УДК 04.56.

Г.А. Жакун
В.В. Лукічов

ШТУЧНЕ СЕРЕДОВИЩЕ СИСТЕМИ ВИЯВЛЕННЯ АТАК З ВИКОРИСТАННЯМ HONEYPOT

Вінницький національний технічний університет

Анотація
Проаналізовано Honeypot та представлено розробку штучного середовища для Honeypot.
Ключові слова: Honeypot, Honeypots

Abstract
Honeypot is analyzed and the development of an artificial environment for Honeypot is presented.
Keywords: Honeypot, Honeypots

Вступ

В нинішній час доволі часто проводять Bruteforce атаки і взлам пароля з допомогою соціальної інженерії. Тому є необхідність мати можливість вивчити слабкі місця систем захисту.

Honeypot – це комп‘ютерна система, яка створена для того, щоб заманювати кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Еволюцію Honeypots можна побачити не озброєним оком, поглянувши на те, як ці системи використовуються разом із IDS для запобігання, виявлення та реагування на атаки. Дійсно, Honeypots все частіше знаходить своє місце поряд з мережевими і хост-системами захисту від вторгнень.

Дозволяючи зловмисникам взаємодіяти з реальними системами, можна вивчити та зафіксувати повний рівень їхньої поведінки. [1]. Honeypot з високою взаємодією може бути фізичною системою, але також може бути реалізований як віртуальна машина [2, 3], і для збору найбільш релевантних даних вони зазвичай передбачають використання тих самих операційних систем і служб, які є. в організації, яка розгортає Honeypot. Як наслідок, організація, яка використовує робочі станції Windows і сервери Linux, ймовірно, розгорне пристосування на базі Windows і Linux. Для того, щоб фактично фіксувати поведінку зловмисника в таких середовищах, також має бути присутнім деяка додаткова система моніторингу, наприклад, перевірка пакетів на рівні мережі або, частіше, як програма на самому хост Honeypot, що є підходом. використовується інструментом збору даних Sebek [4].

Результати дослідження

Honeypot доволі часто можуть виявити як на сервері так і на персональному комп’ютері після чого зловмисник вже не підключається до такого порту або машини і спрямовує атаки на інші частини системи захисту. Для прикладу було вибрано статичні Honeypots які зазвичай відкривають послуги сервера та чекають на атаку зловмисник відправляє певні повідомлення та по отриманим даним розуміє що це Honeypots.

Honeypots, незалежно від того, чи є вони високою чи низькою взаємодією, дозволяють адміністраторам виявляти аномалії, які інакше могли б залишитися непоміченими. Оскільки Honeypots не мають виробничої цінності, будь-яка взаємодія всередині машини може бути або скануванням перед атакою, або потенційною атакою. Це дозволяє системному адміністратору націлювати й аналізувати журнали, створені системою Honeypot, без необхідності визначати, який трафік є підозрілим, а який законним, як це було б під час аналізу журналів із виробничих систем.

Рисунок 1 – Блок-схема роботи штучного середовища.

На рисунку 1 показано роботу штучного середовища для системи виявлення атак для моніторингу є можливість використання різних програм які присутні на ринку. В додаткові функцій можна віднести:

- Додавання вірусного ПЗ
- Штучних файлів
- Штучний захист
- Скопійований захист
- Моніторинг трафіку
- Створення під системи Honeypot

Ряд даних функцій дасть можливість додатково вийти на зловмисника також функцій моделювання захисту дасть можливість знайти слабкості а бо помилки нульового дня. Також є можливість розшити можливості Honeypot якщо створити зв'язок між Honeypot та внутрішньою системою підприємства та дати можливість розкрити даний зв'язок зовні що спровокує зловмисників шукати слабкості в Honeypot для можливості зламу, що в свою чергу дасть можливість дослідити методи та атаки зловмисників.

Висновки

В даній статі було розглянуто Honeypot та його види також було представлено блок схема роботи штучного середовища з можливістю адаптування до різних систем та задач. Ефективний Honeypot повинен окрім можливості досліджувати також створювати приманки і підстроюватися та змінюватися під різні системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Iyad Kuwatly, Malek Sraj, Zaid Al Masri, and Hassan Artail. A Dynamic Honeypot Design for Intrusion Detection, American U. of Beirut. 2004.
2. Quynh, Nguyen Anh. Xebek: A next generation honeypot monitoring system. EUSecWest/core06, London, U.K., Feb 2006.
3. Know Your Enemy: Learning with VMware. Building Virtual Honeynets using VMware. Retrieved April 18, 2006 URL: http://www.honeynet.org/papers/vmware/
4. Sebek Homepage. The Honeynet Project. Retrieved February 15, 2006 URL:http://honeynet.org/tools/sebek/.

Жакун Геннадії Андрійович – студент групи 1БС-20м, факультет інформаційних технологій та комп'ютерної інженерії, кафедра ЗІ, Вінницький національний технічний університет, м. Вінниця, email: gena0537@gmail.com

Науковий керівник: ***Лукічов Віталій Володимирович*** – кандидат технічних наук, старший викладач кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Zhakun Hennadii – student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: gena0537@gmail.com

Vitaliy Lukichov – PhD (Eng), Senior Lecturer of Information Protection Department, Vinnytsia National Technical University, Vinnytsia.