Apprenticeship Virtual Machine Setup

A. Download a Debian net install ISO from http://www.debian.org/CD/netinst
B. VirtualBox install and setup
    1. Download and install VirtualBox from http://www.virtualbox.org
    2. Start VirtualBox
    3. Select from the menu: File/Preferences...
        a. Select from the options list: Network
        b. Click the screwdriver icon entitled "Edit host only network"
        c. Verify the IP address is set to 192.168.56.1
        d. Verify the network mask is set to 255.255.255.0
        e. Deactivate the DHCP server option on the DHCP Server tab
        f. Click OK until back to the main screen
    4. Click the "New" icon to create a new virtual machine
        a. Follow the wizard, type the VM name (any name you like) and selecting Linux for the operating system and Debian for the version.
        b. Select 512 MB for memory
        c. Select "Create a new hard disk"
        d. Select "VDI" for file type
        e. Select "Dynamically allocated"
        f. Set the size to be 6 GB
        g. Click the "Create" button
    5. Select the new virtual machine, then click the "Settings" icon
        a. Under "System", under "Motherboard", deselect all the "Extended Features" options
        b. Under "System", under "Processor", select "Enable PAE/NX"
        c. Under "Storage", under "IDE Controller", click the "Add CD/DVD Device" icon
            i. Select "Choose Disk"
            ii. Select the Debian ISO downloaded earlier and click "OK"
            iii. Select the "Empty" IDE Controller and click the "Remove Attachment" icon toward the bottom of the section
        d. Under "Network":
            i. For each real adapter on the host machine, set 'Attached to:' select box to "Bridged Adapter" and the name of the real adapter
            ii. Set a virtual adapter to "Host-only Adapter" with "VirtualBox Host-Only Ethernet Adapter"
            iii. Leave any other remaining virtual adapters disabled
    6. Click "OK" to return to the VirtualBox Manager main screen
C. Debian install
    1. With the new virtual server instance selected, click the "Start" icon
    2. After boot, click "Install"
    3. Follow the on screen prompts, selecting the defaults (or whatever seems obvious)
    4. When on the "Configure the network" setup screen, the install wizard will ask what network interface to use for primary
        - Select the network interface that has network connectivity (that you set up in step B.5.d.i)
        - For example, if you have Adapter 1 as your local hardline, Adapter 2 as Wifi, and Adapter 3 as your Host-only Adapter, and you are connected via Wifi on the host machine, then select "eth1" for Adapter 2
    5. For the hostname, enter an all lower-case, single word name or something similar (pick a name you like)
    6. For the domain, enter "example.org"
    7. Continue with the installation; user accounts should be first name, all lower-case
    8. Continue with the wizard; when you get to partition disks, select "Guided - use entire disk"
    9. Select "All files in one partition", then "Finish partitioning and write changes to disk", then "Yes"
    10. Select the defaults for the package manager section; leave the HTTP proxy information blank
    11. Do not participate in the package usage survey
    12. Under the "Software selection" screen, deselect all software packages, then continue
    13. Install the GRUB book loader to the master boot record
D. Debian setup
    1. After install is complete, the system will automatically reboot the VM; when it completes, login
    2. `su`
    3. `vi /etc/network/interfaces`
        a. Remove the entire file's contents
        b. Add a localhost loopback

```
auto lo
iface lo inet loopback
```

        c. For each virtual adapter that is a bridged adapter, add a section as follows (incrementing "eth0" to "eth1" and beyond for subsequent adapters):

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

d. The final virtual adapter should then be the Host-only Adapter; include the following for the final adapter (changing "eth2" to be whatever the actual ethernet number is correct given the number of adapters your system has):

```
auto eth2
iface eth2 inet static
address 192.168.56.2
gateway 192.168.56.1
netmask 255.255.255.0
network 192.168.56.0
broadcast 192.168.56.255
```

4. `/etc/init.d/networking restart`
5. Note that you may need to shutdown your Host-only Adapter if you encounter a failure of apt or cpan network installation operation; to do so, but only if necessary: `ifdown eth2`
6. `vi /etc/apt/sources.list`; replace the file with the following:

```
deb http://ftp.us.debian.org/debian/ squeeze main contrib non-free
deb-src http://ftp.us.debian.org/debian/ squeeze main contrib non-free

deb http://security.debian.org/ squeeze/updates main contrib non-free
deb-src http://security.debian.org/ squeeze/updates main contrib non-free

deb http://ftp.us.debian.org/debian/ squeeze-updates main contrib non-free
deb-src http://ftp.us.debian.org/debian/ squeeze-updates main contrib non-free
```

7. `apt-get update`
8. `apt-get dist-upgrade`
9. `apt-get install screen sudo build-essential ssh vim less perl-doc ack-grep zip unzip telnet curl`
10. Setup multi-user screen
    - `chmod u+s /usr/bin/screen`
    - `chmod 755 /var/run/screen`
11. sudo setup
    a. `addgroup sysadmin`
    b. `usermod -a -G sysadmin username` where "username" is your username
    c. `visudo`; At end of file, add: `%sysadmin ALL=NOPASSWD: ALL`

E. Establish a non-console/SSH connection to the local host-only address
1. Open your favorite SSH client and connect to 192.168.56.2 on port 22
2. Login to your user account (not the root account)

F. ssh hardening
1. Setup `~/.ssh` directory as follows:
    a. `cd`
    b. `mkdir .ssh`
    c. `chmod 700 .ssh`
    d. `cd .ssh`
    e. `touch authorized_keys id_rsa known_hosts`
    f. `chmod 644 authorized_keys known_hosts`
    g. `chmod 600 id_rsa`
    h. `vi authorized_keys`
    i. Add all authorized keys, which should look like: `ssh-rsa AAA== name`
        - "AAA" is a very long string of characters
        - "name" is the certificate name
        - These rows are the public keys from the public/private certificate pair for the server that's going to try to contact this server
        - If you don't have a certificate key pair, you can create one with `ssh-keygen` (`man ssh-keygen` for more information)
2. `sudo su -` to become root
3. `vi /etc/ssh/sshd_config`
    - *Line 26:* `PermitRootLogin no`
    - *Line 50:* `PasswordAuthentication no`
4. `/etc/init.d/ssh reload`

G. Establish a non-console/SSH connection to an Internet-connected address
1. Logout of the current SSH connection
2. Using the console window:
    a. `ifconfig` to list the cards and IP addresses currently active
    b. `ifdown eth2` (replace "eth2" with the adapter representing your host-only connection) to shutdown your host-only connection
    c. Shutdown all other adapters except the local loopback adapter and one adapter with an Internet connection
    d. Note the IP address assigned to that one last adapter
3. Open your favorite SSH client (putty is mine on Windows) and connect to the IP address on port 22
4. Login to your user account (not the root account)

5. `sudo su -` to become root

H. shorewall
1. `apt-get install shorewall shorewall-doc`
2. `cp /usr/share/doc/shorewall/examples/one-interface/* /etc/shorewall`
3. `vi /etc/shorewall/rules` and replace the default settings with the following:

```
# ping
ACCEPT net $FW icmp
ACCEPT $FW net icmp

# ssh
ACCEPT net $FW tcp 22

# dns bind packets
ACCEPT net net tcp 53
ACCEPT net net udp 53

# traceroute allowance
Trcrt/ACCEPT all all
```

4. `vi /etc/shorewall/interfaces` and duplicate the "eth0" line for any other interfaces available
5. `vi /etc/default/shorewall` (set startup=1)
6. `/etc/init.d/shorewall restart`

I. nginx
1. `apt-get install libpcre3 libpcre3-dev libpcrecpp0 libssl-dev zlib1g-dev openssl`
2. `apt-get install nginx`
3. `rm -rf /var/www/nginx-default`
4. `mkdir -p /var/www/htdocs`
5. `vi /var/www/htdocs/index.html` and create a simple "Hello World" HTML page
6. `chown -R www-data.www-data /var/www`
7. `mkdir /etc/nginx/certificates; cd /etc/nginx/certificates`
8. `openssl genrsa -des3 -out primary.key 1024` (use "primary" for the passphrase)
9. `openssl req -new -key primary.key -out primary.csr` (use "primary" for the passphrase)

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Example
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:*.example.org
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

10. `openssl rsa -in primary.key -out primary.key` (use "primary" for the passphrase)
11. `openssl x509 -req -days 9000 -in primary.csr -signkey primary.key -out primary.crt`
12. `rm primary.csr`
13. `cd /etc/nginx/`
14. `vi nginx.conf` and replace with the following:

```
user www-data;
worker_processes 5;

error_log /var/log/nginx/error.log;
pid       /var/run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    include      /etc/nginx/mime.types;
    default_type application/octet-stream;
    access_log   /var/log/nginx/access.log;

    sendfile    on;
    tcp_nopush  on;
    tcp_nodelay on;

    gzip              on;
    gzip_proxied      any;
```

```
    gzip_buffers      16 8k;
    gzip_http_version 1.1;
    gzip_vary         on;
    gzip_comp_level   6;
    gzip_disable      "MSIE [1-6]\.";
    gzip_types
        text/plain
        text/css
        application/json
        application/x-javascript
        text/xml
        application/xml
        application/xml+rss
        text/javascript;

    server_names_hash_bucket_size 128;
    keepalive_timeout             65;

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/sites-enabled/*;
}
```

15. `vi ssl.conf` and insert the following:

```
ssl                       on;
ssl_certificate           certificates/primary.crt;
ssl_certificate_key       certificates/primary.key;
ssl_session_timeout       5m;
ssl_protocols             SSLv2 SSLv3 TLSv1;
ssl_ciphers               ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
ssl_prefer_server_ciphers on;
```

16. `vi sites-available/default` and replace with the following:

```
server {
    listen 80;
    server_name example.org www.example.org localhost localhost.localdomain;
    server_name_in_redirect off;

    location / {
         root  /var/www/htdocs;
         index index.html;
    }
}

server {
    listen 443;
    server_name example.org www.example.org localhost localhost.localdomain;
    server_name_in_redirect off;

    include /etc/nginx/ssl.conf;

    location / {
         root  /var/www/htdocs;
         index index.html;
    }
}
```

17. `vi conf.d/proxy.conf` and replace with the following:

```
proxy_redirect          off;
proxy_set_header        Host                    $host;
proxy_set_header        X-Real-IP               $remote_addr;
proxy_set_header        X-Forwarded-For         $proxy_add_x_forwarded_for;
proxy_set_header        X-Forwarded-User        $remote_user;
proxy_set_header        X-Forwarded-Request-Uri $request_uri;
client_max_body_size    10m;
client_body_buffer_size 128k;
proxy_connect_timeout   90;
proxy_send_timeout      90;
proxy_read_timeout      90;
proxy_buffers           32 4k;
```

18. `/etc/init.d/nginx start`
19. Shorewall configuration
    a. `vi /etc/shorewall/rules` and add the following:

```
# http and https
ACCEPT net $FW tcp 80,443
```

b. `/etc/init.d/shorewall restart`

20. Test by pointing a browser to the IP address you connected SSH to last; you should get redirected to HTTPS, then asked to approve the self-signed certificate

J. Samba (optional, not necessary, but helpful)

1. `apt-get install samba smbfs smbclient`
   a. Workgroup: WORKGROUP(change this to whatever matches your local workgroup, or leave defaulted if unsure)
   b. Modify smb.conf: No
2. `vi /etc/samba/smb.conf` and change the following under the "[homes]" section

```
browsable = yes
locking = no
# read only = yes
writable = yes
create mask = 644
directory mask = 755
oplocks = no
level2 oplocks = no
```

3. `/etc/init.d/samba restart`
4. `smbpasswd gryphon` (replace "gryphon" with your username)
5. Shorewall configuration
   a. `vi /etc/shorewall/rules` and add the following:

```
#samba
SMB(ACCEPT) $FW net
SMB(ACCEPT) net $FW
```

   b. `/etc/init.d/shorewall restart`

K. mysql

1. `apt-get install libcrypt-ssleay-perl mysql-server-5.1 mysql-client-5.1 libmysqlclient15-dev libdbi-perl libdbd-mysql-perl`
2. `mysql -uroot -p`
3. Run the following line, but replace "gryphon" with your preferred MySQL username:

```
GRANT ALL ON *.* TO 'gryphon'@'%' IDENTIFIED BY '********' WITH GRANT OPTION;
```

4. `cd /root`
5. `wget http://search.cpan.org/CPAN/authors/id/C/CA/CAPTTOFU/DBD-mysql-4.018.tar.gz`
6. `tar xvfpz DBD-mysql-4.018.tar.gz`
7. `cd DBD-mysql-4.018`
8. `perl Makefile.PL`
9. `make`
10. `make install`
11. `cd ..`
12. `rm -rf DBD-mysql-4.018*`
13. `/etc/init.d/mysql stop`
14. `vi /etc/mysql/my.cnf`
    - Comment-out "bind-address"
    - innodb_file_per_table
    - innodb_thread_concurrency = 4
15. `/etc/init.d/mysql start`

L. Miscellaneous Tools, Programs, and Systems

1. `apt-get install subversion`
2. `apt-get install postgresql postgresql-doc postgresql-contrib-8.4 libdbi-perl libdbd-pg-perl`
3. `apt-get install couchdb`
4. `apt-get install libtemplate-perl libtemplate-perl-doc libtext-csv-perl libyaml-perl libjson-perl`
5. `curl -L cpanmin.us | perl - Mojolicious`