Hardened ssh

Référence :

- https://korben.info/ssh-audit-outil-indispensable-securiser-vos-serveurs.html

Supprimer les algos d'échange de clefs

Ajouter a sshd_config :

```
# Key Exchange
KexAlgorithms -ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,ecdsa-sha2-nistp256,hmac-sha1,ecdsa-sha2-nistp256
```

Supprimer les hosts key type vulnérables

Supprimer les fichiers :

- /etc/ssh/ssh_host_ecdsa_key
- /etc/ssh/ssh_host_ecdsa_key.pub

Supprimer les algos MACs vulnérables

Ajouter a sshd_config :

```
MACs -hmac-sha1,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,sntrup761x25519-sha512@openssh.com,umac-128@openssh.com,umac-64-etm@openssh.com,umac-64@openssh.com
```

Résumé avec une conf adequat

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org
Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

Revision #1
Created 23 July 2025 12:10:30 by Stephane DUGRAVOT
Updated 23 July 2025 12:41:59 by Stephane DUGRAVOT