پردیس بین الملل دانشگاه گیلان

پایان نامه کارشناسی ارشد

شناسایی و مقابله با حملات درون سازمانی در پایگاه های داده ای رابطه ای

پایان‌نامه یا رساله برای دریافت درجه کارشناسی ارشد

در رشته مهندسی فناوری اطلاعات

نام دانشجو : سید هاشم میربهاری

استاد راهنما :

دکتر رضا ابراهیمی آتانی

تابستان ۱۳۹۱

پردیس بین الملل دانشگاه گیلان

پایان نامه کارشناسی ارشد

شناسایی و مقابله با حملات درون سازمانی در پایگاه های داده ای رابطه ای

پایان‌نامه یا رساله برای دریافت درجه کارشناسی ارشد

در رشته مهندسی فناوری اطلاعات

نام دانشجو : سید هاشم میربهاری

استاد راهنما :

دکتر رضا ابراهیمی آتانی

تابستان ۱۳۹۱

به نام خدای مهربان

تقدیم به تمام اساتید گروه کامپیوتر دانشگاه گیلان

و

همسرم و یگانه فرزند دلبندم سید هومن

چکیده

با توجه به گسترش استفاده از کامپیوتر به خصوص کامپیوتر های متصل به شب ــکه موضوع امنیت آنها پیش می آید، این امنیت در نگاه اول توسط افراد غیر مجاز و افراد خارج از شبکه در خطر حملات شبکه می باشد، ولی در نگاه دقیق تر حملاتی نیز توسط افراد داخل شبکه که توانایی استفاده از شبکه را دارند وجود دارد این افراد با در اختیار داشتن یوزر و پسورد لازم وارد شبکه شد ه و به صورت سوء استفاده از اعتماد مدیر شبکه به آن آسیب می رسانند، تهدید آنها به لحاظ دانستن نکات اساسی شبکه و فایل های مهم خطرات بیشتری نسبت به حملات خارجی محسوب می گردد . در این پایان نامه حملات این چنینی که تحت عنوان حملات داخلی مطرح است مد نظر می باشد، حملات داخلی که در این پایان نامه آمده است حملات داخلی به بانک اطلاعاتی را مد نظر قرار داده است، شیوه این تشخیص نفوذ با روش داده کاوی می باشد، در تشخیص نفوذ سعی گردیده، سه شیوه شبکه عصبی و بیض و درختی مورد تحلیل قرارگرفته و سپس با هم مقایسه گردند .

واژه کلیدی : حملات شبکه، حملات داخلی، تشخیص نفوذ، داده کاوی، کلمنتاین، تشخیص نفوذ در پایگاه اطلاعاتی

سپاسگزاری:

- تشکر ویژه از استاد فرزانه جناب دکتر رضا ابراهیمی آتانی که به حق در زمینه امنیت شبکه و تشخیص نفوذ به اینجانب اطلاعات بسیاری ارائه کردند و در این پایان نامه استاد راهنمایی اینجانب بودند
- از آقای دکتر شاه بهرامی مدیر گروه محترم که ارتقاء سطح علمی و گسترش دانش گروه مدیون زحمات ایشان می باشد تشکر می نمایم .
- از آقایان دکتر مهدوی و دکتر مرادی و خانم دکتر نیارکی اساتید محترم دانشگاه گیلان.
- از آقای مهندس قربانی در مرکز تحقیقات مخابرات در شاخه امنیت شبکه و ارتباطات
- از خانم مهندس قانع که در زمینه حملات داخلی مطالب ارزشمندی به اینجانب ارائه داشتند.
- کتابخانه دانشگاه گیلان.
- کتابخانه مرکز تحقیقات مخابرات کشور.
- بعضی دیگر از اساتید که از ذکر نامشان به علت زمینه های فعالیت امنیتی در مرکز تحقیقات مخابرات معذورهستم.
- و در نهایت از تمام همکلاسی های فعال و محقق خوبم تشکر و قدر دانی‌می نمایم.

فهرست مطالب :

فهرست شکل ها :

فهرست جداول :

مقدمه

کامپیوتر در قرن گذشته به وجود آمده و در اواخر دهه قبل به تکامل نسبی خود رسید، تکامل آن بیشتر در دو موضوع حافظه و سرعت پردازش خلاصه شده بود. تا اینکه در دهه ۹۰ میلادی موضوع اینترنت به موضوع کاملاً جدی و حیاتی تبدیل شد و علم کامپیوتر به دلیل ارتقاء کیفیت فناوری، تکامل اینترنت را در افزایش سرعت اینترنت دید.

دانشمندان و مهندسین علوم کامپیوتر با کوچک کردن ابعاد سلول حافظه به مرز های ملکول ها رسیده و به موفقیت های بسیاری دست یافته اند، طوری که دیگر داشتن حافظه های گیگا و ترا در اندازه های قابل حمل عجیب نبوده و در حوضه ریز پردازنده نیز، با ساخت پردازنده های موازی و چند هسته ای به این شاخه از چالش علوم کامپیوتر پاسخ داده اند. برای دست یابی به سرعت های عالی در دسترسی به اینترنت به فناوری های فیبر نوری و مخابرات ماهواره پناه آوردند و البته فیبر نوری در این حوزه کمک های شایانی به سرعت های بالا نموده است.

با افزایش سرعت اینترنت دانشمندان حافظه ها و پردازنده های ابری را مطرح کردند، هم اکنون داشتن حافظه های رایگان ابری در سایت ها به موضوع عادی تبدیل گردیده و این به لطف سرعت بالای اینترنت‌است.

ایجاد فضای ابری باعث گردید پیش از پیش منابع سخت افزاری در اشتراک عموم باشد و این آغاز چالش امنیت اطلاعات بود، زیرا دیگر افراد با نیت های مختلف از جمله کنجکاوی، سوء استفاده، انتقام و ... شروع به حمله به منابع سخت افزاری و از همه مهمتر منابع اطلاعاتی نمودند

در مقابل مهندسین شاخه ی امنیت با ایجاد لایه های امنیتی از کامپیوتر ها محافظت نمودند و این داستان بین دزد و پلیس شروع شد و هر کدام مسلط تر باشد موفق تر خواهد بود. از این رو همین اتفاق حتی شاخه های سایبری در حوزه های امنیتی کشور ها را ایجاد نمود تا اگر به منابع اطلاعات سیاسی بخواهند حمله کنند کسانی در این حوضه نیز باشند تا جلوی آنها را بگیرند . از نمونه حملات سیاسی در فضای اینترنت حمله به تجهیزات سخت افزاری برنامه پذیر انرژی اتمی ایران تحت عنوان استاکس نت بود که توسط رژیم اسرائیل

تولید و در شبکه کار گذاری شده بود، این ویروس توانست باعث تاخیر در بهره برداری از تاسیسات ان رژی هسته ای ایران گردد ولی در بحث تخریب موفقیتی نداشت.

اصولا مهندسین کامپیوتر در گرایش های امنیتی به پنج لایه امنیتی اعتقاد دارند تا شبکه و منابع آن را محافظت نماید، اولین ابزار و لایه امنیتی استفاده از دیوار آتش است. این ابزار در اجازه دادن به ورود بسته های اطلاعاتی بسیار با احتیاط عمل می کند، مگر اینکه این اطلاعات پاسخ هایی به در خواست افراد داخل شبکه باشند یا به اصطلاح آن پورت را باز نگه دارند، ولی خروج اطلاعات در شبکه با حساسیت خیلی کمتری انجام می گیرد، می توان این خاصیت را به سگ نگهبانی فرض کرد که افراد وارد شونده را با مقاومت زیاد ممانعت می کند مگر صاحبش اجازه دهد ولی کسانی که از منزل خارج می شوند را با حساسیت بسیار کمی بررسی می کند، پس مشکل در شبکه با ورود است نه با خروج، و این بدان معنی است که تنها نیاز است به طریقی به شبکه وارد شویم .

آنتی ویروس، این برنامه هم بسیار در امنیت و افزایش امنیت موفق است و برایش مهم نیست که جریان اطلاعات از بیرون یا از داخل شبکه است، هر کس از حافظه استفاده کند عملکردش بررسی خواهد شد، که آیا فایل ها را تخریب می کند یا خیر، آیا از خود کپی می سازد یا خیر، آیا پایگاه داده را به صورت مبهمی بروز رسانی می کند و این قبیل کار ها . از جمله مشکلات برنامه ها این است که معمولا به برنامه های مفید متصل می گردند و باعث اشغال فضای حافظه و کاهش قدرت پردازش می شوند. این برنامه مانند ناظم یک مدرسه است که مواظب است کسی نمرات را دستکاری نکند ، زنگ مدرسه بی نظم زده نشود ، پرونده ها دزدیده و یا پاره نشود و حتی بی دلیل مدرسه تعطیل نگردد.

کشف نفوذ، جایگاه این برنامه در بالا خالی بود ، برنامه ای است که مانند حراست مدرسه عمل می کند و به هیچ کس اعتماد ندارد، مدیر مدرسه هم اگر بخواهد نمرات را بررسی کند فوری حساس شده و عملکرد او بررسی می شود و با رفتار های روزهای قبل او مقایسه خواهد شد، چرا که امکان دارد افرادی در بیرون از مدرسه او را تهدید کنند و ایشان به راحتی می تواند نمرات را تغییر دهد . نه دیوار آتش و نه آنتی ویروس می تواند از عملکرد مدیر باخبر شود، فقط کشف نفوذ است که می تواند رفتار های مشکوک را شناسایی و به مدیر شبکه اعلام کند، با یک مثال عملی از شبکه موضوع را شرح می دهیم، فرض کنید فردی به نام A معمولا

روزی دو بار لاگین می کرد ولی امروز ۳۰ بار لاگین کرده، یا اینکه ایشان یک فرد کم سواد کامپیوتری بود ولی امروز از دستورات بسیار پیشرفته لینوکس برای پویش پورت استفاده می کند، ببینید این حرکات همه مشکوک است و دیوار آتش و آنتی ویروس در تشخیص آن ناتوان هستند.

موضوع بعد برنامه های کاربر دی و کنترل آن ها ازجمله موضوعات مهم د ر شاخه‌ی امنیت می باشد که در حقیقت مسئول کنترل نصب برنامه های افراد داخل شبکه می باشد، چرا که هر برنامه جالب و وسوسه کننده به لحاظ سرگرمی می تواند در درون خود غولی از برنامه مخرب را داشته باشد که در لایه های مختلف شبکه عملیات ه‌ای مخربی را انجام دهد و حتی گاهی صدمه ای به منابع نمی رساند بلکه با ارسال محتوای تایپ های یک کاربر به بیرون از شبکه امنیت اطلاعاتی شبکه را بسیار کاهش خواهد داد. نمونه ای از این قبیل اتفاقات در تبت در گروه دالایلاما پیش آمدکه کاربران آنها از کندی کامپیوترشان گلایه می کردند تا این که وق تی پیشوایشان به اروپا سفر کرده بود موضوع را مطرح می کند و بعد از بررسی های به عمل آمد، نتیجه این شد که دولت چین برنامه ای آلوده جاسوسی را به طریق غیر مستقیم در اختیار آنان قرار داده بود که تمام مکاتبات و عملکرد ها را به دولت چین گزارش می نمود

در نهایت موضوع بعد در امنیت شبکه، موضوع مهندسی اجتماعی است که در واقع نحوء راز داری و جلوگیری از تخلیه اطلاعاتی را آموزش می دهد، در این علم روشهای مختلف برای تحریک افراد داخل سازمان به منظور گرفتن اطلاعات را بررسی می کنند، نحوه پسورد گذاری، طبقه بندی اطلاعات، استفاده از اینترنت و همچنین نحوء ارتباط با ارباب رجوع بررسی می شود، زیرا در صورتی که تمام مراحل نرم افزاری در تهیه امنیت فراهم شود ولی فرد کاربر بی جهت به رقبان اعتماد کند تمام نقشه ها به هم می خورد.

پس امنیت در شبکه ها و کامپیوتر های که به تنهایی به اینترنت مت‌صل می شوند حیاطی است، و در این پایان نامه به بخش کشف نفوذ آن متمرکز شده ایم و راه کاری برای آن به روش داده کاوی ارائه نموده ایم

فصل اول

فصل اول

۱ ـ۱ داده کاوی

این علم یکی از علوم جدید کام‌پیوتر است که در حال ارتقاء می باشد، با یک مثال شروع می کنیم: فرض کنید ما تمام افراد کشورمان را در یک فیلد ذخیره کنیم، این فیلد نام افراد باشد، فیلد دیگری خواهیم ساخت از محل زندگی آنها، فیلد سوم از اندازه قد تشکیل یافته است، و درنهایت فیلد چهارم پاسخ این سوال است که آیا شنا می دانند یا خیر، حال اگر ما عملیات داده کاوی را برای این افراد انجام دهیم باید ابتدا توجه کنیم نام فرد اثری در داده کاوی برای کشف دانش، مربوط به چرا شنا می دانند، نخواهد داشت. یعنی می دانیم که نام حسن یا نقی بودن دلیل بر دانستن شنا نخواه د شد پس این فیلد را پردازش نخواهیم کرد ، همچنین قد نیز نباید جز ء پردازش قرار گیرد چون تأثیری در مهارت شنا ندارد. پس دو فیلد مانده است، شهر و پاسخ سوال.

فیلد ضروری	فیلد غیر ضروری	فیلد ضروری	فیلد غیر ضروری
شنا می دانندیا خیر	قد	شهر	نام
خیر	۱۸۵	اراک	حسن
بله	۱۷۰	تهران	رضا
خیر	۱۷۵	یزد	محمود
بله	۱۸۰	انزلی	اکبر
خیر	۱۷۷	دهلی	مسعود
بله	۱۷۳	بندر عباس	جبار

نویز

جدول ۱: جدول داده ها برای کشف دانش جهت ارتباط شهر با دانستن شنا

در نام شهر ، دهلی آمده است این داده می تواند نویز محسوب گردد و باید برای آن تصمیم گرفته شود، آیا حذف شود یا تصحیح گردد، در کل به مجموعه این گونه عملیات در داده کاوی پیش پردازش و آماده سازی داده می گویند که همه باید توسط یک فرد آگاه تصمیم گیری شود چون در غیر اینصورت ، احتمال ایجاد نتایج عجیب و غیر قابل قبول وجود دارد.

حال باید این اطلاعات را داده کاوی نمود و بعد از این عملیات مشاهده می‌کنیم که افراد ساحل نشین معمولا در شنا مهارت دارند، پس داده کاوی یعنی کشف یک دانشی از انبوه اطلاعات موجود که در این جا دانش عبارت بود از اینکه ساحل نشین ها معمولا شنا می دانند، در حالی که این موضوع در جدول ها آشکار نبود.

۱ ۲ امنیت

امنیت یعنی حفاظت از چیزی که برای ما اهمیت دارد، چه در مقابل حملات عمدی و چه حملات غیر عمدی

۱ ۲ ۱ اقدامات امنیتی یا مثلث امنیت

- پیشگیری و جلو گیری از خسارت
- ردیابی، تشخیص میزان خسارت و هویت دشمن، کیفیت حمله (زمان، مکان، دلایل حمله ،نقاط ضعف)
- واکنش، بازیابی و جبران خسارت، جلوگیری از حملات مجدد

نگهداری اطلاعات در قفسه قفل دار	نگهداری اطلاعات در کامپیوترها
نگهدری قفسه در مکانهای امن	برقراری ارتباط شبکه ای بین کامپیوترها
استفاده از نگهبان	برقراری امنیت در کامپیوتر ها و شبکه ها
استفاده از سیستم های حفاظتی الکترونیکی	

جدول ۲ :تفاوت امنیت در شکل سنتی و شکل نوین

۱ ۳ حملات

حمله تلاش عمدی برای رخنه در یک سیستم یا سوء استفاده از آن است ، حمله نقطه مقابل امنیت می باشد، شکل حملات دارای انواع روش ها و الگو های مختلفی دارد که توسط افراد زیرکی اجرا می گردد، حملات سناریوی یک حمله است که باید برای جلوگیری از آن دانش‌و تجربه لازم را داشت.

رخنه : نقض سیاست های (باید ها و نباید ها) امنیتی یک سیستم و نفوذ.

انواع حمله از نظر مکان جغرافیایی و یا از نظر بودن در لیست افراد مجاز و غیر مجاز به دو گروه تقسیم می گردد: حملات داخلی و حملات خارجی

۱ ۳ ۱ **حملات داخلی** : حملاتی هستند که حمله کننده به Password , Username سیستم دسترسی دارد و این حمله به دو گروه تقسیم می گردد کاربرانی که Password , Username را بدست آورده اند و دوم کاربرانی که Password , Username مربوط به آنها است و از آن سوء استفاده می‌کنند.

۱ ۳ ۲ حملات خارجی : حملاتی هستند که هدف آنها گاهی Password , Username نمی باشد و به آن نیاز ندارد و به سیستم از طریق دیگری واردمی شوند و یا حتی آسیب می رسانند.

۱ ٤ حملات فعال و غیر فعال

در تقسیم بندی دیگری حملات به روش زیر و به دو گروه‌اکتیو و پسیو تقسیم می گردد:

- غیر فعال Passive
  - نوع شبکه Network
    - شنود کابلی یا Wiretapping
    - اسکن و پویش پورت Port scanner
    - اسکن بیکار و آرام Idle scan
- فعال Active
  - حمله محدود کردن سرویس Denial-of-service attack
  - حقه بازی Spoofing
  - شبکه Network
    - مرد میانی یا باز پخش کننده اطلاعات Man in the middle