Урок 8. Практика. Как защитить свой сервер

1. Настроить сетевой фильтр, чтобы из внешней сети можно было обратиться только к сервисам https, http и ssh (443, 80 и 22).
2. Запросы, идущие на порт 8080, перенаправлять на порт 80.
3. Настроить доступ по ssh только для вашего IP-адреса (или из всей сети вашего провайдера).

Client:

- ssh -i ~/.ssh/id_rsa gb@35.233.72.52 *or* Cloud shell (Terminal)

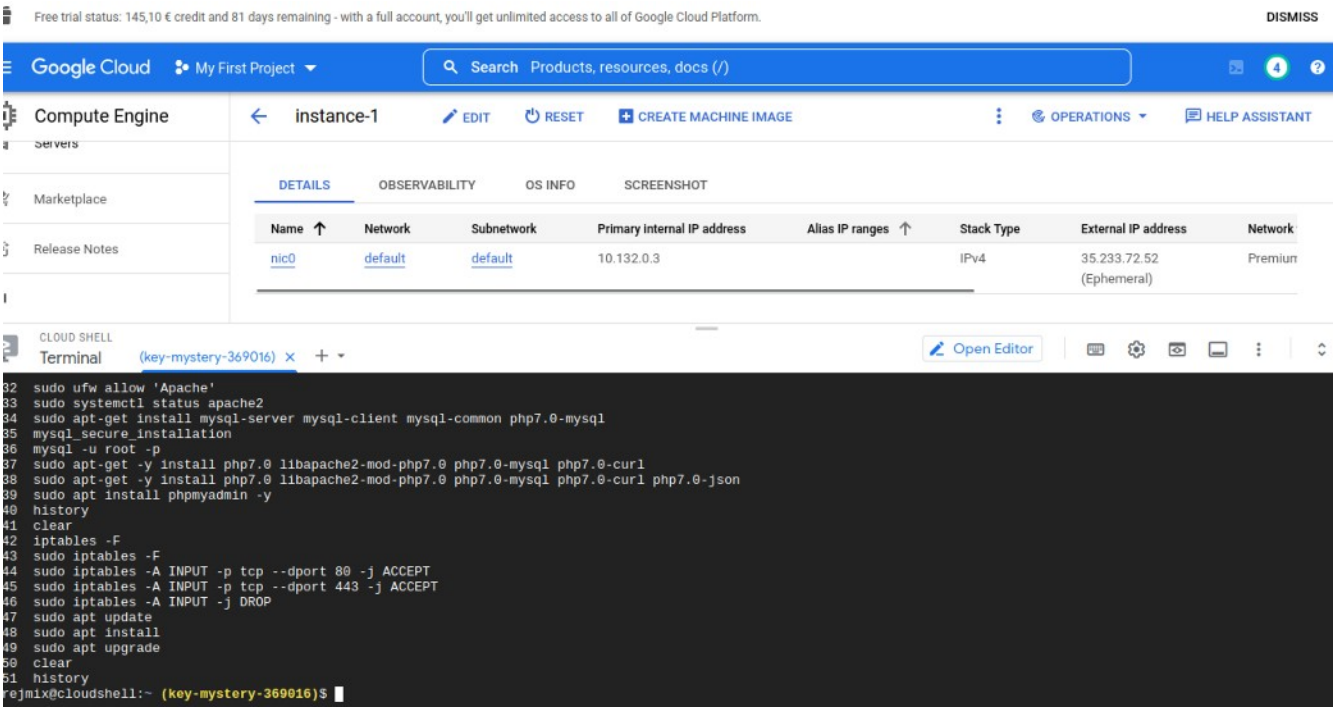
Server:

- apt install openssh-server
- netstat -ntpl
- nano /etc/ssh/sshd_config PermitRootLogin yes
- ip a
- putty (ssh) connect with link/ether inet ip *and* port: 22
- adduser --force-badname NEWUSER11
- password: „867W2o%iTN%&H3A%+ANDPASSWD(m)s27dy7)aH8bj)“
  generate from https://randstuff.ru/password/
- usermod -a -G sudo NEWUSER11
  Блокируем ненужных пользователей
- sudo usermod -L root sudo usermod -L ubuntu и др.
  Защищаем SSH (выбрать любой из случайных *Port_No*)
- cat /proc/sys/net/ipv4/ip_local_port_range
- less /etc/services
- sudo nano /etc/ssh/sshd_config Меняем *Port 22* на выбранный *Port_No* выше
- systemctl restart sshd
- sudo netstat -ntlp|grep *Port_No*
- sudo systemctl reboot
- chmod 600 authorized_keys ключи ... public private
- scp -P *PORT_NO* id_rsa.pub
- ssh -p *PORT_NO* NEWUSER11@ipnumber
  Отключаем возможность логиниться руту и доступ по паролям
- sudo nano /etc/ssh/sshd_config
- PermitRootLogin *no*
- PasswordAuthentication *no*
- sudo systemctl restart sshd
- ls ~/.bash_history
- netstat -ntl
- netstat -ntla
- netstat -ntlap
- ps ax
- cat /etc/passwd
- sudo less /var/log/auth.log
- sudo less /etc/crontab
- less .ssh/authorized_keys

1. Настроить сетевой фильтр, чтобы из внешней сети можно было обратиться только к сервисам https, http и ssh (443, 80 и 22).

Server http (80) и ssh (443):

- `apt install openssh-server`
- `(sudo) iptables -F`
- `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
  разрешить входящий трафик к сервисам HTTP:
- `iptables -A INPUT -p tcp --dport 443 -j ACCEPT`
  разрешить входящий трафик к сервисам HTTPS
- `iptables -A INPUT -j DROP`
  остальной входящий трафик надо запретить



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

- iptables -F
- iptables -A INPUT -p tcp --dport 80 -j ACCEPT
  разрешить входящий трафик к сервисам HTTP
- iptables -A INPUT -p tcp --dport 443 -j ACCEPT
  разрешить входящий трафик к сервисам HTTPS
- iptables -t nat -A PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80
  запросы, идущие на порт 8080, перенаправлять на порт 80
- iptables -A INPUT -j DROP
  остальной входящий трафик надо запретить

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

- `iptables -F`
- `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
  `разрешить входящий трафик к сервисам HTTP`
- `iptables -A INPUT -p tcp --dport 443 -j ACCEPT`
  `разрешить входящий трафик к сервисам HTTPS`
- `iptables -t nat -A PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80`
  `Запросы, идущие на порт 8080, перенаправлять на порт 80`
- `iptables -A INPUT -p tcp --src 35.233.72.52 --dport 22 -j ACCEPT`
  `Входящий трафик по ssh только для вашего IP-адреса (или из всей сети вашего провайдера).`
- `iptables -A INPUT -j DROP`
  `остальной входящий трафик надо запретить`