Roger-Skyline-1

table of contents

Legend

`#OH#` : run on the host machine
`#IN#` : if needed

```
$ command to run
```

```
> return
```

```
file to edit
```

Variables

HOSTNAME	debian
ROOT_PSWD	root
USERNAME	till
USER_PSWD	till
USER_MAIL	tde-roqu@student.42.fr
IP	10.12.130.30
NETMASK	255.255.255.252 / 30
GATEWAY	10.12.254.254
SSH_PORT	55555
HTTP_DEFAULT_PORT	80
HTTPS_DEFAULT_PORT	443
GIT_REPO	https://github.com/tillderoquefeuil/doggos.git
REPO_NAME	doggos.com
PASS_SSL	tillssl

Environnement

VirtualBox
Debian Img

VB settings

New VM > settings > Storage > Controller: IDE empty disk : Choose Virtual Optical Disk File
☑Live CD/DVD

New VM > settings > Network > Adapter 1 > Attached to: Bridged Adapter

VM installation

```
Install

Language
English

Location for timezone
Other > Europe > France

Local settings
United Kingdom

Keyboard
British English

Hostname
<HOSTNAME>

Domain name
*blank*

Root password
<ROOT_PSWD>

Fullname for new user
<USERNAME>

Username
<USERNAME>

New user password
<USER_PSWD>

Partitioning method
Guided - use entire disk

Select disk to partition
SCSI2

Partitioning scheme
Separate /home, /var, and /tmp partitions
```

```
Overview
Finish partitioning and write changes to disk

Write the changes to disks
Yes

Scan another CD or DVD?
No

Debian archive mirror country
France

Debian archive mirror
deb.debian.org

HTTP proxy
*blank*

Participate in the package usage survey
No

Software to install
ssh-server
standard utilities system

Install the GRUB boot loader
Yes

Device for boot loader installation
/dev/sda
```

VM > settings > Storage > Controller: IDE Secondary Master: Remove Disk From Virtual Drive
☐ Live CD/DVD

```
Installation is complete
Continue
```

```
> debian login: <USERNAME>
> Password: ****
```

User set up

```
$ su
$ apt-get install sudo
$ sudo usermod -a -G sudo <USERNAME>
$ nano /etc/sudoers
```

```
root ALL=(ALL:ALL) ALL
<USERNAME> ALL=(ALL:ALL) ALL
```

```
$ su - <USERNAME>
```

TEST

```
$ sudo -v
> [sudo] password for <USERNAME>:
> Sorry, user <USERNAME> may not run sudo on <HOSTNAME>.
```

Update/grade

```
$ sudo apt-get update && sudo apt-get upgrade
```

Static IP

```
$ sudo nano /etc/network/interfaces
```

```
~~iface enp0s3 inet dhcp~~
auto enp0s3
```

```
$ sudo nano /etc/network/interfaces.d/enp0s3
```

```
iface enp0s3 inet static
     address <IP>
     netmask <NETMASK>
     gateway <GATEWAY>
```

```
$ sudo service networking restart
$ sudo reboot
```

TEST

```
$ ip a
> inet <IP>/<NETMASK> brd <IP> scope global enp0s3
> inet <IP>/<NETMASK> brd <IP> scope global dynamic enp0s3

$ ping 8.8.8.8
> PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
> 64 bytes from 8.8.8.8: imcp_seq=1 ttl=55 time=1.69 ms
> From <IP> imcp_seq=1 Destination Host Unreachable
```

SSH

1. configuration ssh

```
$ sudo apt-get install openssh-server #IN#
$ sudo nano /etc/ssh/sshd_config
```

```
port <SSH_PORT>
```

```
$ sudo service sshd restart
$ ssh <USERNAME>@<IP> -p <SSH_PORT> #OH#
```

2. configuration public keys

```
$ ssh-keygen -t rsa #OH#
$ ssh-copy-id -i id_rsa.pub <USERNAME>@<IP> -p <SSH_PORT> #OH#
```

3. block root login & password authentication

```
$ sudo nano /etc/ssh/sshd_config
```

```
PermitRootLogin no
```

```
PasswordAuthentication no
```

```
$ sudo service sshd restart
```

TEST

```
$ ssh <USERNAME>@<IP> -p <SSH_PORT> #OH#
> Enter passphrase for key '~/.ssh/id_rsa':
> <USERNAME>@<IP>'s password:
```

Firewall

1. UFW

```
$ sudo apt-get install ufw #IN#
$ sudo ufw status
$ sudo ufw enable #IN#
$ sudo ufw allow <SSH_PORT>/tcp
$ sudo ufw allow <HTTP_DEFAULT_PORT>/tcp
$ sudo ufw allow <HTTPS_DEFAULT_PORT>
```

2. Denial Of Service Attack

```
$ sudo apt-get install fail2ban #IN#
$ cd /etc/fail2ban/jail.d
$ sudo cp defaults-debian.conf defaults-debian.local
$ sudo nano defaults-debian.local
```

```
[sshd]
enabled = true
port = 55555
bantime = 60
maxentry = 3

[http-get-dos]
enabled = true
port = http,https
filter = http-get-dos
```

```
logpath = /var/log/apache2/access.log
maxretry = 300
findtime = 300
bantime = 600
action = iptables[name=HTTP, port=http, protocol=tcp]
```

```
$ cd /etc/fail2ban/filter.d
$ sudo nano http-get-dos.conf
```

```
# Fail2Ban configuration file
[Definition]

# Note: This regex will match any GET entry in your logs, so basically all
valid and not valid entries are a match.
failregex = ^<HOST> -.*"(GET|POST).*

# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
ignoreregex =
```

3. Restart

```
$ sudo ufw reload
$ sudo service fail2ban restart
```

TEST

```
$ sudo nano /etc/ssh/sshd_config
```

```
#PasswordAuthentication no
```

```
$ sudo service sshd restart
```

```
$ ssh <USERNAME>@<IP> -p <SSH_PORT> #OH#
#try a false password as many time
#as the maxentry value in the [sshd] section
> ssh: connect to host <IP> port <SSH_PORT>: Connection refused #OH#
```

```
> <USERNAME>@<IP>'s password: #OH#
```

RESET

```
#wait for end of ban
#depends on the bantime in the [sshd] section
#in /etc/fail2ban/jail.d/defaults-debian.local
$ sudo fail2ban-client status sshd
> |- Filter
> |  |- Currently failed:     0
> |  |- Total failed:   15
> |  `- File list:      /var/log/auth.log
> `- Actions
>    |- Currently banned:     0
>    |- Total banned:   2
>    `- Banned IP list:
```

Scans protection

```
$ sudo apt-get install portsentry #IN#
$ sudo nano /etc/portsentry/portsentry.conf
```

```
BLOCK_UDP="1"
BLOCK_TCP="1"
...
#KILL_ROUTE="/sbin/route add -host $TARGET$ reject"
...
KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"
```

```
$ sudo nano /etc/default/portsentry
```

```
TCP_MODE="atcp"
UDP_MODE="audp"
```

```
$ sudo service portsentry restart
```

TEST

```
$ nmap -v -Pn -p 0-2000,60000 <IP> #OH#
> Increasing send delay for <IP> from 0 to 5 due to 11 out of 13 dropped
probes since last increase.
> PORT    STATE  SERVICE
> 80/tcp  closed http
> 443/tcp closed https
```

RESET

```
$ sudo nano /etc/hosts.deny
```

```
ALL: <IP> : DENY
```

```
$ sudo iptables -t nat -F
$ sudo iptables -t nat -X
$ sudo iptables -F
$ sudo iptables -X
$ sudo ufw reload
```

Stop services

```
$ sudo systemctl disable console-setup.service
$ sudo systemctl disable keyboard-setup.service
$ sudo systemctl disable apt-daily.timer
$ sudo systemctl disable apt-daily-upgrade.timer
$ sudo systemctl disable syslog.service
```

TEST

```
$ sudo service --status-all
```

Cron update

```
$ sudo nano /usr/bin/update.sh
```

```
#!/bin/sh
(date && sudo apt-get update && sudo apt-get upgrade -y && echo "") | sudo tee -a /var/log/update_script.log
```

```
$ sudo crontab -e
```

```
#UPDATE & UPGRADE PACKAGE
@reboot /usr/bin/update.sh
0 4 * * 6 /usr/bin/update.sh
```

TEST

```
$ sudo crontab -l
> #UPDATE & UPGRADE PACKAGE
> @reboot /usr/bin/update.sh
> 0 4 * * 6 /usr/bin/update.sh
```

OR

```
$ sudo crontab -e
```

```
#...
#UPDATE & UPGRADE PACKAGE
@reboot /usr/bin/update.sh
* * * * * /usr/bin/update.sh
```

```
$ cat /var/log/update_script.log
> ACTUAL DATE
> Hit:1 http://security.debian.org/debian-security buster/updates InRelease
> [...]
> 0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Cron monitoring

```
$ sudo nano /usr/bin/cronMonitor.s
```

```
#!/bin/bash

TMP="/var/tmp/checkcron"
FILE="/etc/crontab"
HASH=$(sudo md5sum $FILE)

if [ ! -f $TMP ]
then
    echo "$HASH" | sudo tee $TMP
    exit 0
fi

if [ "$HASH" != "$(cat $TMP)" ]
then
    echo "$HASH" | sudo tee $TMP > /dev/null
    echo "$FILE has been modified !" | sudo mail -s "$FILE modified" root
fi
```

```
$ sudo crontab -e
```

```
#...
#CHECK ETC/CRONTAB
0 0 * * * /usr/bin/cronMonitor.sh
```

TEST

```
$ sudo crontab -e
```

```
#...
#CHECK ETC/CRONTAB
* * * * * /usr/bin/cronMonitor.sh
```

```
$ sudo nano /etc/crontab
```

```
# ADD ANYTHING AT THE END OF FILE
```

```
$ ls /var/tmp
> checkcron
$ cat /var/mail/<USERNAME>
> From root@debian Tue Oct 01 12:08:01 2019
> [...]
> Subject: /etc/crontab modified
> To: <root@debian>
> [...]
> Date: Tue, 01 Oct 2019 12:08:01 -0400
>
> /etc/crontab has been modified !
```

LAMP

1. A for Apache

```
$ sudo apt-get install apache2 #IN#
$ sudo ufw allow 'WWW Full'
#test apache server on http://<IP>
```

2. M for MariaDb

```
$ sudo apt-get install mariadb-server #IN#
$ sudo mysql_secure_installation
> Enter current password for root (enter for none): <ROOT_PSWD>
> Change the root password? [Y/n] n
> Remove anonymous users? [Y/n] Y
> Disallow root login remotely? [Y/n] Y
> Remove test database and access to it? [Y/n] Y
> Reload privilege tables now? [Y/n] Y

$ sudo mariadb
> MariaDB [(non)]> GRANT ALL ON *.* TO '<USERNAME>'@'localhost' IDENTIFIED
BY '<USER_PSWD>' WITH GRANT OPTION;
> MariaDB [(non)]> FLUSH PRIVILEGES;
```

```
> MariaDB [(non)]> exit
#mariadb -u <USERNAME> -p
```

3. P for PHP

```
$ sudo apt-get install php libapache2-mod-php php-mysql #IN#
$ sudo nano /etc/apache2/mods-enabled/dir.conf
```

```
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl ~~index.php~~
index.xhtml index.htm
</IfModule>
```

```
$ sudo service apache2 restart
```

Web deployment

```
$ sudo apt-get install git #IN#
$ cd /var/www
$ git clone <GIT_REPO> <REPO_NAME>
$ sudo chown -R $USER:$USER /var/www/<REPO_NAME>
$ sudo chown -R 755 /var/www/<REPO_NAME>

$ sudo nano /etc/apache2/sites-available/<REPO_NAME>.conf
```

```
<VirtualHost *:80>
    ServerAdmin <USERNAME>@<REPO_NAME>
    ServerName <REPO_NAME>
    ServerAlias www.<REPO_NAME>
    DocumentRoot /var/www/<REPO_NAME>/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

```
$ sudo a2ensite <REPO_NAME>.conf
$ sudo a2dissite 000-default.conf
```

```
$ sudo service apache2 reload
#test your website on http://<IP>
```

Self signed ssl certificate

```
$ sudo apt-get install openssl #IN#
$ sudo mkdir /var/www/<REPO_NAME>/certs
$ cd /var/www/<REPO_NAME>/certs

$ sudo openssl genrsa -des3 -passout pass:<PASS_SSL> -out server.pass.key
2048
$ sudo openssl rsa -passin pass:<PASS_SSL> -in server.pass.key -out
server.key
$ sudo rm server.pass.key
$ sudo openssl req -new -key server.key -out server.csr
> Country Name (2 letter code) [AU]:FR
> State or Province Name (full name) [Some-State]:Ile-de-France
> Locality Name (eg, city) []:Paris
> Organization Name (eg, company) [Internet Widgits Pty Ltd]:<REPO_NAME>
> Organizational Unit Name (eg, section) []:
> Common Name (e.g. server FQDN or YOUR name) []:<USERNAME>
> Email Address []:<USER_MAIL>
> A challenge password []:
> An optional company name []:

$ sudo openssl x509 -req -sha256 -days 365 -in server.csr -signkey
server.key -out server.crt

$ sudo nano /etc/apache2/sites-available/<REPO_NAME>.conf
```

```
<VirtualHost *:80>
    ...
    Redirect "/" "https://<IP>/"
    ...
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin <USERNAME>@<REPO_NAME>
    ServerName <REPO_NAME>
```

```
    ServerAlias www.<REPO_NAME>
    DocumentRoot /var/www/<REPO_NAME>/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    #SSL
    SSLEngine On
    SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
    SSLCertificateFile "/var/certs/server.crt"
    SSLCertificateKeyFile "/var/certs/server.key"
</VirtualHost>
```

```
$ sudo a2enmod ssl
$ sudo service apache2 restart
#test your website on https://<IP>
```