزیزانی که به نوعی من را همراهی نموده‌اند، کمال تشکر و قدردانی را داشته باشم.

این پایان‌نامه با حمایت‌های مالی
مرکز تحقیقات مخابرات ایران
به انجام رسیده است.

مدیریت تحصیلات تکمیلی	**صورتجلسه دفاعیه پایان نامه دانشجوی** **دوره کارشناسی ارشد**	شناسه: ب/ک/۳ شماره: تاریخ: پیوست:

جلسه دفاعیه پایان نامه تحصیلی آقای: ***وحید آقائی***

دانشجوی کارشناسی ارشد رشته / گرایش: ***مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری***

تحت عنوان: ***بررسی روش‌های تشخیص نفوذ در ترافیک رمز شده***

و تعداد واحد: ۶ در تاریخ ۱۳۸۷/۸/۱ با حضور اعضای هیأت داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیأت داوران، پایان نامه با نمره: به عدد ۱۹/ **به حروف** نوزده تمام **و درجه** عالی **مورد تصویب قرار گرفت.**

عنوان	نام و نام خانوادگی	امضاء
استاد / استادان راهنما	دکتر فضل ا... ادیب‌نیا	
استاد / استادان مشاور	دکتر محمدحسن شیرعلی دکتر محمد قاسم‌زاده	
متخصص و صاحبنظر داخلی	دکتر مهدی صرام	
متخصص و صاحبنظر خارجی	دکتر علیرضا ذوالقدر اصلی (از دانشگاه شیراز)	

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام و نام خانوادگی: حمیدرضا ابوطالبی

امضاء:

چکیده

با فراگیر شدن سرویس‌دهنده‌های مختلف شبکه، حملات به آن‌ها مشکلاتی را ایجاد کرده است. سیستم‌های تشخیص نفوذ، 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 پایان‌نامه، روشی نوین جهت تشخیص رفتارهای غیرمعمول در دسترسی‌های رمزشده با پروتکل SSH به سرویس‌دهنده‌های وب، ftp و انواع پایگاه داده 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. آن‌گاه، 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. با استفاده از مجموعه‌داده ارزیابی DARPA، نشان داده شد که این سیستم توانایی تشخیص حملات را با دقت بالا دارا می‌باشد.

فهرست مطالب

صفحه

صفحه

صفحه

صفحه

فهرست شکل‌ها

صفحه

صفحه

فهرست جدول‌ها

صفحه

فصل اول

مقدمه

۱-۱. مقدمه

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکت‌های دولتی و سازمان‌های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست‌های فضای سایبر، کارمندان ناراضی و هکرها، رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست، بلکه یک ضرورت است. در حالی که بسیاری فناوری اطلاعات و ارتباطات را موجب تسهیل در انتقال اطلاعات می‌دانند، موضوع امنیت در تبادل اطلاعات همواره به عنوان یکی از اصول غافل مانده به شکل معضلی پنهان باقی مانده است. امنیت اطلاعات برای بخش مهمی‌از فعالان بخش فناوری اطلاعات تنها زمانی به عنوان موضوعی حاد مطرح می شود که مشکلی در شبکه به وجود آید. در اغلب مواقع این مشکلات موجب ضربه‌ای سنگین بر شبکه و یا به اطلاعات موجود در آن می‌شود. در واقع می توان گفت رویکرد دیر هنگامی‌است. اینترنت همواره از جهت های گوناگون نقد و ارزیابی شده است، اما واقعیت این است که این شبکه عظیم مانند هر اجتماع عادی انسانی دیگر در معرض تهدیدها و خطرات قرار دارد. از نفوذ داده‌های مخرب گرفته تا تخریب داده‌های سالم و برهم زدن نظم شبکه همه و همه تنها به یک مورد بستگی دارد و آن بحث امنیت اطلاعات در محیط اینترنت است. امروزه امنیت اطلاعات در زمینه اینترنت از یک بحث حاشیه‌ای به یک بحث ضروری تغییر جهت داده است. هرگونه خرید و فروش روی اینترنت و یا انتقال داده‌ها باید تحت یک کنترل امنیتی صورت گیرد.

اگر امنیت شبکه برقرار نشود، مزیت های فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعات عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی قرار می‌گیرند. همچنین دستکاری اطلاعات به عنوان زیربنای فکری ملت ها به دست گروه های سازماندهی شده بین المللی، به نوعی مختل کردن امنیت ملی و تهاجم علیه دولت ها و تهدیدی ملی محسوب می‌شود. هم اکنون نیز بانک‌ها و بسیاری از نهادها و دستگاه‌های دیگر از طریق شبکه فعالیت

می کنند، به همین دلیل جلوگیری از نفوذ عوامل مخرب در شبکه به صورت مسأله‌ای استراتژیک درآمده که نپرداختن به آن موجب ایجاد خساراتی خواهد شد.

امنیت شبکه یکی از بحث های مورد علاقه بسیاری از محققان شده است. کدهای مخرب بسیاری نشان داده است که هکرها توانایی ایجاد خرابی در سیستم‌های متصل به شبکه را دارا می‌باشند. همچنین شرکت مایکروسافت تنها در سال ۲۰۰۴، ۴۵ بولتن انتشار داده است که نشان می‌دهد نفوذپذیری‌های فراوانی در سیستم‌عامل‌های متصل به اینترنت وجود دارد. ابزارهای زیادی از دیوارهای آتش گرفته تا ویروس‌یاب‌ها ایجاد شدند که امنیت شبکه را بهبود ببخشند.

یکی از روش‌های حفاظت از شبکه که به‌طور فزاینده‌ای در حال عمومی‌شدن است، سیستم تشخیص نفوذ (IDS)[1] می‌باشد. سیستم‌های تشخیص نفوذ به دو شکل مختلف وجود دارند که دو نوع برجسته آن سیستم تشخیص نفوذ بر مبنای میزبان (HIDS)[2] و سیستم تشخیص نفوذ بر مبنای شبکه (NIDS)[3] است. همان‌طور که از نام HIDSها معلوم است، بر روی رایانه‌های میزبان به‌صورت انفرادی نصب شده و Log Fileها و System Registryهای آن رایانه را بررسی می‌کنند تا تشخیص دهند که آیا نفوذی انجام گرفته و یا در حال انجام است و یا این‌که سیستم در شرایط عادی به سر می‌برد.

سیستم‌های تشخیص نفوذ در کنار سرویس‌دهنده‌های عمومی‌شبکه قرار گرفته و فعالیت کاربران را با تحلیل پروتکل[4] و تطبیق الگو[5]، مشاهده می‌کند. به عبارت دیگر، سیستم تشخیص نفوذ، سرآیند و متن پروتکل‌هایی مانند http[6] و ftp[7] را از روی پیام‌های مشاهده شده، بازسازی می‌کند و حملات را از مقایسه ترافیک با قوانین حملات[8]، تشخیص می‌دهد. بنابراین، سیستم تشخیص نفوذ باید تمام Payload پیام‌ها را مشاهده کند. سیستم‌های تشخیص نفوذ بر مبنای

---

[1] Intrusion Detection System
[2] Host Base IDS
[3] Network Base IDS
[4] Protocol Analysis
[5] Pattern Matching
[6] Hyper Text Transfer Protocol
[7] File Transfer Protocol
[8] Attack Signature

رفتارهای بد، عمل تطبیق الگو را بر روی بسته‌ها اعمال می‌کنند، در حالی که سیستم‌های تشخیص نفوذ بر مبنای رفتارهای غیرعادی سعی می‌کنند رفتارهای شبکه‌ای عادی را تشخیص دهند و هر مدل ترافیکی که با آن انحراف معیار داشت را هشدار دهند.

اگر یک انتخاب بین HIDS و NIDS باید انجام گیرد، معمولاً NIDS انتخاب می شود. این ابزار یا نرم‌افزار کل یک زیرشبکه را محافظت کرده و معمولاً از بسیاری از HIDSها راحت‌تر مدیریت می‌شود.

روش دیگری که از دیرباز به عنوان یک ضرورت برای حفاظت از اطلاعات خصوصی مقابل دسترسی های غیرمجاز در تجارت و سیاست و مسائل نظامی وجود داشته، رمزنگاری است. به‌طور مثال تلاش برای ارسال یک پیام سری میان دو هم پیمان به گونه‌ای که حتی اگر از سوی دشمن دریافت شود قابل درک نباشد، در رم.قدیم نیز دیده شده است. در سال های اخیر رمزنگاری و تحلیل رمز از یک هنر پا را فراتر گذاشته و یک علم مستقل شده است و در واقع کانال‌های غیرامن همانند تلفن به عنوان یک وسیله عملی برای ارسال اطلاعات محرمانه روی ماهواره ها شناخته می‌شود. پیشرفت علم رمزنگاری موجب به وجود آمدن روش‌های تحلیل مختلفی شده است به گونه‌ای که به‌طور متناوب شبکه‌های رمز مختلف شکسته شده اند. معروف‌ترین نمونه این نوع شبکه‌ها ماشین انیگما بوده است. انیگما ماشین رمزگذار و کدگذار و کدکننده‌ای بوده است که حزب نازی در زمان جنگ جهانی دوم برای ارسال پیام‌هایشان از طریق رادیو به سایر نقاط استفاده می‌کردند. با این حال بسیاری از نفوذگرها برای ارسال دستورهای مخرب خود از رمزنگاری استفاده می‌کنند تا کسی در بین راه از هدف آن‌ها مطلع نشود.

سیستم‌های تشخیص نفوذ مرسوم کمبودهای زیادی دارند. به عنوان مثال نمی‌توانند بدون رمزگشایی ترافیک رمزشده، عمل تطبیق الگو با مشخصه‌های حملات را انجام دهند. در حالی که پروتکل‌های زیادی مانند WEP[1]، IPsec[2]، SSL[3] و SSH[4] وجود دارند که جهت ایجاد راهی برای

---

[1] Wired Equvalent Privacy
[2] IP Security
[3] Secure Sockets Layer
[4] Secure Shell

اطمینان از ارتباطات امن بر روی بسترهای ناامنی همچون اینترنت، پیشنهاد شده‌اند و با رمز کردن ترافیک این پروتکل ها، امکان تصدیق هویت سرویس گیرنده[1] و سرور[2] و حفاظت از درستی و محرمانگی داده‌ها را ممکن می‌سازند.

سیستم‌های تشخیص نفوذ 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، نیازمند به امانت گرفتن کلید اختصاصی توسط سیستم تشخیص نفوذ است [۱]. به عبارت دیگر، این سیستم‌های تشخیص نفوذ پس از آشکارسازی به مشاهده ترافیک می‌پردازند. این روش از نظر مدیریت کلید و پیکربندی شبکه، دارای مشکلاتی است، اما در حال حاضر، بسیار عمومی‌شده است. زیرا سرویس‌هایی که نیاز به ارتباط امن بین سرویس‌گیرنده و سرور دارند، در حال افزایش‌اند. بنابراین، مدیران این‌گونه شبکه‌ها با وضع دشوار تأمین امنیت سرورهایی که از پروتکل SSH [۲] استفاده می‌کنند، مواجه هستند، در حالی که این سیستم‌ها به خاطر ناتوانی در مشاهده ترافیک رمزشده توسط سیستم تشخیص نفوذ، امنیت پایینی دارند. هدف اصلی ما، حل این مشکل است.

در این پایان‌نامه یک روش نوین به منظور تشخیص رفتارهای غیرعادی در دسترسی‌های رمزشده با پروتکل SSH به سرویس‌دهنده‌های وب، ftp و پایگاه‌داده را پیشنهاد شده است. همانطور که می‌دانید در ابتدا پروتکل SSH جهت ایجاد امنیت ارتباطات پروتکل‌هایی مانند Telnet و Rlogin، ایجاد گردید. ولی بعدا پشتیبانی از برقراری امنیت هر نوع نرم‌افزار کاربردی[3] شبکه که به صورت سرویس‌گیرنده / سرور و بر مبنای TCP[4] مانند http، ftp و انواع پایگاه داده کار می‌کنند، با روشی که به اصطلاح Port Forwarding نامیده می‌شود، اضافه شد. استفاده از روش

---

[1] Client
[2] Server
[3] Application
[4] Transfer Control Protocol

Port Forwarding جهت برقراری امنیت نرم‌افزارهای کاربردی در سطح لایه کاربرد مدل OSI[1] هر روز بیشتر شده، در حالی که تشخیص حملاتی که از این طریق رمز می‌شوند، بدون امانت‌گرفتن کلید اختصاصی توسط سیستم‌های تشخیص نفوذ مرسوم، قابل تشخیص نیست. روش پیشنهادی بدون رمزگشایی[2] به تحلیل ترافیک رمزشده می‌پردازد. سیستم پیشنهادی با استفاده از مجموعه‌داده[3] ارزیابی DARPA [۳]، آزمایش می‌شود.

۱-۲. تعریف موضوع، اهداف و فرضیه‌ها

هدف ما از پایان‌نامه واضح است. در حالی که سیستم‌های تشخیص نفوذ به محیط‌های رمزنشده محدود می‌شوند، هدف ما فایق آمدن به این محدودیت در دسترسی‌های رمزشده با پروتکل SSH به سرویس‌دهنده‌های وب، ftp و پایگاه‌داده است. هدف اصلی، ایجاد و طراحی یک روش است که بدون رمزگشایی، امکان بررسی ترافیک رمزشده با پروتکل SSH به سرورهای http، ftp و پایگاه‌داده را فراهم می‌آورد.

هدف دوم ارزیابی روش پیشنهادی با استفاده از مجموعه‌داده ارزیابی DARPA می‌باشد. میزان نرخ خطای[4] False Positive و False Negative این سیستم در شرایط مختلف بررسی می‌گردد.

فرض بر این است که بتوان با بررسی و تحلیل حجم داده ارسالی و فاصله زمانی بین بسته‌های SSH در ارتباط با سرویس‌دهندهای وب، ftp و پایگاه‌داده، رفتارهای عادی را از رفتارهای غیرعادی تشخیص داده و ترافیک حملات را شناسایی شود.

انتظار داریم سیستم پیشنهادی بتواند حملات رمزشده با پروتکل SSH به

---

[1] Open Systems Interconnect
[2] Decryption
[3] Dataset
[4] Error Rate