Код безопасности
ГК «Информзащита»

127018, Москва, а/я 55; т./ф.: (495) 980 23 45
e-mail: market@infosec.ru, web: www.securitycode.ru

Security Studio Honeypot Manager

Введение

Компания «Код Безопасности» представляет сертифицированное средство защиты Honeypot Manager.

Система Honeypot Manager — это программный комплекс, предназначенный для обнаружения несанкционированного доступа к данным в имитируемой с помощью специальных ловушек СУБД Oracle. Honeypot Manager позволяет выявлять нарушителей в локальной вычислительной сети предприятия и анализировать их действия без снижения производительности реальных систем хранения данных — на имитационной системе вы можете включить полный аудит и не опасаться проблем с оперативным доступом пользователей к данным. Также снижается и риск потери реальных данных, так как данные, хранящиеся на имитационной системе, могут быть произвольными.

Возможности продукта

Основная задача системы — регистрация действий злоумышленника и сигнализация о них с целью нейтрализации угрозы получения доступа (чтение, копирование) к реальным данным на реальных системах хранения данных.

Honeypot Manager позволяет сымитировать систему хранения данных с помощью специальных ловушек (сенсоров), отслеживает активность на имитируемой СУБД Oracle и уведомляет о фактах НСД к имитируемым персональным данным, хранящимся в базе данных.

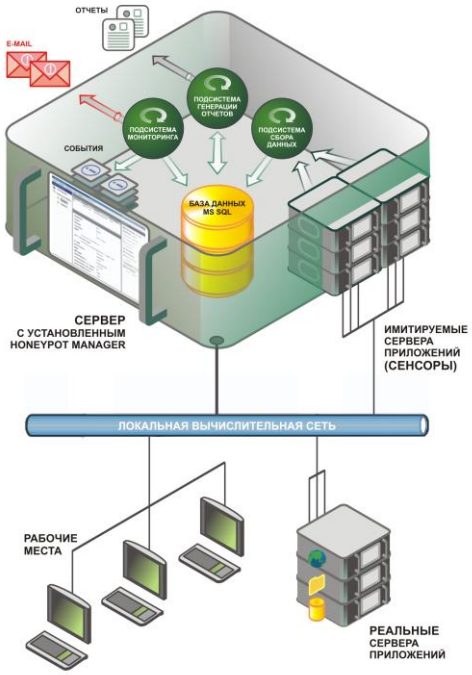
Таким образом, администратор безопасности владеет информацией о том, кто пытается получить доступ к системе и пытается ли вообще, а также может определить перепутал ли сотрудник имя реального сервера и случайно попал на ловушку или действовал преднамеренно и в сети действительно есть нарушители, пытающиеся найти сервера или службы, работающие с данными, представляющими ценность для компании.

Основными функциями продукта являются:

- Обнаружение и регистрация фактов НСД к имитируемым данным;
- Оповещение заинтересованных лиц о попытках НСД к имитируемым данным;
- Имитация реальной системы хранения данных;
- Возможность восстановления модифицированной нарушителем системы к исходному состоянию;
- Генерация отчетов о работе системы за определенные периоды времени;
- Централизованное управление несколькими имитационными системами;
- Авторизация и контроль доступа к управлению системой;
- Механизм контроля работоспособности (диагностика);
- Возможность гибкой настройки правил реагирования на попытки НСД;
- Возможность генерации данных, близких к реальным;
- Возможность периодической смены IP-адресов имитационных систем.

Архитектура

Типовая схема решения выглядит следующим образом:



В состав системы входят следующие основные компоненты:

- **Консоль администратора** является основным органом управления системой. Предназначена для настройки системы и выполнения таких функций, как:
  - Создание и настройка сенсоров;
  - Резервное копирование и восстановление сенсоров;
  - Настройка правил реагирования;
- **Подсистема мониторинга** обеспечивает:
  - Регистрацию информации об активности средства Honeypot Manager и его компонентов в журнале событий Windows;
  - Реализацию оповещения ответственных лиц о фактах НСД и событиях, связанных с работоспособностью средства;
- **Подсистема сбора данных** предназначена для сбора данных аудита с сенсоров;
- **Подсистема генерации отчетов** предоставляет возможность формировать отчеты о произошедших на сенсорах за определенный период времени событиях. Для генерации и отображения отчетов используются службы Microsoft SQL Server Reporting Services;
- **Подсистема управления сенсорами** обеспечивает управление и работу с сенсорами, которые представляют собой виртуальные компьютеры;
- **База данных** содержит всю информацию о работе системы — событиях, произошедших на сенсорах, срабатывании правил, работе самой системы Honeypot Manager. Устанавливается на компьютер совместно с консолью администратора. Для хранения данных используется СУБД Microsoft SQL Server 2005 Express Edition;
- **Вспомогательные утилиты:**

- Утилита диагностирования служит для проверки настройки правил реагирования и уведомлений;
- Утилита перемешивания данных служит для внесения необратимых изменений в оригинальные данные в таблицах Oracle.

Требования к аппаратному и программному обеспечению

Продукт устанавливается на компьютер с операционной системой Microsoft Windows Server 2003 Standard или Enterprise Edition SP2, оснащенный процессором семейства Intel x86 или совместимым с ним.

Аппаратные требования:

Элемент	Требование
Процессор	Pentium 4 3,0 ГГц и выше, рекомендуется многоядерный
Оперативная память	Минимально: 1,3 Гбайт + 700 Мбайт на каждый сенсор Рекомендуется: 2,5 Гбайт + 800 Мбайт на каждый сенсор
Жесткий диск (свободное пространство)	Минимально: 12 Гбайт + 8 Гбайт на каждый сенсор
Сетевой адаптер	Ethernet, минимально 100 Мбит/с

Так как система довольно требовательна к ресурсам, рекомендуется установка Honeypot Manager на выделенный сервер.

Соответствие государственным требованиям

Сертификаты ФСТЭК	НДВ 4, ТУ	**ИСПДн ФСТЭК**	К1, К2, К3
АС ФСТЭК	1Г	**Гостайна**	–

Информацию о продуктах компании «Код Безопасности» можно найти на сайте www.securitycode.ru.

Код безопасности
ГК «Информзащита»

127018, Москва, а/я 55; т./ф.: (495) 980 23 45
e-mail: market@infosec.ru,