



پردیس بین الملل دانشگاه گیلان
پایان نامه کارشناسی ارشد

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

پایان نامه یا رساله برای دریافت درجه کارشناسی ارشد
در رشته مهندسی فناوری اطلاعات

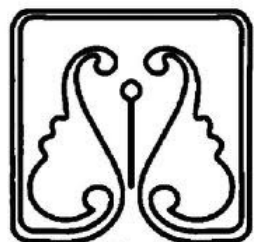
نام دانشجو : سید هاشم میربهراری

استاد راهنما :

دکتر رضا ابراهیمی آتانی

تابستان ۱۳۹۱





دانشگاه گیلان

پردیس بین الملل دانشگاه گیلان

پایان نامه کارشناسی ارشد

شناسایی و مقابله با حملات درون سازمانی در پایگاه های

داده ای رابطه ای

پایان نامه یا رساله برای دریافت درجه کارشناسی ارشد

در رشته مهندسی فناوری اطلاعات

نام دانشجو: سید هاشم میربهراری

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 – که 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 شده 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 چینی 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 قرار گرفته و سپس با هم مقایسه کردند .

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 معذور هستم.
- و در نهایت از تمام همکلاسی های فعال و محقق خوبم تشکر و قدر دانی می نمایم.

فهرست مطالب :

.....ج.....	تقدم
.....د.....	چکیده
.....ه.....	سپاسگزاری
.....و.....	فهرست مطالب
.....ی.....	فهرست شکل ها
.....ل.....	فهرست جداول
.....م.....	مقدمه
.....ن.....	فصل اول
.....س.....	۱-۱ داده کاوی
.....ش.....	۲-۱ امریت
.....ط.....	۱-۲-۱ اقدامات امریتی می مثلث امریت
.....ظ.....	۳-۱ حملات
.....ح.....	۱-۳-۱ حملات داخلی
.....ط.....	۴-۱ حملات فعال و غی فعال ۴
.....ق.....	۱-۴-۱ حمله فیشینگ Phishing
.....ک.....	۱-۴-۲ حملات DOS می Denial Of Service
.....گ.....	۳-۴-۱ حملات تزریق در SQL
.....خ.....	۱-۴-۴ حملات Spoofing می حقه بازی
.....د.....	۵-۱ تشخیص نفوذ.

.....	۱۵	۱-۵-۱ شرح روش تشخیص رفتار غی عادی
.....	۱۵	۲-۵-۱ روش تشخیص مبتدی بر امضاء
.....	۱۵	۱-۵-۳ معماری‌های مختلف سامانه تشخیص نفوذ
.....	۱۶	۴-۵-۱ سامانه تشخیص نفوذ مبتدی بر شبکه (NIDS)
.....	۱۷	۵-۵-۱ سامانه تشخیص نفوذ توزیع شده (DIDS)
.....	۱۹	فصل دوم
.....	۱۹	۱-۲ سرویس های امریجی
.....	۲۲	۲-۲ روش های حمله متداول در شبکه
.....	۲۳	۳-۲ روش های کنترل برای افزایش امریجی
.....	۲۳	۱-۳-۲ روش رمز گذاری
.....	۲۴	۲-۳-۲ کنترل نرم افزاری
.....	۲۴	۳-۳-۲ کنترل های سخت افزاری
.....	۲۴	۴-۳-۲ سرپست های امریجی
.....	۲۶	۵-۳-۲ استفاده از شمارنده ها
.....	۲۶	۶-۳-۲ مهر زمانی
.....	۲۷	۶-۳-۲ ثبت هر گونه دسترسی به سرپست
.....	۲۷	۷-۳-۲ دیواره آتش
.....	۲۸	۴-۲ عوامل جلوگیری از ایجاد یک سرپست امن ی شبکه امن
.....	۲۹	۵-۲ اهداف امریجی
.....	۳۲	فصل سوم
.....	۳۲	۱-۳ نفوذ و روش های تشخیص نفوذ با تکی بر حملات داخلی
.....	۳۲	۱-۳-۱ کامپیتر بر عالی کامپیتر
.....	۳۳	۲-۱-۳ انواع نفوذگران

..... ۳۴	۳-۱-۳ امنیت شبکه های کامپیوتر
..... ۳۶	۳-۲ نفوذ در حملات داخلی
..... ۳۷	۳-۲-۱ تشخیص نفوذ در رفتار غی عادی
..... ۳۷	۳-۲-۲ تعریف برخی تکنیک ها در تشخیص رفتار غی عادی
..... ۳۷	۳-۲-۳ معطر آماری
..... ۳۸	۳-۳ تهدیدات در بانک های اطلاعاتی
..... ۴۰	۴-۳ تعریف تشخیص حملات اشتباه و کلا عدم تشخیص
..... ۴۲	فصل چهارم
..... ۴۳	۴-۱ داده کاوی و تشخیص نفوذ
..... ۴۴	۴-۱-۱ تشخیص بر اساس رصد های غی متعارف
..... ۴۵	۴-۱-۲ داده کاوی در تشخیص نفوذ حملات
..... ۴۵	۴-۱-۳ داده کاوی برای تشخیص نفوذ شبکه
..... ۴۷	۴-۱-۴ استخراج الگو مکرر برای برنامه های مبتنی بر امضاء
..... ۴۷	۴-۱-۵ شیوه تشخیص با الگوریتم Apriori
..... ۴۷	۴-۱-۶ شیوه داده کاوی بر اساس تجزیه و تحلی الگوی متوالی
..... ۴۸	۴-۱-۷ شیوه دسته بندی در کشف نفوذ
..... ۴۹	۴-۱-۸ کشف نفوذ به روش رده بندی
..... ۵۰	۴-۱-۹ کشف نفوذ به روش شبکه های عصبی (داده کاوی عصبی)
..... ۵۰	۴-۱-۱۰ کشف نفوذ برای داده کاوی با الگوریتم خوشه بندی
..... ۵۱	۴-۲ تحلی رویداد های استریم برای تشخیص نفوذ
..... ۵۱	۴-۲-۱ تشخیص آنومالی
..... ۵۲	۴-۲-۲ تحلی و کاوش حسابرسی داده ها
..... ۵۳	۴-۳ نرم افزار SNORT

فصل پنجم

.....۵۶.....

۱-۵ شرح جدول نشست در چندین سناریوی حملات بی‌رفتار عادی

.....۵۶.....

۲-۵ شرح محیط نرم افزار کلمنتاین در داده کاوی اطلاعات حمله

.....۵۷.....

۳-۵ داده کاوی از جدول نشست به روش درختی C۵

.....۵۹.....

۴-۵ داده کاوی از جدول نشست به روش شبکه عصبی

.....۶۱.....

۵-۵ داد کاوی از جدول نشست به روش بقی

.....۶۳.....

۶-۵ مقایسه سه الگوی داده کاوی از نشست های مختلف

.....۶۴.....

نتیجه گیری

.....۶۷.....

مراجع

.....۶۸.....

پیشنهاد ادامه کار

.....۷۰.....

فهرست شکل ها :

..... ۷	شکل ۱: حمله smurf
..... ۸	شکل ۲: حمله Fraggle
..... ۸	شکل ۳: حمله Ping Flood
..... ۹	شکل ۴: حمله SYN Flood
..... ۹	شکل ۵: حمله Land
..... ۱۰	شکل ۶: حمله Teardrop
..... ۱۱	شکل ۷: Bonk
..... ۱۲	شکل ۸: یک صفحه احراز اصالت
..... ۱۶	شکل ۹: تشخیص نفوذ مبتدی بر مبنای (حفاظت از خود)
..... ۱۷	شکل ۱۰: تشخیص نفوذ مبتدی بر شبکه
..... ۱۷	شکل ۱۱: تشخیص نفوذ مبتدی مبتدیان IDS ها
..... ۲۱	شکل ۱۲: مراحل امضای دیجیتال
..... ۲۲	شکل ۱۳: وقفه در اطلاعات
..... ۲۳	شکل ۱۴: دستکاری اطلاعات
..... ۲۳	شکل ۱۵: استراق سمع
..... ۲۳	شکل ۱۶: جعل در اطلاعات
..... ۲۵	شکل ۱۷: اهمیت برای بخشی از منابع
..... ۲۵	شکل ۱۸: اهمیت برای تمام منابع
..... ۲۶	شکل ۱۹: اهمیت بخش از حد و برای منابع بعدی
..... ۲۷	شکل ۲۰: دیوار آتش
..... ۲۹	شکل ۲۱: مراحل اجرای امن سازی یک سرور
..... ۴۴	شکل ۲۲: نمایش فشار کار CPU در قبل و بعد از نفوذ
..... ۴۵	شکل ۲۳: روال داده کاوی در کشف دانش
..... ۴۶	شکل ۲۴: جریان حرکت داده در داده کاوی از داده خام تا نمایش نتیجه
..... ۴۸	شکل ۲۵: روش اول راستنایج نفوذ در پایگاه داده در دوره های نشست کاربر

..... ۴۸	شکل ۲۶: روش دوم استنتاج نفوذ در پایگاه داده در دوره های نشست کاربر [۱۳]
..... ۴۹	شکل ۲۷: در این شکل به زیبایی دو مرحله ای بودن عملیات داده کاوی را نشان می دهد، مرحله اول کشف منطق ی دانش و مرحله بعد تست میباشد [۱۳]
..... ۵۰	شکل ۲۸: خوشه بندی برای انواع تهدید
..... ۵۱	شکل ۲۹: تکامل شریه خوشه بندی را نشان می دهد
..... ۵۲	شکل ۳۰: داده کاوی و تکمیل پرو فای رفتار کاربر
..... ۵۳	شکل ۳۱: کشف رابطه یک اتفاق با اتفاق بعدی به روش داده کاوی
..... ۵۳	شکل ۳۲: شرح نرم افزار snort در تشخیص رفتار غی نرمال
..... ۵۴	شکل ۳۳: چرخه تکامل تشخیص رفتار غی نرمال
..... ۵۷	شکل ۳۴: محیط برنامه کلمنتاین
..... ۵۸	شکل ۳۵: تجمیع و نمایش داده ها
..... ۵۸	شکل ۳۶: داده ها قبل و بعد از جمع شدن
..... ۶۰	شکل ۳۷: تحلی داده کاوی برای تشخیص نفوذ با الگوی سری فای
..... ۶۱	شکل ۳۸: نتایج تحلی داده کاوی برای تشخیص نفوذ با الگوی سری فای
..... ۶۱	شکل ۳۹: حاصل تحلی نمودار درختی که منطقی برای تشخیص رفتار کاربر میباشد
..... ۶۲	شکل ۴۰: تحلی شبکه عصی در داده کاوی برای تشخیص حمله داخلی
..... ۶۲	شکل ۴۱: تحلی با شبکه عصی اعتقاد به مهم بودن گزینه Select دارد و بعد ارزش READ را بالا می داند
..... ۶۳	شکل ۴۲: نتایج تحلی شبکه عصی
..... ۶۳	شکل ۴۳: تحلی با الگوی بعض برای پیدا کردن الگوی نفوذ داخلی
..... ۶۴	شکل ۴۴: نتایج تحلی بعض Write را مهمترین موضوع دانسته است
..... ۶۴	شکل ۴۵: نتایج نشان می دهد الگوی بعض در کشف منطق نفوذ در ۸۴ درصد موفق بوده است
..... ۶۵	شکل ۴۶: نمودار موفقیت سه روش داده کاوی در تشخیص الگوی حمله
..... ۶۶	شکل ۴۷: نمایش میزان موفقیت بعض گویی

فهرست جداول :

فهرست جداول		
۲۰	جدول داده ها برای کشف دانش جهت ارتباط شهر با دانستن شنا	جدول ۱
۲۱	تفاوت امنیت در شکل سنتی و شکل نوین	جدول ۲
۵۷	انواع حملات به پایگاه داده و تحلیل نوع حمله	جدول ۳
۷۷	انواع رفتار یک کاربر در پایگاه داده	جدول ۴
۸۴	تجمیع نتایج سه روش داده کاوی	جدول ۵

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 مهندسين علوم کامپیوتر با کوچک کردن ابعاد سلول حافظه به مرزهای ملکولها رسیده و به موفقیت‌های بسیاری دست یافته‌اند، طوری که دیگر داشتن حافظه‌های گیگا و ترا در اندازه‌های قابل حمل عجیب نبوده و در حوضه ریز پردازنده نیز، با ساخت پردازنده‌های موازی و چند هسته‌ای به این شاخه از چالش علوم کامپیوتر پاسخ داده‌اند. برای دست‌یابی به سرعت‌های عالی در دسترسی به اینترنت به فناوری‌های فیبر نوری و مخابرات ماهواره پناه آوردند و البته فیبر نوری در این حوزه کمک‌های شایانی به سرعت‌های بالا نموده است.

با افزایش سرعت اینترنت دانشمندان حافظه‌ها و پردازنده‌های ابری را مطرح کردند، هم‌اکنون داشتن حافظه‌های رایگان ابری در سایت‌ها به موضوع عادی تبدیل گردیده و این به لطف سرعت بالای اینترنت است.

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

در مقابل مهندسين شاخه‌ی امنیت با ایجاد لایه‌های امنیتی از کامپیوترها محافظت نمودند و این داستان بین دزد و پلیس شروع شد و هر کدام مسلط تر باش نه موفق تر خواه نه بود. از این رو همین اتفاق حتی شاخه‌های سایبری در حوزه‌های امنیتی کشورها 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 سخت‌افزاری برنامه‌پذیر 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 آن 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 درخواست 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 کاربردی و کنترل آن ها از جمله موضوعات مهم در شاخه ای 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 گولی 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 دالایاما پیش آمده که کاربران آنها از کندی کامپیوترشان گلایه می کردند تا این که وقتی 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 عملکردها را به دولت چین گزارش می نمود

در نهایت موضوع بعد در امنیت شبکه، موضوع مهندسی اجتماعی است که در واقع نحوه رازداری 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 نحوه 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 رقیبان اعتماد کند تمام نقشه ها به هم می خورد.

پس امنیت در شبکه ها و کامپیوترهای 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 + 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 در نهایت فیلد چهارم پاسخ این سوال است که آیا شما 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 شما می دانند، نخواهد داشت. یعنی می دانیم که نام حسن یا نقی بودن دلیل بر دانستن شما نخواهد شد پس این فیلد را پردازش نخواهیم کرد، همچنین قد نیز نباید جزء پردازش قرار گیرد چون تأثیری در مهارت شما ندارد. پس دو فیلد مانده است، شهر و پاسخ سوال.

فیلد ضروری	فیلد غیر ضروری	فیلد ضروری	فیلد غیر ضروری
شنا می دانند یا 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

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

در نام شهر، دهلی آمده است این داده می تواند نويز محسوب گردد و بايد براي آن تصميم گرفته شود، آيا حذف شود يا تصحيح گردد، در كل به مجموعه اين گونه عمليات در داده كاوي پيش پردازش و آماده سازي داده مي گويند كه همه بايد توسط يك فرد آگاه تصميم گيري شود چون در غير اينصورت ، احتمال ايجاد نتايج عجيب و غري قابل قبول وجود دارد.

حال بايد اين اطلاعات را داده كاوي نمود و بعد از اين عمليات مشاهده مي كنيم كه افراد ساحل نشين معمولاً در شنا مهارت دارند، پس داده كاوي يعني كشف يك دانشي از انبوه اطلاعات موجود كه در اين جا دانش عبارت بود از اينكه ساحل نشين ها معمولاً شنا مي دانند، در حالي كه اين موضوع در جلول ها آشكار نبود.

۴ ۱ امنیت

امنيت يعني حفاظت از چيزي كه براي ما اهميت دارد، چه در مقابل حملات عمدي و چه حملات غير عمدي

۴ ۱ اقدامات امنيتي يا مثلث امنيت

- پيشگيري و جلو گيري از خسارت
- رد يابي، تشخيص ميزان خسارت و هويت دشمن، كيفيت حمله (زمان، مكان، دلايل حمله، نقاط ضعف)
- واكنش، باز يابي و جبران خسارت، جلو گيري از حملات مجدد

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

جدول ۲: تفاوت امنیت در شکل سنتی و شکل نوین

۴ ۱ 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 دانش و تجربه لازم را داشت.

رنخه : 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

۴ ۱ 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 می کنند.

۴ ۱ ۲ حملات خارجی : حملاتی هستند که هدف آنها گاهی Password , Username نفی باشد و به آن نیاز ندارد و به سیستم از طریق دیگری وارد می شوند و یا حتی آسیب می رسانند.

۴ ۱ حملات فعال و غیر فعال

در تقسیم بندی دیگری حملات به روش زیر و به دو گروه اکتیو 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