بسم الله الرحمن الرحيم

Sudan University Of Science and Technology
College of Graduate Studies

Development and Implementation of Honeypot System

تطوير نظام جرة العسل و تطبيقه

Thesis Submitted in Partial Fulfillment of Requirements for the Degree of M.Sc in Computer Engineering

Prepared By:
Mohamed Mahgoub AbdAlla

Supervisor:
Dr. Yahya AbdAlla

July 2009

Dedication

To My Parents,
To My Wife And Childes,
To All System Administrators,

I dedicate this work.

الايـــــــــــــــه

﴿ اللّهُ لاَ إِلَـــهَ إِلاّ هُوَ الْحَيُّ الْقَيِّومُ لاَ تَأْخُذُهُ سِنَةٌ وَلاَ نَوْمٌ لّهُ مَا فِي السَّمَاوَاتِ وَمَا فِي الأَرْضِ مَن ذَا الّذِي يَشْفَعُ عِنْدَهُ إِلاّ بِإِذْنِهِ يَعْلَمُ مَا بَيْنَ أَيْدِيهِمْ وَمَا خَلْفَهُمْ وَلاَ يُحِيطُونَ بِشَيْءٍ مّنْ عِلْمِهِ إِلاّ بِمَا شَاء وَسِعَ كُرْسِيُّهُ السَّمَاوَاتِ وَالأَرْضَ وَلاَ يَؤُودُهُ حِفْظُهُمَا وَهُوَ الْعَلِيُّ الْعَظِيمُ ﴾

سورة البقرة الآية 255

ACKNOWLEDGEMENT

I'm very grateful to Dr. Yahia AbdAllah for providing me with unwavering support . I also wish to thank Mr Khaled Bashere for his great advices. Finally I wish to thank my colleagues for theire assistance.

Abstract

In networking there is an ongoing war between security managers and crackers, each new day those crackers develop new techniques and technologies to achieve their goals of hacking our systems, and since they stay in the shadow its impossible for the security managers to know about them ,their tools and goals.
But this is changing , with the rise of HoneyPots technologies administrators could learn about their enemies tactics and motivations, which will definitely help achieving a better security level.
The value of HoneyPots and how could they be used is the main area that this study will show, types of HoneyPots available today will be covered and the way to implement them will be discussed, it will also show the draw backs of the current available network protection tools, and how HoneyPots could be used in order to fulfill the gaps they have.
A new technique will be discussed , this new model will mix HoneyPots with real production systems in order to achieve a greater success in fooling the hackers into the HoneyPot trap,and then study them carefully.
This model has been implemented and installed into the severs which have internet access to them ,a new logging mechanism have logged all of the information of different attacks to the honeypots system, this data was analyzed and and summary reports were generated.

مستخلص

في عالمنا اليوم هنالك معركة مستمرة بين المشرفين علي النظم و الشبكات و بين المخترقين الذين يحاولون الوصول الي هذه النظم, و مع التطور الدائم في التقنيات و الادوات التي يستخدمها المخترقين اصبحت عملية حمايتها صعبة و شبه مستحيلة.
ولكن يمكن اليوم و باستخدام تقنية "جرة العسل" العمل علي تغيير هذا الواقع, و ذلك بالحصول علي الكثير من المعلومات و البيانات عن المخترق للنظام أو الشبكة مما يساعدنا علي رفع درجة الحماية الخاصة بنا.
سنقوم في هذه الدراسة بتوضيح الانواع المختلفة ل "جرة العسل" و كيف يمكن لنا باستخدامها و معرفة من يحاول الاختراق , ما هي الادوات التي يستخدمها و ما هي المقاصد الحقيقية من وراء هذا الاختراق, كما ستوضح بعض نقاط الضعف الموجودة في انظمة الحماية الحالية المعروفة مثل الجدار الناري و كيف يمكن الاستفادة من تقنية "جرة العسل" لتقوية و دعم نقاط الضعف هذه.
كما ستظهر هذه الدراسة طريقة مستحدثة لتمويه "جرة العسل" و ذلك بدمجها مع الانظمة الحقيقية حتي يكون من المستحيل اكتشافها من قبل المخترقين و بذلك نكون قد زدنا من مستوي نجاحها في جذب المخترقين اليها و الحصول علي أكبر قدر ممكن من المعلومات عنهم.
تم تنفيذ النظام المقترح و تثبيته علي اجهزة لديها امكانية الدخول الي شبكة الانترنت , حيث قامت الية مخصصة بسجل الدخول بعملية تسجيل جميع عمليات الدخول الي النظام. و من ثم اوضحت الية التحليل مجموعة البيانات التي تم تسجيلها في النظام.