УДК 004.492.3

ОБЗОР СУЩЕСТВУЮЩИХ ИНСТРУМЕНТОВ ОБНАРУЖЕНИЯ РУТКИТОВ В СИСТЕМАХ LINUX

Геннадьев Г.Д. (Санкт-Петербург, Университет ИТМО), **Кирилова К.С.** (Санкт-Петербург, Университет ИТМО)

Научный руководитель – к.т.н., доцент Менщиков А. А.

(Санкт-Петербург, Университет ИТМО)

В работе представлен обзор существующих инструментов обнаружения руткитов в Linux, выделены и сравнены используемые в них методы обнаружения. Также указано, какие из них могут быть использованы применительно к обнаружению руткитов уровня ядра.

Введение. Для обнаружения руткитов в системах на базе Linux существуют различные инструменты и методы, однако отсутствует их четкая систематизация, что затрудняет исследования и разработки в этой области. Те же из них, что нацелены на обнаружение руткитов уровня ядра, либо являются устаревшими и не рабочими на современных системах, либо дают ненадежные результаты, поскольку сами работают на уровне пользователя.
Понимание применяемых в реальных инструментах способов обнаружения руткитов, их достоинств и недостатков позволит подготовить базу для дальнейшей работы, а также выбрать среди них подходящие для решения задачи обнаружения руткитов уровня ядра в современных системах.

Основная часть. В работе рассмотрено 11 инструментов с открытым исходным кодом, не только нацеленных на обнаружение непосредственно руткитов, но также указывающих на следы его присутствия в системе (артефакты). На их основе выделены следующие способы обнаружения руткитов: сигнатурный, поведенческий, по артефактам файловой системы, по артефактам поведения, поиск по шаблонам в оперативной памяти.
Среди них примечательны те, которые могут быть применены к общим техникам скрытия, свойственным руткитами уровня ядра в целом, а не конкретным образцам или семействам, в силу своей большей универсальности. Это: поведенческий способ, по артефактам памяти, по шаблонам в оперативной памяти. Указано, какие инструменты реализуют их и представляют интерес для дальнейшего изучения.

Выводы. Результаты работы представляют собой базу для дальнейших исследований в задаче обнаружения руткитов (в частности, уровня ядра) в Linux. Указаны сильные и слабые рассматриваемых методов обнаружения, а также ограничения их применимости.

Кирилова К.С. (автор) Подпись _____

Менщиков А.А. (научный руководитель) Подпись _____