## Télécom 3000

Camuset Marine
Berrod Morgane
Poux-Berthe Maxime
Notton Dit Coiron Quentin

**Préparation** :

**Matrice de flux :**

| ID | Source IP | Source Port | Destination IP | Destination Port | Protocole | Description | Action |
|---|---|---|---|---|---|---|---|
| **1** | Any | Any | serveur eth0 | 80,443 | TCP | HTTP | Autoriser |
| **2** | réseau d'admin | Any | serveur eth1 | 22 | TCP | SSH | Autoriser |
| **3** | Any | Any | Any | Any | Any | Any | Bloquer |

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

**Expliquer brièvement le choix du service web.**

apache server web car open source

**Expliquer brièvement le choix de la technologie pour la gestion du firewall de l'hôte.**

ufw car "uncomplicated firewall" et on galère déjà pas mal

**Installation** :

```
sudo apt update
```

```
sudo apt install apache2
```

**Configuration d'Apache pour afficher le site :**

```
cd /etc/apache2/sites-available/
```

```
sudo cp 000-default.conf site.conf
```

`sudo nano site.conf` : modifier le répertoire pour /home/kyan/website

```
<VirtualHost *80>
        ServerAdmin webmaster@localhost
        DocumentRoot /home/kyan/website/
        ServerName 192.168.1.25
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        <Directory /home/kyan/website>
                Require all granted
        </Directory>
</VirtualHost>
```

```
sudo a2ensite gci.conf
service apache2 reload
```

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw enable
```

**Configuration** :

Lister les sécurisations mises en place pour la partie web.

- Dans /etc/apache2/apache2.conf
  - TraceEnable off (évite le traçage intersite)
  - ServerSignature Off (pour ne pas révéler le type de serveur web et la version)
  - ServerTokens Prod (pour ne pas révéler le système d'exploitation)
- SSL :
  - `sudo apt-get install openssl`
- `sudo nano /etc/apache2/ports.conf :`

```
Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>
<IfModule mod_ssl.c>
        Listen 443
</IfModule>
```

- Rediriger les requêtes http vers https (/etc/apache2/sites-available/sites.conf):

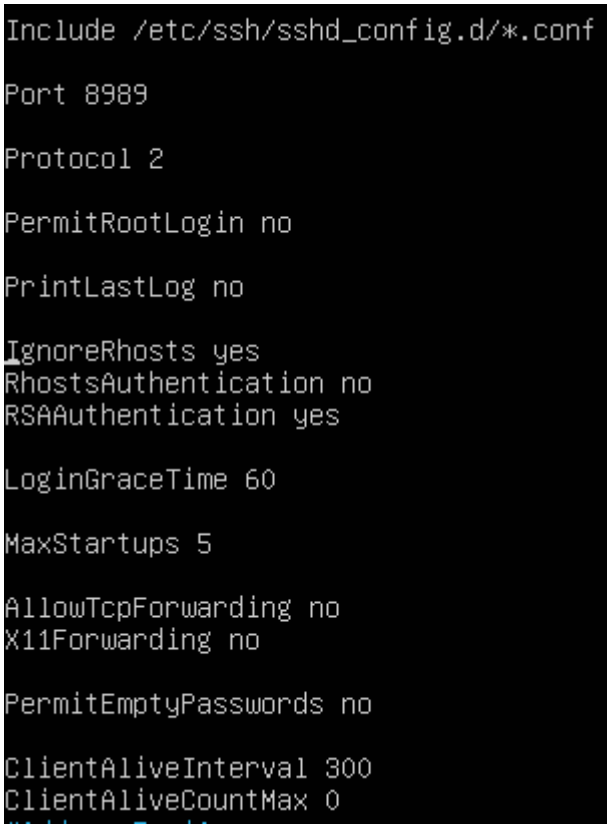
```
 RewriteEngine On
 RewriteCond %{HTTPS} off
 Rewrite (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

- sudo nano /etc/apache2/sites-available/default-ssl.conf :

```
ServerName 192.168.1.25

<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                DocumentRoot /home/kyan/website/
                ServerName 192.168.1.25

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                SSLEngine on

                SSLCertificateFile      /home/kyan/public-selfsigned.crt
                SSLCertificateKeyFile /home/kyan/private-selfsigned.key

                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>

                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>

                <Directory /home/kyan/website/>
                        AllowOverride None
                        Options Indexes FollowSymLinks MultiViews
                        Require all granted
                </Directory>
        </VirtualHost>
</IfModule>
```

- sudo a2enmod ssl
- sudo a2ensite default-ssl
- systemctl restart apache2

Lister les sécurisations mises en place pour la partie SSH.




- Changer le port par défaut
- Utiliser SSH 2
- Désactiver la connexion en root
- Cacher le dernier login
- Restreindre les connexions depuis seulement la machine Administration
- Désactiver Rhosts
- Fermer la connexion après 60 secondes
- Mettre en place un maximum de connexions à 5
- Désactiver le forwarding
- Désactiver les mots de passe vides

Expliquer avec quel moyen vous avez implémenter la politique de mot de passe, et le fichier de configuration.

```
sudo apt-get install libpam-pwquality
```

```
sudo nano /etc/pam.d/common-password
```

→ password requisite pam_pwquality.so retry=3 ucredit=-1 dcredit=-1 ocredit=-1

```
sudo nano /etc/login.defs
```

→ PASS_MAX_DAYS 100

PASS_MIN_DAYS 0

PASS_WARN_AGE 7

Fournir le fichier de configuration des règles du firewall.

`ip addr` (voir les noms de nos interfaces ):

1 : lo

2 : enp0s3

```
sudo ufw allow in on lo to any port 80
```

```
sudo ufw allow in on lo to any port 443
```

```
sudo ufw allow in on enp0s3 to any port 8989
```

```
To                         Action      From
--                         ------      ----
80 on lo                   ALLOW       Anywhere
443 on lo                  ALLOW       Anywhere
22 on enp0s3               ALLOW       Anywhere
8989 on enp0s3             ALLOW       Anywhere
22                         DENY        Anywhere
80 (v6) on lo              ALLOW       Anywhere (v6)
443 (v6) on lo             ALLOW       Anywhere (v6)
22 (v6) on enp0s3          ALLOW       Anywhere (v6)
8989 (v6) on enp0s3        ALLOW       Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)
```

Si des services sont désactivés, les lister et expliquer pourquoi ils l'ont été.

Fournir le fichier de configuration permettant d'activer les mises à jour automatiques.

```
sudo apt install unattended-upgrades
```

**Vérifications** :

Fournir le SSLScan.

Fournir la sortie de la commande NMAP réalisée sur l’interface métier.

Sources :
https://ubuntu.com/tutorials/install-and-configure-apache
https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-18-04
https://geekflare.com/fr/10-best-practices-to-secure-and-harden-your-apache-web-server/