TP Cybersécurité de services informatiques

|  |  |  |
| --- | --- | --- |
| Nom / prénom : Sellier Garis | Date : | Note : / 20 |
| Nom / prénom : STEPIEN Nathan |
| Nom / prénom : PERSONAZ Nicolas |

Dans ce TP, nous allons installer le nécessaire pour faire fonctionner une application web. Pour cela, nous installerons un serveur Apache HTTPD, une base de données MariaDB (anciennement MySQL) et le langage de programmation PHP. Ces installations se feront sur une machine virtuelle utilisant le SE Rocky Linux (anciennement CentOS).

# 1. Installation d'un serveur

1 ) Créez une machine virtuelle en NAT avec 1 CPU, 512 Mo de RAM, 8Go de disque dur, 1 carte réseau et procédez à l'installation de Rocky Linux.

1. Créez une machine virtuelle en NAT avec 2 CPU, 1 024Mo de RAM, 8Go de disque dur, 1 carte réseau et procédez à l'installation de Kali Linux.
2. Pendant que les systèmes s'installent, précisez quelques points sur le protocole H TTP :
   * Comment accède-t-on à une ressource en HTTP ? Donnez un exemple

<http://www.example.com:80/path/to/myfile.html>

procoloe://hote:port/ressources#fragment = url

URI (Uniform Resource Identifier)

* + Donnez un exemple de requête envoyée par un client :

Referer:

https://www.adobe.com/fr/

Sec-Ch-Ua:

"Google Chrome";v="117", "Not;A=Brand";v="8", "Chromium";v="117"

Sec-Ch-Ua-Mobile:

?0

Sec-Ch-Ua-Platform:

"Windows"

User-Agent:

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36

* + Donnez un exemple de réponse retournée par le serveur :

Accept-Ranges:

bytes

Cache-Control:

max-age=21600

Content-Encoding:

gzip

Content-Length:

1554

Content-Security-Policy:

frame-ancestors \*.adobe.com http://adobe.lookbookhq.com https://adobe.lookbookhq.com http://adobeenterprise.lookbookhq.com https://adobeenterprise.lookbookhq.com

Content-Type:

application/javascript

Date:

Mon, 25 Sep 2023 10:31:15 GMT

Expires:

Mon, 25 Sep 2023 16:31:15 GMT

Server:

Apache

Server-Timing:

cdn-cache; desc=HIT, edge; dur=1, ak\_p; desc="1695637875678\_390329647\_102980785\_46\_9153\_6\_0\_219";dur=1

Strict-Transport-Security:

max-age=86400

Vary:

Accept-Encoding

X-Adobe-Cache:

MISS

X-Adobe-Loc:

ew1

X-Adobe-Source:

128.124

X-Content-Type-Options:

nosniff

* + Quels sont les 4 verbes les plus utilisés dans le protocole HTTP ? Précisez leur utilité

Les 4 verbs sont GET, POST, PUT, et DELETE :

GET Récupère des données depuis le serveur sans les modifier, principalement utilisé pour demander des ressources.

POST : Soumet des données au serveur en vue d'une modification ou d'un traitement, souvent utilisé pour créer ou mettre à jour des ressources.

PUT : Met à jour ou crée une ressource spécifiée par l'URI, remplaçant l'ancienne version par la nouvelle.

DELETE Demande au serveur de supprimer la ressource spécifiée par l'URI.

2. Sécurité périmétrique du SE et SSH

a) Nmap

1. Connectez-vous sur Kali et ouvrez un terminal pour taper la commande suivante :

$ sudo nmap ADRESSE IP ROCKY LINUX -O -SV -pi-65535

1. Indiquez ce que cette commande est censée faire :

Ça permet de scan le réseau pour voir les ports en écourte et ça version, l’os et et que sont les port ouvert

b) Changement de pare-feu

Votre serveur sous Rocky Linux est accessible à distance grâce au protocole SSH. Pour vous y connecter, vous pouvez utiliser WSL ou Putty sous Linux et un terminal sous Linux ou MacOS.

L'accès root est certainement désactivé, n'hésitez pas à faire un tour dans le fichier /etc/ssh/sshd\_config pour modifier la valeur de la directive PermitRootLogin.

Maintenant, nous allons désinstaller firewalld et remettre iptables. Pour cela, vous pouvez vous aider de ce tutoriel : https://www.tala-informatique.fr/wiki/index.php/lptables on systemd

1. Rappelez la commande qui permet de lister les règles iptables et expliquez brièvement la configuration de base :

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.7 (protocol 2.0)

9090/tcp closed zeus-admin

MAC Address: 00:0C:29:65:DA:9A (VMware)

1. Relancez le scan avec nmap depuis Kali et notez les différences avec firewalld :

On ne voit pas le 9090/tcp closed et il estite sur la version de l’os

## c) Détection de SE

1. La détection de SE permet à un attaquant de cibler les exploits qu'il va utiliser. En vous aidant du blog ci-dessous, expliquez seulement sans réaliser les modifications, comment vous pouvez limiter les informations récupérées par une telle technique .

<https://sharadchhetri.com/how-to-protect-from-port-scanning-and-smurf-attack-in-linux-server-by-iptables/>

On peut limiter les information récupéré via l’activation du par-feu iptable

1. Le site de nmap propose également des contre-mesures. Expliquez seulement sans réaliser les modifications s'il y a des conséquences négatives à leur implémentation.

### <https://nmap.org/misc/defeat-nmap-osdetect.html>

Cela peut arranger des beug et des diminution des performances.

1. OpenSSH affiche son numéro de version. Expliquez pourquoi les concepteurs d'OpenSSH sont obligés de le faire :

Car il pourrais avoir des pobléme de compatibiliter ou de chiffrement diférent

Car protocol comunication client et serveur

Expliquez en quoi consiste le port knocking et comment il permet d'éviter le problème cidessus :

Le **port-knocking** est une méthode permettant de modifier le comportement d'un firewall en temps réel pour provoquer l'ouverture d'un port suite au lancement préalable d'une suite de connexions sur des ports distincts dans le bon ordre, à l'instar d'un code frappé à une porte.

## d) Force brute

1. Expliquez brièvement le principe d'une attaque par force brute :

Tester a la siute une mutitube de mot de passe au hazard

1. Créez le compte bruteforce sur votre serveur Rocky avec comme mot de passe !QAZ2wsx (caractère spécial, minuscules ET majuscules !!)
2. Sur Kali, décompressez l'archive de mots de passe rockyou qui se trouve dans le répertoire

/usr/share/wordlists et expliquez comment vous utilisez hydra pour retrouver le mot de passe du compte :

On a décompréser un diconner avec une liste de mot de passe couramene utiliser et on test tout les mot de passe avec hydra :

hydra -l <nom\_utilisateur> -P /usr/share/wordlists/rockyou.txt ssh://<adresse\_IP>

Notre connexion SSH n'est clairement pas résistante aux attaques par force brute et pour cela il faudrait mettre en place fai12ban... nous verrons cela dans le cours sur les pare-feux :)

# 3. Hardening du serveur web

## a) Installation et accès réseau

1. Installez le serveur Apache httpd et précisez l'emplacement de son fichier de configuration ainsi que de son répertoire de travail :

/etc/apache2/

/var/www/html/

1. Indiquez comment vous configurez le pare-feu pour autoriser l'accès au service httpd depuis l'extérieur :

sudo Iptables -A INPUT -p tcp -drop 80 -j ACCEPT

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

##### httpd -k graceful

## b) Scan périmétrique

1. Sur Kali, expliquez comment vous utilisez nikto pour scanner le serveur web fraîchement installé sur Rocky :

nikto -h <adresse\_IP\_du\_serveur>

4/8

1. Expliquez brièvement les différentes failles découvertes et comment vous modifiez la configuration d'Apache pour les corriger. Pour plus de simplicité, concentrez vos modifications dans un fichier security.conf dont vous préciserez le contenu ci-dessous et mettez vos explications en commentaires :

Les failles découvert sont que on voit les port ouvert et closed et la verstion de l’os pour changer ca on a activer le iptable et enlever farwel2.

# Désactiver l'affichage des informations de version d'Apache

ServerSignature Off

ServerTokens Prod

# Fichier security.conf

# Configurations de sécurité pour Apache

<IfModule mod\_headers.c>

Header set X-XSS-Protection "1; mode=block"

</IfModule>

# Absence de l'en-tête X-Frame-Options

Header always append X-Frame-Options SAMEORIGIN

# Absence de l'en-tête X-Content-Type-Options

Header always set X-Content-Type-Options nosniff

# Version d'Apache obsolète

# Assurez-vous de mettre à jour Apache vers la dernière version

# et d'appliquer toutes les mises à jour de sécurité.

# Par exemple, utilisez la commande suivante sur une distribution basée sur Red Hat :

# sudo yum update httpd

# Désactivation de la méthode HTTP TRACE

TraceEnable off

# Désactivation de l'indexage de répertoire

# Cela empêche la liste des fichiers dans les répertoires si aucun index.html n'est présent.

<Directory /var/www/html>

Options -Indexes

</Directory>

# Restreindre l'accès au fichier README Apache par défaut

<Files "README">

Require all denied

</Files>

### c) Authentification BASIC et force brute

1. Dans un fichier de configuration, ajoutez une authentification BASIC sur une url de votre choix accessible uniquement par le compte bruteforce ayant le mot de passe jamesbond007

Vous pouvez vous aider du tutoriel suivant :

https://www.tala-informatique.fr/wiki/index.php/HTTPD#Le fichier\_.htaccess

1. Expliquez comment vous utilisez hydra pour retrouver le mot de passe du compte :

On utilise hydra avec une attaque au disconner avec dans la liste le mdp jamesbond007  
hydra -l brute-force -P /usr/share/wordlists/rockyou.txt ssh://<adresse\_IP>

L'authentification « Basic » n'est clairement pas résistante aux attaques par force brute et pour cela il faudrait modifier fai12ban... nous verrons cela dans le cours sur les pare-feux c'est promis :)

### d) Installation de PHP

Installez PHP sur votre serveur Rocky et créez une page index.php dans le répertoire de travail d'Apache qui affiche bonjour le monde.

1. Sur Kali, lorsque vous relancez nikto, que constatez-vous ?  
   que on voit la version de php
2. Proposez un correctif au niveau PHP :

Vi /etc/php.ini  
Expose\_php = off

Dans le monde professionnel, les applications web sont très souvent proxyfiées pour éviter de répéter de la configuration ou tout simplement pour gérer la partie SSL. Dans ce contexte, votre correctif ne serait pas portable et devrait être répété sur tous les serveurs web utilisant PHP... oui, on verra ça dans le cours sur les pare-feux ;)

# 4. Hardening de MariaDB

## a) Installation et accès réseau

Sur votre serveur Rocky, installez le client et le serveur MariaDB puis démarrez le serveur.

1. Expliquez comment vous faites pour ouvrir le pare-feu :

sudo Iptables -A INPUT -p tcp -drop 3306 -j ACCEPT

1. Expliquez comment vous faites pour créer un utilisateur bruteforce avec le mot de passe assalamualaikum :

Dnf -y install mariadb maria-server

Systectl start mariadb

Systemctl enable mariadb

mysql -u root -ppassword ;

CREATE USER 'bruteforce' IDENTIFIED BY 'assalamualaikum';

FLUSH PRIVILEGES ;

Expliquez ce que font les requêtes suivantes :

* + show databases

utilisée pour afficher la liste de toutes les bases de données disponibles dans le système de gestion de base de données (SGBD) en cours d'utilisation. Cette commande est généralement utilisée pour récupérer des informations sur les bases de données disponibles pour l'utilisateur connecté.

* + use mysql ,

utilisée pour sélectionner (ou changer) la base de données actuellement active dans un système de gestion de base de données (SGBD) MySQL ou MariaDB. Lorsque vous exécutez cette commande, vous basculez votre session SQL vers la base de données spécifiée, ce qui signifie que toutes les requêtes ultérieures que vous exécutez seront effectuées dans le contexte de cette base de données.

* + select host, user, password from user ;

Cette requête retourne les colonnes "host", "user", et "password" pour chaque enregistrement dans la table user.

Conservez le hash du mot de passe pour pouvoir l'utiliser plus tard...

## b) Bruteforce

1. Expliquez comment vous faites avec Hydra pour « essayer » de retrouver le mot de passe MariaDB

hydra -l <nom\_utilisateur> -P /usr/share/wordlists/rockyou.txt mysql://<adresse\_IP> :3306

1. Que se passe-t-il ?

On ce fait blocker /ban ip

1. Expliquez comment vous utilisez John the Ripper pour retrouver le mot de passe en clair depuis le hash :

On créer un fichier lemotdepassetropfort.txt, dedans on ajoute : login:password (hashé) puis sur le terminal de commande on fait : john lemotdepassetropfort.txt --show

Pour bien faire, les concepteurs de MariaDB mettent un script à disposition des administrateurs système pour sécuriser leur base de données : mysql\_secure installation.

1. Détaillez ce que fait ce script :

Suppression de comptes inutiles

Modification du mot de passe de l'utilisateur root

Désactivation de la connexion root à distance

Suppression de la base de données de test

Rechargement des privilèges

L'accès à la base de données à distance n'est pas recommandé et nécessite d'utiliser soit un VPN, que l'on verra dans le cours « Admi. Poste clients Gestion Accès », soit d'utiliser un tunnel SSH, que l'on verra dans le cours sur les pares-feux :-)