Мониторинг вредоносной активности через SSH

Автор: Попов Кирилл
Научный руководитель: Зеленчук Илья

Санкт-Петербургский государственный университет.
Математико-Механический факультет, кафедра Системного Программирования
2013

Цели

1. Провести анализ вредоносной активности через SSH.
2. Не допустить использование исследуемого сервера в качестве узла атаки.
3. Не допустить нанесение вреда серверу, на котором проводится исследование.

Задачи

- провести анализ существующих решений, если таковые имеются;
- разработать средство мониторинга вредоносной активности;
- провести анализ полученных данных;

Анализ Honeypot шелов

Название: Kippo

URL: http://code.google.com/p/kippo/

Язык программирования: Python

OpenSource: Да

Ложная файловая система: Да

Сохранение скаченных файлов: Да

Анализ Honeypot шелов

Название: Kojoney

URL: http://kojoney.sourceforge.net/

Язык программирования: Python (opt. Perl)

OpenSource: Да

Ложная файловая система: Неизвестно

Сохранение скаченных файлов: Неизвестно

Особенности:

- Умеет отличать людей от ботов.

Анализ Honeypot шелов

Название: Honeypot-ssh

URL: http://code.google.com/p/honeypot-ssh/, https://www.truecode.com.au/pages/sshhoneypot, http://au.hive.sshhoneypot.com/download.php

Язык программирования: C++

OpenSource: Да

Ложная файловая система: Неизвестно

Сохранение скаченных файлов: Неизвестно

Особенности:

- умеет отличать людей от ботов;

Проблемы

- защита программы мониторинга активности от обнаружения;
- выбор способа мониторинга активности;
- защита исследуемого сервера от взлома;

Способы ведения мониторинга активности

1. Модификация шелла.
2. Модификация OpenSSH сервера.
3. Мониторинг tty.

Программа для мониторинга

- язык программирования C;
- работает как демон;
- проводит мониторинг tty;
- использует подсистему Linux inotify для слежения за /dev/pts;
- может логгировать действия только определенной группы пользователей;

Защита сервера

- помещение вошедших пользователей в chroot;
- настройка chroot окружения;
- правильное конфигурирование OpenSSH;

Промежуточные итоги

- Программа для мониторинга работает на действующем honeypot'e.
- ≈588 попыток авторизации в день.
- Были выявлены и устранены ряд критических уязвимостей свзяанных с безопасностью (спасибо Соболеву Артему из 344гр).
- Получены первые образцы rootkit'ов.