

Authentication native

- Le fichier `/etc/passwd` contient :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
```

- Le fichier `/etc/shadow` contient les empreintes des mots de passe

```
root:$6$GkfJ0/H/$IDtJEzDO1vh8VyDG5rnnLLMXwZl.cikulTg4wtXjq98Vlcf/
PA2D1QsT7VHSsu46B/od4IJlqENMtc8dSpBEa1:14592:0:99999:7:::
daemon:x:14592:0:99999:7:::
bin:x:14592:0:99999:7:::
sys:x:14592:0:99999:7:::
sync:x:14592:0:99999:7:::
```

Structure de l'empreinte

- Exemple d'une empreinte (obtenue par une fonction de hachage)
 - \$1\$abcdefgh\$cHJi5PXp/ki/ktXzqlk6I1
- Signification des différents termes : **\$(1)\$(abcdefgh)\$(cHJi5PXp/ki/ktXzqlk6I1)**
 - \$1 : Algorithme MD5
 - \$2 : Algorithme Blowfish
 - \$5 : Algorithme sha256
 - \$6 : Algorithme sha512
 - \$2 : Piment (salt)
 - Protection contre les attaques par dictionnaire précalculé
 - Piment en clair
 - \$3 : Empreinte résultante