# SAE24-CYBER

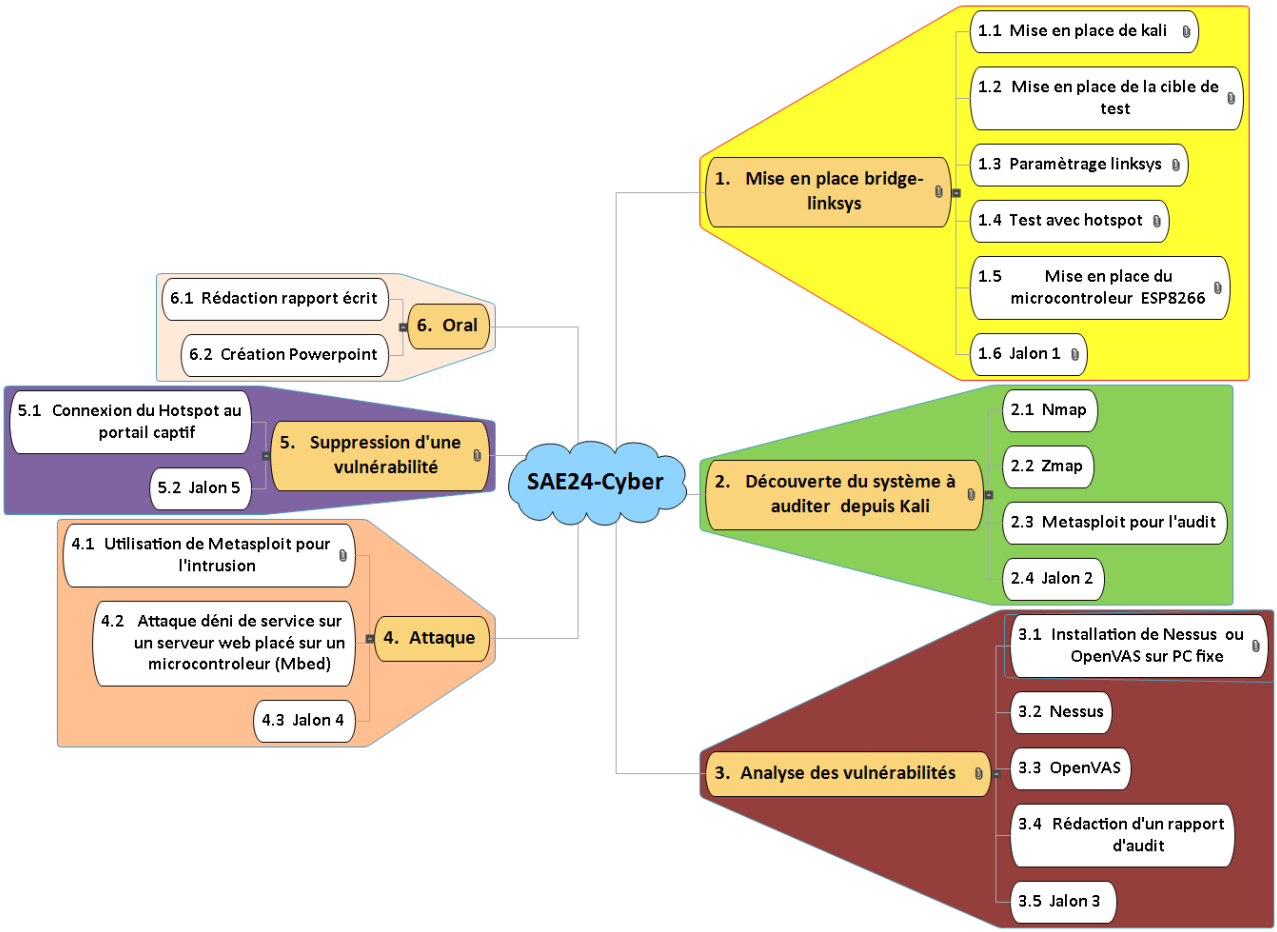



**Figure 1 : carte mentale SAE24**

**Travail en Trinome:**

Matériel:

lecteur de carte SD- USB

Borne linksys

Pour kali :Rpi pi4,alim USB C, hdmi micro, clavier et souris, carte micro SD

Pour RasPwnOS: Rpi pi3,alim classique, câble HDMI classique

# 1 MISE EN PLACE D'UN BRIDGE-LINKSYS

L'objectif est de paramétrer la borne linksys ( **voir figure 2**) afin d'étendre la portée d'un réseau sans fil grâce à un répéteur (routeur secondaire) qui augmente la portée du routeur primaire (dans notre cas, le hotspot RasPwnOS_X). Certains routeurs secondaires acceptent des connexions à fil ET sans fil.

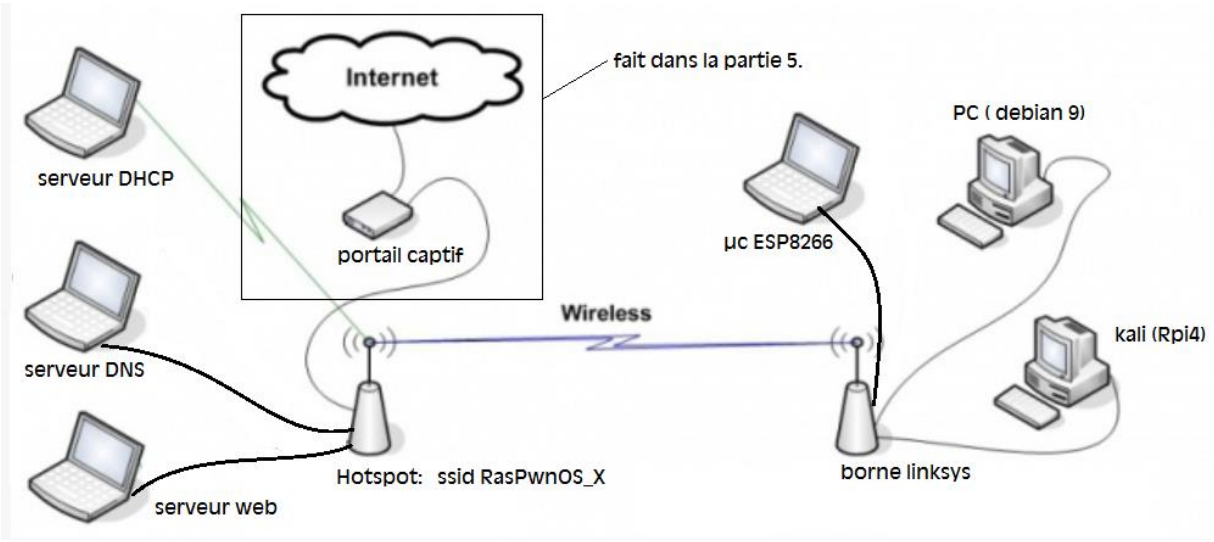



**Figure 2 : schéma du réseau informatique à mettre en place**

Le mode bridge permet de relier deux segments de réseau par une liaison sans fil. Chaque segment physique est organisé autour d'un routeur. Le routeur primaire (**hotspot**) sera relié à internet via un portail captif ( cela sera fait dans la partie 5 voir figure 1-carte mentale), alors que le routeur secondaire( borne Linksys) se connecte sans fil au routeur primaire et permet aux clients situés dans son segment d'accéder à internet et aux machines situées dans l'autre segment via le routeur primaire.

Un raspberryPi 4 ( avec Kali), un PC et un microcontrôleur seront connectés sur le second segment en filaire pour les 2 premiers et en wifi pour le dernier.

Les deux segments seront dans le même sous-réseau et apparaîtront pour tous les ordinateurs du réseau exactement comme deux switches ethernet reliés par un câble. Comme tous les ordinateurs sont dans le même sous-réseau, les broadcasts atteindront toutes les machines, permettant à tous les clients DHCP d'obtenir leurs adresses IP auprès d'un seul serveur DHCP, même si elles se trouvent dans un autre segment physique du réseau.

Ce principe est utilisé afin de connecter des ordinateurs situés dans un local et d'autres dans un local distant sans devoir tirer un câble ethernet entre ces deux locaux.

Mais un bridge sans fil standard a une limitation en ce que le segment de réseau créé autour du routeur secondaire n'accepte que des clients connectés par câble. Depuis la version V24 de DD-WRT, les clients peuvent se connecter indifféremment en ethernet ou sans fil.

Dans le cas qui nous intéresse, le routeur secondaire sous DD-WRT est configuré en Répéteur bridge connecté (sans fil) au routeur sans fil primaire.

## 1.1 MISE EN PLACE DE KALI

Après avoir connecté votre PC sur le portail captif de la salle ( voir fiche 1 : *TP_fiche1_utilisation_portail_captif.pdf*) , vous téléchargerez l'image de Kali ( voir fiche 7 : *TP_fiche7_mise_en_place_Kali_RPi4.pdf*)

Rappel : login : **kali** et mot de passe : **kali**

L'usage des outils de scan, d'attaque est INTERDIT ailleurs que sur le resaeu RasPwnOS ou qu'au sein de votre LAN.
*Sachez que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.*

## 1.2 MISE EN PLACE DE LA CIBLE DE TEST

### 1.2.1 DESCRIPTION DE LA CIBLE : RASPWN

Raspwn émule un serveur Debian Wheezy vulnérable. Une fois connecté, vous pouvez explorer le sous-réseau 192.168.99.0/24 et le domaine *.playground.raspwn.org

Les applications Web existent dans leur propre petit univers. Chacun reçoit son DNS de Raspwn et tout le courrier sortant vers *@playground.raspwn.org est livré au serveur de messagerie local à mail.playground.raspwn.org et peut être récupéré via IMAP à partir de cet hôte ou affiché à partir de Roundcube dans le playground. Tout, du DNS au MTA en passant par MySQL et Apache2, est déjà configuré.

Deux comptes de messagerie ont été configurés .

Les services réseau exécutés dans Raspwn incluent :

- Bind9 (192.168.99.A) - Serveur DNS
- Postfix (192.168.99.B) - Agent de transfert de courrier
- Dovecot (192.168.99.C) - Serveur client de messagerie
- Samba (192.168.99.D) - Serveur de partage de fichiers Windows
- Apache2 (192.168.99.E) - Serveur Web
- Nginx (192.168.99.F) - Serveur Web
- Serveur MySQL (127.0.0.1) - Serveur de base de données

- OpenSSH (92.168.99.1) - Serveur SSH

###Applications Web Playground Applications Web intentionnellement vulnérables-

- Briques OWASP - https://www.owasp.org/index.php/OWASP_Bricks
- Application Web vulnérable (DVWA) - http://www.dvwa.co.uk/
- OWASP Hackademic - https://www.owasp.org/index.php/OWASP_Hackademic_Challenges_Project
- OWASP Mutillidae II - https://sourceforge.net/projects/mutillidae/
- Peruggia - https://sourceforge.net/projects/peruggia/
- WackoPicko - https://github.com/adamdoupe/WackoPicko
- WebGoat - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Applications Web obsolètes

- Concrete 5.6.3.4 - https://www.concrete5.org/
- Drupal 6.34 - https://www.drupal.org/
- Drupal 7.34 - https://www.drupal.org/
- Joomla 2.5.28 - https://www.joomla.org/
- Joomla 3.4.0 - https://www.joomla.org/
- osCommerce 2.3 - https://www.oscommerce.com/
- phpBB 3.0.13 - https://www.phpbb.com/
- Wordpress 3.8.1 - https://wordpress.com
- Wordpress 4.1 - https://wordpress.com
- Zen Cart 1.5.4 - https://www.zen-cart.com/
- PhpMyAdmin 3.4.11 - https://www.phpmyadmin.net/
- Samba SWAT 3.6.6 - https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/SWAT.html
- Roundcube 0.7.2 - https://roundcube.net/

Pour l'utiliser, démarrez simplement Raspwn, puis connectez-vous au SSID WiFi "RasPwn OS". (Mot de passe - 'In53cur3!')

Le terrain de jeu Web Raspwn peut être trouvé sur http://playground.raspwn.org (192.168.99.13)

### 1.2.2 INSTALLER RASPWN

L'installation est la même que pour toute autre image pour le Raspberry Pi, mais l'image nécessite un Raspberry Pi 3. Le système d'exploitation Raspwn nécessite les éléments suivants :

- Un Raspberry Pi 3b **dont le** WiFi sera géré par l'application hostapd. Une alimentation micro-USB 5V pour le pi
- Une carte MicroSD - 4 Go minimum (8 Go ou plus recommandés, classe 10 recommandée)

Image zip à graver site=> **https://raspwn.org/install**

Puis depuis le terminal, afin de graver votre carte SD, exécutez :

*sudo dd if= path_of_your_image.img of=/dev/disk n bs=1M*

N'oubliez pas de remplacer n par la valeur de votre carte SD par exemple :

*sudo dd if=mon_image_kali.img of=/dev/disk4 bs=1M*

### 1.2.3 PARAMETRER RASPWN

Ce Rpi va émettre un hotspot dont le SSID est nommé RasPwnOS et afin qu'aucun système ne puisse se brouiller, il faut modifier le nom de chaque SSID.

Chaque binome changera son SSID par **RasPwnOS_X** dans lequel X représente le numéro de binome. Le mot de passe sera inchangé( Mot de passe : **In53cur3!** par défaut)

Le fichier de configuration du hostspot /etc/hostapd/hostapd.conf contient tous les paramètres de configuration du point d'accès Wi-Fi.

La seule modification de configuration du fichier hostapd.conf sera la suivante :

.....

# Nom du spot Wi-Fi

ssid=RasPwnOS_X

……..

### 1.2.4 LES MOTS DE PASSE DU RASPWN

| Application web | ssh | mail 1 | mail 2 |
|---|---|---|---|
| admin<br>*Pa55w0rd !* | pi<br>*pwnme!* | admin@playground.raspwn.org<br>*Pa55w0rd !* | mrbill@playground.raspwn.org<br>*OhNoMrBill !* |

| | | | |
|---|---|---|---|

Rappel accès ssid: SSID= RasPwnOS_X et mot de passe : **In53cur3!**

L'exemple de fichier de configuration est fourni dans /etc/hostapd/hostapd.conf - modifiez-le selon vos besoins (changez le BSSID et la clé WPA).

Décommentez ensuite la ligne DAEMON_CONF dans /etc/default/hostapd pour déverrouiller le script d'initialisation.

Enfin, lancez le script d'initialisation : /etc/init.d/hostapd start

## 1.3 PARAMETRAGE LINKSYS

On suppose que le routeur (hotspot) primaire est configuré dans un sous-réseau 192.168.99.X et attribue des adresses DHCP dans ce même sous-réseau. Le routeur secondaire a le firmware DD-WRT V24 .

Paramétrer la borne linksys afin de créer un bridge wifi avec le hotspot que vous venez de mettre en place.

Solution :
Parametrage de la borne linksys
Onglet Wireless=> basic Setting
Dans le champ "wireless Physical Interface wl0 ( 2,4 GHz)
* Wireless Mode => mettre Client Bridge
* Wireless Network Mode => mettre Mixed
* Wireless Network Name => mettre RasPwnOS_x ( avec x = votre numéro de binome) il devra être identique au réseau wifi produit par votre Rpi
*Network Configuration=> mettre Bridged
**Question : faut-il mettre le mot de passe du hotspot ?**

## 1.4 TEST AVEC HOTSPOT

Mettre sous tension le hotspot ainsi que le routeur secondaire.

**Travail**: Donner l'adresse IP de votre PC et du Rpi-Kali

## 1.5 MISE EN PLACE DU MICROCONTROLEUR ESP8266

Le microcontroleur sera programmé pour être connecté en wifi au hotspot et un serveur web sera aussi installé dessus ( voir fiche 8 : ***TP_fiche8_mise_en_place_ESP_8266_lolin.pdf***)

Ce serveur sera la cible de l'attaque Ddos que vous ferez dans la partie 4.

Afin de vérifier le bon fonctionnement du serveur web, vous accéderez à ce serveur de 2 manières différentes.

### 1.5.1 MISE EN PLACE DU SERVEUR WEB SUR ESP

Votre serveur web doit vous renvoyer « Hello from esp8266 and binome X « dans un premier temps puis « Hello from esp8266 and binome X + mac=xx.xx.xx.xx.xx.xx » en ajoutant l'adresse mac de votre ESP

### 1.5.2 ACCES VIA EXPLORATEUR INTERNET

Depuis kali ou le PC, aller sur la page web de l'ESP et faire une copie d'écran de cette page.

### 1.5.3 ACCES VIA LIGNE DE COMMANDE

Depuis kali ou le PC, via une fenêtre « terminal », accéder au serveur web via la commande wget :

***wget -O verif_serveur_web.txt http://192.168.99.x***

Cette commande va enregistrer le code HTML de la page dans le fichier **« *verif_serveur_web.txt* »** dans le répertoire courant.
Vous n'avez donc plus qu'à lire le fichier avec la commande

***cat verif_serveur_web.txt***

## 1.6 JALON 1

- Schéma de hotspot/repeteur/serveur DHCP sur Packet Tracer.
- Adresse IP de votre PC et du Rpi-Kali
- Copie d'écran de la page d'accueil du serveur web
- Copie du contenu de fichier ***verif_serveur_web.txt***

# 2 DECOUVERTE DU SYSTEME A AUDITER DEPUIS KALI

L'objectif de cette partie est d'utiliser divers outils pour scanner le réseau afin d'obtenir la liste des adresses IP, des ports ouverts et des versions des applications.

## 2.1 NMAP

Il y a une commande qui s'appelle arp-scan et qui permet d'aller lire la table ARP sur un réseau et lister les adresses IPs.

```
# arp-scan -l
```

A l'aide de nmap puis de curl, vous allez établir la liste des adresses IP, des ports ouverts et propriétés des pages web

Qq commandes :

**nmap –0 192.168 .99.0/24  (=> donne les ports/les services/version OS)**

**nmap –sV 192.168 .99.0/24(=> donne les ports/les services/les versions des services/**

**nmap –A 192.168 .99.0/24(=> donne  toutes les infos mm l'organisation site web**

Recherche des infos sur les serveurs web :

Pour chaque port http, vous éditerez l'ensemble des informations en utilisant cURL.

cURL est un outil qui permet le transfert de données en se basant sur la syntaxe d'une URL. Avec l'option –I, cette commande renvoie l'entête http

**#curl –I 192.168.99.x**

Quelques combinaisons d'options sympa.

| Options | Descriptions |
|---|---|
| -sS | SYN scan via TCP pour effectuer un scan discrèt sur les ports ouvert/fermer grâce au réponse ICMP de la cible (si le firewall bloque ICMP impossible de savoir) |
| -sU | scan via UDP pour voir les ports ouvert/fermer grâce au réponse ICMP de la cible (si le firewall bloque ICMP impossible de savoir) |
| -Pn | Réaliser un scan de type half-scan (c-a-d un scan sans établir de connexion) permet de bypasser le blocage de réponse ICMP par un firewall |
| -A | Permet de faire des scans agressif (systeme d'exploitation, port ouvert, service qui tourne et leur version etc...) |
| -sV | Permet d'analyser les banière applicative d'un programme (prologue envoyé par un programme pour souhaiter la bienvenue à un utilisateur) |
| sN | Permet de montrer si les ports sont filtrés par un firewall |
| -v | Mode verbeux, permet d'afficher les résultats du scan en temps réel et ne pas attendre jusqu'a ce que le scan soit entièrement fini |

**utiliser > pour récupérer l'ensemble des données dans un fichier mon_systeme.txt**

## 2.2 METASPLOIT POUR L'AUDIT

Sous kali, dans la menu application, menu 8 :Exploitation Tools=>matasploit framework

Faire un scan agressif :

```
msf6 > db_nmap -v -sS -A 192.168.99.0/24
```

Metasploit permet de stocker le résultat de nos scans dans sa base de donnée.

```
msf6 > hosts
```

On peut voir les services que nous avons scannés

```
msf6 > services
```

### Scanner le service SMTP

nous allons énuméré les utilisateurs du service SMTP.on recherche les modules utilisant SMTP avec la commande search

```
msf > search smtp_enum
```

On utilise ensuite la commande use avec le numéro du module soit le nom du module avec son chemin

```
msf > use auxiliary/scanner/smtp/smtp_enum
```

On liste les options de ce module avec la commande show options

```
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
```

On fixe les options manquantes  avec la commande set

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.99.18
```

puis on lance le scan avec la commande run ou exploit

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

### Se connecter au service SMTP en utilisant telnet

nous allons nous connecter au service SMTP en utilisant telnet :

telnet 192.168.99.18 25

On execute ensuite la commande suivante pour dire Hello à SMTP et voir et voir ce qu'il nous répond.

```
ehlo localhost
```

SMTP nous répond en envoyant les commandes qui peuvent être passées à SMTP

On observe qu'on peut renseigner pas mal de commande et notamment **VRFY**.

VRFY permet de savoir **si une adresse mail existe ou non**

```
VRFY toto
```
Faites des tests avec des noms classiques afin de voir si l'adresse mail existe. La réponse du serveur sera :

```
252 2.0.0 nom_mail

VRFY root
VRFY admin
```

## 2.3 JALON 2

- Sous packet Tracer, indiquer l'ensemble des services disponibles
- Faire un tableau avec l'ensemble des services et des versions des différentes applications
- Copie d'écran des pages d'accueil des différents serveurs web

# 3 ANALYSE DES VULNERABILITES

Il existe de nombreux outils permettant de faire de l'audit de vulnérabilités. Nous avons NESSUS et OPENVAS.

Le premier est payant  mais dispose d'une version gratuite suffisante pour nos tests.

Le second est gratuit.

Le site **https://www.cvedetails.com** permet de voir les vulnérabilités suivant les versions des services ( debian 8-9, php 5.4.36…)

## 3.1 INSTALLATION DE NESSUS  SUR PC FIXE

Demander aux étudiants de créer un compte afin de récupérer un code d'activation.

Connexion du PC sur le portail captif

Attention, le téléchargement des plugins dure 1h

## 3.2 NESSUS

Vous allez travailler avec une application appelée NESSUS ( version gratuite nommée nessus-essentials) qui permet de scanner les vulnérabilités d'une machine ( ports ouverts, version logiciels...).

Cependant, la mise en place de cet outil demande un code d'activation qui peut prendre quelque temps à obtenir. Cette demande se fait sur le lien suivant :

https://www.tenable.com/products/nessus/nessus-essentials

Ce code d'activation sera déposé dans le JALON 0 de cette SAE avant le début de cette SAE et fera partie de la notation de votre SAE.

### 3.2.1 INSTALLATION DE NESSUS

Afin de fonctionner sur les PC de l'IUT qui sont en debian 10, ce sera le fichier **Nessus-10.1.2-debian6_amd64.deb** qui devra être installé. Le lien suivant permet de comprendre le processus d'installation https://www.youtube.com/watch?v=CKZfTqDBq4A

Pour installer ( depuis le répertoire contenant le fichier.deb):

```
#sudo apt install ./Nessus-10.1.2-debian6_amd64.deb
```
lancer Nessus avec:

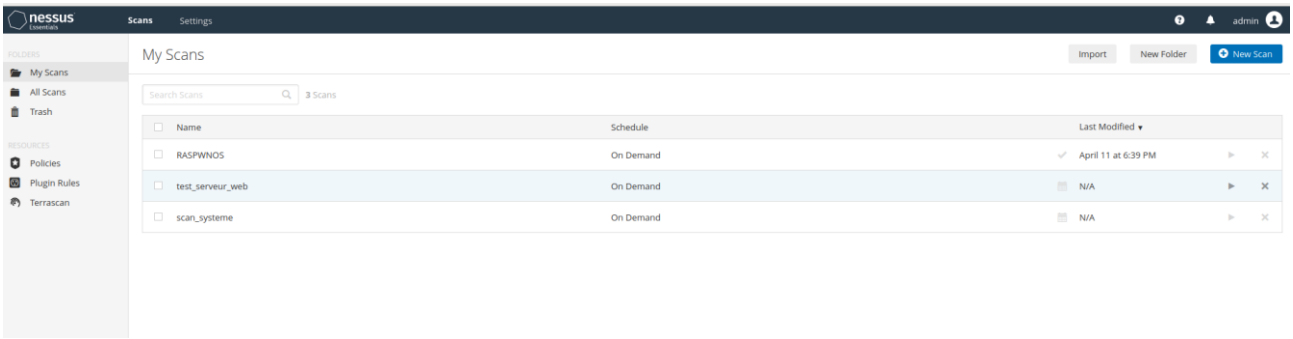
```
#sudo /bin/systemctl start nessusd.service
```
Pour vérifier que tout fonctionne :

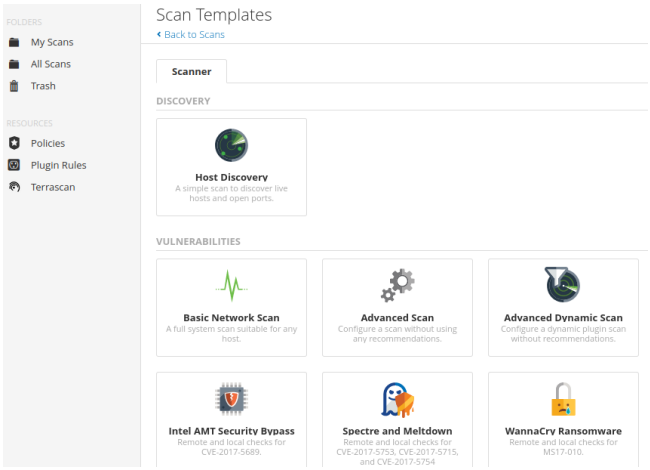
```
#systemctl status nessusd
```
Pour administrer Nessus, aller dans l'URL `https://localhost:8834`

Rentrer votre code d'activation puis choisir un login/mot de passe pour l'utilisateur de Nessus

### 3.2.2 MISE EN PLACE DE SCAN DU RESEAU PAR NESSUS

Pour effectuer un scan, New scan puis choisissez un « basic Network Scan »






### 3.2.3 EXPORT DU RAPPORT D'AUDIT

Vous exporterez le rapport d'audit « vulnerability operations » qui donnera le détail des vulnérabilités pour chaque machine scannée.

### 3.2.4 EXPORT BASE DE DONNEES :

A l'issue du scan, allez dans EXPORT ( en haut à droite) puis NESSUS . Le fichier sera exporté en .xml dans le répertoire de Téléchargement

## 3.3 INSTALLATION DE METASPLOIT

### 3.3.1 INSTALLATION

L'ensemble de l'installation est décrit dans la lien ci-dessous :

https://computingforgeeks.com/install-metasploit-framework-on-debian/

```
$ sudo apt update
```

```
$ sudo apt install curl wget gnupg2
```

```
$ curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall
```

Une fois le script téléchargé, rendez le exécutable.

```
$ chmod +x msfinstall
```

```
$ ./msfinstall
```

`$msfdb init` ( initailisation)

( répondre Yes si vous voulez aussi une admi via page web)

`$ msfupdate` ( mise à jour)

`$ msfconsole` ( pour lancer la msf)

### 3.3.2 LIEN ENTRE NESSUS ET METASPLOIT

Sous metasploit, utiliser la commande db_import pour importer le fichier xml précédement créé par Nessus

`msf6 > db_import mon_repertoire/ma_base_donnees.nessus`

A l'aide des commandes `hosts` et `services`, vous pouvez voir l'ensemble des adresses IP scannées et des services détectés.

La commande `vulns` permet de voir les vulnérabilités

`msf6 > vulns help` => permet de voir les options de cette commandes

`msf6 > vulns -p 22` => permet de lister les vulnérabilités du port 22

Travail :

En fonction des vulnérabilités CVE identifiées, rechercher sous metasploit les exploits pouvant être utilisés pour chaque CVE

msf6 > search cve:xxxx-xxxx

Lorsqu'un exploit a été identifié, allez dans www.cve.details.com afin de relever les conséquences de cette failles.

## 3.4 JALON 3

Vous déposerez sur Moodle :

- La rapport d'audit fait par Nessus
- Copie d'écran de la fenêtre terminal « metasploit » avec la liste de l'ensemble des services identifiés suite à la commande
  msf6 > services
- Copie d'écran de la fenêtre terminal « metasploit » avec la liste des cve du port 53
- Copie d'écran de la fenêtre terminal « metasploit » avec la liste des exploits possibles en lien avec le ou les cve détectés.

# 4 ATTAQUE

## 4.1 DENI DE SERVICE

Vous allez mettre en place une attaque par deni de service.

La cible sera le micro-controleur

Avec l'utilisation de hping3, on peut saturer un serveur. La commande suivante permet « d'inonder » un serveur.

***sudo hping3 -1 - - flood ad_IP_cible***

(attention cette commande ne fonctionne qu'en root )

## 4.2 UTILISATION DE METASPLOIT POUR L'INTRUSION

Commencez par effectuer une recherche sur la vulnerabilité dans la msfconsole avec la commande

msf6 > search Samba NDR MS-RPC

Cela devrait vous afficher une liste d'exploits disponibles. Nous allons utiliser exploit/multi/samba/usermap_script mais vous pouvez en tester d'autres.

Pour utiliser cet exploit, faites un use exploit/multi/samba/usermap_script dans la console. Vous êtes maintenant en train de l'utiliser. Mais exploiter une machine ne suffit pas, il faut en faire quelque chose, executer un code, nous donner un shell, installer un backdoor, ces actions sont appellées charges, ou payloads en anglais.

Pour afficher la liste des payloads disponibles avec cet exploit, utilisez la commande

show payloads

Vous aurez donc une liste de charges disponibles. Nous allons ici utiliser la charge cmd/unix/bind_netcat afin de nous donner un shell en root sur la machine cible.

Effectuez cette commande : set payload cmd/unix/bind_netcat

Une fois la charge sélectionnée, il faut maintenant la configurer.

Tapez show options et vous aurez une liste des options à configurer pour que l'exploit fontionne.

Dans notre cas, il n'y a que l'option RHOST à configurer. Cela signifie Remote Host, c'est la machine cible, en gros.

Il faut donc renseigner l'adresse de la cible: set RHOST 192.168.99.10

Refaites un show options pour vérifier que les options sont bien configurées.

Tout est prêt, il ne vous manque plus qu'à lancer l'exploit avec la commande exploit

Voici un résultat réussi de l'exploit. Vous pouvez à présent executer des commandes en shell, comme si vous aviez un accès direct à la machine.

Libre à vous d'installer une backdoor, d'upload un virus, de fermer les antivirus, les firewalls, de copier des fichiers, de supprimer le /root (S'il y a des crashers parmis les lecteurs) enfin bref, vous avez un accès à la machine.

## 4.3 ATTAQUE MAN IN THE MIDDLE

### 4.3.1 DESCRIPTION DE L'ATTAQUE

L'objectif est d'insérer l'attaquant ( raspberryPi Kali) entre 2 PC victimes. Vous ne pouvez pas utiliser le RASPWN comme victime car le spoofing ARP qui sera utilisé sature le fonctionnement de ce dernier.

Il faudra ajouter un second PC fixe

Victime 1 : PC1 fixe sous debian

Victime 2 : PC2 fixe sous debian

Afin de charger les tables ARP des PC, faire un ping entre les 2 PC

Relever dans un tableau comme celui ci-dessous les paramètres de chaque PC.

| | Adresse IP V4 : | Adresse MAC de la carte réseau |
|---|---|---|
| PC1 debian | | |
| PC2 debian | | |
| Rpi Kali | | |

### 4.3.2 MISE EN PLACE DE L'ATTAQUE ARP SPOOFING.

Voir : https://itigic.com/fr/arp-poisoning-attack-how-to-do-it-on-kali-linux/

Sous kali, dans Applications=>sniffing & spoofing=>lancer ethercap -graphical

Valider le choix eth0, sniffing at startup. Cliquer sur l'icône accept afin de valider votre initialisation.

Lancer le scan du réseau en cliquant sur l'icône loupe ( scan for hosts)

Cliquer sur l'icône liste (hosts list)

Choisir vos 2 cibles entre lesquelles Kali va s'immiscer. ( mettre l'attaque dans les 2 sens en mettant spécifiant que l'usurpation va de la machine 1 debian vers de la machine 2 debian mais aussi de la machine 2 debian vers la machine1 debian).

Vous venez de mettre en place les outils pour lancer l'attaque.

### 4.3.3 MISE EN EVIDENCE DE L'USURPATION A TRAVERS L'ANALYSE D'UN PING

Lancer l'attaque =>icone terre (MITM MENU) => choisir ARP poissoning =>cliquer OK pour lancer l'attaque.

Vous pouvez faire un ping entre vos 2 cibles et analyser les trames avec wireshark.

Analyser de la nouvelle table ARP d'une des 2 cibles. Elle doit être commentée.

En quoi consiste une attaque MITM ? Quel est le protocole des trames envoyées et qui les envoie ?

## 4.4 JALON 4

- Copie d'écran de la page d'accueil du µc en mode ddos.
- Copie d'écran de la fenêtre terminal « metasploit » lors de la tentative d'intrusion
- Copie de l'acquisition wireshark montrant que l'adresse IP de la machine 1 est associée à l'adresse mac de rpi sous kali
- Copie de la nouvelle table ARP d'une des 2 cibles. Elle doit être commentée.
- En quoi consiste une attaque MITM ? Quel est le protocole des trames envoyées et qui les envoie ?

# 5 SUPPRESSION D'UNE VULNERABILITE

## 5.1 CONNEXION DU HOTSPOT AU PORTAIL CAPTIF

Le Rpi pi3 est placé sur le portail captif via le câble Ethernet filaire et fera une mise à jour de php.
Analyse avec NESSUS. Comparaison des vulnérabilités

## 5.2 JALON 5

Copie du rapport nessus mettant en évidence la suppression de la vulnérabilité.

# 6 ORAL

## 6.1 REDACTION RAPPORT ECRIT

## 6.2 CREATION POWERPOINT