تصميم نظام إحصائي لكشف المتطفلين

م.م علي حبيب كشمر
قسم علوم الحاسبات/ كلية العلوم
جامعة بغداد

م.م صلاح طه علاوي
قسم علوم الحاسبات/ كلية العلوم
الجامعة ألمستنصريه

المستخلص:
في هذا البحث تم تصميم نظام حماية بسيط للكشف عن المتطفل الذي يقوم بالدخول غير المشروع للبيانات. تم أعطاء فكرة بسيطة عن المتطفل، وتم استخدام التقنية الإحصائية في تصميم هذا النظام، وبصورة خاصة الوسط الحسابي والانحراف القياسي كطريقة لاكتشاف المتطفلين

Statistical System for Detection of Hackers

Abstract:

In this research we design a simple protection system to detect Hackers, which can used different ways to access data. We have given a simple idea for Hackers, and used statistical technique, particularly, Arithmetic Mean and Standard Deviation, to design intrusion detection system (IDS)

١- المـقدمـة:

البيانات عبارة عن معلومات مسجلة بطريقة معينة وهناك درجات لتصنيف هذه البيانات حسب الأهمية والتي قد تكون حساسة أو ثمينة. الطرق التقليدية البسيطة المتمثلة بتسجيل البيانات على الورق والمحافظة عليها لم تعد ذات جدوى بعد ظهور تقنية المعلومات حيث يتم حفظ المعلومات الأساسية الحساسة والثمينة في وسائل خزن تحت سيطرة الحاسوب والتي يمكن لعدد محدود من المستخدمين الإطلاع عليها والتعامل معها [17] . لا يمكن تحقيق أمنية تامة للمعلومات التي تعالج بواسطة الحاسوب ولكن من الممكن استخدام بعض إجراءات السيطرة الفعالة لتقليل خطر استخدام أو كشف المعلومات بصورة فعالة ومؤثرة [1] . من أهم التهديدات الرئيسية للمعلومات - فقدان أو العبث بالمعلومات نتيجة خطأ غير متعمد- ضياع أو تخريب المعلومات نتيجة خطأ متعمد- معالجة البيانات للحصول على فائدة شخصية - و توقف عمل أجهزة معالجة البيانات. وقد ظهرت أساليب عديدة لحماية البيانات منها التشفير وإخفاء البيانات التي تستخدم لمنع الأشخاص غير المخولين من الوصول إلى البيانات والإطلاع عليها. البيانات المطبوعة بسبب سلامتها وسهولة قراءتها أصبحت هدف رئيسي وواسع اكثر من الهجوم على المكونات المادية أو البرمجيات[18] لذلك نجد أن مفردات البيانات لها قيمة اكبر نسبة إلى المكونات المادية والبرمجيات. لكلا المكونات المادية والبرمجيات عمرا طويلا نسبيا مع التدرج تنازل على مر الزمن في حين قد تكون قيمة البيانات عالية أو تكون لفترة وجيزة خلافا للمكونات المادية والبرمجيات[16]. أن دراسة حماية البيانات تبرز قاعدة حمايتها لغاية فقدان قيمتها [18] . ينص هذا المبدأ من الممكن حماية البيانات ذات العمر القصير عن طريق إجراءات أمنية فعالة فقط في ذلك العمر القصير. التطور السريع في علم الاتصالات جعل من السهولة تعرض بنية الحاسوب إلى تهديدات عديدة سواء الأجهزة المادية أو البرمجيات وهذه تسبب صعوبة الحصول على البيانات ويمكن أدراج قائمة طويلة بما يمكن إن يسببه الإنسان من تهديدات. البرمجيات قد تواجه تهديدات تكون اخطر وتدخل ضمن اهتمام الكثير من المخترقين لأنة يتعامل مع برامج وإمكانية تعرض البرامج بسهولة إلى الحذف أو التحديث والتي يمكن من خلالها إحداث الضرر أو تغير وظيفة من خلال أحصنة طروادة أو البوابات السرية أو البرامج تسرب البيانات التي تسمح بالوصول إلى البيانات من قبل مصدر غير مخول سواء كان شخص أو برامج. يمكن إن تتعرض البيانات إلى تهديدات عديدة منها الإعاقة والتي تجعل الأجهزة غير قادرة على العمل أو يصعب استخدامها أو فشل في نظام التشغيل. والمقطعة وفيها يكون الدخول غير المشروع على الأجهزة من قبل شخص او نظام وقيامة باستنساخ البيانات أو البرامج. والتحوير وهي الدخول إلى الأنظمة والبيانات وأجراء التحوير على البيانات أو عمل البرامج بما يلحق الضرر في قاعدة البيانات

أو ملف المعلومات وأخيرا الاختلاق وهو خلق حالة غير طبيعية على البيانات أو البرامج مثل إضافة بيانات أو قيود جديدة أو أجراء تغيير في عمل البرامج يجعله يؤدي وظيفة غير مرغوب فيها دون علم المستخدم. حماية البيانات تشمل الحفاظ على الأجهزة والبرامج والمعلومات من الضياع أو التلف ومن أخطاء المستخدمين (المتعمدة والعفوية) والكوارث الطبيعية وأخطاء الأجهزة و البرمجيات بالإضافة إلى ذلك تشمل حماية البيانات من محاولات إيقاع الضرر أو العطل الذي يمكن أن يحصل نتيجة لعدم وضوح الإجراءات الأمنية اللازمة لحمايتها ومحاولة منع حدوث سرقتها ولكن في حالة الفشل في ذلك من المهم معرفة الثغرات التي حصل فيها ذلك لمنع حدوثها مستقبلا [18] ونستطيع تقسيم حماية المعلومات إلى عدة مستويات،المستوى الأول يشمل الحماية الفيزيائية، والمستوى الثاني يمثل كلمات السر أو البطاقات الشخصية والبصمات الوراثية وتمييز الصوت والعين،والمستوى الثالث هو تشفير وإخفاء البيانات فعند عبور المتطفل المستويين الأول والثاني والوصول إلى البيانات سوف يجدها إما مشفرة لا يستطيع الاستفادة منها إلا بعد فك شفرتها والتي قد تستغرق وقت طويل، أو مخفية لا يستطيع الوصول إليها إلا بعد معرفة طريقة إخفاءها.

٢ـ الاختراقات

الاختراق: هو محاولة التسلل عبر الشبكات والتحكم بها اعتمادا على أساليب غير قانونية وهو على نوعين حسب الأضرار المتسبب بها التطفلي، يحصل المخترق في هذا النوع على الفائدة مع الإضرار بالمستخدم الأصلي، والتعايشي يستفيد المخترق دون الإضرار بالمستخدم الأصلي [2] . أسباب التعرض للاختراق كثيرة ومتنوعة منها قلة الوعي في السيطرة على الأجهزة وعدم وجود اثر لمعرفة الشخص او الجهة التي قامت بالاختراق وكذلك عدم وجود مسؤولية خاصة للإشراف والسيطرة واستخدام برامج غير موثوق بها. توجد عدة أهداف قد تدفع جهة معينة أو شخص لاختراق الحاسبات الشخصية والشبكات للحصول على المعلومات منها أسباب سياسية أو اقتصادية أو بدافع الانتقام او ذات طبيعة تخريبية. أن سهولة استخدام الانترنيت واستخدام البرامج الحديثة والتطورات التكنولوجية لتسهيل الاستنساخ والأسعار المرتفعة للبرمجيات كلها عوامل مساعدة في انتشار القرصنة[4] [2] . تتبع الدول المتقدمة استراتيجيات مختلفة للحد من القرصنة منها الحظر التجاري واتخاذ الإجراءات القانونية لحماية (الملكية الفكرية) وحماية الاستنساخ وانتشار مجلات تكنولوجيا المعلومات وكذلك استخدام وسائل حديثة ومغرية لجذب المستخدم إلى شراء النسخ الأصلية. يتبع المخترقين أساليب عديدة في عملية الدخول واختراق الشبكات وتختلف هذه الأساليب من موقع إلى أخر بناءا على نوع نظام التشغيل المستخدم [7] منها الدخول بهوية مخفية غير

منفذ بروتوكول FTP حيث يتمكن المخترق من الحصول على كلمة السر الخاصة بالحاسبة الشخصية أو الشبكة ويعمل على فك الشفرة باستخدام عدة طرق منها brute force, jack the ripper, creakier luck, john the ripper . أو باستخدام بروتوكول telnet وكذلك استغلال الثغرات الأمنية في الشبكات واستخدام نظم التشغيل. ومن الطرق الشائعة في الاختراق طريقة Alec Muller وتستخدم لاختراق كلمات الرمز نوع (Unix) السرية والتي تعتبر المقياس الصناعي لضبط الأعمال وبالتالي تشخيص كلمات سر الشفرات الضعيفة والتي اكتشفت من قبل Ales D.E Muller [10] .وهناك طريقة خرق الملكية الفكرية للبرمجيات منها خروقات حقوق النشر، القرصنة الصناعية، القرصنة المؤسسية، قرصنة الوسطاء، والقرصنة المنزلية. أطلقت كلمة (Hacker) المشتقة من كلمة (Hack) والتي تعني (يقطع اربا) في أواخر الستينات على مجموعة من الطلبة في معهد ماساشوستي للتقنيات(Massachusetts institute of technology)(MIT) في الولايات المتحدة الأمريكية وكان سبب تسميتهم بهذا الاسم هو رغبتهم العارمة سد أغوار الحواسيب وابتكار طرق التعامل مع أجزائها الدقيقة ومنذ ذلك الحين وحتى أواخر السبعينات أطلق هذا الاسم على المتمكنين ومن ذوي الخبرة من الهواة وبشكل خاص الذين يملكون القدرات على ابتكار طرق عمل وأساليب جديدة لانجاز المهمات ومع بداية الثمانينات وانتشار الشبكات والحواسيب بشكل كبير تحول هذا الوصف إلى تهمة والسبب في ذلك أن عدد كبير من المبرمجين المتمكنين سخروا إمكانياتهم وخبراتهم في مجال تقنية المعلومات لإغراض شخصية مخالفة للقانون حملت في معظم الأحيان طابعا تخريبيا كالتسلل إلى أنظمة حصينة والحصول على معلومات سرية منها او تخريب نظام معين وإحداث خسائر مادية جسيمة ومنذ ذلك الحين حتى يومنا هذا استحدثت عشرات القوانين في مختلف دول العالم لملاحقة ومعاقبة من يطلق عليهم (Hackers) [10] .ظهرت منذ بداية الثمانينات مجموعة من المبرمجين تبنت أفكار وطرق وأساليب مختلفة للاختراق المخالفة للقانون واندرجت جميع هذه المجموعات تحت اسم (Hackers) إلا أن المبرمجين الذين لا زالوا يحافظون على المفهوم الأساسي لكلمة Hackers والتي شملت معنى حب المعرفة والتقنية والابتكار رفضوا على ان يطلق على مخالفي القوانين الاسم ذاته لذا صنف Hackers إلى أصناف وظهرت تسميات جديدة لكل صنف واصطلح على تسمية المجموعات التي تعمل بالخفاء بالمجتمع السفلي (Underground Community) واصطلح على إطلاق الأسماء التالية على الأصناف المختلفة من Hackers المخترق-المتسلل- مؤلفو الفيروسات-العابثون بالشفرات- الفوضويون[2]

٣ـ الفيروسات:

حملت البرامج او الملفات الخبيثة اسم الفيروس لأنها تشبه هذه العضوية في سلوكها للفناء. وهي بالأساس برامج تحمل ضررا خفيا للحاسبات.الفيروس عبارة عن كود يقوم بعمليات تستحضر داخل نظام الحاسبة او لتعديل برنامج اعتيادي لتمويه العمل لمصلحة مصمم الفيروس [18] .والفيروسات برامج صغيرة تصيب الأجهزة وتسبب الكثير من المشاكل مسح الذاكرة الصلبة ومسح بعض الملفات الخاصة بأنظمة التشغيل أو القيام بإصدار الأوامر لبعض البرامج دون علمك او بتدخل مباشر منك مثل ما يفعله فيروس الحب .وهناك أنواع عديدة من الفيروسات منها ملوثات الملف وفيروسات قطاع التجزئة والإقلاع والفيروسات المرافقة (ماكنج) وفيروسات الماكرو (جافا سكربت) وديدان الانترنيت (ديدان الحب) وجواسيس البريد الالكتروني وغيرها. هناك الكثير من وسائل السيطرة المتاحة لمنع اختراق الحواسيب منها وسائل السيطرة على البرمجيات والأجهزة واعتماد السياسات والأجهزة المتبعة للحفاظ على سياقات العمل وتحديد حركة الأفراد والجماعات المخولين واقوى أنواع السيطرة هو استخدام التشفير كونه يجهز أمنية عالية إضافة الى ذلك فأنه يستخدم في توفير السلامة والحماية لأنظمة الحاسبات [7].

٤ـ تقنيات استخدام الكشف:

تكنولوجيا الكشف ألتداخلي تدمج كل من الإشارة والكشف الإحصائي، وتقنيات الذكاء الاصطناعي (AI) وقد تم استخدامها في الكثير من البحوث ولكنها ليست مؤثرة تجاريا. فانعدام التوفير يهم العديد من الناس لأنهم يعتقدون بان الذكاء الاصطناعي سيجعل أمر الكشف ألتداخلي ذو قوة كبيرة -لا تخف- فأنظمة الذكاء الاصطناعي ذات تقنية مشكوك بها وللعديد من طرق التحليل الإحصائي المتوفرة تجاريا ذات محددات واضحة [19]. توجد العديد من تقنيات الكشف وكل تقنية تتميز بمميزات ولها مساوي وفوائد تختص بها منها:

٤ـ١ـ آليات شبكة الكشف:

لشبكة الإشارة شكلان أساسيان هما نماذج ضمن صندوق المحتويات ونماذج ضمن مؤشر المعلومات، تذكر إن نظام شبكة الكشف ألتداخلي يشبه كاميرا الفيديو خارج مجموعة من البيانات التي يتطلب حمايتها، فأنت تصل لتعرف ما يحصل بين هذه البيانات، مؤشر المعلومات ، ما يحصل في صندوق المحتويات، ويزيد التشفير من القابلية على رؤية محتويات الصندوق وبذلك نحتاج إلى الاعتماد أكثر على تحليل المؤشر إذا كان متضمن أستخدام لشبكة التشفير. ويمكن تقسيم هذه الآليات إلى [19]:

١. أشارات صندوق المحتويات:
هي بالأصل نماذج من صندوق المحتويات ويعرف صندوق المحتويات أيضا بالحمولة الدافعة (Payload) وهي معلومات شبكة الصندوق التي يتم الاتصال به من المصدر إلى الماكنه المعينة، وإشارات المحتوى الأكثر شيوعا والتي تزود بتفاصيل كثيرة في الكشف المحدد وهناك عدة اساليب منها.

- أسلوب FTP SIT Exes
- هجوم PHF

٢. مؤشر الصندوق (تحليل التعريفة):
نظام التعريفة هو طريقة لكشف نشاط الشبكة المشكوك بها دون الحاجة إلى النظر إلى محتويات الصندوق ، فمؤشر الصندوق يتضمن معلومات الطريق للصندوق. هناك كمية كبيرة من المعلومات الممكن اشتقاقها من تحليل التعريفة ولكن قد تجدها مختلفا جدا من التعود على رؤيتها اذا استعملت برامج للصندوق التجاري. هناك وسيلة تسمى shadow طورها Stephen North cut عندما كان في مركز البحرية والتي تسند الشبكة الإدارية بنوع من الكشف Shadow يستخدم برنامج tedium أصلا ليتم تطويره من المركز الأمريكي للطاقة [19] .

٣. Broad Cast:
هي مجموعات من الهجوم التي تسبب تحطيم الماكنة . ويحدث ذلك عندما نقوم بإرسال الصندوق إلى النظام مع المصدر وميدان الهدف المشابهة international وهي حالة طبيعية لا تثير اي قلق وكما يحدث في العديد من تطبيقات [19].

٤. ميدان الهجوم:
هناك العديد من المشتقات لنظام الهجوم واحدهما Land attack حيث Sync flog (علم) ينصب ويزود Stephen Norton في كتابة دليل المحلل لكشف ألتداخل في العديد من نماذج الكشف التي تستخدم لتحليل المتجه. وتتضمن طريقة تحليل المعلومات out of band التي يعتبر المصدر الهدف أرقام تتابع كشف تجزئي. [19]

٤-٢- أشارات المضيف الآلية:
تتميز اشارات هواة الكشف الشائع في أنظمة المضيف فهذه الإشارات تعرف مسبقا النماذج التي تم تعريفها كمستفيد من قبل أدارة الحماية ، ومثال الإشارة هو Three failed login حيث الإشارات تعرف أنها أنظمة مستندة على قواعد ولما كانت تعطي بداية يبدأ منها بتوليد التحذير، يتم تنفيذ استجابة ويتم إرسال أعلام بالأمر أو أن تحدث بعض الأحداث والميزة التي تكون آلية قاعدة جيدة وهو التعود بسهولة الاستخدام والتجنب. والإشارات هي قواعد أولية تقوم بتعريف تتابع لأحداث ومجموعات الائتلاف بين الأحداث والأحداث المسبقة الذكر وهي ثابتة لا تتغير .

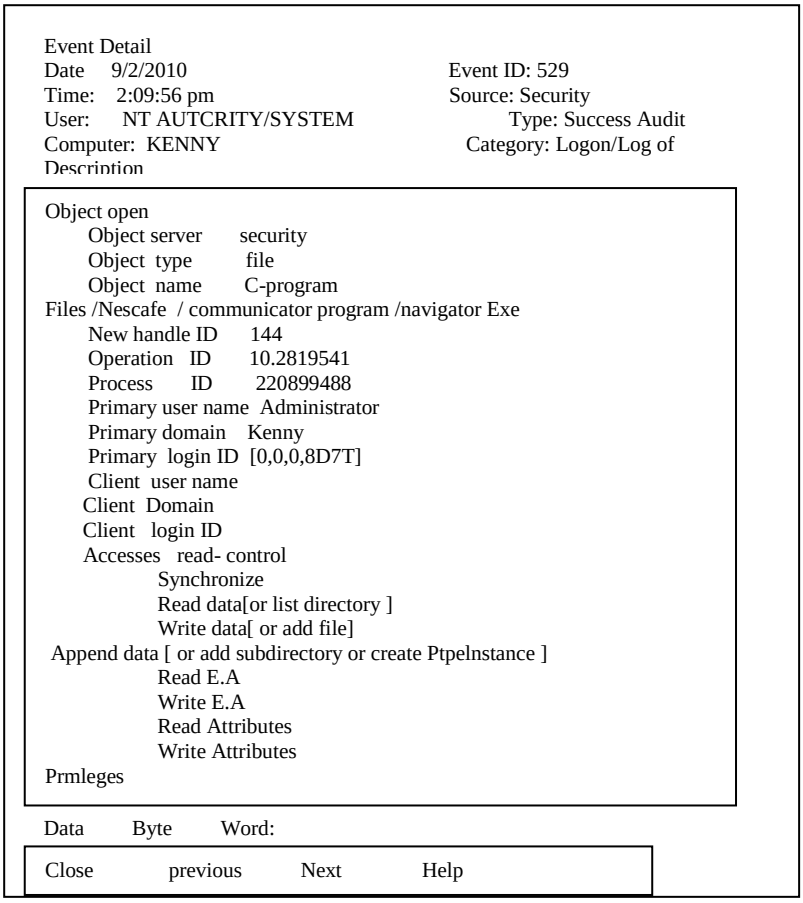
إساءة استخدام هو تداخل لأنه قد يستخدم استجابات أخرى مثل الاغماء أو التنويم ألتدميري وهناك العديد من الأنواع المختلفة للإشارة المختلفة المتضمنة للحدث المنفرد المتنوع أو المضيف المتعدد المشرع والإشارة المركبة ومعظم الإشارات هي أحداث منفردة ويمكن تقسيمها إلى عدة إشارات هي [19].

١. أشارات الحدث المنفرد:

أن الحدث المنفرد ذو الخصائص المميزة التي تشير الى نشاط الفائدة حيث ٩٠% من الإشارات هو حدث منفرد. وهذا يقود الى كون نشاط الفعالية ممكن تنفيذها بأحداث منفردة مع ذلك فان أشارات الحدث المنفرد لا يمكن اعتبارها بسيطة بسبب عدم وجود حدث واحد. وهناك العديد من ميادين الحدث المنفرد مجموعة نماذج المعلومات الميدانية الممكن تعقيدها كإشارات حدث منفرد -الكتابة للتنفيذ- وهي مثال على الحدث المنفرد، النموذج هو المراد الوصول آليه لأنه يكتب للمنفذ ومن وجهة نظر الحماية لا تكتب أحيانا، فهذه تحدث عادة عند تحديث البرمجيات والنشاط الإداري المنظم للنشاط وعلى أي حال فان المهاجمين الذين يزرعون حصان طروادة الفيروسات المسببة يتم الكشف عنها باستعمال حدث منفرد. جدول رقم (١) يظهر نموذج أشارات او مفتاح الإشارة على المادة ويسجل ملفا منتهيا ب exe وعلم fiag يظهر write data معلومات الكتابة.

جدول (١) Single Event Signature : Writing to an Executable

Field	Pattern
Event	560 Object Access
Object Name	*exe
Access	Write Data

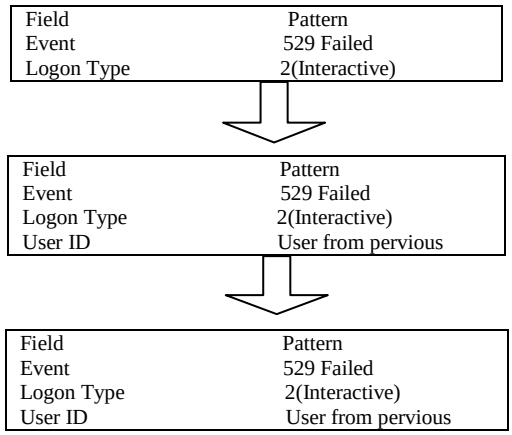


شكل (١) Writing to an Executable

شكل (١) يظهر الحدث من Windowsnt التي تعطي بداية الإشارة ، فالمستخدم يستلزم كتابة ال Netscape navigation وهذا يتم الإشارة آليه بإعلام .E.A write Altitudes append (addle)write dit, write الممكن بالكتابة بعض هذه بدون معنى مجرد مثلA tribute chg والتي تشير فقط إلى كون دليل المدخل مفتوحا ولا يشير مباشرة كون الملف مكتوبا ولا يوجد سوىwrite data ذو صلة. ومن الممكن اشتقاق معلومات إضافية من هذا السجل باستعمال المعلومات الموجودة في سجل الكشف، فعلى سبيل المثال تتبع ID نحو سجل العملية التنفيذية ، يودي إلى تحديد البرنامج الممكن استخدامه لتحسين مصدر navigation باستعمال هذه المعلومات ممكن الكشف باستخدام تاريخ ذلك البرنامج المجدد أذا أصيب بفيروس حصان طروادة [19] .

٢. إشارات الموت المتعدد:

أن إشارات الموت المتعدد هي سلسلة تضم اثنين أو أكثر من الأحداث لمجموعة من التنقلات بين الأحداث، وقليل جدا الأحداث المتعددة مقارنة بالأحداث المنفردة ومثال بسيط على أشارات الحدث المتعدد Three failed logins وهي مؤشر لتعين كلمة السر وعلى الرغم من أن هذا الهجوم هو نسبيا منخفض من الممكن ان يكون مؤشرا لكون المستخدم يكون دائما ذات خيارات قليلة لكلمة السر. أشيع كون نصف كلمات السر في منطق دالاس هي مشتقات Cowboys ولسوء الحظ تخمين كلمة السر هو عادة شائعة جدا ، جاعلا إياه الإشارة ذات الصلة. وهذه الإشارة المتعددة الأحداث تمثل به مجموعة من الأحداث والتنقلات بين الأحداث حيث الظاهر في شكل (٢) هو Three failed login متفاعلة مع أسهم تشير إلى نظام الأحداث فالتناقلات هي التسجيلات التابعة للأخرى في النظام الزمني من نفس المستخدم .التناقلات في الإشارة مباشرة جدا، مع ذلك ،التناقلات قد تكون متوسعة ومن الممكن إن تحدد بالزمن على سبيل المثال ضمن ٣٠ ثانية أو تشير إلى تغير في واحد أو أكثر من ميادين سجلات المتابعة اللاحقة باالاستناد على الميادين المناسبة في السجل السابق على سبيل المثال سجل تابع له يتناسب مع إجراء ID الأول.



شكل (٢) Multi-event Signature: Three Failed Logins

ولرؤية السجلات التي تعطي البداية للإشارة سنتبع ثلاث سجلات بأحداث مفردة من حدث مفرد Kenny . الشكل (٣) يظهر هذه الرؤية، لاحظ فشل login وهي تتجمع سوية من الكشف البسيطة ونادرا ما يكون هذا البسيط في العالم الحقيقي ولاحظ أيضا أن هناك لا توجد معلومات في رأي الحدث تشير إلى سبب هذا الفشل أو اسم المستخدم له ، ويشير المستخدم (User) إلى أن هناك الأجراء الذي كتب السجل System يملك أجراء login وهي معلومات غير مفيدة ومن الممكن

Date	Time	source	category	Event	User Computer	
9-2-2010	2:10:07pm	security	Detailed Tracking	592	Administrator	KENNY
9-2-2010	2:10:02pm	security	Detailed Tracking	592	SYSTEM	KENNY
9-2-2010	2:10:02pm	security	Detailed Tracking	592	SYSTEM	KENNY
9-2-2010	2:10:01pm	security	Logon / Logoff	538	Administrator	KENNY
9-2-2010	2:10:01pm	security	Privilege Use	576	Administrator	KENNY
9-2-2010	2:10:01pm	security	Logon / Logoff	528	Administrator	KENNY
9-2-2010	2:10:00pm	security	Privilege Use	576	Administrator	KENNY
9-2-2010	2:10:00pm	security	Logon / Logoff	528	Administrator	KENNY
9-2-2010	2:09:56pm	security	Logon / Logoff	529	SYSTEM	KENNY
9-2-2010	2:09:53pm	security	Logon / Logoff	529	SYSTEM	KENNY
9-2-2010	2:09:50pm	security	Logon / Logoff	529	SYSTEM	KENNY
9-2-2010	2:09:43pm	security	Detailed Tracking	593	Administrator	KENNY
9-2-2010	2:09:28pm	security	Detailed Tracking	593	Administrator	KENNY
9-2-2010	2:09:28pm	security	Detailed Tracking	593	Administrator	KENNY

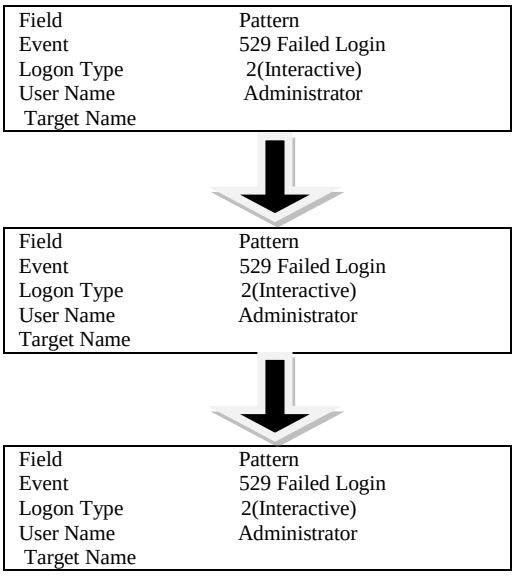
شكل (٣) Three Failed Login Attempts

رؤية الثلاث Logins حيث يحاول الدخول Administrator وأيضا ممكن رؤية logins تتفاعل وان سبب الفشل هو اسم المستخدم الغير معرف أو كلمة السر سيئة والحقيقة أن كل Failed login تحدث ضمن فترة ست ثواني وهو متناسق مع وضع المستخدم لكلمة السر. ولابد من ملاحظة كوننا لا نملك فكرة عن المستخدم لأنه login مشترك ويعد الاتصال هو احد الأسباب التي هي ان سجلات administrator عاجزة وان اي شخص باعتباره administrator يعطي اسم login الفريد من نوعه ،ومستوى الفائدة الذي تحظى به في هذه الإشارة هو وظيفة سياسة العمل [19] .

٣. إشارات المضيف المتعدد:

إشارات المضيف المتعدد هي كما يوحي اسمها إشارات تأتي من تراكم الأحداث للمضيفات المتعددة والتي تشير إلى أحداث سجل الذاكرة فإشارات المضيفات المتعددة مفيدة للكشف عن الهجمات السرية تكون عندما يكون الهجوم بسيط .انظر الشكل (٤) إلى تعريف الإشارة للThree failed logins من خلال أحداث متعددة الاختلاف الجوهري بين هذا المثال والمثال السابق هو أن

اسم الهدف تمت إضافة إلى التحديدات ان اسم المستخدم تم تضييفه (تحديده) على اسم administer فقط



شكل (٤)
Multi-Host Signature: Three Failed Logins access Multiple targets

هنالك العديد من التحديدات المرتبطة بتطبيق وتشكيل إشارات المضيف المتعددة في صيغة بشكل خاص لتبني آلية كشف فعالية لهذه الإشارة بسبب كون الزمن المتتابع من الأحداث التي تكون ذات مؤقتات ضعيفة فإشارات الكشف المتعدد للمضيف تتطلب تراكم معلومات بالموقع المركزي حيث هو ذو تحديد واضح للتركيب المعماري للوقت الحقيقي مع آليات كشف موزعة في المضيف المستخدم. ففي هذا المثال ستعطى الإشارة بأية failed login الحالة لحساب administration هدف في الشركة. وستبدو السجلات مشابهه للإشكال (٣ و٤) مع استثناء واضح هو السجلات ستأتي في ثلاث أماكن في الأهداف المنفصلة بشكل كامل والتي تشير إلى أن من تخمين كلمة المرور السرية والمنظمة التي ضمن الشركة [19] .

٤. الإشارات المركبة (الشبكة والمضيف)

ترتبط الإشارات المركبة مع مصدر online المتعددة مثل مجموعة أحداث المضيف وأحداث الشبكة فالإشارات المركبة تحصى بفوائد متعددة (التالي هو شكر Don master في فريق centran بمؤسسة cybersale) أشارات الشبكة تشير دائما إلى نشاط متتابع (ناجح) وافتراض إن مستخدما بعيدا استخدم ثقب حمايةFTP administrator login فان تبع نشاط المضيف successful administrator login فأنة يشير إلى أن الشبكة ناجحة. هجمات الضيف لا تزود دائما بالمعلومات عن مصدر الهجوم خصوصا أذا كان الهجوم من المضيف البعيد فإلاشارات المعقدة تترابط مع منبهة المضيف بمصدر معلومات ذو صلة، مثل مصدر port و IPK ،واسم المضيف. تزود الإشارات المركبة بنموذج الفعالية الممكن تحليلها من المصادر المقدر او من مصدر منفرد. وهذه الصيغة من الاتجاه ستكون حتما مفيدة أكثر من نشاط الشبكة فقط. وفي بعض الحالات، نشاط المضيف أو الشبكة لا يكون ذو شان لبعض المستخدمين وفي بعض الحالات هذه قد تمثل مواقع مزيفة على اي حال المستخدم قد يعتبر الإشارة المركبة حرجة. وبالإشارة المركبة المستخدم ممكن له وضع أوليات قليلة للفعاليات المنفردة لكنها قيمة عندما يكون هناك ترابط حرج. على العموم الإشارات المركبة مؤشر لهجوم متعمد. هجوم للمضيف قد يحدث خلال جلسة والتي تبدأ بهجوم الشبكة. فإلاشارات المركبة تجعل من السهل أحداث شق في التأثير الكمي لهجوم الشبكة. والخدمة لكشف فرع الكشف هي بالقدرة على قراءة أنواع المعلومات المتعددة في ماكنة كشف منفردة[19] .

٤-٣- آليات كشف الإشارة:

على الرغم من وجود مجموعة غنية من أنواع الإشارات فنظام الحماية ينبغي أن يكون متحفظا في تأسيس مجموعة القواعد لإزالة التوظيف بسبب كون الإشارات الكثيرة جدا مسببة لتنفيذ ضعيف وإدارة هزيلة ، فأنظمة الكشف ألتداخلي التجارية مهمة مع إشارات معرفة مسبقا، ونظام الحماية ممكن له التعود على القاعدة القياسية او يخلق قواعد جديدة. هناك العديد من الآليات المختلفة الإشارات.فتطبيقات آلية الكشف ذات تأثير واضح على قدرة التناسق مع متطلبات النظام المحدودة. فبعضها متضمن والأخر مبرمج وأخريات تم تطبيقها بأنظمة خبيرة Expert system .التضمين واحدة من آليات الكشف وهي متضمنة في النظام ومعترض فقط من خلال المحرر وهذا بسبب سهولة الاستخدام لان تعقيد آليات الكشف مخفي من غاية المستخدم . فعلى سبيل المثال نظام الحماية سيكون قادر على الاختيار من قائمة المستخدمين ، المواد التي تخلق القواعد وهذا تطبيق شائع في المنتجات التجارية ومثال الإشارة المتضمنة للواجهة الداخلية يتضمن[19]

- Cybercafé corporation من Centrex
- Internet security system من safe suite
- Security dynamic من kennel security monition

البرمجة تقنية أخرى من تقنيات الكشف حيث ان ماكنات الكشف المبرمج تحظى برمجة او لغة الكتابة القواعد فما كتاب الكشف المبرمج ذات مرونة عالية لكتاب تتطلب قدرا من الذي دربوا العمل .وأمثلة أنظمة الكشف ألتداخلي مع قواعد البرمجة تتضمن:

- المنبهة ألتداخلي(ITA) من Axent تزويد بلغة كتابة وملكية.
- سجل network Flight ذات لغة كتابة تسمى N-code
- Stalker from hay stack تزود بوسيلة للكتابة وبلغة برمجة C
- وتزود شبكة التداخل T-sight engraved Technologies لنظام الكشف APF لخلق أشارة بلغة C

٥- نموذج IDS الإحصائي:

أن هدف كشف الخرق بواسطة فحص تدقيق المستند هو تقدير متى دخل نظام الحاسبة حالة معابة او مقتحمة. حيث يركز نظام الكشف الإحصائي على فحص تدقيق المستند ويؤسس قراره على السلوك المتوقع من السلوك المتبع. يتألف نظام IDS الإحصائي من نموذجين ، الأول هو الوسط الحسابي والانحراف القياسي والثاني هو نموذج Bay وسيتم اخذ النموذج الأول كمثال للعمل. في بحثنا هذا. الإحصاءات تشكل مجموعة التنظيم والتحليل والتأويل للمعلومات . أن الإحصاءات عادة تقسم إلى قسمين رئيسيين هما الوصفية والاستدلالية. الإحصاءات الوصفية تتعامل مع التنظيم والإيجاز والعرض الكتابي للمعلومات. أما الإحصاءات الاستدلالية فتمكننا من الحصول على معلومات حول السكان التي لا يمكن قياسها لسعتها. ويمكن استخدامها أيضا في اتخاذ قرارات مهمة. الوسط الحسابي هو المعدل الذي يمكن إيجاده بتقسيم الكم (n) اي مجموع العناصر على العدد (n) وكما يأتي[13]

$$mean = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (1)$$

ان اختلاف مجموعة من الأرقام هو يعتبر مقياس لتشتت الأرقام الموجودة حول الوسط الحسابي[13] . أن الانحراف القياسي هو احد الأفكار المنفردة والأكثر أهمية في الإحصاءات

$$Var = \frac{\sum_{i=1}^{n} X^2 - n * mean^2}{n-1} \qquad (2)$$

$$S = \sqrt{Var} \quad (3)$$

عند اخذ قيمه d > 1 ، وإعطاء أية مجموعة قياسات مع الوسط الحسابي والانحراف القياسي ، على الأقل فان $(1 - \frac{1}{d^2})$ لهذه القياسات سيتم العثور عليه بين الموجب والسالب d انحرافات قياسية للوسط الحسابي . أن التوزيع الاحتمالي يحتوي على كل القيم الممكنة نظريا والتي يمكن افتراضها بمتغير عشوائي . كذلك فهي تشمل احتمالات هذه القيم ، حيث مجموع هذه الاحتمالية يساوي 1 [13] .ان التوزيع النظري واسع الاستخدام دائما هو التوزيع الطبيعي. وهو جرسي الشكل وهو متماثل بخصوص الوسط الحسابي (μ) حيث أن 50% تحته [12] . أن نظرية Chebyshev's تصف العلاقة المعينة بدون اي توزيع والانحراف القياسي لذلك التوزيع . حيث ان إعطاء توزيع اعتيادي يمكننا من تطبيق القاعدة التجريبية، والتي تكون القيم الايجابية (σ) فيها موجودة على يمين الوسط الحسابي والقيم السلبية (σ) فيها على يسار الوسط الحسابي . القاعدة التجريبية منصوص عليها القيم أدناه:

تقريبا 68% من المساحة تحت المنحني الطبيعي حيث تقع بين (-1σ) و ($+1\sigma$)

تقريبا 95% من المساحة تحت المنحني الطبيعي حيث تقع بين (-2σ) و ($+2\sigma$)

تقريبا 99% من المساحة تحت المنحني الطبيعي حيث تقع بين (-3σ) و ($+3\sigma$)

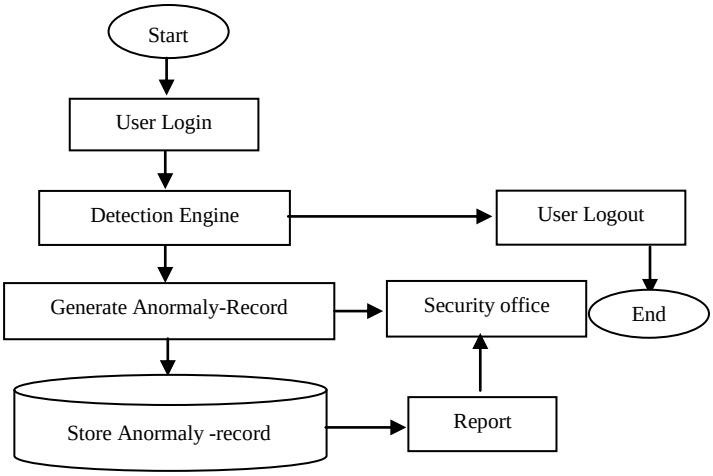
المساحات تحت المنحني تختلف تبعا لقيم μ و σ لذلك فالنظرية العامة لاحتساب المساحات تحت المنحني تكون على أساس تقيس التوزيع الطبيعي.المساحات بين قياسات معطاة (X) والوسط الحسابي μ يعبر عنها ب $(X - \mu)$. وبالإمكان التعبير عن هذه المساحة بمصطلحات أرقام الانحرافات القياسية باستخدام الصيغة التالية:

$$Z = \frac{X - \mu}{\sigma} \quad (4)$$

حيث Z يمثل الانحراف الطبيعي القياسي ويمثل الارقام للانحرافات الطبيعية بين X, μ [13] .

٥- ١- معمارية IDS المفترضة:

أن معمارية نظام التداخل الكشفي مبين بالشكل(٥) ومحدد في النقاط أدناه [14] .



شكل (٥) يمثل معمارية IDS المفترضة

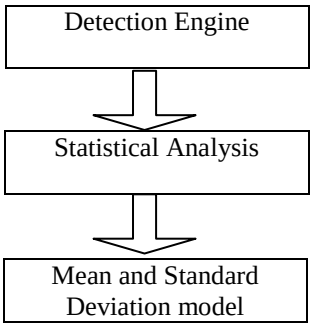
أن بحوث ماكنة الكشف للسلوك الشاذ يقارن المعلومات الجارية مع المعلومات التاريخية. أن معمارية ماكنة الكشف وكما هو مبين بالشكل (٦)

١-التسجيل – الشاذ يتولد عند ملاحظة سلوك غير طبيعي . أن التسجيل- الشاذ يرسل إلى عدد من نظم فرعية مختلفة لضابط الأمن . الاستجابة والخزن.

٢- أن ضابط الأمن يعلم به من خلال طريقة مرئية.

٣- خزن التسجيل – الشاذ لاستخدامه في شكل جديد متوقع للتداخل.

٤- يمكن خلق تقارير وتسلم إلى ضابط الأمن.



الشكل(٦) ماكنة الكشف المفترضة لل IDS

٥- ٢- النماذج الإحصائية

ليكن x متغير عشوائي ل n من المشاهدات $x_1, x_2, \ldots x_n$ ان عرض النموذج الإحصائي ل X لتقرير فيما اذا كان ملاحظ جديد X هو شاذ مع الملاحظ السابق . النظام الإحصائي IDS يتضمن النموذج التشغيلي ونموذج الوسط الحسابي والانحراف القياسي الذي يقوم على قاعدة افتراضية معروفة وهي الوسط الحسابي والانحراف القياسي والزمن المقرر لها هو دقيقتين:

$$sum = X_1 + X_2 + \cdots + X_n \quad (5)$$

$$sumsquare = X_1^2 + X_2^2 + \cdots + X_n^2 \quad (6)$$

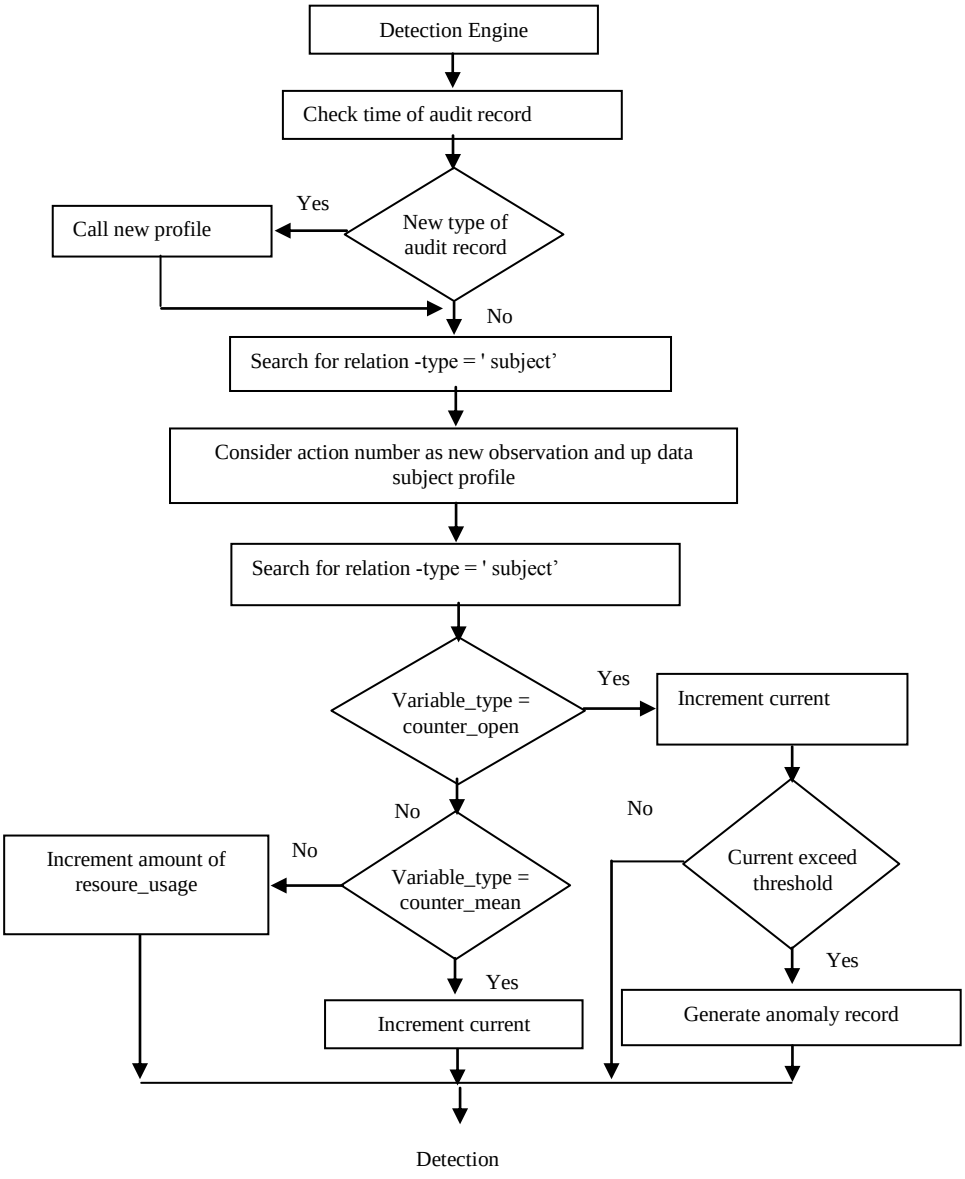
$$mean = \frac{sum}{n} \quad (7)$$

$$stdev = \sqrt{\frac{sumsquare - n * mean^2}{n-1}} \quad (8)$$

وقد تم تعريف ملاحظة جديدة لتكون شاذة اذا وقعت خارج فترة الثقة وهي الانحرافات القياسية من الوسط الحسابي لبعض المعلمات d .

$$confidence - interval = mean = d * stdev \quad (9)$$

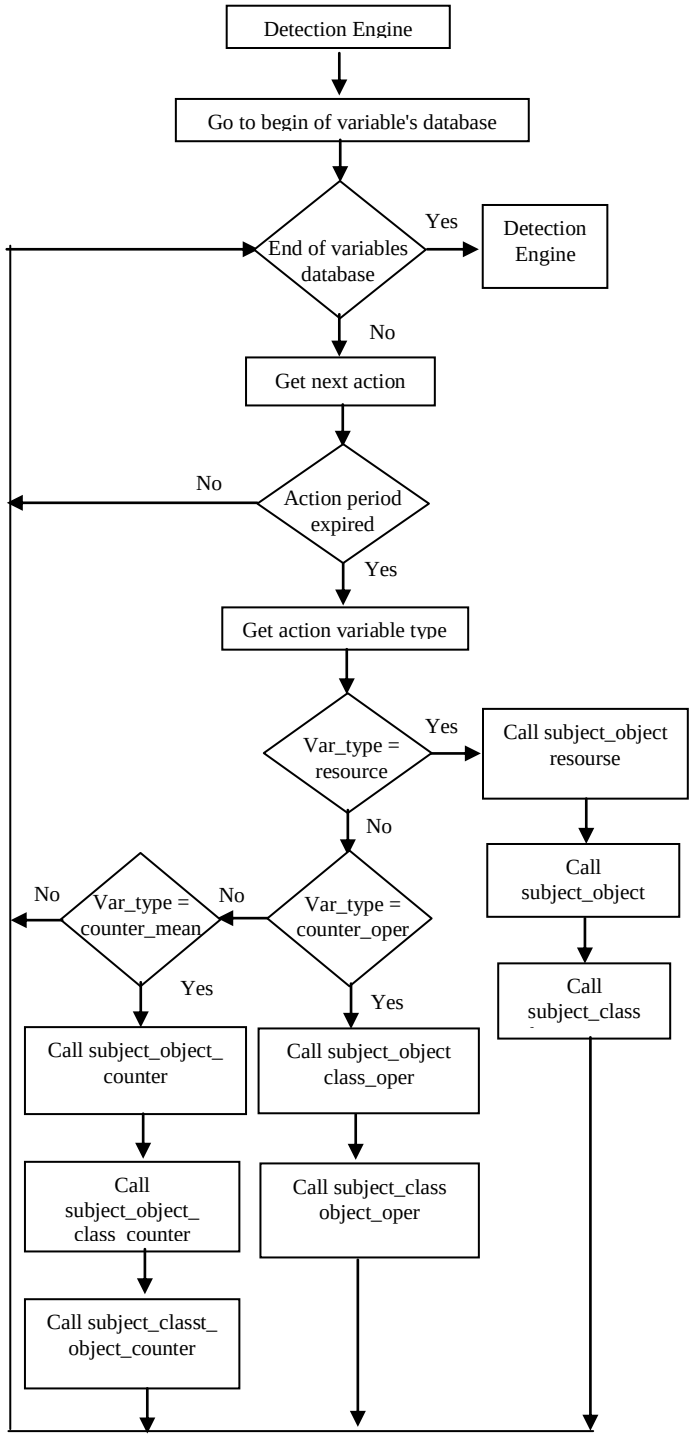
وبتفاوت Chebyshev's فان احتمالية القيمة الساقطة خارج الفترة هي على الأغلب تساوي $(1ld^2)$. عند استخدام النموذج التشغيلي مع أعداد الحدث تكتب اختصارا (التشغيل-العداد) وعند استخدام مقياس الأصل مع نموذج الانحراف القياسي تكتب (الوسط الحسابي- المصدر) . وعند استخدام العداد الحدث مع نموذج الانحراف القياسي والوسط الحسابي تكتب (الوسط الحسابي- العداد) وعند توليد سجل تدقيق جديد فأنة يطلق سجل التدقيق الى العمل [14]. أن قاعدة التدقيق تدعى أسلوب معالجة التدقيق وأسلوب Bay معا. المخطط التالي شكل (٧) يمثل إجراءات معالجة التدقيق.



شكل رقم (٧) يمثل مخطط إجراءات معالجة التدقيق

أن إجراء تدقيق الوقت يختلف أذا كان الوقت الفعلي المباشر في وقته الصحيح مستخدما حقل الموضوع لسجل التدقيق وجدول (اضبارة المستخدم) . كذلك يدقق إذا كان الفعل قد تولد من الموضوع في يوم غلقه ، حيث يدخل إجراء مظهر جانبي –جديد ، مظهر (مظاهر) جانية جديدة من النوع (الموضوع) أو/ و (الشيء- موضوع) في حين أن إجراء سجل – شواذ – توليد يدخل سجل شاذ جديد إلى قاعدة البيانات. في (الوسط الحسابي بمصدر) و (الوسط الحسابي بعداد) فان الشواذ لم تدقق ماعدا القيم (النمط المستخدم بمصدر) و (الجاري) تزداد كونها تحدث في قاعدة (تحديث – النشاط - الفترة) كل دقيقة تدققها قاعدة تحديث – النشاط- الفترة (المتغيرات) لقاعدة المعلومات للتأكد إذا كانت إحدى فترات الفعل قد نفذت. حيث إذا كان كذلك فسنقوم القاعدة بتحديث المظاهر الجانبية التي تحتوي على نفس الفعل ومخطط (٨) معالجه الفترة يوضح ذلك[14] . نحن نقوم بفصل (المتغيرات) لقاعدة المعلومات لجعل النظام أكثر مرونة وليتمكن ضابط الأمن ليضيف-يحذف-يزيد-ينقص من قيم الفترة لكل فعل. ان إجراء (مصدر- الشيء- الموضوع) يقوم بتدقيق كمية المصادر المستهلكة من قبل الموضوع قياسا إلى الشيء إلى الشذوذ وذلك بأخذ قيمة حقل (نمط- استخدام-المصدر) وافتراضه كرقابة جديدة، بعدها نستخرج قيمة جديدة من المراقبة[14] مثل X=observation وفحص الشذوذ بالشرط التالي:

$$[x < (mean - threshold * stdev)] and [x > (mean + threshold * stdev)] \qquad (10)$$



شكل رقم (٨) إجراءات معالجة الفترة

إذا كانت نتيجة الحالة أعلاه حقيقية ، سندعوها سجل-الشذوذ-تولد، وإلا سنتابع بتطبيق الخطوات التالية:

$$n = n + 1 \quad (11)$$

$$sum = sum + x \quad (12)$$

$$sum_sqr = sum_sqr + x^2 \quad (13)$$

بعد ان نقوم بالتدقيق لصنع الخبير المستخدم بمقارنة عدد المراقبات (n) مع حد المستخدم الخبراء التي وضعها مدير النظام، حيث إن قيمة حقل(نمط-المستخدم – المصدر – عداد) بصفر ومرة أخرى نقوم بتدقيق القيمة لحقل الحد ان استطعنا تقليصها وهذا يتفق مع نتائج الباحث [14] . أن إجراء عمل العداد – الشيء-الموضوع هو بالضبط نفس الموصوف أعلاه عدا الملاحظة الجديدة المعطاة من الحقل الحالي بدل حقل نمط- استخدام-المصدر . وكذلك القيمة الحالية المحدد بصفر بعد ذلك. وفي حالة إجراءات المصدر-طبقة الشيء- الموضوع و المصدر – الشيء – طبقة الموضوع فالعمل هو نفسه الموصوف في إجراء المصدر – الشيء-الموضوع ماعدا قيمة نمط – الاستخدام – المصدر فهي تجمعت على المظاهر الجانبية التي تحتوي (الشيء- الموضوع) في حقل نوع – العلاقة وحددت الفعل في حقل الفعل . بعدها يؤخذ بنظر الاعتبار القيمة الناتجة كرقابة جديدة وتطبيق اللوغاريتم أعلاه. وان كان المظهر الجانبي طبقة الشيء-الموضوع او الشيء-طبقة الموضوع لم يظهر فستخلقه الإجراءات وكما حصل علية الباحث [14] . ان إجراء عملية – طبقة الشيء- الموضوع هي لغرض تجميع قيم الحقل الجاري ومقارنة القيمة الناتجة مع قيمة معينة ، وان هجوما يشتمل على كلمة مرور مفردة تجريبية حول عدة قيم مقارنة مظهر جانبي لجميع المستخدمين.عند نفاذ فترة عدة تقرير- الشواذ، فهو تنبيه لضابط الأمن حول جميع التداخلات المكتشفة في النظام في الفترة الجارية. كذلك يستطيع ضابط الأمن تعيين نوع الاستجابة الحاضرة في النظام مثل إنذار ضابط الأمن إعادة تشغيل الحاسبة او غلق النظام وهذا متطابق مع ما توصل اليه الباحث [14] .

مثال:

عندما يقوم المستخدم ‘‘علي’’ بقراءة الاضبارة ١ في الساعة 10:00:00 قبل الظهر فان محتويات سجل التدقيق ستكون كما يلي: ["علي"،"قراءة"،"اضبارة١"،10:00:00 قبل الظهر] ، الفعل في سجل-التدقيق هو قراءة-الشيء-اضبارة١. كما وان ضابط الأمن قد حدد عداد – الحدث كمتري وانحراف قياسي والوسط الحسابي القراءة ، وهذا هو كم مرة حدث هذا

الحدث في الفترة المحددة . يقوم النظام بالبحث في المظاهر الجانبية قاعدة المعلومات عن مظهر جانبي الذي تشبع حقول الشيء والموضوع في السجل- التدقيق وكذلك نوع علاقة تساوي (الشيء-الموضوع) .ومتى وجد (أو خلق) النظام المظهر الجانبي المعين ، فيقوم بتحديد المظهر الجانبي معتمد على نموذج المتري والإحصائي (كما مبين في الشكل ٧) . أن النظام في هذا المثال يقوم بزيادة العداد بانتظار نهاية الفترة- التدقيق- الشواذ. وبعد انتهاء الفترة يضع العداد إلى الصفر . وان كانت قيمة العداد خارج الفترة ، فان النظام يخلق سجل – الشواذ وينبه ضابط الأمن حول هذا الفعل . لذا فالغرض تقليل السلبي الكاذب ، فهذا يعتمد على الاختيار المناسب للنموذج الإحصائي والمتري لكل فعل.

٦- الاستنتاجات والمقترحات:

نتيجة استخدام الشبكات اصبحت عملية الوصول الى المعلومات من قبل المتطفلين كثيرة ويصعب اكتشافها لذلك يجب ان يكون هناك انظمة حماية لاكتشاف المتطفل. أن العديد من التدخلات سببها عوامل بشرية مثل التصنت أو كلمات المرور المفتوحة أو بواسطة مطلعين أساءوا استخدام امتيازاتهم. وعند فشل القياسات المانعة في تاثيراتها فان نظام كشف التدخل يمكن أن يستدعى للمساعدة للامساك بالمتدخلين. أن نظام كتشاف الاختراق قادر على اكتشاف الكثير من الاخطاء التي تحدث نتيجة الاستخدام الخاطئ للحاسبات. نظام أكتشاف الاختراق يعتمد على مراقبة سجلات التوثيق التي تجري في انظمة اكتشاف انتهاكات الامنية. نظام اكتشاف الاختراق يتضمن ملفات سلوك المستخدم وفقا الى مكونات النظام بدلالة مقاييس ونماذج أحصائية وكذلك قواعد لاكتساب المعرفة حول سلوك المستخدم من سجلات التوثيق ولاكتشاف السلوك الشاذ. إن النظام المقترح يستخدم طرق إحصائية لبناء ملف المستخدم للتحقيق من الشواذ في السلوك أن الطرق الإحصائية هي نموذج الانحراف القياسي والاعتدال .وقد استنتجنا النقاط التالية من النظام المقترح :

١ -إن نظام IDS يجهز قاعدة متينة لغرض تطوير كشف تدخل حقيقي وقوي قادر على امتداد عريض من التدخلات ذات العلاقة بالتدخلات التي تتم المحاولة عليها.التنكر (تدخلات ناجحة) خروقات النظام أو إي إساءات استخدامات أخرى من قبل مستخدمين شرعيين.

٢ -النظام يسمح ببعض الخروقات لتكشف بدون معرفة العيوب في هدف النظام التي تسمح للخرق بالحدوث . وبدون الملاحظة الضرورية للفعل المعين المستثمر للعيب.

٣ -إن خصائص القياسية للمعمارية تسمح لتكون سهلة الامتداد. بشكل معدل . إما بإضافة أجزاء جديدة ، أو باستبدال الأجزاء عند استخدامها للتحديث.

٤ -يمكن اعتبار النظام المقترح كنموذج أساس قاعدة لمطابقة النظام . عند القيام بتوليد سجل تدقيق فسيتم مطابقة مقابل الأضابير البحث عن سلوك شاذ وتطوير المعلومات في ألاضباره المطابقة فيما أذا لم يتم الكشف عن الشواذ المكتشفة .إن تركيبات القوانين والأضابير هي غالبا نظام مستقل.

٥ -بالنسبة للمستخدمين الجدد ، فان مشكلة توليد سجلات شذوذ متوالية تكون حاضرة. لذلك فان فترات الثقة تكون ابتداءأ كبيرة وهكذا فكثير من التنوع قد تم احتماله في حين ان المعلومات تم تجميدها بدل سلوك احد المستخدمين . وبعدها فان الفترات تنكمش في حين ان عدد الملاحظات تتزايد. وهذا يقلل التنبيهات الكاذبة التي يسببها مظهر جانبي لأحد المستخدمين المحددين ولكنها لا تحمي النظام من مستخدمين جدد أو مستخدمين نادرين . والذي يكون سلوكهم منحرف أومن المستخدمين الذين يؤسسون سلوك غير طبيعي من البداية يتصور بان سلوك المستخدم من البداية طبيعي.

٦-١- اقتراحات للعمل المستقبلي:

١- لتسهيل الإخبار عن الشواذ، فان النظام يمكن إن يعزز لتضمينه مظاهر جانبية شاذة. وان مظهر جانبيا شاذا سيكون مشابها لنشاط جانبي عدا التحديد فسيتم إطلاقه بتوليد سجل شاذ في حدود IDS قياسا إلى سجل تدقيق من هدف النظام .فيما اذا كان مثل هذا التركيب مفيدا.على كل حال فهو غير واضح

٢- إن مقياس سجل موحد مع معلومات ذاتية التعريف ستكون مفضلة وهكذا فان كشف الخرق لبرمجيات يكون استقلال النظام ويمكن الحصول على ذلك بتعديل البرمجيات التي تنتج سجلات تدقيق في هدف النظام. أو بواسطة كتابة مرشح الذي يترجم التسجيلات إلى مقياس قياسي

٣- أما باقي النماذج الإحصائية يمكن اعتبارها مثلا نموذج معالجة ما ركوف . وهذا الموديل الذي يطبق فقط إلى عداد الحدث. يلاحظ كل نوع مميز لحدث (سجل تدقيق) كحالة متغيرة . ويستخدم قالب انتقال المسالة لغرض تشخيص تردد الانتقال بين الحالات (بدل ترددات فقط للحالات الفردية مثل سجلات التدقيق المأخوذة بشكل منفصل) حيث ملاحظة جديدة قد تم تعريفها لتكون غير طبيعية إذا كانت احتماليتها قد تم إقرارها في الحالة السابقة وكان قالب الانتقال واطئ جدا وهذا النموذج قد يكون مفيدا للاطلاع على الانتقال بين أوامر معينة حيث تكون أوامرها المتتالية مهمة.

٤- ولغرض الحصول على نتائج جيدة في نطاق الكشف. فنحن نقترح ربط طريقتي الكشف والتي هي كشف شاذ وكشف سوء استخدام وتصميم نظام جديد.

المصادر References

١ -أ.د. علاء حسين ألحمامي "إخفاء المعلومات طريقة جديدة للحماية "- كلية الرافدين الجامعة ٢٠٠٢.
٢ -أ. د. هلال محمد يوسف ألبياتي "الجوانب القانونية والأخلاقية في مجتمع المعلوماتية" – المعهد العالي للحاسوب والمعلوماتية ٢٠٠٠.
٣ -عبد الله الديوجي " الملكية الفكرية للبرمجيات والمعلومات " المستشار الإقليمي للاتصالات ١٩٩٩.
٤ -"مجلة الانترنيت في العالم العربي" تشرين الاول ١٩٩٩.
٥ -أ.د. هلال محمد يوسف " البيانات المخزونة في الحاسبة الشخصية" المعهد العالي للحاسوب والمعلوماتية ٢٠٠٠
٦ -د. وسيم عبد الأمير الحمداني " أنظمة التشفير" ١٩٩٧
7- WW.SPYzone.com, yahoo@ Search Results for Authorization.
٨- د. محمود خليل العبيدي " نظام التشفير للحاسبة الشخصية" معهد العالي للحاسوب والمعلوماتية ٢٠٠٠.
9- http://WWW.ditnet.com.
10- http://WWW.arbian.intenet.
١١- أ.د هلال محمد يوسف " حماية المعلومات في شبكة الانترنيت " المعهد العالي للحاسوب والمعلوماتية ٢٠٠٠
12-Denning D.E., "An intrusion Detection Model", IEEE Transactions on software Engineering. Vol. SE.13,No.2,Feberuary 1987
13-Duncan C.R>, Knapp G.R. and Millar M.C. ,"introductory Biostatistics for the Health Science" ,John Wiley & Sons Inc.,1977
14-Saffa Obeis Nahdi & prof Dr.Hilal M.Yousif & Dr.Nada M.AL-Salamy " Statistical Approaches for Intrusion Detection System", University of Technology,2002
15- http://WWW.alsarami@alriyadh-np.com
16- http://WWW. Cisco.com
17- http://WWW.icsa.net
18- http://WWW.practicalsecurity.com
19-The Practical intrusion detection handbook, Paul E. Proctor, February 2000.