Table des matières

[Sécurisation de base d'un site 2](#_Toc59626596)

[Enoncé 2](#_Toc59626597)

[Virtual box 2](#_Toc59626598)

[Situation 2](#_Toc59626599)

[Configuration de l'interface 3](#_Toc59626600)

[Configuration du hosts 3](#_Toc59626601)

[Création des dossiers et des index.html 3](#_Toc59626602)

[Création des utilisateurs 3](#_Toc59626603)

[Création du fichier secure.txt 3](#_Toc59626604)

[Création d'un fichier protection.conf 4](#_Toc59626605)

[Création du virtual.conf 4](#_Toc59626606)

[Testez vos configurations 4](#_Toc59626607)

[! Expliquez le principe de l'authentification Basic 4](#_Toc59626608)

[Expliquez le codage Base64 5](#_Toc59626609)

[Testez avec tshark que la méthode d'authentification 'Basic' n'est pas sécurisée. 5](#_Toc59626610)

[Testez d'autres outils permettant de (de)coder un message chiffre par la methode Base64. 5](#_Toc59626611)

[Sécurisation d'un site par SSL 6](#_Toc59626612)

[Enoncé 6](#_Toc59626613)

[Situation 6](#_Toc59626614)

[Configuration de l'interface 7](#_Toc59626615)

[Configuration du hosts 7](#_Toc59626616)

[Création des dossiers et des index.html 7](#_Toc59626617)

[SSL 7](#_Toc59626618)

[Etape 1 : installer openSSL et son module Apache 7](#_Toc59626619)

[Etape 2 : création de la clé privée du serveur 7](#_Toc59626620)

[Etape 3 : création du CSR (Certificate Signing Request) 7](#_Toc59626621)

[Etape 4 : création du certificat 7](#_Toc59626622)

[Etape 5 : copie des clés et des certificats au bon endroit 8](#_Toc59626623)

[Modification du virtual.conf 8](#_Toc59626624)

[Tester 8](#_Toc59626625)

[Importer le certificat dans firefox ou chrome 8](#_Toc59626626)

[Redirection avec le site vh3 du TP Apache de service réseau 8](#_Toc59626627)

# Sécurisation de base d'un site

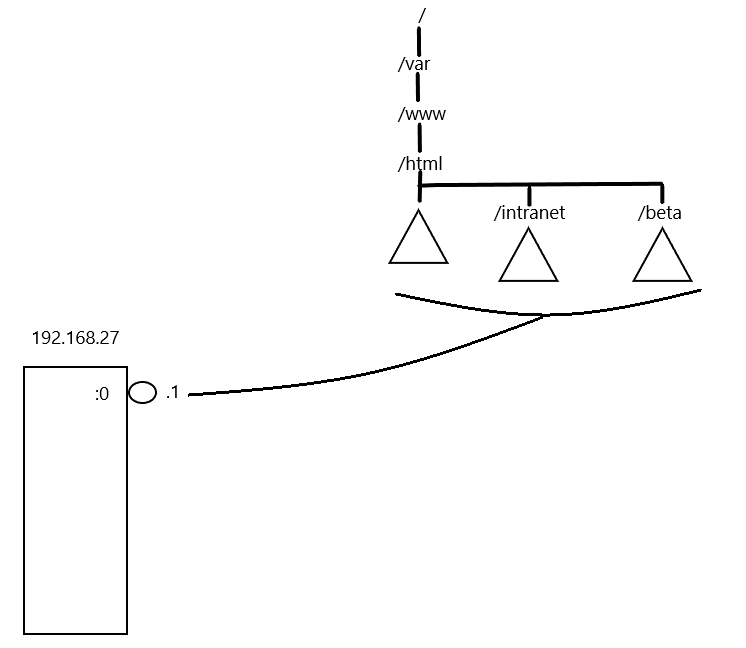
## Enoncé

* Configurez Apache pour :
  + Rendre l'entrée d'un intranet (<http://www.mysite.be/intranet>) uniquement accessible par les machines de notre réseau local 192.168.27.0/24.
  + Que les utilisateurs 'tux', 'bill', 'louis' et 'jean' puissent s'authentifier lorsqu'ils accèdent au site http://www.mysite.be/beta en sachant que seuls 'tux' et 'bill' auront le droit d'accéder a ses ressources.
* Testez vos configurations.
* Expliquez le principe de l'authentification Basic.
* Expliquez le codage Base64.
* Testez avec tshark que la méthode d'authentification 'Basic' n'est pas sécurisée.
* Testez d'autres outils permettant de (de)coder un message chiffre par la méthode Base64.

## Virtual box

Server en accès par pont

## Situation



## Configuration de l'interface

/etc/sysconfig/network-scripts/ifcfg-enp0s3:0

IPADDR=192.168.27.1  
NETMASK=255.255.255.0  
ONBOOT=yes  
NAME=enp0s3:0  
DEVICE=enp0s3:0

## Configuration du hosts

/etc/host

192.168.27.1 www.mysite.be

## Création des dossiers et des index.html

cd /var/www/html  
mkdir intranet  
mkdir beta

|  |  |
| --- | --- |
| /var/www/html/index.html  <html>  <head>  <title> Test du site web de base </title>  </head>  <body>  <h1>Site web de base. Ca marche !!! </h1>  </body>  </html | /var/www/html/intranet/index.html  <html>  <head>  <title> Test du site intranet</title>  </head>  <body>  <h1>Site intranet. Ca marche !!! </h1>  </body>  </html |
| /var/www/html/beta/index.html  <html>  <head>  <title> Test du site beta </title>  </head>  <body>  <h1>Site beta. Ca marche !!! </h1>  </body>  </html |  |

## Création des utilisateurs

|  |  |
| --- | --- |
| useradd jean | echo jean | passwd –stdin jean |
| useradd louis | echo louis | passwd –stdin louis |
| useradd tux | echo tux | passwd –stdin tux |
| useradd bill | echo bill | passwd –stdin bill |

## Création du fichier secure.txt

cd /var/www mkdir securite cd securite

htpasswd -c secure.txt tux (-c = crée le fichier)  
htpasswd -b secure.txt bill bill (-b = attribution du mot de passe depuis la ligne de commande)  
htpasswd -b secure.txt louis louis  
htpasswd -b secure.txt jean jean

## Création d'un fichier protection.conf

/etc/httpd/conf .d/protection.conf

<Directory /var/www/html/intranet>

Require ip 192.168.27

</Directory>

<Directory /var/www/html/beta>

AuthName "Accès au site beta"  
 AuthType Basic  
 AuthUserFile /var/www/securite/secure.txt  
 Require user tux bill

</Directory>

## Création du virtual.conf

/etc/httpd/conf.d/virtual.conf

<VirtualHost 192.168.27.1>

ServerName [www.mysite.be](http://www.mysite.be)  
 DocumentRoot /var/www/html

</VirtualHost>

## Testez vos configurations

lynx [www.mysite.be/intranet](http://www.mysite.be/intranet)  
 Si la machine est dans le bon range ip, on pourra se connecter.

lynx www.mysite.be/beta

Lors que la page s'affiche, il demande un utilisateur et un mot de passe.  
 Si c'est tux ou bill qui entre ses "coordonnées" ils auront accès à la "ressources".  
 Si c'est quelqu'un d'autre, l'accès sera refusé.

## Expliquez le codage Base64

<https://fr.wikipedia.org/wiki/Base64>

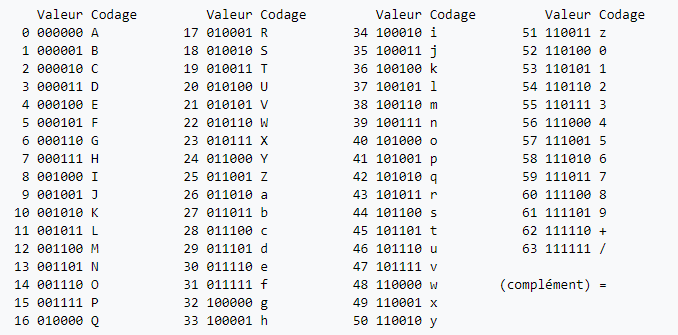
On commence par transformer les caractères en binaire  
t u x : t u x  
01110100 01110101 01111000 00111010 01110100 01110101 01111000

Ensuite, on les divise en "paquet" de 6. Le codage Base64 travail par 6bits.

011101 - 000111 - 010101 - 111000 - 001110 - 100111 - 010001 - 110101 - 011110 - 00

Puis, il suffit, grâce à la table de conversion, de les retransformer en caractères.

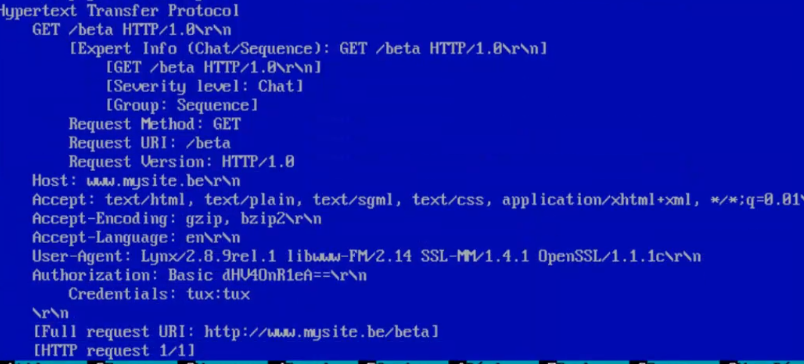
d H V 4 O n R 1 e A=



## Testez avec tshark que la méthode d'authentification 'Basic' n'est pas sécurisée.

Sur un premier terminal : tshark port 80 > sniff.txt  
Sur un 2eme terminal : lynx www.mysite.be/beta et introduire les coordonnées

En allant regarder dans sniff.txt



On peut constater à la ligne "Credentials" que le nom de l'utilisateur et son mot de passe son en clair.

## Testez d'autres outils permettant de (de)coder un message chiffre par la méthode Base64.

Coder un mdp en base64 : echo -n tux:tux | base64  
Décoder un mdp en base64 : echo dHV40nR1eA== | base64 -d

# Sécurisation d'un site par SSL

## Enoncé

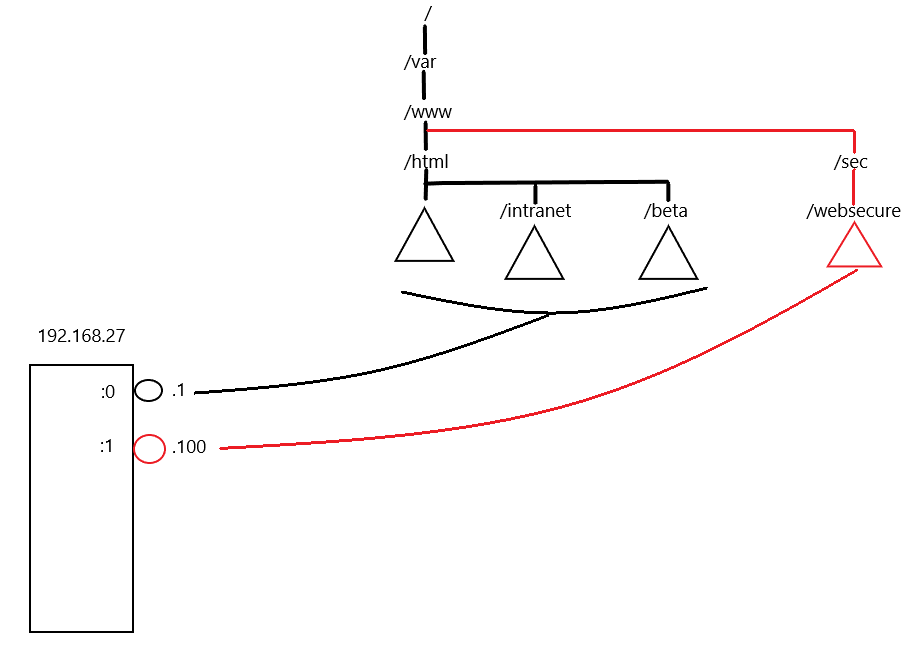
Continuez la configuration d'Apache pour que :

* La page d'accueil de www.mysite.be offre en plus la possibilité d'accéder à un secret via un lien "Cliquez ici pour voir le secret".
* Un clic sur ce lien nous redirige vers la page d'accueil de secure.mysite.be d'un hôte virtuel SSL héberge par Ip sur 192.168.27.100. Cette page sera enregistrée dans /var/www/html/sec/websecure et contiendra le secret.
  + Importez le certificat dans Firefox de façon à ne plus avoir à "Comprendre les risques" lors de l'accès au site SSL.
  + Tracez à l'aide d'un renifleur toute la conversation de [www.mysite.be](http://www.mysite.be) jusque secure.mysite.be.

Récupérer vh3 du TP Apache de Service Réseau.

* Les requetés http://vh3.mysite.be et <https://vh3.mysite.be> nous offrent, de manière sécurisée, la page d'accueil du site.
  + Gênerez un nouveau certificat auto-signe pour ce site
  + Les 2 requetés seront envoyés sur l'IP 192.168.27.2

## Situation



## Configuration de l'interface

/etc/sysconfig/network-scripts/ifcfg-enp0s3:1

IPADDR=192.168.27.100  
NETMASK=255.255.255.0  
ONBOOT=yes  
NAME=enp0s3:1  
DEVICE=enp0s3:1

## Configuration du hosts

/etc/host

192.168.27.1 [www.mysite.be](http://www.mysite.be)  
 192.168.27.100 secure.mysite.be

## Création des dossiers et des index.html

mkdir /var/www/sec/   
mkdir /var/www/sec/websecure  
mcedit /var/www/sec/websecure/index.html

|  |  |
| --- | --- |
| /var/www/html/index.html  <html>  <head>  <title> Test du site web de base </title>  </head>  <body>  <h1>Site web de base. Ca marche !!! </h1>  <a href="../sec/websecure/index.html">Cliquez ici pour aller sur le site sécurisé</a>  </body>  </html | /var/www/sec/websecure/index.html  <html>  <head>  <title> Test du site sécurisé</title>  </head>  <body>  <h1>Site sécurisé. Ca marche !!! </h1>  </body>  </html |

## SSL

### Etape 1 : installer openSSL et son module Apache

dnf install openssl mod\_ssl -y

### Etape 2 : création de la clé privée du serveur

cd /tmp  
openssl genrsa -out secure.mysite.be.key 2048  
cat secure.mysite.be.key

### Etape 3 : création du CSR (Certificate Signing Request)

openssl req -new -key secure.mysite.be.key -out secure.mysite.be.csr

*Remplir le formulaire*

cat secure.mysite.be.csr

### Etape 4 : création du certificat

cd /tmp  
openssl x509 -in secure.mysite.be.csr -out secure.mysite.be.crt -req -signkey secure.mysite.be.key -days 3650

### Etape 5 : copie des clés et des certificats au bon endroit

cd /tmp  
cp secure.mysite.be.crt /etc/pki/tls/certs  
cp secure.mysite.be.csr /etc/pki/tls/private  
cp secure.mysite.be.key /etc/pki/tls/private

## Modification du virtual.conf

/etc/httpd/conf.d/virtual.conf

<VirtualHost 192.168.27.100:443>

ServerName secure.mysite.be  
 DocumentRoot /var/www/sec/websecure

SSLEngine on  
 SSLCertificateFile /etc/pki/tls/certs/secure.mysite.be.crt  
 SSLCertificateKeyFile /etc/pki/tls/private/secure.mysite.be.key

</VirtualHost>

## Tester

lynx www.mysite.be

Cliquez sur le lien -> o (oui)  


## Importer le certificat dans firefox ou chrome

Mettre la vm en host only  
Importer le certificat

Terminal windows (hors machine):  
 scp [root@192.168.56.101:/etc/pki/tls/certs/secure.mysite.be.crt](mailto:root@192.168.56.101:/etc/pki/tls/certs/secure.mysite.be.crt) C:\Users\Pipoune\Desktop

Puis aller dans les paramètres de firefox ou chrome et ajouter le certificat.

## Redirection avec le site vh3 du TP Apache de service réseau

Soit on réutilise le certificat, soit on en crée un nouveau avec la même manipulation précédente.  
On reprend les configurations de vh3 et on implémente dans ce serveur.  
Ses fichiers se trouvent dans /var/www/vh/vh3.  
Créer l'interface enp0s3:2 et lui mettre l'adresse 192.168.27.2  
Dans le /etc/hosts ajouter : 192.168.27.2 vh3.mysite.be  
Virtualhost:

|  |  |
| --- | --- |
| <VirtualHost 192.168.27.2:80>  ServerName vh3.mysite.be  DocumentRoot /var/www/vh/vh3  **Redirect permanent / https://**vh3.mysite.be  </VirtualHost> | <VirtualHost 192.168.27.2:443>  ServerName vh3.mysite.be  DocumentRoot /var/www/vh/vh3  SSLEngine on  SSLCertificateFile /etc/pki/tls/certs/secure.mysite.be.crt  SSLCertificateKeyFile /etc/pki/tls/private/secure.mysite.be.key  </VirtualHost> |