SP2 — Mise en place de Nextcloud avec authentification OpenLDAP

Présentation du projet

Ce projet consiste à déployer une instance **Nextcloud** accessible via le nom de domaine `nextcloud.portfolio.org`, avec une authentification centralisée via un annuaire **OpenLDAP**, une base de données **MariaDB** dédiée, et un chiffrement **HTTPS** par certificat auto-signé.

Plan d'action

Étape	Description
1. DNS	Créer l'enregistrement A : `nextcloud.portfolio.org` → `10.31.202.80`
2. OpenLDAP	Créer un CT Debian sur Proxmox + installer/configurer OpenLDAP + créer les utilisateurs
3. MariaDB	Créer un CT Debian sur Proxmox + installer MariaDB + créer la base Nextcloud
4. Serveur Web	Installer Nextcloud + PHP + configurer Apache + virtualhost `nextcloud.portfolio.org`
5. Liaison Nextcloud ↔ OpenLDAP	Configurer le plugin LDAP dans Nextcloud
6. Pare-feu	Ouvrir les flux nécessaires entre VLANs

Notions sur OpenLDAP

OpenLDAP est un annuaire très structuré. Tout est organisé en arbre appelé le **DIT** (Directory Information Tree).

Chaque entrée dans l'arbre a une adresse unique appelée **DN** (Distinguished Name).

Exemple de structure :

```
dc=portfolio,dc=org        ← racine
├── ou=users               ← dossier utilisateurs
│   ├── uid=jdupont        ← un utilisateur
│   └── uid=mmartin        ← un autre
└── ou=groups              ← dossier groupes
```

Les objectClass

Chaque entrée doit avoir un **objectClass** qui définit ce qu'elle est et quels attributs elle peut/doit avoir. C'est comme un modèle obligatoire.

objectClass	Sert à
organizationalUnit	Créer un dossier/OU
inetOrgPerson	Créer un utilisateur
posixGroup	Créer un groupe

Étape 1 — Configuration DNS

1.1 Ajout de la zone portfolio.org

Dans le fichier `/etc/bind/named.conf.local`, ajout de la zone pour le domaine Nextcloud :

```
zone "portfolio.org" IN {
    type master;
    file "/etc/bind/db.portfolio.org";
    allow-transfer { 10.31.200.54; };
};
```

1.2 Fichier de zone db.portfolio.org

Création du fichier de configuration avec les enregistrements DNS :

```
$TTL 604800
@   IN  SOA ns1-pub.portfolio.org. admin.portfolio.org. (
            2026032702  ; Serial
            3600        ; Refresh
            600         ; Retry
            2419200     ; Expire
            604800 )    ; Minimum TTL

@       IN  NS  ns1-pub.portfolio.org.
@       IN  NS  ns2-pub.portfolio.org.

@       IN  A   10.31.202.80

ns1-pub     IN  A   10.31.200.53
ns2-pub     IN  A   10.31.200.54

nextcloud   IN  A   10.31.202.80
ldap        IN  A   10.31.204.87
```

1.3 Vérification et redémarrage

```
named-checkzone portfolio.org /etc/bind/zones/db.portfolio.org
systemctl restart bind9
```

Test de résolution depuis une machine cliente :

```
nslookup ldap.portfolio.org 10.31.200.53
# Résultat attendu : Address: 10.31.204.87
```

Étape 2 — Conteneur OpenLDAP

2.1 Créer le CT sur Proxmox

Création d'un conteneur Proxmox (CT Debian) avec l'IP `10.31.204.87/23` (VLAN SRV — serveurs internes).

2.2 Installer OpenLDAP

Mise à jour de la machine :

```
apt update && apt upgrade -y
```

Installation de slapd et des utilitaires LDAP :

```
apt install slapd ldap-utils -y
```

Un mot de passe administrateur est demandé à l'installation — choisir un mot de passe robuste.

2.3 Reconfigurer slapd

```
dpkg-reconfigure slapd
```

Répondre aux questions comme suit :

Question	**Réponse**
Omettre la configuration ?	**Non**
Nom DNS	**portfolio.org**
Nom de l'organisation	**portfolio**
Mot de passe admin	*(votre mot de passe)*
Supprimer la BDD si purge ?	**Non**
Déplacer l'ancienne BDD ?	**Oui**

2.4 Vérification avec slapcat

```
slapcat
```

Le résultat doit afficher l'entrée racine `dc=portfolio,dc=org`.

Étape 3 — Structure LDAP (OUs + utilisateurs)

3.1 Créer les unités organisationnelles

Les OU (Organizational Units) fonctionnent comme des dossiers dans l'annuaire. On crée ici `users` et `groups`.

Création du fichier LDIF :

```
nano /etc/ldap/structure.ldif
```

Contenu :

```
dn: ou=users,dc=portfolio,dc=org
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=portfolio,dc=org
objectClass: organizationalUnit
ou: groups
```

Application :

```
ldapadd -x -D "cn=admin,dc=portfolio,dc=org" -W -f /etc/ldap/structure.ldif
```

> Le mot de passe administrateur LDAP est demandé.

3.2 Créer un utilisateur

Création du fichier LDIF utilisateur :

```
nano /etc/ldap/utilisateur.ldif
```

Contenu :

```
dn: uid=jdupont,ou=users,dc=portfolio,dc=org
objectClass: inetOrgPerson
cn: Jean Dupont
sn: Dupont
uid: jdupont
mail: jdupont@portfolio.org
userPassword: {SSHA}MotDePasseHashé
```

Génération du mot de passe haché avec slappasswd :

```
slappasswd
```

Copier le hash généré (format {SSHA}…) dans le champ userPassword du fichier LDIF, puis appliquer :

```
ldapadd -x -D "cn=admin,dc=portfolio,dc=org" -W -f
/etc/ldap/utilisateur.ldif
```

Vérification :

```
ldapsearch -x -b "dc=portfolio,dc=org" "(uid=jdupont)"
```

Étape 4 — Conteneur MariaDB

IP du conteneur BDD : 10.31.204.34 (privdb2)

4.1 Créer la base de données Nextcloud

Connexion à MariaDB :

```
mysql -u root -p
```

Création de la base et de l'utilisateur :

```
CREATE DATABASE nextcloud CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE USER 'nextcloud'@'10.31.202.80' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'10.31.202.80';
FLUSH PRIVILEGES;
EXIT;
```

4.2 Autoriser les connexions distantes

```
nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

Modifier la ligne :

```
bind-address = 0.0.0.0
```

Redémarrage du service :

```
systemctl restart mariadb
```

4.3 Test de connexion distante

Depuis le serveur web :

```
apt install mariadb-client -y
mysql -h 10.31.204.34 -u nextcloud -p
```

La commande `SHOW DATABASES;` doit afficher la base `nextcloud`.

Étape 5 — Installation de Nextcloud

Serveur web : `10.31.202.80`

5.1 Installer les dépendances

```
apt update && apt upgrade -y
apt install apache2 php php-gd php-json php-mysql php-curl php-mbstring \
    php-intl php-imagick php-xml php-zip php-ldap unzip wget -y
```

5.2 Télécharger et déployer Nextcloud

```
cd /tmp
wget https://download.nextcloud.com/server/releases/latest.zip
unzip latest.zip
mv nextcloud /var/www/
chown -R www-data:www-data /var/www/nextcloud
chmod -R 755 /var/www/nextcloud
```

5.3 Configurer le VirtualHost Apache

```
nano /etc/apache2/sites-available/nextcloud.conf
```

Contenu :

```
<VirtualHost *:80>
    ServerName nextcloud.portfolio.org
    DocumentRoot /var/www/nextcloud

    <Directory /var/www/nextcloud>
        AllowOverride All
        Require all granted
        Options FollowSymLinks MultiViews
    </Directory>
```

```
    ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
    CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
</VirtualHost>
```

Activation du site et des modules nécessaires :

```
a2ensite nextcloud.conf
a2enmod rewrite headers env dir mime
systemctl restart apache2
```

Nextcloud est maintenant accessible à l'adresse : http://nextcloud.portfolio.org

5.4 Flux à autoriser entre VLANs

Source	Destination	Port	Protocole	Raison
Clients (tous VLANs)	10.31.202.80	80 / 443	TCP	Accès Nextcloud HTTP/HTTPS
10.31.202.80	10.31.204.34	3306	TCP	Nextcloud → MariaDB
10.31.202.80	10.31.204.87	389	TCP	Nextcloud → OpenLDAP
Tous les CTs	10.31.200.53	53	TCP/UDP	Résolution DNS
Admin	10.31.192.1	8006	TCP	Interface Proxmox

Étape 6 — Intégration OpenLDAP dans Nextcloud

6.1 Activer le plugin LDAP

Dans l'interface Nextcloud :

1. Aller dans **Profil → Applications → Vos applications**
2. Activer **“LDAP user and group backend”**

6.2 Configurer la connexion au serveur LDAP

Aller dans **Profil → Paramètres d'administration → Intégration LDAP/AD**, puis renseigner :

Champ	Valeur
Hôte	`10.31.204.87`
Port	389
Utilisateur DN	`cn=admin,dc=portfolio,dc=org`
Mot de passe	*(mot de passe admin LDAP)*
DN de base	`dc=portfolio,dc=org`

Cliquer sur **“Tester la configuration”** → doit afficher : *Configuration valide, connexion établie !*

6.3 Configurer les attributs de connexion

Dans l'onglet **“Attributs de connexion”** :

1. Cocher **Nom d'utilisateur LDAP/AD**
2. Filtre LDAP : `(&(objectclass=inetOrgPerson)(uid=%uid))`
3. Tester avec le login `jdupont` → doit afficher : *Configuration valide, connexion établie !*

6.4 Dépannage — mot de passe manquant

Si la connexion avec `jdupont` échoue sur Nextcloud, vérifier d'abord que l'utilisateur existe dans l'annuaire :

```
ldapsearch -x -b "ou=users,dc=portfolio,dc=org" "(uid=jdupont)"
```

Si l'utilisateur est bien présent mais sans mot de passe défini, le définir avec :

```
ldappasswd -x -D "cn=admin,dc=portfolio,dc=org" -W -S \
    "uid=jdupont,ou=users,dc=portfolio,dc=org"
```

> Le nouveau mot de passe utilisateur et le mot de passe admin LDAP sont demandés.

Retenter ensuite la connexion sur Nextcloud avec le nouveau mot de passe.

Étape 7 — HTTPS avec certificat auto-signé

Afin de garantir la confidentialité et l'intégrité des données, on met en place le chiffrement SSL/TLS via HTTPS. Un certificat auto-signé est utilisé car les services sont internes.

7.1 Générer le certificat

Sur le serveur web `10.31.202.80` :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
    -keyout /etc/ssl/private/nextcloud.key \
    -out /etc/ssl/certs/nextcloud.crt
```

Renseigner les informations du certificat :

Champ	Valeur
Country Name	FR
State or Province	`Nouvelle Aquitaine`
Locality	`Limoges`
Organization	`portfolio`

Champ	Valeur
Common Name	nextcloud.portfolio.org

7.2 Activer le module SSL Apache

```
a2enmod ssl
```

7.3 Modifier le VirtualHost

```
nano /etc/apache2/sites-available/nextcloud.conf
```

Contenu final (redirection HTTP → HTTPS + VirtualHost 443) :

```
<VirtualHost *:80>
    ServerName nextcloud.portfolio.org
    Redirect permanent / https://nextcloud.portfolio.org/
</VirtualHost>

<VirtualHost *:443>
    ServerName nextcloud.portfolio.org
    DocumentRoot /var/www/nextcloud

    SSLEngine on
    SSLCertificateFile    /etc/ssl/certs/nextcloud.crt
    SSLCertificateKeyFile /etc/ssl/private/nextcloud.key

    <Directory /var/www/nextcloud>
        AllowOverride All
        Require all granted
        Options FollowSymLinks MultiViews
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
    CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
</VirtualHost>
```

Redémarrage d'Apache :

```
systemctl restart apache2
```

7.4 Mettre à jour la configuration Nextcloud

```
nano /var/www/nextcloud/config/config.php
```

Vérifier que `nextcloud.portfolio.org` est bien présent dans `trusted_domains`, puis ajouter :

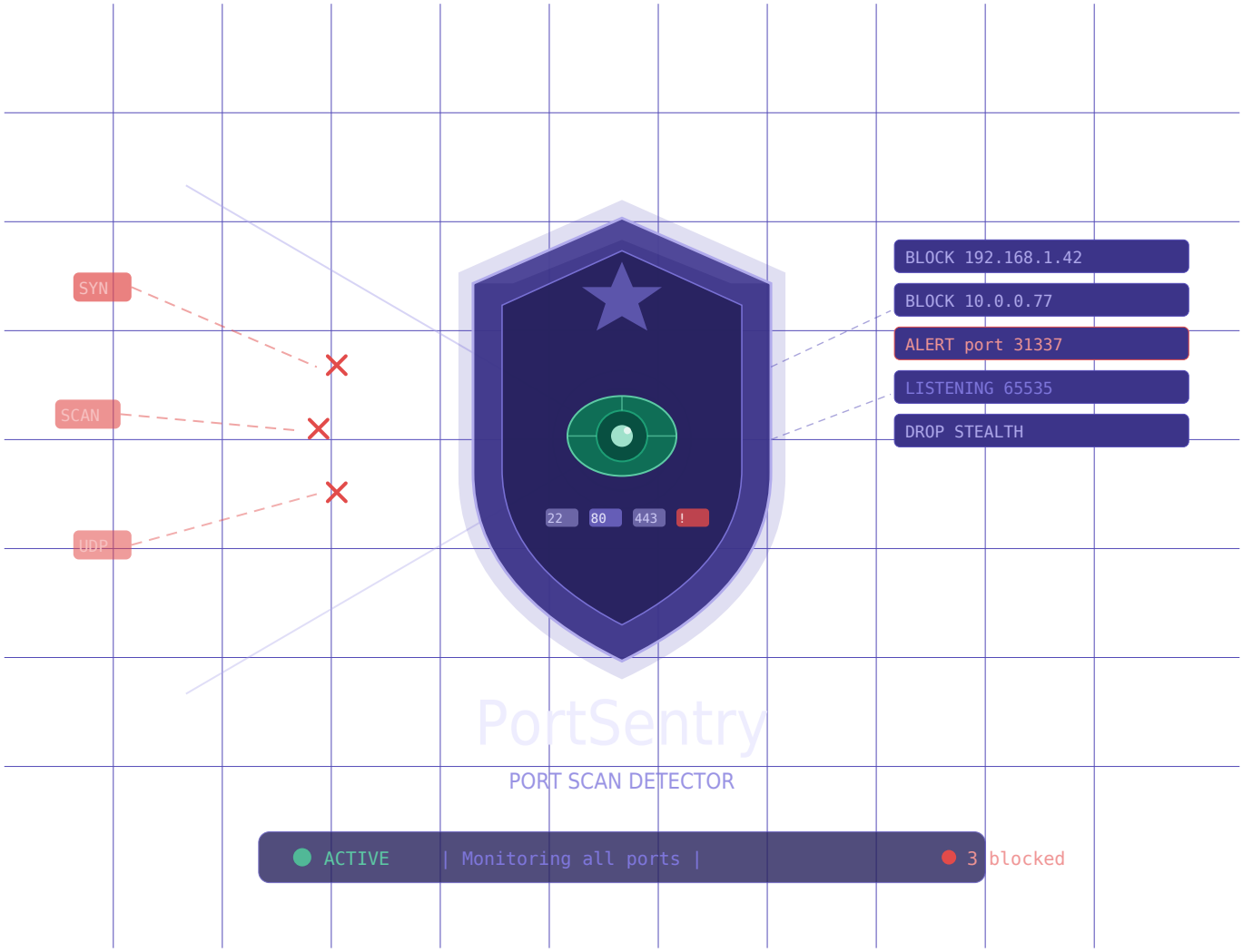
```
'overwrite.cli.url' => 'https://nextcloud.portfolio.org',
```

```
'forcessl' => true,
```

> Ces deux directives forcent l'utilisation de HTTPS et définissent l'URL d'accès officielle du service.

Étape 8 — Outil de détection contre les intrusions

Afin de sécuriser d'avantage l'infrastructure, nous allons **mettre en place un outil de protection contre les scans de ports : Portsentry**



PortSentry est un outil de détection d'intrusion réseau qui **détecte les scans de ports** et **réagit automatiquement** selon sa configuration.

A) Principe de fonctionnement

PortSentry **écoute sur les ports non utilisés** du réseau. Lorsqu'un attaquant scanne une machine, **il teste une grande plage de ports** — parfois la totalité des **65 536 ports disponibles**. En touchant inévitablement un **port surveillé par PortSentry**, il se trahit.

La logique est simple : **un utilisateur légitime ne contacte jamais un port au hasard**. Toute connexion sur un port silencieux est donc **considérée comme suspecte.**

B) Réactions possibles

Une fois un **scan détecté**, **PortSentry** peut réagir de deux façons :

Réaction	Mécanisme	Durée
Blocage firewall	Ajout d'une règle `iptables` bloquant l'IP de l'attaquant	Temporaire
Liste noire	Ajout de l'IP dans `/etc/hosts.deny`	Persistant

C) Ce que Porsentry enregistre

Chaque détection est journalisée via **syslog** avec les informations suivantes :

- L'adresse IP source de l'attaquant
- Le port ciblé
- L'horodatage de la tentative

D) Points clés

PortSentry fonctionne en mode **furtif** : il n'envoie aucune réponse sur les ports qu'il surveille. L'attaquant est bloqué sans savoir qu'il a été détecté.

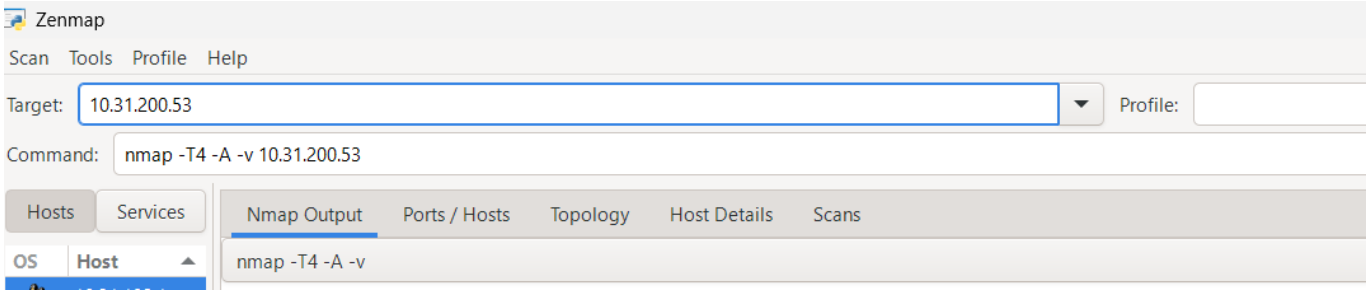
2. Installation et configuration

2.1 Scan des ports

Avant de mettre en place **Portsentry,** nous allons **effectuer un scan de ports** sur le conteneur que **l'on souhaite protéger.**

On installe **la dernière version de Nmap** (outil de **scan de ports**) : https://nmap.org/

Une fois installer, on **ouvre l'application** et **définit une adresse IP en cible** ou un **nom de domaine** (ici, c'est **mon serveur DNS** que je cible) :



Résultat du SCAN

```
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 7+deb13u1 (protocol 2.0)
53/tcp open  domain  ISC BIND 9.20.21-1~deb13u1 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.20.21-1~deb13u1-Debian
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.19 - 5.15
Uptime guess: 43.306 days (since Mon Feb 16 01:58:41 2026)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   828.00 ms 10.187.20.10
2   882.00 ms 172.31.192.254
3   886.00 ms 10.31.200.53

NSE: Script Post-scanning.
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Initiating NSE at 10:18
Completed NSE at 10:18, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.30 seconds
           Raw packets sent: 1046 (46.938KB) | Rcvd: 1046 (42.958KB)
```

On peut voir ici que **le scan de ports à détecter deux port ouverts**, le **22 (SSH)** et et le **53 (DNS)**.

Le scan a également **relevé des informations** tel que **la version de l'OS, la distribution Linux utilisée, la latence du réseau (800-900ms),** etc...

2.2 Installation de Portsentry

Comme dit précédemment, **nous installerons et configurerons l'outil Portsentry** sur **mon serveur DNS** car c'est un des services **qui contacte internet.**

On met à jour la machine :

```
root@ns1-pub:#~ apt update && apt upgrade -y
```

On installe l'outil depuis les dépôts Debian :

```
root@ns1-pub:#~ apt-get install portsentry
```

On configure le mode de détection :

```
root@ns1-pub:#~ nano /etc/default/portsentry

TCP_MODE="atcp"
UDP_MODE="audp"
```

En **ajoutant la lettre “a” devant tcp et udp**, nous venons de passer au **mode de détection**

avancé de Portsentry.

Au lieu de de **surveiller les ports définit dans le fichier /etc/portsentry/portsentry.conf**, **Portsentry** surveille désormais une **liste aléatoire de ports**, **adaptés aux services de l'entreprise.**

Ensuite, nous allons nous rendre dans **le fichier de configuration de Portsentry** afin de **définir les actions à effectuer lorsque qu'une analyse de ports est détectée.**

```
root@ns1-pub:#~ nano /etc/portsentry/portsentry.conf
```

Afin d'améliorer la sécurité de la réponse, nous allons commenté la ligne suivante :

```
KILL_ROUTE="/sbin/route add -host $TARGET$ reject"   #rejète les paquets depuis/vers cette IP au niveau de la table de routage.
```

Pour décommenté celle ci :

```
KILL_ROUTE="/sbin/iptables -I INPUT -s $TARGET$ -j DROP"    # bloque les paquets entrant depuis l'IP de l'attaquant au niveau du pare-feu noyau.
```

On active le blocage des IP en mettant la valeure 1 :

```
BLOCK_UDP="1"
BLOCK_TCP="1"
```

On redémarre le service Portsentry :

```
root@ns1-pub:#~ /etc/init.d/portsentry restart
```

<panel type=“primary” title=“2.3 Test de sécurité ”>

Nous avons **configuré Portsentry** pour qu'il **bloque les scans de ports provenant de n'importe quelle machine distante en les mettant dans le fichier : /etc/host.deny**

De plus, lorsqu'un **scan de ports est détecté**, **Portsentry log les informations dans le fichier de log linux : /var/log/syslog**

Nous allons donc **tester** en **effectuant un scan de ports depuis une machine distante.**

On met à jour la machine de test :

```
root@test-sécurité:#~ apt update && apt upgrade
```

On installe nmap (outil de scan de ports) :

```
root@test-sécurité:#~ apt-get install nmap
```

On effectue un scan vers la machine qui contient Portsentry :

```
root@test-sécurité:#~ nmap -sS 10.31.200.53
```

On retourne dans notre **machine qui a subit le scan** et on vérifie :

- **le fichier de log :**

```
root@ns1-pub:#~ cat /var/log/syslog
```

```
026-03-31T09:46:41.806345+00:00 ns1-pub portsentry[6659]: attackalert: TCP SYN/Normal scan from host: 10.31.202.80/10.31.
.80 to TCP port: 82
026-03-31T09:46:41.806368+00:00 ns1-pub portsentry[6659]: attackalert: Host: 10.31.202.80/10.31.202.80 is already blocked
noring
026-03-31T09:46:41.806390+00:00 ns1-pub portsentry[6659]: attackalert: ERROR: cannot open ignore file. Blocking host anyw

026-03-31T09:46:41.806413+00:00 ns1-pub portsentry[6659]: attackalert: TCP SYN/Normal scan from host: 10.31.202.80/10.31.
.80 to TCP port: 765
026-03-31T09:46:41.806436+00:00 ns1-pub portsentry[6659]: attackalert: Host: 10.31.202.80/10.31.202.80 is already blocked
noring
026-03-31T09:46:41.806456+00:00 ns1-pub portsentry[6659]: attackalert: ERROR: cannot open ignore file. Blocking host anyw

026-03-31T09:46:41.806476+00:00 ns1-pub portsentry[6659]: attackalert: TCP SYN/Normal scan from host: 10.31.202.80/10.31.
.80 to TCP port: 911
026-03-31T09:46:41.806499+00:00 ns1-pub portsentry[6659]: attackalert: Host: 10.31.202.80/10.31.202.80 is already blocked
noring
026-03-31T09:46:41.806521+00:00 ns1-pub portsentry[6659]: attackalert: ERROR: cannot open ignore file. Blocking host anyw
```

On peut voir que **Portsentry a bien log les informations d'attaques dans ce fichier.**

Nous allons maintenant vérifier si **l'adresse IP de l'attaquant est inscrite dans le fichier /etc/hosts.deny**

```
root@ns1-pub:#~ nano /etc/hosts.deny
```

```
# validate looked up hostnames still
# versions of Debian this has been t
# ALL: PARANOID

ALL: 10.31.202.80 : DENY
ALL: 10.31.195.80 : DENY
ALL: 10.187.20.136 : DENY
```

L'adresse IP de l'attaquant est bien **inscrite dans le fichier de bannissement des IP.**

La dernière étape **consiste à renseigner les adresses IP** de notre réseau dans **la white liste de portsentry** afin **qu'elles ne soient pas bloquées** si elles contactent la machine **sur un port non habituel.**

On se rend dans le fichier white liste :

```
root@ns1-pub:#~ nano /etc/portsentry/portsentry.ignore.static
```

On renseigne les adresse IP tout en bas

Bilan

L'infrastructure déployée comprend :

- Un serveur **DNS** (BIND9) résolvant `nextcloud.portfolio.org` et `ldap.portfolio.org`
- Un conteneur **OpenLDAP** (`10.31.204.87`) avec une OU `users` et un utilisateur de test `jdupont`
- Un conteneur **MariaDB** (`10.31.204.34`) hébergeant la base `nextcloud`
- Un serveur **Web Apache** (`10.31.202.80`) déployant Nextcloud en HTTPS avec certificat auto-signé
- Une **authentification centralisée** via le plugin LDAP de Nextcloud
- Un outil de détection contre les intrusions via Portsentry