

Sécurité des serveurs et des systèmes**TP n°3 : Sécurisation des échanges d'un service Web Apache 2.0 sous Linux Debian****Durée : 1h30**

Moyens mis à disposition des étudiants	
Matériels : • 2 ordinateurs fixes ou portables • Switch cisco SG 300-10 • Câbles RJ45	Logiciels et systèmes d'exploitation : • VirtualBox 7.1.12 • Windows 10 ou 11 professionnel • Linux Debian 12.11 Bookworm • Wireshark 4.4.9 • Navigateur Internet (au choix)
Divers : Accès à Internet	

Savoir-faire mis en œuvre
❖ Installer et configurer des éléments d'infrastructure ❖ Déployer une solution d'infrastructure ❖ Administrer un système ❖ Tester l'intégration et l'acceptation d'une solution d'infrastructure ❖ Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure

Conditions de travail :

- Binôme (certains tests peuvent être réalisés avec un autre étudiant si votre poste de travail n'est pas suffisamment performant pour lancer 2 machines virtuelles simultanément).
- **Le compte-rendu de ce TP sera rédigé sous la forme d'une documentation technique (page de garde + sommaire + bibliographie et/ou sitographie)** présentant les étapes d'installation, de configuration, de paramétrage ainsi qu'une phase de recette (les tests) des services déployés via Linux Debian Bookworm.
- Les configurations matérielles requises pour les serveurs et les postes de travail sont présentées en annexes **document 1**.
- L'infrastructure que vous devez mettre en place est présentée en annexes **document 2**.

Contexte professionnel : Madame Bourgeois, Responsable de l'entreprise « Jardins de Saint-Eloi », souhaite sécuriser les transactions (échanges) réalisées entre son site web et les clients, internautes.

Madame Bourgeois a sollicité l'ESN (Entreprise de services numériques) C2I Caraïbes, implantée en Guadeloupe et en Martinique, afin de mener à bien ce projet.

Ce projet sera mené par un Développeur de C2I Caraïbes, spécialiste dans la création d'applications métiers basées sur les technologies web traditionnelles et 3.0.

Annexe I : Infrastructure réseau à réaliser.

MISSION : Vous êtes stagiaire chez C2I Caraïbes, le Responsable de la MOE fait appel à vous pour aider le Développeur dans la réalisation d'une solution technique afin de sécuriser à l'aide des protocoles SSL/TLS le site web hébergé.

Etape 0 : Installation de Wireshark

Wireshark est un logiciel gratuit qui permet de capturer et d'analyser les informations qui circulent sur le réseau entre plusieurs machines (serveurs et postes de travail).

- Téléchargez et installez **Wireshark 4.4.9** sur votre poste de travail (**poste0** ou **poste1**) ainsi que tous les outils proposés.
- Installez aussi les modules « **Npcap 1.79** » et « **USBcap 1.5.4.0** »

Etape n°1 : Réalisation de l'infrastructure réseau

- Réalisez l'infrastructure réseau présentée en annexe **document 2**, voir le support du **TP n°2 du bloc n°2**.
- Configurez les interfaces réseaux des VM à l'aide du plan d'adressage IP fourni en annexe **document 1**.
- Il sera nécessaire de passer en mode super-utilisateur pour avoir le droit d'accès et modifier le contenu des fichiers de configuration d'un système Unix/Linux :
 - Ainsi pour accéder au mode administrateur « **root** », il suffit de savoir la commande suivante : « **\$ su** » et de saisir le mot de passe du compte « **root** ».
 - La commande « **# exit** » permet de quitter le mode d'accès « **root** » ainsi que la session qui ne sera plus active.

Voici les fichiers et paramètres de configuration à prendre en compte pour le système Linux Debian Bookworm :

- Fichier de configuration : « **/etc/network/interfaces** »,
- Les paramètres : **auto enp0sX, iface enp0sX inet dhcp, iface enp0sX inet static, address, netmask, gateway**.
- Indiquez le rôle de chaque paramètre.

Observations : Avant les systèmes Linux, quelles que soient les distributions, proposaient un nommage des interfaces réseaux, identifiées de la façon suivante : ethX à savoir carte Ethernet et X le numéro de la carte **par exemple eth0**. Au lieu d'utiliser le schéma de nom d'interface réseau traditionnel ("eth0", "eth1", "wlan0", ...), le nouveau « **systemd** » de la distribution Debian utilise "des noms d'interface réseau prévisibles (Predictable Network Interface Names)" semblable à « **enp0s25** », « **ens31** », ...

Par défaut, certains outils logiciels qui permettent de configurer les interfaces réseaux de votre système Linux Debian, ne sont pas installés. Pour obtenir les informations sur les cartes ethernet de votre système, il suffit de saisir la commande « **ip a** ». Je vous invite à consulter le manuel de cette commande.

- Relancez le service réseau des VM Linux Debian pour prendre en compte les nouvelles configurations réseau : « **/etc/init.d/networking restart** ou **service networking restart** »
- Testez la connectivité entre les différentes VMs.
- Pensez à ajouter les enregistrements DNS nécessaires à la résolution de noms pour :
 - le serveur Linux ayant pour nom d'hôte « **srvlinux** »
 - ainsi que pour le site web, qui devra être accessible depuis ces noms d'hôtes « **www** » et « **www2** ».
- Ajoutez une capture d'écran et indiquez les enregistrements DNS créés. Justifiez !

Etape n°2 : Mise à jour des paquets du SE Linux Debian Bookworm

Observations : Deux orientations peuvent être envisagées pour installer un logiciel sur un système Linux :

- Soit à partir des fichiers sources compressés avec l'extension « **.tar.gz** », il suffit de télécharger ce dernier sur le site officiel de l'éditeur du logiciel.
- Soit depuis l'utilitaire « **apt** » qui gère les paquets logiciels disponibles sur votre système, il suffit d'indiquer des sites miroirs (serveurs distants présents sur Internet qui sont le dépôt des paquets (logiciels) à jour (dernière version) des différentes versions d'une distribution de Linux).

Nous utiliserons la seconde possibilité.

- A l'aide de la commande « **nano** », éditez et saisissez les lignes suivantes dans le fichier « **/etc/apt/sources.list** » pour indiquer les sites miroirs depuis lesquels vous allez télécharger et installez vos paquets ou autres mises à jour :

```
deb http://deb.debian.org/debian/ bookworm main contrib non-free
deb-src http://deb.debian.org/debian/ bookworm main contrib non-free
```

```
deb http://deb.debian.org/debian-security bookworm-security main contrib non-free
deb-src http://deb.debian.org/debian-security bookworm-security main contrib non-free
```

```
deb http://deb.debian.org/debian/ bookworm-updates main contrib non-free
deb-src http://deb.debian.org/debian/ bookworm-updates main contrib non-free
```

- Indiquez le rôle des lignes précédentes.
- Saisissez les commandes suivantes :
apt update
apt upgrade
- Indiquez les opérations effectuées par ces deux commandes.

Maintenant, vérifiez le nom de votre machine en « **srvlinux** » en procédant ainsi :

- A l'aide de la commande « **nano** », éditez le fichier suivant « **/etc/hostname** » et changez le nom spécifié en « **srvlinux** », si nécessaire et relancez votre serveur pour rendre effective la modification.

Etape n°3 : Capture et analyse d'une trame Ethernet avec Wireshark depuis un poste de travail

La capture d'une trame Ethernet sur Wireshark se fait en 3 étapes :

1. Choisir l'interface réseau depuis laquelle les trames sont échangées : « Ethernet »
2. Préciser le filtre d'affichage : à l'aide d'opérateurs logiques et de comparaisons.
3. Lancer et arrêter la capture avant de débiter l'analyse

Ci-dessous quelques exemples de filtre d'affichage utilisables sur WireShark :

Désignation	Filtre associé
Segments TCP uniquement	tcp
Paquets relatifs à TCP uniquement	ip.proto == 0x06
Adresse ip 192.168.0.1 ou 192.168.1.5	ip.addr == 192.168.0.1 ip.addr == 192.168.1.5
Trafic HTTP uniquement	http
Segment TCP sauf sur port 80	tcp && !(tcp.port == 80)
Adresse Ethernet 00:FF:12:34:AE:FF	eth.addr == 00:FF:12:34:AE:FF
Trafic 192.168.0.1 vers 197.168.10.5	ip.src == 192.168.0.1 && ip.dst == 197.168.10.5
Trafic UDP entre ports 40 et 67	udp && udp.port >= 40 && udp.port <=67

- Videz l'historique et la cache de votre navigateur Internet
- Lancez Wireshark et double-cliquez sur l'interface réseau « **Ethernet** », qui est connectée au serveur « **srvlinux** » en mode « **réseau interne** ».
- Appliquez le filtre d'affichage suivant : **(ip.src==adresseIP_client) && (ip.dst==adresseIP_serveur && tcp.port==80)**
- Lancez la capture de trames Ethernet.
- Depuis votre navigateur Internet, connectez-vous au site de la ville des Abymes.
- Une fois la connexion établie, revenez sur **Wireshark** et arrêtez la capture de trames.

- Dans le cadre « **vert** » du dessus, sélectionnez la dernière requête HTTP.
- Dans le cadre en bas à gauche, développez la section « **HyperText Transfer Protocol** », allez dans la rubrique « **Authorization** », que constatez-vous ?
- Enregistrez votre capture de trame pour les prochains tests.

Etape n°4 : Sécurisation du service web Apache2 à l'aide des protocoles SSL/TLS

- Installez le paquet « **openssl** » sur le serveur « **srvlinux** », à l'aide de la commande « **apt install** ».
- A l'aide de la commande « **mkdir** », créez un sous-répertoire nommé « **ssl** » dans le répertoire « **/etc/apache2** ».
- Déplacez-vous dans le répertoire « **/etc/apache2/ssl** »
- Depuis le répertoire précédemment cité, générez une clé privée et un certificat numérique (x509) auto-signé à l'aide de la commande suivante :
 - `#openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out srvlinux.crt -keyout srvlinux.key`
- Indiquez le rôle de chaque option et paramètres de la commande précédente.
- Précisez les informations suivantes lors de la création du certificat numérique :
 - PAYS : FR
 - Etat/province : Guadeloupe
 - Localité : Les Abymes
 - Organisation/entreprise : Jardins de StEloi
 - Section : Entreprise
 - Nom commun : www.jardinssteloi.fr
 - Email : m.bourgeois@jardinssteloi.fr
- A l'aide de la commande « **ls** », vérifiez la liste de fichiers du sous-répertoire « **/etc/apache2/ssl** »
- Maintenez, il faut configurer le service web Apache 2 pour la prise en compte de la clé privée et du certificat numérique x509. Editez le fichier « **jardinssteloi.conf** » et configurez-le avec les paramètres suivants :
 - **Port** : 443
 - **SSLEngine** : Activé
 - **SSLprotocol** : toutes les versions en plus de TLSv1.3
 - **SSLCertificateFile** : chemin d'accès au fichier contenant le certificat numérique
 - **SSLCertificateKeyFile** : chemin d'accès au fichier contenant la clé privée
- Activez le module **SSL** pour le service web Apache 2 à partir de la commande « **a2enmod** ».
- Relancez le service web Apache 2 à partir de la commande « **systemctl** ».
- Maintenant, désactivez et activez le site de la ville des Abymes depuis la commande « **a2dissite** » et « **a2ensite** ».
- Maintenant, relancez le service web Apache 2 depuis la commande « **systemctl** ».

Etape n°5 : Tests du dispositif de sécurisation de service web Apache 2

Afin de vérifier que les informations qui sont transmises sont bien sécurisées, vous devez capturer et analyser les trames Ethernet échangées entre le poste de travail (**poste0** ou **poste1**) et le serveur web « **srvlinux** », ci-dessous, la procédure à suivre pas à pas :

1. Indiquez la démarche que vous avez mise en œuvre pour effectuer vos tests, à l'aide de Wireshark.
 - Remarque : Vous devez préciser également le « **filtre d'affichage** » retenu.
2. Indiquez ce que vous avez constaté et expliquez ces résultats.
3. Affichez le certificat numérique et listez/relevez les informations qui s'y trouvent.
4. Concluez en justifiant la sécurisation ou non des données échangées.

Bon travail !!!