AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Mise en place d'un serveur web sécurisé

Identification du document	
Référence	Ue_Cybersécurité-Serveur_web.Docx
Date de création	14/09/2018
Rédaction (R)	BERTRAND Cédric
Version	V 0.1
Nombre de pages	8

Documents de référence

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T.+33 (0)1 58 45 32 50
esante.gouv.fr

Sommaire

1 Objet du document

Vous êtes chargés d'auditer et de sécuriser le serveur web de votre entreprise. L'entreprise utilise un CMS de type Joomla.

2 Contexte

2.1 Résultat attendu

Ce travail pratique est noté et doit être réalisé par équipe de 2.

Pour chaque question, **prendre des captures d'écran avant/après, copier/expliquer les commandes correspondantes et le résultat obtenu**. Pour le rendu final, faire un rapport et ajouter les fichiers de configuration suivants :

- Configuration du serveur Apache
- Configuration ssh
- Fichier des règles iptables
- Rapports Nessus
- Résultats d'audit (cmsmap, joomscan, nmapetc.)

L'objectif est de me montrer que vous avez compris les étapes réalisées.

Intégrer dans le rapport en introduction une capture d'écran de votre configuration ip.

Intégrer dans le rapport en introduction une capture d'écran de la configuration ip de la machine virtuelle

Si un document entre 2 équipes et trop « similaire », chaque équipe se verra attribué une pénalité de -5 points.

Si les captures d'écran semblent avoir été modifiées afin de correspondre au résultat souhaité, l'équipe se verra attribuée une pénalité de 5 points.

En cas de doute sur le résultat d'une question, une démonstration sera demandée en cours, en cas d'échec, l'équipe se verra attribuée une pénalité de 5 points.

Me remettre un rapport avec l'ensemble des documents demandés.

2.2 Outils et configuration

Pour réaliser le travail pratique, vous pouvez installer virtualbox et importer la machine virtuelle disponible pour ce tp.

Pour la machine cliente, il est suggéré d'utiliser une distribution Kali.

2.2.1 Serveur web

2.2.1.1 Configuration

OS : Debian 8

Serveur web : Apache2

SGBD : Mysql

CMS : Joomla 3.4.4

2.2.1.2 Répertoires

Apache : /etc/apache2

Joomla : /var/www/html/joomla

Mod-security : /etc/modsecurity

2.2.1.3 Identifiants

Eleve :eleve

Root :pentest

2.2.1.4 Urls

Phpmyadmin : http://<ip>/phpmyadmin

Joomla : http://<ip>/joomla

Interface admin Joomla : http://<ip>/joomla/administrator/

2.2.1.5 Wordlist

Simple_users2.txt : liste d'utilisateurs

weaksauce.txt : fichier de mots de passé

fuzz_common.txt : répertoires les plus communs

2.2.2 Outils à utiliser

Nessus : scanneur de vulnérabilités

Cmsmap : scanneur de cms

Joomscan : scanneur pour le cms Joomla

Nmap : scanneur de port

Burp : proxy

Wfuzz : fuzzer

Utilisation de metasploit : Par défaut, l'utilisation de metasploit est autorisée. Quand celle-ci n'est pas souhaitée, ceci est indiqué.

Utilisation de Crunch : Par défaut, l'utilisation de crunch n'est pas autorisée. Difficile de l'empêcher mais les captures d'écran tendront à montrer l'utilisation d'un tel outil.

3 Indications

Quand il s'agira de trouver un mot de passe, utiliser la liste fournie (fichier weaksauce.txt)

La forme du mot de passe est souvent indiquée, par exemple :

<mot_en_minuscules>[0-9](0-9](0-9] (exemple de mot de passe sous cette forme password784)

Les questions sont indépendantes les unes des autres, si vous ne parvenez pas à en faire une, vous pouvez passer à l'autre.

Par exemple, dans le tp, il faut à un moment cracker une authentification htaccess avec Burp pour récupérer une archive zip puis la cracker avec John. Si vous ne parvenez pas à cracker le mot de passe htaccess, rien ne vous empêche de récupérer l'archive zip avec le compte root (vous n'aurez juste pas tous les points ☺)

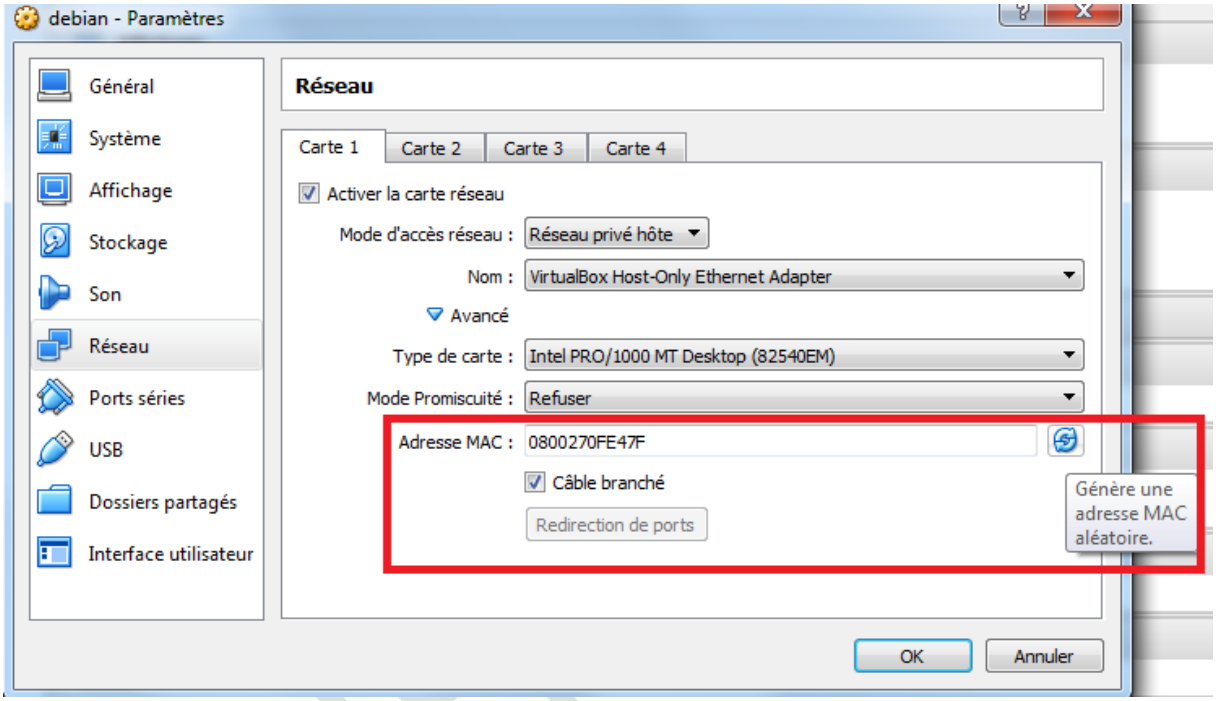
4 Mise en place du serveur web

4.1 Introduction

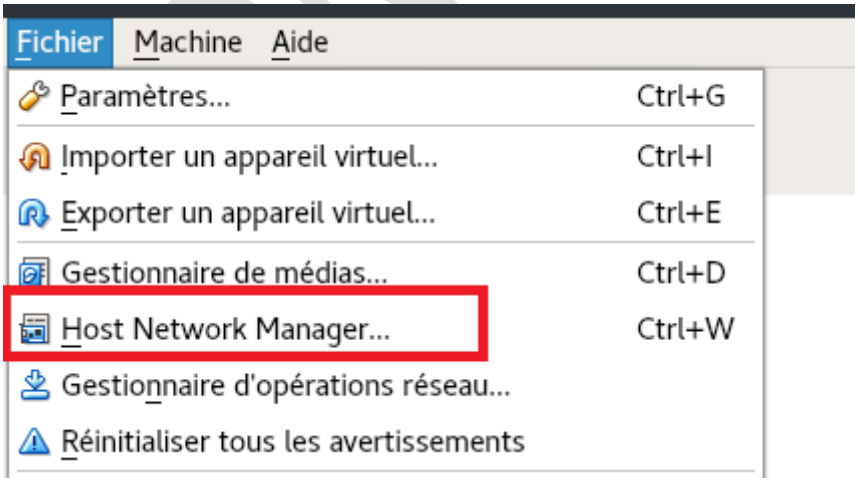
Faites une capture d'écran de votre configuration ip.

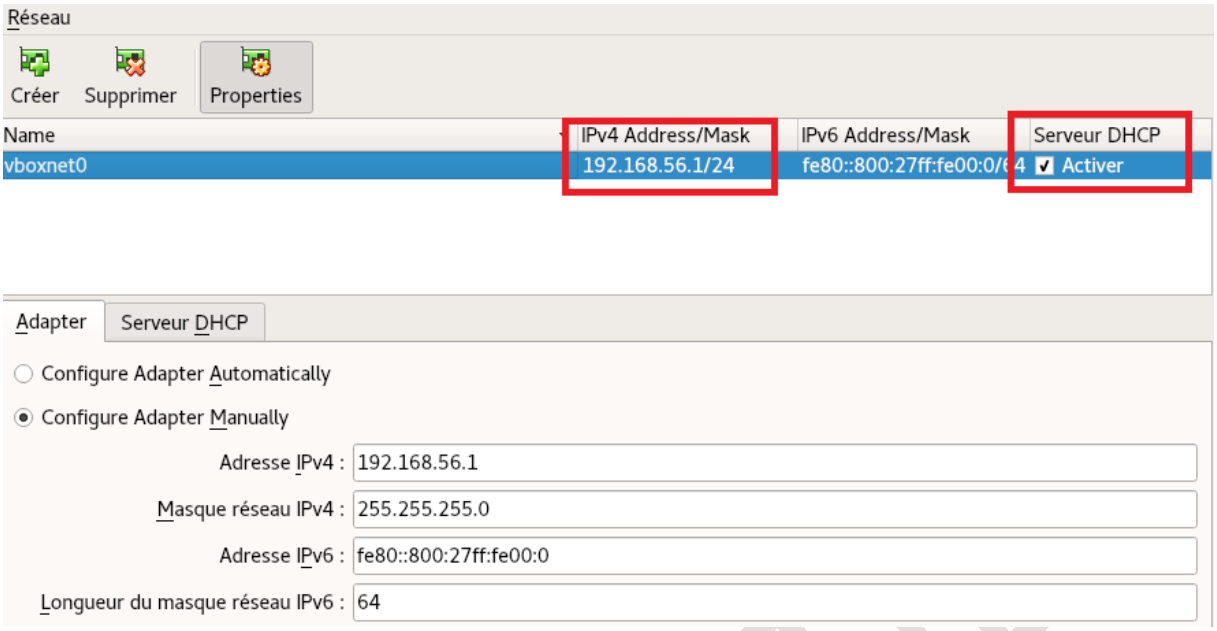
4.2 Configuration préalable

Importer la machine dans virtualbox. Penser à re-générer une adresse MAC



Penser à activer aussi le dhcp sous Virtualbox





Si toujours une erreur pour obtenir une adresse IP :

-> réinitialiser adresse mac
-> se connecter en root et supprimer la règle suivante :
rm -f /lib/udev/rules/80-networking.rules

Changer le nom de la machine dans /etc/hosts

Configurer le réseau afin de pouvoir accéder localement à la machine et de lui donner accès à Internet.

Tester l'accès ssh et l'accès à joomla (http://<ip>/joomla)