Выполнил Мешечкин Д. Инфобез-2345

Задание 1: Настроить сетевой фильтр, чтобы из внешней сети можно было обратиться только к сервисам http и ssh (80 и 443).

Выполнение данного задания аналогично заданию 3* из Домашнего задания урока 6. Для выполнения данного задания берётся всё та же многострадальная ВМ сервиса Cloud.Yandex, на момент выполнения ДЗ виртуалке был присвоен IP 51.250.111.203; для выполнения задания очистим все цепочки iptables:

```
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -t nat -F
sudo iptables -t mangle -F
sudo iptables -F
sudo iptables -X #дополнительно можно "прибить" сохранённый конфиг iptables
```

Далее начал заполнять цепочки iptables :

```
#iptables -A INPUT -p tcp --dport=22 -j ACCEPT #для дальнейшей работы по ssh со своей машины
#iptables -A INPUT -p tcp --dport=80 -j ACCEPT
#iptables -A INPUT -p udp --dport=80 -j ACCEPT
#iptables -A INPUT -p tcp --dport=443 -j ACCEPT
#iptables -A INPUT -p udp --dport=443 -j ACCEPT
#iptables -A INPUT -p icmp --icmp-type echo-request
-j ACCEPT
#iptables -P INPUT DROP
#данный список отрежет любые подключения к ВМ из внешней сети, кроме портов 22, 80, 443, дополнительно оставлен прием запросов icmp для пинга сервера. Таким образом была настроена цепочка INPUT. Дополнительно можно пробить с помощью nmap
#nmap 51.250.111.203 #самое простое быстрое сканирование, которое показывает открыте порты 22, 80, 443, впрочем что и требовалось.
```

Дополнительно можно установить правила для цепочки OUTPUT, выставив правила RELATED,ESTABLISHED для установленных соединений, а все остальные - в "DROP".

Задание 2: Запросы, идущие на порт 8080, перенаправлять на порт 80.

iptables -t nat -I PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80 #переадрессация пакетов tcp порта с 8080 на порт 80
iptables -t nat -I PREROUTING -p udp --dport 8080 -j REDIRECT --to-port 80 #переадрессация пакетов udp порта с 8080 на порт 80
#Проверял через iptables -t nat -L -nv, количество запросов на порт 8080 отображается в 1 и 2 столбцах вывода в виде количества пакетов и байтах прошедших через цепочку.

Задание 3: Настроить доступ по ssh только для вашего IP-адреса (или из всей сети вашего провайдера).

Для выполнения данного задания желательно иметь белый IP, спасибо провайдеру (нет), данную услугу он не предоставляет за разумные средства в силу региона ¯_(-_-)_/¯
За "постоянный белый IP" приму тот серый, который выдает провайдер, от него и будут все танцы, IP выданный провайдером 194.190.63.232;

#iptables -I INPUT -p tcp -s 194.190.63.232 --dport=22 -j ACCEPT #добавил правило подключения в цепочку на первую строку цепочки, где -s - источник, в формате address[/mask]. Маска не была указана по причине отсутствия информации от провайдера.
#iptables -D INPUT -p tcp --dport=22 -j ACCEPT #удаление записи сделанной в первом задании. В данном случае есть некоторое везение в сохранении подключения по SSH.

По большому счёту - задание кажется выполненным. Для дальнейшей работы с данными параметрами сохраняю их **#iptables-save > /etc/iptables-conf/iptables-rule_new.ipv4**; последующая загрузка списка цепочек **#iptables-restore -v /etc/iptables-conf/iptables-rule_new.ipv4**

Задание 4*/5* не выполнялись на данный момент, но их выполнение не будет закинуто в мусорку.