

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

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

۱۳۸۸/۷/۱

شهریورماه ۱۳۸۷

تست شده در مرکز تحقیقات  
تست شده در مرکز

۱۲۶۸۸۰

تقدیم به

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

و همسرم فریبا

و دوستی که هر چه بر سر ما می‌رود، محبتت اوست

و تمام آن‌هایی که دوستان داریم و نمی‌دانند چقدر

و تمام آن‌هایی که دوستان دارند و نمی‌دانیم چقدر

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

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 راهنمایی‌های 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 پایان نامه با حمایت های 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 آقایی

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.

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

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام و نام خانوادگی: حمیدرضا ابوطالبی

امضاء:

## چکیده

با فراگیر شدن سرویس دهنده‌های 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 رمز شده 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 رمز شده با پروتکل SSH به سرویس دهنده‌های 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 رمز شده انجام می‌گیرد، نیاز ندارد. با استفاده از مجموعه داده ارزیابی DARPA، نشان داده شد که این سیستم توانایی تشخیص حملات را با دقت بالا دارا می‌باشد.

## فهرست مطالب

### صفحه

	فصل اول: مقدمه
۲	۱-۱. مقدمه
۶	۲-۱. تعریف موضوع، اهداف و فرضیه‌ها
۷	۳-۱. روش تحقیق
	فصل دوم: معرفی سیستم‌های تشخیص نفوذ
۹	۱-۲. سیستم تشخیص نفوذ
۱۰	۲-۲. ماتریس سیستم تشخیص نفوذ
۱۱	۳-۲. تفاوت تشخیص با پیش‌گیری
۱۲	۱-۳-۲. تشخیص نفوذ
۱۲	۲-۳-۲. پیش‌گیری از نفوذ
۱۴	۴-۲. انواع سیستم تشخیص نفوذ
۱۴	۱-۴-۲. سیستم‌های تشخیص نفوذ مبتنی بر میزبان
۱۵	۱-۱-۴-۲. مزایا
۱۶	۲-۱-۴-۲. معایب
۱۶	۲-۴-۲. سیستم‌های تشخیص نفوذ مبتنی بر شبکه
۱۸	۱-۲-۴-۲. مزایا
۱۸	۲-۲-۴-۲. معایب
۱۹	۵-۲. تکنیک‌های سیستم تشخیص نفوذ
۱۹	۱-۵-۲. تشخیص نمونه‌های غیرمتعارف
۲۰	۲-۵-۲. کشف از روی نشانه یا سوء استفاده



صفحه

۲۱	۳-۵-۲ . نظارت بر هدف
۲۱	۴-۵-۲ . کاوش نهایی
۲۲	۶-۲ . چگونگی عملکرد سیستم تشخیص نفوذ
۲۳	۷-۲ . مدل‌های تجزیه و تحلیل در سیستم‌های تشخیص نفوذ
۲۳	۱-۷-۲ . مدل سیستم‌های مبتنی بر الگویابی
۲۴	۲-۷-۲ . مدل سیستم‌های مبتنی بر تشخیص رفتارهای ناهنجار
۲۵	۸-۲ . اجزا سیستم‌های تشخیص نفوذ
۲۵	۱-۸-۲ . حس‌گرها
۲۷	۲-۸-۲ . تحلیل‌گرها
۲۷	۳-۸-۲ . انباره وقایع
۲۷	۴-۸-۲ . واحدهای پاسخ‌دهی
۲۸	۹-۲ . چگونگی قرارگرفتن سیستم تشخیص نفوذ در شبکه
۲۹	۱۰-۲ . مزایا و معایب سیستم‌های تشخیص نفوذ

**فصل سوم: پروتکل Secure Shell**

۳۳	۱-۳ . آشنایی با پروتکل Secure Shell
۳۴	۲-۳ . پروتکل SSHv1
۳۸	۱-۲-۳ . تصدیق هویت سرور
۴۲	X11 Forwarding . ۲-۲-۳
۴۳	Port Forwarding . ۳-۲-۳
۴۸	۳-۳ . پروتکل SSH2
۴۸	۱-۳-۳ . پروتکل انتقال SSHv2
۵۲	۲-۳-۳ . الگوریتم مذاکره و تبادل کلید

صفحه

۵۶	X11 Forwarding . ۳-۳-۳
۵۷	Port Forwarding . ۴-۳-۳
<b>فصل چهارم: مجموعه داده ارزیابی Darpa</b>	
۶۱	۱-۴ . مقدمه
۶۱	۲-۴ . شبکه شبیه سازی
۶۲	۱-۲-۴ . مدل کردن شبکه شبیه سازی نیروی هوایی آمریکا
۶۲	۲-۲-۴ . سخت افزار و توپولوژی شبکه شبیه سازی
۶۴	۳-۲-۴ . نرم افزارهای شبیه سازی
۶۴	۴-۲-۴ . ماشین های مجازی
۶۵	۵-۲-۴ . تولید ترافیک
۶۶	۳-۴ . رخنه
۶۶	۱-۳-۴ . منابع
۶۷	۲-۳-۴ . طول عمر رخنه
۶۹	۴-۴ . کاربردهای مجموعه داده ارزیابی Darpa
<b>فصل پنجم: پیاده سازی سیستم پیشنهادی</b>	
۷۱	۱-۵ . مقدمه
۷۲	۲-۵ . ساختار سیستم پیشنهادی
۷۲	۱-۲-۵ . تشخیص ترافیک SSH
۷۳	۲-۲-۵ . جداسازی فعالیت های مربوط به هر سرویس گیرنده
۷۴	۳-۲-۵ . به روز رسانی جدول سرویس گیرنده ها
۷۵	۱-۳-۲-۵ . شماره سرویس گیرنده
۷۵	۲-۳-۲-۵ . آدرس IP سرویس گیرنده

صفحه

۷۵	۳-۳-۲-۵ . گونه پروتکل SSH
۷۷	۴-۳-۲-۵ . تعداد بیت فیلد MAC برای سرویس گیرنده های SSH2
۷۷	۴-۲-۵ . مشخص کردن هر فعالیت از یک سرویس گیرنده
۷۸	۵-۲-۵ . محاسبه حجم داده ارسالی در هر پیام SSH
۸۰	۶-۲-۵ . تولید ماتریس حالت هر فعالیت
۸۱	۷-۲-۵ . تحلیل فرکانسی
۸۳	۸-۲-۵ . به روز رسانی گروه های حالت
۸۵	۹-۲-۵ . تشخیص حمله و یا نرمال / غیرنرمال بودن فعالیت
۸۶	۳-۵ . انواع حملات قابل تشخیص
	<b>فصل ششم: ارزیابی سیستم پیشنهادی</b>
۹۰	۱-۶ . زبان برنامه نویسی
۹۰	۲-۶ . آماده سازی جهت ارزیابی
۹۰	۱-۲-۶ . نرم افزار Ethereal
۹۲	۲-۲-۶ . ایستگاه کاری VMware
۹۵	۳-۶ . ارزیابی سیستم پیشنهادی
۹۹	۱-۳-۶ . بهبود سیستم پیشنهادی
	<b>فصل هفتم: مطالعات مرتبط، نتیجه گیری و پیشنهادات</b>
۱۰۵	۱-۷ . مطالعات مرتبط
۱۰۶	۲-۷ . نتیجه گیری
۱۰۶	۳-۷ . پیشنهادات
۱۰۸	منابع و مراجع

## فهرست شکل‌ها

### صفحه

۲۳	شکل ۱-۲: چگونگی عملکرد سیستم تشخیص نفوذ
۲۶	شکل ۲-۲: چارچوب کاری مشترک سیستم‌های تشخیص نفوذ
۳۴	شکل ۱-۳: SSH به عنوان Remote Shell
۳۶	شکل ۲-۳: ساختار بسته‌های SSHv1
۳۹	شکل ۳-۳: تصدیق هویت سرور SSHv1
۴۰	شکل ۴-۳: پیام SSH-SMSG-PUBLIC-KEY
۴۱	شکل ۵-۳: پیام SSH-CMSG-SESSION-KEY
۴۳	شکل ۶-۳: ارسال ارتباط X11
۴۴	شکل ۷-۳: Local Port Forwarding
۴۵	شکل ۸-۳: Remote port forwarding
۴۵	شکل ۹-۳: تبادل پیام‌های Port Forwarding
۴۶	شکل ۱۰-۳: پیام SSH-SMG-PORT-OPEN
۴۷	شکل ۱۱-۳: پیام SSH-CMSG-PORT-FORWARD-REQUEST
۴۸	شکل ۱۲-۳: لایه‌های پروتکل SSHv2 که بر روی TCP قرار گرفته‌اند
۵۰	شکل ۱۳-۳: ساختار بسته‌های SSHv2
۵۳	شکل ۱۴-۳: مذاکره الگوریتم و تبادل کلید
۵۴	شکل ۱۵-۳: پیام SSH-MSG-KEXINIT
۵۷	شکل ۱۶-۳: پیام درخواست X11 forwarding
۵۸	شکل ۱۷-۳: اطلاعات مخصوص درخواست در پیام local port forwarding
۵۸	شکل ۱۸-۳: اطلاعات مخصوص درخواست در پیام remote port forwarding

- شکل ۴-۱: توپولوژی شبکه شبیه‌سازی ۶۳
- شکل ۴-۲: آسیب‌پذیری حملات جدید در طول زمان کاهش می‌یابد ۶۷
- شکل ۵-۱: ساختار سیستم پیشنهادی ۷۳
- شکل ۵-۲: جداسازی فعالیت‌های مربوط به هر سرویس‌گیرنده از روی آدرس ۷۴
- شکل ۵-۳: پیام‌های ردوبدل شده در یک ارتباط SSH مشاهده شده توسط نرم‌افزار Ethereal ۷۵
- شکل ۵-۴: مشخص کردن هر فعالیت از یک سرویس‌گیرنده با استفاده از فاصله زمانی ۷۸
- شکل ۵-۵: نمونه‌ای از ترافیک SSH2 مونیتور شده با نرم‌افزار Ethereal ۸۰
- شکل ۵-۶: حجم داده ارسالی از طرف سرویس‌گیرنده به سرور و از طرف سرور به سرویس‌گیرنده ۸۱
- شکل ۵-۷: نحوه دسته‌بندی ماتریس‌های حالت ۸۲
- شکل ۵-۸: مثالی از ترافیک درخواست / پاسخ یک سرور وب در حالت نرمال ۸۵
- شکل ۶-۱: شمایی از نرم‌افزار شبیه‌ساز VMWare ۹۴
- شکل ۶-۲: شمایی از نرم‌افزار Packet Player ۹۵
- شکل ۶-۳: نرخ خطا به ازای مقادیر مختلف  $Th_{req}$  در ارزیابی اولیه با پروتکل SSH1 ۹۷
- شکل ۶-۴: نرخ خطا به ازای مقادیر مختلف  $Th_{res}$  در ارزیابی اولیه با پروتکل SSH1 ۹۷
- شکل ۶-۵: نرخ خطا به ازای مقادیر مختلف  $Th_{req}$  در ارزیابی اولیه با پروتکل SSH2 ۹۸
- شکل ۶-۶: نرخ خطا به ازای مقادیر مختلف  $Th_{res}$  در ارزیابی اولیه با پروتکل SSH2 ۹۸
- شکل ۶-۷: نرخ خطا به ازای مقادیر مختلف  $Th_{req}$  در ارزیابی نهایی با پروتکل SSH1 ۱۰۱
- شکل ۶-۸: نرخ خطا به ازای مقادیر مختلف  $Th_{res}$  در ارزیابی نهایی با پروتکل SSH1 ۱۰۱
- شکل ۶-۹: نرخ خطا به ازای مقادیر مختلف  $Th_{req}$  در ارزیابی نهایی با پروتکل SSH2 ۱۰۲
- شکل ۶-۱۰: نرخ خطا به ازای مقادیر مختلف  $Th_{res}$  در ارزیابی نهایی با پروتکل SSH2 ۱۰۲

## فهرست جدول‌ها

### صفحه

۳۶	جدول ۱-۳: نوع پیام‌های SSHv1
۵۱	جدول ۲-۳: انواع پیام‌های انتقال SSHv1
۶۸	جدول ۱-۴: حملاتی که در مجموعه داده ارزیابی تشخیص نفوذ Darpa استفاده شده است
۷۶	جدول ۱-۵: تشخیص گونه پروتکل SSH از روی پیام‌های شناسایی سرویس‌گیرنده و سرور
۷۷	جدول ۲-۵: اندازه فیلد MAC به ازای الگوریتم‌های مختلف محاسبه Hash
۷۸	جدول ۳-۵: مثالی از جدول سرویس‌گیرنده‌ها
۸۷	جدول ۴-۵: مثالی از جدول تشخیص حملات Flooding
	جدول ۱-۶: شماره پورت انواع نرم‌افزارهای کاربردی که حمله به آن‌ها توسط سیستم پیشنهادی ما
۹۱	تشخیص داده می‌شود.

# 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 می‌طلبد. 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 مهمی از فعالان بخش فناوری اطلاعات تنها زمانی به عنوان موضوعی حاد مطرح می‌شود 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 می‌توان گفت رویکرد دیر هنگامی است. اینترنت همواره از جهت‌های 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، مزیت‌های 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 ملت‌ها به دست گروه‌های سازماندهی شده بین‌المللی، به نوعی مختل کردن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود. هم‌اکنون 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 سیستم های متصل به شبکه را دارا می باشند. همچنین شرکت مایکروسافت تنها در سال ۲۰۰۴، ۴۵ بولتن انتشار داده است که نشان می دهد نفوذپذیری های فراوانی در سیستم عامل های متصل به اینترنت وجود دارد. ابزارهای زیادی از دیوارهای آتش گرفته تا ویروس یابها ایجاد شدند که امنیت شبکه را بهبود ببخشند.

یکی از روش های حفاظت از شبکه که به طور فزاینده ای در حال عمومی شدن است، سیستم تشخیص نفوذ (IDS)<sup>۱</sup> می باشد. سیستم های تشخیص نفوذ به دو شکل مختلف وجود دارند که دو نوع برجسته آن سیستم تشخیص نفوذ بر مبنای میزبان (HIDS)<sup>۲</sup> و سیستم تشخیص نفوذ بر مبنای شبکه (NIDS)<sup>۳</sup> است. همان طور که از نام HIDS ها معلوم است، بر روی رایانه های میزبان به صورت انفرادی نصب شده و Log File ها و System Registry های آن رایانه را بررسی می کنند تا تشخیص دهند که آیا نفوذی انجام گرفته و یا در حال انجام است و یا این که سیستم در شرایط عادی به سر می برد.

سیستم های تشخیص نفوذ در کنار سرویس دهنده های عمومی شبکه قرار گرفته و فعالیت کاربران را با تحلیل پروتکل<sup>۴</sup> و تطبیق الگو<sup>۵</sup>، مشاهده می کند. به عبارت دیگر، سیستم تشخیص نفوذ، سرآیند و متن پروتکل هایی مانند http<sup>۶</sup> و ftp<sup>۷</sup> را از روی پیام های مشاهده شده، بازسازی می کند و حملات را از مقایسه ترافیک با قوانین حملات<sup>۸</sup>، تشخیص می دهد. بنابراین، سیستم تشخیص نفوذ باید تمام Payload پیام ها را مشاهده کند. سیستم های تشخیص نفوذ بر مبنای

<sup>1</sup> Intrusion Detection System

<sup>2</sup> Host Base IDS

<sup>3</sup> Network Base IDS

<sup>4</sup> Protocol Analysis

<sup>5</sup> Pattern Matching

<sup>6</sup> Hyper Text Transfer Protocol

<sup>7</sup> File Transfer Protocol

<sup>8</sup> 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 می‌شود. 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 دسترسی‌های غیرمجاز در تجارت و سیاست و مسائل نظامی وجود داشته، رمزنگاری است. به‌طور مثال تلاش برای ارسال یک پیام سری میان دو هم‌پیمان به گونه‌ای که حتی اگر از سوی دشمن دریافت شود قابل درک نباشد، در رم‌قدیم نیز دیده شده است. در سال‌های 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 ماهواره‌ها شناخته می‌شود. پیشرفت علم رمزنگاری موجب به وجود آمدن روش‌های تحلیل مختلفی شده است به گونه‌ای که به‌طور متناوب شبکه‌های رمز مختلف شکسته شده‌اند. 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 رمز شده، عمل تطبیق الگو با مشخصه‌های حملات را انجام دهند. در حالی که پروتکل‌های زیادی مانند WEP<sup>1</sup>، IPsec<sup>2</sup>، SSL<sup>3</sup> و SSH<sup>4</sup> وجود دارند که جهت ایجاد راهی برای

---

Wired Equivalent Privacy<sup>1</sup>  
IP Security<sup>2</sup>  
Secure Sockets Layer<sup>3</sup>  
Secure Shell<sup>4</sup>

اطمینان از ارتباطات امن بر روی بسترهای ناامنی همچون اینترنت، پیشنهاد شده‌اند و با رمز کردن ترافیک این پروتکل‌ها، امکان تصدیق هویت سرویس‌گیرنده<sup>۱</sup> و سرور<sup>۲</sup> 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 پیگیربندی 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 بعداً پشتیبانی از برقراری امنیت هر نوع نرم‌افزار کاربردی<sup>۳</sup> شبکه که به صورت سرویس‌گیرنده / سرور و بر مبنای TCP<sup>۴</sup> مانند http، ftp و انواع پایگاه داده کار می‌کنند، با روشی که به اصطلاح Port Forwarding نامیده می‌شود، اضافه شد. استفاده از روش

---

Client<sup>1</sup>  
Server<sup>2</sup>  
Application<sup>3</sup>  
Transfer Control Protocol<sup>4</sup>

Port Forwarding جهت برقراری امنیت نرم افزارهای کاربردی در سطح لایه کاربرد مدل OSI<sup>1</sup> هر روز بیشتر شده، در حالی که تشخیص حملاتی که از این طریق رمز می‌شوند، بدون امانت گرفتن کلید اختصاصی توسط سیستم‌های تشخیص نفوذ مرسوم، قابل تشخیص نیست. روش پیشنهادی بدون رمزگشایی<sup>2</sup> به تحلیل ترافیک رمز شده می‌پردازد. سیستم پیشنهادی با استفاده از مجموعه داده<sup>3</sup> ارزیابی DARPA [3]، آزمایش می‌شود.

## ۲-۱. تعریف موضوع، اهداف و فرضیه‌ها

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

هدف دوم ارزیابی روش پیشنهادی با استفاده از مجموعه داده ارزیابی DARPA می‌باشد. میزان نرخ خطای<sup>4</sup> 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 سرویس‌دهنده‌های وب، ftp و پایگاه داده، رفتارهای عادی را از رفتارهای غیرعادی تشخیص داده و ترافیک حملات را شناسایی شود.

انتظار داریم سیستم پیشنهادی بتواند حملات رمز شده با پروتکل SSH به

---

Open Systems Interconnect<sup>1</sup>

Decryption<sup>2</sup>

Dataset<sup>3</sup>

Error Rate<sup>4</sup>