Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):6-9
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

TOOLS OF COMPUTER EXPERTISE WITH OPEN SOURCE CODE IN CYBORG HAWK LINUX

O. Ilarionov, N. Ilarionova, N. Tmenova

Taras Shevchenko National University of Kyiv

ABSTRACT

The community of free software developers is constantly creating assemblies of utilities designed for software and technical expertise. The most popular is the KaliLinux collection, while Cyborg Hawk Linux is undeservedly ignored. The purpose of our research is to describe the capabilities of the Cyborg Hawk Linux tools

KEYWORDS: forensic tools, open source tools, software and technical expertise.

АННОТАЦИЯ:

Сообщество разработчиков бесплатного программного обеспечения постоянно создает сборки утилит, предназначенных для проведения программно-технической экспертизы. Наибольшей популярностью пользуется сборник KaliLinux, тогда как Cyborg Hawk Linux незаслуженно обходят вниманием. Целью нашего исследования является описание возможностей инструментов Cyborg Hawk Linux.

Компьютерные преступления в Интернете в настоящее время растут, и программно-техническая экспертиза (компьютерная криминалистика) играет важную роль в их предупреждении и обнаружении.

Программно-техническая экспертиза использует разные инструменты для создания цифрового доказательства, и по своей сути это сложный и разнообразный процесс. Цифровая экспертиза предусматривает проведение трех этапов. На первом этапе создается цифровой «образ» исследуемого объекта для углубленного анализа на другом устройстве. На втором этапе идентифицируют цифровые данные с использованием различных методов, таких как восстановление удаленных файлов, получение информации об учетных записях пользователей, идентификация информации о подключенных устройствах, таких как USB, CD / DVD приводы, внешние жесткие диски и т.д. Третий этап – восстанавливают фактический сценарий, основанный на последовательности действий, происходящих в исследуемом объекте.

Инструменты программно-технической экспертизы могут быть как коммерческими (проприетарными) так и бесплатными (с открытым кодом). Выбор того или иного инструмента

зависит от природы исследования, получаемых результатов, требований к безопасности и экономической эффективности инструмента. Исследование, проведенное Б. Карриером (Brain Career [1]) показало, что инструменты с открытым исходным кодом столь же эффективны и надежны, как и проприетарные. Этот вывод подтверждается и Д. Мэнсоном в [2], где показано, что при использовании одного бесплатного и двух коммерческих инструментов получено одинаковые результаты.

Сообщество разработчиков бесплатного программного обеспечения постоянно создает сборки утилит, предназначенных для проведения программно-технической экспертизы.

К наиболее популярным сборкам утилит, предназначенных для проведения программно-технической экспертизы можно отнести:

- CAINE [3] (Computer Aided Investigative Environment) – дистрибутив с открытым кодом на основе Linux. Оснащен единым графическим интерфейсом для управления набором разноплановых утилит. Не требует установки.
- DEFT [4] (Digital Evidence & Forensic Toolkit) – дистрибутив, созданный для компьютерной криминалистики, с целью запуска вживую на системах без вмешательства или повреждения устройств (жестких дисков и т.д.) подключенных к ПК.
- KaliLinux (старое название BackTrack) [5] Проект предназначен прежде всего для проведения тестов на безопасность.
- PHLAK [6] (Professional Hacker’s Linux Assault Kit) – модульный дистрибутив на основе Linux, не требующий установки. Предназначен прежде всего для тестирования на проникновение, проведения компьютерной криминалистики и анализа сетей.
- Cyborg Hawk Linux [7] – дистрибутив, в состав которого входят утилиты для проведения тестирования на проникновение

Использование именно сборки, а не отдельных программных средств, позволяет повысить надежность, безопасность и производительность работы. Наибольшей популярностью пользуется сборник Kali Linux, который содержит около 300 утилит, тогда как Cyborg Hawk Linux [4] , который содержит более 800 инструментов, незаслуженно обходят вниманием.

Целью нашего исследования является описание возможностей инструментов Cyborg Hawk Linux.

Исследование образа диска Cyborg Hawk Linux проводили на виртуальной машине VMware Workstation, работающий на 64-битном компьютере.

В сборнике инструментов программно-технической экспертизы Cyborg Hawk Linux есть 15 классов, каждый из которых разбит на категории и подкатегории, которые содержат разное количество утилит (таблица).

Таблица - Классы и категории инструментов с открытым исходным кодом программно-технической экспертизы в Cyborg Hawk Linux

Класс	Категория	Количество инструментов
1. Сбор информации	Исследования сети	68
	Прокси	3
	VPN анализ	3
	Каталогизация Web	63
2. Оценка уязвимости	Сеть	14
	Веб приложения	68
3. Эксплойты	Платформы для захвата браузеров	1
	Базы данных	5
	Сеть	23

Класс	Категория	Количество инструментов
	Социальная инженерия	2
	Веб атаки	19
4. Повышение привилегий	Атаки на пароли	66
	Прослушивание каналов (снифинг)	29
	Подмена (спуфинг)	31
5. Поддержка доступа		25
6. Отчеты	Работа з доказательствами	7
	Радиозахват данных с экрана	2
	Документирование ПО	2
7. Реверс инжиниринг	Дебагеры	4
	Дезассемблирование	6
	Инструменты разработки эксплойтов	4
	Инструменты для моделирования (RE Tools)	15
8. Тестирование надежности (стресс-тесты)	DOC	21
	Фазеры	22
	Стресс тестирование беспроводных сетей	2
9. Форензика	Захват	21
	Восстановление данных	42
	Цифровая антифорензика	1
	Цифровая форензика	14
	Инструменты оценки форензики	40
	Наборы инструментов форензики	5
	Исследования сети	2
	Безопасное удаление данных	4
	Стеганография	8
10. Инструменты беспроводных атак	Блутуз	25
	Разные инструменты	8
	Мониторинг радиоканала	10
	WiFi	36
11. RFID / NFC инструменты		43
12. Взлом аппаратного обеспечения		4
13. Анализ VOIP		24
14. Мобильная безопасность	Инструменты для разработки	3
	Форензика устройств	9
	Тестирование на проникновение	9
	Реверс инжиниринг	20
	Беспроводные анализаторы	6
15. Анализ вредоносных программных средств		5

В каждой категории было выбрано несколько утилит, для которых мы исследовали ее цель, последовательность и результаты работы на нашей виртуальной машине. Одним из выводов, полученных в исследовании является то, что многие утилиты выполняют несколько функций, и поэтому в сборнике они относятся к разным классам и категориям. Поэтому оригинальных программ гораздо меньше, чем заявлено разработчиками сборки. Кроме того, существенным ограничением в использовании сборника является то, что она рассчитана только на работу с 64-битными процессорами.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

[1] B. Carrier “Open Source Digital Forensics Tools: The legal argument”. AtStake. October 2002. [Online]. Available: http://dl.packetstormsecurity.net/papers/IDS/atstake_opensource_forensics.pdf
[2] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, and J. Treichelt. “Is the Open Way a Better Way? Digital Forensics Using Open Source Tools” *System Sciences. HICSS 2007. 40th Annual Hawaii International Conference on Science*, pp 266-270. [Online]. Available: https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550266b.pdf
[3] Официальный сайт CAINE (Computer Aided INvestigative Environment) [Электронный ресурс]. Режим доступа: http://www.caine-live.net/
[4] Официальный сайт DEFT (Digital Evidence & Forensics Toolkit) [Электронный ресурс]. Режим доступа: http://www.deftlinux.net/
[5] Официальный сайт KaliLinux [Электронный ресурс]. Режим доступа: https://www.kali.org/
[6] Официальный сайт PHLAK [Электронный ресурс]. Режим доступа: https://sourceforge.net/projects/phlakproject/
[7] Официальный сайт Cyborg Hawk Linux [Электронный ресурс]. Режим доступа: http://cyborg.ztrela.com/