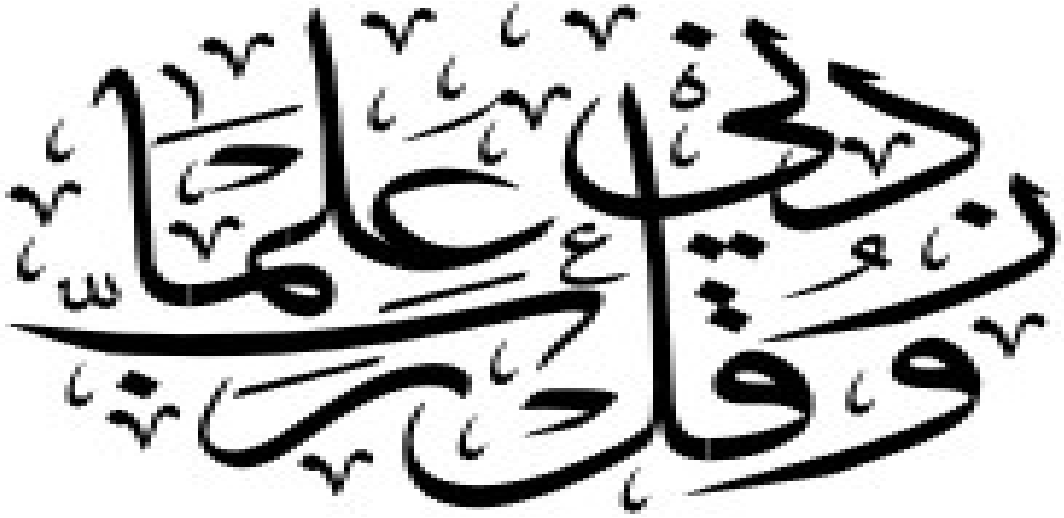
آيــة

بسم الله الرحمن الرحيم



صدق الله العظيم

(سورة طه 114)

الإهداء

اهدي هذا العمل المتواضع إلي من ربياني صغيرا أمي وأبي ،،،

وإلي :

إخواني وأخواتي ،،،

الأهل الأعزاء ،،،

الأساتذة الكرام ،،،

الأصدقاء الأوفياء ،،،

الشكر والعرفان

الشكر أوله وأخره لله عز وجل ومن بعده لرسوله الكريم سيد الخلق أجمعين سيدنا وحبيبنا محمد صلي الله عليه وسلم ولأصحابه إلي يوم الدين وبعد ،

ومن ثم إلي جامعة السودان للعلوم والتكنولوجيا والي جميع أساتذتها الأجلاء وبالأخص الدكتور عوض محمد عوض الكريم الذي افخر واعتز بأن يكون هو من اشرف علي هذا العمل ، ولولا جهده وصبره لما كان ،،،

أخيرا وليس أخرا الشكر لكل الزملاء دراسة أو عمل ،،،

Abstract

With the growth of the Internet service, has become necessary to protect the information available and how to reach them since the

protection of computer has become one of concerns needed to manage businesses and governments as well as in many other areas, so the desire to benefit from the advantages of the Internet for electronic commerce, advertising, information distribution and access, but they are worried about the possibility of being hacked of information available.

This research presents the concepts of breach of ethical hacking and penetration testing, and then list the steps the framework represents the basic steps carried out by ethical hacker to perform the test, then apply and proposed framework in practical terms in a virtual environment was reached Results can be applied in a corporate environment and institutions for achieving the security required.

المستخلص

نسبة لازدهار خدمة الانترنت وتوسعها أصبح من الضروري حماية المعلومات المتوفرة وطريقة الوصول إليها حيث أن حماية الحاسوب أصبحت من الاهتمامات الضرورية لإدارة الأعمال والحكومات وكذلك في مجالات كثيرة أخري ، لذلك تكون الرغبة في الاستفادة من محاسن الانترنت من خلال التعامل بالتجارة الالكترونية والإعلانات والوصول للمعلومات الموزعة في الانترنت. لكن البعض يبدي قلقه حول إمكانية اختراق المعلومات المتوفرة.

يعرض هذا البحث مفاهيم الاختراق الأخلاقي واختبار الاختراق ومن ثم سرد لخطوات إطار عمل يمثل الخطوات الأساسية التي يقوم بها المخترق الأخلاقي لأداء الاختبار، ثم تطبيق إطار العمل المقترح بشكل عملي في بيئة افتراضية وتم التوصل لنتائج يمكن تطبيقها في بيئة الشركات والمؤسسات لتحقيق السرية المطلوبة.

فهرس الأشكال

19.5	.(يوضح (نجاح عملية الاستغلال واختراق الجهاز الهدف	50

فهرس المحتويات

الباب الرابع

إطار العمل المقترح

الباب الخامس

تطبيق إطار العمل المقترح

الباب السادس

الخلاصة والتوصيات

المصطلحات

1- التهديد **(Threat)** :

هو عبارة عن أحداث او أنشطة يحتمل ان تضر بأنظمة المعلومات او الشبكة (Networks).

2- الثغرات (vulnerabilities):

هي عبارة عن ضعف في الحماية يمكن استغلالها بواسطة التهديد(Attack) ،تؤدي الي ضرر في نظم المعلومات والشبكات وتكون موجودة في العتاد (Hardware) ونظم التشغيل (Operating Systems) والتطبيقات (Applications) .

حيث ان مصطلح الثغرة الأمنية يطلق على مناطق ضعيفة في أنظمة تشغيل الحاسوب مثل ويندوز(Windows) ، هذه المناطق الضعيفة يمكن التسلل عبرها إلى داخل نظام التشغيل ، ومن ثم يتم التعديل فيه لتدميره نهائيا مثلا ، أو للتجسس على المعلومات الخاصة لصاحب الحاسوب المخترق ، أو ما يعرف بجهاز الضحية.

3- المخاطر (risks):

هي احتمالية الأضرار او فقدان لأنظمة المعلومات او الشبكة وهي علي الأغلب تتجسد في شكل تهديد (Attack).

4- الهجوم (Attacks):

هي أحداث ضد نظم المعلومات او الشبكات وهي محاولة لخرق سياسات نظم المعلومات ،وهي دائماً نتيجة للتهديدات.

5- الاستغلال (Exploits)

معني الاستغلال هو ضعف او ثغرة في نظم تقنية المعلومات (IT) لخرق نظم السرية.

6- المخترق (Hacker)

هو عبارة عن شخص خبير في نظم الحاسوب يميل تفكيره دائماً إلي الفضول ويرغب في تعلم الكثير حول أنظمة الحاسوب.الشخص الذي يكون مخترق يكون مطور ومحسن للبرمجيات لزيادة الأداء لنظم الحاسوب.

أو هو شخص يحاول تحطيم أنظمة الآخرين بخلفية برمجية جيدة أو معرفة وخبرة كبيرة في مجال الأعمال الإلكترونية. وهو يدظم معرفته للقيام بمحاولات كشف وتعريف الأخطاء البرمجية والثغرات الأمنية واستخدامها لتخريب الأنظمة أو لأهداف خبيثة أخرى.