Боевой Linux. Обзор самых мощных дистрибутивов для пентестов и OSINT

Alexander Obenshan, Product Manager at Yandex Cloud

Содержание статьи

1. KALI
2. DEFT
3. Tsurugi
4. Parrot
5. Blackarch
6. Buscador
7. Trinity
8. Subgraph
9. Tails
10. Whonix
11. Tinfoil
12. Tiger
13. Backbox
14. Bugtraq
15. Sumuri
16. Bonus
17. Сводная таблица
18. Выводы

Собирать время от времени материал про «топ» — это отлично, не только тренить брать на вооружение новые инструменты, но и сравнивать их с уже знакомыми. Так, в прошлом году я сравнивал Kali Linux с Parrot, в этом — Kali с Tsurugi. Сравнение, кстати, оказалось эффективным, а в ответ на обсуждения в Telegram появилось.

Дистрибутивы для пентестов бывают разные. Одни полезны, другие — не очень, но все они занимают одно место дробовика и перевода на русский не хватит. Поэтому в этой статье я сравнил 10 дистрибутивов, которые, по моему мнению, заслуживают внимания. Для каждого дистрибутива я сделал краткий обзор, сравнил его с другими и выбрал лучшие в нескольких номинациях. Все дистрибутивы, за исключением Tails, основаны на Debian. Если вы хотите узнать — читайте под катом.

Если вы интересуетесь кибербезопасностью и хотите внести свой вклад в развитие сообщества, пишите в Telegram-канал @cybersecurityrussia или в чат @cybersecurityrussiachat.

KALI

Kali

- Релиз версии: 2013 год
- Основан на: Debian
- Размер: 3GB
- Поддерживаемые архитектуры: AMD64

Сравнить

Начнем традиционно, со «топ» по версии интернет-сообщества Kali Linux. Дистрибутив поддерживается компанией Offensive Security, которая также занимается разработкой и поддержкой таких известных проектов, как Metasploit и Exploit-db. Kali Linux — это, по сути, набор инструментов для пентестов и OSINT. Все инструменты, которые есть в Kali, можно скачать и установить отдельно, но зачем, если все это уже собрано, настроено и работает из коробки?

Kali Linux — это, по сути, набор инструментов для пентестов и OSINT. Все инструменты, которые есть в Kali, можно скачать и установить отдельно, но зачем, если все это уже собрано, настроено и работает из коробки?

Kali Linux поддерживает большое количество аппаратных платформ, в частности, на ARM-процессорах. Есть даже версия для Raspberry Pi. Также Kali Linux поддерживает большое количество сетевых карт, в том числе беспроводных. Для Kali Linux есть свой форум, свой репозиторий, свой IRC-канал, свой Twitter и свой блог. Сообщество Kali Linux — одно из самых крупных сообществ в области кибербезопасности.

Kali Linux — это, по сути, набор инструментов для пентестов и OSINT. Все инструменты, которые есть в Kali, можно скачать и установить отдельно, но зачем, если все это уже собрано, настроено и работает из коробки?