Linux

- ???? ?? ????? ? SSH
- ?????? ??????? ? ?? root ? ????????? ??
- ????????? fail2ban (?????? ?? ?????????)
- ?????????? ??????? ?? ??? ? iptables
- ??????? ?? Linux Hardening (?????????)
- ?????????? ?????????? ???????????? ?????? IP ? UFW

Вход по ключу в SSH

?????? ????????????? SSH ?? ?? ??????????? ????? (?? ???????), ????? ??????? ?????? ????????? ???? ?? ?????. ???? ?????? SSH ??????? ???????? ?? ????????? ? ??????? ???????. ?????????? ?????? ???????????? ? ?????????????? ??????????, ??? ?????????? ??? ???????. ?????? ????? ???????? ?????? ??????, ?? ??????? ????????? ???????? ????.

????????????? ? ???????? ?????? ??????? ?? ?????????? ??????? ?????????? ????????? ????? . ? ?????? ????????????? ??????? ????????? ?????? ????????? ? ????????????.

?? ? ??????? 2023 ???? ?????????? ??????? ?????? ? ????????? ????????????? ????????? RSA, ??? ????????? ????? ?? ????? ???????????? ??????? ???????????? ????????????? ??????. ?? ?????? Linux (???? ? ??? ?) ????????? ????????? ???????:

```
ssh-keygen -t ecdsa -b 521
```

????? ???????? ?????? ??????? Enter. ???? ????? ?????? ??? ??? ???????? ???? ??? ???????? ??????.

> ?????????? ?????? ? ????????? ????? ????????? ????????????? ?????????????.

????????? ???????? ?? ?????? ?? ??????? ????? ???????? ?? SSH (???? ?), ? ???????? ?????????? ???????????? ???? ??? ????? `.ssh`, ?? ?? ?????????? ???????:

```
cd ~
mkdir .ssh
```

???????? ?????????? ?????????? ????? (`my_key.pub`) ? ????????? ??? ?????????? ? ???? ???????? ?????????? ???????????? root `authorized_keys` ? ????? `.ssh` ?????? ??????? ????, ??? ???????? ????? ???????????? ??????? ??? ????????? ???????? (? ????? ?????? ????????? ???? ??? ?????????? ?? ???? ?):

```
cat my_key.pub >> .ssh/authorized_keys
```

???? ???????? ???? ????? ????????? ? ??????? ?????? ???????:

```
ssh-copy-id -i /root/.ssh/my_key root@<???? ?>
```

?????? ?? ????? ? ????? ???????? ?????? ??????? sshd, ????? ?? SSH ?? ?????? ???? ??? ????????:

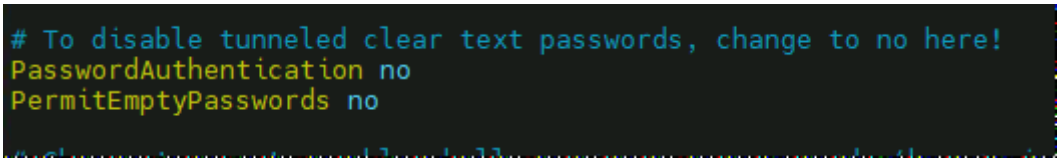
```
vi /etc/ssh/sshd_config
```

??????????????/????????? ????????? ??????:

```
PasswordAuthentication no
PermitEmptypasswords no
LoginGraceTime 0

# if ssh tunnels need
AllowTcpForwarding yes
GatewayPorts yes
```

??????? ?????????:



??????? ?? ????????????? ? ??????????? (??? vi ??????????? ????????? ??????, ????? ?????? ??? ?????? ????? - ?????).

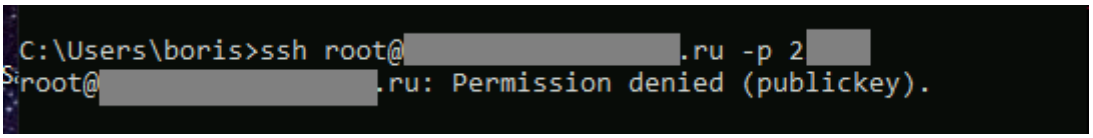
????????????? ?????? ??????? SSH ?? ????? ?:

```
systemctl restart ssh.service
```

?????? ?? ???? ? ????? ????? ?? ??????, ??? ??????????? ???????? ????, ?????? ??????? ??????????? ? ?????? ?? Linux ????????:

```
ssh -i my_key root@<???? ?>
```

? ??? ??????? ????? ?? ?????? ?? ???? ? ????? ????????? ???????? ??????:



Запрет доступа с УЗ root и служебные УЗ

?????? ??? ????????? ?????? ??? root ???????? ?????????? ???????????? `admin` ? ???????? ??????????? ? ? ???????? ?? SSH ?? ????? (???? ?????????? ????????????? ????????????? ??. **эту** ??????):

```
useradd -m admin
usermod -aG sudo admin
passwd admin
su admin
mkdir /home/admin/.ssh
cat ssh_key.pub >> /home/admin/.ssh/authorized_keys
chown -R admin:admin /home/admin/.ssh
chmod 700 /home/admin/.ssh
chmod 600 /home/admin/.ssh/authorized_keys
```

????????? ??????????? ????? ????????????? admin.

???????? ???? ?? SSH ???????????? root, ??? ????? ????? ???????? ?????? ??????? sshd:

```
vi /etc/ssh/sshd_config
```

??????? ??? ????????? (???? ????? ?????? ???) ????????? ??????:

```
PermitRootLogin no
```

??????? ?? ????????????? ? ???????????.

????????????? ?????? ??????? SSH:

```
systemctl restart sshd.service
```

????? ?????????? ?????? ??? ?? root:

```
sudo passwd -l root
```

Служебные УЗ

УЗ без возможности входа в систему

????? ?? ????? ????????????? ???????? ??? ???????? ?????? ??? SSH ????????????? ? ?.?. ???? ?????? ???????? ????? ??:

```
useradd -m portfwd
passwd portfwd
usermod -s /sbin/nologin portfwd
```

Создание УЗ для удаленных бекапов по SCP

?? ???????? Linux ??????, ?????? ????? ?????????? ??????, ?????????? ??????? ????????? ??????????? ?? ? ???????? ? ???????????? ?????, ? ????? ?????? ??? ????? `/backup` ???? ???????????? ????????? ??????:

```
adduser --home /backup user_back; chown user_back:user_back /backup; chmod 744 /backup
```

????? ?????????? ??????? ???? ?????? ??? ????????????? ????? ?? ???? ??:

```
sudo -u user_back ssh-keygen
# ???????? ???????? ?? ?????????? ????? *pub ? authorized_keys ? ???????? ?????????? ???????????? user_back
nano /backup/.ssh/authorized_keys
```

???????? ???? (??? ?????????? pub) ?????????? ??????????? ?? ????????? ????, ??????? ????? ????????????? ??? ??????? ? ???????? ??????. ????? ??? ??????????? ????? ???????????? ????????? ??????? (??? 2222 ???? SSH):

```
chmod 700 /root/.ssh/user_back_key
/usr/bin/scp -i /root/.ssh/user_back_key -P 2222 user_back@source.server:/backup/local-backup.tar.gz
/source_server_backup/source-server-backup_$(date +"%d%m%Y").tar.gz
```

??? ????????????? ????? ???????? ??? ??????? ? ??????????? ????? CRON:

```
crontab -e
```

??? ?????? ?????? ??????????? ? 00:00 ????? ???????? ????????? ?????? ? ????? ?????:

```
0 0 * * 0 /usr/bin/scp -i /root/.ssh/user_back_key -P 2222 user_back@source.server:/backup/local-backup.tar.gz
/source_server_backup/source-server-backup_$(date +"%d%m%Y").tar.gz
```

??? ???????????? ?????????? ????? ???????????? ???? ?????? https://crontab.guru/

????? ??????? ?????? ?????? 30 ????, ????? ? ??????????? ????? ???????? ????????? ???????:

```
find /source_server_backup/*.gz -type f -mtime +30 -delete
```

Настройка fail2ban (защита от брутфорса)

Fail2ban ?????? ? Linux ??????? ?? log–?????? ?????????? ????? ?????????? ????????????? ? ????????????? ??? IP ?????. ????????? ????? ???????? ? ?????????? ??????? ?? ??? ?????????? *NIX–???????, ????? ??? Apache, Nginx, Guacamole, sshd, Exim, Postfix ? ??????. ? ?????? ?????? ?? ????? ???????? ?????? SSH.

?????????:

```
apt-get -y install fail2ban
```

???????? ?????????? ? ?????????:

```
systemctl enable fail2ban
systemctl status fail2ban
systemctl start fail2ban
```

?????? ?????? ????:

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
vi /etc/fail2ban/jail.local
```

?????????? ????? jail.local:

```
[DEFAULT]
bantime  = 1d
findtime  = 4h
maxretry = 2

[sshd]
enabled = true
mode = aggressive
port = 2222
# incremental banning:
bantime.increment = true
# default factor (causes increment - 1h -> 1d 2d 4d 8d 16d 32d ...):
bantime.factor = 24
# max banning time = 6 week:
bantime.maxtime = 6w
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

? ??????? ???? fail2ban ??????? ???? 2222 ?????? ssh, ????? ?????????? ?? 1 ???? ????????? ??????????? ? ?????? 2 ???????? ??????? ????? ? ??????? 4 ?????, ?????????? ??????????????, ? ?????? ???? ???? ?? ???????? ???????? ???????? ???????? - ???? ?? 2 ??? ? ??? ?? ????????????? ????? ?????????? ?? 6 ??????.

?????????? ?????? ??? ?????????? ????? ????????????:

```
systemctl restart fail2ban
```

???????? ??????? fail2ban:

```
less /var/log/fail2ban.log
```

??????? ?????????? ??????????? ?? ???????:

```
cat /var/log/fail2ban.log | grep "\[sshd\] Ban" | wc -l
```

???????? ?????????????? IP-???????:

```
fail2ban-client status | grep "Jail list" | sed -E 's/^[^:]+:[ \t]+//' | sed 's/,//g'
```

????????????? ??????:

```
fail2ban-client set YOURJAILNAMEHERE unbanip IPADDRESSHERE
```

Разрешение доступа по гео с iptables

????????????? ??????????? ??????:

```
apt-get -y install iptables-persistent
apt-get -y install ipset
```

??? ???????????? ?????? ipset ?????????? ??????? ?????? `/etc/systemd/system/ipset-persistent.service`:

```
[Unit]
Description=ipset persistent configuration
Before=network.target

# ipset sets should be loaded before iptables
# Because creating iptables rules with names of non-existent sets is not possible
Before=netfilter-persistent.service
Before=ufw.service

ConditionFileNotEmpty=/etc/iptables/ipset

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/sbin/ipset restore -exist -file /etc/iptables/ipset
# Uncomment to save changed sets on reboot
# ExecStop=/sbin/ipset save -file /etc/iptables/ipset
ExecStop=/sbin/ipset flush
ExecStopPost=/sbin/ipset destroy

[Install]
WantedBy=multi-user.target
RequiredBy=netfilter-persistent.service
RequiredBy=ufw.service
```

???????? ???? ??????:

```
systemctl daemon-reload
systemctl enable ipset-persistent.service
systemctl restart ipset-persistent.service
```

??????? ????? ???? ?????????? ?????????? ???????:

```
ipset create "RU_zone" hash:net
for IP in $(wget -O - https://www.ipdeny.com/ipblocks/data/countries/ru.zone); do ipset add "RU_zone" $IP; done
```

?????????, ??? ?????????? ??????? ? ????:

```
ipset -L RU_zone | less
```

??? ???????????????? ???????? ????????? ? ?????????? ?? ?? ?????:

```
ipset save > /etc/iptables/ipset
ipset restore < /etc/iptables/ipset
```

????????? ??????? ??????? iptables:

```
iptables-save > /root/rules.v4
```

????????? ?????????? ? ?????? ????? (?????????? ??? ?????????????) ??????? ?? ??? ? ??????????? ????? /root/rules.v4:

```
-A INPUT -p tcp -m set --match-set RU_zone src -m tcp --dport 22000 -j ACCEPT
```

??? ???????????????? ?????? ????????? ??:

```
cp /root/rules.v4 /etc/iptables/rules.v4
```

?????????? ????? ?????? iptables:

```
iptables-restore < /etc/iptables/rules.v4
```



???????? ??????? ??? ??????????? ?????? iptables - **iptstate**

Команды по Linux Hardening (Харденинг)

?????? ?? ???????? ????? ???????????

?????? ?????? ??? ?????? ?????????? `sudo`:

```
echo "Defaults timestamp_timeout=0" >> /etc/sudoers
```

???? ? ??????? ??? ?? root ????????:

```
sudo passwd -l root
```

??????????? ????? `crontab` ?????????? ??? ????, ????? ?????????:

```
chown root:root /etc/crontab
chmod og-rwx /etc/crontab
chown root:root /etc/cron.hourly/
chmod og-rwx /etc/cron.hourly/
chown root:root /etc/cron.daily/
chmod og-rwx /etc/cron.daily/
chown root:root /etc/cron.weekly/
chmod og-rwx /etc/cron.weekly/
chown root:root /etc/cron.monthly/
chmod og-rwx /etc/cron.monthly/
chown root:root /etc/cron.d/
chmod og-rwx /etc/cron.d/
```

???????? ????????? ??????? `/home`, `/tmp`, `/var/tmp`, `/dev/shm` ?? ???????? ? ??????????
??????????? ???????? ? ???, ????????????? ??? ???????? ??????? ? ????? / `etc/fstab`:

```
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
tmpfs /dev/shm tmpfs defaults,noexec,nodev,nosuid,seclabel 0 0
```

????????? ???? ?????????? ??:

```
sudo apt purge -y ubuntu-report popularity-contest apport whoopsie
sudo apt autoremove -y
sudo apt-get autoclean
```

Блокировка источников динамическим листом IP с UFW

????????????? ??????????? ??????:

```
apt-get -y install ipset
```

??????? ???? ????:

```
ipset create "IP_ipsum4_block" hash:ip
```

????????? ???? ???????? ?? ????????????? ????? IPsum (????????????? ??? level 4 - very low false positives) ? ????????? ? ???? `/etc/ipset.rules`:

```
ipset flush "IP_ipsum4_block"; for IP in $(wget -O -
https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt); do ipset add "IP_ipsum4_block" $IP;
done; ipset save > /etc/ipset.rules
```

????????? ?????????? ?????????? ????? ? crontab (??? ????????????? ????????????: `crontab -e`):

```
0 0 * * * ipset flush "IP_ipsum4_block"; for IP in $(wget -O -
https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt); do ipset add "IP_ipsum4_block" $IP;
done; ipset save > /etc/ipset.rules
```

??? ????????????? ipset ??? ???????????? ??????? ? CRON:

```
crontab -e
```

???????? ?????? ? ??????? ? ???????????:

```
@reboot ipset restore < /etc/ipset.rules; ufw reload
```

Переустановка UFW

```
sudo apt-get purge --auto-remove ufw
sudo apt-get install ufw
sudo ufw allow 22/tcp
sudo ufw enable
sudo ufw reload
```

????? ??????? ??????? ? UFW:

```
sudo nano /etc/ufw/before.rules
```

???????? ????????? ???????? ?? COMMIT:

```
# block by ipsum4 src IPs
-A ufw-before-input -m set --match-set IP_ipsum4_block src -j DROP
```

```
# allow MULTICAST UPnP for service discovery (be sure the MULTICAST line above
# is uncommented)
-A ufw-before-input -p udp -d 239.255.255.250 --dport 1900 -j ACCEPT

# block by ipsum4 src IPs
-A ufw-before-input -m set --match-set IP_ipsum4_block src -j DROP

# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```

????????????? UFW:

```
sudo ufw reload
```

?????????, ??? ??????? ??????????? (??????????? ?????? ?????? ????????? ? ?????? ??????):

```
sudo iptables -S ufw-before-input
```

Полезные команды UFW

```
ufw status verbose
ufw allow in on eth0 from 203.0.113.102
ufw allow from 203.0.113.103 proto tcp to any port 22
ufw allow proto tcp from any to any port 80,443
ufw allow from 203.0.113.0/24 to any port 3306
sudo ufw allow 13647:13650/tcp
ufw deny out 25
ufw status numbered
ufw delete 13
ufw --force delete 13
ufw reset
```