ЛЕКЦИЯ 15. ИНСТРУМЕНТЫ ПЕНТЕСТИНГА В KALI LINUX

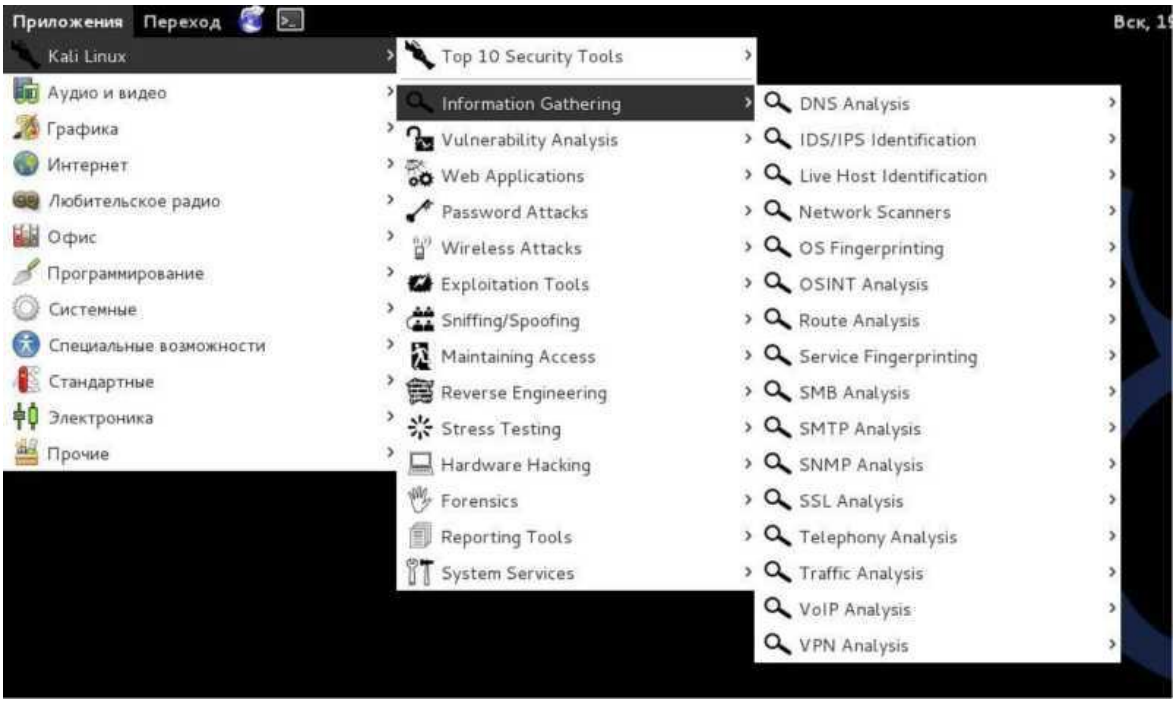
Вероятно, самый популярный дистрибутив для тестирования на проникновения, основанный на Debian Wheezy. Kali разработан компанией Offensive Security Ltd и является продолжением более раннего проекта BackTrack Linux.

Kali доступ в виде 32-битных и 64-битных ISO-образов, которые можно записать на USB-носитель или CD диск, или даже установить на жесткий диск или твердотельный накопитель. Проект также поддерживает архитектуру ARM и может запускаться даже на одноплатном компьютере Raspberry Pi, а также включает огромное количество инструментов анализа и тестирования.

Основным рабочим столом является Gnome, но Kali позволяет создать персонализированный ISO-образ с другой средой рабочего стола. Этот гибко настраиваемый дистрибутив позволяет пользователям даже изменять и пересобирать ядро Linux, чтобы соответствовать конкретным требованиям.

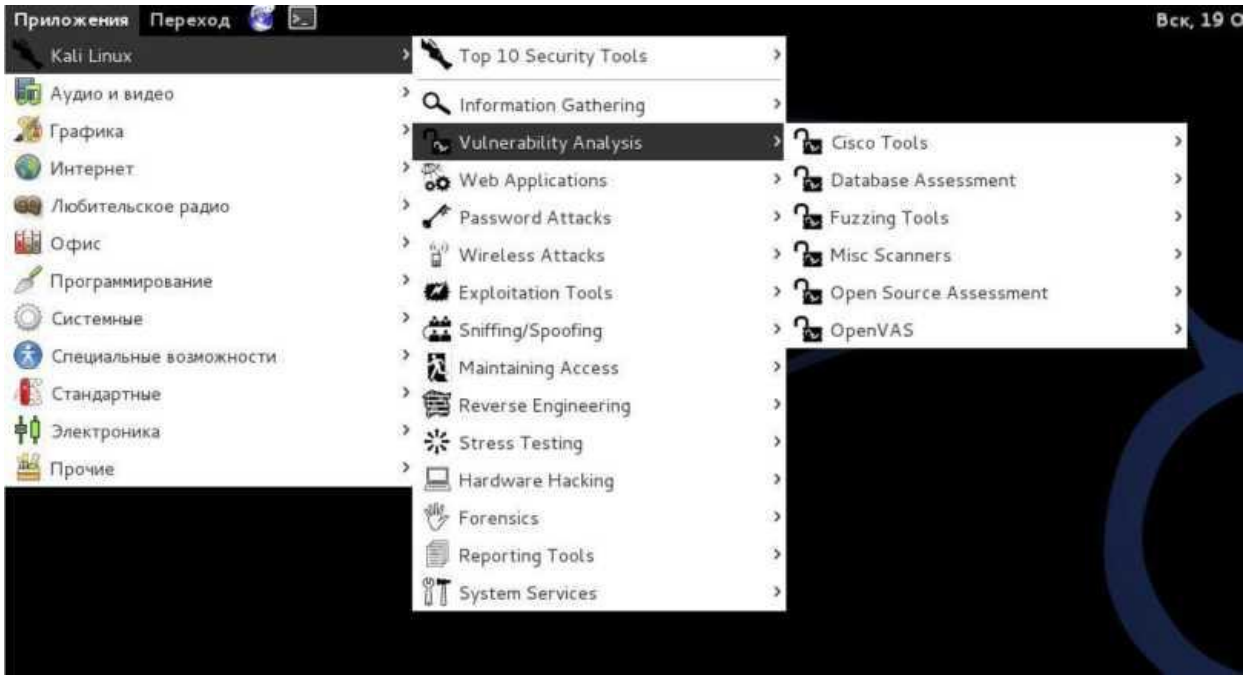
О популярности Kali можно судить по тому, что система является совместимой и поддерживаемой платформой для MetaSpoilt Framework - мощного инструмента, который позволяет разрабатывать и выполнять код эксплойта на удаленном компьютере.

15.1. Information Gathering



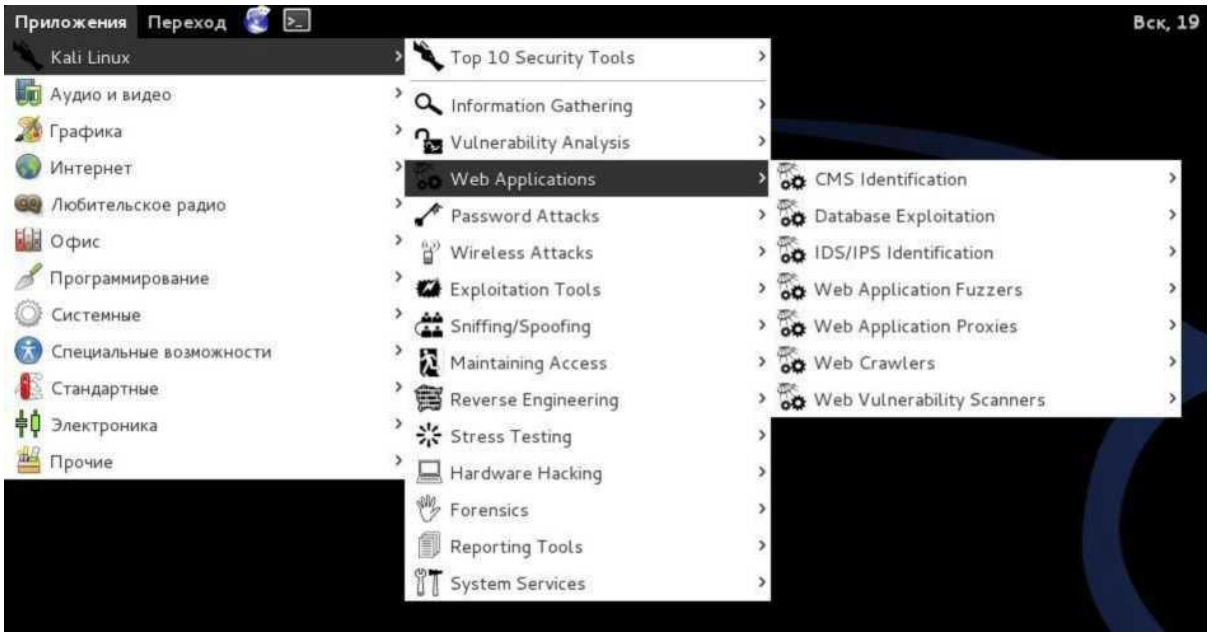
Эти инструменты для разведки используются для сбора данных по целевой сети или устройствам. Инструменты охватывают от идентификаторов устройств до анализа используемых протоколов.

15.2. Vulnerability Analysis



Инструменты из этой секции фокусируются на оценке систем в плане уязвимостей. Обычно, они запускаются в соответствии с информацией, полученной с помощью инструментов для разведки (из раздела Information Gathering).

15.3. Web Applications

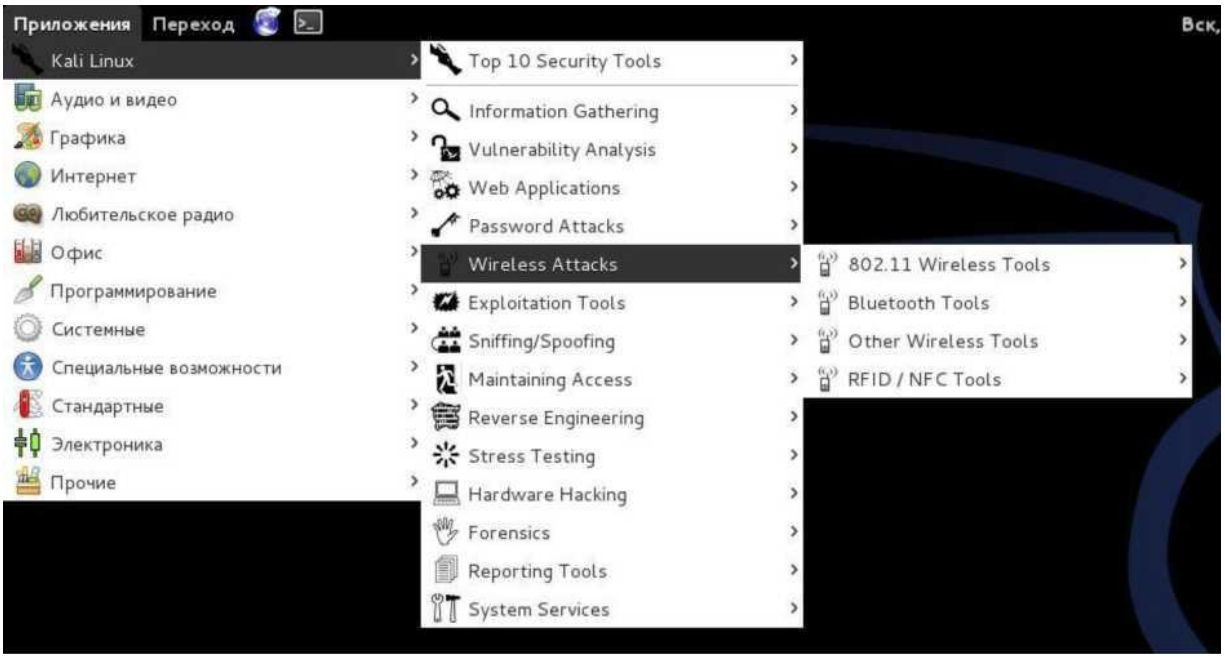


Эти инструменты используются для аудита и эксплуатации уязвимостей в веб-серверах. Многие из инструментов для аудита находятся прямо в этой категории. Как бы там ни было, не все веб-приложения направлены на атаку веб-серверов, некоторые из них просто сетевые инструменты. Например, веб-прокси могут быть найдены в этой секции.

15.4. Password Attacks

Эта секция инструментов, главным образам имеющих дело с брутфорсингом (перебором всех возможных значений) или вычисления паролей или расшаривания ключей используемых для аутентификации.

15.5. Wireless Attacks



Эти инструменты используются для эксплуатации уязвимостей найденных в беспроводных протоколах. Инструменты 802.11 будут найдены здесь, включая инструменты, такие как aircrack, airmon и инструменты взлома беспроводных паролей. В дополнение, эта секция имеет инструменты связанные также с уязвимостями RFID и Bluetooth. Во многих случаях, инструменты в этой секции нужно использовать с беспроводным адаптером, который может быть настроен Kali в состояние прослушивания.

15.6. Exploitation Tools

Эти инструменты используются для эксплуатации уязвимостей найденных в системах. Обычно уязвимости идентифицируются во время оценки уязвимостей (Vulnerability Assessment) цели.

15.7. Sniffing and Spoofing

Эти инструменты используются для захвата сетевых пакетов, манипуляции с сетевыми пакетами, создания пакетов приложениями и веб подмены (spoofing). Есть также несколько приложений реконструкции VoIP.

15.8. Maintaining Access

Инструменты поддержки доступа (Maintaining Access) используются как плацдарм и устанавливаются в целевой системе или сети. Обычное дело найти на скомпрометированных системах большое количество бэкдоров и других способов контроля атакующим, чтобы обеспечить альтернативные маршруты на тот случай, если уязвимость, которой воспользовался атакующий, будет найдена или устранена.

15.9. Reverse Engineering

Эти инструменты используются для модификации, анализа, отладки (debug) программ. Цель обратной инженерии — это анализ как программа была разработана, следовательно, она может быть скопирована, модифицирована, использована для развития других программ. Обратная инженерия также используется для анализа вредоносного кода, чтобы выяснить, что исполняемый файл делает, или попытаться исследователями найти уязвимости в программном обеспечении.

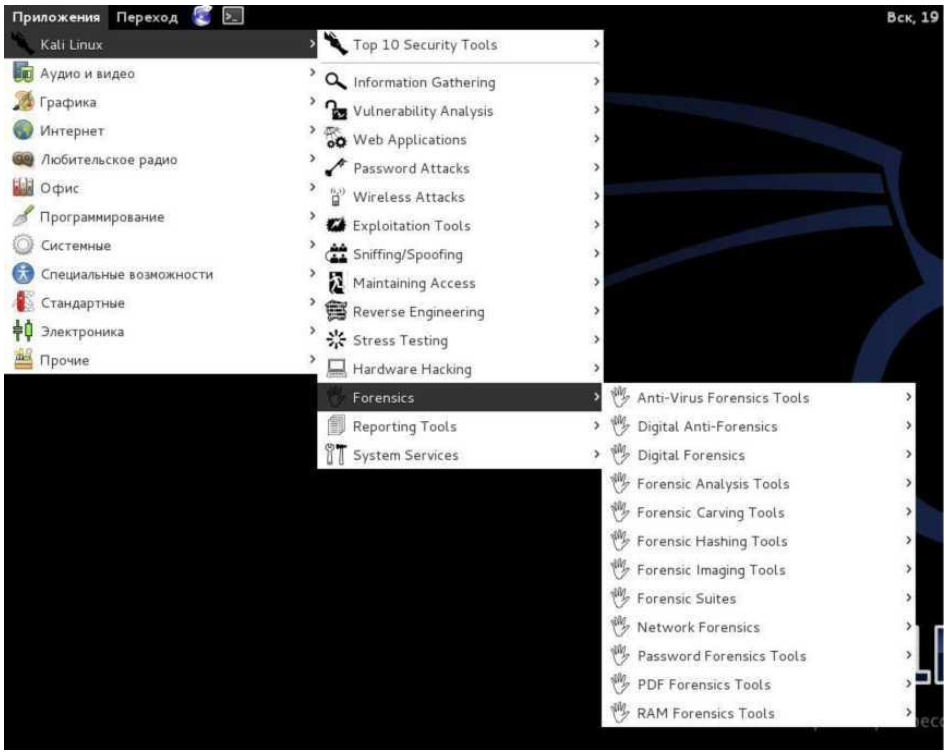
15.10. Stress Testing

Инструменты для стресс тестинга (Stress Testing) используются для вычисления как много данных система может «переварить». Нежелательные результаты могут быть получены от перегрузки системы, такие как стать причиной открытия всех коммуникационных каналов устройством контроля сети или отключения системы (также известное как атака отказа в обслуживании).

15.11. Hardware Hacking

Эта секция содержит инструменты для Android, которые могут быть классифицированы как мобильные и инструменты Android, которые используются для программирования и контроля маленьких электронных устройств

15.12. Forensics

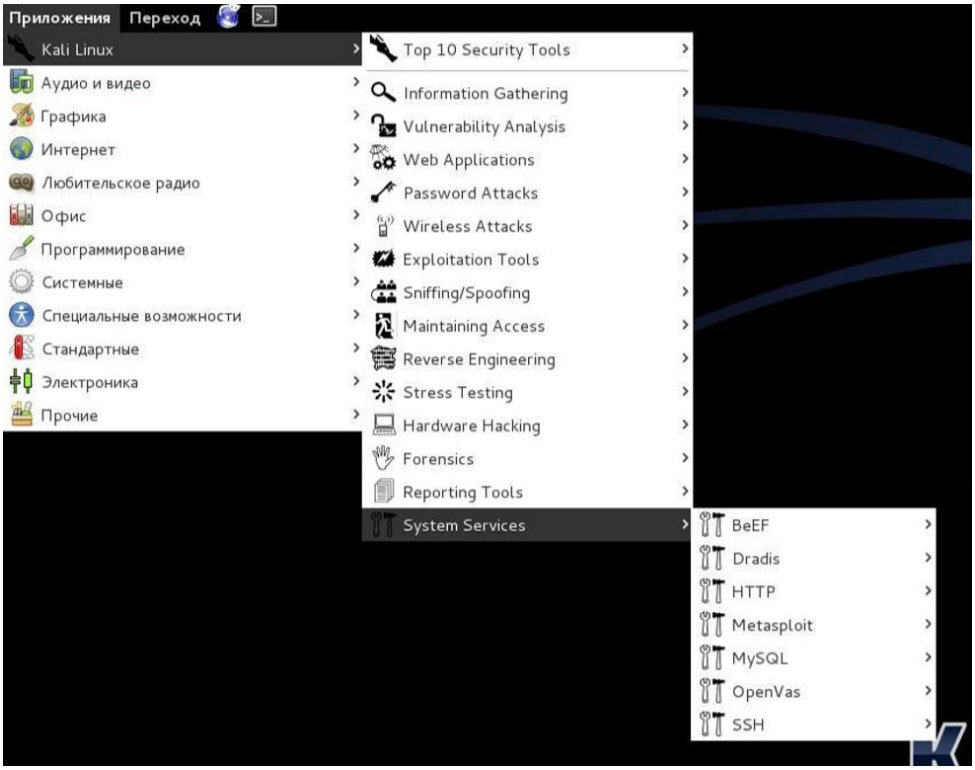


Инструменты криминалистики (Forensics) используются для мониторинга и анализа компьютера, сетевого трафика и приложений.

15.13. Reporting Tools

Инструменты для отчётов (Reporting tools) — это методы доставки информации, найденной во время исполнения проникновения.

15.14. System Services



Здесь вы можете включить или отключить сервисы Kali. Сервисы сгруппированы в BeEF, Dradis, HTTP, Metasploit, MySQL, и SSH.

В сборку Kali Linux включены также и другие инструменты, например, веб-браузеры, быстрые ссылки на тюнинг сборки Kali Linux, которые можно увидеть в других разделах меню (сеть, инструменты поиска и другие полезные приложения).