Ecole d'ingénieurs et d'architectes de Fribourg
Hochschule für Technik und Architektur Freiburg

5: SSHD

Hes·so// FRIBOURG FREIBURG
Haute Ecole Spécialisée
de Suisse occidentale
Fachhochschule Westschweiz

References

[1]: http://cvedetails.com
http://www.osvdb.org
http://secunia.com
http://www.securityfocus.com
http://cve.mitre.org

Install the last version of openssh

Install the last version of sshd on the nanoPi.

1) Check the signature of the openssh package (www.openssh.com, for other systems: Linux)
2) Configure package (./configure) with these options for Intel processor:
   - With hardening (what are the hardening options)
   - Don’t install to the default directories (--prefix and *perhaps sysconfdir* (for the configuration file) options)
   - Generate code for Intel processor, check if files are stripped

3) Like point 2, but for nanoPi
4) Install sshd, ssh-keygen, moduli, sshd_config on nanoPi in this directory /root/sshd.
5) On nanoPi, create these keys (without password): rsa 4096 bits, dsa 1024 bits, ecdsa 521, ed25519 256bits. These keys are stored in /root/sshd
6) Configure sshd
   - Sshd uses only IPv4
   - Don’t allow port forwarding
   - Allow these encryption-hash algorithms: Ciphers aes256-cbc, aes256-ctr, aes128-cbc, hmac-sha-256, hmac-sha1
   - The login root is not allowed
   - Indicate a banner
7) **Optional:** Nmap scan gives the version of sshd :) `nmap –sV –p 22 192.168.0.11` → `22/tcp open ssh` **`OpenSSH 8.8`** `(protocol 2.0)`
   Modify sshd and change the original version with this string: “It is a ssh server without version”