Министерство образования Республики Беларусь

ПОЛОЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра вычислительных систем и сетей

**Методические указания по выполнению лабораторной работы № 3 по курсу «Защита информационных ресурсов компьютерных систем и сетей»**

Обнаружение аномальной активности хоста

Старший преподаватель,

кандидат технических наук,

Раханов Константин Яковлевич

**Полоцк, 2014**

**Содержание**

[Теоретические сведения 3](#_Toc403637184)

[Цель работы 4](#_Toc403637185)

[Требования, предъявляемые к лабораторной работе 4](#_Toc403637186)

[Ход выполнения работы 4](#_Toc403637187)

[Содержание отчета 4](#_Toc403637188)

**Теоретические сведения**

Полноценная реализация системы обнаружения атак (типовая архитектура которой рассмотрена в лабораторной работе №2) требует наличие хостового сенсора аномальной активности. Хостовый сенсор – это программный агент, который ведет наблюдение за активностью хоста, на который установлен. Такой агент не запускается непосредственно для решения задачи, а активизируются самостоятельно при запуске операционной системы.

Целью хостового сенсора является слежение за всеми событиями, происходящими в компьютерной системе, и проверка их на соответствие модели безопасности. В то время, как сетевой сенсор отслеживает проходящие сетевые пакеты, хостовый сенсор проверяет, какая программа к каким ресурсам обращается и может обнаружить, что, например, текстовый процессор вдруг начал менять системную базу паролей. Хостовый сенсор просто ведет наблюдение за текущим состоянием системы, за хранимой информацией (как в оперативной памяти, так и в файловой системе), за данными системных логов и проверяет, насколько это состояние соответствует «нормальному».

Зафиксированные события безопасности на хосте сенсором передаются в анализатор, установленный на сервере безопасности. Анализатор определяет наличие или отсутствие аномальной активности. В случае обнаружения аномальной активности (атаки) анализатор отсылает команду в блок реагирования для оповещения администратора безопасности (средствами электронной почты, вывода сообщения на консоль или отправки на пэйджер) и блокирования пользовательских регистрационных записей, приложений и т.п. с целью немедленного прекращения атак.

Примеры событий безопасности, отслеживаемых хостовым сенсором:

* авторизация пользователя в операционной системе;
* авторизация пользователя в системных приложения (например, в панели управления межсетевых экранов, антивирусов и т.п.);
* авторизация в пользовательских приложениях (например, в базе данных, чатах, системах контроля версий и т.п.);
* доступ к файловой системе или отдельным файловым ресурсам;
* события безопасности операционной системы, которые ведутся в журналах операционной системы;
* запуск и выполнение приложений и служб;
* обращение приложениями и службами к определенным ресурсам;
* установка и настройка дополнительных устройств в системе (флэш-накопителей, модемов, дисков и т.п.);
* конфигурирования системных и пользовательских приложений;
* и другие.

**Цель работы**

Разработать систему обнаружения аномальной активности хоста, в состав которой входит сенсор и анализатор активности на хосте.

**Требования, предъявляемые к лабораторной работе**

Язык программирования: определяется студентом.

Алгоритм обнаружения и критерий аномальной активности на хосте: определяется студентом.

Обязательные компоненты, которые должны быть реализованы:

* хостовый сенсор для мониторинга событий безопасности на хосте. Хостовый сенсор должен быть реализован в виде программного агента (службы);
* анализатор событий для обнаруживает аномальной активности;
* модуль реагирования для уведомления о наличии аномальной активности либо блокировки ресурсов;
* модуль логирования.

**Ход выполнения работы**

1. Изучить теоретические сведения.
2. Выбрать технологию разработки, обосновать критерий анормальности хостовой активности, разработать структуру приложения.
3. Реализовать приложение для обнаружения аномальной активности на хосте.
4. Написать отчет о проделанной работе.
5. Защитить отчет.
6. Предоставить отчет и исходные коды приложения в архиве (формат архива: «ZIRKSiS\_Lab\_3\_IT-1\_Фамилия\_на\_транслите.zip»).

**Содержание отчета**

1. Титульный лист, содержащий пункты «Разработал», «Проверил».
2. Описания реализации приложения с листингом основных функций, скриншотами, демонстрирующими работу приложения.
3. Вывод о функционировании полученного приложения, содержащий СОБСТВЕННОЕ заключение о результатах работы приложения.