УДК 004.4

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ОБНАРУЖЕНИЯ РУТКИТОВ В ОС LINUX

Ломоносов А. В. (ИТМО)
Научный руководитель – Грозов В. А.
(ИТМО)

Введение. Современные операционные системы, включая Linux, подвержены угрозам, связанным с руткитами — вредоносными программами, способными скрывать свое присутствие и предоставлять злоумышленникам привилегированный доступ. Обнаружение руткитов является сложной задачей из-за их способности модифицировать системные вызовы, файловую систему и оперативную память. Разработка эффективного программного средства для их выявления играет важную роль в обеспечении безопасности информационных систем. Данный доклад посвящен исследованию методов обнаружения руткитов в Linux и разработке программного решения, способного анализировать признаки их активности.

Основная часть. Для обнаружения руткитов в Linux используются различные подходы, которые можно разделить на следующие категории:

– Методы анализа целостности системы – основаны на сравнении текущего состояния системы с эталонными значениями, включая проверку файловых систем, контрольных сумм бинарных файлов и конфигурационных файлов.

– Мониторинг активности системы – отслеживание подозрительных процессов, необычных соединений, скрытых файлов и модификаций в ядре.

– Анализ поведения ядра – выявление признаков перехвата системных вызовов, изменений в таблице системных вызовов (syscall table) и внедрения модулей ядра.

Разработка предполагаемого программного средства для обнаружения руткитов предполагает реализацию нескольких ключевых механизмов:

– Проверка целостности системных файлов и модулей ядра.

– Сканирование процессов и сетевых соединений на предмет аномальной активности.

– Выявление изменений в системных вызовах и хуков в ядре.

В ходе работы был проведен сравнительный анализ существующих инструментов для обнаружения руткитов **rkhunter** и рассмотрен метод анализа целостности системы.

Выводы. Проведен анализ метода обнаружения руткитов через метод контроля целостности системных файлов в ОС Linux.

Список использованных источников:

1. Positive Technologies Руткиты: эволюция и способы обнаружения // URL: https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and-detection-methods/ – 2021.

2. Зайцев О. Rootkits, SpyWare_AdWare, Keyloggers & BackDoors. Обнаружение и защита / Олег Зайцев. — Санкт-Петербург: БХВ-Петербург, 2006.