SSH Hardening Guides

Рекомендации по настройке максимально безопасных настроек для SSH (и клиента и сервера): https://www.ssh-audit.com/hardening_guides.html

Там же можно запустить аудит: https://www.ssh-audit.com и посмотреть насколько плохо обстоят дела.

Ubuntu 22.04 LTS Server

Note: all commands below are to be executed as the root user.

Re-generate the RSA and ED25519 keys

```
rm /etc/ssh/ssh_host_*
ssh-keygen -t rsa -b 4096 -f /etc/ssh/ssh_host_rsa_key -N ""
ssh-keygen -t ed25519 -f /etc/ssh/ssh_host_ed25519_key -N ""
```

Remove small Diffie-Hellman moduli

```
awk '$5 >= 3071' /etc/ssh/moduli > /etc/ssh/moduli.safe
mv /etc/ssh/moduli.safe /etc/ssh/moduli
```

Enable the RSA and ED25519 HostKey directives in the /etc/ssh/sshd_config file:

```
sed -i 's/^\#HostKey \/etc\/ssh\/ssh_host_\(rsa\|ed25519\)_key$/HostKey
\/etc\/ssh\/ssh_host_\1_key/g' /etc/ssh/sshd_config
```

Restrict supported key exchange, cipher, and MAC algorithms

```
echo -e "\n# Restrict key exchange, cipher, and MAC algorithms, as per
sshaudit.com\n# hardening guide.\nKexAlgorithms sntrup761x25519-
sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,gss-
curve25519-sha256-,diffie-hellman-group16-sha512,gss-group16-sha512-,diffie-
hellman-group18-sha512,diffie-hellman-group-exchange-sha256\nCiphers
chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr\nMACs hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128-
etm@openssh.com\nHostKeyAlgorithms ssh-ed25519,ssh-ed25519-cert-
v01@openssh.com,sk-ssh-ed25519@openssh.com,sk-ssh-ed25519-cert-
v01@openssh.com,rsa-sha2-512,rsa-sha2-512-cert-v01@openssh.com,rsa-
sha2-256,rsa-sha2-256-cert-v01@openssh.com" > /etc/ssh/sshd_config.d/ssh-
audit_hardening.conf
```

Restart OpenSSH server

```
service ssh restart
```

Note: Because of a bug in OpenSSH, 2048-bit DH moduli will still be used in some limited circumstances. Only a maximum score of 95% is possible.

ssh, hardening, audit

From:
https://wiki.rtzra.ru/ - **RTzRa's hive**

Permanent link:
https://wiki.rtzra.ru/software/ssh/ssh-hardening-guides

Last update: **2023/11/02 17:11**