Hardening

- SSHD Hardened config [2018]

SSHD Hardened config [2018]

```
#

# This is Havoks hardened sshd_config
# Settings have been taken from https://infosec.mozilla.org/guidelines/openssh

Port 22
#ListenAddress 0.0.0.0
#ListenAddress ::

Protocol 2
# keys are default generated, but might need new keys as e.g. rsa is only 2048 bits long
HostKey /etc/ssh/ssh_host_ed25519_key
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key

# only use strong ciphers and macs
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-
nistp256,diffie-hellman-group-exchange-sha256
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-
ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

# Logging
LogLevel VERBOSE
Subsystem sftp  /usr/lib/ssh/sftp-server -f AUTHPRIV -l INFO

# Disable Root Login
PermitRootLogin no
PermitEmptyPasswords no
MaxAuthTries 3

# only enable pubkey
AuthenticationMethods publickey

# Change to yes to enable challenge-response passwords (beware issues with
```

```
# some PAM modules and threads)
ChallengeResponseAuthentication no
UsePAM yes

X11Forwarding no
PrintMotd no

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*
AllowUsers markus

IgnoreRhosts yes
```