الآيــة

(وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ)

التوبة 105

الأهداء

إلى أبي العزيز

أمي الغالية

إلى أخوتي

الي أصدقائي الاعزاء

الشكر والعرفان

الحمد لله ربّ العالمين

وأخص بالشكر

جامعة البحر الأحمر- كلية الدراسات العليا

كما أخص بالشكر أيضاً

الدكتور/ هشام علي مصطفى

الذي لم يبخل في تقديم كل المساعدات من نصح وإرشاد ومتابعة وإشراف علي هذا البحث

والشكر أيضاً

لشركة زاغروس للتجارة

لتعاونهم ودعمي بما أحتاج له من معلومات وبيانات

ولايفوتني أن أشكر

المهندس : أسامة قنديل أبوبكر

المهندس :ابراهيم محمد سليمان

المهندس: لنا تاج السر فضل المولى

لهم جميعاً أهدي شكري وتقديري

المستخلص

تهدف الدراسة لتصميم نظام أمني مدمج ذاتي التعلم، والمساهمة في تطوير الأنظمة الأمنية لكشف السلوك غير الطبيعي، والتسلل على قواعد البيانات، كما تناولت الدراسة المقدرة على إكتشاف أي نشاط غير قانوني من قبل المستخدم لقواعد البيانات.

إتبعت الدراسة تحليل نظام محاسبي وتحليل الثغرات الأمنية فيه وإضافة نظام كشف التسلل ليعملا سوياً، و تصميم نظام حسابات ليكون منصة يمكن من خلالها تصميم وتجربة نظام كشف التسلل، و من ثم يتم تقييم هذه الطرق و الوسائل الأمنية، وتَستخدِم هذه الدراسة بيانات حقيقية لتعطي تقييماً أكثر واقعية.

من خلال التحليل و الدراسة النظرية أثبت هذا البحث أن الوسائل التقليدية لتأمين قواعد البيانات ليست كافية و لا يمكن الإعتماد عليها كخط دفاع وحيد لحماية قاعدة البيانات، فكلمة المرور تكون في كثير من الحالات ضعيفة أو يتم إهمال تغييرها مما يسهل عملية حفظها وتخمينها، و وجدت الدراسة أن وضع سياسات أمنية وتتبع سلوك المستخدم يقلل من الوصول غير المسموح به، فقد وصل معدل إكتشاف حالات التسلل في هذا النظام إلى 88.47%.

من خلال تصميم وتنفيذ نظام بديل لتأمين قواعد البيانات يقدم البحث آلية مقترحة للإستجابة (Response Method) تعمل عند إكتشاف أي من حالات التسلل أو السلوك غير الطبيعي و تقوم بالإستجابة بصورة آلية و توفر معلومات لمدير النظام كوسيلة من وسائل الإنذار المبكر، و يمكن أن تقوم بوقف صلاحيات المستخدم (المشتبه به) لحين التأكد من سلوكه، و يتم كل ذلك إعتماداً على خدمة الرسائل القصيرة (SMS) عبر الهواتف المحمولة التي يتم تسجيلها عند إنشاء المستخدم لأول مرة .

يوصي الباحث بالإهتمام بتطوير الأنظمة الأمنية المدمجة في البرامج وتحسين أداءها، والإهتمام بالنواحي الأمنية للأنظمة من قبل مستخدميها و إجراء إختبارات للثغرات على الأنظمة قبل الإعتماد عليها لتفادي العبث بالبيانات.

ABSTRACT

The study aims to design a self-learning built-in security system to contribute to the development of security systems at detection of intrusion, abnormal behavior and illegal activities.

The study has been applied on an accounting system by analyzing the security vulnerabilities in the system and then adding intrusion detection system to work with the accounting system as a built-in security system. An accounting system has been designed for designing, testing and evaluating of the intrusion detection system using real data to ensure more real evaluation.

By applying analysis and theoretical studies this research proved that traditional ways of security systems are inadequate and should not be used as a single line of defense. The study found that developing security policies and tracking user behavior reduces unauthorized access, in this system the rate of intrusion detection reached 88.47%.

Through the design and implementation of an alternative database security system, the study introduces a proposed mechanism for response (response method) which works when detecting intrusion or abnormal behavior and responds automatically by providing information to the system administrator and it can stop the user's permissions until his behavior confirmed using SMS service on phone numbers saved at signing up.

The researcher recommends developing built-in security systems and improving their performance, paying more attention to security aspects of systems and testing systems vulnerabilities before relying on them.

فهرس المحتويات

الرقم	المحـــــــــــتويات	رقم الصفحة
1	الآية	أ
2	الإهداء	ب
3	الشكر والعرفان	ت
4	المستخلص	ث
5	Abstract	ج
6	فهرس المحتويات	ح
7	فهرس الأشكال	ذ
8	فهرس الجداول	ص
الفصـــل الأول – أساسيات البحث		
1.1	المقدمة	2
2.1	مشكلة البحث	3
3.1	أسباب أختيار موضوع الدراسة	4
4.1	أهمية البحث	6
5.1	أهداف البحث	6
6.1	منهجية البحث	6
7.1	أدوات جمع البيانات	6
8.1	مساهمة البحث	7
9.1	حدود البحث	7
10.1	تنظيم البحث	8
الفصـــل الثـــاني– أدبيات البحث والدراسات السابقة		
1.2	تمهيد	10
2.2	أمن المعلومات	11

الرقم	المحـــــــــــتويات	رقم الصفحة
3.2	الاتجاهات العامة (المهددات الأمنية)	13
4.1	جرائم تقنية المعلومات	13
5.2	سبل مواجهة المهددات الأمنية	15
6.2	الدراسات السابقة	18
الفصـــل الثـــالث – طرق وأدوات البحث		
1.3	تمهيد	33
2.3	مفهوم التحليل	33
3.3	النظام الحالي	35
4.3	مخرجات النظام	39
5.3	عمليات النظام	39
6.3	مدخلات النظام	39
7.3	المشاكل التي تواجه النظام	40
8.3	النظام المقترح	41
9.3	نظام كشف التسلل	42
10.3	دراسة الجدوى	47
الفـــصل الـرابـــع – التصميم		
1.4	تمهيد	52
2.4	البرمجيات والأدوات المستخدمة	52
3.4	وصف النظام	52
4.4	القوائم الرئيسية	53
5.4	شاشات الإدخال	58
6.4	تصميم الملفات	73
7.4	تصميم مخرجات النظام	77

الرقم	المحـــــــــــتويات	رقم الصفحة
8.4	آلية نظام كشف التسلل	83
9.4	آلية استجابة نظام كشف التسلل	89
10.4	إشعارات النظام	91
11.4	إنشاء الحسابات والصلاحيات	95
الفصـــل الخـــامس – النتائج والتوصيات		
1.5	تمهيد	100
2.5	تقييم النظام	100
3.5	النتائج	115
4.5	الخلاصة	116
5.5	التوصيات	117
	المراجع والمصادر	119
	الملاحق	123

قائمة الأشكال

الرقم	المحـــــتويات	رقم الصفحة
شكل(1.2)	كشف التسلل في قواعد البيانات عن طريق عملية التوقيع	20
شكل(2.2)	يوضح الكشف عن المعاملات الخبيثة	23
شكل(3.2)	يوضح نظام لكشف التسلل الأمني في قاعدة البيانات	25
شكل(4.2)	يوضح تنقيب البيانات لكشف التطفل في شبكات الحاسوب	28
شكل(5.2)	يوضح شجرة القرار	28
شكل(1.3)	يوضح عملية التحقق	45
شكل(2.3)	يوضح مراحل التقييم	46
شكل(3.3)	يوضح مراحل التأكد	47
شكل(1.4)	يوضح واجهة النظام	53
شكل(2.4)	يوضح القوائم الرئيسية – مستندات الإدخال	54
شكل(3.4)	يوضح القوائم الرئيسية – شاشات المبيعات	54
شكل(4.4)	يوضح القوائم الرئيسية – التقارير المحاسبية	55
شكل(5.4)	يوضح القوائم الرئيسية – العملات الأجنبية	55
شكل(6.4)	يوضح القوائم الرئيسية – المدخلات الأساسية	56
شكل(7.4)	يوضح القوائم الرئيسية – المرتبات	56
شكل(8.4)	يوضح القوائم الرئيسية – صيانة النظام	57
شكل(9.4)	يوضح القوائم الرئيسية – الأمن والسرية	57
شكل(10.4)	يوضح شاشات الإدخال– معلومات الموردين والأصناف	58
شكل(11.4)	يوضح شاشات الإدخال – حسابات العملاء	58
شكل(12.4)	يوضح شاشات الإدخال – توزيع مناطق البيع	59
شكل(13.4)	يوضح شاشات الإدخال– تغيير إسم ورقم الحساب	59

الرقم	المحـــــتويات	رقم الصفحة
شكل(14.4)	يوضح شاشات الإدخال – الدليل المحاسبي	60
شكل(15.4)	يوضح شاشات الإدخال – تفاصيل سند خصم	60
شكل(16.4)	يوضح شاشات الإدخال – سند إستلام نقدي	61
شكل(17.4)	يوضح شاشات الإدخال – إذن صرف داخلي	61
شكل(18.4)	يوضح شاشات الإدخال – تعديل مستند إشعار إضافة	62
شكل(19.4)	يوضح شاشات الإدخال – إستلام شيكات تحت التحصيل	62
شكل(20.4)	يوضح شاشات الإدخال – الشيكات المرتدة	63
شكل(21.4)	يوضح شاشات الإدخال – حافظة توريد شيكات	63
شكل(22.4)	يوضح شاشات الإدخال – الشيكات غير المستخدمة	64
شكل(23.4)	يوضح شاشات الإدخال – تقارير محاسبية متنوعة	64
شكل(24.4)	يوضح شاشات الإدخال – كشف حساب عميل	65
شكل(25.4)	يوضح شاشات الإدخال – تحليل مبيعات	65
شكل(26.4)	يوضح شاشات الإدخال – الأرصدة الإفتتاحية	65
شكل(27.4)	يوضح شاشات الإدخال – تغيير كلمة المرور	66
شكل(28.4)	يوضح شاشات الإدخال – حقوق الوصول للنظام	66
شكل(29.4)	يوضح شاشات الإدخال – القيود والتسويات	67
شكل(30.4)	يوضح شاشات الإدخال – فاتورة مبيعات	67
شكل(31.4)	يوضح تقارير أمن وسرية النظام	68
شكل(32.4)	يوضح شاشات الإدخال – معلومات الموظف الأساسية	68
شكل(33.4)	يوضح شاشات الإدخال – تفاصيل مرتب	69
شكل(34.4)	يوضح شاشات الإدخال – خصومات مجدولة	69
شكل(35.4)	يوضح شاشات الإدخال – إنشاء كشف مرتبات	70
شكل(36.4)	يوضح شاشات الإدخال – تفاصيل عامل	70

الرقم	المحـــــتويات	رقم الصفحة
شكل(37.4)	يوضح شاشات الإدخال – معلومات المخزون	71
شكل(38.4)	يوضح شاشات الإدخال – فاتورة بضائع مرتجعة	71
شكل(39.4)	يوضح شاشات الإدخال –مشتروات مستوردة	72
شكل(40.4)	يوضح شاشات الإدخال – مشتروات محلية	72
شكل(41.4)	يوضح شاشات الإدخال – الدمغات والقيمة المضافة	73
شكل(42.4)	زمن الدخول علي النظام	77
شكل(43.4)	الخطأ في كلمة المرور	77
شكل(44.4)	ملخص أحداث الخطأ في الدخول	78
شكل(45.4)	يوضح جميع أحداث الدخول للنظام	78
شكل(46.4)	زمن الخروج من النظام	79
شكل(47.4)	قائمة مستخدمي النظام	79
شكل(48.4)	عنوان فيزيائي مصرح به	80
شكل(49.4)	عنوان فريائي غير مصرح به	80
شكل(50.4)	طلب كلمة المرور	81
شكل(51.4)	يوم عمل غير مصرح به	81
شكل(52.4)	وقت عمل غير مصرح به	82
شكل(53.4)	نشاط المستخدمين	82
شكل(54.4)	يوضح رسالة أمن النظام (العنوان الفيزيائي)	84
شكل(55.4)	يوضح رسالة أمن النظام (خطأ في إدخال كلمة المرور)	84
شكل(56.4)	يوضح رسالة أمن النظام (كتابة كلمة المرور خطأ لثلاث مرات)	85
شكل(57.4)	يوضح رسالة أمن النظام (تاريخ الإستخدام)	85
شكل(58.4)	يوضح رسالة أمن النظام (سلوك المستخدم في التنقل)	86
شكل(59.4)	يوضح رسالة أمن النظام (زمن الإستخدام)	87

الرقم	المحـــــتويات	رقم الصفحة
شكل(60.4)	يوضح رسالة أمن النظام (سرعة الإدخال)	87
شكل(61.4)	يوضح رسالة أمن النظام (عمليات الإضافة)	88
شكل(62.4)	يوضح رسالة أمن النظام (عمليات التعديل)	88
شكل(63.4)	يوضح رسالة أمن النظام (عمليات الحذف)	89
شكل(64.4)	يوضح رسالة أمن النظام للتأكد من المستخدم	89
شكل(65.4)	يوضح رسالة أمن النظام لإدخال الرقم التعريفي	90
شكل(66.4)	يوضح رسالة أمن النظام لإدخال الرقم التعريفي للمستخدم	90
شكل(67.4)	يوضح شاشة الدخول على النظام	90
شكل(68.4)	يوضح رسالة أمن النظام لمدير النظام (محاولة دخول عشوائي)	91
شكل(69.4)	يوضح رسالة أمن النظام لمدير النظام (إدخال كلمة مرور خاطئة)	91
شكل(70.4)	يوضح رسالة أمن النظام (محاولة دخول من جهاز غير مصرح)	92
شكل(71.4)	يوضح رسالة أمن النظام (محاولة دخول في زمن غير مصرح)	92
شكل(72.4)	يوضح رسالة أمن النظام (محاولة دخول في يوم غير مصرح)	93
شكل(73.4)	يوضح رسالة أمن النظام لمدير النظام(عمليات إضافة متعددة)	93
شكل(74.4)	يوضح رسالة أمن النظام لمدير النظام(عمليات تعديل متعددة)	94
شكل(75.4)	يوضح رسالة أمن النظام لمدير النظام(عمليات حذف متعددة)	94
شكل(76.4)	يوضح رسالة أمن النظام لمدير النظام (مراقبة المستخدمين)	94
شكل(77.4)	يوضح شاشة إضافة مستخدم جديد	95
شكل(78.4)	يوضح رسالة أمن النظام لمدير النظام (بوجود المستخدم في النظام)	95
شكل(79.4)	يوضح رسالة أمن النظام لمدير النظام(خطأ في إدخال الهاتف)	96
شكل(80.4)	يوضح رسالة أمن النظام (إستخدام رقم هاتف مستخدم آخر)	96
شكل(81.4)	يوضح شاشة تعطيل المستخدم	96
شكل(82.4)	يوضح صلاحيات المستخدم (الأيام وزمن الإستخدام)	97

الرقم	المحـــــتويات	رقم الصفحة
شكل(83.4)	يوضح شاشة صلاحيات المستخدم في نوافذ النظام	98
شكل(1.5)	يوضح مخطط بياني يوضح الأداء العام للمعايير السبعة	107
شكل(2.5)	يوضح مخطط بياني يوضح أداء النظام في إستخدام الفأرة	109
شكل(3.5)	يوضح مخطط بياني يوضح أداء النظام في إستخدام لوحة المفاتيح	110
شكل(4.5)	يوضح مخطط بياني يوضح أداء النظام في إستخدام سرعة الكتابة	112
شكل(5.5)	يوضح مخطط بياني يوضح أداء النظام في سرعة الكتابة وإستخدام الفأرة	112
شكل(6.5)	يوضح مخطط بياني يوضح الأداء العام للنظام	114

فهرس الجداول

الرقم	المحتويات	رقم الصفحة
جدول(1.3)	يوضح الجدول الزمني	48
جدول(2.3)	يوضح الأجهزة والمعدات	49
جدول(3.3)	يوضح الجدوي التشغيلية	49
جدول(1.4)	يوضح صلاحيات المستخدم على النظام	73
جدول(2.4)	يوضح الأيام المصرخ بها للمستخدم	74
جدول(3.4)	يوضح بيانات العنوان الفيزيائي المصرح للمستخدم في النظام	74
جدول(4.4)	يوضح أزمنة المستخدام المصرح به للمستخدم على النظام	75
جدول(5.4)	يوضح العمليات الخاطئة التي تمت على النظام	75
جدول(6.4)	يوضح عمليات الدخول على النظام	76
جدول(7.4)	يوضح بيانات المستخدم	76
جدول(1.5)	تقييم أداء العنوان الفيزيائي	101
جدول(2.5)	تقييم أداء كلمة المرور	102
جدول(3.5)	تقييم أداء نظام صلاحيات الأيام	103
جدول(4.5)	تقييم أداء النظام في صلاحيات وقت العمل	104
جدول(5.5)	تقييم أداء النظام في عمليات الإضافة	105
جدول(6.5)	تقييم أداء النظام في عمليات التعديل	106
جدول(7.5)	تقييم أداء النظام في عمليات الحذف	107
جدول(8.5)	تقييم أداء النظام في إستخدام الفأرة	108
جدول(9.5)	تقييم أداء النظام في إستخدام لوحة المفاتيح	109
جدول(10.5)	تقييم أداء النظام في سرعة الكتابة	111
جدول(11,5)	تقييم الأداء العام لنظام كشف التسلل	113