جـامعـة المـوصـل
كلية علوم الحاسوب والرياضيات

تصميم وتنفيذ جرة عسل الزبون

نجوان زهير ويسي التحافي

رسـالة ماجستير
علـوم الحاسـوب

بإشراف

د. نجلاء بديع إبراهيم الدباغ

أستاذ مساعد

١٤٣٥هـ ٢٠١٤م

الخلاصة

أصبح مستخدمو الحاسوب من الزبائن في السنوات القليلة الماضية الهدف الرئيس للهجمات، إذ يعتقد المهاجِم أن المستخدم النهائي هو أضعف حلقة في السلسلة الأمنية، لذا أصبحت مصائد مخترقي الشبكات التقليدية وأدواتها الأمنية غير فعالة ضد هذه الهجمات الجديدة، ومن ثم فقد ظهرت جرة العسل الزبون بوصفها تقنية جديدة تكمّل أدوات الحماية الحالية. وتعد جرة العسل الزبون وسيلة تشبه الشرك تستهدف الإيقاع بالمواقع الضارة على شبكة الإنترنت.

تهدف الرسالة إلى استعراض لجميع أنواع جرة العسل، و تصميم جرة عسل الزبون وتنفيذها للكشف عن مواقع الويب الخبيثة من نوع بروتوكول نقل الملف (File Transfer Protocol :FTP) والتي لها القدرة على الكشف عن أنواع متعددة من ملفات فيروس حصان طروادة المعروفة، إذ يتم بناء قاعدة بيانات لبصمات متنوعة من أنواع فيروس حصان طروادة والتي تمكن من كشف أنواع كثيرة من الفيروس الذي يكون متواجدا داخل مواقع ويب نوع FTP وتقديم دراسة لخصائصه وبعض سلوكياته.

جرة عسل الزبون المقترحة اعتمدت نوعي التحليل الثابت والمتحرك (Static And Dynamic Analysis). يتمثل التحليل الثابت باستخدام تقنية البصمة واستخدام أدوات الهندسة العكسية المتمثلة بالأداة (Ollydbg) لتحليل ملفات الفيروسات. أما التحليل المتحرك فاعتمد تقنية فحص سجلات نظام التشغيل (Registry) بعد تنفيذ الفيروس.

وأظهرت النتائج أنه يمكن استخدام جرة العسل المقترحة في فحص الملفات الموجودة في أي مزود خدمة FTP، وتمييزها إذا كانت خبيثة أو حميدة. كما إن استخدام خوارزمية (Boyer-More) المستخدمة في تقنية البصمة أعطت سرعة تنفيذ مختلفة خصوصا للتواقيع الطويلة فضلا عن أن استخدام أدوات الهندسة العكسية أعطت تحليلا دقيقا لملف البرنامج الخبيث.

University of Mosul
College of
Computer Sciences And Mathematics

Design and Implementation of Client Honeypot

Najwan Zuhair Waysi Al-Tuhafi

M.Sc./Thesis
Computer Science

Supervised By

Dr. Najla Badie Ibraheem Al-Dabagh
assistant professor

2014 A.D. **1435 A.H.**

Abstract

Recently , client user became the main target for attacks and attackers as well, that fact the knowing the adversary believe that the end user is the weakest link in the security chain. Traditional honeypots and security tools are not effective against these new attacks. Therefore, client honeypot has appeared as new technology to supplement the existing protection tools. Client honeypot is a honeypot actively searches for malicious sites on the web.

The thesis aims to investigate comprehensively all Honeypots types also design and implementing a client Honeypot to detect FTP malicious websites .The honeypot designed in this study has the ability to detect multiple types of known Trojan horse virus files. A signature database of various types of Trojan horse viruses was built to detect many types viruses located within the FTP Websites to study their properties and some of their behaviors .

The proposed client honeypot adopted both Static and Dynamic Analysis techniques . The Static analysis is based on the fixed signature technique and reverse engineering tools (the Ollydbg tool in this study) to analyze the virus files . The Dynamic analysis technique based on checking the operating system's Registry files after running the virus. The results showed that the proposed honeypot can be used to check the files in any FTP service provider and it is capable of distinguishing between the malicious and benign files. The use of the (Boyer-More) algorithm in the signature technique resulted in high implementation speed of especially with long signatures when compared with the other matching algorithms while the reverse engineering tools resulted in a thorough analysis of the malicious program file.