FORMATECH

Projet de mise en place d'un serveur dédié à la gestion des badges du personnel

Matthias BAGARRY / BSOD Consulting

Sommaire

1) Reformulation du besoin

Vous désirez pouvoir contrôler, et vérifier le système de badge de vos 34 employés, situés sur deux sites géographiques différents.

Nous avons noté que le traitement et la connexion à ce système sera géré par une société extérieure et que vous souhaitez un contrôle des connexions afin d'en sécuriser l'ensemble.

Nous comprenons également que vous souhaitez que ce système soit nominatif et permette un contrôle des accès selon le profil de l'utilisateur.

2) Analyse de l'existant

Nous savons que le nombre d'utilisateurs du système est de 34 personnes. Il y' a deux sites géographiques différents à gérer.

Formatech dispose déjà de ses locaux et infrastructures/réseaux, et est déjà sous contrat avec une société extérieure pour la gestion des connexions des badges.

Nous estimons que la solution la plus adaptée est un serveur dédié configuré avec le logiciel Ubuntu 24.04.3 qui possède tous les outils nécessaires pour répondre à votre demande.

3) Proposition de solution

3.1) Description

Nous proposons de mettre en place un serveur dédié, tournant sous Linux (UBUNTU 24.04.3). Cet OS permet un contrôle et une gestion efficace, sécurisée, et offre tous les outils nécessaire pour y accéder à distance.

Nous allons le configurer comme indiqué ci dessous :

- création de différents groupes selon la position géographique (Info et Tech) avec un système de droits et d'autorisations selon les profils.

- une connexion à distance permettant de gérer et modifier le serveur dédié.

- une sécurisation des connexion par la méthode Fail2ban avec 5 mots de passe erronés maximum autorisés.

3.2) Planification

	Objectif	Temps	Personnel
A	**Réunion avec les responsables sur place pour proposer notre solution et trouver un accord.**	**4H**	**MB**
B	**Installation de Ubuntu, création des utilisateurs et dossiers, gestion des droits par profil.**	**6H**	**MB**
C	**Installation du service SSH, configuration de l'accès à distance, tests.**	**2H**	**MB**
D	**Installation du service Fail2Ban, configuration des exclusions, tests.**	**2H**	**MB**

4.1) Étapes 1 du GANTT

Nous participons à une réunion afin de vous présenter les solutions les plus adaptées, notre plan de route pour l'ensemble du projet et nos prix. Après négociations nous trouvons un accord.

4.2) Étapes 2 du GANTT

Nous commençons par l'installation du serveur et de son OS, UBUNTU version 24.04.3 , en utilisant un fichier .iso.

Nous créons ensuite un compte administrateur et débutons sa configuration.

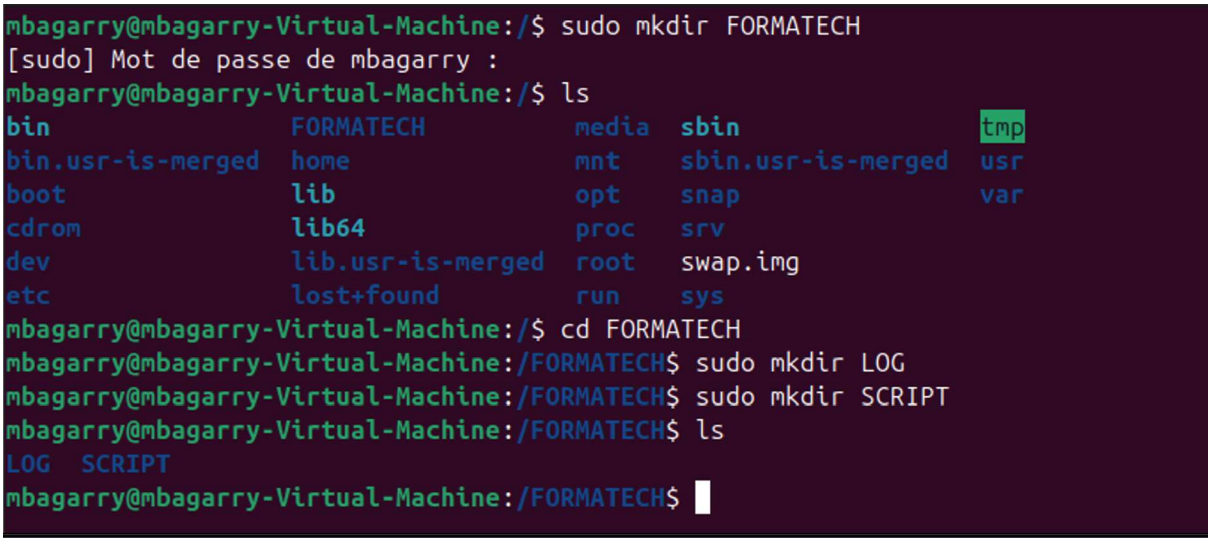
Par soucis de clarté, nous commençons par la création d'un dossier Formatech à la racine de l'arborescence du serveur.

sudo mkdir FORMATECH

Nous créons ensuite les deux dossiers LOG et SCRIPT permettant d'organiser le contrôle des badges :

sudo mkdir /FORMATECH/LOG
sudo mkdir /FORMATECH/SCRIPT

Sur la copie ci dessous, nous sommes directement dans le dossier FORMATECH



Nous créons ensuite les utilisateurs avec la commande :

sudo adduser badg1
sudo adduser badg2
sudo adduser badg3
sudo adduser badg4
sudo adduser badg5
sudo adduser badg6

(je n'ai mis qu'une seule copie pour badg1 mais la méthode et résultat sont similaires pour l'ensemble des utilisateurs)

```
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo adduser badg1
[sudo] Mot de passe de mbagarry :
info: Ajout de l'utilisateur « badg1 » ...
info: Choix d'un UID/GID dans la plage 1000 à 59999 ...
info: Ajout du nouveau groupe « badg1 » (1001) ...
info: Ajout du nouvel utilisateur « badg1 » (1001) avec le groupe « badg1 » (100
1) ...
info: Création du répertoire personnel « /home/badg1 » ...
info: Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour badg1
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
info: Ajout du nouvel utilisateur « badg1 » aux groupes supplémentaires « users
```

Nous finalisons la procédure en créant l'utilisateur maître « BADGE » :

sudo adduser badg0

```
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo adduser badg0
info: Ajout de l'utilisateur « badg0 » ...
info: Choix d'un UID/GID dans la plage 1000 à 59999 ...
info: Ajout du nouveau groupe « badg0 » (1007) ...
info: Ajout du nouvel utilisateur « badg0 » (1007) avec le groupe « badg0 » (100
7) ...
info: Création du répertoire personnel « /home/badg0 » ...
info: Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour badg0
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
info: Ajout du nouvel utilisateur « badg0 » aux groupes supplémentaires « users
```

Il nous est possible de voir l'ensemble des utilisateurs avec la commande :

cat /etc/passwd

```
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-deskto
p:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin
/nologin
mbagarry:x:1000:1000:mbagarry:/home/mbagarry:/bin/bash
sshd:x:122:65534::/run/sshd:/usr/sbin/nologin
badg1:x:1001:1001:,,,:/home/badg1:/bin/bash
badg2:x:1002:1002:,,,:/home/badg2:/bin/bash
badg3:x:1003:1003:,,,:/home/badg3:/bin/bash
badg4:x:1004:1004:,,,:/home/badg4:/bin/bash
badg5:x:1005:1005:,,,:/home/badg5:/bin/bash
badg6:x:1006:1006:,,,:/home/badg6:/bin/bash
badg0:x:1007:1007:,,,:/home/badg0:/bin/bash
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$
```

Nous avons la confirmation que tout est ok pour les utilisateurs, nous passons à la création des groupes et à la répartition des utilisateurs selon les consignes du client :

sudo usermod -aG « dossier » « user »

```
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo addgroup tech
[sudo] Mot de passe de mbagarry :
info: Choix d'un GID dans la plage 1000 à 59999 ...
info: Ajout du groupe « tech » (GID 1008)...
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo addgroup info
info: Choix d'un GID dans la plage 1000 à 59999 ...
info: Ajout du groupe « info » (GID 1009)...
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo usermod -aG tech badg1
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo usermod -aG tech badg2
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo usermod -aG tech badg3
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo usermod -aG info badg4
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo usermod -aG info badg5
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo usermod -aG info badg6
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$
```

Nous donnons au compte maître Badge (Badg0) la propriété des deux dossiers, et nous rendons le groupe info propriétaire du dossier SCRIPT

sudo chown « user » « dossier »
sudo chgrp « groupe » « dossier »

```
mbagarry@mbagarry-Virtual-Machine:/$ sudo chown badg0 /FORMATECH/LOG
mbagarry@mbagarry-Virtual-Machine:/$ sudo chown badg0 /FORMATECH/SCRIPT
mbagarry@mbagarry-Virtual-Machine:/$ sudo chgrp info /FORMATECH/SCRIPT
mbagarry@mbagarry-Virtual-Machine:/$
```

Il est nécessaire que les deux groupes soient également propriétaires du dossier LOG afin d'en recevoir les mêmes droits, cependant il n'est pas possible de donner la propriété à deux groupes sur un seul dossier.

Il existe une solution en utilisant la commande

sudo setfacl -m g:info:rx,g:tech:rx LOG

Avec cette commande nous donnons aux deux groupes les mêmes droits de lecture et d'exécution.

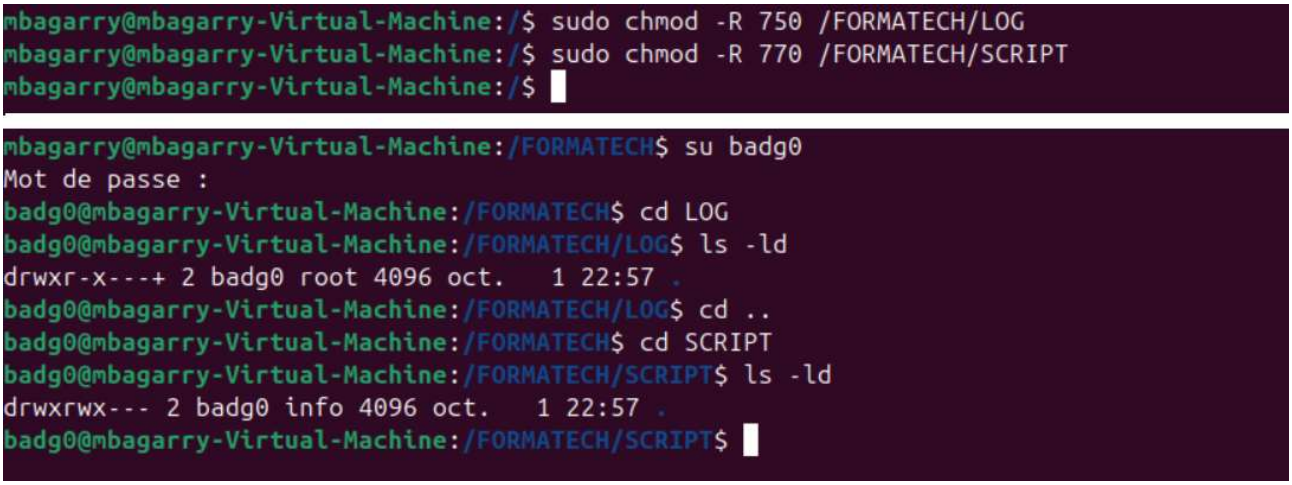
```
mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ sudo setfacl -m g:info:rx,g:tech:rx LOG

mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ getfacl LOG
# file: LOG
# owner: badg0
# group: root
user::rwx
group::r-x
group:tech:r-x
group:info:r-x
mask::r-x
other::r-x

mbagarry@mbagarry-Virtual-Machine:/FORMATECH$ getfacl SCRIPT
# file: SCRIPT
# owner: badg0
# group: info
user::rwx
group::r-x
other::r-x

mbagarry@mbagarry-Virtual-Machine:/FORMATECH$
```

Nous configurons donc le système pour que le compte BADGE ait le droit d'écriture et de lecture sur les deux dossiers, et que le groupe « info » soit également propriétaire du dossier SCRIPT pour un droit de lecture, d'écriture.

Les deux groupes « tech » et « info » sont également en lecture sur le dossier LOG comme vu ci-dessus.

sudo chmod -R 750 /FORMATECH/LOG
sudo chmod -R 770 /FORMATECH/SCRIPT

Nous utilisons la commande : ls -ld afin de vérifier les dossiers et leurs propriétaires :



4.3) Étapes 3 du GANTT

INSTALLATION DU SSH

Afin de pouvoir contrôler le serveur à distance (ici une société extérieure va gérer le service de badge) nous installons Open SSH sur le serveur :

sudo apt-get install open-ssh server

Nous vérifions ensuite si le service SSH est activé (enabled) et enclenché avec la commande

sudo systemctl status ssh
sudo systemctl enable ssh
sudo systemctl start ssh

```
mbagarry@mbagarry-Virtual-Machine:/$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-10-05 22:02:02 CEST; 35min ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1003 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1016 (sshd)
      Tasks: 1 (limit: 4602)
     Memory: 2.1M (peak: 2.5M)
        CPU: 40ms
     CGroup: /system.slice/ssh.service
             └─1016 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct. 05 22:02:02 mbagarry-Virtual-Machine systemd[1]: Starting ssh.service - OpenBSD S>
oct. 05 22:02:02 mbagarry-Virtual-Machine sshd[1016]: Server listening on 0.0.0.0 port>
oct. 05 22:02:02 mbagarry-Virtual-Machine sshd[1016]: Server listening on :: port 22.
oct. 05 22:02:02 mbagarry-Virtual-Machine systemd[1]: Started ssh.service - OpenBSD Se>
lines 1-18/18 (END)
```

Il est nécessaire d'interdire le SSH au dossier Root, c'est pourquoi nous allons configurer le fichier de config SSH avec Nano.

sudo nano /etc/ssh/sshd_config

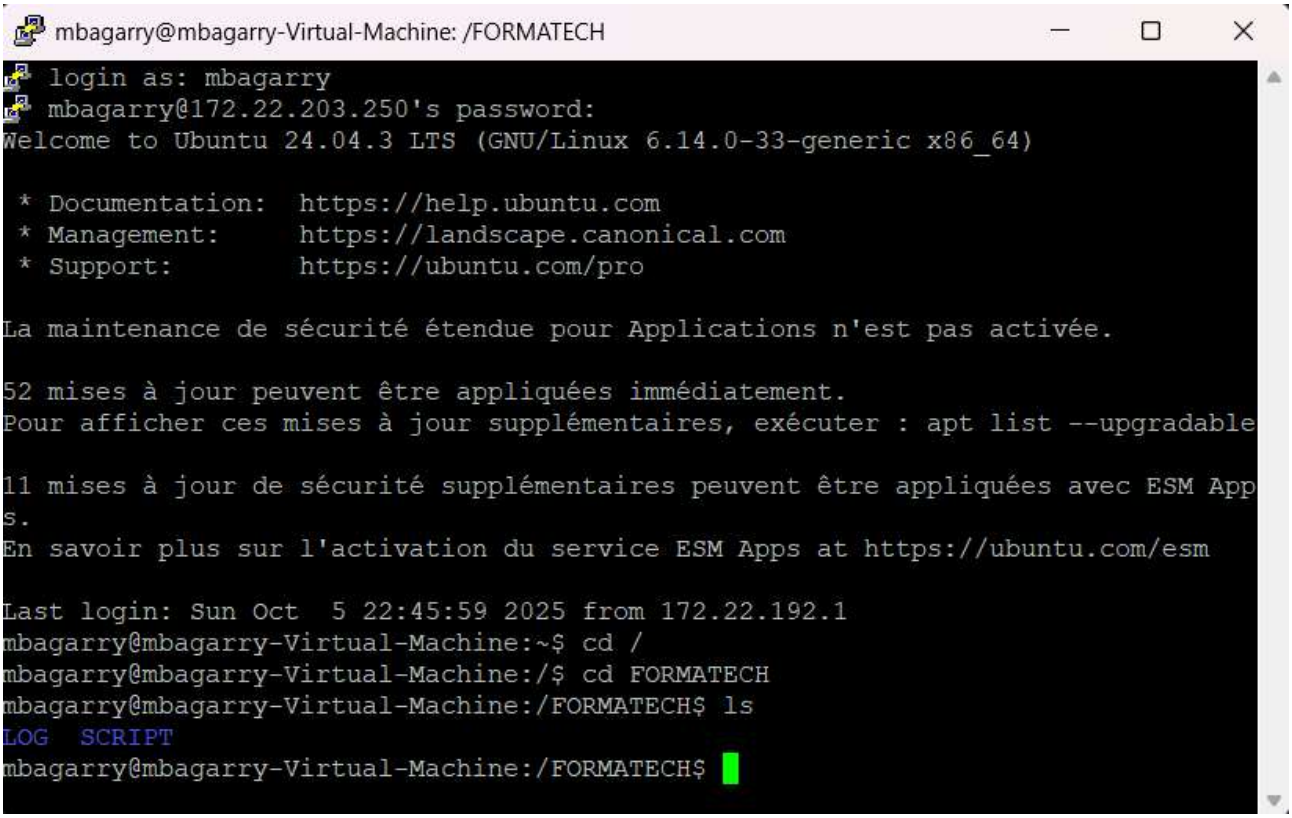
Nous y cherchons la ligne « permit root login » que nous mettons à « no »

PermitRootLogin no

```
  GNU nano 7.2                        etc/ssh/sshd_config *
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2
```

```
mbagarry@mbagarry-Virtual-Machine:/$ sudo systemctl restart ssh
mbagarry@mbagarry-Virtual-Machine:/$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-10-05 22:44:06 CEST; 12s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3628 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3630 (sshd)
      Tasks: 1 (limit: 4602)
     Memory: 1.2M (peak: 1.5M)
        CPU: 28ms
     CGroup: /system.slice/ssh.service
             └─3630 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

oct. 05 22:44:06 mbagarry-Virtual-Machine systemd[1]: Starting ssh.service - OpenBSD S>
oct. 05 22:44:06 mbagarry-Virtual-Machine sshd[3630]: Server listening on 0.0.0.0 port>
oct. 05 22:44:06 mbagarry-Virtual-Machine sshd[3630]: Server listening on :: port 22.
oct. 05 22:44:06 mbagarry-Virtual-Machine systemd[1]: Started ssh.service - OpenBSD Se>
lines 1-18/18 (END)
```

Nous sauvegardons et relançons le service SSH pour que les modifications soient pris en compte. Après avoir vérifié l'ip de la VM avec la commande « ip a », nous nous connectons via l'hôte windows pour verifier si le SSH fonctionne (avec Putty ou Mobaxterm)



4.4) Étapes 4 du GANTT

INSTALLATION DU FAIL 2 BAN

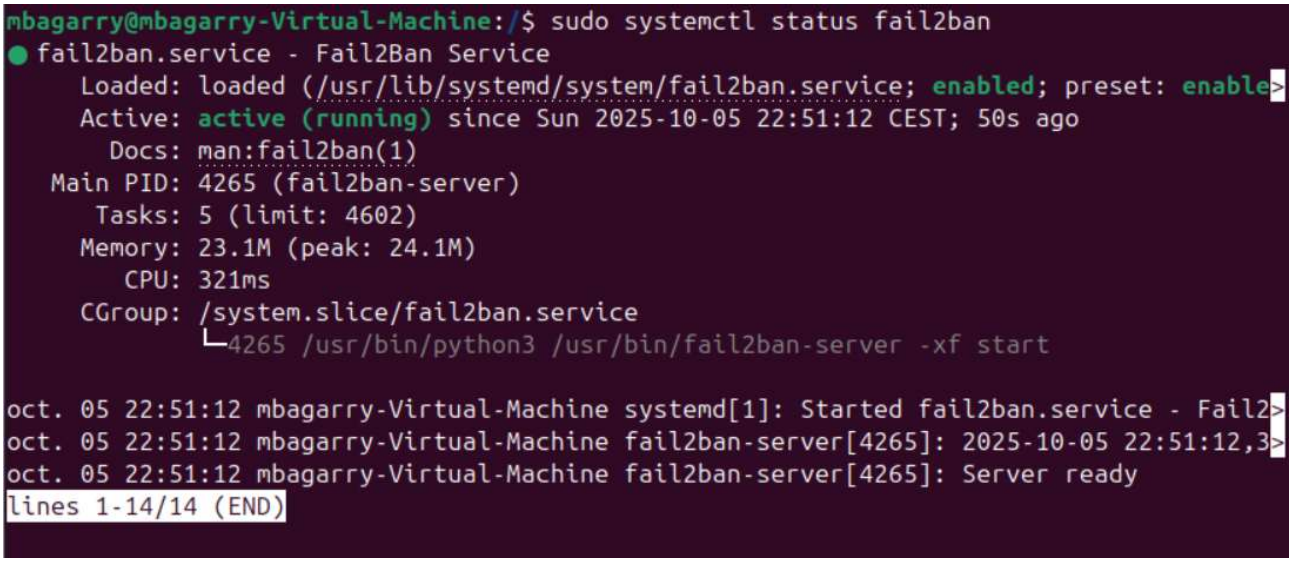
Afin de sécuriser l'ensemble du système nous installons le service Fail2Ban que nous configurons pour bloquer l'accès après 5 tentatives erronées.

Sudo apt-get install fail2ban -y

(le -y indique que nous indiquons YES à toutes les questions lors de l'installation)

Nous vérifions son activation avec la commande :

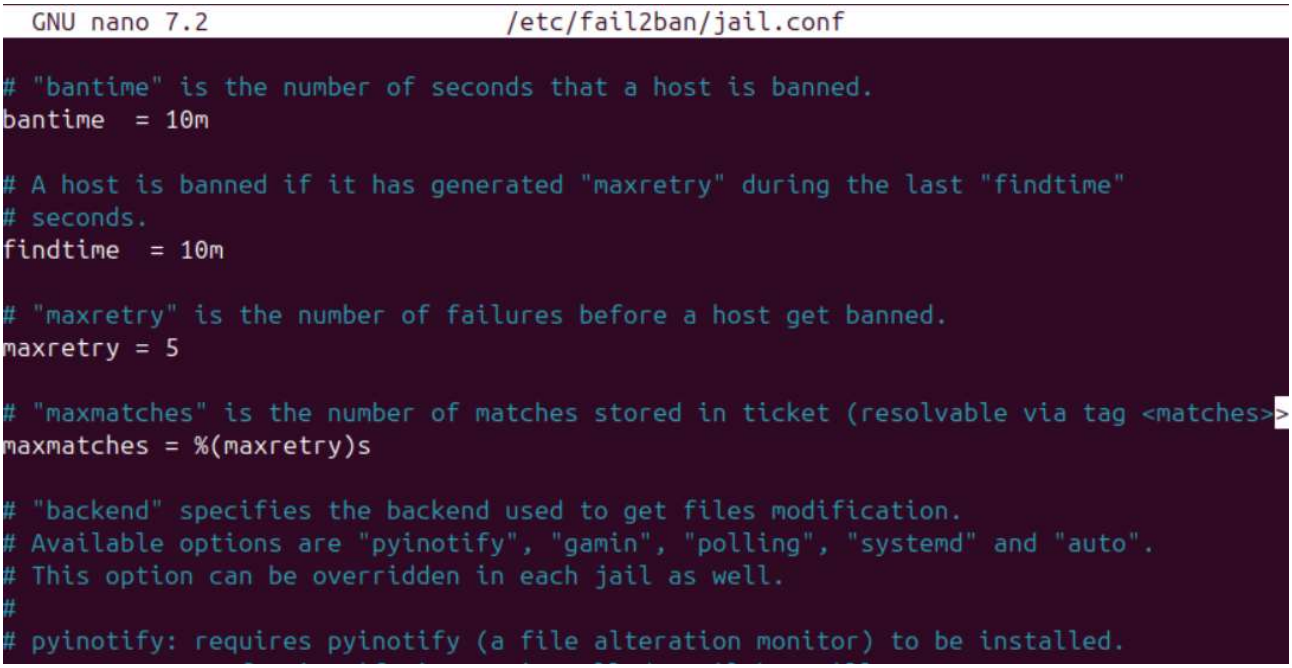
sudo systemctl status fail2ban
sudo ststemctl enable fail2ban (si nécessaire)
sudo systemctl start fail2ban (si nécessaire)



Pour configurer le bannissement automatique, nous éditons le ficher jail.conf

sudo nano /etc/fail2ban/jail.conf

sur lequel nous pouvons effectuer, si nécessaire, les modifications sur la durée du bannissement et le nombre d'essais possibles.



5) Tests de fin

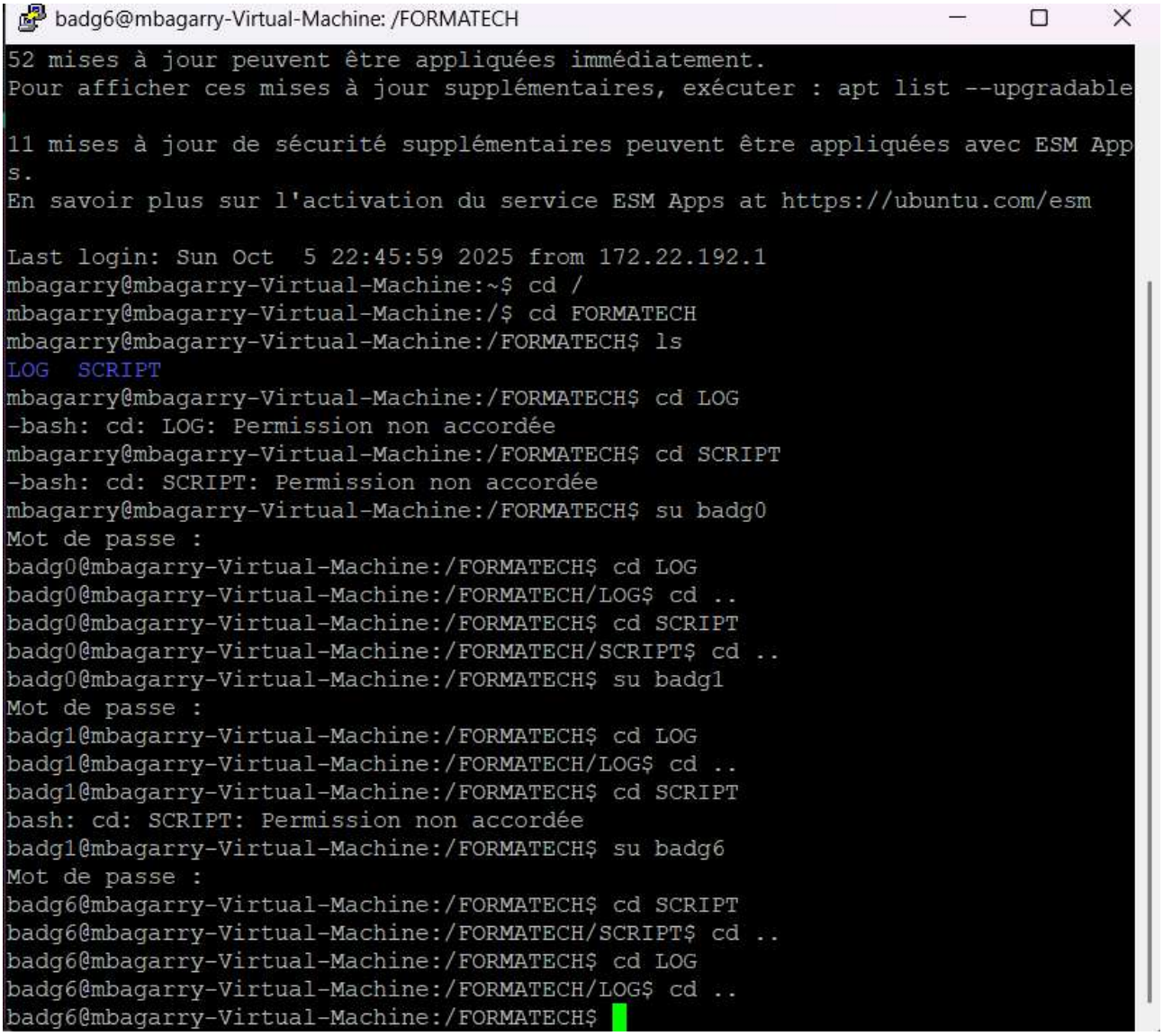
Pour effectuer les premiers test, nous utilisons le logiciel PUTTY pour se connecter à distance au serveur. Nous utilisons la commande

ip a

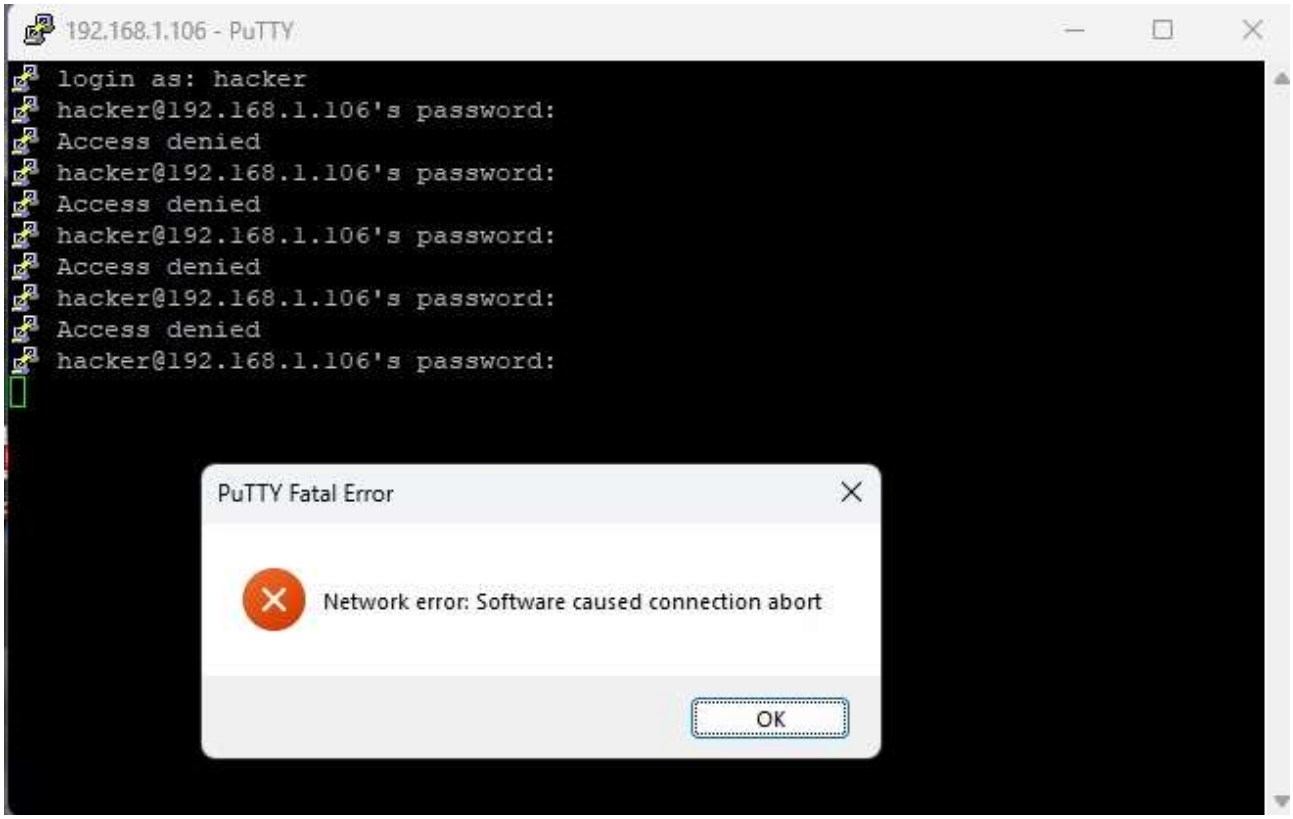
afin de trouver l'adresse Ip correspondant.

Une fois connecté nous effectuons différents test sur les différents utilisateurs et groupes afin de vérifier que les droits sont bien actifs et correctement ajustés.

Ci-dessous une copie exhaustive où nous voyons que le compte BADGE Maître (Badg0) a bien les droits sur les deux dossiers, que le membre du groupe Tech n'a pas accès au dossier SCRIPT mais que le membre du groupe Info a bien accès aux deux dossiers.

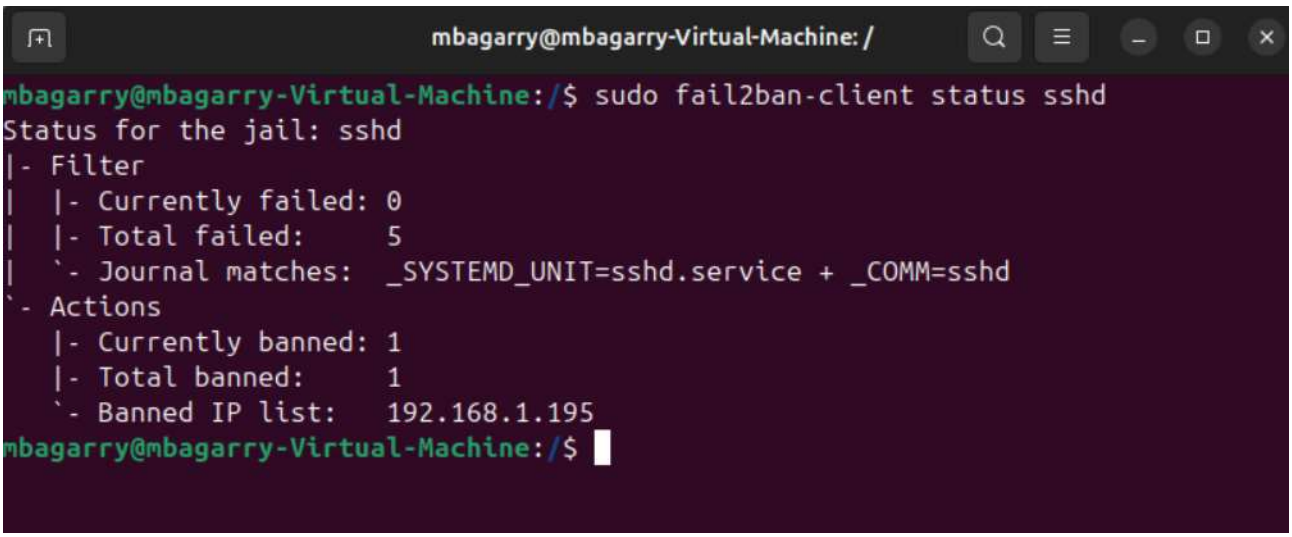


Nous allons maintenant vérifier si le service Fail2ban est actif en se connectant au serveur via un autre PC et en effectuant le nombre d'erreurs de mots de passe nécessaires au bannissement.



L'utilisateur Hacker a tenté de se connecter en utilisant 5 mots de passe et a bien été banni du serveur.

Nous le vérifions en consultant le fichier Jail du service Fail2ban



L'adresse IP 192.168.1.195 du compte Hacker est bien dans la liste de bannissement.

6) Problèmes rencontrés / solutions apporté / Bibliographie

J’ai utilisé principalement l’aide de Chat GPT pour certaine commande, notamment celle qui m’a permit de mettre deux groupes propriétaires d’un dossier, ou pour configurer le ssh et les permissions du Root.