FreeBSD 13 Base System OpenSSH Server Hardening

Date:	2022-03-17
modified:	2022-03-18
tags:	FreeBSD, OpenSSH, Hardening, SSH
description:	Howto harden the built-in OpenSSH Server on FreeBSD 13
category:	Unix
slug:	freebsd_13_base_system_openssh_server_hardening
Author:	Dominik Wombacher
lang:	en
transid:	freebsd_13_base_system_openssh_server_hardening
Status:	published

Default sshd configs tend to focus more on compatibility instead security. Therefore hardening should be one of the first things after setup a new system.

I'm using the OpenSSH Daemon which comes with the FreeBSD Base System. When you want to use the `openssh-portable` port instead, skip *Step 3*, the rest should be identical.

Step 1) Delete existing host keys, generate new rsa and ed25519 key:

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

Step 2) Create new Diffie-Hellman groups and avoid small moduli

```
ssh-keygen -G moduli-3072.candidates -b 3072
ssh-keygen -T moduli-3072 -f moduli-3072.candidates
mv moduli-3072 /etc/ssh/moduli
rm moduli-3072.candidates
```

Step 3) Disable DSA and ECDSA host keys, only use RSA and ED25519

```
sysrc sshd_dsa_enable="NO"
sysrc sshd_ecdsa_enable="NO"
sysrc sshd_ed25519_enable="YES"
sysrc sshd_rsa_enable="YES"
```

Step 4) Optimize `/etc/ssh/sshd_config`, improve security, restrict allowed key exchange, cipher and MAC algorithms

```
# Hardening
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,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-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128-etm@openssh.com
HostKeyAlgorithms ssh-ed25519,ssh-ed25519-cert-v01@openssh.com

# Security
PermitRootLogin no
AuthenticationMethods publickey
ChallengeResponseAuthentication no
UsePAM no
VersionAddendum none
X11Forwarding no
AuthorizedKeysFile .ssh/authorized_keys
Subsystem sftp /usr/libexec/sftp-server
```

Run `service sshd restart` to apply the new settings, to verify the results of your hardening, you can use the CLI Tool ssh-audit which is also available as Online Version.

Following a Custom Policy for ssh-audit based on the above recommendations:

```
name = "Custom Policy - FreeBSD 13 Base System OpenSSH Daemon (2022/03/17)"
version = 1
dh_modulus_size_diffie-hellman-group-exchange-sha256 = 2048
host keys = ssh-ed25519
key exchanges = curve25519-sha256, curve25519-sha256@libssh.org, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, 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-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, umac-128-etm@openssh.com
```

Copy the policy into a file and run `ssh-audit -P=<policy.txt> <servername>`. The result should be similar to following example without warnings or errors:

```
# general
(gen) banner: SSH-2.0-OpenSSH_8.8
(gen) software: OpenSSH 8.8
(gen) compatibility: OpenSSH 7.4+, Dropbear SSH 2018.76+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256                     -- [info] available since OpenSSH 7.4, Dropbear SSH 2018.76
(kex) curve25519-sha256@libssh.org          -- [info] available since OpenSSH 6.5, Dropbear SSH 2013.62
(kex) diffie-hellman-group16-sha512         -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(kex) diffie-hellman-group18-sha512         -- [info] available since OpenSSH 7.3
(kex) diffie-hellman-group-exchange-sha256 (2048-bit) -- [info] available since OpenSSH 4.4

# host-key algorithms
(key) ssh-ed25519                           -- [info] available since OpenSSH 6.5

# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com         -- [info] available since OpenSSH 6.5
                                            `- [info] default cipher since OpenSSH 6.9.
(enc) aes256-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes128-gcm@openssh.com                -- [info] available since OpenSSH 6.2
(enc) aes256-ctr                            -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes192-ctr                            -- [info] available since OpenSSH 3.7
(enc) aes128-ctr                            -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52

# message authentication code algorithms
(mac) hmac-sha2-256-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com         -- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com              -- [info] available since OpenSSH 6.2

# fingerprints
(fin) ssh-ed25519: SHA256:uN9Oton+VmLL793KirVFB+ilD3Bndra4I/3yFntgX8k

# algorithm recommendations (for OpenSSH 8.8)
(rec) +diffie-hellman-group14-sha256        -- kex algorithm to append
(rec) +rsa-sha2-256                         -- key algorithm to append
(rec) +rsa-sha2-512                         -- key algorithm to append
```

Sources:

- https://ozgurkazancci.com/ssh-server-security-audit-hardening-freebsd (Archive: [1], [2])
- https://gist.github.com/koobs/e01cf8869484a095605404cd0051eb11 (Archive: [1], [2])
- https://www.ssh-audit.com/hardening_guides.html (Archive: [1], [2])