i**192.168.56.2**

**• Размер диска 8Гб**

**• Хотя бы один раздел размером 4.2 Гб**

fdisk -l - проверка размера диска

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Создание non-root юзера для работы за машиной**

**• Настройка sudo**

su - авторизация под рутом

adduser nu - создание пользователя с правами по дефолту

apt-get install sudo - скачивание и установка пакетов с судо

adduser nu sudo - добавление пользователя в судо группу

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Настройка статического ip с маской сети /30**

Host Network Manager в VB -> Create

30 маска сети - это 255.255.255.252

DHCP Server - off

Debian -> Settings -> Network -> Adapter 2 (Attached to Host-only Adapter; Name vboxnet 0)

sudo vim /etc/network/interfaces

Изменение конфига:

# The primary network interface - интерфейс для обычной сети

allow-hotplug enp0s3 - перезапуск интерфейса при падении

auto enp0s3 - запуск интерфейса при включении системы

iface enp0s3 inet static - статический ip

address 10.0.2.1

gateway 10.0.2.2

netmask 255.255.255.252

# The second network interface - интерфейс для SSH

allow-hotplug enp0s8

auto enp0s8

iface enp0s8 inet static

address 192.168.56.2

netmask 255.255.255.252

Проверить наличие ssh сервиса

Проверить, активный ли он service Ssh status

скачать emacs для нормальной работы s

Ip a - проверка интерфейсов

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Смена дефолтного порта SSH**

**• Доступ по SSH должен быть настроен по ключам**

**• sudd**

**• Авторизация без пароля**

ssh-copy-id -p5458 nu@192.168.56.2 - с хоста, который подключается по SSH

sudo :

port 5458

PermitRootLogin no - авторизация под рутом через SSH

PasswordAuthentication no - авторизация без пароля

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Правила файрвола должны быть настроены только с сервисам, используемыми извне VM (SSH, http, https)**

**• Защита от DoS атаки**

**• Защита от сканирования**

ipables -L - просмотр правил файрвола

Правила файрвола:

iptables -p INPUT DROP - политика INPUT по дефолту на DROP

iptables -p FORWARD DROP - политика FORWARD по дефолту на DROP

iptables -p OUTPUT ACCEPT - политика OUTPUT по дефолту на ACCEPT

iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT - разрешение только установленных соединений или связанных с установленными

iptables -A INPUT -f -j DROP - сброс фрагментированных пакетов

iptables -A INPUT -p tcp -m recent --rcheck --seconds 60 --hitcount 2 --name scan --mask 255.255.255.255 --rsource -j DROP - подсчет и огран-mичение подключений по tcp для защиты от сканирования портов при 2 подключениях, которые не прошли по правилам

iptables -A INPUT -p udp -m recent --rcheck --seconds 60 --hitcount 1 --name scan --mask 255.255.255.255 --rsource -j DROP - подсчет и ограничение подключений по ump для защиты от сканирования портов при 1 подключении, которое не прошло по правилам

iptables -A INPUT -p tcp --dport 5458 -m recent --rcheck --seconds 200 --hitcount 5 --name scan\_ssh —rsource -j DROP - подсчет и ограничение подключений по ssh

iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate NEW -m limit --limit 40/sec --limit-burst 40 -j ACCEPT - разрешение на подключение по http, https не больше 40 за секунду

iptables -A INPUT -p tcp --dport 5458 -m recent --set --name scan\_ssh —rsource - подсчет подключений по SSH

iptables -A INPUT -p tcp -m multiport --dports 5458 -m conntrack --ctstate NEW -j ACCEPT - разрешение на подключение по ssh

iptables -A INPUT -p tcp -m multiport --dports 80,443 -m connlimit --connlimit-above 10 --connlimit-mask 32 -j DROP - разрешение на 10 подключений с уникального ip

iptables -A INPUT -p tcp --dport 5458 -m connlimit --connlimit-above 2 -j DROP - не больше двух подключений по SSH

iptables -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST -m limit --limit 1/s --limit-burst 2 -j DROP - защита от спама определенными типами пакетов

iptables -A INPUT -p tcp ! --dport 5458 -m recent --set --name scan --rsource - подсчет подключений не по SSH

iptables -A INPUT -p udp -m recent --set --name scan --rsource - подсчет подключений по udp

b) ufw - упрощенный вариант манипулирования iptables.

• ufw default deny incoming - выключить входящие запросы.

• ufw default allow outgoing - включить выходящие запросы.

• ufw allow 8822/tcp - открыть порт для ssh.

• ufw allow http - открыть порт для http.

• ufw allow https - открыть порт для https.

с) Чтобы проверить порты - nmap:

• nmap (your ip) -p 1-65535

7. portsentry - утилита защищающая от сканирований.

• В /etc/portsentry/portsentry.conf изменить:

a) BLOCK\_UDP=“1” BLOCK\_TCP=“1"

b) KILL\_ROUTE=“/sbin/iptables -I INPUT -s $TARGET$ -j DROP”

• В /etc/default/portsentry изменить:

a) TCP\_MODE=“atcp”

b) UDP\_MODE=“audp”

• В /etc/portsentry/portsentry.ignore.static добавить:

a) 192.168.58.53/255.255.255.252

• /etc/init.d/portsentry restart

• В системных логах (/var/log/syslog) должно появится:

a) debian portsentry[1001]: adminalert: PortSentry is now active and listening.

• После этих манипуляций защита от сканирований установлена.

https://www.youtube.com/watch?v=24M8dStXARg

http://aidalinux.ru/w/PortSentry\_-\_средство\_противодействия\_сканированию\_портов

http://www.smeegul.kiev.ua/portsentry.html

https://www.lissyara.su/articles/freebsd/security/portsentry/kreilly

Для обновления конфигурации iptables при каждом ребуте используется утилита iptables-persistent

Iptables-save > /etc/iptables/rules.v4

service netfilter-persistent restart

Backup iptables - /home/idunaver/iptables.backup

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сканирование портов

nmap 192.168.56.2

DoS attack

cd slowloris 192.168.56.2

python slowloris.py 192.168.56.2

Проверка активности nginx - service nginx status

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Остановка сервисов, которые вам не нужны для этого проекта**

service —status-all - проверка статусы всех сервисов

sudo systemctl disable applciation - убрать сервис из автозагрузки

service application stop - отключение сервиса

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Написать скрипт, который обновляет пакеты, легирует обновления в файл /var/log/update\_script.log. Создайте отложенную задачу, запускающую скрипт раз в неделю в 4 часа ночи и каждый раз, когда машины будет перезагружена.**

**• Напишите скрипт, который будет мониторить изменения файла /etc/crontab и отправлять емейл ауту, если файл будет изменен. Он должен запускаться каждый день в полночь.**

crontab -l - вывести конфигурации crontab

sudo vim /etc/crontab - настройка правил crontab

0 4 \* \* 1 root sh ~/scripts/update\_script.sh

@reboot root sh ~/scripts/update\_script.sh

0 0 \* \* \* root sh ~/scripts/modif\_cron.sh

@reboot root sh ~/scripts/deployment.sh

https://crontab.guru - расшифровка

update\_script.sh

#!bin/bash

echo "###START OF UPDATE###" >> /var/log/update\_script.log

echo "Update date:" >> /var/log/update\_script.log

date >> /var/log/update\_script.log

echo >> /var/log/update\_script.log

echo "LASTEST UPDATED PACKAGES:" >> /var/log/update\_script.log

apt-get update -y && apt-get upgrade -y

grep upgrade /var/log/dpkg.log >> /var/log/update\_script.log

echo "\n" >> /var/log/update\_script.log

modif\_cron.sh

#!bin/bash

SHASUM1=$(shasum /etc/crontab | awk '{ print $1 }')

SHASUM2=$(shasum /root/scripts/cronfile/crontab | awk '{ print $1 }')

if [ "$SHASUM1" != "$SHASUM2" ] ; then

echo "Cron modified" | sendmail -v tulupov1995@gmail.com

cp /etc/crontab /root/scripts/cronfile/crontab

fi

exit 0

Отправка писем происходит через smtp

Настройка smtp

http://itautsors.ru/ssmtp-nastroyka-otpravki-pochty-s-ubuntudebianlinux

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Сервер, который доступен по ip**

**• Установка самоподписанного SSL сертификата**

http://192.168.56.2

https://192.168.56.2

Создание SSL-сертификата

sudo mkdir /etc/nginx/ssl - директория для ssl

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt - создание ключа и сертификата при помощи следующей команды

**• openssl**: базовый инструмент командной строки для создания и управления сертификатами, ключами и другими файлами OpenSSL.

**• req**: эта подкоманда указывает, что на данном этапе нужно использовать запрос на подпись сертификата X.509 (CSR). X.509 – это стандарт инфраструктуры открытого ключа, которого придерживаются SSL и TLS при управлении ключами и сертификатами. То есть, данная команда позволяет создать новый сертификат X.509.

**• —x509**: данная опция вносит поправку в предыдущую субкоманду, сообщая утилите о том, что вместо запроса на подписание сертификата необходимо создать самоподписанный сертификат.

**• —nodes**: говорит OpenSSL пропустить опцию защиты сертификата парольной фразой. Нужно, чтобы при запуске сервер Nginx имел возможность читать файл без вмешательства пользователя. Установив пароль, придется вводить его после каждой перезагрузки.

**• —days 365**: эта опция устанавливает срок действия сертификата (как видите, в данном случае сертификат действителен в течение года).

• —**newkey rsa:2048**: эта опция позволяет одновременно создать новый сертификат и новый ключ. Поскольку ключ, необходимый для подписания сертификата, не был создан ранее, нужно создать его вместе с сертификатом. Данная опция создаст ключ RSA на 2048 бит.

**• —keyout:** эта опция сообщает OpenSSL, куда поместить сгенерированный файл ключа.

**• —out**: сообщает OpenSSL, куда поместить созданный сертификат.

Country Name (2 letter code) [AU]:RU

State or Province Name (full name) [Some-State]:Moscow

Locality Name (eg, city) []:Moscow

Organization Name (eg, company) [Internet Widgits Pty Ltd]:21School

Organizational Unit Name (eg, section) []:

Common Name (e.g. server FQDN or YOUR name) []:192.168.56.2

Email Address []:email

Настройка Nginx для поддержки SSL

vim /etc/nginx/sites-aviable/default

Добавление строк в конфиг

listen 443 ssl;

ssl\_certificate /etc/nginx/ssl/nginx.crt;

ssl\_certificate\_key /etc/nginx/ssl/nginx.key;

sudo service nginx restart - перезагрузка nginx

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Веб-приложение**

Настройка виртуальных хостов http://devacademy.ru/posts/nginx-ubuntu-1404/

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**• Автоматическое развертывание**

deployment.sh

#!/bin/bash

wget -O /var/www/example.com/html/index.html https://raw.githubusercontent.com/TulupovArtem/idunaver\_general/master/roger/index.html

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_