

? Walking in Light with Christ - Faith, Computing, Diary Free Software GNU Linux, FreeBSD, Unix, Windows, Mac OS -Hacks, Goodies, Tips and Tricks and The True Meaning of life https://www.pc-freak.net/blog

Linux SSH Hardening: Good OpenSSH /etc/ssh/sshd options for increasing System Security

Author: admin



Security Hardening is a standard thing that is rarely done by most system administrators. As SSH is the standard for remote terminal access due to its simplicity encryption and wide use, the most basic thing to do as a first step of security improve on fresh installed GNU / Linux.

This is few of the things I'm aware of that improves sshd service security.

1. Strengthen OpenSSH encryption cyphers supported (usually to enable ones known with stronger encryption opts:

Ciphers aes128-ctr,aes192-ctr,aes256-ctr MACs hmac-sha2-256,hmac-sha2-512,hmac-ripemd160 KexAlgorithms diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-

1/6



? Walking in Light with Christ - Faith, Computing, Diary Free Software GNU Linux, FreeBSD, Unix, Windows, Mac OS - Hacks, Goodies, Tips and Tricks and The True Meaning of life https://www.pc-freak.net/blog

sha2-nistp384,ecdh-sha2-nistp521

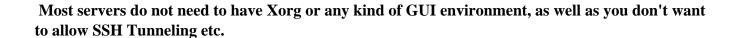
2. Disabling remote root login access
PermitRootLogin no
?3. Make User sessions exprit /setting client timeout values etc.
Default expiry interval is 5 minutes, reducing this to smth like 3 minutes is usually a good, this is done with below 2 opts.
ClientAliveInterval - Sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. ClientAliveCountMax - Sets the limit of how long a client are allowed to stay unresponsive before being disconnected.
4. Require always password on login (do not check for SSH Key auth)
PasswordAuthentication yes
- Some refer to allow only Authentication with keys also for security, if you're one of those use:
Password Authentication no



? Walking in Light with Christ - Faith, Computing, Diary Free Software GNU Linux, FreeBSD, Unix, Windows, Mac OS -Hacks, Goodies, Tips and Tricks and The True Meaning of life https://www.pc-freak.net/blog

PubkeyAuthentication yes ChallengeResponseAuthentication no

5. Disable XForwarding



X11Forwarding no

6. Disable GSSAPIAuthentication

This option is for **Single Sign on (SSO)** authentication with a password or kerberos ticket exchange. Some corporations do use it due to their complex environments to save people the hassle to use different separte passwords with the SSO) ..

- If for some reason you need this feature enabled

GSSAPIAuthentication yes GSSAPICleanupCredentials yes

7. Disable DNS lookup on remote machine (disable attempt of sshd to resolve remote hostname)



? Walking in Light with Christ - Faith, Computing, Diary

Free Software GNU Linux, FreeBSD, Unix, Windows, Mac OS - Hacks, Goodies, Tips and Tricks and The True Meaning of life https://www.pc-freak.net/blog

UseDNS no

Below is the overall good configuration to improve a bit OpenSSH security, hence make sure /etc/ssh/sshd_config have it.

vim /etc/ssh/sshd_config

Protocol 2

AddressFamily inet

AddressFamily any

 $\# Ciphers\ chacha 20\text{-poly} 1305 @ opens sh. com, aes 256\text{-gcm} @ opens sh. com, aes 128\text{-gcm} @ opens sh. com, aes 128\text{$

h.com,aes256-ctr,aes192-ctr,aes128-ctr

Ciphers aes128-ctr,aes192-ctr,aes256-ctr

MACs hmac-sha2-256,hmac-sha2-512,hmac-ripemd160

KexAlgorithms diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-

sha2-nistp384,ecdh-sha2-nistp521

##PasswordAuthentication no # yes for Isaac 1 server only

PasswordAuthentication ves

PasswordAuthentication no # yes for Isaac 1 server only

PermitRootLogin no

GSSAPI options

GSSAPIAuthentication no

GSSAPICleanupCredentials no

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no

#GSSAPIEnablek5users no

##ClientAliveCountMax 3

ClientAliveInterval 86400

ClientAliveCountMax 0

ClientAliveInterval 600

ClientAliveCountMax 3

4/6



? Walking in Light with Christ - Faith, Computing, Diary

Free Software GNU Linux, FreeBSD, Unix, Windows, Mac OS - Hacks, Goodies, Tips and Tricks and The True Meaning of life https://www.pc-freak.net/blog

ChallengeResponseAuthentication yes X11Forwarding no TCPKeepAlive no ## UseDNS no UseDNS yes

This conifg is working on most recent SSH versions as of 2020 and should work fine on most recent RHELs / Debian / SuSEs / Fedora / Ubuntu and virtually anything from the multiple Linux OS based devices bundled with **SSH Daemon**.

After sshd_config is editted test is for configuration errors.

root@linux:~# sshd -t
/etc/ssh/sshd_config line 15: Deprecated option UsePrivilegeSeparation

Deprecated options can be safely ignore but it is good practice to clear them up, they might occur if you have updated the server for multiple years due to the fact in newer OpenSSH releases some of the older configuration values were removed.

To load new made config reload sshd

root@linux:~# systemctl restart sshd
root@linux:~#

root@linux:~# systemctl status sshd

? sshd.service - OpenSSH server daemon

Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)

Active: active (running) since Fr 2020-03-06 15:47:48 CET; 1 months 1 days ago

Docs: man:sshd(8)

man:sshd_config(5)

Main PID: 4162 (sshd)

Tasks: 1



? Walking in Light with Christ - Faith, Computing, Diary Free Software GNU Linux, FreeBSD, Unix, Windows, Mac OS - Hacks, Goodies, Tips and Tricks and The True Meaning of life https://www.pc-freak.net/blog

CGroup: /system.slice/sshd.service ??4162 /usr/sbin/sshd -D

Of course keeping a good set of security is a question of always keeping up to date OpenSSH server, so besides this nice values make sure you are frequently patching sshd. Perhaps I'm missing something so if you stumble this article and you see I miss some sshd security tuning option share it.

6/6