Advanced DNS Operations & Security

A few UNIX basics

Our chosen platform

FreeBSD 9.0 64 bit

- UNIX OS, BSD variant
- 30 year history
- no GUI, we administer using SSH

- There are other platforms you could use:
  - Ubuntu, Debian, CentOS/RedHat, …
- This isn't a UNIX admin course
  - Worksheets are mostly step-by-step
  - Please help each other or ask us for help

Some things we'll need to do…

Be *root* when necessary: `sudo <cmd>`

Install packages:

```
pkg_add -r <package_name>
```

Edit files:

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

Installed editors include ee, jed, joe and vi*

vi editor

- The default editor for all UNIX
- Can be difficult to use
- If you know it and prefer to use vi please do
- We provide a PDF reference in the materials on the workshop wiki

Other editors

ee

- ESC brings up the editor menu
- Cursors work as you expect

jed

- F10 brings up the editor menu
- Cursors work as you expect

joe

- Ctrl-k-h brings up the editor menu
- Ctrl-c aborts
- Cursors work as you expect

Other tools

Terminate foreground program: 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      ← here press CTRL + C
```

Browse the filesystem:

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

Rename and delete files

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

Starting and stopping services

Standard method

- `/etc/rc.d/named restart`

Check for a process by name

- `ps auxwww | grep named`

```
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
```

Viewing files

Sometimes files are viewed through a pager program (“more”, “less”, “cat”). Examples:

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

- Space bar for next page
- “b” to go backwards
- “q” to quit
- “/” and a pattern (/text) to search

“`less` is more”

Troubleshooting: Logfiles

Log files are critical to solve problems. They reside (largely) in /var/log/

Some popular log files include:

/var/log/messages
/var/log/httpd-error.log
/var/log/maillog
/etc/namedb/log/* (this class only)

To view the last entry in a log file:

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

To view new entries as they happen:

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

Connecting via SSH to machines

Login to your virtual machine using ssh. On Windows use putty.exe - download from:

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

or

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

Connect as user "*adm*" to:

- master.grpX ➔ 10.10.X.1
- cache.grpX ➔ 10.10.X.2
- auth.grpX ➔ 10.10.X.3

Where "X" is your group number. The password is given in class.

Logging in

Linux/MacOS

First, open a terminal, then:

```
ssh -l adm master.grpX.ws.nsrc.org
```

Windows

Putty (or other SSH program) connect to:

```
master.grpX.ws.nsrc.org
```

1. As user "*adm*"
2. Accept the key
3. Repeat for `cache.grpX` and `auth.grpX`

"X" is the number of your group

After you are logged in…

- Experiment with the `ee` editor
  - … or `vi` or `joe` or `jed` if you prefer
- Edit the "message of the day" to identify your virtual machine as yours:
  - `sudo ee /etc/motd`
- Log out and log in again to see your changes. Repeat this for each virtual machine…

Questions

?