جامعة الملك سعود

كلية علوم الحاسب والمعلومات

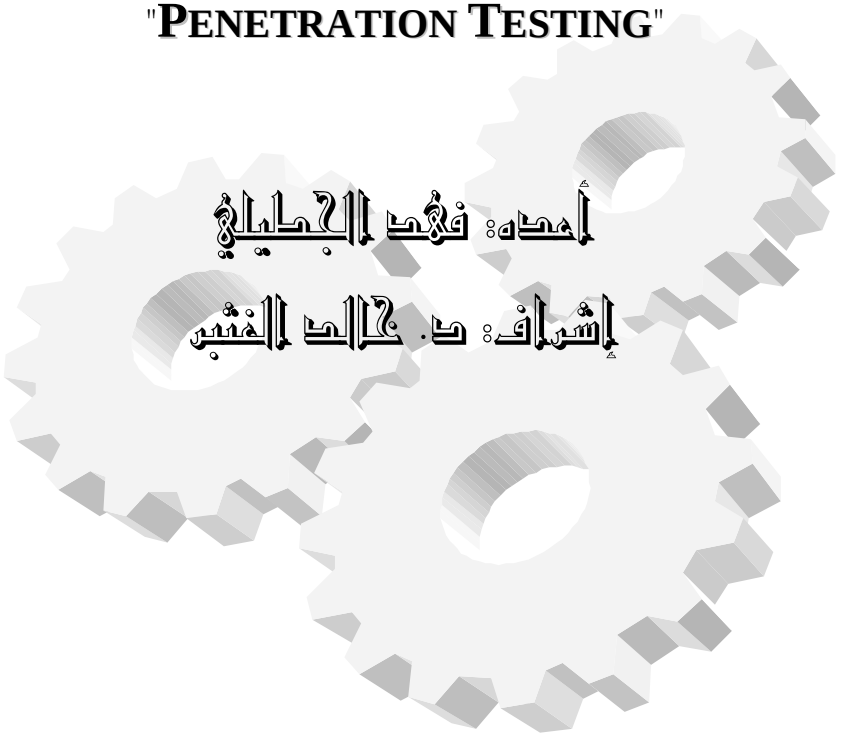
قسم نظم المعلومات

برنامج الماجستير

بحث

إختبار الاختراق

"**PENETRATION TESTING**"



أعده: فهد الجليل

إشراف: د. خالد الغثبر

اختبار الاختراق
PENTERATION TESTING

مقدمة:

في السنوات القليلة الماضية، سمعنا في الأخبار عن هجمات حجب الخدمة (DoS) حدثت لشركات كبيرة ومعروفة مثل ياهو و مايكروسوفت. وكذلك سمعنا عن زيادة الهجمات التخريبية للمواقع الإلكترونية والتي تحدث للآلاف من الشركات المنتشرة حول العالم. وقد حان الوقت لكي نعمل على حماية أنفسنا من الشركات المنافسة أو من الهاكرز أو حتى من المراهقين الذين يلعبون في أجهزة الكمبيوتر. نحتاج لحماية البُنى التحتية لشركاتنا، كما تفعل بيوتنا وممتلكاتنا الخاصة. للعقدين أو الثلاث عقود الماضية كانت الناس تترك بيوتها، محلاتها وحتى سياراتها غير مقفلة وذلك لقلة الجريمة التي قد تهدد مصالح الناس الخاصة. ومع مرور الوقت والتطور السريع في جميع مناحي الحياة، وبخاصة في مجال التكنولوجيا زادت المشاكل وارتفع مستوى الجريمة وأصبح مجال الجريمة الإلكترونية واسع وكبير وخطورته عالية.

أما في مجال الشبكات، أفضل طريقة لحمايتها هو معرفة الفجوات الحالية والسابقة وعمل الترقيع " Patch " لكل الأجهزة والأنظمة في حال وجود مرقعاً لهذه الفجوات. على كل حال، هذا لا يكفي لحمايتنا، وذلك لأن الإنسان مخلوق معرض لعمل الخطأ؛ حيث أنه قد يقوم بعمل تصريح دخول للنظام لشخص غير مصرح له عن طريق الخطأ. ولهذا ليس مهماً كم من الترقيع عمل للبيئة المحيطة، حيث أن الأنظمة ما زالت تحتوي على الفجوات التي قد تكون عرضة للهجوم من خلالها.

من هنا يأتي دور اختبار الاختراق. الهاكرز وأناس آخرين ممن يريدون الدخول إلى شبكتك، سوف يقومون بعمل الهجمات والمحاولات الكثيرة لكي يصلوا إلى الأنظمة التي تعتمد عليها. وعليه تحتاج أنت لإيجاد الأساليب التي يستخدمها هؤلاء الأشخاص، لتعملها بنفس الطريقة التي يستخدمونها في الهجوم ومحاولة اختراق شبكتك لكي يفضحوا الأنظمة أو يخربوها. ولهذا الشكل تقوم أنت بسد هذه الثغرات.

ما هو إختبار الإختراق PENTERATION TESTING

كما هو واضح من مقتضى الاسم " اختبار الاختراق " أنه مجموعة من الأنشطة التي تُعمل لتعريف أو كشف الثغرات الأمنية؛ والفكرة هي إيجاد مدى السهولة أو الصعوبة على شخص ما لاختراق آليات التحكم الأمنية في المنظمة أو الحصول على الدخول الغير مصرح به إلى الأنظمة المعلوماتية لها.

اختبار الاختراق يتضمن فريق صغير من الأشخاص موكّلين من المنظمة لكي يقوموا بعمل هذا الاختبار . وهذا الفريق يحاول كشف الثغرات التي توجد في أنظمة أمن المعلومات للمنظمة، وذلك بمحاكاة الشخص الغير مصرح له أو ما يعرف بالهاكر، للهجوم على النظام باستخدام نفس الأدوات والتقنيات .

فرق اختبار الإختراق تشمل مجموعة أشخاص من قسم الرقابة والمتابعة الداخلية " Internal Audit " أو من قطاع تقنية المعلومات " IT " أو من شركة استشارية متخصصة في مثل هذا المجال . هدفهم هو تعريف الثغرات الأمنية في الظروف التي تحت سيطرة الشركة، ومن ثم يقومون بإزالتها قبل أن تكتشف من قبل الأشخاص الغير مصرح لهم .

ولأن اختبار الاختراق هو عمل مصرح به لمحاكاة أنشطة الهاكرز يطلق عليه القرصنة الأخلاقية " ETHICAL HACKING " .

من هي الهاكر:

هو شخص يحاول تحطيم أنظمة الآخرين بخلفية برمجية جيدة أو معرفة وخبرة كبيرة في مجال الأعمال الإلكترونية .

وهو ينظم معرفته للقيام بمحاولات كشف وتعريف الأخطاء البرمجية والثغرات الأمنية واستخدامها لتخريب الأنظمة أو لأهداف خبيثة أخرى .

الهدف من اختبار الاختراق:

الهدف هو معرفة ما مدى أمن شبكتك، أو من وجهه نظر الهاكرز كيف شبكتك غير آمنة . أنت تحتاج لاختبار جميع الأنظمة الموجودة على الشبكة، من غير الاهتمام بأي نظام تشغيل أو تطبيق يعمل عليها، إذا كان هناك شيء وحيد يجب أن يتذكره الشخص هو أنه جميع الأنظمة تحتوي على الثغرات وتختلف من نظام إلى نظام، لكن لا يوجد نظام على الإطلاق ١٠٠% ، آمن ليس الآن ولا حتى في المستقبل . إذا لم يقم الشخص بعمل اختبار الاختراق لشبكته وأنه لم يقم بعمل ترقيع "Patch" لجميع الأجهزة والأنظمة التشغيلية والتطبيقات بآخر الترقيعات الأمنية فإنه سوف يكون عرضة بل وعرضة سهلة للهجمات التخريبية .

لعمل اختبار الاختراق سوف يحتاج الشخص لعمل مسح شامل لجميع الأنظمة من الداخل ومن الخارج لمعرفة المدى الذي يمكن الحصول عليه من المعلومات . الهاكرز يحاولون الدخول إلى أحد الأجهزة في الشبكة لتكون نقطة انطلاقهم داخل أنظمة المنظمة، وأغلب الأحيان يستخدمون الإنترنت أو يقومون بمحاولة الاتصال إلى خوادم الدخول البعيد "RAS" لإتمام عملهم .

هل تمتلك أي مودمات "طلب الاتصال" ملحقة بأجهزة الكمبيوتر وموصلة على خطوط الهاتف ؟ إذا كنت تمتلك تلك الإمكانية، حاول أن تقوم بعمل اختبار الاختراق لها وأنظر ما النتيجة .

بعض الهاكرز يريدون فقط أن يقولوا أنهم قاموا بإختراق هذا النظام أو ذاك، ويقوموا بنشر ما فعلوه على المواقع الإلكترونية متفاخرين بذكائهم وإمكانياتهم . وبعضهم الآخر يقوم بالدخول على معلومات الناس الشخصية ويستعملها لأغراضه الخاصة أو يقوم ببيعها أو استخدامها بطريقة سيئة .

الاختبار الذي يقوم به الشخص سوف يوضح لأي مدى أنظمة المنظمة في خطر، وعليه بإمكانه أخذ الدعم من الإدارة العليا في المنظمة لعمل ما هو مهم بهذا الخصوص، من وضع سياسات أمنية وعمل جدولة زمنية للقيام بعملية الترقيع للأنظمة في المنظمة . عملية الترقيع لا يجب أن تكون متمركزة على الأنظمة الرئيسية بل لكل الأنظمة؛ وذلك تبعاً للمقولة الشائعة "لا تترك حجراً لم يقلب " . إذا قام الشخص بعمل الاختبار على الأجهزة في الشبكة وعمل لها الترقيع اللازم فإنه لا يجب أن يتركها من غير الاستمرارية بنفس الطريقة من متابعة التحديثات للأنظمة وما إلى ذلك . وإذا وجد جهاز أو جهازان في الشبكة يحتويان على ثغرات أمنية فإنهما عرضة ليستخدما في نشر الفيروسات أو الديدان أو أي برامج هجومية أخرى لعمل ضرر بالأنظمة النظيفة الأخرى .

ماذا يتضمن اختبار الاختراق:

مجال " Scope " مشروع اختبار الاختراق يكون موضوع المفاوضة بين المنظمة وفريق الاختبار، وسوف يكون مختلفاً، اعتماداً على أهداف محددة كي تنجز؛ حيث أن الهدف الرئيسي للاختبار هو تحديد أن الثغرات الأمنية للمنظمة يمكن أن تكتشف وتفتضح أنظمتها .

عمل مثل هذا الاختبار يكون بالحصول على المعلومات عن أنظمة المعلومات والأنظمة الأمنية للمنظمة ومن ثم استخدامها لمحاولة تعريف وكشف الثغرات المعروفة أو الخفية .

الدليل أو الشاهد لدعم قدرات فريق عمل اختبار الاختراق في كشف الثغرات الأمنية قد يكون مختلفاً، ومثال ذلك الحصول على لقطات لشاشة الكمبيوتر " Computer Screen shot " أو نسخ معلومات حساسة أو إمكانية إنشاء حساب مستخدم جديد في النظام أو إمكانية حذف وإضافة ملف محدد على خوادم المنظمة .

اختبار الاختراق ممكن أن يحتوي على عدد من الأهداف الثانوية مثل، اختبار تعريف الحوادث الأمنية للمنظمة وإمكانية الرد عليها، اختبار المعرفة الأمنية للموظفين أو اختبار امتثال المستخدمين للسياسات الأمنية المنصوص عليها .

استراتيجيات الاختبار:

توجد استراتيجيات مختلفة في اختبار الاختراق، وتعتمد في ذلك على الأهداف المراد إنجازها:

١.الاختبار الداخلي والاختبار الخارجي:

الاختبار الخارجي يشير إلى الهجوم على محيط شبكة المنظمة باستخدام إجراءات تؤدى من خارج أنظمة المنظمة؛ وتكون على الأغلب من الإنترنت للقيام بالاختبار، فريق الاختبار يبدءون باستهداف الأجهزة أو الخوادم الظاهرة خارجياً في الشركة مثل خادم اسم النطاق DNS، خادم البريد الإلكتروني Email خادم الموقع الإلكتروني Web أو الجدر النارية Firewall.

الاختبار الداخلي يكون من داخل البيئة التقنية للمنظمة . يكون التركيز في هذه الاختبارات على فهم ماذا يمكن أن يحدث إذا تم اختراق محيط الشبكة بنجاح، أو ماذا يمكن أن يفعل شخص لاختراق مصادر معلومات محددة داخل شبكة المنظمة .

٢.إستراتيجية اختبار الهدف المحدد واختبار العمى Blind والعمى المضاعف:

* في إستراتيجية ***اختبار العمى***، يزوّد فريق الاختبار بمعلومات محدودة جداً عن الأنظمة المستخدمة . وكذلك يجب أن يستخدم فريق اختبار الاختراق المعلومات المتوفرة بشكل عام، و مثال ذلك موقع الشركة الإلكتروني، وكذلك سجل اسم النطاق وما إلى ذلك؛ وهذه المعلومات ستساعدهم في معرفة هدفهم لكي يبدءوا عملية الاختبار .

اختبار العمى قد يعطي معلومات عن المنظمة، يمكن أن تكون غير معروفة لهم مسبقاً، ولكنها هذا الشكل من الاختبارات قد تكون أكثر احتياجاً للوقت ومكلفة جداً مقارنة بغيرها من اختبارات الاختراق، وذلك لأنها تحتاج جهد كبير من فريق الاختبار للبحث عن الهدف .

* ***اختبار العمى المضاعف*** "Double-blind" هو توسيع لإستراتيجية اختبار العمى، حيث أنه لا أحد من المنظمة أو مسئولي أمن المعلومات له معرفة بهذا الاختبار والأنشطة التي تؤدى فيه . اختبار العمى المضاعف بإمكانه اختبار مراقبة الأمن داخل المنظمة ، تعريف الحوادث الأمنية "Incident Identification" من قبل الموظفين المسئولين وإجراءات الرد "Response Procedures" . عادةً عدد قليل جداً من الناس داخل المنظمة يعلم بهذا الاختبار ويكون غالباً الشخص المسئول عن المشروع من المنظمة .

* ***اختبار الهدف المحدد*** وعادةً يطلق عليه اختبار الأنوار المشعلة "Lights-Turn-On" . ويشمل كلاً من فريق تقنية المعلومات من المنظمة وفريق الاختبار وهذا الفريق الذي هو يكون عنده الدراية بكل الأنشطة التي سوف تؤدى في

الاختبار، ويكون فريق الاختبار على دراية بالهدف وعنده معلومات عن تصميم الشبكة وما إلى ذلك من معلومات عن ما يستهدفون.

اختبار الهدف المحدد يركز على الإعدادات الفنية أو على تصميم الشبكة أكثر من التركيز على الاستجابة للحوادث في المنظمة أو أي إجراءات تشغيلية أخرى. وهو يأخذ وقتاً وجهداً أقل لإكماله مقارنة باختبار العمى، لكنه قد لا يزوّد المنظمة بالصورة الكاملة عن الثغرات الأمنية وإمكانية الرد السريع على الحوادث الأمنية.

أنواع الاختبارات:

بالإضافة لاستراتيجيات اختبار الاختراق التي يمكن استخدامها، فلابد من ذكر أنواع الاختبارات التي يقوم بها فريق الاختبار، وهي كما يلي:

١. اختبار أمن التطبيقات:

أكثر الشركات توفر خدمة الدخول إلى خدماتها الرئيسية من خلال تطبيقات عن طريق المواقع الإلكترونية web-based؛ هذا النوع من الدخول ينشأ ثغرات أمنية جديدة، لأنه حتى مع وجود الجُدر النارية وأنظمة المراقبة الأخرى، فالأمن ممكن أن يُخترق؛ حيث أن سير البيانات يجب أن يكون مسموحاً له العبور من خلال الجدر النارية. والهدف من هذا الاختبار هو تقييم التحكم بالتطبيقات وجريان عملياتها.

موضوعٌ مهم يجب أن يقيم كذلك، ألا وهو استخدام التشفير لحماية السرية وتكامل البيانات، وكذلك كيفية التأكد من هوية المستخدم وضمان تكامل البيانات المنقولة بين المستخدم والتطبيق على الجهاز الخادم في المنظمة من خلال الإنترنت.

٢. اختبار حجب الخدمة "DoS":

الهدف من هذا الاختبار هو تقييم قابلية النظام لتحمل الهجوم الذي سوف يمنعه من تقديم الخدمة للآخرين حيث أنه إذا تمت عملية حجب الخدمة، فسوف تمنع جميع عمليات أو محاولات الدخول على النظام.

٣. اختبار حرب الإتصال " War Dialing":

اختبار حرب الاتصال هي طريقة أو تقنية لعمل اتصال نظامي على مجموعة من خطوط الهاتف داخل المنظمة، وفي ذلك محاولة لتعريف المودمات أو أجهزة الدخول البعيد ومن ثم عمل اتصال مع كمبيوترات تكون موصولة على شبكة المنظمة؛ حُسن النية عند بعض المستخدمين داخل المنظمة، قد يجعل شبكة المنظمة عرضة للثغرات الخطيرة باستخدام هذه التقنية، من غير

أخذ الحيطة اللازمة. وعندما يتم تعريف المودمات أو أي أجهزة تسمح بالدخول البعيد، تتم من بعدها عملية التحليل باستخدام بعض التقنيات لعمل الدخول الغير مسموح به ومن ثم يتم اختراق نظم معلومات المنظمة.

ج. اختبار اختراق الشبكة اللاسلكية:

وجود الشبكات اللاسلكية بالطرق النظامية أو عن طريق حسن النية من قبل المستخدمين، يُوجد لدينا هتك جديد لأمن المنظمة. بعض الأحيان يطلق مسمى سيارة الحرب "War Driving" على هذا النوع من الاختراق.

الهاكرز أصبحوا أكثر مهارة في تعريف الشبكات اللاسلكية وكشفها وذلك بقيادة السيارة أو حتى المشي حول المباني أو المكاتب مستخدمين أجهزة الشبكات اللاسلكية. والهدف من هذا الاختبار هو تعريف الفجوات الأمنية أو الأخطاء التي عُملت في تصميم أو تنفيذ وتشغيل شبكات لاسلكية داخل المنظمات.

د. اختبار اختراق الهندسة الاجتماعية "Social Engineering"

عادة يكون هذا الاختبار مرتبطاً باستراتيجية اختبار العمى أو اختبار العمى المضاعف؛ وهو يشير إلى التقنيات المستخدمة في التواصل الاجتماعي ويكون في الغالب مع موظفي المنظمة أو المزودين أو المتعهدين أو غيرهم ممن له علاقة مباشرة بأنظمة المنظمة، والهدف من هذا الاختبار هو الحصول على المعلومات التي من خلالها يتم اختراق أنظمة المنظمة. ومثل هذه التقنيات تحتوي على التالي:.

- انتحال شخصية موظف الدعم الفني في المنظمة ومن ثم طرح الأسئلة على المستخدمين، ومثال تلك الأسئلة: سؤال المستخدم عن معلومات الحسابات – الكلمات السرية – التي يستخدمها في الدخول على الأنظمة.
- انتحال شخصية الموظف ومن ثم الدخول على مناطق عالية الحساسية والتي تحتوي على الأنظمة، حيث أن هذه الأنظمة محمية بواسطة موظفي الأمن داخل المنظمة.
- اعتراض الرسائل داخل المنظمة أو حتى اعتراض الموظف المراسل أو كذلك البحث في قمامة ومخلفات المكاتب عن معلومات حساسة تم طباعتها.

اختبار الهندسة الاجتماعية يختبر الأمور الفنية بشكل قليل، ولكنه يعادل في أهميته الاختبارات الأخرى لما قد يعرض المنظمة من مخاطر وثغرات قاتلة في أنظمتها.

هل الجدر النارية FIREWALLS وأنظمة كشف التطفل IDS كافية:

معظم المنظمات تمتلك تقنيات أمنية معقدة مثل الجدر النارية أو أنظمة كشف التطفل، وذلك لتساعدها في حماية معلوماتها وسرعة التعرف على الهجمات الخفية. وحيث أن هذه التقنيات مهمة جداً إلا أنها غير آمنة ١٠٠%. وذلك لأن الجدر النارية

غير محمية مما هو مسموح الدخول عليه مثل التطبيقات ذات الدخول المباشر ON LINE أو أي خدمات أخرى مسموح الوصول إليها داخل المنظمة. وكذلك بالنسبة لأنظمة كشف التطفل ليس باستطاعتها كشف ما ليس مبرمجاً فيها لكشفه والتعرف عليه، وهي لن تكون فعالة إن لم تكن الشركة تمتلك نظام مراقبة ورد سريع على التنبيهات التي تصدر من هذه الأنظمة.

الجدر النارية وأنظمة كشف التطفل لن تكون ذات جدوى ونفع إن لم تكن تُحدث باستمرار بآخر التحديثات والإصدارات لها وإلا سوف تفقد فاعليتها في كشف ومنع الهجمات الخطرة على أنظمة المنظمة.

واستخدام اختبار الاختراق سوف يثبت مدى فاعلية ما قامت به المنظمة من عمل التحصينات باستخدام هذه الأنظمة والتقنيات.

شبكتي آمنة:

كثير من المنظمات تقول أن شبكاتها آمنة، لماذا احتاج إنفاق الكثير من المال لعمل فحص لأمن شبكتي وهو غير لازم، ولماذا ولماذا ولماذا . . . ؟ الجواب بسيط جداً . . . هو عدم الأمن. قد يعتقد الشخص أنه آمن، ولكن في معظم الأحيان تجد الشركات ومن أول اختبار أو اختراق لها بأن معظم بياناتها الشخصية والسرية عرضة للفصح أو أنها قد فضحت.

كان الناس قبل أحداث ١١ سبتمبر تعتقد أن الدول حصينة من الداخل وأن عندها التحكم الكامل لما تملك وقد ثبت غير ذلك. وعليه فإنه لا يوجد شيء آمن وهذا ينطبق على الأشخاص، المنظمات وحتى على الدول نفسها. من هنا يأتي الحرص على عمل أنظمة توفر الأمن بشكل كبير من جميع النواحي.

"ينطبق وصف النعامة التي تضع رأسها في التراب على من يقول أن شبكته آمنة"

بعض البرامج التي تستخدم في اختبار الاختراق:

فيما يلي مجموعة مهمة من البرامج المجانية والتجارية المستخدمة في اختبار الاختراق.

☒ Nessus : www.nessus.org

برنامج لمسح الشبكة وكشف الثغرات فيها، يستخدم مع نظام يونكس.

☒ Sara : www.arc.com/sara

برنامج كذلك لمسح الشبكة وكشف الثغرات فيها.

☒ Hping : www.kyuzz.org

برنامج يستخدم لإرسال رزم " packets " من نوع ICMP, UDP, TCP . ويسمح باختبار قوانين الجدر النارية ويدعم اختبار الرزم المجزئة.

☒ Firewalk : www.packettactory.net

أداة تستخدم لخرق قوائم تحكم الدخول "ACL" من خلال الجدر النارية ويعطي الإمكانية لرسم خريطة الشبكة.

☒ John The Ripper : www.openwall.com/John

أداة تستخدم لكسر كلمات السر.

☒ Crack/Libcrack : www.vsers.dircon.co.uk

أداة تستخدم لكسر كلمات السر وتستخدم مع نظام يونكس.

☒ Toneloc. :

أداة تستخدم في حرب الاتصال WarDialing حيث تقوم بعمل فحص للمودمات الموضوعة على وضعية الرد الأتوماتيكي.

☒ Internet Security Server : www.iss.net

برنامج تجاري رائع يستخدم من قبل معظم شركات اختبار الاختراق ويستخدم لكشف الثغرات. .

☒ Cybercop: www.10pht.com

برنامج تجاري جيد، يستخدم في كشف الثغرات الأمنية.

☒ Phone sweep : www.sandstorm.net

برنامج حرب الاتصال War-Dialer ويستخدم لكشف الأنظمة المستخدمة للمودمات بغرض الدخول البعيد.

☒ NMAP : www.nmap.org

برنامج رائع لكشف وعمل خريطة الشبكات من خلال الجدر النارية.

☒ Ethereal: www.ethereal.com

برنامج يقوم بتحليل بروتوكولات الشبكة حيث يقوم بشم محتواها من خلال اتصال الجهاز الذي نُصّب عليه هذا البرنامج بها. ويعمل مع ويندوز ولينكس.

خـــــــاتمـــــــــة:

من المهـم الإشـارة، أن اختبـار الاختـراق لا يمكنه التنبوء أو كشف جميع الثغـرات الأمنية في الأنظمة، وكذلك لا يمكنه أن يعطي الضمانات للمنظمات بأن معلوماتهـم وأنظمتها آمنة، حيث أنه يعمل في وقت محدود ومعين. التقنيات الجديدة وأدوات الهاكرز الجديدة والثغرات في نظم معلومات المنظمات ينشأ هتكاً وخطراً لم يكتشف أثناء القيام باختبار الاختراق. ويزاد عليه، أن الاختبار قد تم على منطقة معينة من المنظمة، وتم في فترة معينة من الزمن ومع وجود مصادر معينة. وكذلك اختبار الاختراق في أغلب الأوقات يركز على كشف الثغرات الأمنية التي قد تسمح بدخول الأشخاص الغير مصرح لهم، وليس من الضروري أن يحسب حاسب الثغرات الأمنية التي قد تحدث بشكل عرضي أو بخطأ مستخدم أو غير ذلك. وعليه فان توفير أمن المعلومات بشكل كبير للمنظمات يحتاج إلى تضافر جهود جميع الأطراف في المنظمة من حراس الأمن إلى أعلى مسؤول في المنظمة.

يجب أن لا ينسى المرء أنه لا يوجد نظام أمن ١٠٠%.

مواقع وارتباطات تعتبر مراجع في أمن المعلومات:

- آخر أخبار أمن المعلومات.
  - http://www.Incidents.org
  - http://www.theregister.co.uk
  - http://www.silicon.com
  - http://www.security-protocols.com/index.php
- الثغرات الجديدة.
  - http://www.cert.org/nav/index_red.html
  - http://www.microsoft.com/security
  - http://www.ciac.org/ciac/bulletinsByType/bul_vendor_list.html
- استشاريين.
  - http://www.cisco.com/en/US/products/products_security_advisories_listing.html
  - http://www.nsa.gov/snac/
- معلومات الجدر النارية.
  - http://www.snort.org
- الهاكرز.
  - http://www.webstore.fr/webabonnes/tahiti/nt.htm
  - http://www.cavebear.com/CaveBear/Ethernet/vendor.html

- TCP ports.
  - http://www.chebucto.ns.ca/~rakerman/port-table.html
  - http://www.iana.org/assignments/port-numbers
  - http://www.tsmservices.com/masq/
  - http://www.stengel.net/tcpports.htm

REFERENCES

[1]- Dave Burrows, "Introduction to becoming a Penetration Tester", SANS Institute, part of the Information Security Reading Room, June,2 2003.

[2]- Clark Weissman, "SECURITY PENETRATION TESTING GUIDELINE", A Chapter of the Handbook for the Computer Security Certification of Trusted Systems, Dec,1 1992.

[3]- Dominick Baier, "Improving Application Security through Penetration Testing", Oct,10 2004.

[4]- Gary McGraw, "Software Penetration Testing", Dec, 17 2004.

[5]- Jessica Lowery," Penetration Testing: The Third Party Hacker", SANS Institute, As part of the Information Security Reading Room, Feb, 2002.

[6]- Mount Ararat Blossom, "FIREWALL PENETRATION TESTING", Nov, 20 2000.

[7]- Deborah D. Downs and Ranwa Haddad, "Penetration Testing – The Gold Standard for Security Rating and Ranking", The Aerospace Corporation 2350 E. El Segundo Bl., March 2001.

[8]- Cynthia E. Irvine, "Security: Where Testing Fails", Department of Computer Science, Naval Postgraduate School, Monterey, CA 93943, April, 9 2000.

[9]- Andrew J Clrak and john R Sherwood, "Security Auditing A Methodology", July, 26 1998.

[10]- VeriSign White Paper, "An Introduction to Network Vulnerability Testing", March, 13 2003.