Table of Contents

Debian SSH hardening

Apply:

```
echo 'DebianBanner no' > /etc/ssh/sshd_config.d/debian_banner.conf
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.BAK
sed -i -e 's/^X11Forwarding yes/#X11Forwarding yes/g' /etc/ssh/sshd_config
echo 'ChallengeResponseAuthentication no' >> /etc/ssh/sshd_config
echo 'AllowAgentForwarding no' >> /etc/ssh/sshd_config
echo 'AllowTcpForwarding no' >> /etc/ssh/sshd_config
echo 'MaxAuthTries 3' >> /etc/ssh/sshd_config
echo 'PasswordAuthentication yes' >> /etc/ssh/sshd_config
echo 'PermitRootLogin no' >> /etc/ssh/sshd_config
echo 'ClientAliveCountMax 0' >> /etc/ssh/sshd_config
echo 'LoginGraceTime 60' >> /etc/ssh/sshd_config
echo 'MaxStartups 10:30:60' >> /etc/ssh/sshd_config
```

Debian 9

```
echo 'KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-
sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256' >>
/etc/ssh/sshd_config
echo 'Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-
ctr,aes128-ctr' >> /etc/ssh/sshd_config
echo 'MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-
sha1' >> /etc/ssh/sshd_config
```

Debian 10

Debian 11

Networking

Edit /etc/sysctl.conf and add:

```
net.ipv4.icmp_echo_ignore_all=1
net.ipv4.ip_forward = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_synack_retries = 5
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.log_martians = 1
```

```
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

References

- https://www.digitalocean.com/community/tutorials/how-to-harden-openssh-on-ubuntu-18-04
- https://gist.github.com/latuminggi/491b4433ca3c787633321f83c37d6d3d
- https://help.defense.com/en/articles/7947052-ssh-weak-key-exchange-algorithms-enabled-linux-vulnerability
- https://unix.stackexchange.com/questions/412446/how-to-disable-ping-response-icmp-echo-in-linux-all-the-time
- https://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening/