|  |
| --- |
|  |
| **Politique de Sécurité** |
| **M1 : Master Cyber sécurité Et Cybercriminalité** |
|  |
|  |
|  |
|  |

Rapport Du Projet De Politique de Sécurité

|  |
| --- |
|  |

**Réalisé par :**

**Oumnia Ba Ahmed**

**Issam Najah**

**Walid Arjouan**

**Sommaire**

**SOMMAIRE……………………………………………………………….……………………………………..**

**LISTE DES FIGURES…………………………………………….………………………………………......**

**Introduction…………………………………………………………………………………………………**

**Chapitre 1 : Installation et Configuration d'infrastructure réseau…**

**1. Active Directory: Installation sur Windows Server 2008……………………………..**

**1.1Le rôle, les avantages et les contraintes de l’active Directory:………………**

1. **L’utilité d’active directory ………………………………………………**
2. **L’installation d’AD………………………………………………………..**
3. **Attribution des rôles aux utilisateurs……………………………………**

**2. Serveur DNS (Bind9) …………………………………………………………………….**

**2.1 Définition………………………………………………………………………..**

**2.2 Installation de serveur sous Linux……………………………………………..**

**2.3 Configuration de Serveur DNS Bind9 ………………………………………**

**a. Configuration de fichier named.conf.local ………………………………..**

**b. Configuration de fichier zone……………………………………………..**

**c. Création de fichier de zone inversée………………………………………..**

**d. Vérification la syntaxe de configuration de BIND ……………………….**

**e. Redémarrer BIND ………………………………………………………….**

**3. Serveur Mail(postfix)…………………………………………………………………….**

**3.1 Définition: ……………………………………………………………………..**

**3.2 avantages : …………………………………………………………………….**

**3.3 installation et Configuration du serveur : …………………………………….**

**a. installation des paquets ……………………………………………………**

**b. configuration ………………………………………………………………..**

**4. Serveur web (Wamp) …………………………………………………………………..**

**4.1 Base de données (MySQL) : …………………………………………………..**

**4.2 Les interfaces de l’application :………………………………………………**

**a. Page index :…………………………………………………………………**

**b. Page contact: ………………………………………………………………..**

**c. Page contrat:………………………………………………………………..**

**5. Serveur DHCP :………………………………………………………………………….**

**5.1. Définition :……………………………………………………………………**

**5.2. Installation :…………………………………………………………………….**

**5.2. Configuration :………………………………………………………………..**

**Chapitre2 : Identification des risques**

**2. Les risques de réseau : ................................................................................................... 24**

**1. Les risques physiques : .............................................................................................. 24**

**1.1. Les risques d’électricité : ........................................................................... 24**

**1.2. Sécurité de l’accès à la salle informatique : .................................................. 24**

**2.3. Panne au niveau des climatiseurs : ………………………………………………………………………….**

**3. Les risques d’exploitation : .......................................................................................... 24**

**3.1. Email Bombing : ………………………………..……………………............................. 24**

**3.2. SQL injection :................................................................................................................ 24**

**3.3. Attaque l’homme du milieu .............................................................................................. 25**

**3.4. Attaque tcp syn :……………………………………………………………………………………**

**3.5. Attaque par déni de service……………………………………………………………………….**

**3.4. Portes non sécurise........................................................................................................ 26**

**3.5. Elévation des privilèges .................................................................................................. 26**

**3.6. Code arbitraire .................................................................................................................. 26**

**3.7. Atteinte à la confidentialité donnée ................................................................................. 27**

**4. Les risques logiques : .................................................................................................................. 27**

**4.1. Ingénierie sociale :......................................................................................................... 27**

**5. Les risques liés au traitement des données : ..................................................................... 27**

**Chapitre 3 : Mise en place de la politique de sécurité............................. 27**

**1. Proposer une politique de sécurité adéquation : .................................................... 28**

**1.1. Sécurité des salles .................................................................................... 28**

**a. Installation des caméras et installer un system de refroidissement..... 28**

**b. L’accès aux salles des serveurs……………………………………………………**

**1.2. Duplication des serveurs ........................................................................... 28**

**a. DNS ........................................................................................... 28**

**b.DHCP……………………………………………………………………….**

**c. Contrôleur de domaines ........................................................ 28**

**d. Mail serveur : ....................................................................... 28**

**e. Creation d’un backup d’application web: ....................................................... 28**

**1.3. Sécurité de réseau............................................................................ 28**

**a. DMZ : (Zone démilitarisée) ..................................................... 28**

**b. Utilisation des routeurs asa (Firewall) : ...................................................... 29**

**c.IDS…………………………………………………………….…………**

**d. Duplication des routeurs :………………………………………………………**

**e. Réseau de CLOS : .................................................................... 29**

**1.4. Sécurité de données : ........................................................................... 29**

**a. LVM:.................................................................................. 29**

**2. Implémentation et test de politique de sécurité : ............................................ 29**

**2.1.Configuration de protocole HSRP……………………………………………………**

**2.2. DNS : ............................................................................. 30**

**2.3. Contrôleur de domaines : .......................................................... 30**

**2.4. Mail serveur : ..................................................................................................... 30**

**2.5. DHCP :…………………………………………………………………………….**

**2.6.DMZ :………………………………………………………………………………….**

**2.7.Renforcé la sécurité des routeurs :…………………………………………………………..**

**3. Architecture finale : ..................................................................................... 33**

**4. Les limites et les points à améliorer de votre proposition :................. 33**

**Conclusion ....................................................................................................... 34**

**LISTE DES FIGURES :**

[Figure 1:Nom de domaine: 6](#_Toc36420350)

[Figure 2:Installation des services des de domaine. 7](#_Toc36420351)

[Figure 3:Résumé serveur . 7](#_Toc36420352)

[Figure 4:les utilisateurs et ordinateurs Active Directory. 9](#_Toc36420353)

[Figure 5:Architecture finale. 9](#_Toc36420354)

[Figure 6:Installation de serveur. 10](#_Toc36420355)

[Figure 7:Configuration de fichier named.conf.local : 10](#_Toc36420356)

[Figure 8:Configuration de fichier zone. 11](#_Toc36420357)

[Figure 9:Configuration de fichier zone. 11](#_Toc36420358)

[Figure 10:Vérification du syntaxe et redémarrage. 12](#_Toc36420359)

[Figure 11:Installation des paquets . 12](#_Toc36420360)

[Figure 12:Installation des paquets common, imap, pop, et squirelmail. 13](#_Toc36420361)

[Figure 13:Configuration postfix. 13](#_Toc36420362)

[Figure 14:Configuration type de messagerie. 13](#_Toc36420363)

[Figure 15:Configuration type de messagerie. 13](#_Toc36420364)

[Figure 16:Configuration destinataire des courriels. 14](#_Toc36420365)

[Figure 17:Protocol internet. 14](#_Toc36420366)

[Figure 18:Configuration squirremail. 15](#_Toc36420367)

[Figure 19:fichier dovecot.conf: 15](#_Toc36420368)

[Figure 20:page login. 16](#_Toc36420369)

[Figure 21:page login: 17](#_Toc36420370)

[Figure 22:page contact. 17](#_Toc36420371)

[Figure 23:page contact. 18](#_Toc36420372)

[Figure 24:Installation DHCP. 19](#_Toc36420373)

[Figure 25:Configuration du fichier dhcpd.conf. 19](#_Toc36420374)

[Figure 26:Configuration du fichier dhcpd.conf (suite). 20](#_Toc36420375)

[Figure 27:Redémarrage du serveur. 20](#_Toc36420376)

[Figure 28:SQL injection. 21](#_Toc36420377)

[Figure 29:Exemple du code injecté. 21](#_Toc36420378)

[Figure 30:attaque l’homme du milieu. 21](#_Toc36420379)

[Figure 31:Attaque TCP SYN. 23](#_Toc36420380)

[Figure 32:Attaque par déni de service. 23](#_Toc36420381)

[**Figure 33:une zone démilitarisée.** 26](#_Toc36420382)

[**Figure 34:La gestion par volumes logiques.** 27](#_Toc36420383)

[Figure 35:La première interface. 28](#_Toc36420384)

[Figure 36:La deuxième interface. 28](#_Toc36420385)

[Figure 37:La première interface. 28](#_Toc36420386)

[Figure 38:La deuxième interface. 29](#_Toc36420387)

[Figure 39:configuration fichier named.conf.options. 29](#_Toc36420388)

[Figure 40:configuration du deuxième serveur DHCP. 29](#_Toc36420389)

[Figure 41:contrôle d’accès. 30](#_Toc36420390)

[Figure 42:ACL. 30](#_Toc36420391)

[Figure 43:Désactivation du bootp.. 30](#_Toc36420392)

[Figure 44:Désactivation du service finger. 30](#_Toc36420393)

[Figure 45:Désactivation du service CDP. 30](#_Toc36420394)

[Figure 46:Désactivation des services de configuration à distances. 30](#_Toc36420395)

[Figure 47:Désactivation de l’IP sans classe. 30](#_Toc36420396)

[Figure 48:Désactivation des requêtes TFTP. 30](#_Toc36420397)

[Figure 49:A réaliser dans les interfaces désirées. 31](#_Toc36420398)

[Figure 50:A réaliser dans les interfaces désirées. 31](#_Toc36420399)

[Figure 51:Désactivation du routage par la source. 31](#_Toc36420400)

[Figure 52: A réaliser dans les interfaces désirées.: 31](#_Toc36420401)

[Figure 53:Sécurisation des accès administratifs par mot de passe. 31](#_Toc36420402)

[Figure 54:Configurer la longueur minimale d’un mot de passe. 31](#_Toc36420403)

[Figure 55:Limiter le nombre de tentatives de connexions échouées. 31](#_Toc36420404)

[Figure 56:Désactiver le service de réinitialisation des mots de passe. 31](#_Toc36420405)

[Figure 57:Architecture finale .: 32](#_Toc36420406)

**Introduction**

Le déploiement ainsi que l’exploitation d’un réseau informatique est primordiale pour le bon fonctionnement d’une entreprise de nos jours. Mis à part la mise à disposition à divers utilisateurs allant du simple employé au directeur, il faut faire face à des challenges quotidiens que ce soit au niveau de la disponibilité et le bon fonctionnement des ressources réseaux, mais aussi au niveau de la sécurité de ce dernier. Le travail à fournir avant le déploiement du réseau est donc de tester de manière virtuelle si ce réseau serait capable d’offrir un fonctionnement consistant en toute sûreté.

Après avoir réfléchis à une structure du réseau interne ainsi qu’externe, à savoir déterminer les différents serveurs/fonctionnalités nécessaires à notre réseau, nous allons finir par établir une politique de sécurité et réfléchir à des améliorations qui peuvent être faites afin d'optimiser l’ergonomie et la bonne manœuvrabilité de notre réseau.

**Chapitre 1 : Installation et Configuration d'infrastructure réseau :**

**1. Active Directory: Installation sur Windows Server 2012**

**1.1 Le rôle, les avantages et les contraintes de l’active Directory :**

* + - 1. **L’utilité d’Active Directory :**

**L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, MacOs et encore Linux. Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l’accès aux ressources répertoriées.**

**Une infrastructure Active Directory fonctionne selon une hiérarchie qui représente une entité de sécurité hébergeant utilisateurs et ordinateurs. Cette infrastructure forme ainsi une arborescence composée de domaines, d’arbres de domaine ou de forêts. Les différents domaines constituants une arborescence communiquent entre eux via des relations d’approbation.**

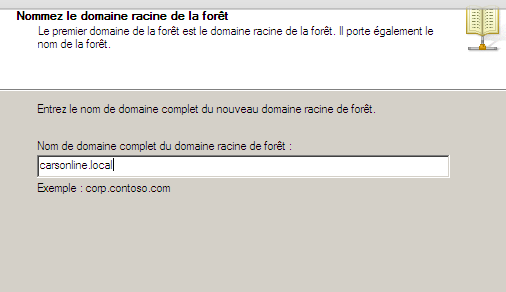
**Une forêt est un regroupement de plusieurs domaines Active Directory et possède un seul schéma. Le premier domaine installé dans une forêt est appelé domaine racine de la forêt. Plusieurs arbres de domaines dont l’espace de nom n’est pas continu représentent une forêt.**

Figure 1:Nom de domaine:

* + - 1. **Installation de l’AD :**

**AD s’installe comme tout autre fonctionnalité d’un serveur ( DNS , DHCP …), il faut ajouter un rôle/fonction au serveur. Comme AD fait partie d’une forêt, il faut alors choisir un nom de domaine pour la racine de ce dernier.**

**A la fin des choix des différents paramètres, l’installation se complète et l’’on doit par la suite redémarrer le serveur.**

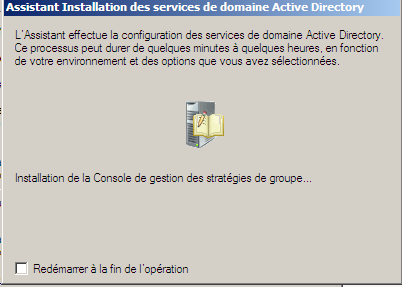


Figure 2:Installation des services des de domaine.

**Toute à la fin, l’installation a bien été effective, nous avons créer un domaine local pour l’Active Directory.**

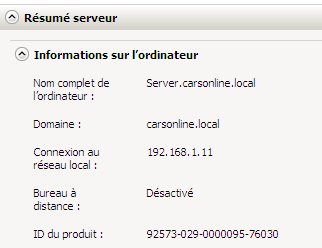
****

Figure 3:Résumé serveur .

* + - 1. **Attribution des rôles aux utilisateurs :**

**Maintenant que l’installation a été faite, il faut désormais attribuer des rôles aux différents utilisateurs du réseau.**

**Certaines fonctions - on parle de rôles - ne peuvent être attribués chacun qu'à un seul serveur à la fois, qui devient alors le maître d'opérations (Operations master en anglais) pour un ou plusieurs rôles. L'ensemble de ces rôles, appelés en anglais FSMO (pour Flexible Single Master Operations), peuvent donc être répartis sur un ou plusieurs contrôleurs de domaine. Ils sont au nombre de 5**[**4**](https://fr.wikipedia.org/wiki/Active_Directory#cite_note-4) **:**

|  |  |  |
| --- | --- | --- |
| **Nom du rôle** | **Position** | **Description** |
| **Maître de schéma (Schema Master)** | **1 par forêt** | **Contrôle les modifications apportées au schéma de données Active Directory.** |
| **Maître d'attribution de noms de domaine (Domain Naming Master)** | **1 par forêt** | **Contrôle l'ajout et la suppression des noms de domaines dans une forêt afin de garantir leur unicité.** |
| **Émulateur de PDC (PDC Emulator)** | **1 par domaine** | **Se comporte comme un contrôleur de domaine NT4 pour permettre le support de clients NT4 (par exemple pour gérer les changements de mots de passe), ce contrôleur fournit également l'horloge de référence du domaine.** |
| **Maître RID (RID Master)** | **1 par domaine** | **Fournit des tranches d'identifiants uniques aux autres contrôleurs de domaine.** |
| **Maître d'infrastructure (Infrastructure Master)** | **1 par domaine** | **Synchronise les changements inter-domaines.** |

**On peut alors créer des utilisateurs, avec login et mot de passe, qui vont avoir certaines permissions ou restrictions sur l’utilisation des fonctionnalités du réseau.**

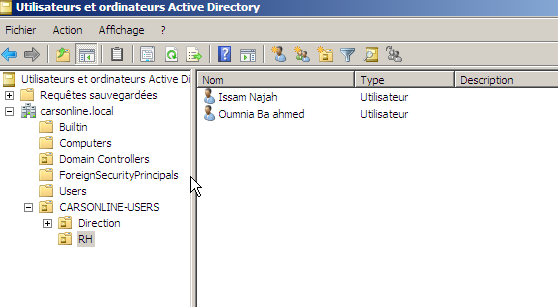


Figure 4:les utilisateurs et ordinateurs Active Directory.

**Ou encore avoir quelques administrateurs qui vont avoir tous les droits possibles et imaginables sur la gestion du serveur.**

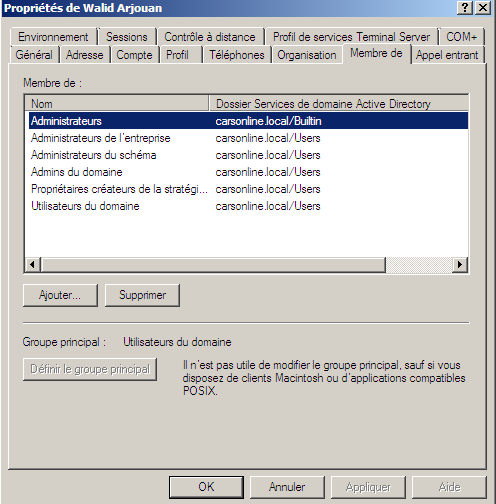


Figure 5:Architecture finale.

**2. Serveur DNS (Bind9) :**

**2.1 Définition:**

**BIND est le serveur** [**DNS**](https://fr.wikipedia.org/wiki/Domain_Name_System) **le plus utilisé sur** [**Internet**](https://fr.wikipedia.org/wiki/Internet)**(79 % des serveurs en 2008**[**5**](https://fr.wikipedia.org/wiki/BIND#cite_note-5)**), spécialement sur les systèmes de type** [**UNIX**](https://fr.wikipedia.org/wiki/UNIX) **et est devenu *de facto* un** [**standard**](https://fr.wikipedia.org/wiki/Normalisation_(industrie_et_service))**.**

**2.2 Installation de serveur sous Linux(Ubuntu):**

* **L’installation se fait par la commande :**

**“sudo apt-get install bind9 bind9utils bind9-doc”**



Figure 6:Installation de serveur.

**2.3 Configuration de Serveur DNS Bind9 :**

**a. Configuration de fichier named.conf.local :**

**Déclaration des zones:**

**On va maintenant ajouter nos zones Dns, pour chaque site internet que vous hébergerez sur ce serveur vous devrez rajouter une zone Dns dans le fichier “/etc/bind/named.conf.local”**

**Ici le nom de domaine est toujours oumnia et la configuration de la zone pour oumnia.ma se fera dans le fichier /etc/bind/oumnia.ma**

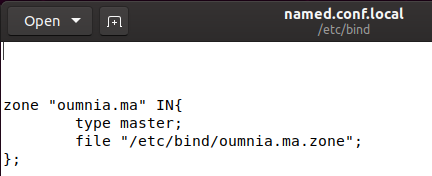
****

Figure 7:Configuration de fichier named.conf.local :

**b. Configuration de fichier zone :**

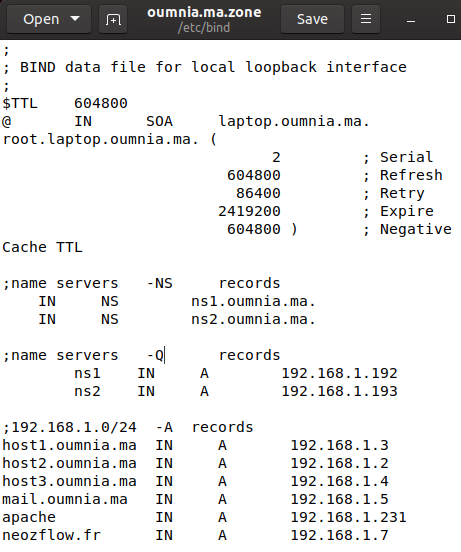
**On créent le fichier de résolution de zone /etc/bind/oumnia.ma. et pour faciliter la configuration on copier la configuration de fichier db. local vers oumnia.ma.zone par la commande cp db.local oumnia.ma.zone.**

Figure 8:Configuration de fichier zone.

**Maintenant on peut spécifier les noms de domaines avec les adresses IP par exemple : Apache c’est le nom de domaine de serveur web qui a l’adresse IP 192.168.1.231 Mail.oumnia.ma est le nom de domaine de serveur mail qui a l’adresse IP 192.168.1.45.**

**c. Création de fichier de zone inversée :**

**Dans ce fichier on configure l’inverse.**

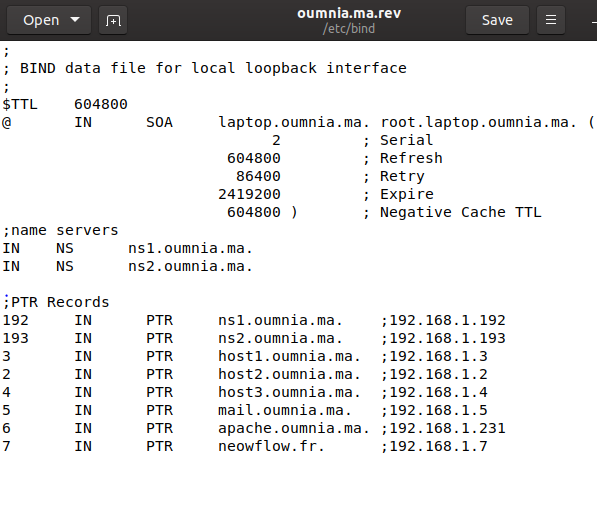


Figure 9:Configuration de fichier zone.

1. **Vérification la syntaxe de configuration de BIND :**

**On peut vérifier la syntaxe de configuration par la commande “named-checkconf”**

**Redémarrer BIND avec la commande “service bind9 restart”**

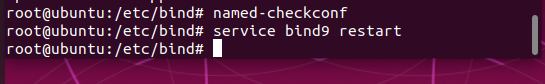


Figure 10:Vérification du syntaxe et redémarrage.

**3. Serveur Mail (postfix)**

**3.1. Définition de postfix :**

**Postfix est un**[**serveur de messagerie électronique**](https://fr.wikipedia.org/wiki/Serveur_de_messagerie_%C3%A9lectronique)**et un**[**logiciel libre**](https://fr.wikipedia.org/wiki/Logiciel_libre)**développé par [Wietse Venema](https://fr.wikipedia.org/wiki/Wietse_Venema" \o "Wietse Venema) et plusieurs contributeurs. Il se charge de la livraison de**[**courriers électroniques**](https://fr.wikipedia.org/wiki/Courriers_%C3%A9lectroniques)**(**[**courriels**](https://fr.wikipedia.org/wiki/Courriel)**) et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique [Sendmail](https://fr.wikipedia.org/wiki/Sendmail" \o "Sendmail).**

**2.3.Avantage de postfix.**

* **Il est adapté pour des gros besoins**
* **Facile à installer et à configurer**
* **Maintenance aisée**
* **Sécurisé avec anti Spam**
* **Codes sources libres**
* **Multi plate-forme de type UNIX (MAC OS, GNU/LINUX).**
* **Gratuit**
* **Accessible en mobilité**

**3.3 Installation et configuration.**

**a. Installation des paquets**

**Pour installer postifix, on exécute cette commande « apt-get install postfix** » **et laissons d'abord tous les différents paramétrages qui seront tout au long de l’installation par défaut.**



Figure 11:Installation des paquets .

**Nous allons installer les autres paquets qu'on avait cité plus haut : common, imap, pop, et squirelmail.**

**Sur notre invité de commande exécuter : apt-get install dovecot-common dovecot-imapd dovecot-pop3d squirelmail .**



Figure 12:Installation des paquets common, imap, pop, et squirelmail.

**b. Configuration postfix**

**Nous allons maintenant configurer postfix. Ouvrons notre terminal et on exécutons**«**dpkg-reconfigure postfix** »



Figure 13:Configuration postfix.

**Sur la première fenêtre on sélectionne « Local uniquement »**

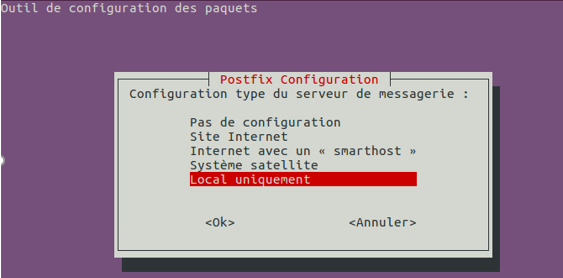


Figure 14:Configuration type de messagerie.

**Ensuite sur la fenêtre qui suit, notre nom de courrier : « mail.supmail.net ».**

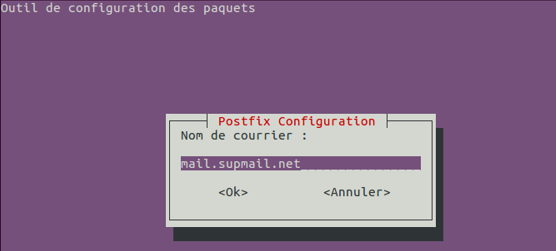


Figure 15:Configuration type de messagerie.

Remplissons la fenêtre suivante comme indiquer sur la figure ci-dessous en ajoutant cette fois-ci nos destinataires des courriels root et postmaster tout en indiquant encore notre nom de courrier "mail.supmail.net" et notre nom de domaine "supmail.net".

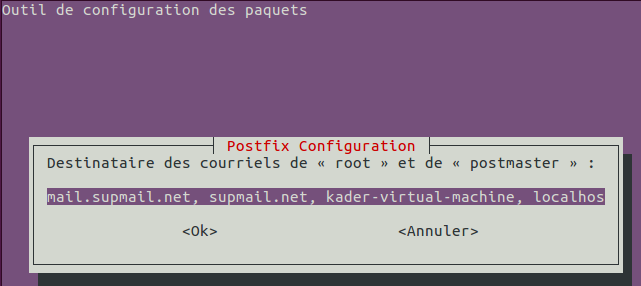


Figure 16:Configuration destinataire des courriels.

**Laisser les deux prochaines fenêtres par défaut, et sur celle qui va suivre on nous demandera de choisir le Protocol internet à utiliser, choisissez**« tous »**et faites OK pour finalisez votre configuration.**

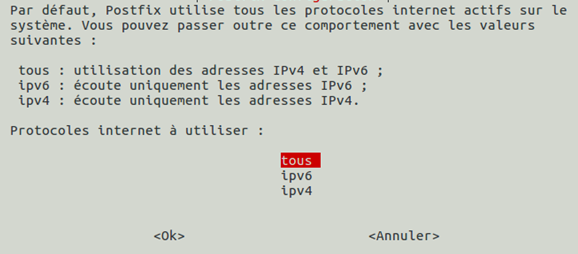


Figure 17:Protocol internet.

**c. Configuration squirremail**

**On exécute nano** **/etc/squirremail/apache.cong , on remplace** webmail.exemple.com**par notre nom de courrier « mail.supmail.com » comme indiquer sur l’image ci-dessous :**

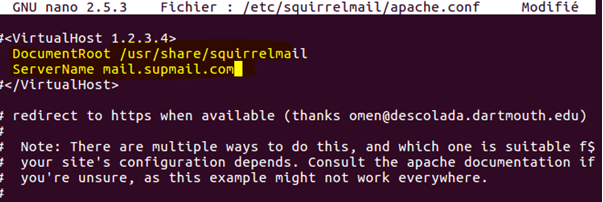


Figure 18:Configuration squirremail.

**Ensuite Nous allons aussi modifier notre fichier dovecot.conf. On Exécute la commande « nano /etc/dovecot.conf ». Et dans fichier, on ajoute les lignes suivantes :**

**Protocols = imap pop3**

**#disable\_plaintext\_auth = no**

**mail\_location = mbox :~/mail :INBOX=/var/mail/%u**

**mail\_location = maildir :~/Maildir**

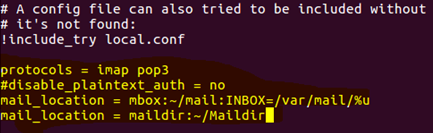


Figure 19:fichier dovecot.conf:

**Après cette configuration, on va maintenant attribuer une adresse IP statique à notre machine, on exécute la commande « ifconfig eth0 192.168.1.5 netmask 255.255.255.0**

**Enfin on rédemarrer tous les services, c’est-à-dire le service Bind, dovecot et postfix sur votre terminal :**

**- Bind :** **pour redémarrer bind, exécutez la commande /etc/init.d/bind9 restart**

- **apache :** **pour redémarrer, apache exécutez la commande /etc/init.d/apache2 restart**

- **postfix :** **pour redémarrer postfix, exécutez la commande : /etc/init.d/ postfix restart**

**4. Serveur web (Wamp) :**

**4.1. Serveur web (Wamp) :**

**WampServer (anciennement WAMP5) est une plateforme de développement Web de type** [**WAMP**](https://fr.wikipedia.org/wiki/WAMP)**, permettant de faire fonctionner localement (sans avoir à se connecter à un serveur externe) des scripts** [**PHP**](https://fr.wikipedia.org/wiki/PHP)**. WampServer n’est pas en soi un logiciel, mais un environnement comprenant trois serveurs (**[**Apache**](https://fr.wikipedia.org/wiki/Apache_HTTP_Server)**,** [**MySQL**](https://fr.wikipedia.org/wiki/MySQL) **et** [**MariaDB**](https://fr.wikipedia.org/wiki/MariaDB)**), un interpréteur de script (PHP), ainsi que** [**phpMyAdmin**](https://fr.wikipedia.org/wiki/PhpMyAdmin) **pour l’administration Web des bases MySQL.**

**4.2Base de données (MySQL) :** 

**MySQL est un** [**système de gestion de bases de données**](https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_gestion_de_base_de_donn%C3%A9es) **relationnelles (SGBDR). Il est distribué sous une double licence** [**GPL**](https://fr.wikipedia.org/wiki/Licence_publique_g%C3%A9n%C3%A9rale_GNU) **et** [**propriétaire**](https://fr.wikipedia.org/wiki/Logiciel_propri%C3%A9taire)**. Il fait partie des logiciels de gestion de** [**base de données**](https://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es) **les plus utilisés au monde**[**4**](https://fr.wikipedia.org/wiki/MySQL#cite_note-4)**, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec** [**Oracle**](https://fr.wikipedia.org/wiki/Oracle_Database)**,** [**PostgreSQL**](https://fr.wikipedia.org/wiki/PostgreSQL) **et** [**Microsoft SQL Server**](https://fr.wikipedia.org/wiki/Microsoft_SQL_Server)**.**

**4.3. Les interfaces de l’application :**

**a-Page connexion:**

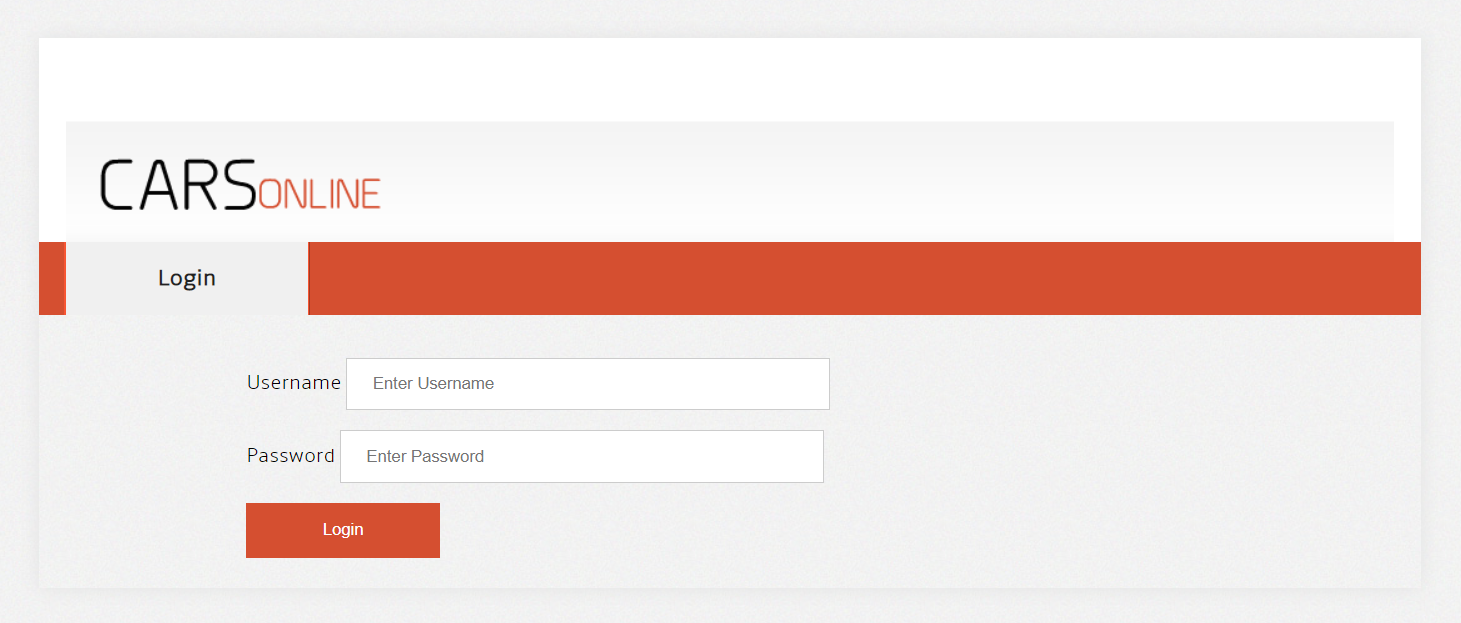


Figure 20:page login.

**b-Page index:**

**C’est la page d’accueil de notre application contient tous les voitures disponibles pour louer .**

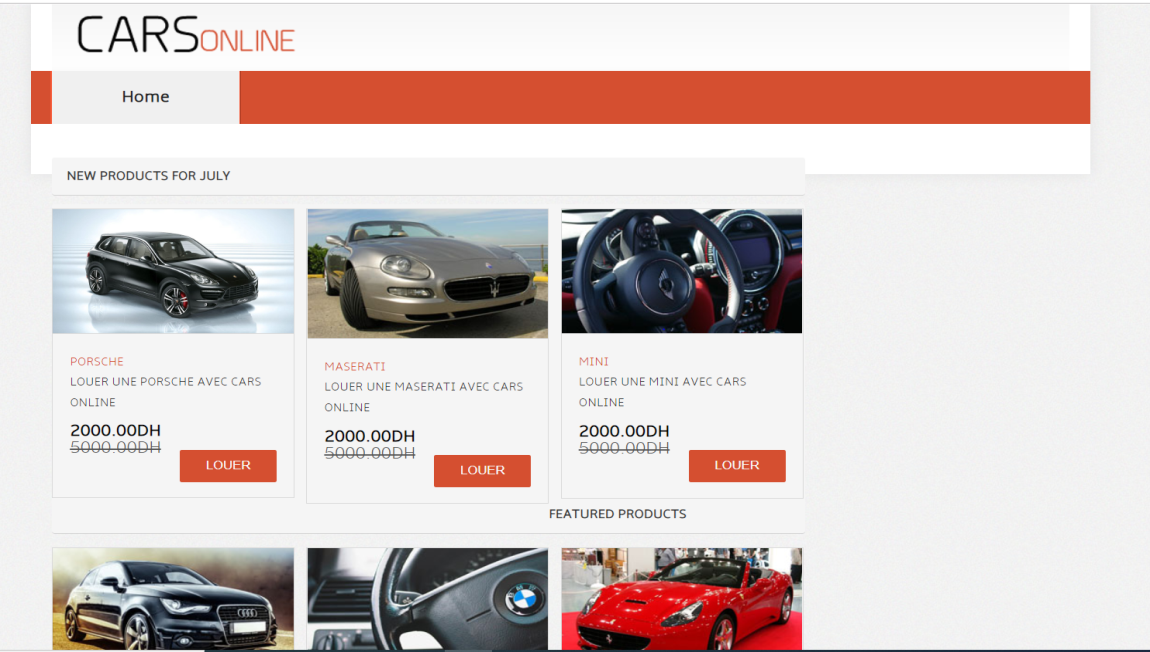
****

Figure 21:page login:

**c. Page Contact:**

**Cette page contient les champs qui concernent les informations du client.**

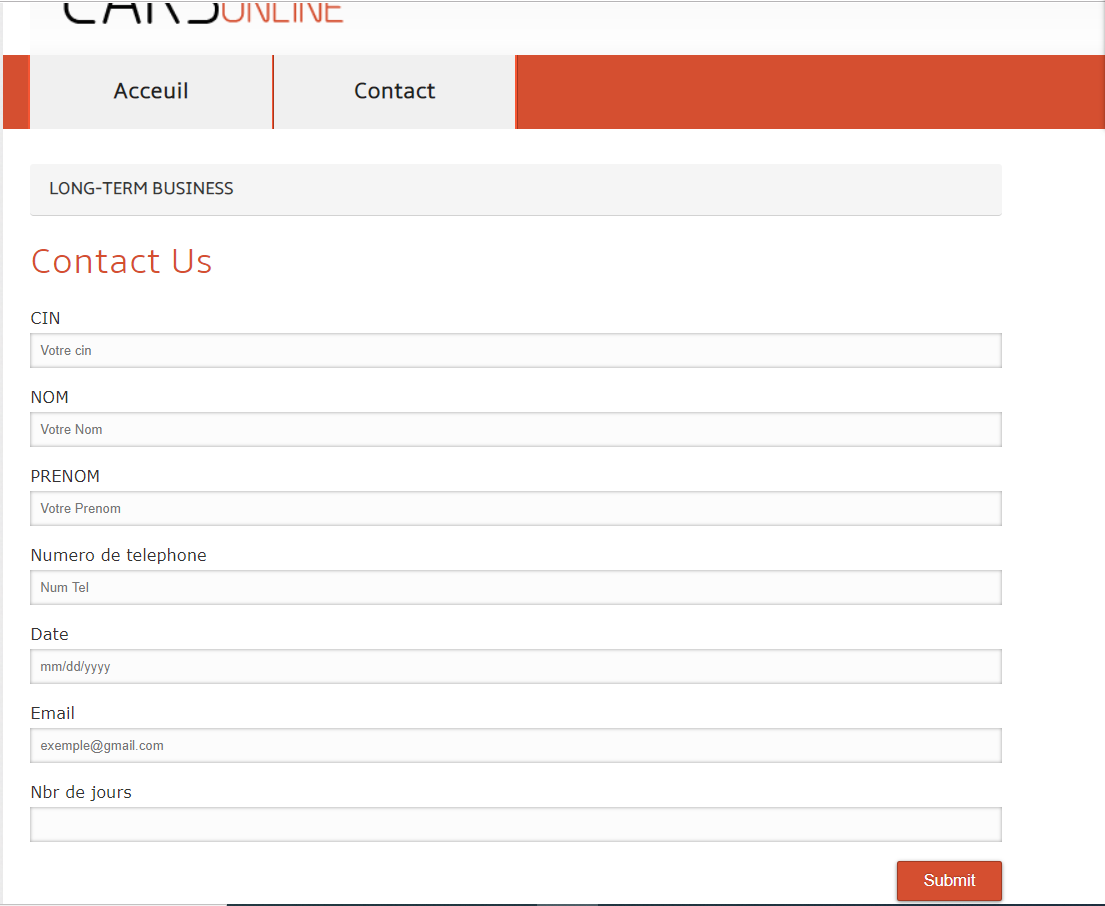


Figure 22:page contact.

**d. Page Contrat:**

**C’est la page qui contient les informations du client et de la voiture.**

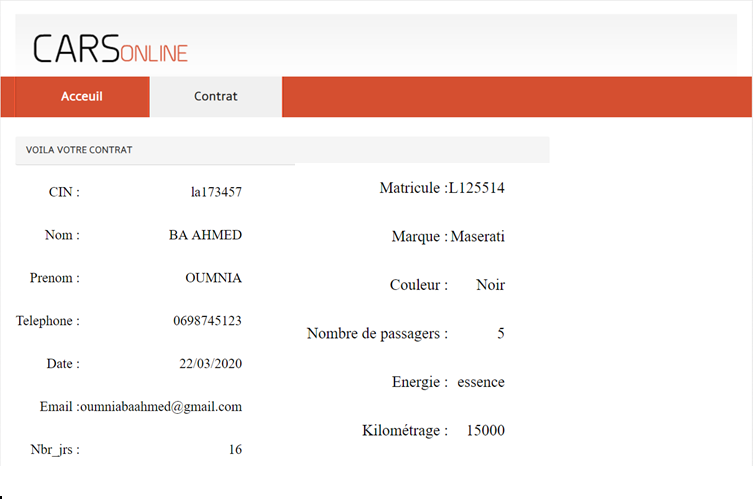


Figure 23:page contact.

**5. Serveur DHCP :**

**5.1. Définition :**

***Dynamic Host Configuration Protocol***  **est un**[**protocole réseau**](https://fr.wikipedia.org/wiki/Protocole_r%C3%A9seau)**dont le rôle est d’assurer la configuration automatique des paramètres IP d’une**[**station**](https://fr.wikipedia.org/wiki/Station_de_travail)**ou d'une machine, notamment en lui attribuant automatiquement une**[**adresse IP**](https://fr.wikipedia.org/wiki/Adresse_IP)**et un**[**masque de sous-réseau**](https://fr.wikipedia.org/wiki/Masque_de_sous-r%C3%A9seau).

**5.2. Installation :**

* **L’installation se fait par la commande :**

**¨apt-get install isc-dhcp-server ¨**

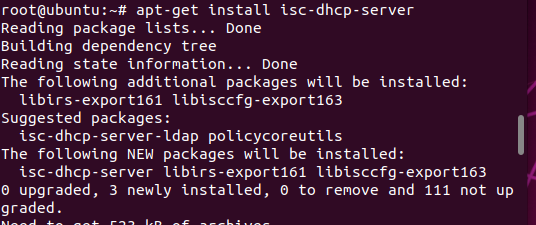


Figure 24:Installation DHCP.

**5.2. Configuration :**

**Le serveur DHCP assignera au client une adresse IP comprise entre 192.168.1.10 et 192.168.1.100 pour une durée de 600 secondes. Le client peut spécifier une période de temps spécifique, dans ce cas, le temps d'allocation maximum est de 7200 secondes.**

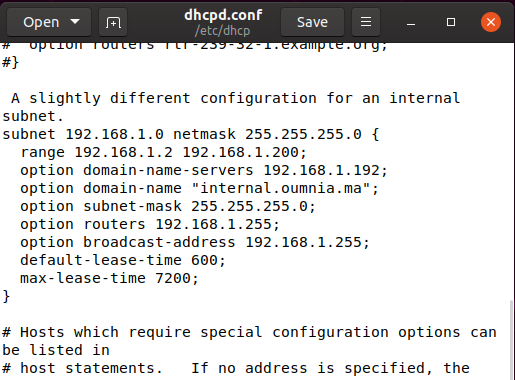
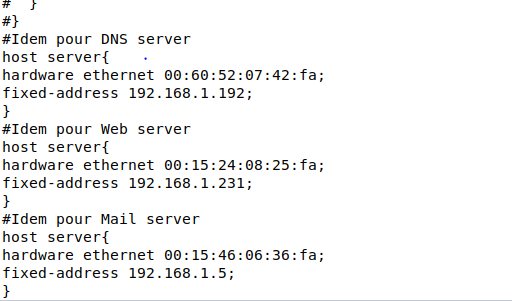


Figure 25:Configuration du fichier dhcpd.conf.

**Dans ce cas, l'adresse IP que reçoit le client est toujours la même. Pour cela il suffit d'ajouter une directive *host* dans la définition du subnet. Pour chaque client, il faut donner son adresse fixe en fonction de son adresse MAC.**



**.**

Figure 26:Configuration du fichier dhcpd.conf (suite).

**-le démarrage de serveur DHCP**

Figure 27:Redémarrage du serveur.

**Chapitre2 : les risques de sécurité.**

**Nous avons essayé d'identifier le maximum des risques et le classe selon leur type avec leur effet, Pour bien Sécuriser cette infrastructure.**

:

**1. Les risques de réseau :**

**• Routeur tombe en panne : (faible)**

**• Port non sécurisée : (faible-moyenne)**

**• L’utilisation des mots de passe par défaut : (faible)**

**• Attaque sur le réseau: (moyenne)**

**2.Les risques physiques :**

**Les risques physiques sont tout simplement ceux liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels.**

* 1. **Les risques d’électricité : (faible)**

**Défaillance du fournisseur d’électricité (coupure, qualité) surtension, une baisse de tension, sabotage, etc. …, qui donne comme conséquences : incendie, arrêt de l’activité et perte de l’exploitation, destruction de données et de fichiers, matériels en panne, etc.**

* 1. **Sécurité de l’accès à la salle informatique : (faible)**

**Evènement naturel, un attentat, des manifestations, des émeutes, suite à une décision de justice, etc. qui donne comme des résultats :la salle informatique cesse de fonctionner, dégradation de tous les équipements, etc.**

**2.3. Panne au niveau des climatiseurs : (faible)**

**3. Les risques d’exploitation :**

**3.1. Email Bombing :(moyenne)**

**C’est une attaque de type DDos permet de bombarder la messagerie, cette technique d’attaque visant à envoyer plusieurs milliers de messages identiques à une boîte aux lettres électronique afin de la saturer.**

**3.2.** **SQL injection : (moyenne)**

**L'injection SQL est une méthode d'attaque très connue. C'est un vecteur d'attaque extrêmement puissant quand il est bien exploité. Il consiste à modifier une requête SQL en injectant des morceaux de code non filtrés, généralement par le biais d'un formulaire.**

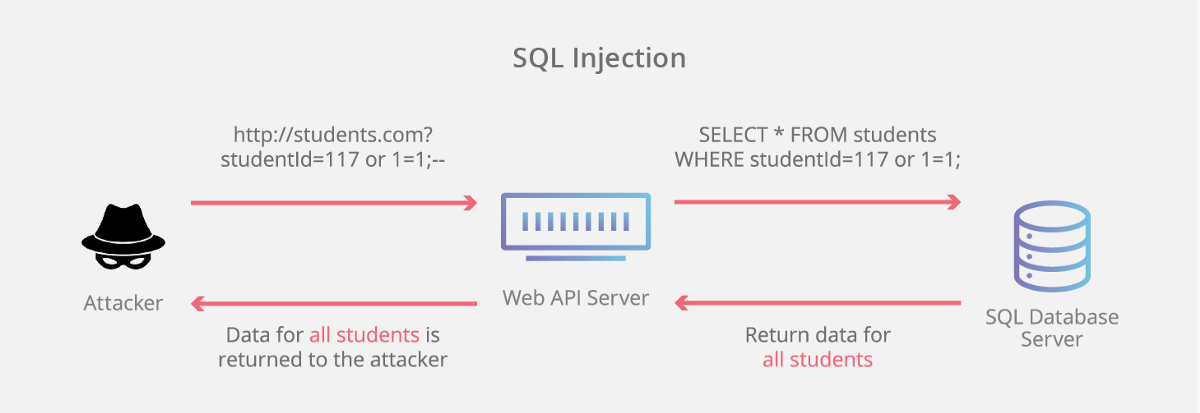


Figure 28:SQL injection.

**Exemple du code injecté :**

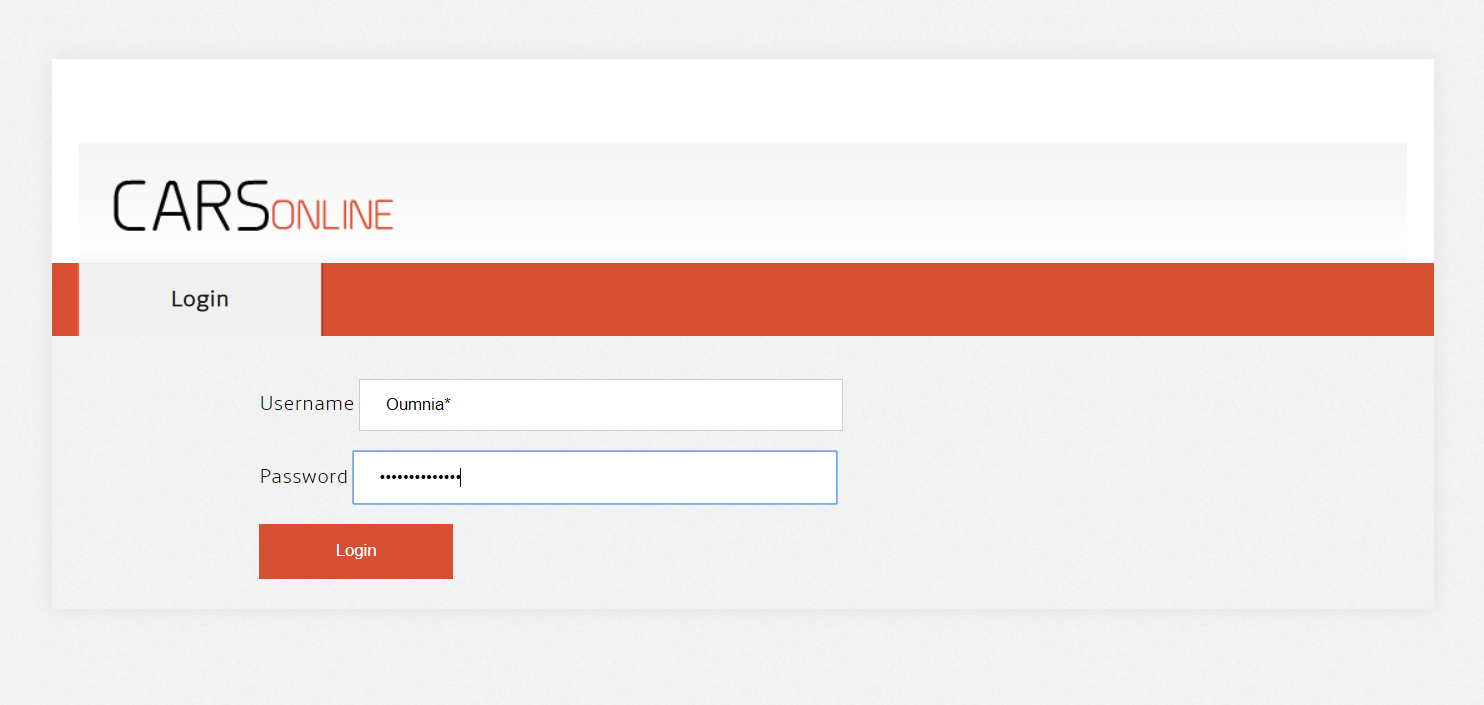


Figure 29:Exemple du code injecté.

Les caractères -- marquent le début d'un commentaire en SQL ce qui annule la suite. La requête est donc équivalente à :



**3.3. Attaque l’homme du milieu**

**L'attaque de l'homme du milieu est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.**

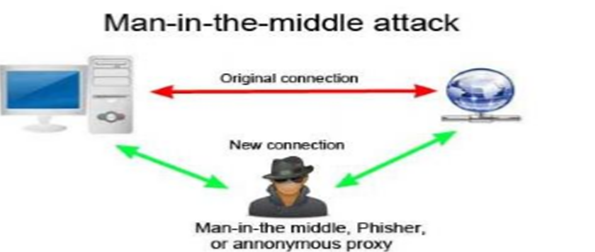


Figure 30:attaque l’homme du milieu.

**3.4. Attaque tcp syn :**

**Le SYN flood est une attaque informatique visant à atteindre un**[**déni de service**](https://fr.wikipedia.org/wiki/D%C3%A9ni_de_service)**. Elle s'applique dans le cadre du protocole**[**TCP**](https://fr.wikipedia.org/wiki/Transmission_Control_Protocol)**et consiste à envoyer une succession de**[**requêtes**](https://fr.wikipedia.org/wiki/Paquet_(r%C3%A9seau))**SYN vers la cible**.

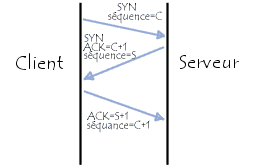


Figure 31:Attaque TCP SYN.

**3.5. Attaque par déni de service.**

**Une attaque par déni de service ([abr.](https://fr.wikipedia.org/wiki/Abr%C3%A9viation" \o "Abréviation) DoS attack pour Denial of Service attack en anglais) est une attaque**[**informatique**](https://fr.wikipedia.org/wiki/Informatique)**ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l’heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abr. DDoS attack pour Distributed Denial of Service attack). Il peut s'agir de :**

* **l’**[**inondation**](https://fr.wikipedia.org/wiki/Flood_(Internet))**d’un**[**réseau**](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique)**afin d'empêcher son fonctionnement ;**
* **la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;**
* **l'obstruction d'accès à un service pour une personne en particulier ;**
* **également le fait d'envoyer des milliards d'octets à une box internet.**

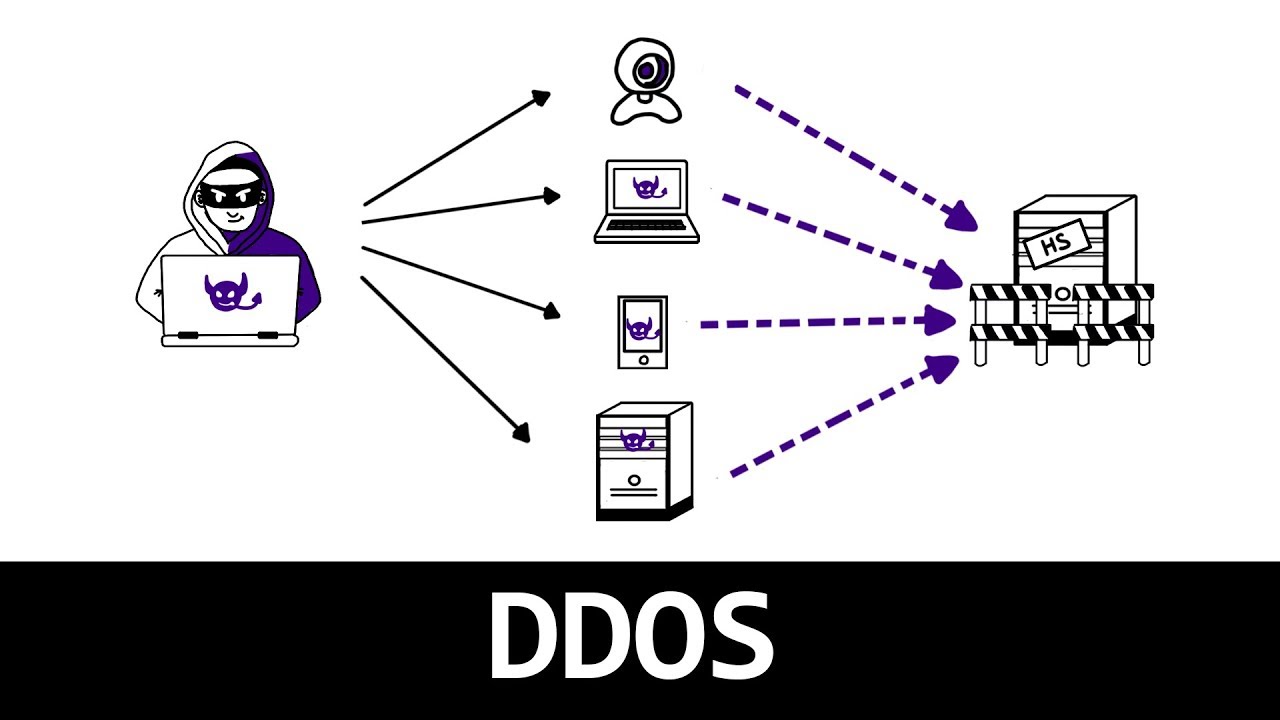
**L'attaque par déni de service peut ainsi bloquer un**[**serveur de fichiers**](https://fr.wikipedia.org/wiki/Serveur_de_fichiers)**, rendre impossible l'accès à un**[**serveur web**](https://fr.wikipedia.org/wiki/Serveur_HTTP)**ou empêcher la distribution de**[**courriel**](https://fr.wikipedia.org/wiki/Courriel)**dans une entreprise.**

Figure 32:Attaque par déni de service.

**3.6. Portes non sécurise (moyenne)**

**3.7. Elévation des privilèges**

**En informatique, un mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement.**

**• Conséquence : contrôle total d'un système.**

**• Solution : exploiter une faille de sécurité, en local sur le système (s'il est déjà connecté dessus), ou à distance (si le système est connecté à un réseau)**

**3.8. Code arbitraire**

**Est employé pour nommer, en parlant de piratage informatique, une action à faire faire une machine sans que le propriétaire soit d'accord.**

**• Conséquences : ouvrir une session super-utilisateur sur une machine distante, modifier une base de données, ou plus généralement donner accès à une information non disponible.**

**• Solution : La mise à jour de sécurité corrige la vulnérabilité.**

**3.9. Atteinte à la confidentialité donnée**

**Un utilisateur laisse son navigateur ouvert après s'être déconnecté d'une application et si un attaquant rouvre l'application dans le navigateur directement après.**

**• Conséquence : permettre la divulgation d’informations.**

**• Solution : La mise à jour de sécurité corrige la vulnérabilité en s'assurant que le processus de déconnexion déconnecte correctement l'utilisateur.**

**4. Les risques logiques :**

**4.1. Ingénierie sociale : (moyenne)**

**En utilisant les moyens usuels (téléphone, email…) et en usurpant une identité, un attaquant cherche à obtenir des informations confidentielles auprès du personnel de l’entreprise en vue d’une intrusion future.**

**5. Les risques liés au traitement des données :**

• **Information confidentielle : (moyenne) Ce sont les données qui sont confidentiels de l’entreprise**

**• Perte des données : (faible)**

**• Sabotage Informatique : (moyenne)**

**Chapitre 3 : Mise en place de la politique de sécurité :**

1. **Une politique de sécurité adéquation :**

**1.1. Sécurité physique**

**a.** **Installation des caméras et installer un system de refroidissement**

**Les cameras jouent un grand rôle pour améliorer la sécurité des salles, et avoir la possibilité de bien protéger notre system d’information, au tant que les system de refroidissement qui permet de faire la protection contre les incendies.**

**b. L’accès aux salles des serveurs.**

**L’accès aux salles des serveurs juste pour les personnes autorise.**

**1.2. Duplication des serveurs**

**Nous avons essayé de dupliquer les serveurs que nous avons installé dans le cas qu’un tomber en panne, le deuxième prendre le travail.**

**Exemple :**

**a.DNS**

Nous **avons 2 serveurs DNS .si un serveur tombe en panne le deuxième se fonctionne.**

**Master : ns1.oumnia.ma**

**Auxiliaire : ns2.oumnia.ma**

**b.DHCP**

**Nous avons 2 serveurs DHCP :**

**Master : ROUTEUR ASA**

**Auxiliaire : SERVEUR DHCP**

**c.Contrôleur de domaines**

**Nous avons 2 contrôleurs de domaines :**

**Master : carsonline.local**

**Auxiliaire : carsonline1.g3**

**d.Mail serveur :**

**Nous avons 2 serveurs Mail : Le temps pour que les services sont reconnectés au deuxième serveur est : 10 seconds.**

**e.Creation d’un backup application web:**

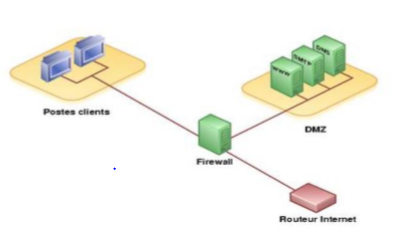
**Le backup d’application web est la copie de dossier d’application web. Dans le cas au notre application tomber en panne, nous avons créé un backup d’application web qui se trouve dans un notre serveur web 2 : apache2.group3.ma.**

**1.3. Sécurité de réseau**

**a. DMZ :**

**Une zone démilitarisée, ou DMZ est un**[**sous-réseau**](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique)**séparé du**[**réseau local**](https://fr.wikipedia.org/wiki/R%C3%A9seau_local)**et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un**[**pare-feu**](https://fr.wikipedia.org/wiki/Pare-feu_(informatique))**. Ce sous-réseau contient**

**les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.**

****

**Figure 33:une zone démilitarisée.**

**b. Utilisation des routeurs asa (Firewall) :**

**Les routeurs Cisco asa contient firewall ce qui facilite l’implémentation de DMZ.**

**c. IDS :**

**Un système de détection d'intrusion (ou IDS : Intrusion detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussie comme échouées des intrusions.**

**d. Duplication des routeurs :**

**Le protocole HSRP sélectionne l'un des routeurs comme routeur actif. Le routeur actif fait fonction de passerelle par défaut des périphériques finaux. L'autre routeur devient le routeur de secours (standby). En cas de** **défaillance du routeur, le routeur de secours prend automatiquement le relais comme routeur actif. Il devient la passerelle par défaut des périphériques finaux.**

**e. Réseau de CLOS :**

**C’est une topologie implémenter dans les centres de données, pour que le réseau soit toujours disponible.**

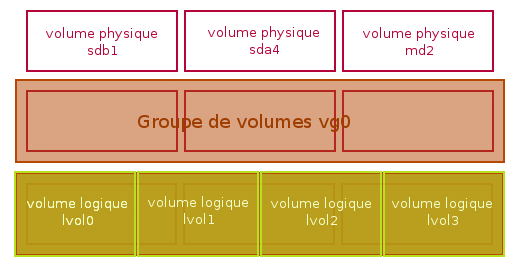
**f. Renforcé la sécurité des routeurs.**

* **Désactivation des services inutiles.**
* **Ajout de mot de passe.**
* **Sécurisation des accès administratifs par mot de passe.**

**1.4. Sécurité de données :**

**a. LVM :**

**La gestion par volumes logiques (en anglais, logical volume management ou LVM) est à la fois une méthode et un logiciel de gestion de l'utilisation des espaces de stockage d'un ordinateur. Il permet de gérer, sécuriser et optimiser de manière souple les espaces de stockage en ligne dans les**[**systèmes d'exploitation**](https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation)**de type**[**UNIX**](https://fr.wikipedia.org/wiki/UNIX)**.**



**Figure 34:La gestion par volumes logiques.**

1. **Implémentation et test de politique de sécurité :**
   1. **Configuration de protocole HSRP.**

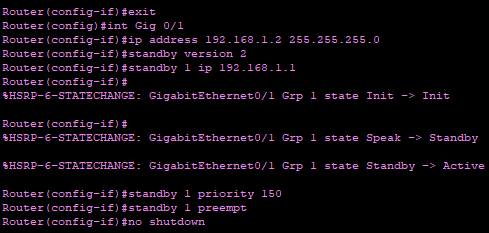
**Pour configurer HSRP, procédez comme suit :**

**Étape 1. Configurez HSRP version 2.**

**Étape 2. Configurez l'adresse IP virtuelle du groupe.**

**Étape 3. Configurez la priorité pour que le routeur actif requis ait une priorité supérieure à 100.**

**Étape 4. Configurez le paramètre de préemption du routeur actif de sorte qu'il puisse prendre la main dans le cas où le routeur de secours serait disponible avant lui.**

**Configuration de routeurs actifs :**

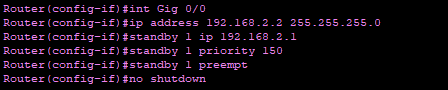
Figure 35:La première interface.

Figure 36:La deuxième interface.

**Configuration de routeur de secours :**

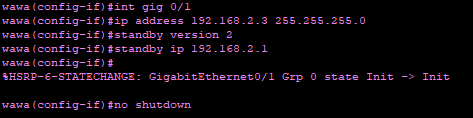
****

Figure 37:La première interface.

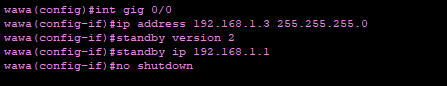


Figure 38:La deuxième interface.

* 1. **DNS :**

**Le temps pour que les services sont reconnectés au deuxième serveur est : 10seconds.**

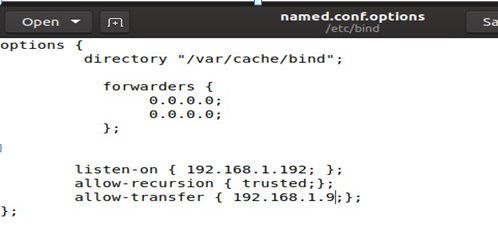
**Comme ça la transmission se passe automatique dans le réseau.**

Figure 39:configuration fichier named.conf.options.

**2.3. Contrôleur de domaines :**

**Si le contrôleur de domaines principales tombe en panne, il faut déconnecter de ce domaine et de connecter au 2eme dans tout le réseau.**

**Le temps pour de déconnecter de se contrôleur et de se connecter au deuxième est : 1 min.**

**2.4. Mail serveur :**

**Si le mail serveur tome en panne, il faut déconnecter de ce serveur et utiliser le deuxième mail serveur.**

**Le temps pour de déconnecter de se contrôleur et de se connecter au deuxième est : 1 min.**

**2.5. DHCP :**

**Premièrement on a configuré un serveur DHCP sur une machine Ubuntu mais si ce serveur tombe en panne les machines ne peuvent pas configure leurs adresse IP dynamiquement.**

**Donc on va configure un deuxième serveur DHCP sur le routeur asa.**

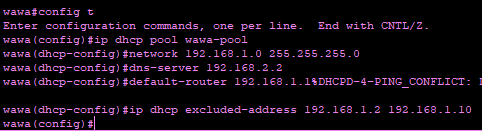
****

Figure 40:configuration du deuxième serveur DHCP.

**2.6. DMZ :**

**Nous avons isolé notre réseau LAN où se trouvent les données de réseau DMZ.**

**Et pour bien sécuriser notre réseau nous avons utilisé le routeur asa 5505 qui joue le rôle d’un routeur et le rôle d’un firewall.**

**Nous avons créé une List de contrôle d’accès au niveau de routeur pour autorise juste la communication avec le protocole DNS, mail et web.**

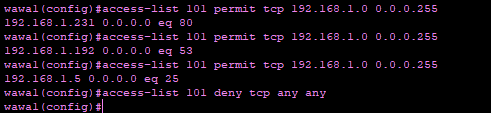


Figure 41:contrôle d’accès.

**Puis on va appliquer cette ACL au niveau d’interface le plus proche au destination.**



Figure 42:ACL.

**2.7. Renforcé la sécurité des routeurs :**

C:\Users\issam najah\Pictures\Saved Pictures\r11.PNG**Désactivation des services inutiles :**

Figure 43:Désactivation du bootp..

C:\Users\issam najah\Pictures\Saved Pictures\r12.PNG

Figure 44:Désactivation du service finger.

C:\Users\issam najah\Pictures\Saved Pictures\r13.PNG

Figure 45:Désactivation du service CDP.

C:\Users\issam najah\Pictures\Saved Pictures\r14.PNG

Figure 46:Désactivation des services de configuration à distances.

C:\Users\issam najah\Pictures\Saved Pictures\r15.PNG

C:\Users\issam najah\Pictures\Saved Pictures\r16.PNGFigure 47:Désactivation de l’IP sans classe.

Figure 48:Désactivation des requêtes TFTP.

**Désactivation des broadcasts dirigés :**

C:\Users\issam najah\Pictures\Saved Pictures\r17.PNG

Figure 49:A réaliser dans les interfaces désirées.

**Désactivation Le routage des redirections ICMP :**

C:\Users\issam najah\Pictures\Saved Pictures\r18.PNG

Figure 50:A réaliser dans les interfaces désirées.

C:\Users\issam najah\Pictures\Saved Pictures\r19.PNG

**Figure 51:Désactivation du routage par la source.**

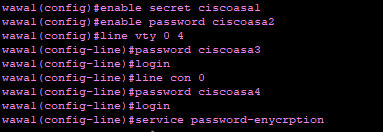
**Désactivation de l’IP unreachable :**

C:\Users\issam najah\Pictures\Saved Pictures\r20.PNG

**Figure 52: A réaliser dans les interfaces désirées.:**

**Ajout de mot de passe :**

* + Le MDP du mode privilégié
  + Le MDP du mode secret
  + Le chiffrement des mots de passes est bien activé
  + Le mot de passe d’accès à la console
  + Le mode de passe de l’accès telnet et SSH :



**Figure 53:Sécurisation des accès administratifs par mot de passe.**

C:\Users\issam najah\Pictures\Saved Pictures\r21.PNG

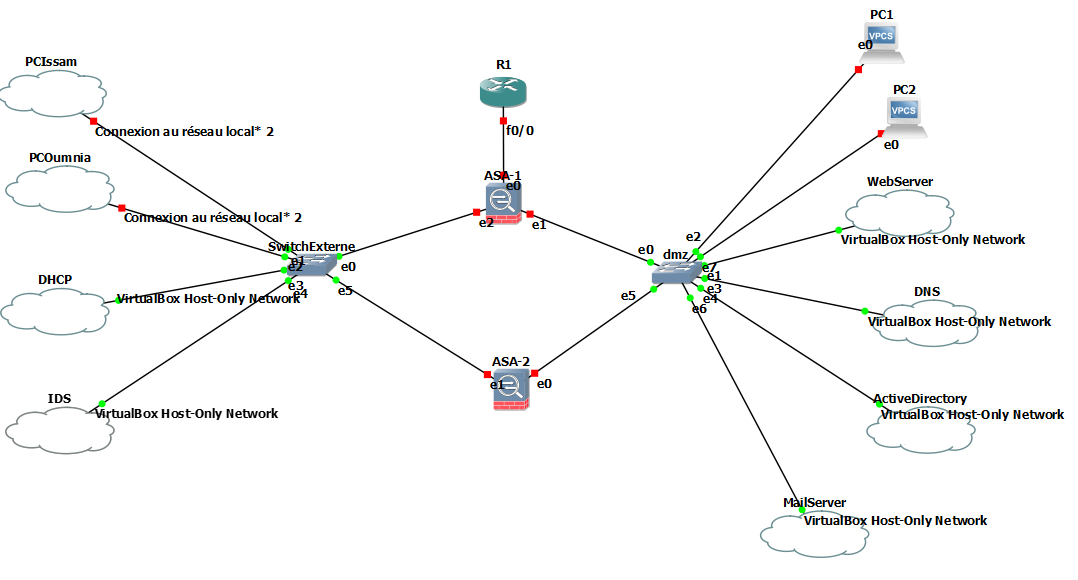
**Figure 54:Configurer la longueur minimale d’un mot de passe.**

C:\Users\issam najah\Pictures\Saved Pictures\r22.PNG

**Figure 55:Limiter le nombre de tentatives de connexions échouées.**

**C:\Users\issam najah\Pictures\Saved Pictures\21.PNG**

**Figure 56:Désactiver le service de réinitialisation des mots de passe.**

**3. Architecture finale :**

**Figure 57:Architecture finale .:**

**4. Les limites et les points à améliorer de votre proposition :**

1. Installation des anti-virus payant.
2. Crypter les données dans base de données
3. Utiliser les services de cloud
4. Implémenter le réseau de Cloud.

Conclusion

Ce projet a été très bénéfique. Ce travail était l'occasion d'apprendre des nouvelles technologies et aussi appliquer quelque connaissance acquise. Les acquis du cours de politique de sécurité étaient sans ces sollicités et cette nouvelle réalisation de ce projet nous a encore permis d'aller plus loin dans les possibilités d'acquérir de nouvelles connaissances surtout en politique de sécurité.

Pour conclure, il existe toujours des améliorations à envisager pour rendre un projet de politique de sécurité encore plus performant.