ANTCOLONY

Linux Shell

Подсказки для системных администраторов

Для кого:

Данное руководство охватывает то, что мы считаем наиболее полезными примитивами Linux shell и основными утилитами. Эти инструменты могут быть крайне полезны для автоматизации процессов анализа, генерации вывода, который затем можно скопировать и вставить в отчет или таблицу, а также для обеспечения быстрой реакции, когда полный набор инструментов недоступен.

Помните: если вы можете выполнить задачу в shell через SSH даже по медленному dialup-соединению, у вас будет больше шансов стать «летальным» forensic-специалистом, когда это действительно имеет значение!

Разделы:

Работа по цепочке

Linux предпочитает небольшие, универсальные функции и утилиты. Объедините их в цепочку с помощью “канала”, который передает выходные данные одной команды в следующую в качестве входных данных.

```
$ grep pattern input.txt | sort | uniq -c
```

Последовательно создайте серию команд для создания выходных данных, которые полностью соответствуют вашим требованиям.

Редирект вывода

Перенаправляет выходные данные в файл, а не в саму оболочку, используя символ “больше, чем”.
(Внимание: перезаписывает все существующее содержимое!)

```
$ grep pat1 input.txt > results.txt
```

Добавить к существующим файлам значение “в два раза больше, чем”.

```
$ grep pat2 input.txt >> results.txt
```

Нарезание

cut

Удаляет разделы из каждой строки ввода

```
$ cut -d ',' -f 2,5,7 input.txt
```

`-d`	Указывает альтернативный разделитель (по умолчанию используется TAB)
`-f`	Отображает номера полей

Комплексные инструменты

sed

Потоковый редактор для фильтрации и преобразования текста

```
$ sed 's/<regex>/<replacement>/' input.txt
```

awk

Язык сканирования и обработка шаблонов

```
$ awk -F ',' '{ print $1,$6,$3 }' in.txt
```

-F	Указывает альтернативный разделитель (по умолчанию используется space)

Разделители полей ввода и вывода могут быть заданы в самом awk-скрипте с помощью переменных FS и OFS:

```
$ awk '{ FS = ","; OFS = "\t"; \
print $2,$4 }' in.txt
```

Смена разрешений

chown

Меняет владельца файла (необязательно его группу)

```
$ chown username[:groupname] file.txt
```

-R	Рекурсивно изменить права собственности на содержимое каталога

chmod

Меняет права доступа к файлам

```
$ chmod  file.txt
```

-R	Рекурсивно изменить права собственности на содержимое каталога

Права

rwx	r = чтение; w = запись; x = выполнение (файлы), перемещение (каталоги)

Присваивается восьмеричными значениями (r = 4, w = 2, x = 1) или понятными для пользователя/группы/другими значениями:

755	rwx для пользователей, rx для групп, rx для других
400	r для пользователей, ничего для групп и других
664	rw для пользователей, rw для групп, r для других
u=rwx	Назначает права на чтение, запись и выполнение для владельца файла
g+rx	Добавляет права на чтение и выполнение для группы владельцев
a-w	Удаляет права на запись для всех

Полезные команды

man

Интерфейс к онлайн-руководством

```
$ man find
```

`-k` Выполните поиск по ключевым словам на всех страницах руководства

Используйте встроенную справку по командам, где это возможно – многие команды содержат краткие инструкции по использованию с параметрами “--help" или “-h”.

```
$ tcpdump --help
```

ANTCOLONY

Повышение точности, скорости и эффективности

Tab Completion

Нажмите клавишу <TAB>, чтобы развернуть первые несколько символов команды, имени каталога, файла или переменной.
Если существует более одного возможного варианта, он будет завершен, насколько это возможно.
Нажмите <TAB> еще раз, чтобы просмотреть возможные варианты завершения.

Стандартные переменные

~	Псевдоним для домашнего каталога текущего пользователя (также **$HOME**)
$PATH	Путь поиска команды
$?	Значение завершения предыдущей команды
$PWD	Текущий рабочий каталог

История команд

history	Используйте команду, чтобы просмотреть список буфера истории команд. (При выходе из программы BASH записывает в этот буфер значение /.bash_history, перезаписывая все существующее содержимое.)
Ctrl-R	для поиска в истории команд, соответствующих строке поиска
	Переключайтесь между предыдущими командами, нажимая
	Измените предыдущие команды

Поиск

grep

Выводит строки, соответствующие шаблону

```
$ grep pattern input.txt
```

`-i`	Сопоставление с шаблоном без учета регистра
`-v`	Выводит строки, которые не совпадают
`-c`	Подсчитывает совпадающие строки, не выводит их
`-l`	Выводит имена файлов, содержащие совпадающие строки
`-h`	команда не указывать имена файлов при поиске нескольких входных файлов (например, output*.txt)

Сортировка

sort

Сортирует строки в алфавитном или номерном порядке

```
$ sort input.txt
```

`-n`	Сортировка в числовом порядке (от 5 до 10)
`-r`	Обратный порядок сортировки
`-k`	Указать альтернативное поле сортировки
`-t`	Указать разделитель полей для -k

Дедупликация

uniq

выводит только последовательные совпадающие строки один раз

```
$ grep pattern input.txt | uniq
```

`-c` Выводит количество последовательных строк

Помните:

Данная команда находит только последовательные совпадающие строки!
Наиболее полезен при вводе данных по конвейеру из команды sort

```
$ grep pattern input.txt | sort | uniq
```

Замещающие символы

tr

Перевод (замена) или удаление символов

```
$ grep foo input.txt | tr '\t' ','
```

`-d` Удаляет указанный символ, а не заменяет его другим (принимает только один аргумент)

Плывите по (сетевому) течению

nfdump

Обработка данных NetFlow из файлов на диске

```
$ nfdump -R ./ -b -O tstart –o extended
```

-R	Рекурсивно считывает данные из указанного каталога
-b	Агрегирует записи двунаправленно
-a	Агрегирует по протоколам, src/dst IP-адресам, src/dst портам
-A	Задает пользовательскую агрегацию
-t	Временной интервал в формате “ГГГГ/ММ/ДД.чч:мм:сс”
-s	Генерирует статистику “TopN”
-O	Определяет порядок вывода
-o	Определяет формат вывода

Поиск пакетов без GUI

tshark

Сбор и анализ сетевого трафика
(он же “Wireshark в оболочке”)

```
$ tshark -n -r in.pcap -Y '<disp filter>'
```

-n	Предотвращает поиск по DNS и портам
-r	Выполняет чтение из файла pcap, а не из сети
-w	Записывает выходные данные в файл pcap, а не в терминал
-T	Изменяет формат вывода (текст, поля и т.д.)
-e	Используя “-T fields”, добавьте поле к выводимым данным
-Y	Для применения фильтра отображения, учитывающего протокол
-z	Для использования режимов статистического вывода

Смотрите справочную страницу wireshark-filter для получения информации о создании фильтров отображения, учитывающих протокол.

Поиск пакетов без GUI

tcpdump

Сборbсетевого трафика

```
$ sudo tcpdump -i eth0 '<BPF filter>'
```

-D	Перечисляет сетевые интерфейсы (полезно для Windows)
-w	Записывает данные пакетов в файл
-s	Количество байт в пакете для захвата
-i	Указывает сетевой интерфейс, с помощью которого будет осуществляться захват
-r	Считывает из существующего файла pcap вместо сетевого
-C	Количество байт, которые необходимо сохранить в файле записи перед запуском нового файла
-G	Количество секунд, которое необходимо сохранить в файле записи перед запуском нового файла
-W	При использовании с параметрами -C или -G ограничивает количество перемещаемых файлов (т.е. создает “ring buffer”)
-n	Предотвращает поиск в DNS по IP-адресам. Используйте дважды, чтобы также предотвратить поиск по портам в сервисах
-x	Отображает содержимое пакета в шестнадцатеричном формате

Обратите внимание, что tcpdump требует привилегий root для произвольного перехвата сетевого трафика.
Для управления существующими файлами перехвата достаточно разрешений на уровне пользователя.