DNS: Эксплуатация и защита данных. Продвинутый курс

Немного основ системы UNIX

Наша платформа

FreeBSD 9.x 64 бита

- UNIX OS, вариант BSD
- 30 лет истории
- Без графического интерфейса GUI, администрируем через SSH

- Другие платформы вы можете использовать:
  - Ubuntu, Debian, CentOS/RedHat, …
- Это не курс системного администрировани UNIX
  - Упражнения обычно шаг-за-шагом
  - Помогайте другим или просите нашей помощи

Некоторые вещи вам нужно будет делать…

Стать администратором (*root), когда нужно:* `sudo <cmd>`

Устанавливать пакеты:

```
pkg add <package_name>
```

Редактировать файлы:

```
sudo ee /etc/motd
sudo vi /etc/motd
```

Установленные редакторы включают в себя ee, jed, joe и vi*

Редактор vi

- Редактор по умолчанию на любом UNIXe
- Может быть тяжел в использовании
- Если вы его уже знаете и предпочитаете – используйте его
- Мы предоставляем справку в формате PDF на wiki семинара

Другие редакторы

ee

– ESC – меню редактора

– Стрелки работают ожидаемо

jed

– F10 – меню редактора

– Стрелки работают ожидаемо

joe

– Ctrl-k-h - меню редактора

– Ctrl-c – отмена

– Стрелки работают ожидаемо

Другие инструменты

Завершить текущую программу: CTRL+C

```
$ ping yahoo.com
PING yahoo.com (67.195.160.76): 56 data bytes
64 bytes from 67.195.160.76: icmp_seq=0 ttl=45 time=221.053 ms
64 bytes from 67.195.160.76: icmp_seq=1 ttl=45 time=224.145 ms
^C      ← нажмите CTRL + C
```

Просмотр файловой системы:

- `cd /etc`
- `ls`
- `ls -l`

Переименование и удаление файлов

- `mv file file.bak`
- `rm file.bak`

Запуск и остановка сервисов

Стандартный метод

```
sudo service named [stop|start|
restart]
```

Проверка процесса по имени

- `ps auxwww | grep http`

```
gollum# ps auxwww | grep http
root        2694   0.0  0.2 147672   6592  ??  Ss    5:32AM   0:00.03 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2695   0.0  0.2 147672   6900  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2696   0.0  0.2 147672   6900  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2697   0.0  0.2 147672   6588  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2698   0.0  0.2 147672   6588  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2699   0.0  0.2 147672   6588  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2700   0.0  0.2 147672   6908  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2701   0.0  0.2 147672   6780  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2702   0.0  0.2 147672   6704  ??  I     5:32AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
www         2749   0.0  0.2 147672   6896  ??  I     5:34AM   0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT
root        4072   0.0  0.0  10056   1088  v0  I+    5:40AM   0:00.00 tail -f /var/log/httpd-access.log
root        4091   0.0  0.0  16424   1472   2  S+    5:44AM   0:00.00 grep http
```

Просмотр файлов

Иногда файлы просматриваются при помощи программы постраничного просмотра (“more”, “less”). Examples:

```
man sudo
less /usr/local/etc/nagios/nagios.cfg-sample
```

- Пробел для следующей страницы
- “b” страница назад
- “q” выход
- “/” и образец для поиска (/text)

“`less` это more”

Отладка: файлы логов

Логи важны при решении проблем. Они (главным образом) лежат в /var/log/

Популярные лог файлы:

/var/log/messages

/var/log/httpd-error.log

/var/log/maillog

/etc/namedb/log/* (только в этом курсе)

Посмотреть последнюю запись в логе:

```
tail /var/log/messages
```

Видеть новые строки по мере их появления:

```
tail -f /var/log/messages
```

Подсоединение к машинам при помощи SSH

Зайти на вашу виртуальную машину можно через ssh. На Windows пользуйтесь putty.exe – скачать здесь:

http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

или здесь

http://noc.ws.nsrc.org/

Вход пользователем “sys*adm*” на:

- auth1.grpX ➔ 10.20.X.1
- auth2.grpX ➔ 10.20.X.2
- resolv.grpX ➔ 10.20.X.3

Где “X” - номер вашей группы. Пароль получите в классе.

Логин

Linux/MacOS

Откройте терминал, затем:

```
ssh -l adm auth1.grpX.dns.nsrc.org
```

Windows

Putty (или другой клиент SSH) соединитесь с:

```
auth1.grpX.dns.nsrc.org
```

- Как пользователь ”*sysadm*”
- Согласитесь принять ключ
- Повторите для `resolv.grpX` и `auth2.grpX` **(если есть)**

“X” - номер вашей группы

После соединения…

- Поиграйтесь с редактором ee
  - … или `vi` или `joe` или `jed`
- Отредактируйте “message of the day” чтобы идентифицировать машину как вашу:
  - `sudo ee /etc/motd`
- Отсоединитесь и зайдите снова чтобы увидеть ваши изменения. Повторите для каждой виртуальной машины…

Вопросы

?