Le 01/02/2022

HELHa
Haute École Louvain en Hainaut

Wilfart Emmanuel
Site Rue Frinoise 12
7500 Tournai

Réseaux applicatifs et sécurité : pratique

Laboratoire 1 : Installation d'un serveur DNS dans un environnement Linux (Debian) sécurisé

1. Descriptif du laboratoire :

1. Installer, dans un environnement virtuel, la distribution Debian. La seule interface réseau utilisée est une interface nattée vous permettant l'installation des différents paquets de votre système d'exploitation.
2. Configurer votre environnement virtuel en ajoutant une interface bridgée. Cette interface devra être configurée dans votre environnement Debian.
3. Installer le package Bind9
4. Installer le package Iptables et configurer la table filter via les chaines INPUT et OUTPUT de la façon suivante :

	Autoriser les connexions SSH provenant de votre propre système d'exploitation hôte ainsi que la station de travail de votre voisin. Les autres connexions doivent être bloquées.
	Autoriser les requêtes DNS sur votre serveur provenant de n'importe quel hôte.
	Autoriser les paquets ICMP provenant de tout hôte externe mais bloquer les réponses ECHO-REPLY provenant de votre serveur.
	Autoriser votre serveur à envoyer des requêtes DNS vers tout hôte externe.
	Autoriser votre serveur à envoyer des requêtes HTTP et HTTPS vers tout hôte externe.
	Autoriser votre serveur à envoyer des requêtes ICMP vers tout hôte externe.

   Aucun package « Stateful » ne sera installé et vous devez donc, pour chaque requête envoyée ou reçue de votre serveur, accepter les réponses correspondantes.

5. Configurer votre serveur Debian de sorte que les règles ajoutées à vos tables deviennent persistantes.

6. Ajouter une nouvelle zone dans votre serveur DNS sur laquelle votre serveur a autorité. La zone doit avoir le nom suivant : VotreNom.local (Vous remplacez « VotreNom » par votre nom de famille). Ajouter les records obligatoires dans votre fichier de zone en choisissant les valeurs recommandées pour chacun des paramètres.
7. Ajouter un record MX et un record d'adresse pour l'hôte www. Tout record d'adresse ajouté dans votre fichier de zone doit pointer vers votre propre adresse IP de votre serveur.
8. Ajouter une zone esclave sur votre serveur DNS de sorte d'héberger une copie de zone pour le serveur d'un de vos voisins de laboratoire et inversement.
9. Configurer votre serveur de sorte que seul votre voisin qui est « esclave » de votre zone soit autorisé à demander des transferts de zone.
10. Configurer votre serveur de sorte d'autoriser les requêtes itératives de tout hôte externe et de n'autoriser les requêtes récursives que provenant de votre voisin de laboratoire via son adresse IP.
11. Optionnellement : installer et configurer le package Fail2Ban de sorte de protéger votre serveur SSH contre les tentatives de connexion de type « attaque brute de force »

2. Evaluation du laboratoire :

1	Installation de la distribution Debian dans un environnement virtuel.	
2	Configuration d'une nouvelle interface virtuelle bridgée	
3	Installation du package Bind9	
4	Installation du package Iptables	
5	Configuration de la table filter pour répondre aux besoins suivants	
	Autoriser les connexions SSH provenant de votre propre système d'exploitation hôte ainsi que la station de travail de votre voisin. Les autres connexions doivent être bloquées.	
	Autoriser les requêtes DNS sur votre serveur provenant de n'importe quel hôte.	
	Autoriser les paquets ICMP provenant de tout hôte externe mais bloquer les réponses ECHO-REPLY provenant de votre serveur.	
	Autoriser votre serveur à envoyer des requêtes DNS vers tout hôte externe.	
	Autoriser votre serveur à envoyer des requêtes HTTP et HTTPS vers tout hôte externe.	
	Autoriser votre serveur à envoyer des requêtes ICMP vers tout hôte externe.	
6	Configuration de votre serveur Debian de sorte que les règles ajoutées à vos tables deviennent persistantes (survivre à un reboot).	
7	Ajout de votre nouvelle zone comprenant votre nom dans votre serveur DNS	
8	Ajout des records obligatoires dans votre fichier de zone et paramétrage en respectant les valeurs recommandées.	
9	Ajout d'un record MX et d'un record www. Ajout des records d'adresses correspondants.	

10	Ajout d'une zone esclave pour la zone de votre voisin de table de laboratoire et inversement.	
11	Sécurisation de votre serveur de sorte que seul le serveur de votre voisin de table soit autorisé à effectuer des demandes de transfert de zone.	
12	Configuration de votre serveur de sorte que les requêtes itératives de tout hôte extérieur soient acceptées mais n'accepter que les requêtes récursives provenant de votre voisin de table de laboratoire via son adresse IP	
13	Installation et configuration de Fail2Ban (Optionnellement)	