

PKI sur Linux (3/4/24)

Etapas

- Générer une clé publique et une clé privée via Bitwise



https://youtu.be/eZD8fXwBGT8?si=w0Prh4Dvv6dPX6N_

- Exporter la clé publique vers le serveur Linux approprié
 - Dans `/home/`, créez un fichier appelé `authorized_keys`, collez la clé publique dans ce fichier.
 - Facultatif : changer le propriétaire et le mode du fichier `authorized_keys`

```
#Change le mode du fichier afin que seul l'utilisateur mgbi peut l'écrire, le lire et l'exécuter
chmod 700 /home/mgbi/.ssh/authorized_keys
#Change le propriétaire du fichier en l'utilisateur mgbi et le groupe mgbi (ceci et ce qui précède sont complémentaires)
chown mgbi:mgbi /home/mgbi/.ssh/authorized_keys
#Énumérez la modification apportée après ces commandes
ls -l /home/mgbi/.ssh/authorized_keys
```

- Dans `/etc/ssh/sshd_config` : PubkeyAuthentication yes / PermitTunnel yes
 - `systemctl restart sshd`
- Spécifier la clé privée pour décrypter la clé publique