Аннотация к дипломной работе

Тема: «Разработка модуля ядра для аудита изменений файловой системы и реестра в операционных системах семейства Windows»

Исполнитель:

Руководитель: Головач А.Л., ассистент кафедры технологий программирования, Курбацкий Александр Николаевич, профессор, д.т.н.

Кафедра: Технологий программирования, специальность «Прикладная информатика», специализация «Программное обеспечение встроен
Объем работы: 48 страниц, 11 иллюстраций, 12 источников.

Ключевые слова: Аудит, драйвер, перехват, уровень ядра ОС, графический интерфейс.

Результат: Разработан программный комплекс, состоящий из двух частей – модуль перехвата операций, реализованный как драйвер в WDK и сервис Windows, и модуль анализа данных с графическим интерфейсом, реализующий по различным шаблонам поиск подозрительных операций среди всех операций, происходящих в системе.

ЗАКЛЮЧЕНИЕ

В работе исследована проблема сбора полной информации о событиях, происходящих в системе и анализа собранных событий с целью расследования инцидентов.

Теоретической частью дипломной работы стало, во-первых, изучение существующих решений в области контроля за состоянием операционной системы, их возможностей, архитектуры, преимуществ и недостатков. По результатам этого исследования приведен краткий обзор.

Второй важной частью теоретической работы было изучение методов разработки аналогичных решений, в частности, использование технологий Windows Driver Kit, возможностей и средств, предоставляемых этим программным обеспечением.

Основная практическая часть дипломной работы состоит из двух главных компонентов.

Первый компонент отвечает за сбор и сохранение информации обо всех событиях, происходящих в операционной системе, и изменяющих её состояние. Среди таких событий можно выделить изменение файловой системы, реестра, создание и завершение процессов, открытие и закрытие сетевых соединений. Для сбора используются методы перехвата на уровне ядра ОС, в частности, минифильтры файловой системы, фильтры реестра. Кроме того, на уровне пользователя ОС реализован сервис, осуществляющий постоянный сбор информации от компонента ядра и сохранение (включая сжатие без потерь) данных на диск.

Вторым компонентом практической части стало приложение, способное анализировать системные журналы, собранные с помощью компонента ядра, показывать различные статистики, а также уведомлять пользователя о происходящих событиях, косвенно указывающих на нарушение безопасности ПК, например, присутствия вредоносного программного обеспечения или нарушения целостности системы. Для приложения разработан графический интерфейс и модули, отвечающие за анализ данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP, Windows 2000. Мастер-класс – М. Руссинович, Д. Соломон, Питер, Русская Редакция СПб, 2008 – 992 с. ISBN 978-5-469-01174-3, 978-5-7502-0085-6, 0-7356-1917-4

2. [Электрон. ресурс] Microsoft Developers Network. http://msdn.microsoft.com/en-US/

3. [Электрон. ресурс] Разработка Minifilter-драйвера. http://habrahabr.ru/post/176739/

4. Программирование драйверов для Windows – Комиссарова И.И., БХВ-Петербург, 2007 – 256 с. ISBN 978-5-9775-0023-4

5. [Электрон. ресурс] Как изменить integrity level процесса из уровня ядра http://kaimi.ru/2014/10/kernel-mode-process-integrity-level/

6. [Электрон. ресурс] Виртуальная отладка: отладка kernel mode кода с использованием VMware – онлайн-версия журнала xakep. https://xakep.ru/2009/06/23/48628/

7. [Электрон. ресурс] Process Monitor - отслеживание активности процессов Windows. http://ab57.ru/procmon.html

8. Защита информации в персональном компьютере – Емельянова, Партыка, Попов – М., Форум, 2009, 368 с., ил. ISBN 978-5-91134-328-6

9. [Электрон. ресурс] Практическое руководство – создание интерфейса в Windows Forms. https://msdn.microsoft.com/ru-ru/library/zh2fe5a5(v=vs.110).aspx

10. [Электрон. ресурс] Microsoft Developers Network. Working with the AppInit_DLLs registry value. http://support.microsoft.com/kb/197571/

11. [Электрон. ресурс] Методики обнаружения вредоносного ПО. http://www.z-oleg.com/secur/articles/spyhunt.php

12. [Электрон. ресурс] Хакерство и безопасность. Поиск и удаление вирусов вручную.
http://www.diwaxx.ru/hak/poisk-virus.php