ЛЕКЦИЯ 09. ОПЕРАЦИОННЫЕ СИСТЕМЫ ДЛЯ ПЕНТЕСТА

Тестирование на проникновение (жарг. Пентест) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу целевой системы, либо полный отказ в обслуживании. Анализ ведется с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы.

Результатом работы является отчет, содержащий в себе все найденные уязвимости системы безопасности, а также может содержать рекомендации по их устранению. Цель испытаний на проникновение — оценить возможность его осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки. Испытание на проникновение является частью аудита безопасности.

Рассмотрим дистрибутивы Linux, которые специально предназначены для усиленной защиты приватности и/или проведения тестирований на вторжения.

9.1. Backbox

Backbox - дистрибутив на базе Ubuntu, разработанный для тестирования вторжений. За счет использования XFCE в качестве стандартного оконного менеджера, работает очень быстро.

Репозитории программных решений постоянно обновляются, чтобы пользователь всегда имел дело с последними версиями встроенных инструментов, которые позволяют выполнять анализ веб-приложений, стресс-тесты, оценку потенциальных уязвимостей, привилегий и многое другое.

В отличие от других дистрибутивов, которые включают большой набор различных приложений, Backbox не содержит подобной избыточности. Здесь Вы найдете только лучшие инструменты для каждой отдельной задачи или цели. Все инструменты отсортированы по категориям, что упрощает их обнаружение.

На Википедии представлены краткие обзоры многих встроенных инструментов. Несмотря на то, что Backbox первоначально создавался исключительно для тестирования, дистрибутив также поддерживает сеть Tor, которая поможет скрыть ваше цифровое присутствие.

9.2. Kali

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.

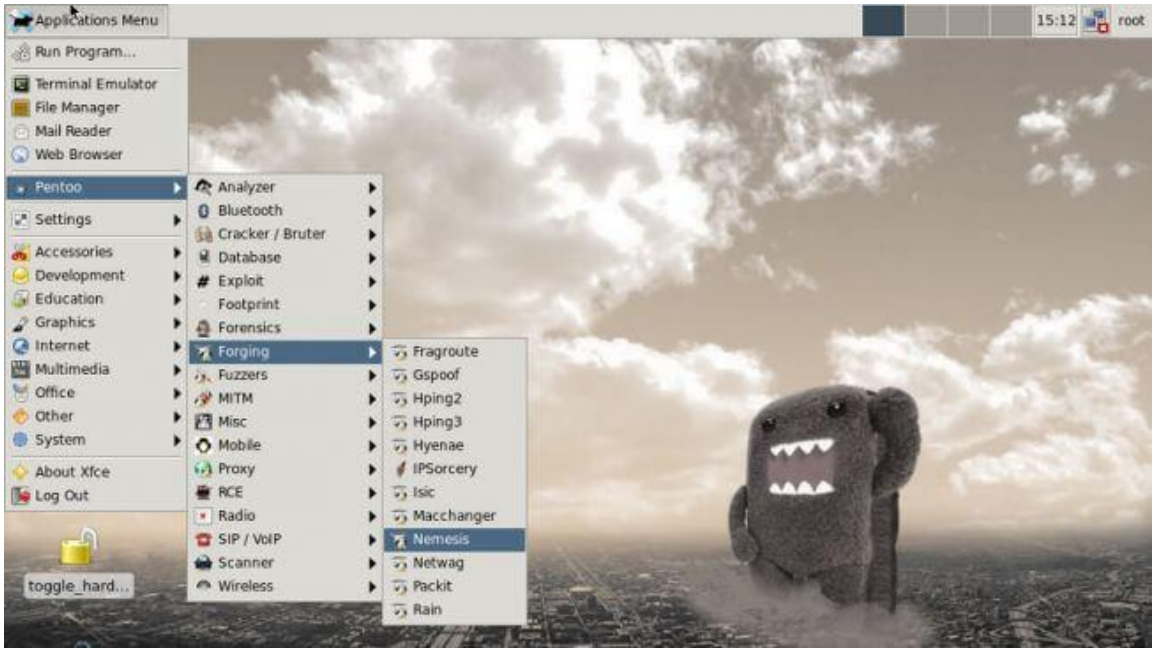
Основным рабочим столом является Gnome, но Kali позволяет создать персонализированный ISO-образ с другой средой рабочего стола. Этот гибко настраиваемый дистрибутив позволяет пользователям даже изменять и пересобирать ядро Linux, чтобы соответствовать конкретным требованиям.

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.

9.3. Pentoo

Доступный для 32-битных и 64-битных машин, Pentoo является дистрибутивом для тестирования вторжений, который основан на Gentoo Linux. Пользователи Gentoo могут дополнительно устанавливать Pentoo, который будет инсталлироваться поверх основной системы. Дистрибутив основан на XFCE и поддерживает сохранение изменений, поэтому при отключении USB-носителя, все примененные изменения будут сохранены для будущих сессий.

Встроенные инструменты делятся на 15 различных категорий, например, Exploit, Fingerprint, Cracker, Database, Scanner и т.д. Будучи основанным на Gentoo, дистрибутив унаследовал набор защитных функций Gentoo, которые позволяют выполнять дополнительные настройки безопасности и более детально управлять дистрибутивом. Вы можете использовать утилиту Application Finder для быстрого обнаружения приложений, расположенных в различных категориях.



Поскольку дистрибутив основан на Gentoo, потребуется выполнить некоторые манипуляции, чтобы заставить работать сетевую карту и другие аппаратные компоненты. При загрузке выберите опцию проверки и настройте все ваши устройства.

9.4. Security Onion

Основанный на Ubuntu, данный дистрибутив разработан для обнаружения вторжений и мониторинга сетевой безопасности. В отличие от других дистрибутивов для пентестинга, которые носят скорее наступательный характер, Security Onion представляет собой более оборонительную систему.

Тем не менее, проект включает большое количество инструментов наступательного толка, которые встречаются в других дистрибутивах для тестирования на проникновение,

а также инструменты мониторинга сети, например, сниффер пакетов Wireshark и утилита обнаружения вторжений Suricata.

Security Onion построен вокруг XFCE и включает все самые необходимые приложения, имеющиеся в Xubuntu. Security Onion не предназначен для любителей, а скорее подойдет опытным специалистам, которые имеют определенный уровень знаний в области мониторинга сети и предотвращения вторжений. К счастью проект постоянно сопровождается подробными руководствами и видеоуроками, чтобы помочь в работе с сложным встроенным ПО.

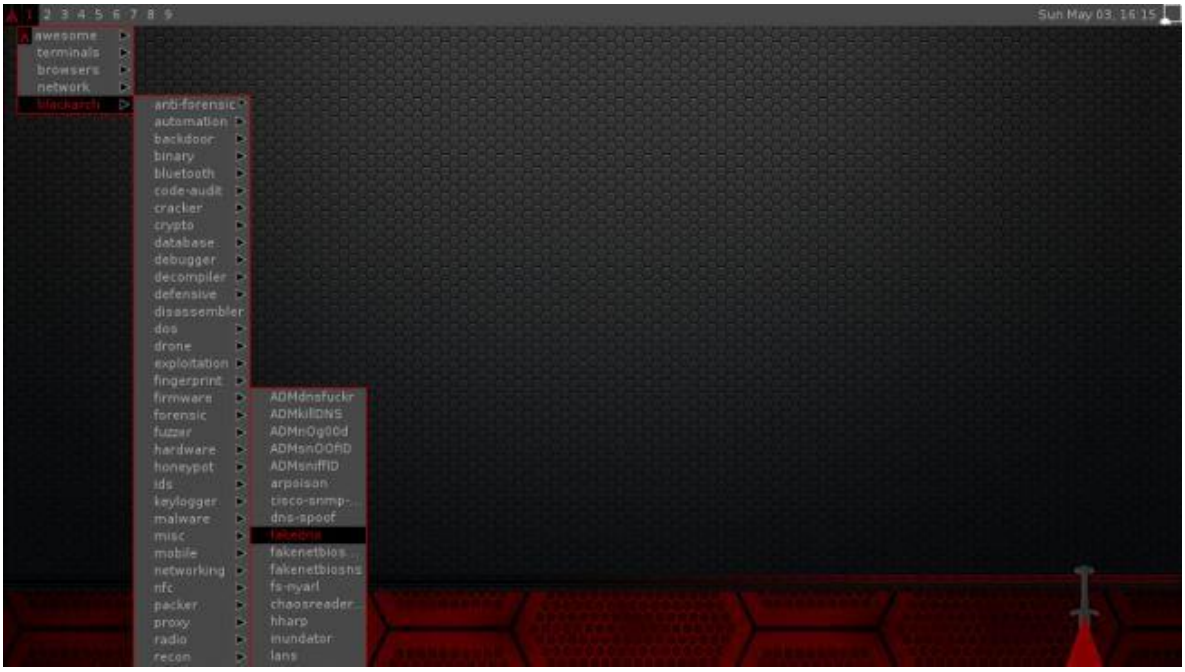
9.5. Caine

Caine является аббревиатурой от Computer Aided INvestigation Environment (среда помощи исследования компьютера). Дистрибутив распространяется с помощью Live диска и построен на последней версии Ubuntu 14.04. В качестве установщика используется SystemBack. Систему можно запустить и с локального диска после установки или с переносного USB-устройства флеш-памяти или CD. Дистрибутив стремится обеспечить дружественный интерфейс и включает богатый набор инструментов для экспертизы безопасности.

Caine отличается от других подобных проектов за счет интеграции довольно редких инструментов, например, rbfstab - утилиты, которая позволяет безопасно монтировать подключаемые устройства в режиме чтения для проведения анализа и тестирования.

Кроме огромного количества приложения для работы с памятью, базами данных и сетью, Caine также включает стандартные популярные приложения - браузеры, офисные программы, почтовые клиенты и т.д.

9.6. BlackArch



BlackArch является разновидностью Gentoo и позиционируется как легковесный вариант Arch Linux. BlackArch доступен как Live-образ для инсталляции, но пользователи Arch могут устанавливать BlackArch поверх существующей системы. Для создания загрузочного USB-накопителя рекомендуется использовать команду dd вместо утилиты UNetBootin.

Учетная запись по умолчанию: root:blackarch. BlackArch имеет размер более 4 гигабайт и поставляется с несколькими различными оконными менеджерами, включая Fluxbox, Openbox, Awesome.

В отличие от других дистрибутивов для тестирования на проникновение, BlackArch также может использоваться в качестве инструмента повышенной конфиденциальности. Кроме различных инструментов анализа, мониторинга и тестирования, дистрибутив также включает инструменты защиты от слежения, в частности sswap и ropeadope для безопасного стирания содержимого файла подкачки и системных журналов соответственно и многие другие программы для обеспечения приватности.

9.7. Parrot Security OS

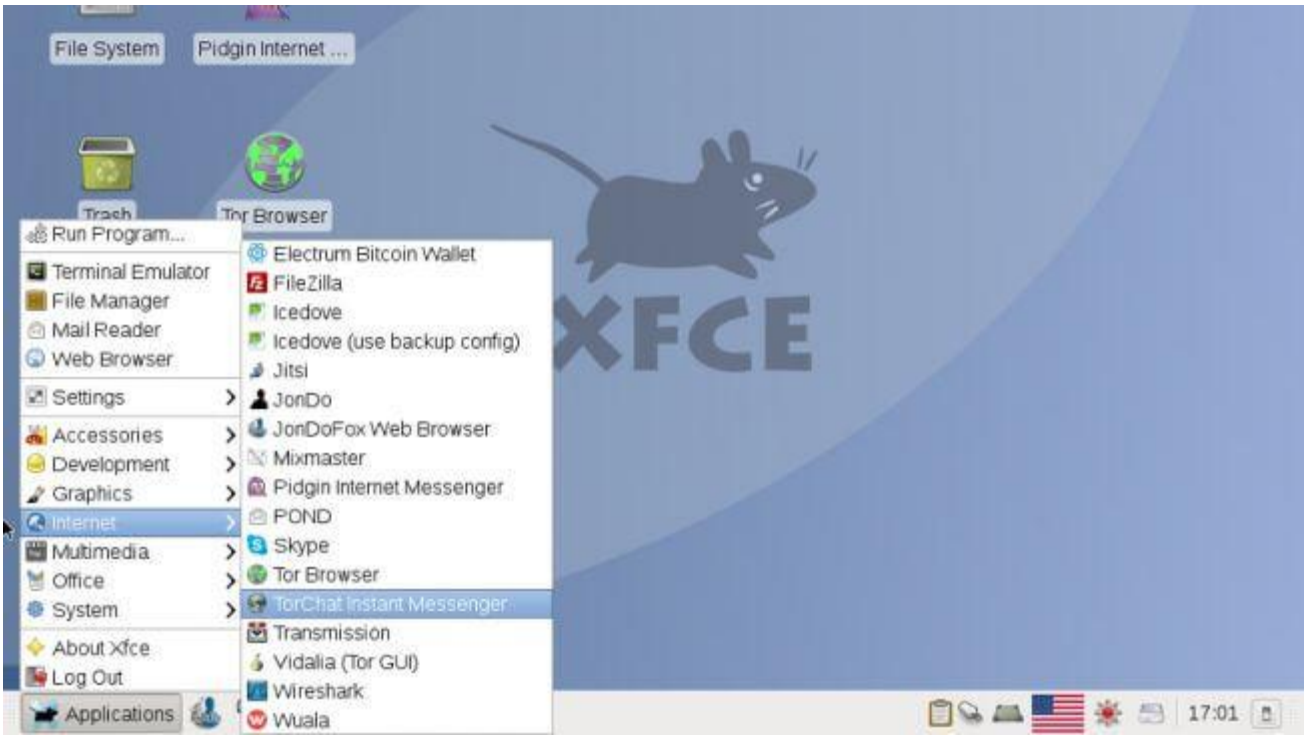
Разработанный итальянской сетью Frozenbox, посвященной IT-безопасности и программированию, основанный на Debian, Parrot Security OS может использоваться для тестирования вторжений и поддержания конфиденциальности. Также как BlackArch, Parrot Security OS является дистрибутивом плавающего релиза. Логин по умолчанию для Live-сессии: root:toor.

Устанавливаемый Live-образ предлагает несколько опций загрузки, например, устойчивый режим или устойчивый режим с шифрованием данных. Кроме аналитических инструментов, дистрибутив включает несколько программ для анонимности и даже криптографическое ПО.

Персонализируемая среда рабочего стола Mate предлагает привлекательный интерфейс, а сам Parrot Security OS работает очень шустро даже на машинах с 2 гигабайтами ОЗУ. В систему встроено несколько нишевых утилит, например, apktool - инструмент изменения APK файлов.

Для пользователей, которые заботятся о приватности, в дистрибутиве предусмотрена специальная категория приложений, где пользователи могут включить анонимный режим серфинга в Интернете (используются сети Tor) за один клик.

9.8. JonDo



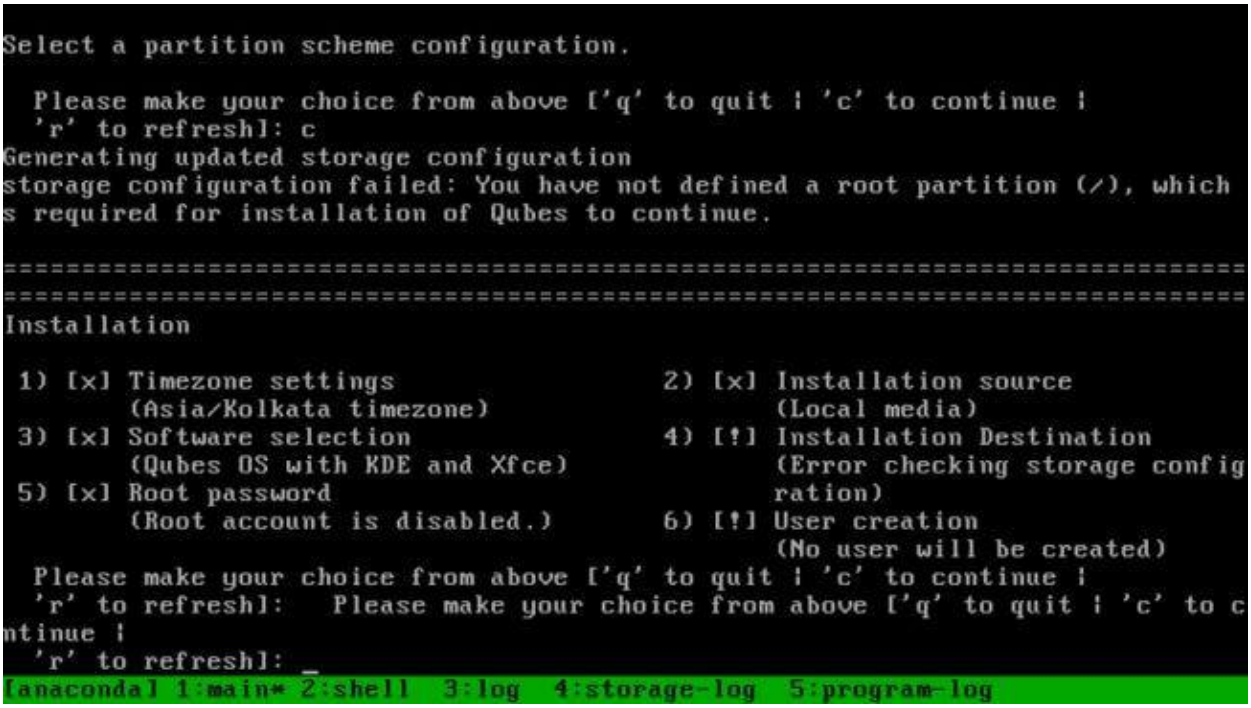
JonDo - построенный на Debian дистрибутив, разработанный специально для анонимного серфинга в сети. JonDo предоставляет анонимный прокси-сервер, доступный для различных платформ, включая Linux, BSD, Windows и Mac.Live-версия предлагает

пользователям использовать JonDo или Tor прокси для защиты конфиденциальности онлайн.

Все встроенные приложения предварительно сконфигурированы и настроены на максимальную анонимность. Например, мессенджер Pidgin настроен на анонимную передачу сообщений. Дистрибутив включает несколько клиентов мгновенного обмена сообщениями, в частности Pidgin и TorChat и приватные браузеры JonDoFox и TorBrowser.

У проекта есть свой форум, wiki-справочник и различные руководства для пользователей, которые хотят получить максимум от встроенных приложений.

9.9. Qubes

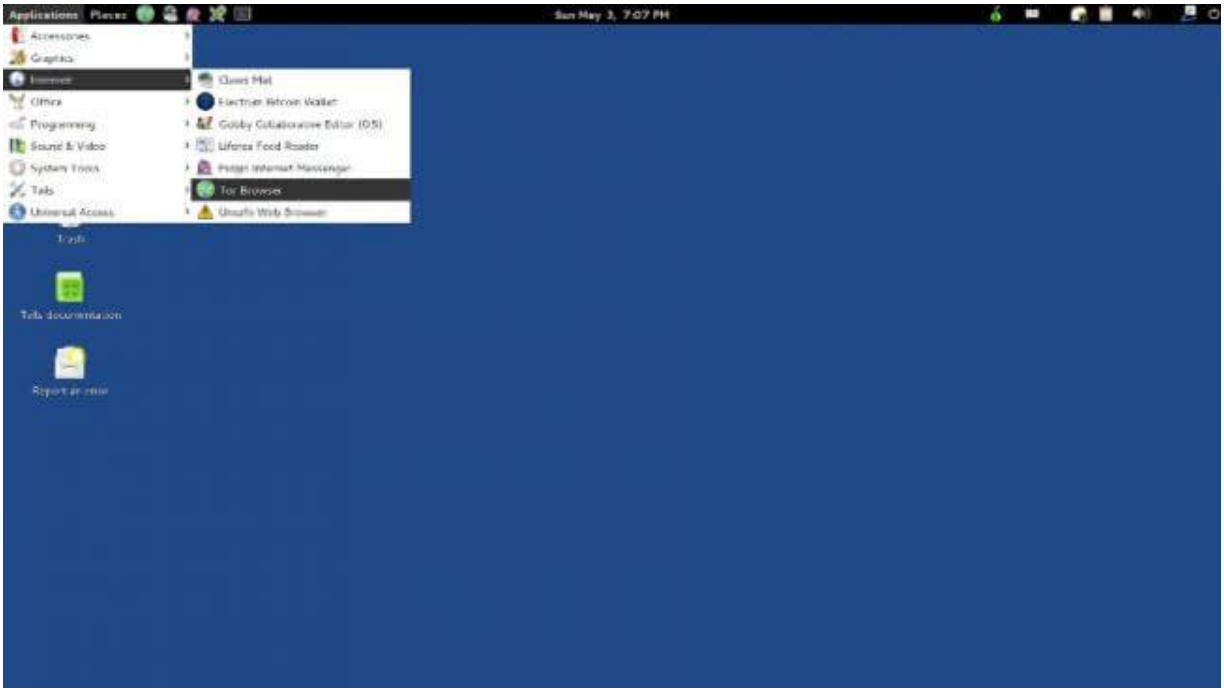


Основанный на Fedora, Qubes доступен только для установки и предоставляет защиту конфиденциальности благодаря тотальной изоляции. Проект использует Xen для создания изолированной виртуальной машины, которая обращается только к нужным для данной конкретной функции службам, что снижает потенциальный риск угрозы. Несмотря на использование виртуализации, Qubes предлагает простой и удобный рабочий стол.

Для установки дистрибутива нужно выполнить инструкции текстового инсталлятора anaconda. Дистрибутив позволяет выбирать среду рабочего стола при установке: KDE, XFCE или обе.

Qubes предлагает стандартные инструменты управления разделами и менеджер логических томов, для запуска на некоторых машинах возможно потребуется выбрать опцию BTRFS. Процесс установки довольно сложен, особенно во время графических установщиков, но на выходе Вы получаете невероятно безопасный дистрибутив.

9.10. Tails



Также, как и JonDo, Tails Linux также поставляется с широким спектром различных приложений для работы в Интернете, которые предварительно сконфигурированы для максимальной анонимности. Вы можете выбрать устойчивый режим для сохранения всех файлов и настроек для будущих сессий при запуске Tails с USB-носителя. Согласно официальному сайту проекта, Вы можете запустить Tails даже с SD-карты.

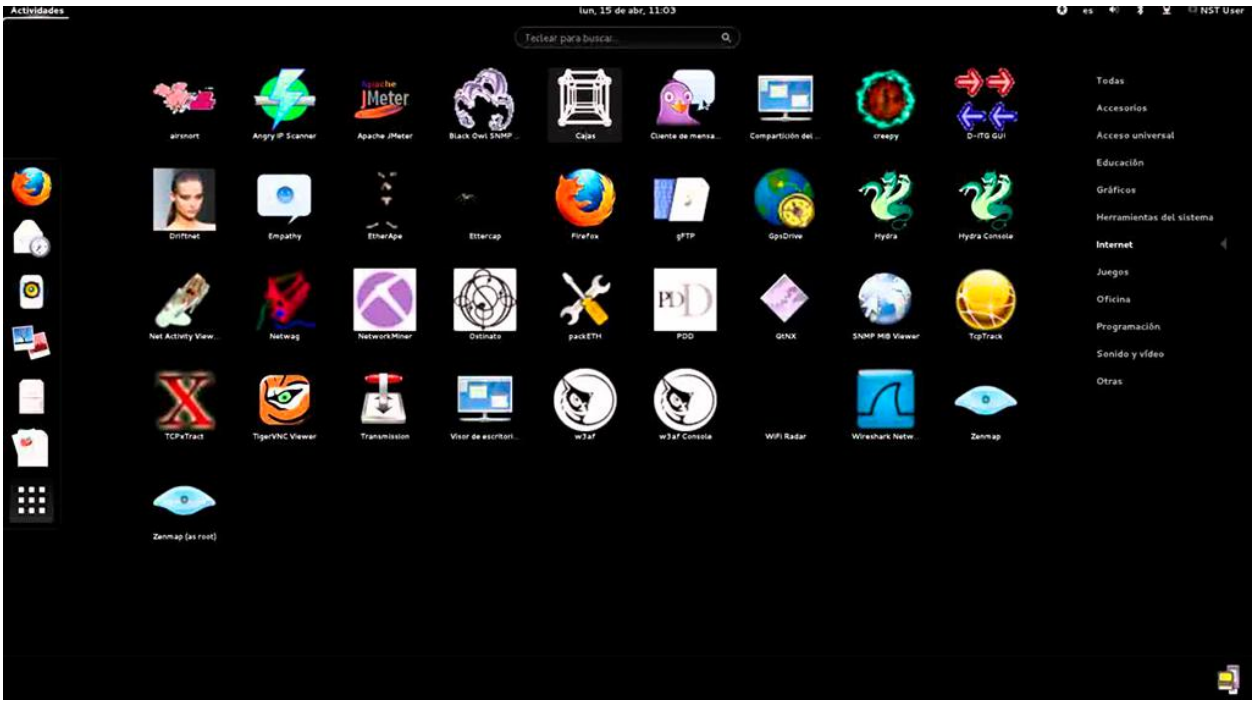
По умолчанию дистрибутив использует сеть Tor для анонимизации всего трафика, включая данные, передаваемые браузерами, почтовыми клиентами или мессенджерами. Tails стирает все следы активности в сети и использует криптографические технологии для шифрования всех файлов, сообщений и писем.

Несколько важных плагинов, например, AdBlock Plus, NoScript и другие уже включены по умолчанию в Firefox. Последняя версия поставляется с кошельком Electrum Bitcoin и позволяет маскировать систему под Windows 8, а также визуально подделывать MAC-адрес.

9.11. Network Security Toolkit

Network Security Toolkit — это один из многих дистрибутивов Linux типа Live CD, направленных на анализ безопасности сети. NST дает администраторам простой доступ к широкому множеству открытых сетевых приложений, многие из которых включены в сотню лучших средств безопасности, рекомендованных сайтом insecure.org. Основан на Fedora Linux.

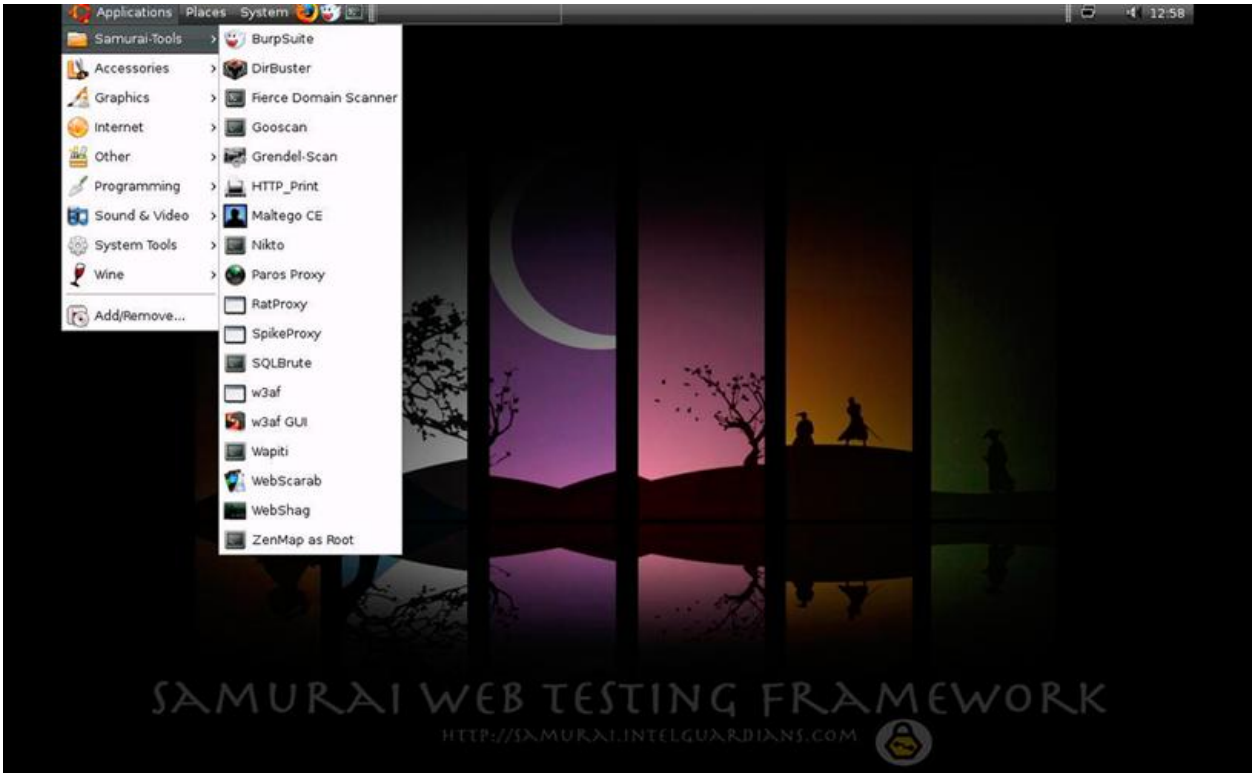
Обладая сбалансированным набором средств сетевого мониторинга, анализа и безопасности, может дать явные преимущества сетевому администратору, для контроля безопасности вверенной ему инфраструктуры.



9.12. Samurai Web Security Framework

Основное предназначение этого дистрибутива — тестирование на проникновения различных веб-приложений.

Поставляется в виде образа виртуальной машины, содержащий наиболее популярные Open Source утилиты для сбора информации и проведения различных атак на веб-приложения.



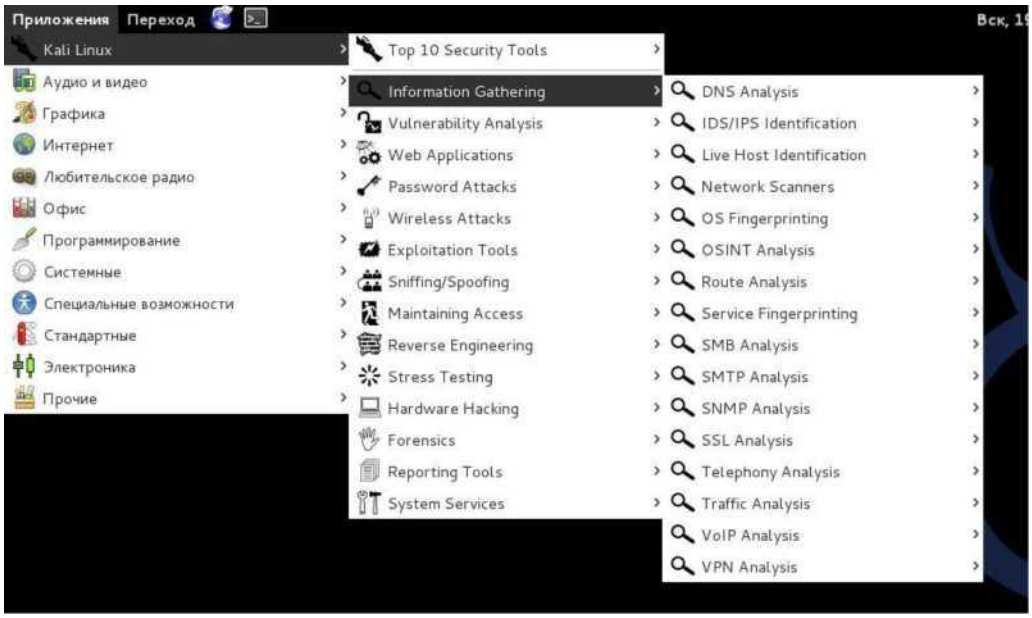
9.13. WifiSlax

Это специализированный дистрибутива с подборкой инструментов для проверки безопасности систем WiFi-сетей и проведения криминалистического анализа. Дистрибутив построен на базе Slackware linux.

В настоящее время, это один из наиболее часто используемых инструментов для аудита WiFi сетей, в него включены большинстов популярных утилит для анализа защищенности беспроводных сетей, поддерживается большинство производитей сетевых карт.

9.14. Обзор разделов инструментов Kali Linux

9.14.1. Information Gathering

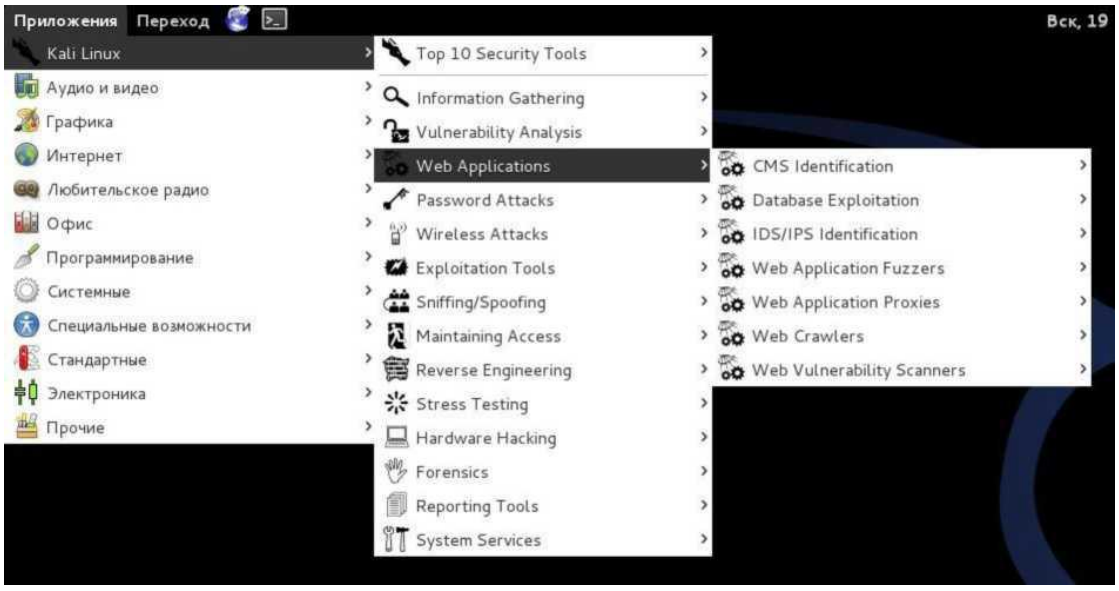


Эти инструменты для разведки используются для сбора данных по целевой сети или устройствам. Инструменты охватывают от идентификаторов устройств до анализа используемых протоколов.

9.14.2. 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).

9.14.3. Web Applications

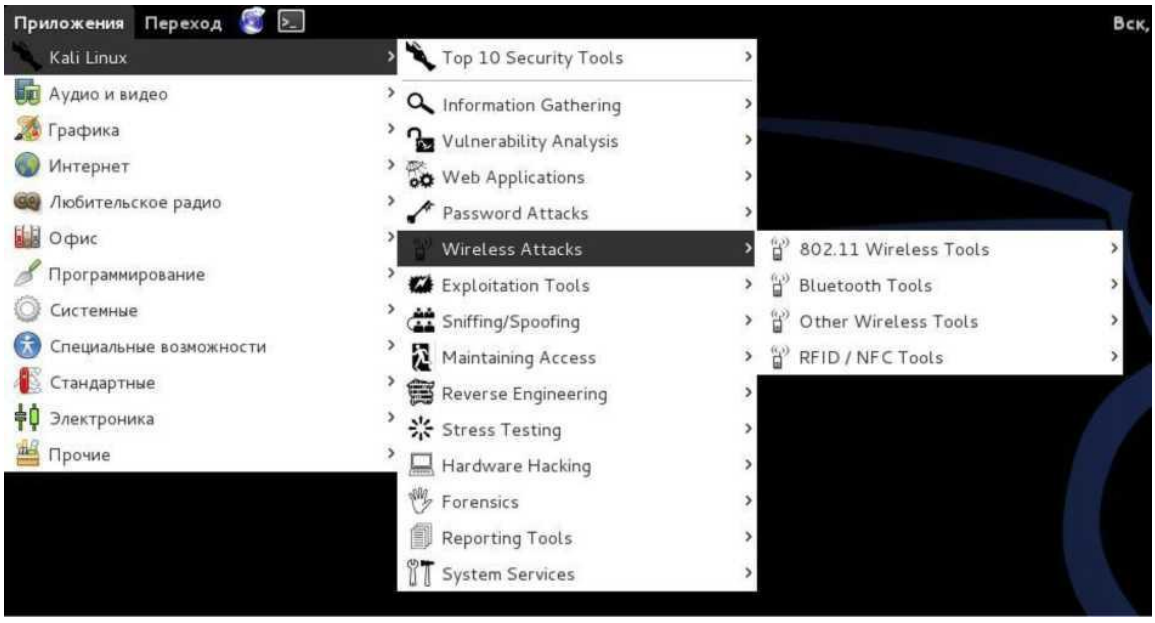


Эти инструменты используются для аудита и эксплуатации уязвимостей в веб-серверах. Многие из инструментов для аудита находятся прямо в этой категории. Как бы там ни было, не все веб-приложения направлены на атаку веб-серверов, некоторые из них просто сетевые инструменты. Например, веб-прокси могут быть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

9.14.4. Password Attacks

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

9.14.5. 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.

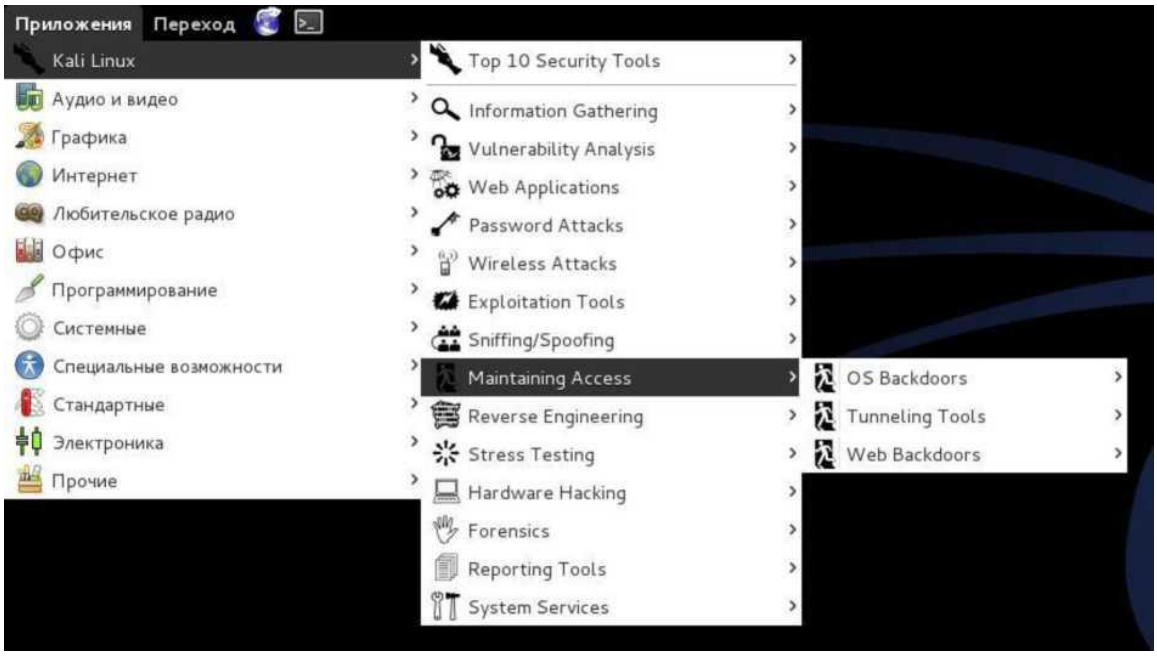
9.14.6. Exploitation Tools

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

9.14.7. 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.

9.14.8. 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.

9.14.9. 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.

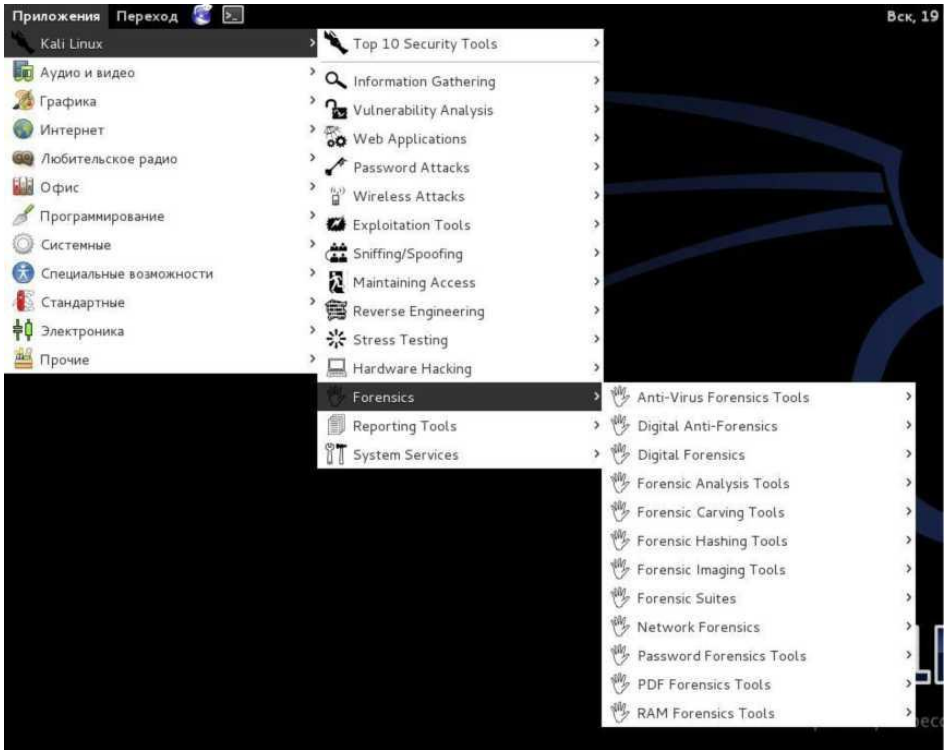
9.14.10. Stress Testing

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).

9.14.11. 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

9.14.12. Forensics

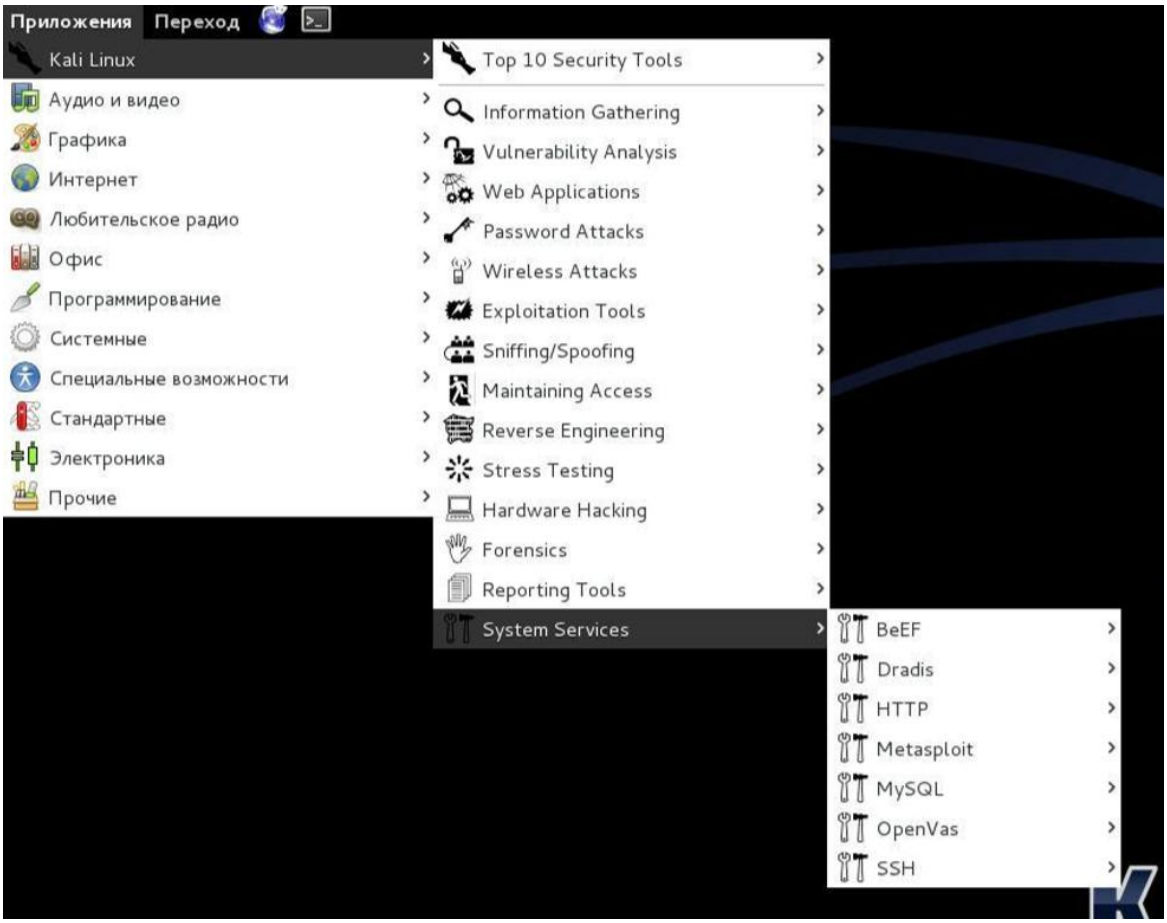


Инструменты криминалистики (Forensics) используются для мониторинга и анализа компьютера, сетевого трафика и приложений.

9.14.13. Reporting Tools

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

9.14.14. 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).