BTS SIO2
bloc 3

B3-Act1-TP1 – Mise en place d'un serveur web sécurisé (6h)

Vous êtes membre de l'équipe Systèmes & Réseaux de l'entreprise « SODECAF » de Montauban. Votre responsable vous demande d'installer un nouveau serveur web Apache2, permettant d'héberger le site web de l'entreprise. Ce serveur web sera sécurisé afin d'en assurer une protection contre des actes malveillants.

Apache est un serveur web : tout comme IIS (prononcé 2 i s de chez Microsoft) et Nginx (prononcé [ˌɛndʒɪnˈɛks], libre), il permet de servir des pages web aux internautes. La figure ci-contre montre l'évolution des serveurs web les plus utilisés dans le monde.

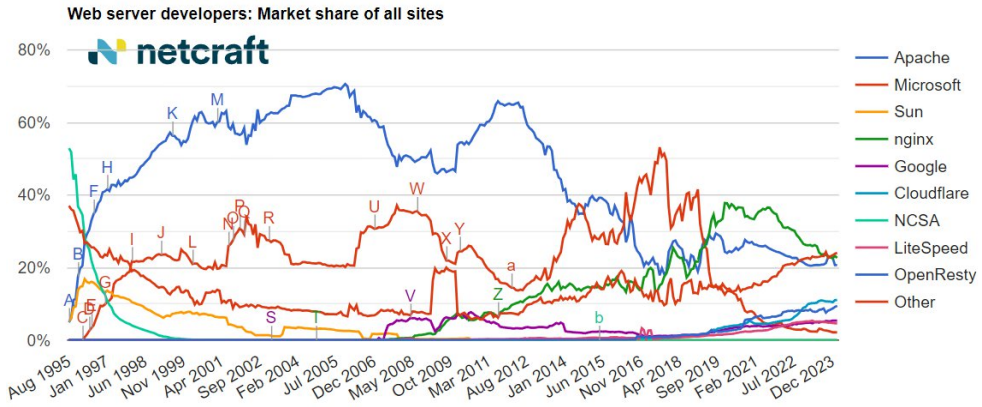
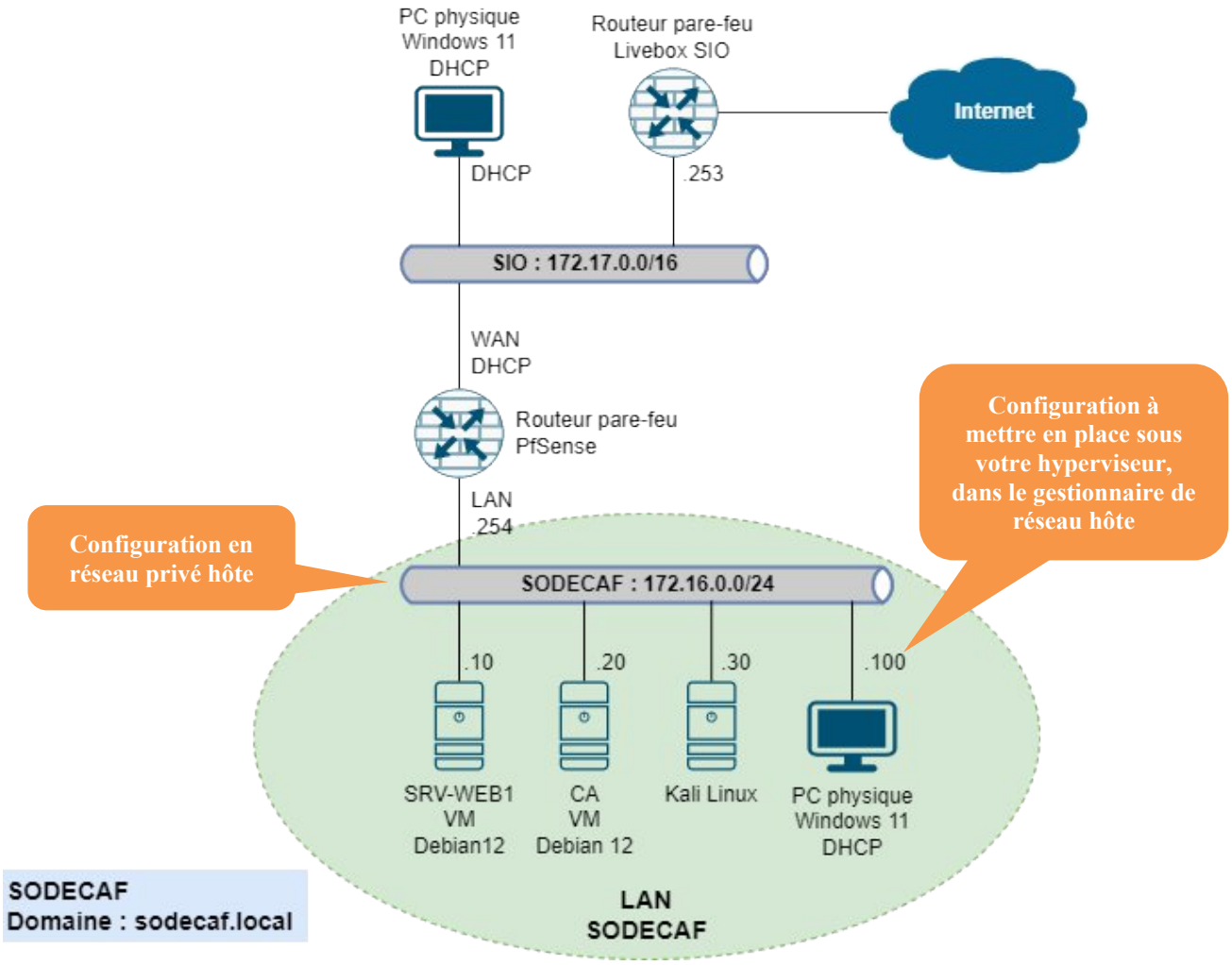


Schéma de l'infrastructure



Documents ressources sur le réseau

- fichier OVA *pfSense2-7*
- fichier OVA *debian12*
- fichier *kali-linux-2022.1-virtualbox-amd64.ova*
- document d'installation *Annexe 1 - Comment installer le serveur Web Apache sur Debian 10.pdf*
- vidéo *Le chiffrement SSL TLS expliqué en emojis.mp4*
- document d'installation *Annexe 2 - mise en place de l'HTTPS*

Travail à réaliser

- Pour commencer, vous devez installer une machine virtuelle PFSENSE 2.7 en important le fichier OVA (à télécharger sur le réseau). Configurez les connexions des interfaces sous WMware Workstation. Démarrez la VM et configurez l'IP de l'interface côté LAN (172.16.0.254).
- Configurez le réseau privé hôte sur WMware Workstation (menu Fichier > Gestionnaire de réseau hôte). Votre PC physique aura ainsi accès au réseau privé de la SODECAF.
- A partir du PC physique, accédez à l'interface web de PFSENSE et configurez les règles de filtrage de base, afin d'autoriser sur l'interface LAN les pings, et le trafic web.
- Ensuite, vous devez créer une machine virtuelle SRV-WEB1 à partir du fichier ISO debian 12 (à télécharger sur le réseau).
- Clonez cette machine et renommez cette machine CA (comme Certification Authority).
- Configurez les adresses IP des deux VM (voir le schéma). Renommez également ces machines sous Linux. Mettez à jour les paquets puis l'OS installé.
- Ajoutez des paquets utiles, comme vim et openssh-server sur les deux VM.
- En utilisant le document *Annexe 1 - Comment installer le serveur Web Apache sur Debian.pdf*, procédez à l'installation, à la configuration et aux tests du serveur web sur la machine SRV-WEB1. Les fichiers du site de la SODECAF sont sur le Drive dans l'archive sodecaf.tar.

Votre serveur web est installé et opérationnel. Toutefois, cette installation minimale n'est pas assez sécurisée et expose ce serveur à des attaques de personnes malveillantes. Votre DSI vous demande de mettre en place un premier niveau de sécurité sur ce serveur.

Dans un premier temps, vous allez utiliser une VM Kali Linux et ses nombreux outils afin d'observer des failles de sécurité dans votre installation.

- Importez la machine virtuelle Kali Linux (fichier *kali-linux-2022.1-WMware Workstation-amd64.ova*). Paramétrez son adresse IP. Le login de cette VM est *kali* avec pour mot de passe *kali*. Pour obtenir un clavier an Français, vous modifierez le fichier */etc/default/keyboard* en remplaçant *us* par *fr*.
- Dans la console de la Kali, utilisez la commande whatweb pour obtenir des informations sur votre site web.

```
kali@kali:~$ whatweb 172.16.0.10
http://172.16.0.10 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTML5, H
TTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[172.16.0.10], JQuery, M
ark-of-the-Web[https://www.sodecaf.com/], MetaGenerator[WordPress 4.9.3], S
cript[text/javascript], Title[SODECAF - Entreprise de Construction et de ré
novation tous corps d'état], WordPress[4.9.3], X-UA-Compatible[IE=10]
```

Votre serveur web est beaucoup trop bavard ! Il renvoie trop d'informations précises sur le système d'exploitation installé sur le serveur et la version du service Apache utilisée. Ceci est une aide précieuse pour l'attaquant, qui n'aura qu'a rechercher les failles de sécurité sur ces versions installées.

- En utilisant la première partie du document *Annexe 2 – Sécuriser son serveur web Apache*, effectuez les modifications dans la configuration de votre serveur afin de limiter ces informations.

Une des attaques classiques sur un serveur web est l'attaque DOS (Denial Of Service ou Déni de Service). Cette attaque a pour but de rendre indisponible le serveur web en l'inondant de requêtes TCP SYNC répétées.

- Utilisez l'outil hping3 de la Kali pour envoyer des requêtes multiples sur votre serveur web. Observez l'allongement du temps de réponse du serveur (commande ping dans une autre fenêtre à partir de la kali).

L'attaque ici n'est pas suffisante pour faire tomber le service, il serait nécessaire de mettre en place une attaque de type DDOS (Distributed Denial Of Service) avec plusieurs attaquants, mais nous avons tout de même observé l'impact sur le temps de réponse de notre serveur web.

```
kali@kali:~$ sudo hping3 --flood -d 120 --rand-source -S -p 80 172.16.0.10
HPING 172.16.0.10 (eth0 172.16.0.10): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

- En utilisant la suite de l'*Annexe 2 – Sécuriser son serveur web Apache*, effectuez les modifications afin de limiter l'impact d'une attaque DOS.

Il est également possible de faire une attaque DOS en sollicitant à de multiples reprises le service web su serveur. Nous allons utiliser pour cela la commande **slowhttptest** dans la Kali.

- Sur la Kali, installez le paquet slowhttptest, qui installe un outil permettant d'effectuer des attaques de type DOS. La commande ci-dessous permet de « bombarder » de requêtes notre serveur web. Effectuez le test et vérifiez l'impact sur le site web.

```
$slowhttptest -c 10000 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://172.16.0.10 -x 24 -p 80
```

Cet exemple ouvre 10000 connexions simultanées et envoie toutes les 10ms et 200 requêtes/s, en mode Slowloris (requêtes HTTP incomplètes) de type GET, vers notre serveur web.

Pour contrer les attaques de type DOS ou DDOS sur un serveur, il est préférable d'utiliser un outil de type **IPS (Intrusion Prevention System)**, comme **fail2ban**. Cet outil va détecter les requêtes répétées de mêmes machines, dans les fichiers logs, et bannir ces requêtes.

- Visualisez le fichier de log Apache2 avec la commande *tail -n 20 /var/log/apache2/access.log*. Retrouvez les nombreuses requêtes reçues de la part de la Kali Linux.
- Installez le logiciel fail2ban (nom du paquet : fail2ban). Si le service Fail2ban ne démarre pas sous debian12, modifiez le fichier /etc/fail2ban/jail.conf comme suit :

```
[sshd]
enabled = true
port    = ssh
logpath = %(sshd_log)s
backend = systemd
```

- Redémarrez le service fail2ban et vérifiez qu'il est bien actif.

Nous allons **utiliser fail2ban pour protéger le service apache2 contre des attaques DOS**. Suivez les étapes ci-dessous ou utilisez le site https://pipo.blog/articles/20210915-fail2ban-apache-dos.

- Sur le serveur web, ouvrez le fichier /etc/apache2/apache2.conf pour modifier les règles d'écriture des logs Apache. Commentez la ligne ci-dessous et remplacez-la par celle donnée. redémarrez le service Apache2.

```
#LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t %I %O \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %V %p" combined
```

On indique à fail2ban le fichier log à analyser ainsi que les ports concernés. Créez le fichier /etc/fail2ban/jail.d/apache-get-dos.conf et copiez son contenu :

```
[apache-get-dos]
enabled  = true
port     = http,https
filter   = apache-get-dos
logpath  = /var/log/apache2/access.log
datepattern = %%d/%%b/%%Y:%%H:%%M:%%S %%z
```

```
maxretry = 300
findtime = 5m
bantime  = 1h
```

- On définit les règles par défaut de bannissement : créez le fichier /etc/fail2ban/jail.d/custom.conf et copiez son contenu :

```
[DEFAULT]
bantime  = 300
findtime = 300
banaction = iptables-allports
```

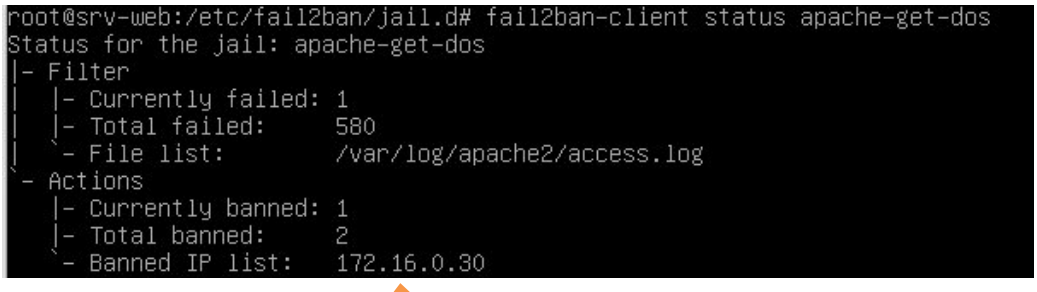
- Enfin, on définit des règles de filtrage des requêtes http arrivant sur le serveur web. Pour cela, créez le fichier /etc/fail2ban/filter.d/apache-get-dos.conf et copiez son contenu :

```
# Fail2Ban filter to scan Apache access.log for DoS attacks

[INCLUDES]
before = common.conf

[Definition]
# Option:  failregex
# Notes.:  regex to match GET requests in the logfile resulting in one of the
#          following status codes: 401, 403, 404, 503.
#          The host must be matched by a group named "host". The tag "<HOST>"
#          can be used for standard IP/hostname matching and is only an alias for
#          (?:::f{4,6}:)?(?P<host>[\w\-.^_]+)
# Values:  TEXT
failregex = ^<HOST> .*"GET (?!\/robots\.txt).*" (200|301|302|400|401|403|404|408|503)\s

# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is ignored.
# Values:  TEXT
#
ignoreregex =
```

- Redémarrez alors le service fail2ban.
- Effectuez de nouveau le test d'attaque DOS avec la commande slowhttptest.

```
$slowhttptest -c 10000 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://172.16.0.10 -x 24 -p 24
```

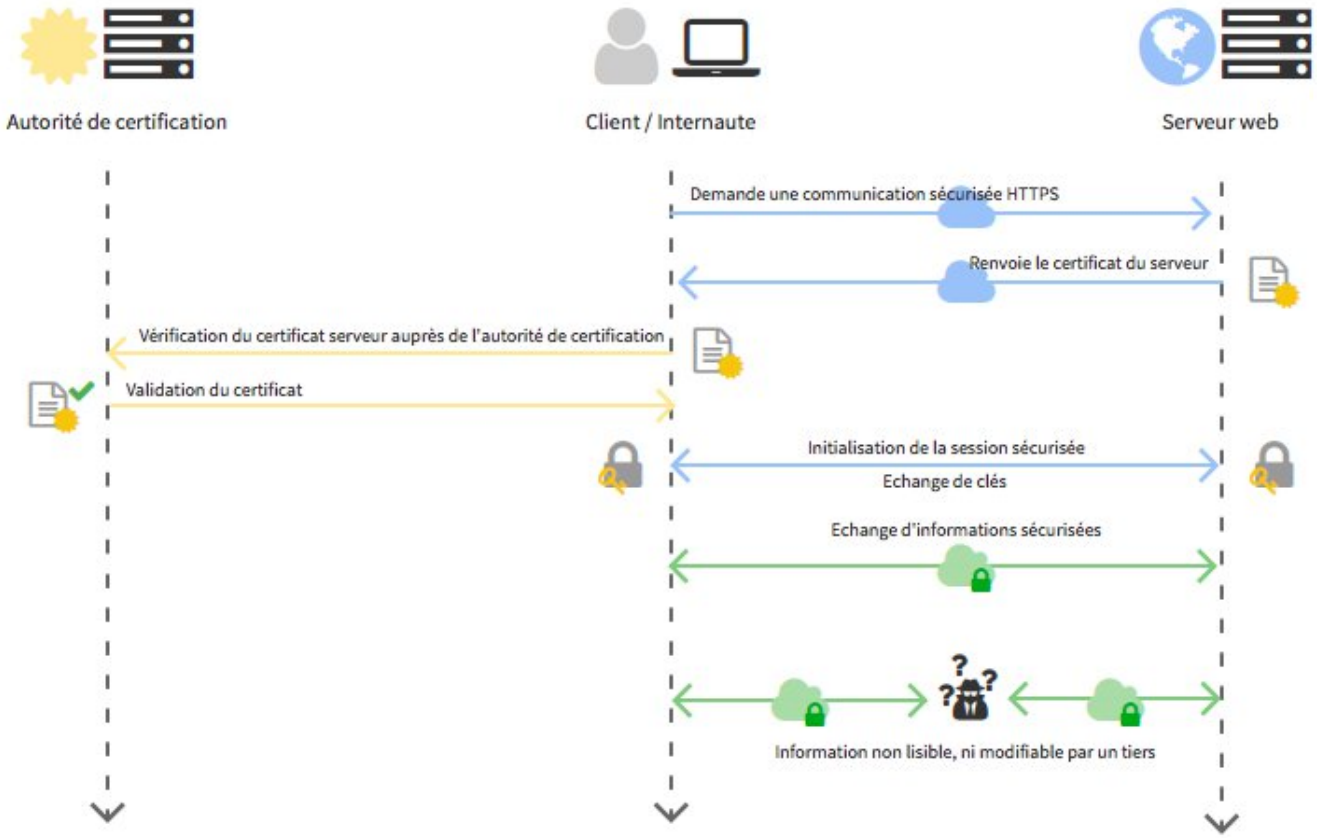
- Au bout de quelques secondes, tapez la commande *fail2ban-client status apache-get-dos* sur le serveur web.



L'adresse IP de l'attaquant est bannie

- Pour effectuer plusieurs tests, vous devez taper la commande *fail2ban-client unban 172.16.0.30*.

Votre site web est maintenant opérationnel, seulement, les informations circulent en clair entre le serveur web et les clients. Afin de **chiffrer ces échanges, il est nécessaire d'utiliser le protocole HTTPS à la place du protocole HTTP**.



- Visualisez la vidéo « *Le chiffrement SSL TLS expliqué en emojis.mp4* » afin de découvrir le principe de chiffrement utilisé en HTTPS. Vous pouvez également suivre la vidéo « Comprends le SSL HTTPS.mp4 ».

- En utilisant le document *Annexe 3 – mise en place de l'HTTPS.pdf*, procédez à la mise en place de l'HTTPS pour votre site web.