



EC2LT/Master 1/M.DIOKH

(Remplir et rendre ce document)

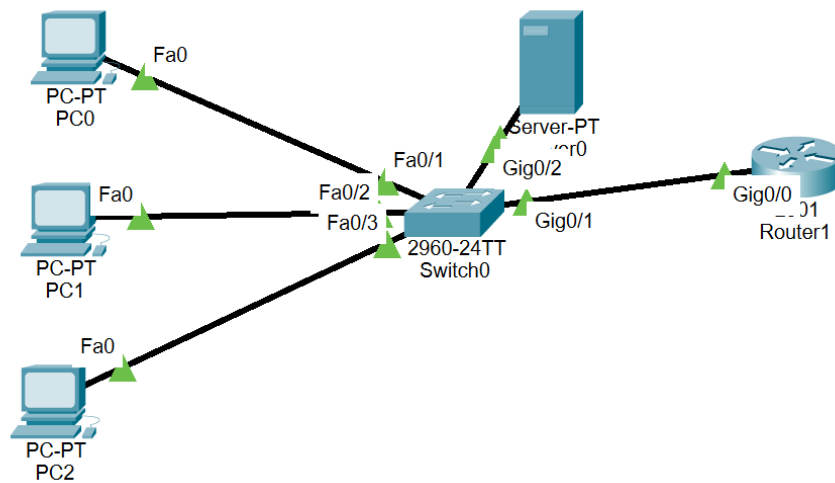
NB : Les **captures d'écran** doivent contenir le prompt ou la barre de votre terminal :

```
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$  
sysadmin@srv:~$ cal  
      Juin 2020  
di lu ma me je ve sa  
  1  2  3  4  5  6  
  7  8  9 10 11 12 13  
14 15 16 17 18 19 20  
21 22 23 24 25 26 27  
28 29 30  
  
sysadmin@srv:~$ _
```

NOM : Diallo

Prénom : Amadou Bory

1 DHCP Snooping



Sur le switch, configurer le port de confiance sur lequel doit être connecté le serveur DHCP autorisé (le routeur Router1).

Activer les événements du DHCP Snooping (debug ip dhcp snooping event et debug ip dhcp snooping packet).

Selon mon archi, voici le voisinage autour du switch

```
switch(config)#do sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce   Holdtme    Capability Platform Port ID
Server-PT      Fas 1/0         130        R S I     3745     Fas 0/0
Router-1       Fas 1/1         168        R S I     3745     Fas 0/0
switch(config)#
```

1.1 Montrer les captures d'écran de la configuration.

.....

1.2 Montrer que le serveur DHCP Server-PT ne donne d'adresse aux machines.

.....

1.3 Montrer la capture des événements sur le switch.

.....

2 Web : Apache2

NB : Installer l'application **curl**

2.1 Désactiver l'affichage de la version du Serveur et la signature

Capture d'écran de la configuration :

```
# apt install apache2 curl -y
```

```
# nano /etc/apache2/conf-available/security.conf
```

```
# service apache2 restart
```

```
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#ServerSignature Off
ServerSignature Off
```

Capture d'écran du résultat de la commande : **curl -I localhost**

```

root@bory-diallo:/etc/apache2# grep -r ServerToken
conf-available/security.conf:# ServerTokens
conf-available/security.conf:#ServerTokens Minimal
conf-available/security.conf:ServerTokens Prod
conf-available/security.conf:#ServerTokens Full
root@bory-diallo:/etc/apache2# curl -I localhost
HTTP/1.1 200 OK
Date: Tue, 13 Dec 2022 18:34:30 GMT
Server: Apache
Last-Modified: Fri, 21 Oct 2022 00:55:39 GMT
ETag: "2aa6-5eb80e68e6ab1"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html

root@bory-diallo:/etc/apache2#

```

Nous ne voyons ni la version de Apache, ni le système d'exploitation sur lequel tourne le serveur !

2.2 Site virtuel par nom : Créer un site virtuel pour le nom `www.master.sn`. **`www.master.sn` doit afficher le message "Bienvenue sur le site de Master"**

Capture d'écran de la configuration :

```
# nano /etc/apache2/sites-available/examen.conf
```

```

root@bory-diallo:~# nano /etc/apache2/sites-available/examen.conf
root@bory-diallo:~# cat /etc/apache2/sites-available/examen.conf
<VirtualHost *:80>
    DocumentRoot    /var/www/html/examen/
    ServerName       www.master.sn
    DirectoryIndex   index.html
</VirtualHost>
root@bory-diallo:~# a2ensite examen.conf
Enabling site examen.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@bory-diallo:~# service apache2 restart
root@bory-diallo:~#

```

```
# mkdir /var/www/html/examen/
```

```
# cd /var/www/html/examen/
```

```
# nano index.html
```

```

root@bory-diallo:~# cat /var/www/html/examen/index.html
<html>
    <p>Bienvenue sur le site de Master</p>
</html>
root@bory-diallo:~#

```

Capture d'écran du résultat de la commande : `curl www.master.sn`

```
root@bory-diallo:~# cat /etc/hosts
127.0.0.1      localhost    www.master.sn
127.0.1.1      bory-diallo

192.168.2.118  www.master.sn
# The following lines are desirable for IPv6 capable hosts
::1           ip6-localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
root@bory-diallo:~# curl www.master.sn
<html>
  <p>Bienvenue sur le site de Master</p>
</html>
root@bory-diallo:~#
```

2.3 Mettre en place une PKI :

(Pays : SN ; Localité : Sénégal ; ville : Dakar ; Organisation : EC2LT ; Unité Organisationnelle : Master)

- Délivrer le certificat du CA pour une durée de deux ans ;
- Délivrer un certificat pour votre serveur web pour une durée de 180 jours ;
- Délivrer un certificat client qui porte votre prénom pour une durée de 90 jours ;
- Générer une liste de révocation de certificats.

Voici les prérequis pour cette partie

```
# mkdir private
# mkdir newcerts
# mkdir cacerts
# mkdir demoCA
# touch demoCA/index.txt
# echo "01" > demoCA/serial
# mkdir crl
# echo 01 > demoCA/crlnumber
```

Délivrons le certificat du CA pour une durée de deux ans

```
bory@bory-diallo:~/ssl$ openssl req -x509 -nodes -newkey rsa:2048 -days 730 -keyout private/caKey.pem -out cacerts/caCert.pem -subj "/C=SN/ST=Senegal/L=Dakar/O=EC2LT/OU=Master"
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to 'private/caKey.pem'
-----
bory@bory-diallo:~/ssl$
```

Un certificat pour le serveur

```
bory@bory-diallo:~/ssl$ openssl req -nodes -newkey rsa:2048 -days 180 -keyout private/serverKey.pem -out private/serverCert.csr -subj "/C=SN/ST=Senegal/L=Dakar/O=EC2LT/OU=Master/CN=www.master.sn"
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to 'private/serverKey.pem'
-----
bory@bory-diallo:~/ssl$
```

Délivrer un certificat client qui porte votre prénom pour une durée de 90 jours ;

```
bory@bory-diallo:~/ssl$ openssl req -nodes -newkey rsa:2048 -days 90 -keyout private/bory.pem -out private/bory.csr -subj "/C=SN/ST=Senegal/L=Dakar/O=EC2LT/OU=Master/CN=bory"
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to 'private/bory.pem'
-----
bory@bory-diallo:~/ssl$
```

Générons une liste de révocation de certificat

```
bory@bory-diallo:~/ssl$ openssl ca -cert cacerts/caCert.pem -keyfile private/caKey.pem -gencrl -crl days 15 -out crl/ca.crl
Using configuration from /usr/lib/ssl/openssl.cnf
bory@bory-diallo:~/ssl$
```

Le voici d'ailleurs

```

bory@bory-diallo:~/ssl$ openssl crl -in crl/ca.crl -text -noout
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=SN, ST=Senegal, L=Dakar, O=EC2LT, OU=Master
  Last Update: Dec 13 19:40:35 2022 GMT
  Next Update: Dec 28 19:40:35 2022 GMT
  CRL extensions:
    X509v3 CRL Number:
      5
No Revoked Certificates.
  Signature Algorithm: sha256WithRSAEncryption
    90:8f:79:9c:7a:71:ec:07:ae:17:a0:1d:76:12:aa:68:5a:eb:
    f7:e6:6b:e5:82:34:2c:c6:f0:4b:2b:f0:92:cc:e9:ef:49:4d:
    70:c3:83:69:da:e9:1a:6f:74:a4:b0:82:cd:82:7a:60:ae:e9:
    31:b1:10:77:07:c1:d3:e9:d0:61:53:08:f2:9f:3e:15:f1:be:
    e3:4e:2d:86:72:fd:32:26:2f:b6:79:f9:81:e6:fc:39:aa:0f:
    a6:f9:00:a8:47:29:e0:03:c9:24:a0:b5:17:45:b7:40:9c:c9:
    e8:86:82:14:aa:79:56:ba:9e:d0:66:e3:01:75:22:dc:16:cd:
    72:60:67:1b:e7:49:f4:68:6b:f2:04:fd:2f:7c:12:d3:f7:88:
    8a:2d:f9:45:6c:b4:fd:92:f3:85:75:39:e4:cb:78:cd:6b:3e:
    76:6d:71:02:2d:14:36:f2:a1:fb:d4:f6:ea:81:1d:14:cb:2d:
    12:c5:f6:be:08:e9:68:73:6a:23:5a:17:d0:6f:36:56:1a:88:
    85:ad:c0:fa:6d:ec:f0:1f:37:e9:6e:2b:f3:7e:86:8d:5a:77:
    46:b7:f5:5d:1e:1e:b2:90:4f:da:f1:8d:8e:7f:97:32:43:a2:
    64:e5:91:af:8c:c7:e4:04:2d:1a:96:33:b6:aa:95:f1:c4:24:
    a4:c9:98:47
bory@bory-diallo:~/ssl$

```

Avant toute chose, il faut tout d'abord auto-signé les différents certificats

Signature du certificat du serveur

```

root@bory-diallo:~/ssl# openssl ca -in private/serverCert.csr -days 180 -out newcerts/server.crt -notext -cert
cacerts/caCert.pem -keyfile private/caKey.pem -outdir newcerts/
Using configuration from /usr/lib/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Dec 13 20:01:32 2022 GMT
    Not After : Jun 11 20:01:32 2023 GMT
  Subject:
    countryName           = SN
    stateOrProvinceName   = Senegal
    organizationName       = EC2LT
    organizationalUnitName = Master
    commonName             = www.master.sn
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      65:0A:66:1A:CC:68:D5:08:06:E5:A1:85:C3:96:6E:B2:17:48:CC
    X509v3 Authority Key Identifier:
      keyid:B6:BE:C4:E5:B8:2D:FD:5C:75:D0:61:6E:92:36:E2:14:6E:5B:C8:55

Certificate is to be certified until Jun 11 20:01:32 2023 GMT (180 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@bory-diallo:~/ssl#

```

Pour le user bory

```
bory@bory-diallo:~/ssl$
bory@bory-diallo:~/ssl$ openssl ca -in private/bory.csr -days 90 -out newcerts/bory.crt -notext -cert cacerts/
caCert.pem -keyfile private/caKey.pem -outdir newcerts/
Using configuration from /usr/lib/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 2 (0x2)
  Validity
    Not Before: Dec 13 20:09:46 2022 GMT
    Not After : Mar 13 20:09:46 2023 GMT
  Subject:
    countryName           = SN
    stateOrProvinceName   = Senegal
    organizationName      = EC2LT
    organizationalUnitName = Master
    commonName            = bory
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      CE:0A:98:68:D3:18:6F:BB:6A:14:01:B3:7F:17:65:BD:D2:69:31:E5
    X509v3 Authority Key Identifier:
      keyid:B6:BE:C4:E5:B8:2D:FD:5C:75:D0:61:6E:92:36:E2:14:6E:5B:C8:55

Certificate is to be certified until Mar 13 20:09:46 2023 GMT (90 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
bory@bory-diallo:~/ssl$
```

2.4 Configurer votre serveur web pour qu'il utilise le protocole HTTPS avec le certificat délivré.

Capture d'écran

Les configs se trouvent plus bas !

2.5 Le client doit présenter un certificat valide pour accéder à votre site.


```

<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        ServerName      www.master.sn
        DocumentRoot    /var/www/html/examen

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
        SSLEngine on

```

La suite du fichier

```

#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile    /home/bory/ssl/private/serverKey.pem
SSLCertificateKeyFile /home/bory/ssl/private/serverCert.csr

```

À la fin nous il y a la balise fermante : </VirtualHost>

aenmod ssl

2.6 Révoquer le certificat d'un client et mettre à jour la liste de révocation de certificats.

Capture d'écran

```

root@bory-diallo:~/ssl# openssl ca -cert cacerts/caCert.pem -keyfile private/caKey.pem -revoke newcerts/bory.c
rt
Using configuration from /usr/lib/ssl/openssl.cnf
Revoking Certificate 02.
Data Base Updated

```

Mise à jour

```

root@bory-diallo:~/ssl# openssl ca -cert cacerts/caCert.pem -keyfile private/caKey.pem -gencrl -crl days 15 -ou
t crl/ca.crl
Using configuration from /usr/lib/ssl/openssl.cnf
root@bory-diallo:~/ssl#

```

Voici l'état de la lise de revocation

```
root@bory-diallo:~/ssl# openssl crl -in crl/ca.crl -text -noout
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=SN, ST=Senegal, L=Dakar, O=EC2LT, OU=Master
  Last Update: Dec 13 20:28:06 2022 GMT
  Next Update: Dec 28 20:28:06 2022 GMT
  CRL extensions:
    X509v3 CRL Number:
      7
Revoked Certificates:
  Serial Number: 02
  Revocation Date: Dec 13 20:25:19 2022 GMT
  Signature Algorithm: sha256WithRSAEncryption
    9c:62:97:f3:e4:16:0e:32:a5:2b:61:71:bd:f9:f8:40:c1:98:
    46:ae:31:c7:d3:97:44:dc:90:98:34:82:de:3e:6d:06:f7:3e:
    87:37:31:3b:0e:51:f4:4e:63:9f:8e:48:64:7e:8f:d7:06:98:
    c7:1d:3b:93:73:2c:46:e5:73:17:b2:5f:88:27:b8:af:5f:41:
    44:35:fe:7d:81:0f:f9:c9:fb:0c:5b:f9:2b:c5:b0:9b:4c:f7:
    f4:19:c3:67:76:37:a4:49:36:d5:d7:1b:72:db:91:20:b7:3c:
    79:4b:8f:3e:87:37:a3:9e:bd:60:4d:ea:51:1d:87:ba:41:51:
    bb:d2:3c:31:5b:5c:ad:6f:1f:68:76:89:c7:ce:16:7b:18:a3:
    ec:00:ec:fb:64:e1:93:de:37:84:9e:77:ba:1c:1e:d4:86:92:
    84:b7:e8:cd:47:ac:b5:bb:05:7c:fc:37:f5:6a:68:07:83:c5:
    2e:ea:12:09:7f:82:82:b9:b4:2b:99:a8:42:81:25:2a:ac:29:
    4c:dd:62:c0:09:41:b3:5c:c5:a4:cd:40:8d:bb:f5:c9:66:5a:
    9a:de:03:72:e1:30:54:3f:e1:ef:97:6d:b9:3d:e8:4e:ad:5d:
    fb:0a:06:03:40:49:96:7b:62:36:30:f4:01:14:0f:a4:a8:d7:
    4b:29:ee:ee
root@bory-diallo:~/ssl#
```

2.7 SSL: Faire la redirection <http://www.master.sn> vers <https://www.master.sn>

Capture d'écran de la configuration : redirection

nano /etc/apache2/sites-available/examen.conf

```
root@bory-diallo:/etc/apache2/sites-available# cat examen.conf
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName      www.master.sn
    DocumentRoot    /var/www/html/examen
    DirectoryIndex  index.html
    redirect permanent / https://www.master.sn
    ErrorLog ${APACHE_LOG_DIR}/error.log
    SSLEngine on
    SSLCertificateFile      /home/bory/ssl/newcerts/server.crt
    SSLCertificateKeyFile   /home/bory/ssl/private/serverKey.pem
    SSLCACertificateFile    /home/bory/ssl/cacerts/caCert.pem
    SSLVerifyClient require
    SSLVerifyDepth  10
</VirtualHost>
root@bory-diallo:/etc/apache2/sites-available#
```

service apache2 reload

Capture d'écran de la configuration : SSL

```
# cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/examen.conf
```

```
# nano /etc/apache2/sites-available/examen.conf
```

```
root@bory-diallo:/etc/apache2/sites-available# cat examen.conf
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName      www.master.sn
    DocumentRoot    /var/www/html/examen
    DirectoryIndex  index.html
    redirect permanent / https://www.master.sn
    ErrorLog ${APACHE_LOG_DIR}/error.log
    SSLEngine on
    SSLCertificateFile      /home/bory/ssl/newcerts/server.crt
    SSLCertificateKeyFile   /home/bory/ssl/private/serverKey.pem
    SSLCACertificateFile    /home/bory/ssl/cacerts/caCert.pem
    SSLVerifyClient require
    SSLVerifyDepth 10
</VirtualHost>
root@bory-diallo:/etc/apache2/sites-available#
```

Activer le site et redémarrer apache

```
root@bory-diallo:/etc/apache2/sites-available# a2ensite examen.conf
Enabling site examen.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@bory-diallo:/etc/apache2/sites-available# service apache2 restart

root@bory-diallo:/etc/apache2/sites-available#
root@bory-diallo:/etc/apache2/sites-available#
```

Capture d'écran du résultat de la commande : curl www.master.sn

```
root@bory-diallo:/etc/apache2/sites-available# !curl
curl www.master.sn

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2016-11-16
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
```

2.8 Limiter l'accès par SSH à votre serveur

Désactiver la connexion SSH de l'utilisateur root

Capture de la configuration :

```
# nano /etc/ssh/sshd_config
```

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

service ssh restart

Définir une liste de deux utilisateurs autorisés à se connecter via SSH

Capture de la configuration :

```
# PermitTTY no
# ForceCommand cvs server

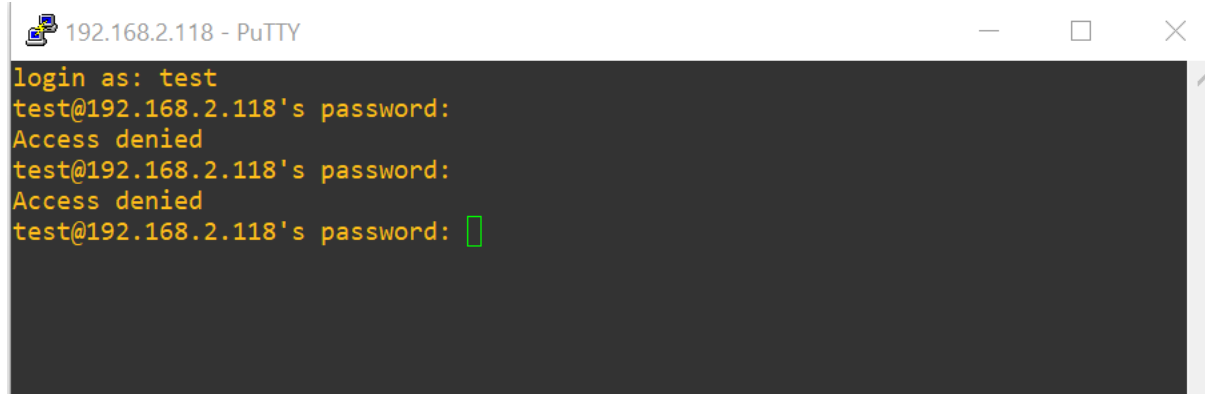
AllowUsers toto bory
```

Capture des tests:

Pour les tests, notre serveur a comme IP 192.168.2.118

Nous allons tenter de nous connecter avec le user test qui est créé

```
root@bory-diallo:~# grep -r test /etc/passwd
test:x:1001:1001:,,,:/home/test:/bin/bash
root@bory-diallo:~#
```



2.9 Configuration de fail2ban

Installer afin d'éviter les attaques de types Bruteforce ; Bloquer pendant 1 semaine toute machine ayant effectuée 3 requêtes d'authentification échouée sur une période de 5 minutes.

Capture de la configuration :

```
# apt install fail2ban -y
```

Configuration

```
# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

```
# nano /etc/fail2ban/jail.local
```

Il existe plusieurs sections en fonction des services, mais dans notre cas c'est la section ssh qui nous interesse.

```
[sshd]
```

```
port = ssh
```

```
logpath = %(sshd_log)s
```

```
backend = %(sshd_backend)s
```

Dans la section Default pour définir les actions et règles qui seront appliquées en cas de tentative d'attaque par bruteforce

```
[DEFAULT]
```

```
ignoreip = 127.0.0.1/8
```

```
bantime = 604800
```

```
findtime = 300
```

```
maxretry = 3
```

```
backend = auto
```

```
usedns = warn
```

```
logencoding = auto
```

```
enabled = false
```

```
protocol = tcp
```

```
chain = <known/chain>
```

```
port = 0:65535
```

```
banaction = iptables-multiport
```

```
banaction_allports = iptables-allports
```

Après ces config, redémarrer le service et regarder son statut

```
# service fail2ban restart
```

```

root@bory-diallo:~# fail2ban-client restart sshd
OK
root@bory-diallo:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     0
|   `-- File list:      /var/log/auth.log
`- Actions
    |- Currently banned: 0
    |- Total banned:     0
    `-- Banned IP list:
root@bory-diallo:~#

```

Capture des tests avec SSH

Nous avons défini un essai maximum de 3 tentatives, faisons le test avec une machine du réseau

```

bory@sysAdmin: ~
bory@sysAdmin:~$ ssh bory@192.168.0.106
bory@192.168.0.106's password:
Permission denied, please try again.
bory@192.168.0.106's password:
.caa
^C
bory@sysAdmin:~$ ssh bory@192.168.0.106
ssh: connect to host 192.168.0.106 port 22: Connection refused
bory@sysAdmin:~$

```

Nous avons saisis trois fois le mauvais mot de passe, teston à nouveau à nous connecter

```

bory@sysAdmin: ~
bory@sysAdmin:~$ ssh bory@192.168.0.106
ssh: connect to host 192.168.0.106 port 22: Connection refused
bory@sysAdmin:~$

```

On peut même voir le statut et la liste des adresses IP bloquées

```
root@bory-diallo: ~  
root@bory-diallo:~# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
|   |- Currently failed: 1  
|   |- Total failed: 7  
|   - File list: /var/log/auth.log  
- Actions  
|   |- Currently banned: 1  
|   |- Total banned: 2  
|   - Banned IP list: 192.168.0.107  
root@bory-diallo:~#
```

Capture des logs de Fail2ban

```
root@bory-diallo: ~  
root@bory-diallo:~# tail -f /var/log/fail2ban.log  
2023-01-17 10:43:48,297 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:43:46  
2023-01-17 10:43:48,297 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:43:48  
2023-01-17 10:44:02,422 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:44:02  
2023-01-17 10:44:02,991 fail2ban.actions [21752]: NOTICE [sshd] Ban 192.168.0.107  
2023-01-17 10:44:05,131 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:44:04  
2023-01-17 10:44:28,912 fail2ban.actions [21752]: NOTICE [sshd] Unban 192.168.0.107  
2023-01-17 10:44:36,063 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:44:36  
2023-01-17 10:44:38,136 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:44:38  
2023-01-17 10:44:38,298 fail2ban.actions [21752]: NOTICE [sshd] Ban 192.168.0.107  
2023-01-17 10:44:40,845 fail2ban.filter [21752]: INFO [sshd] Found 192.168.0.107 - 2023-  
01-17 10:44:40  
^
```

Capture de résultat de la commande iptables -nL

```
root@bory-diallo: ~  
root@bory-diallo:~# iptables -nL  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
f2b-sshd tcp -- 0.0.0.0/0 0.0.0.0/0 multiport dports 22  
  
Chain FORWARD (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
  
Chain f2b-sshd (1 references)  
target prot opt source destination  
REJECT all -- 192.168.0.107 0.0.0.0/0 reject-with icmp-port-unreachable  
RETURN all -- 0.0.0.0/0 0.0.0.0/0  
root@bory-diallo:~#
```