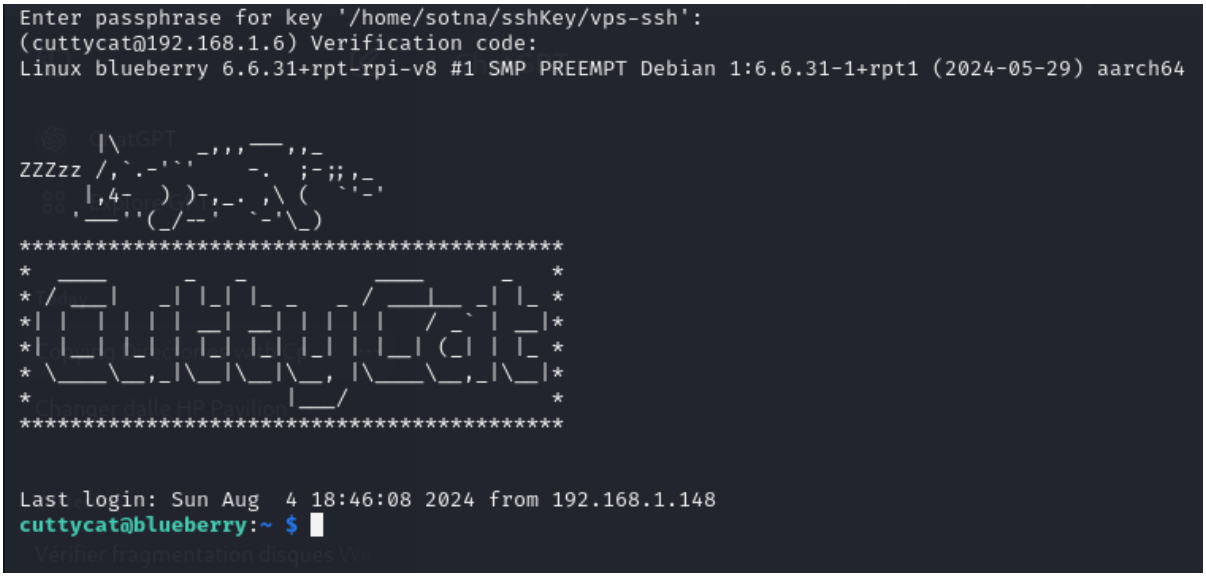
# Rapport de réalisation : Cuttycat

## Antoine GAUTREAU




Août 2024

# Table des matières

## 1. Introduction

CuttyCat est un serveur SSH dont l'accès est très sécurisé. Sa configuration m'a permis d'en apprendre beaucoup sur Linux ainsi que sur les mesures courantes de sécurisation des serveurs.

## 2. Configuration

| | |
|---|---|
| User | cuttycat |
| Hostname | blueberry |
| Distro | Raspberry Pi OS Lite |
| Device | Raspberry Pi 3 |

## 3. Sécurisation

Voici toutes les mesures de sécurité mise en œuvre :

**ssh/sshd_config :**

- Utilisation d'un port ssh différent que 22
- Utilisateur root désactivé
- Connexion SSH autorisée pour cuttycat seulement
- Connexion par mot de passe interdite
- Connexion par clé privée seulement
- 5 sessions en même temps seulement
- Exclusion du serveur au bout de 10 minutes d'inactivités
- 2FA Google Authenticator (PAM)

**fail2ban/jail.local :**

- 3 essais seulement sinon bannissement pendant 24 heures (fail2ban)

**ufw :**

- Le Firewall autorise seulement le protocole tcp sur un port spécifique seulement

**key-gen :**

- Clé rsa de 4096 bits protégée par passphrase

## 4. Connexion

Script permettant de faciliter la connexion au ssh :

**ssh -p "$PORT" -i "$KEY_PATH" "$USER"@"$HOST"**

Il faudra ensuite rentrer le passphrase puis le code temporaire généré par Google Authenticator.

## 5. Automatisation

Des scripts me permettant d'automatiser la configuration de machines linux sont déposées sur ce serveur ssh.

La configuration du terminal, mise à jour du système et installation d'outils à partir d'une liste font notamment partis de ces scripts.

Je peux les récupérer grâce à scp.

**scp -p ''$PORT" -i ''$KEY_PATH" "$USER"@"$HOST":/"$SCRIPT_PATH" /home/"$USER"**

## 6. Conclusion

Ce projet était très enrichissant j'en ai beaucoup appris.

Bonus : Le **motd** est personnalisé.