RAPPORT DE PROJET:

Sécurisation d'un réseau universitaire par la mise en place de services réseau et d'un pare-feu

Licence 1 Informatique Réseaux et Télécommunications

Réalisé par :
DOUMBIA Awa Salif

1. Introduction

Dans le cadre de ce projet académique, l'objectif était de mettre en place et de sécuriser les principaux services réseau d'un environnement universitaire.
Le projet repose sur l'installation, la configuration et la sécurisation des services suivants :

- Serveur **DNS**
- Serveur **Web (Apache)**
- Serveur **FTP**
- Serveur **DHCP**
- Mise en place de bonnes pratiques de sécurité (isolation, restrictions, contrôle d'accès)

L'ensemble des services est déployé sur un serveur Linux (Ubuntu Server) au sein d'un réseau local universitaire simulé.

---

2. Présentation et rôle du DNS

2.1 Définition du DNS

Le **DNS (Domain Name System)** est un service fondamental d'Internet qui agit comme un traducteur entre les humains et les machines.

Lorsqu'un utilisateur saisit une adresse comme :
`www.mata.com`

Le DNS permet de :

- Traduire ce **nom de domaine** en **adresse IP**
- Identifier le serveur qui héberge le site
- Fournir cette adresse IP au navigateur web afin d'établir la connexion

Sans le DNS, l'utilisateur devrait mémoriser des adresses IP numériques, ce qui serait peu pratique.

2.2 Hiérarchie du DNS

Le DNS fonctionne selon une hiérarchie bien définie :

- **Racine (.)**
- **Top Level Domain (TLD)** : `.com`, `.org`, `.fr`
- **Domaine de second niveau** : `it-connect`
- **Sous-domaines** : `www`, `mail`, `ftp`

Exemple complet :
`www.it-connect.fr`

2.3 Ports et protocoles utilisés

- **Port 53**
- **UDP** (par défaut, plus rapide)
- **TCP** (utilisé notamment avec DNSSEC ou pour les réponses volumineuses)

Le protocole UDP est privilégié pour sa rapidité, tandis que TCP assure une meilleure fiabilité.

2.4 DNSSEC

Le **DNSSEC (Domain Name System Security Extensions)** est une extension de sécurité du DNS permettant de garantir :

- L'authenticité des réponses DNS
- L'intégrité des données
- La protection contre les attaques de type spoofing ou cache poisoning

---

3. Mise à jour du système

Avant toute installation, le système est mis à jour afin d'éviter les failles connues :

```
apt update
```

---

4. Installation et configuration du serveur Web Apache

4.1 Présentation d'Apache

Apache est l'un des serveurs web les plus utilisés au monde.
Il permet d'héberger et de servir des pages web aux clients via le protocole HTTP.

4.2 Installation

```
apt install apache2
```

4.3 Vérification du fonctionnement

Depuis un navigateur web, on accède à l'adresse IP du serveur :

```
http://192.168.248.150
```

L'affichage de la page par défaut d'Apache confirme que le serveur web est fonctionnel.

---

5. Installation et configuration du serveur DNS (Bind9)

5.1 Présentation de Bind9

Bind9 (Berkeley Internet Name Domain) est une implémentation open source du protocole DNS, largement utilisée sur les serveurs Linux.

5.2 Installation

```
apt install bind9 bind9utils bind9-doc -y
```

5.3 Configuration des zones DNS

5.3.1 Déclaration des zones

Fichier de configuration :

```
sudo nano /etc/bind/named.conf.local
```

Ajout des zones :

```
zone "ra" {
    type master;
    file "/etc/bind/db.ra";
};

zone "248.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

- **Zone directe** : résolution nom → IP
- **Zone inverse** : résolution IP → nom

5.3.2 Création du fichier de zone directe

```
cp /etc/bind/db.local /etc/bind/db.ra
nano /etc/bind/db.ra
```

Contenu principal :

```
$TTL    604800
@   IN  SOA serveur.ra. root.serveur.ra. (
        2
        604800
        86400
        2419200
        604800 )

@       IN  NS  serveur.ra.
@       IN  A   192.168.248.150
serveur.ra. IN A 192.168.248.150
```

TTL : durée de mise en cache des informations DNS (7 jours).

5.3.3 Configuration de la zone inverse

```
cp /etc/bind/db.127 /etc/bind/db.192
nano /etc/bind/db.192
```

Configuration :

```
150 IN PTR serveur.ra.
```

La résolution inverse permet de retrouver un nom de domaine à partir d'une adresse IP.

5.4 Vérification et redémarrage

```
named-checkzone ra /etc/bind/db.ra
named-checkzone 248.168.192.in-addr.arpa /etc/bind/db.192
named-checkconf
systemctl restart bind9
```

5.5 Modification du fichier hosts (client Windows)

Chemin :

```
C:\Windows\System32\drivers\etc\hosts
```

Ajout :

```
192.168.248.150 serveur.ra
```

Test dans le navigateur :

```
http://serveur.ra
```

---

6. Mise en place du serveur FTP

6.1 Présentation de FTP

Le **FTP (File Transfer Protocol)** permet le transfert de fichiers entre un client et un serveur distant.

- Port 21 : contrôle
- Port 20 : données

6.2 Installation de vsftpd

```
apt install vsftpd -y
```

6.3 Création d'un utilisateur FTP

```
adduser ftpuser
mkdir -p /home/ftpuser/ftp/upload
```

6.4 Sécurisation des permissions

```
chown nobody:nogroup /home/ftpuser/ftp
chmod a-w /home/ftpuser/ftp
chown ftpuser:ftpuser /home/ftpuser/ftp/upload
```

Ces restrictions empêchent les modifications non autorisées et isolent l'utilisateur.

6.5 Sauvegarde et configuration

```
cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
nano /etc/vsftpd.conf
```

Paramètres principaux :

```
listen=YES
listen_ipv6=NO
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
allow_writeable_chroot=YES
```

Redémarrage :

```
systemctl restart vsftpd
```

---

7. Mise en place du serveur DHCP

7.1 Présentation du DHCP

Le **DHCP (Dynamic Host Configuration Protocol)** permet d'attribuer automatiquement :

- Adresse IP
- Masque
- Passerelle
- DNS

Ports utilisés :

- Client : 68
- Serveur : 67

7.2 Installation

```
apt install isc-dhcp-server
```

7.3 Configuration de l'interface réseau

```
nano /etc/default/isc-dhcp-server

INTERFACESv4="ens33"
```

7.4 Configuration du serveur DHCP

```
nano /etc/dhcp/dhcpd.conf

subnet 192.168.248.0 netmask 255.255.255.0 {
    range 192.168.248.100 192.168.248.150;
```

```
    option domain-name-servers 192.168.248.150;
    option domain-name "ra";
    option routers 192.168.248.1;
    option broadcast-address 192.168.248.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

7.5 Vérification

```
systemctl restart isc-dhcp-server
systemctl status isc-dhcp-server
```

Sur un client :

```
apt install isc-dhcp-client
dhclient
ip a
```

---

8. Conclusion

Ce projet m'a permis de comprendre concrètement :

- Le fonctionnement des services réseau fondamentaux
- Leur interaction dans un environnement universitaire
- Les principes de base de la sécurisation des services
- L'importance des permissions, de l'isolation et des contrôles d'accès

Ce travail constitue une base solide pour des projets plus avancés en **administration système**, **réseaux** et **cybersécurité**.