

# TABLE DES MATIÈRES

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1. AVANT-PROPOS .....	1
1.2. MISE EN SITUATION .....	2
<b>2. ETAT DE L'ART.....</b>	<b>4</b>
2.1. TABLEAU RÉCAPITULATIF .....	5
2.2. OS PENTEST.....	7
2.2.1. <i>Android Rooté</i> .....	7
2.2.2. <i>NetHunter</i> .....	8
2.2.3. <i>CyanogenMod</i> .....	11
2.2.4. <i>Android PI</i> .....	12
2.2.5. <i>Pwn Pad</i> .....	13
2.3. PACKAGE PENTEST .....	14
2.3.1. <i>Revenssis</i> .....	14
2.3.2. <i>Deploy Linux</i> .....	16
2.3.3. <i>MobSF</i> .....	16
2.3.4. <i>Bugtroid</i> .....	17
2.3.5. <i>PenTest Tools</i> .....	19
2.4. APPLICATION PENTEST .....	20
2.4.1. <i>Application de découverte réseau</i> .....	20
2.4.2. <i>Application d'attaque Man In The Middle</i> .....	25
2.4.3. <i>Application d'attaque DDoS</i> .....	28
<b>3. DÉPLOIEMENTS ET ÉVALUATIONS DES SOLUTIONS .....</b>	<b>31</b>
3.1. INSTALLATION OS PENTEST .....	31
3.1.1. <i>Android Root</i> .....	31
3.1.2. <i>Nethunter</i> .....	34
3.1.3. <i>Cyanogenmod 12</i> .....	34
3.1.4. <i>ANDROID PI</i> .....	35

3.2.	INSTALLATION PACKAGE PENTEST .....	36
3.2.1.	<i>MOBSF</i> .....	36
3.2.2.	<i>BUGTROID et Pentest tools</i> .....	37
3.2.3.	<i>Revenssis</i> .....	37
3.3.	INSTALLATION APPLICATION PENTEST .....	37
3.3.1.	<i>NMAP</i> .....	37
3.3.2.	<i>Pamn IP Scanner</i> .....	37
3.3.3.	<i>FING</i> .....	37
3.3.4.	<i>Zanti</i> .....	38
3.3.5.	<i>MITMF</i> .....	38
3.3.6.	<i>Metasploit</i> .....	38
3.3.7.	<i>LOIC</i> .....	38
3.3.8.	<i>AnDOSid</i> .....	38
3.4.	DÉCISION.....	39
3.4.1.	<i>OS Pentest – Choix retenus</i> .....	39
3.4.2.	<i>OS Pentest – Choix écartés</i> .....	40
3.4.3.	<i>Packages Pentest retenus</i> .....	41
3.4.4.	<i>Packages Pentest écartés</i> .....	42
3.4.5.	<i>Applications Pentest retenues</i> .....	43
3.5.	TABLEAU RÉCAPITULATIF DES DÉCISIONS.....	44
3.6.	MISE EN PLACE DU LABORATOIRE.....	45
3.6.1.	<i>Appareils à disposition</i> .....	45
3.6.2.	<i>Réseau fermé</i> .....	45
3.6.3.	<i>Architecture des technologies</i> .....	47
<b>4.</b>	<b>CAS PRATIQUES.....</b>	<b>48</b>
4.1.	RÉCAPITULATION DES APPLICATIONS.....	48
4.2.	DÉCOUVERTE RÉSEAU.....	49
4.2.1.	<i>Applications retenues</i> .....	49
4.2.2.	<i>Critères de comparaison</i> .....	49
4.2.3.	<i>NMAP NetHunter</i> .....	50

4.2.4.	<i>NMAP Android rooté</i>	52
4.2.5.	<i>Fing</i>	53
4.2.6.	<i>Pamn IP Scanner</i>	54
4.2.7.	<i>Zanti Scan</i>	56
4.2.8.	<i>Choix</i>	57
4.3.	ATTAQUE MAN IN THE MIDDLE	58
4.3.1.	<i>Applications retenues</i>	58
4.3.2.	<i>Critère de comparaison</i>	58
4.3.3.	<i>MITMF</i>	59
4.3.4.	<i>Zanti</i>	61
4.3.5.	<i>Récapitulatif</i>	64
4.3.6.	<i>Choix</i>	64
4.4.	ATTAQUE DDoS	65
4.4.1.	<i>Applications retenues</i>	65
4.4.2.	<i>Critère de sélection</i>	65
4.4.3.	<i>LOIC</i>	66
4.4.4.	<i>Metasploit DDoS</i>	67
4.4.5.	<i>AnDOSid</i>	69
4.4.6.	<i>Récapitulatif</i>	70
4.4.7.	<i>Choix</i>	70
<b>5.</b>	<b>CONCLUSION</b>	<b>71</b>
5.1.	OUTILS CONSEILLÉS	71
5.2.	AMÉLIORATIONS	72
5.3.	PENTEST MOBILE ET PENTEST ORDINATEUR	72

## LISTE DES TABLEAUX

Tableau 1 : Avantages et inconvénients de l'Android rooté .....	39
Tableau 2 : Avantages et inconvénients de NetHunter .....	40
Tableau 3 : Avantages et inconvénients de Bugtroid.....	41
Tableau 4 : Avantages et inconvénients PenTestTools .....	42
Tableau 5 : Appareils à disposition .....	45
Tableau 6 : Résumé de l'analyse du NMAP de NetHunter.....	52
Tableau 7 : Résumé de l'analyse du NMAP d'Android .....	53
Tableau 8 : Résumé de l'analyse de Fing.....	54
Tableau 9 : Résumé de l'analyse de Pamn IP Scanner .....	55
Tableau 10 : Résumé de l'analyse de Zanti Scan.....	57
Tableau 11 : Récapitulatif des applications de découverte réseau .....	57
Tableau 12 : Récapitulatif de l'analyse de MITMF .....	61
Tableau 13 : Récapitulatif de l'analyse de Zanti MITM .....	63
Tableau 14 : Récapitulatif des applications d'attaque Man In The Middle .....	64
Tableau 15 : Récapitulatif de l'analyse de LOIC .....	67
Tableau 16 : Récapitulatif de l'analyse de Metasploit DDoS .....	69
Tableau 17 : Récapitulatif de l'analyse de AnDOSid .....	69
Tableau 18 : Récapitulatif des applications d'attaque DDoS .....	70

## LISTE DES FIGURES

Figure 1 : Phase du rapport.....	2
Figure 2 : Black box contre white box .....	3
Figure 3: Partie du tableau récapitulatif de l'état de l'art.....	5
Figure 4 : Code couleur du tableau récapitulatif .....	6
Figure 5 : SuperSU logos.....	7
Figure 6 : Autoriser une application à utiliser le root .....	8
Figure 7: NetHunter sur une tablette Nexus.....	10
Figure 8 : NetHunter application.....	10
Figure 9 : Nombre de téléchargement CM .....	11
Figure 10: Logo de CyanogenMod .....	11
Figure 11 : Screenshot Cyanogenmod 12 .....	12
Figure 12 : Android PI.....	13
Figure 14 : Android PI en version Android 4.0.3 .....	13
Figure 18 : Pwn Pad de Pwnie Express.....	14
Figure 15: Revenssis et toutes ses possibilités.....	15
Figure 16 : Kali Linux sur un smartphone Android .....	16
Figure 17 : Logo de MobSF designé par Amrutha VC.....	17
Figure 19 : Logo de l'application BugTroid Pro .....	18
Figure 20 : Application BugTroid .....	19
Figure 21 : PenTest Tools est une application avec un design certain .....	20
Figure 22 : Logo de NMAP .....	21
Figure 23 : NMAP avec NetHunter .....	22
Figure 24 : Interface NMAP Android .....	23
Figure 25 : Pamn IP Scanner Application .....	24
Figure 26 : Scan NMAP avec Zanti.....	24
Figure 27 : Scan sur l'application Fing .....	25
Figure 28 : L'attaque de l'homme du milieu .....	26
Figure 29 : Man In The Middle sous NetHunter.....	26

Figure 30 : Metasploit est disponible en ligne de commande .....	29
Figure 31 : Interface de LOIC .....	30
Figure 32 : Logo d'AnDOSid .....	30
Figure 33 : HTC One M7 .....	32
Figure 34: Nexus 7 (2012) .....	33
Figure 13 : Menu boot Berry à son démarrage .....	36
Figure 35 : Tableau récapitulatif des décisions .....	44
Figure 36 : Plan d'adressage de notre laboratoire .....	46
Figure 37 : Résumé des technologies choisies et placement de l'univers de travail .....	47
Figure 38 : Applications retenues pour la phase de tests .....	48
Figure 39 : NMAP sous NetHunter .....	50
Figure 40 : Résultat requête NMAP sous NetHunter .....	51
Figure 41 : NMAP sous l'android rooté (avec -O pour les OS) .....	53
Figure 42 : Scan Pamn IP Scanner sur tous les appareils connectés au routeur .....	55
Figure 43 : Scan automatique de Zanti .....	56
Figure 44 : Liste des applications sélectionnées pour la phase de découverte réseau .....	58
Figure 45 : Ligne de commande pour une attaque MITM avec NetHunter.....	60
Figure 46 : MITM avec NetHunter.....	60
Figure 47 : Interface Zanti .....	62
Figure 48 : Zanti permet d'avoir les mots de passe de la cible .....	62
Figure 49 : Replace image sur le site du 20 minutes.....	63
Figure 50 : Application sélectionnée pour l'attaque Man In The Middle .....	64
Figure 51 : Interface de LOIC .....	66
Figure 52 : Analyse wireshark d'une attaque DDoS TCP de LOIC.....	67
Figure 53 : Attaque DDoS avec Metasploit sous NetHunter .....	68
Figure 54 : Situation de l'adresse IP 211.166.14.196 .....	68
Figure 55 : Application sélectionnée pour l'attaque DDoS .....	70

## 1. Introduction

### 1.1. Avant-propos

Dans le cadre de la thèse de bachelor « Environnements de test pour mobiles et tablettes », l'objectif sera dans un premier temps d'effectuer l'état de l'art de l'ensemble des technologies déjà existantes.

Une première batterie de tests sera effectuée sur les découvertes. L'idée n'est pas ici de réaliser une étude précise de la technologie analysée. Il s'agit plutôt de tester si le dispositif convient à la recherche ou non.

Par la suite la mise en place d'un laboratoire virtuel mais également physique verra le jour, avec pour but d'offrir une base solide aux tests qui suivront. Le laboratoire virtuel permettra d'essayer un grand nombre d'outils à moindre coût. La partie physique pourra être utilisée afin d'avoir un contact direct avec la machine qu'il s'agisse d'un smartphone, d'une tablette, d'un Raspberry, ou de tous ce qui donnerait la possibilité d'expérimenter les technologies trouvées.

Une fois les laboratoires mis en place, le but sera de vérifier les différentes possibilités offertes et découvertes lors de la première étape. Il s'agira d'effectuer un essai sur l'ensemble des frameworks, packages ou applications. A la fin de cette étape, des décisions seront prises et dirigeront la suite du travail. C'est à ce moment que les technologies intéressantes seront conservées et les autres abandonnées.

Le monde des tests de pénétration bien que peu connu du grand public est déjà vaste dans l'univers mobile. Il contient déjà de nombreuses technologies qui seront détaillées lors de l'état de l'art. Par conséquent, il est important de pouvoir ressortir des points qui seront approfondis et qui donneront au travail un relief et une phase de recherche plus détaillée.

C'est donc après la mise en place des deux laboratoires et des tests effectués sur les frameworks que la décision sera prise de se tourner vers tel ou tel outil.

Pour finir, durant la phase d'analyse, des expérimentations vraiment précises seront effectuées afin de proposer un retour d'utilisation complet. Plusieurs comparaisons seront présentées en toute fin du rapport et permettront de retirer la substantifique moelle de ce travail. La phase d'analyses détaillées est un point important de cette thèse. Ci-dessous, nous présentons sous forme graphique l'orientation de notre travail.

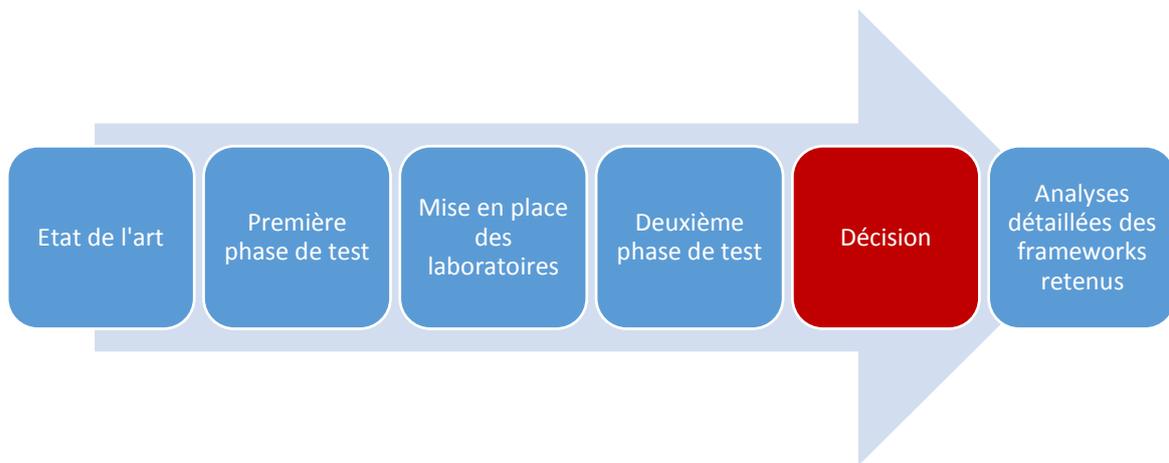


Figure 1 : Phase du rapport  
Graphique de l'auteur

## 1.2. Mise en situation

Les tests de pénétration sont un rempart incontesté contre les failles des systèmes informatiques des entreprises. Ils ont pour but de détecter les problèmes et de les réparer afin d'optimiser la sécurité d'une infrastructure informatique. Le pentesting est un outil qui a vu le jour au milieu des années 60 à la suite d'une conférence organisée par System Development Corporation, basé à Santa Monica en Californie. C'est au cours de cette conférence que les premiers tests de pénétration ont été pensés. En 1971, James P. Anderson à la suite d'une analyse approfondie sur le système informatique du Pentagone a ressorti une marche à suivre pour la pratique du pentesting (Phmadore, 2015) :

- 1) Trouver une vulnérabilité exploitable

- 2) Concevoir une attaque autour de cette dernière
- 3) Tester la brèche
- 4) Saisir une ligne en cours d'utilisation
- 5) Entrez dans la brèche
- 6) Exploiter l'entrée pour la récupération d'information

Dans le siècle dernier, les ordinateurs étaient beaucoup moins utilisés dans le monde professionnel. Certainement dû à leur taille, leur complexité ou encore leur prix. De nos jours, on compte plus 8 milliards d'appareils mobiles à usage personnel (Cherki, 2012). La nécessité de protéger son réseau est devenue primordiale, et encore plus pour les entreprises. Le pentesting est une façon intéressante d'analyser ses faiblesses et de les renforcer. Le pentester peut mettre à l'épreuve l'infrastructure via plusieurs situations.

- Black box : C'est un test réalisé avec peu d'information
- White box : Le testeur possède tous les informations disponibles
- Grey box : Entre le black box et le white box



Figure 2 : Black box contre white box  
<http://www.testingexcellence.com/3-main-types-of-software-testing/>

Ces différentes possibilités permettent de se situer depuis plusieurs angles d'attaque et par conséquent d'élargir le spectre des possibles offensives informatiques. Dans le cadre de ce travail, le but est d'offrir la possibilité à des testeurs d'effectuer des vérifications via un smartphone ou une tablette sur l'environnement d'une entreprise consentante.

## 2. Etat de l'art

Durant cette première étape, nous avons cherché à ressortir les possibilités de tests de pénétration par le biais de trois axes :

- L'OS Pentest
  - Il existe des versions modifiées d'Android qui permettent de réaliser des tests d'intrusion. Certains OS apportent une application particulière ou carrément un package complet. Nous considérons un système d'opération comme tel uniquement à partir du moment où nous devons installer un nouvel environnement mobile sur notre smartphone ou notre tablette.
- Le package Pentest
  - C'est une sorte d'annuaire qui contient un grand nombre d'applications de pentesting. Le Package fait office de centralisateur d'apps et propose l'installation de ces dernières. Il est tout aussi possible que le package renvoie l'utilisateur vers des sites proposant l'application.
- L'application Pentest
  - Ici, nous faisons référence aux applications que l'on peut trouver sur internet ou sur le PlayStore par le biais d'un package ou non. Elles sont séparées en plusieurs catégories telles que « Découverte réseau », « Attaque Man In The Middle » ou « Attaque DDoS ». Ces classifications permettent de séparer les applications afin de regrouper celles ayant le même fonctionnement.

Une fois l'état de l'art terminé, nous prendrons une décision quant aux technologies que nous conserverons. L'objectif est de pouvoir ressortir 2 OS, 2 packages ainsi que 3 types d'application de pentesting. L'objectif étant de pouvoir par la suite se concentrer sur des outils spécifiques et fournir une démonstration pratique de ces derniers.

## 2.1. Tableau récapitulatif

Board control		Pen TEST
OS Pentest	Package Pentest	Application Pentest
<b>NetHunter</b>	<b>Revensis</b>	<b>NMAP</b>
Installé avec succès sur le Nexus 7	<a href="https://sourceforge.net/projects/revensis/">https://sourceforge.net/projects/revensis/</a>	Découverte réseau
Impossible d'accéder au fastboot	Impossible d'installer. Out of Date	Nécessite rootage
Excellent OS de Pentest	Ce package n'est plus d'actualité	Scanner de réseau
<b>CyanogenMod 12</b>	<b>Deploy Linux</b>	<b>Zanfi</b>
Installé avec succès sur le HTC M7	<a href="https://www.youtube.com/watch?v=u22eDb9EgE">https://www.youtube.com/watch?v=u22eDb9EgE</a>	Découverte réseau et Attaque MITM
Impossible d'accéder au fastboot	Hors projet	Nécessite rootage
Ce n'est pas une custom rom de pen test	Hors projet	Application complète
<b>Android Roof</b>	<b>MobSF</b>	<b>MITMf</b>
Testé via le CyanogenMod 12. Installé correctement sur HTC M7	<a href="https://github.com/ajinabraham/Mobile-Security-Framework-MobSF">https://github.com/ajinabraham/Mobile-Security-Framework-MobSF</a>	Attaque MITM
Installé via YMI/are	Fastidieuse et pas forcément facile du premier coup (Nécessite KitKat)	Nécessite rootage
Intéressant et possible package et appli pen test	Intéressant mais pas réussi à installer correctement	Attaque Homme du milieu via NetHunter
<b>Android PI</b>	<b>bugtroid</b>	<b>LOIC</b>
Raspberry peut accueillir Android	<a href="https://play.google.com/store/apps/details?id=com.bugtroid.free.es&amp;hl=fr">https://play.google.com/store/apps/details?id=com.bugtroid.free.es&amp;hl=fr</a>	Attaque DDoS
Connexion Internet et fastboot à prioris pas accessible	Facile à installer via le play store (root)	Nécessite rootage
Intéressant mais pas encore au point. Moins pratique	Très complet et comprend un catalogue d'app	Attaque DDoS via Android rooté
<b>Pwn Pad/Phone</b>		<b>Melasploit DDoS</b>
Sur achat		Attaque DDoS
N'existe pas en version virtuelle		Nécessite rootage
Payant - Jamais pu le tester		DDoS puissant NetHunter

Figure 3: Partie du tableau récapitulatif de l'état de l'art  
Créé par l'auteur

Ci-dessus, nous présentons le « board control<sup>1</sup> » qui est un tableau récapitulatif de notre état de l'art. Il est à préciser que chaque section n'a pas la même couleur. Chacune représente un type d'information. Selon le type de pentest, certaines sont plus importantes que d'autres. Par exemple, en ce qui concerne l'OS Pentest, nous jugeons primordial de ressortir la différence entre le côté virtuel et le côté physique. En effet, dans le courant de notre recherche, nous avons décidé de créer deux mondes parallèles afin d'en comparer les différences. Dans un premier temps, nous avons créé un monde virtuel à l'aide de VmWare<sup>2</sup>. Le but était de pouvoir à moindre coup et sans matériel tester différents outils de pentesting. Ce point correspond spécifiquement au OS Pentest car si le système d'opération dispose d'une partie virtuelle, cela signifie que le package et l'application également.

<sup>1</sup> Il est disponible en entier sous la rubrique « 3 Tableaux » sous le nom BoardControl.xlsx

<sup>2</sup> Software permettant d'émuler des ordinateurs virtuels

Dans le cas du package Pentest, il est plus intéressant d’avoir à disposition le lien de téléchargement ainsi que des informations sur son installation. Il est utile d’avoir la possibilité de trouver rapidement son lien d’installation ce qui nous évite de le rechercher dans le dossier contenant tous les liens du projet. Dans un second temps, nous avons ajouté une partie correspondant à l’avancée de l’installation. Cela nous a permis d’avoir un point global sur la situation actuelle de la mise en place.

Pour finir, au niveau des applications, il est utile de savoir si le routage est nécessaire ainsi que la catégorie de l’application. Certaines applications ne nécessitant pas le rootage, nous trouvons essentiel de faire ressortir ce point. Le type d’application permet quant à lui de situer le software par rapport aux autres.

Vous trouvez ci-dessous un tableau qui correspond aux couleurs données ainsi qu’une explication concernant lesdites couleurs.

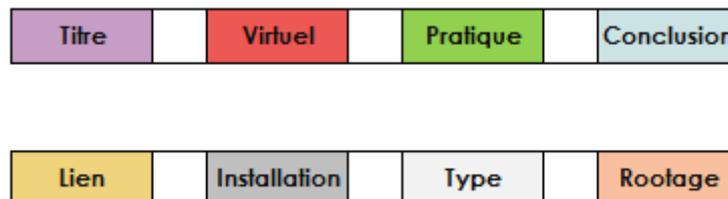


Figure 4 : Code couleur du tableau récapitulatif  
 Créé par l’auteur

- Titre : Nom du programme, package ou de l’application
- Virtuel : OS → Comment l’OS se comporte sur un environnement virtuel
- Pratique : OS → Comme l’OS se comporte sur un environnement physique
- Lien : Package → Le lien de téléchargement du package
- Installation : Package → Feedback sur l’installation du package
- Type : Application → La catégorie de l’application
- Rootage : Application → Si le routage est nécessaire pour l’application
- Conclusion : brève conclusion du programme, package ou de l’application

## 2.2. OS Pentest

### 2.2.1. Android Rooté

#### Physique

Le plus basique des frameworks à notre disposition est une rom Android rootée. Il s'agit d'un Android classique comme sur l'appareil de monsieur tout le monde, à la différence que nous le rootons afin de l'exploiter à 100%. Le root est expliqué lors de la phase de déploiement. C'est une manipulation spécifique à chaque appareil qui octroie à son utilisateur tous les droits comme lorsque l'on est en root<sup>3</sup> sous linux. Une fois cette opération effectuée, nous offrons la possibilité à notre téléphone ou à notre tablette d'accéder à des ressources insoupçonnées. Après avoir été débloqué, l'appareil acquiert une application nommée « SuperSU » qui s'installe automatiquement après le rootage du smartphone ou de la tablette. Avec « SuperSU », nous pouvons choisir si nous autorisons une application à s'exécuter en tant que root ou si nous l'en empêchons.



Figure 5 : SuperSU logos

<https://play.google.com/store/apps/details?id=eu.chainfire.supersu&hl=fr>

Il est important de comprendre qu'autoriser une application à accéder à certaines informations peut s'avérer dangereux pour l'utilisateur. C'est pourquoi il faut faire des recherches préalables sur celle que nous téléchargerons. L'exemple le plus parlant est lorsque certaines applications demandent la possibilité d'envoyer des messages. Effectivement, lors de l'installation d'une application, elle a l'obligation de vous avertir sur la

---

<sup>3</sup> Sous Linux, il existe un utilisateur nommé « Root » qui possède tous les droits et peut par conséquent faire tous ce qu'il veut et ce même au dépend de la machine.

portée de son contrôle. Or, lors d'un essai, une application voulait avoir l'autorisation d'envoyer des sms. Il s'agit très certainement d'un piège destiné à ruiner son utilisateur.

## Virtuel

Il existe des architectures Android spécifiques pour les machines virtuelles. Nous appelons ceci des Androidx86 en référence à l'architecture x86 propre aux ordinateurs. Nous avons rooté le smartphone virtuel à l'aide d'une ligne de commande<sup>4</sup> et en quelques secondes, notre dispositif était prêt et en fonction. Nous testons le dispositif sous plusieurs versions d'Android avec succès et pouvons valider la partie virtuelle de cette technologie. Nous restons cependant dépendant des technologies présentes en téléchargement sur internet et particulièrement sur le site d'Android-x86<sup>5</sup> qui en contient un grand nombre.

## Capture d'écran

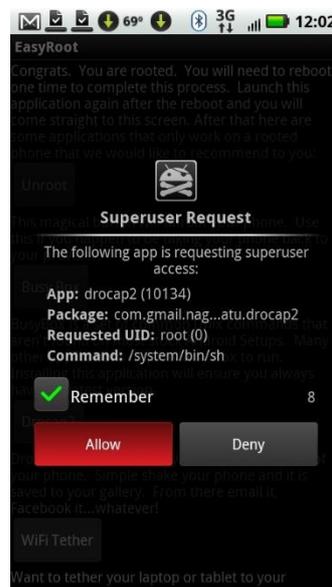


Figure 6 : Autoriser une application à utiliser le root  
[http://www.pcworld.com/article/205336/root\\_android\\_the\\_easy\\_way.html](http://www.pcworld.com/article/205336/root_android_the_easy_way.html)

## 2.2.2. NetHunter

<sup>4</sup> L'astuce est disponible à sous « 2 Tutoriaux » avec le nom « RootAndroidSousVMWare »

<sup>5</sup> <http://www.android-x86.org/download>

## Physique

NetHunter est une sorte de petit frère mobile de Kali Linux<sup>6</sup>. De part ce fait, NetHunter est certainement l'un des OS les plus professionnels à disposition gratuitement pour les pentesters mobile. Il est à noter que NetHunter a été fait en coopération entre Global Offensive et BinkyBear membre de la communauté de Kali. Il a été le premier projet Open Source à voir le jour pour les appareils Nexus de Google (Kali Linux NetHunter, 2016).

Les applications proposées par NetHunter sont les suivantes :

- Kali Services
- Custom commands
- MAC Changer
- VNC Manager
- HID Attacks
- DuckHunter
- Bad USB
- Mana Wireless Toolkit
- MITM
- NMAP
- Metasploit Payload Generator
- SearchSploit

Nous l'installerons sur notre tablette Nexus 7 (2012) mais il est également possible de l'installer sur de nombreux Android<sup>7</sup> tels que les OnePlus, Certains Samsung Galaxy<sup>8</sup>, Les tablettes NVidia SHIELD ainsi que pour le G5 de LG (Adduono, 2016).

---

<sup>6</sup> Kali Linux est une distribution Linux offrant la possibilité de pratiquer des tests de sécurité.  
<https://www.kali.org/>

<sup>7</sup> La liste complète est dans les annexes sous « 6 Divers » au nom de NetHunterDevices

<sup>8</sup> Galaxy Note 3 et le Galaxy S5



Figure 7: NetHunter sur une tablette Nexus  
<https://www.offensive-security.com/kali-linux-nethunter-download/>

Ce framework a l'avantage d'être toujours tenu à jour. En effet, le Github<sup>9</sup> contenant les roms a été modifié très récemment. Ce dernier explique par ailleurs clairement comment l'installer sur son appareil à condition qu'il fasse parti de la liste citée plus haut.

## Virtuel

Nous avons essayé d'installer NetHunter sous une forme virtuelle avec l'aide de VmWare mais également virtualBox malheureusement sans succès. Nous y reviendrons dans la partie mise en place, néanmoins, il faut s'avoir que le chemin pour installer NetHunter n'est pas disponible sur un environnement virtuel.

## Capture d'écran

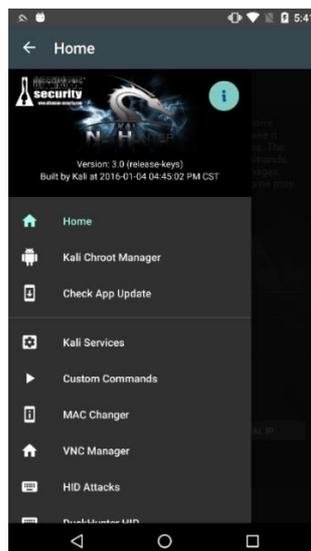


Figure 8 : NetHunter application  
<https://www.offensive-security.com/kali-nethunter/nethunter-3-0-released/>

<sup>9</sup> Github est une plateforme d'hébergement de projet grandement utile aux programmeurs.

### 2.2.3. CyanogenMod

#### Physique

CyanogenMod est le troisième framework analysé. CM comme on peut également l'appeler est l'une des customs roms les plus connues sur le marché. Elle a été installée plus de 10 millions de fois ! Certaines marques de téléphones tels que OnePlus fournit leurs smartphones directement avec ce framework installé (One Plus One, 2016).

#### Total Installs

Type	Total
Official Installs	5,518,845
Unofficial Installs	4,585,473
<b>Total Installs</b>	<b>10,104,318</b>

Figure 9 : Nombre de téléchargement CM

<http://www.romandroid.ch/discussions/cyanogenmod-passe-la-barre-des-10-millions-utilisateurs>

Cyanogenmod est disponible pour plus de 370 sortes d'appareils Android (Devices, 2014). Il a l'avantage d'être également présent sous différentes versions d'Android. Son installation est grandement facilitée par la quantité astronomique de tutoriel aussi bien sous forme écrite ou vidéo que l'on peut trouver sur Internet.



Figure 10: Logo de CyanogenMod

<http://www.androidpit.fr/cyanogenmod-nouveautes-compatibilites-fonctionnalites>

#### Virtuel

Pour la même raison que NetHunter, il est pour le moment impossible d'installer une version Cyanogenmod sur un environnement virtuel.

## Capture d'écran



Figure 11 : Screenshot Cyanogenmod 12

<http://www.androidauthority.com/best-cyanogenmod-themes-by-developer-586864/>

## 2.2.4. Android PI

### Physique et virtuel

Le Raspberry PI pourrait faire office de machine à café si on le lui demandait. C'est donc tout naturellement qu'il a été pris dans les mailles du filet lors de l'état de l'art. Un développeur Android du nom de Naren a commencé à travailler sur l'intégration d'Android sur le Raspberry PI en 2012 (Upton, 2012). Android PI<sup>10</sup> est toujours d'actualité malgré le peu d'informations sur le site du constructeur. Sa sortie sur le Raspberry PI 3 ne sera bientôt plus un rêve car il semble que Google veuille s'associer au projet (Amadeo, 2016).

Il reste néanmoins possible de télécharger des versions Android pour Raspberry sur internet. Elles ne sont cependant pas proposées par le constructeur et pour la plupart ne fonctionnent pas.

<sup>10</sup> Android PI est le nom donné à la version Android sur Raspberry PI



Figure 12 : Android PI  
<http://the-raspberry.com/android-sur-le-raspberry-pi>

Ayant été bloqué dans la phase virtuelle car peu de solutions au niveau Android existe, nous avons essayé d'étudier les possibilités d'Android, sur le Raspberry PI afin de pouvoir peut-être migrer la partie machine virtuelle sur ce micro-ordinateur. Toutefois, nous avons rencontré les mêmes problèmes que précédemment et avons du décider que la partie virtuelle se ferait uniquement sur Android rooté.

### Capture d'écran



Figure 13 : Android PI en version Android 4.0.3  
<http://www.pcp.com/news/General-Tech/Developer-Working-Porting-Android-40-ICS-Raspberry-Pi>

### 2.2.5. Pwn Pad

Pwn Pad est une tablette Nexus 7 vendue par l'entreprise Pwnie Express. Cette société a la particularité de proposer une tablette spécialisée avec un OS de pentest directement intégré. Elle est disponible pour la somme de \$ 995.- sur le site<sup>11</sup> de Pwnie Express. Elle est vendue avec plusieurs accessoires et avec plus de 100 outils de pentest inclus. Il existe également un Pwn Phone (Pwn Pad 2014, s.d.).

<sup>11</sup> <https://store.pwnieexpress.com/product/pwn-pad-2014-penetration-testing-tablet/>

Notre travail étant de rechercher des outils gratuits ou à bas coût, nous devons malheureusement la sortie du projet. Toutefois, il est intéressant de noter qu'il existe du matériel mobile de pentest déjà confectionné et prêt à l'emploi.



Figure 14 : Pwn Pad de Pwnie Express  
<https://store.pwnieexpress.com/product/pwn-pad-2014-penetration-testing-tablet/>

## 2.3. Package Pentest

### 2.3.1. Revenssis

Revenssis fait partie d'un type d'apk<sup>12</sup> très prisé par les spécialistes. Il regroupe un grand nombre d'applications et permet d'avoir une boîte à outils contenant la plupart des instruments utiles dans le cadre d'un test d'intrusion.

Le problème de ce dernier est qu'il n'est plus tenu à jour et que sa dernière version ne peut plus être ouverte. C'est dommage car la description du package sur sa page de téléchargement sourceForge ainsi que son nombre d'outils auraient été les bienvenus dans notre projet. Nous pouvons d'ailleurs observer ci-dessous la liste proposée à l'époque par revenssis :

- All Web Vulnerability Scanners including:
- SQL injection scanner
- XSS scanner

---

<sup>12</sup> Un .apk est une application pour Android. .apk correspond à l'extension de cette dernière

- DDOS scanner
- CSRF scanner
- SSL misconfiguration scanner
- Remote and Local File Inclusion (RFI/LFI) scanners
- Useful utilities such as:
  - WHOIS lookup, IP finder, Shell, SSH, Blacklist lookup tool, Ping tool,
  - Forensic tools (in imlementation) such as malware analyzers, hash crackers, network sniffer, ZIP/RAR password finder, social engineering toolset, reverse engineering tool
- Vulnerability research lab (sources include: Shodan vulnerability search engine, ExploitSearch, Exploit DB, OSVDB and NVD NIST
- Self scan and Defence tools for your Android phone against vulnerabilities
- Connectivity Security Tools for Bluetooth, Wifi and Internet. (NFC, Wifi Direct and USB in implementation) (Revenssis, 2014)

### Capture d'écran



Figure 15: Revenssis et toutes ses possibilités  
<https://sourceforge.net/projects/revenssis/>

### 2.3.2. Deploy Linux

Il s'agit d'une application téléchargeable sur le PlayStore de Google. Avec l'aide de ce software, la possibilité de démarrer Kali Linux sur un téléphone ou une tablette devient réelle. Cette application permettra d'émuler Kali Linux directement sur le smartphone mais nécessite un appareil mobile rooté. Comme le démontre cette vidéo<sup>13</sup> de Dave Bennett, c'est un moyen relativement rapide et à moindre coût qui permet à son utilisateur de faire des tests de pénétration avec l'un si ce n'est le meilleur OS linux de pentest gratuit sur le marché.

Nous n'avons pas été jusqu'à la phase de test pour cette technologie. Elle a été classifiée comme étant hors sujet et a par conséquent été abandonnée.

#### Capture d'écran

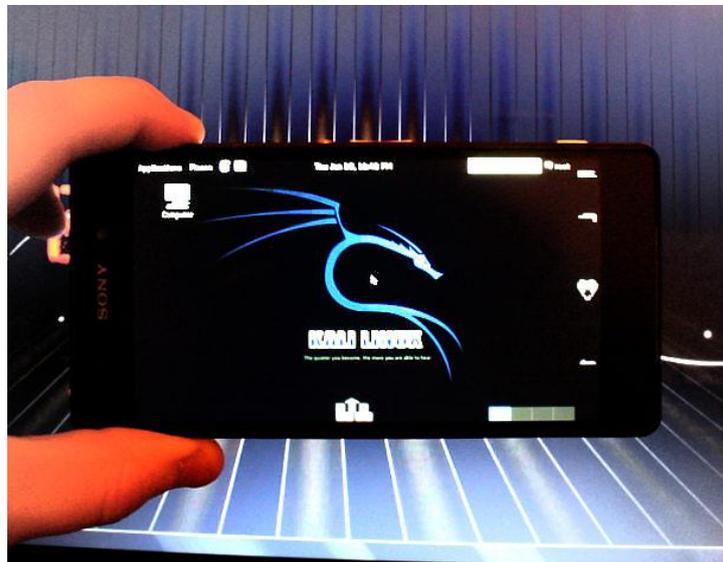


Figure 16 : Kali Linux sur un smartphone Android  
<http://www.couponbies.com/>

### 2.3.3. MobSF

<sup>13</sup> La vidéo est à l'url suivant : <https://www.youtube.com/watch?v=uZ2eDb9EjzE>

MoBSF de son nom complet Mobile Security Framework est un package open source de pentest automatisé. Il a été créé par Ajin Abraham un ingénieur en sécurité indien (Abraham, 2016). Nous avons découvert le logiciel en arrivant sur le github de MobSF. Il a le grand avantage d'être tenu très régulièrement à jour. De plus, dans cette page github, un wiki est aussi mis à disposition où nous avons pu suivre les différents tutoriaux disponibles pour l'installation de ce package.



Figure 17 : Logo de MobSF designé par Amrutha VC  
<https://github.com/ajinabraham/Mobile-Security-Framework-MobSF>

#### 2.3.4. Bugtroid

Bugtroid fait office d'annuaire téléphonique pour les logiciels de pentest. C'est un package pour Android rooté qui centralise plus de 200 applications (Bugtroid Pentesting pro, 2013). Afin de mieux trouver celle recherchée, Bugtroid contient deux répertoires principaux :

- Android Pentest
  - o Catégories : Anonymity, 802.11, Brute Force, DDOS, Crypto, Forensics, Networking, Pentesting, Peoplesearch, Remote, Scripting Security, Sniffers, System, Web et Av's
- Linux Pentest
  - o Catégories : Web, Anonymity, 802.11, Brute force, DDOS, Networking, Pentesting, Remote, Security, Sniffers, Crypto et System

Il est à noter que pour pouvoir utiliser la partie Linux Pentest ainsi que pour télécharger les applications directement depuis l'application, l'utilisateur doit posséder la version pro qui coute CHF 5.30 sur le PlayStore de Google.



*Figure 18 : Logo de l'application BugTroid Pro  
<http://bugtraq-team.com/bugtroid>*

BugTroid Pro permet par conséquent de découvrir un grand nombre de software mobile de pentesting. De l'autre côté, sous Linux Pentest, l'utilisateur peut télécharger des fichiers contenant des outils de pentest pour Linux.

Notre but étant de trouver des applications gratuites nous choisissons de conserver Bugtroid dans sa forme gratuite. Ce package nous sera nécessaire pour trouver les applications intéressantes du Playstore.

### **Capture d'écran**



Figure 19 : Application BugTroid  
<http://playboard.me/android/channels/55ad8532ea9e19f71cee60ec>

### 2.3.5. PenTest Tools

#### Introduction

Au même titre que Bugtroid, c'est une application que nous avons découverte sur le PlayStore de Google. Il s'agit d'un package gratuite qui redirige l'utilisateur vers plusieurs endroits proposant l'application sélectionnée. Elle a été téléchargée plus de 100'000 fois et possède une note de 4 sur 5 dans le PlayStore. Elle contient un répertoire de 221 applications (Pentest Tools List, s.d.).

#### Capture d'écran



Figure 20 : PenTest Tools est une application avec un design certain  
<http://playboard.me/android/channels/50bddb0809f27c623b000063>

## 2.4. Application PenTest

Il existe un grand nombre d'applications prévues pour le pentest, et qui nécessite pratiquement toutes un appareil rooté. Dans cette catégorie, Bugtroid fait office d'annuaire où chacune des entrées équivaut à une application.

### 2.4.1. Application de découverte réseau

La première catégorie d'applications que nous pouvons ressortir sont celles de type « découverte réseau ». C'est un premier pas que doit faire tout pentester dans le but d'acquérir des informations sur l'architecture du réseau. Il en existe beaucoup mais aucune n'est comparable à NMAP. Nous avons commencé par le tester car il est un acteur très connu de la découverte réseau. Nous pouvons utiliser une telle application aussi bien lors d'une white box que d'une black box. Il est à prendre en compte que ce genre d'application prend plus son sens lors d'une black box. L'attaquant ne connaissant rien du réseau, une

application telle que NMAP permettra à son utilisateur de découvrir l'architecture qu'il doit attaquer.

### **NMAP NetHunter et NMAP Android**

Il s'agit d'une solution open-source créée par Gordon « Fyodor » Lyon. NMAP est un outil gratuit de découverte du réseau (NMAP Sécurité scanner, s.d.). Nous avons déjà eu l'occasion de nous en servir lors de projet précédant par le biais de Kali Linux.



Figure 21 : Logo de NMAP

[https://home-assistant.io/components/device\\_tracker.nmap\\_scanner/](https://home-assistant.io/components/device_tracker.nmap_scanner/)

NMAP est certainement le mappeur le plus connu et l'un si ce n'est le meilleur du marché. C'est pourquoi nous l'avons sélectionné dans nos choix de recherche. De plus, il est disponible sur Nethunter mais également sur l'Android rooté. Son design sur ces deux derniers OS paraît tout de même un peu archaïque mais sa puissance de recherche est incroyable. Sous la rubrique capture d'écran, nous vous proposons un exemple de recherche NMAP sur une ligne de commande NetHunter.

### **Capture d'écran**

```

1) No title
root@kali:~# nmap -T 3 -sS -sV scanme.nmap.org -p80
Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-05 02:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.082s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.68 seconds
root@kali:~#

```

Figure 22 : NMAP avec NetHunter<sup>14</sup>  
<https://vimeo.com/150745391>

Sous NetHunter, nous avons un grand nombre d'option avancée disponible telles que

- Enable OS Versiondetect, scriptscan, and traceroute
  - Raccourci en ligne de commande : -A
    - Propose une estimation de l'OS ciblé
    - Un traceroute vers la cible
- Ping Scan
  - Raccourci en ligne de commande : -sn
    - Ping la cible
- Service/Version Detection
  - Raccourci en ligne de commande : -sV
    - Retourne l'OS de la cible ainsi que son CPE<sup>15</sup>
- Enable OS Detection
  - Raccourci en ligne de commande : -O
    - Donne un pourcentage de probabilité de l'OS de la cible
- Enable IPv6
  - Raccourci en ligne de commande : -6
    - Permet de lancer le scan avec une adresse IPv6
- Ports

<sup>14</sup> Il s'agit également d'une courte vidéo hébergée sous <https://vimeo.com/150745391>

<sup>15</sup> Common Platform Enumeration. Exemple : cpe:/o :microsoft:windows

- Permet de gérer les ports scannés
- Timing template
  - Permet de gérer le style de scan
    - Paranoid, sneaky, polite, normal, aggressive, insane<sup>16</sup>
- Scans techniques
  - Possibilité de choisir quelle technique de scan nous effectuons
    - TCP SYN, Connect(), ACK, Windows, Maimon, TCP Null, FIN, XMAS
    - La possibilité de faire un scan UDP

Sous L'Android rooté, il existe peu d'option. L'utilisateur peut uniquement insérer l'IP et les éventuels arguments.

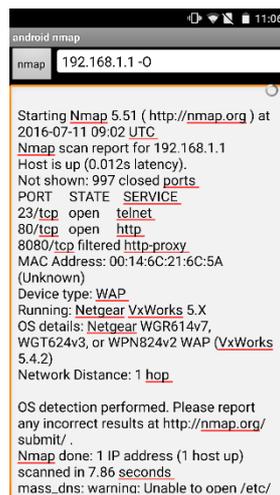


Figure 23 : Interface NMAP Android  
Créé par l'auteur

## Pamn IP Scanner

Il s'agit d'une application utilisant également NMAP qui est disponible sous le PlayStore de Google pour la modique somme de CHF 2.66. Il s'agit d'une application complète contenant un historique des précédents scans et également un bouton exécutant la commande -h<sup>17</sup>. Son design est épuré et très ergonomique.

<sup>16</sup> Dans le CD, vous avez accès à l'explication de ces différents timing templates sous « 6 Divers » avec le nom NMAPTimingTemplate

<sup>17</sup> NMAP [IP] -h affiche les options possibles avec NMAP



Figure 24 : Pamn IP Scanner Application  
Créé par l'auteur

## Zanti

Zanti est une application Android dont l'.apk est disponible sur le site du constructeur gratuitement<sup>18</sup>. Il réalise un scan du réseau à l'aide de NMAP comme les différents outils susmentionnés. Il possède également un historique des scans précédents ce qui permet de ne pas avoir besoin de constamment relancer un même scan. Il propose une rubrique commentaire afin de laisser un message en mémoire.

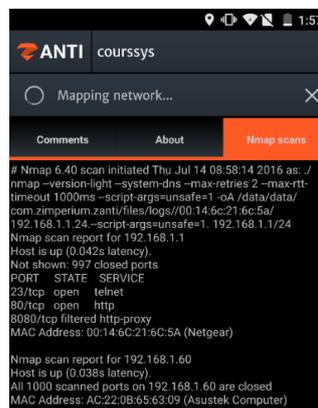


Figure 25 : Scan NMAP avec Zanti  
Créé par l'auteur

## Fing

Fing est une application de mappage réseau. Elle permet à l'instar d'un NMAP de créer une carte des appareils connectés sur le réseau. Elle est disponible depuis le PlayStore de

<sup>18</sup> L'.apk en question est également disponible sous « 6 Divers » avec le nom ZantiAPK

Google. Elle se trouve également sur les deux packages cités plus haut. Elle permet de ressortir les ports ouverts après un second scan de l'adresse IP de la cible.



Figure 26 : Scan sur l'application Fing  
<https://www.androidpit.com/app/com.overlook.android.fing>

## 2.4.2. Application d'attaque Man In The Middle

La seconde catégorie que nous analyserons dans le cadre de ce travail se nomme application d'attaque Man In The Middle. Une fois l'architecture analysée, il est possible de réaliser des attaques sur cette dernière afin de s'assurer de la protection actuelle. Le MITM peut faire de gros dégâts à une entreprise. Il est important de sensibiliser son personnel à cette dernière et mettre les moyens afin de se protéger au mieux. Une attaque Man In The Middle est interdite par la loi que ce soit en Suisse ou dans le monde entier, l'attaquant risque une lourde amende et de la prison. En effet, la loi n'autorise pas l'intrusion sans le consentement de la victime (kenmaster, 2016).

MITM est l'abréviation de Man In The Middle ou en français l'attaque de l'homme du milieu. Il s'agit d'une attaque informatique où l'attaquant se place entre deux communications. Il peut ainsi voir les informations transitées et également les modifier (Attaque man in the middle, s.d.).

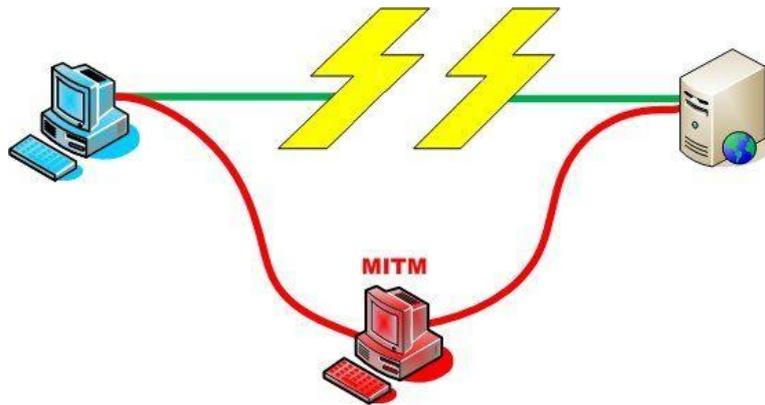


Figure 27 : L'attaque de l'homme du milieu

<http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/informatique-attaque-man-in-middle-10048/>

## MITMF

MITMF ou littéralement Man In The Middle Framework est disponible sous Nethunter. L'utilisateur peut connaître les déplacements de sa victime et selon la protection de ses mots de passe, les décrypter rapidement.

## Capture d'écran

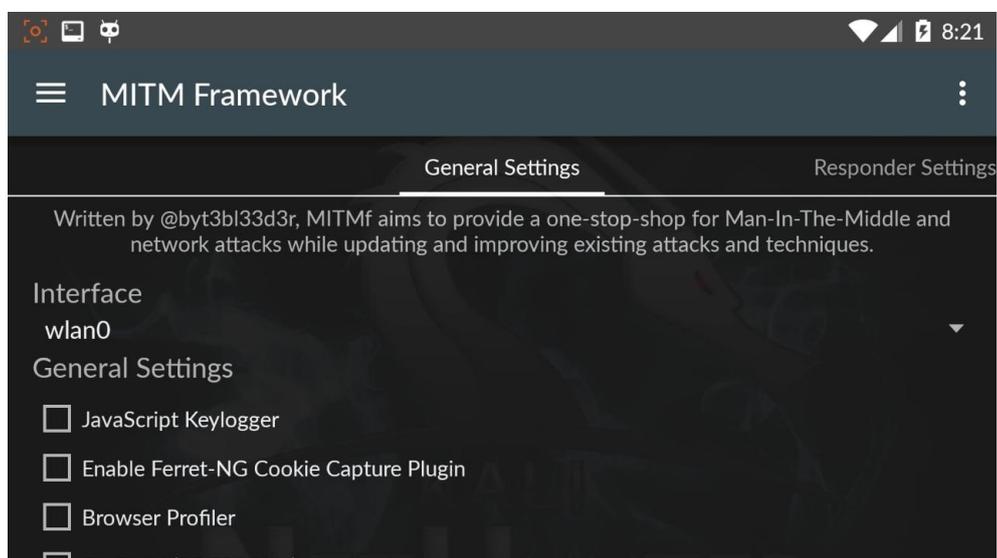


Figure 28 : Man In The Middle sous NetHunter  
<https://vimeo.com/150745388>

MITMF possède plusieurs catégories de paramètre<sup>19</sup>. A chaque ajout, NetHunter modifie les arguments de sa ligne de commande afin de proposer le résultat désiré. Il existe :

- General Settings
  - Interface, General Settings et Screenshooter
- Responder Settings
- Inject Settings
- Spoof Settings
- MITMf Configuration

Dans notre cas, nous avons surtout besoin d'utiliser le spoof settings où nous devons modifier la target ainsi que la gateway. Il nous faut aussi vérifier l'interface sous général settings.

## Zanti

Il s'agit de la même application citée dans la partie découverte réseau. Elle permet également, une fois le scan NMAP réalisé, d'attaquer sa cible avec un Man In The Middle. Il dispose de plusieurs possibilités tels que :

- MITM Method
  - Changer le type de paquets scannés (ICMP ou ARP)
- SSL Strip
  - Permet de forcer la victime à utiliser un lien non sécurisé (http au lieu https)
- Redirect http
  - Redirige la requête http sur l'IP de l'attaquant
- Replace Images
  - Remplace les images de tout le browser par une image définie au préalable
- Capture download

---

<sup>19</sup> Sous « 2 Tutoriaux », nous avons inséré une explication de MITMf pour NetHunter. Il porte le nom MITMfNetHunter

- Capture le téléchargement de la victime et le télécharge automatiquement chez l'attaquant
- Intercept download
  - Remplace le fichier téléchargé de la cible par un défini au préalable
- Insert HTML
  - Insert du code HTML au début de chaque page ouverte par la cible.

### 2.4.3. Application d'attaque DDoS

Dans notre troisième et dernière rubrique, nous parlons des applications d'attaque DDoS. DDoS signifie Distributed Denial of Service en anglais. En français, il s'agit d'une attaque de déni de service distribué (Attaque DDoS, 2015). Le but est de rendre un service en ligne indisponible. Il est possible d'acheter pour une semaine une attaque DDoS sur le marché noir pour \$ 150.-. Chaque jour plus de 2'000 attaques par déni de service sont observées par Arbor Networks<sup>20</sup> (What is a DDoS Attack, 2013). Le principe est simple mais diablement efficace. Il suffit d'inonder un site de requêtes afin de le faire tomber et occasionner des problèmes à la cible. Par exemple, nous savons qu'en 2014, Facebook a été victime d'une attaque DDoS provenant de la Chine. Durant 30 minutes, le réseau social fut indisponible (Polo, 2014).

#### DDoS Metasploit

Il est possible depuis la ligne de commande Kali Linux disponible sous NetHunter de réaliser une attaque DDoS. A l'aide de la commande `msfconsole`<sup>21</sup>, il suffit de définir une cible et de lancer une attaque DDoS. Il est possible de régler plusieurs paramètres utiles tels que :

- L'interface utilisée
- Le nombre de requête envoyé à la cible
- L'IP de la cible

---

<sup>20</sup> Solution de protection DDoS (<http://fr.arbornetworks.com/>)

<sup>21</sup> Commande Kali Linux permettant d'accéder à metasploit

- Le port de la cible

```
# cowsay++  
  
< metasploit >  
-----  
      \   ('oo)_____  
         (__)      )\  
          ||--||  *
```

Figure 29 : Metasploit est disponible en ligne de commande  
Créé par l'auteur

## LOIC

LOIC ou Low Orbit Ion Cannon est un outil disponible sous Bugtroid dans le répertoire Ddos. Il offre la possibilité à son utilisateur de réaliser une attaque de déni de service rapidement à l'aide d'une application Android.

Dans un premier temps, nous définissons l'adresse IP de la cible et dans un second temps, nous gérons les options de l'attaque. Une fois ces deux paramètres définis, nous pouvons lancer l'attaque à l'aide du bouton « Fire ».

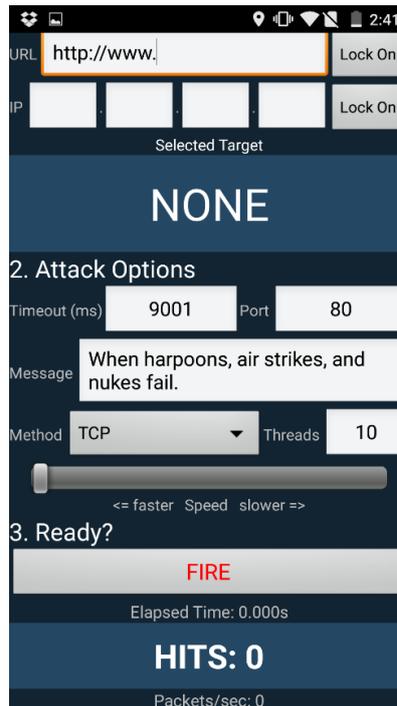


Figure 30 : Interface de LOIC  
Cr  e par l'auteur

## AnDOSid

AnDOSid est en t  l  chargement via nos deux packages. C'est un outil r  serv   aux testeurs d  sirant s'assurer de la solidit   de leur site internet. Il n'est pas possible de r  aliser le ping d'une machine avec ce software. Il est sp  cifique et n'accepte que les adresses URL des victimes.



Figure 31 : Logo d'AnDOSid  
Cr  e par l'auteur

### 3. Déploiements et évaluations des solutions

Dans la partie dite de déploiements et évaluations des solutions, nous vous présentons l'installation des différents outils relaté, dans l'état de l'art. Nous introduirons l'aspect de root ainsi que la façon de rooté les appareils à notre disposition.

En guise de conclusion de cette phase, nous évoquerons les décisions prises quant aux 2 OS, 2 Packages et 3 types applications conservés pour la suite du projet.

#### 3.1. Installation OS Pentest

##### 3.1.1. Android Root

###### Root

Dans un premier temps, il est nécessaire de « rooter » le smartphone ou la tablette utilisé. Le mot rooter vient du terme root qui correspond à l'utilisateur suprême. L'utilisateur qui n'a aucune restriction et qui peut par conséquent faire tout ce que bon lui semble. Il reste toutefois dangereux pour des néophytes d'accéder à un appareil par le biais de cet utilisateur. En effet, l'atout majeur de cette manipulation est de pouvoir accéder à la totalité de son appareil mais l'utilisateur peut dans cette configuration casser de manière irrémédiable son dispositif. Il est par conséquent conseiller de ne pas réaliser des choses inconnues ou non maîtrisées avec une machine rooté. Cette dernière présente un autre point négatif qui est d'échoir la garantie de votre appareil. Pour terminer, c'est une manipulation technique et de ce fait n'est pas facile à réaliser sans aide ou tutoriaux. (El\_FuerTos, 2012)

Dans ce chapitre, nous détaillerons le root du smartphone HTC M7 ainsi que la tablette Nexus 7 (2012). Les différents tutoriaux utilisés pour la réalisation du rootage de ces appareils sont cités en lien de bas de page. Nous ajoutons à cette thèse des informations utiles qui nous ont permis de débloquent nos deux appareils mobiles.

Une fois l'appareil rooté, il faudra installer la « custom rom » sur le smartphone ou la tablette. Une « Custom rom » est un OS Android modifié qui peut être traduit en français par ROM personnalisé ou alternative. En soi, il n'est pas nécessaire de rooter son téléphone ou sa tablette pour installer une « Custom rom ». Néanmoins, lesdites ROM personnalisées peuvent demander d'accéder à des données disponibles uniquement pour un dispositif rooté. (Balt, 2016)

Une ROM alternative permet de changer le design d'un appareil Android mais peut également embarquer plusieurs applications utiles et qui ne seront disponibles que sur cet OS.

### HTC M7

Le One M7 de HTC est un smartphone sorti par la marque taïwanaise en avril 2013. Il est apparu sous Android 4.3. Il s'agit du premier téléphone HTC de la gamme One (htc, s.d.).



Figure 32 : HTC One M7  
<http://www.htc.com/fr/smartphones/htc-one-m7/>

HTC propose un système de rootage différent des autres smartphones. Il faut passer par le site HTC dev<sup>22</sup> qui vous permettra de déverrouiller votre HTC. Pour faire cette manœuvre, vous devez suivre le tutoriel présent dans les annexes<sup>23</sup>.

Ce tutoriel est l'un des meilleurs pour le rootage du HTC M7. Le tutoriel est divisé en deux parties identiques, il est possible de le suivre via une vidéo ou simplement avec des images. Il explique également l'installation de TWRP<sup>24</sup> qui est un recovery<sup>25</sup> efficace et possédant un design certain.

### **Nexus 7 (2012)**

La tablette Nexus 7 de Google a été créée par ce dernier mais produite par Asus (Graff, 2015). Elle est apparue sous Android 4.1.1. C'est une tablette agréable à l'utilisation avec son écran 7 pouces, elle n'est ni trop grande ni trop petite.



Figure 33: Nexus 7 (2012)

<http://www.lesnumeriques.com/tablette-tactile/google-nexus-7-p13744/test.html>

Le tutoriel est disponible sur la vidéo de Souvik Biswas<sup>26</sup>. Il permettra de débloquent le bootloader<sup>27</sup> ce qui est une partie essentielle du rootage de notre dispositif.

<sup>22</sup> <https://www.htcdev.com/>

<sup>23</sup> Le tutoriel est disponible sous « 2 Tutoriaux » avec le nom RootHTCM7

<sup>24</sup> Team Win Recovery Project est le meilleur recovery testé

<sup>25</sup> Le Recovery offre la possibilité d'installer des roms, effacer les données, réaliser un backup et plus encore

<sup>26</sup> Lien de la vidéo : [https://www.youtube.com/watch?v=GbRiSfj\\_1e0](https://www.youtube.com/watch?v=GbRiSfj_1e0)

Il faut tenir compte de la version de l'Android rootée. En l'occurrence dans le cas du Nexus 7 susmentionné, elle se trouve sous Marshmallow (Android 6). Il faut également bien tenir compte du matériel choisi. Typiquement, le Nexus 7 (2012) comporte le piège d'avoir une petite sœur portant le même nom mais qui est sortie en 2013. La version wifi de cette dernière fonctionne avec notre tablette mais pas la seconde version.

### 3.1.2. Nethunter

Dans un premier temps, son installation s'est faite sur le Nexus 7 (2012) à disposition pour le projet. L'installation a été un succès pour la partie pratique, malheureusement aucune rom n'a été trouvée pour la partie virtuelle. Que ce soit sur VMWare ou sur VirtualBox, il n'existe pour l'heure aucune solution NetHunter. Nous avons également essayé d'accéder au Fastboot virtuel afin de pouvoir l'installer à l'instar d'un appareil physique mais nous avons rencontré un problème à ce niveau. Le Fastboot<sup>28</sup> est inatteignable sur une architecture Android X86<sup>29</sup> et par conséquent nous n'avons pas pu atteindre le recovery et installer NetHunter sous un environnement virtuel.

La partie physique a été une formalité au niveau de l'installation. Nous avons la chance de posséder un Nexus qui fait partie des tablettes concernées par la solution portable de Kali Linux. Nous accédons au recovery de la machine et lançons l'installation. Quelques minutes plus tard, nous sommes en possession d'une tablette sous NetHunter.

### 3.1.3. Cyanogenmod 12

---

<sup>27</sup> Le bootloader correspond au BIOS d'un smartphone. Depuis ce dernier, vous pourrez vous diriger dans le recovery

<sup>28</sup> Le Fastboot permet d'avoir accès à son téléphone sans pour autant le démarrer réellement. Il s'agit d'un mode accessible depuis le bootloader.

<sup>29</sup> Un Android X86 est une solution Android prévu pour les ordinateurs et de ce fait pour les machines virtuelles. On peut retrouver plusieurs .iso ou .img à cet url <http://www.android-x86.org/download>

Il est primordial pour l'installation de Cyanogenmod d'avoir un appareil rooté. Dans notre cas, nous avons installé cette custom rom sur le HTC M7. Nous avons eu certains problèmes de compréhension car il est à prendre en compte que la custom Rom doit être faite pour le bon appareil et la bonne version<sup>30</sup>. Nous avons installé un CM12 HTC M7 mais avec la mauvaise version d'Android<sup>31</sup>. Le smartphone paraissait cassé mais nous avons pu atteindre le recovery via le bootloader et réinstaller la bonne custom rom.

En finalité, il s'agit de la même formalité que NetHunter. Il suffit d'avoir la bonne custom rom et de l'installer via le recovery.

Il faudra toutefois prévoir un fichier .zip supplémentaire à installer. Nous faisons référence au gAPP<sup>32</sup>. Une fois l'installation de CM12 terminée, nous avons perdu tous nos outils Google dont le PlayStore. Il est possible de télécharger ce fichier sous le site de opengapps<sup>33</sup>. Comme susmentionné, il est impossible pour l'heure d'installer Cyanogenmod sur un environnement virtuel étant donné que nous ne pouvons accéder au recovery.

#### 3.1.4. ANDROID PI

Son installation ne nécessite pas énormément de ressources. Nous nous sommes équipés d'une carte microSD ainsi que du Raspberry PI 3 (Victor, s.d.). Plusieurs OS circulent sur internet mais peu sont exploitables. Deux OS Android PI étaient défectueux. L'essai a été réalisé sur deux Raspberry distincts<sup>34</sup> afin d'en avoir le cœur net. Par la suite, un OS d'Android PI a fonctionné avec Cyanogenmod<sup>35</sup> et de surcroît rooté. Cependant, cette version comporte un grand nombre de ralentissement au point qu'elle était pratiquement inutilisable. Enfin pour terminer, via Bootberry<sup>36</sup> qui est un écran de sélection de boot, il a

---

<sup>30</sup> En effet, il faut trouver sur internet une custom rom correspondante à votre smartphone ainsi qu'à sa version. Nous avons dû trouver une rom pour HTC M7 sous Lollipop.

<sup>31</sup> Lollipop (Android 5) au lieu de Marshmallow (Android 6)

<sup>32</sup> Google Application. Tutoriel d'installation sous « 2 Tutoriaux » avec le nom InstallerGoogleApps

<sup>33</sup> <http://opengapps.org/?api=6.0&variant=nano>

<sup>34</sup> Une fois sous le Raspberry PI 1B et une fois sous le Raspberry PI 3B

<sup>35</sup> Il est disponible sur l'adresse suivante : [http://androidpi.wikia.com/wiki/Android\\_Pi\\_Wiki](http://androidpi.wikia.com/wiki/Android_Pi_Wiki)

<sup>36</sup> Il est possible de télécharger gratuitement Bootberry sous ce lien :

été possible d'installer Android KitKat non rooté. Il y avait peu de ralentissement à noter hormis lors d'effets tels que le déverrouillage.

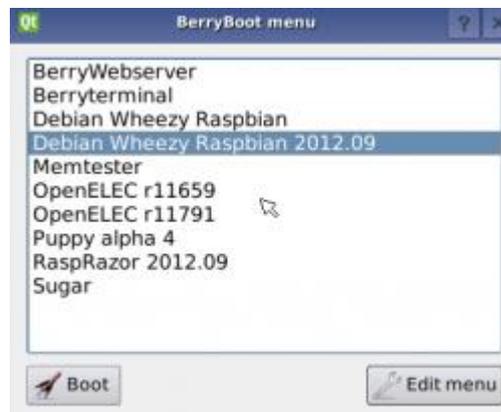


Figure 34 : Menu boot Berry à son démarrage  
<http://www.berryterminal.com/doku.php/berryboot>

Une fois l'installation effectuée, nous avons tenté d'accéder au bootloader et directement au recovery pour modifier la custom rom Android Kitkat que nous possédions. Encore une fois, nous sommes arrivés à la conclusion après plusieurs heures de recherches que ces modes n'existaient pas sur le Raspberry PI version Android.

## 3.2. Installation Package Pentest

### 3.2.1. MOBSF

Le framework avait l'air de présenter une solution de pentesting pour Android et ios. C'est après avoir tenté plusieurs fois son installation que nous avons découvert qu'il ne s'agissait peut-être pas exactement du package auquel nous pensions. Afin d'en être certain, nous avons contacté M. Ajin Abraham par e-mail<sup>37</sup> afin de bien comprendre les possibilités de son application open-source. Dans sa réponse, il indique la possibilité d'utiliser un smartphone ou une tablette pour réaliser des tests dynamiques. Ceux-ci sont démarrés

---

<http://www.berryterminal.com/doku.php/berryboot>

<sup>37</sup> Conversation avec M. Ajin Abraham sous « 6 Divers » avec le nom EmailAjinAbraham

depuis un appareil mobile. Cependant les résultats apparaissent obligatoirement sur un ordinateur contenant toute l'architecture MobSF.

Nous avons pris la décision de le considérer comme hors sujet étant donné qu'un ordinateur était nécessaire pour la bonne marche des tests d'intrusions.

### **3.2.2. BUGTROID et Pentest tools**

L'installation est rapide et simple à effectuer. Nous les avons trouvés sous le PlayStore et les avons téléchargés comme n'importe quelle application. En ce qui concerne Bugroid, nous avons téléchargé la version gratuite.

### **3.2.3. Revenssis**

Comme susmentionné dans l'état de l'art, nous avons installé le package<sup>38</sup> sur notre smartphone. Malheureusement, une fois lancée, l'application nous a notifié qu'elle n'était plus tenue à jour. Aussi, nous avons pris la décision d'abandonner ce package.

## **3.3. Installation application Pentest**

### **3.3.1. NMAP**

NMAP est téléchargeable gratuitement sur PenTest Tools pour les Android rootés.

NMAP fait également partie du package NetHunter une fois ce dernier installé et ce à moindre coût.

### **3.3.2. Pamn IP Scanner**

Pamn IP Scanner coûte CHF 2.66 sur le PlayStore de Google.

### **3.3.3. FING**

---

<sup>38</sup> Le .apk est disponible à cette adresse : <https://sourceforge.net/projects/revenssis/>

Fing est disponible gratuitement sur le PlayStore

### **3.3.4. Zanti**

Afin de télécharger Zanti, nous avons été sur le site internet<sup>39</sup> du fabricant. Il suffit d'insérer son email et Zanti nous envoie gratuitement son .apk<sup>40</sup>. Une fois reçue, nous l'avons installée sur notre smartphone rooté.

### **3.3.5. MITMF**

MITMF est une application qui apparaît uniquement dans NetHunter dans le package ajouté lors de son installation. Il n'est pas possible de le faire depuis un Android rooté.

### **3.3.6. Metasploit**

Metasploit est présent dans la ligne de commande de commande Kali Linux dans NetHunter par le biais de la commande msfconsole.

### **3.3.7. LOIC**

L'application LOIC est disponible directement depuis le package Bugtroid et Pentest Tools. Attention, il existe une application portant le même nom sur le PlayStore mais moins performante.

### **3.3.8. AnDOSid**

L'application AnDOSid est disponible via nos deux packages sous la rubrique DDoS pour Bugtroid et Denial of Service sur PenTest Tools

---

<sup>39</sup> <https://www.zimperium.com/zanti-mobile-penetration-testing>

<sup>40</sup> Son .apk est également disponible dans sur le CD dans la rubrique « 6 Divers » avec le nom ZantiAPK

### 3.4. Décision

Nous présentons sous ce point nos choix découlant des découvertes faites lors de l'état de l'art ainsi que la phase de mise en place. Pour rappel, nous avons décidé de ressortir 2 OS, 2 packages et 3 types applications. Chaque catégorie sera divisée en deux sous-catégories. La première sous-catégorie correspond aux choix retenus et la seconde à ceux écartés. Dans ceux retenus, nous insérons un tableau d'avantages et de désavantages afin de permettre aux lecteurs de se remémorer les points importants de chaque technologie. Nous y écrivons également un avis personnel sur la technologie. Dans les choix écartés, nous expliquons notre prise de position et pourquoi nous avons choisi de sortir la technologie de la suite de l'analyse.

#### 3.4.1. OS Pentest – Choix retenus

##### Android Rooté

Avantages	Inconvénients
Aucune custom rom à trouver	En cas de problème, l'appareil peut devenir inutilisable
Android rooté peut s'exécuter sur une interface virtuelle	Le niveau de complexité du rootage dépend de l'appareil
Donne accès à des apps de pentesting	
Design smartphone et portatif	

Tableau 1 : Avantages et inconvénients de l'Android rooté

Il s'agit de la solution la plus basique mais permet de grandes possibilités. Le potentiel d'un Android rooté au niveau du pentest nous encourage à le conserver dans nos choix en vue d'une étude poussée.

## NetHunter

Avantages	Inconvénients
Gratuit	Nécessite de rooter l'appareil
Orienté Pentest	Installation impossible sur des appareils autres que susmentionnés
Terminal Kali Linux qui permet l'utilisation de certaines commandes de pentest	Incompatible avec la virtualisation
Bonne prise en main avec le Nexus 7 (2012) <sup>41</sup>	
Régulièrement mis à jour par les développeurs	

Tableau 2 : Avantages et inconvénients de NetHunter

Notre choix s'est vite tourné vers NetHunter car nous avons déjà eu la chance de travailler avec son grand frère Kali Linux en matière de pentesting. Sans les citer à nouveau, ses nombreux avantages nous ont convaincu de le faire passer à une phase d'analyse approfondie.

### 3.4.2. OS Pentest – Choix écartés

#### Cyanogenmod

Cyanogenmod fut la première custom rom testée. A la découverte du monde du pentest mobile, il fallait commencer quelque part afin de pouvoir créer une première expérience. Il a nécessité de rooter le HTC M7 qui était à disposition. Cette première étape, bien que peu concluante car Cyanogenmod n'est absolument pas un OS de pentest, nous aura permis de faire nos premiers pas dans l'architecture d'un smartphone Android. Cyanogenmod n'a d'ailleurs pas été jeté à la poubelle. En effet, il est encore utilisé dans le cadre de l'Android rooté. Il est arrivé durant le projet de devoir « Downgrader » une version Android afin de

<sup>41</sup> Tablette utilisée dans le cadre du travail de bachelor

passer d'Android Lollipop à Android Kitkat et c'est en grande partie avec l'aide de Cyanogenmod que cela a pu être fait. Cyanogenmod existe en effet en plusieurs versions disponibles et téléchargeables sur Internet ce qui facilite grandement la vie des testeurs (Cyanogenmod downloads, 2016).

Pour revenir au refus de Cyanogenmod, il s'agit d'un OS prévu pour le design. Il permet à ses utilisateurs de customiser son smartphone ou sa tablette mais ne nous donne pas la possibilité de faire du pentesting uniquement grâce à lui.

### Android PI

C'est après ce travail d'analyse et de recherche que le Raspberry a paru moins utile que premièrement estimé. L'idée était de pouvoir accéder au fastboot comme sur un mobile physique ce qui aurait permis au Raspberry de devenir la partie virtuelle du travail. Malheureusement, il fut impossible d'accéder à ce fameux fastboot et par conséquent pouvoir installer des customs roms. D'autant plus que ces derniers sont prévus pour un type d'appareil précis sur une version précise. Toutefois, il existe des OS de pentests dédié à Raspberry PI tels que Kali Linux ou Parrot Security. Nous avons considéré ces OS comme hors projet vu qu'il ne s'agissait pas d'un mobile ou d'une tablette.

### 3.4.3. Packages Pentest retenus

#### Bugtroid

Avantages	Inconvénients
Grande base d'application de pentest	La version pro coûte CHF 5,30
Installation rapide et facile d'.apk	Android rooté
Linux Pentest (Pro)	
Bien trié avec les catégories	

Tableau 3 : Avantages et inconvénients de Bugtroid

C'est une sorte de mine d'or pour ce travail de bachelor. La possibilité est offerte de tester un grand nombre d'applications depuis un Android rooté. Une analyse profonde est requise afin de pouvoir ressortir de ce package un maximum d'applications intéressantes pour notre futur smartphone/tablette de pentest.

### PenTestTools

Avantages	Inconvénients
Grande base d'application de pentest	Design réduisant la lisibilité
Installation rapide et facile d'.apk	
Gratuite	
Tags permettant de trouver un type précis d'application	

Tableau 4 : Avantages et inconvénients PenTestTools

PenTest Tools ressemble à Bugtroid. Nous l'avons conservée car elle se démarque par son aspect entièrement gratuit. Nous trouvons également intéressant de pouvoir télécharger les .apk depuis des sites internet car ceux-ci ne sont pas forcément répertoriés sur le PlayStore et offre une plus grande sélection.

#### 3.4.4. Packages Pentest écartés

##### Revenssis

Revenssis est une suite de tests de pénétration. Il est composé de plusieurs outils qui ont dû être certainement très utiles aux pentesters d'autant plus qu'il s'agit d'.apk téléchargeables sur internet gratuitement. Toutefois, lors de son installation, le logiciel nous a vite fait comprendre qu'il n'était plus à jour et qu'il ne pourrait par conséquent pas s'exécuter. Il existe un site internet qui est également tombé aux oubliettes.

## Deploy Linux

Il s'agit d'une application disponible sur le PlayStore et permettant d'émuler un pc sous Linux, sur notre smartphone ou sur notre tablette. Il existe une version utilisable de Kali Linux qui aurait permis de réaliser des pentests de Kali depuis un environnement mobile. Cependant, l'application a été définie comme hors sujet car le but est d'utiliser des moyens adaptés aux appareils mobiles à disposition.

## MobSF

Le framework de Ajin Abraham avait été sélectionné car il présentait la possibilité de réaliser des tests également sur Android. Cependant, il ne s'agit que d'analyses dynamiques qui une fois effectuées sont lisibles uniquement depuis un ordinateur. Il est par conséquent placé dans la catégorie des hors thèmes.

### 3.4.5. Applications Pentest retenues

Nous avons présenté plus haut trois sortes d'applications. La découverte réseau, l'attaque MITM et l'attaque DDoS sont conservées dans le cadre de ce travail de bachelor. Nous analyserons l'ensemble des applications présentées dans l'état de l'art et la mise en place.

- Découverte réseau
  - NMAP NetHunter
  - NMAP Android
  - Zanti (NMAP)
  - Fing
- Attaque MITM
  - MITMf
  - Zanti (MITM)
- Attaque DDoS
  - DDoS Metasploit
  - LOIC
  - AnDOSid

### 3.5. Tableau récapitulatif des décisions

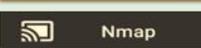
	OS PENTEST	PACKAGES PENTEST	APPLICATIONS PENTEST
Retenus	 Android Root  NetHunter	 Bugtroid  PenTest Tools List	Découvert réseau  Nmap  NMAP Android  Zanti  Pamn IP Scanner  FING
Ecartés	 Android Pi  Cyanogenmod	 MobSF  Renvessis	Attaque MITM  MITMf  Zanti
			Attaque DDoS  Metasploit DDoS  LOIC  AnDOSid

Figure 35 : Tableau récapitulatif des décisions<sup>42</sup>  
 Créé par l'auteur

<sup>42</sup> Tableau disponible sous « 3 Tableaux » avec le nom DecisionRecapitulatifBoard

## 3.6. Mise en place du laboratoire

### 3.6.1. Appareils à disposition

Comme mentionné au préalable, nous disposons d'un smartphone de chez HTC et une tablette Nexus. Ces deux appareils sont sous Android. Nous possédons également un Android x86 tournant sous VMWare. Il s'agit d'un Android Kitkat avec la version 4.4.4. De plus, afin d'effectuer les tests nous avons installé une machine virtuelle Windows 7 sous VMWare ainsi qu'un ordinateur physique de la marque HP.

Nous avons choisi de conserver NetHunter et l'Android rooté. NetHunter étant prévu pour les tablettes Nexus de Google, nous prévoyons de l'installer sur cette dernière. Quant au HTC M7 que nous avons, nous décidons d'utiliser sa partie rootée afin de réaliser nos tests.

Type	Marque	OS	Utilisation
Ordinateur	HP	Windows 10	Test
Ordinateur	Virtuel VMWare	Windows 7	Test
Smartphone	Virtuel VMWare	Android Kitkat	Test
Smartphone	HTC One M7	Android Lolipop	Pentesting
Tablette	Nexus 7 (2012)	NetHunter	Pentesting

Tableau 5 : Appareils à disposition

### 3.6.2. Réseau fermé

Afin de réaliser des tests dans un environnement sain et fermé , nous avons reçu un routeur de la marque Netgear. Ce dernier fait office de gateway<sup>43</sup> pour tous les appareils susmentionnés. Avant de commencer les différents tests, nous avons créé un plan d'adressage. Chacun des appareils s'y retrouve avec des informations complémentaires telles que :

- L'adresse IP

<sup>43</sup> Une Gateway ou passerelle en français est un propre au routeur. Il permet de lier plusieurs réseaux entre eux. Dans notre cas, nous créons un réseau local avec notre gateway.

- Le masque de sous-réseaux
- La gateway
- L'adresse MAC

L'adresse mac revêt une certaine importance car elle permet de paramétrer une adresse IP fixe dans le routeur pour tous les appareils.

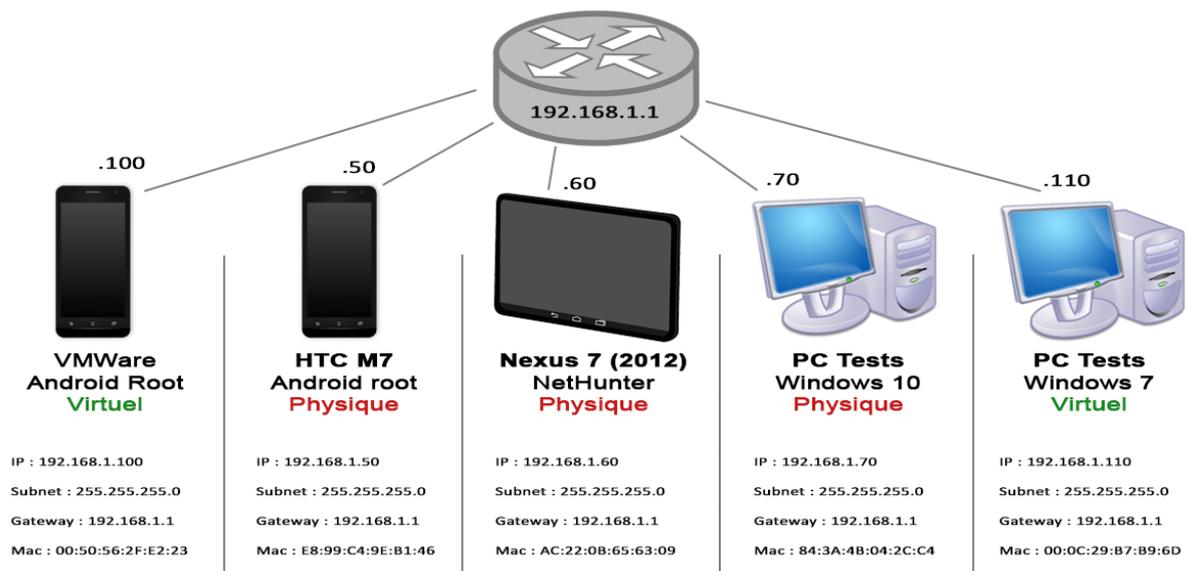


Figure 36 : Plan d'adressage de notre laboratoire<sup>44</sup>  
Créé par l'auteur

Notre laboratoire est un réseau 192.168.1.0 avec un masque de sous-réseau de 255.255.255.0 ce qui nous offre largement plus d'adresses que nécessaire. Si l'on retire le routeur NetGear qui aura obligatoirement le 192.168.1.1, nous possédons 253 adresses disponibles dans notre range<sup>45</sup>.

Notre réseau contient deux types d'appareils qui sont les physiques et les virtuels. Les physiques posséderont toujours une IP inférieure à 192.168.1.100 tandis que les virtuels seront toujours au-dessus. Pour la clarté, nous choisissons de séparer chaque dispositif par 10 adresses.

<sup>44</sup> Illustration disponible sous « 3 Tableaux » avec le nom PlanAdressage

<sup>45</sup> Un range défini les adresses d'un même sous-réseau. Sa taille est définie par le masque de sous-réseau. Ayant un masque de sous réseau en /24 (255.255.255.0), nous disposons de 253 adresses car nous retirons l'adresse réseau (.0), celle du routeur (.1) et celle du broadcast (.255)

Nous avons réussi à intégrer les machines virtuelles sur notre réseau avec l'aide de la fonction bridge<sup>46</sup> de VMWare. Celles-ci disposent également d'une adresse MAC. Cependant, notre machine Android virtuelle ne dévoile pas son adresse MAC dans ses statuts une fois démarrée. Il faut aller dans les paramètres de la carte réseau dans VMWare afin de pouvoir en générer une.

### 3.6.3. Architecture des technologies

En conclusion, il est important de bien comprendre le fonctionnement global des technologies. Nos deux OS comportent chacun des packages distincts. Chaque packages contient des applications propres à son environnement. La figure ci-dessous permet de finaliser la compréhension de notre univers de travail.

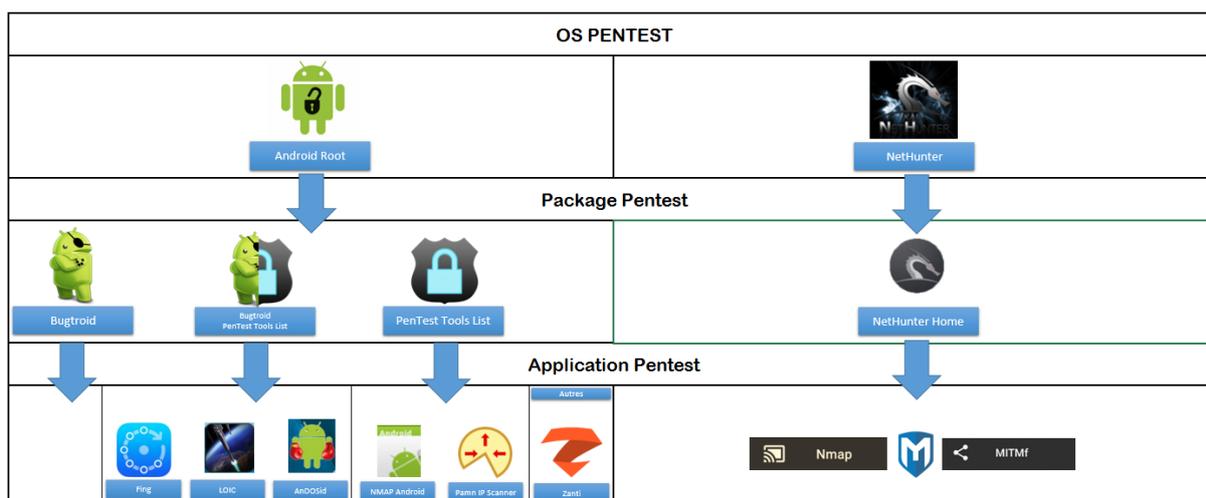


Figure 37 : Résumé des technologies choisies et placement de l'univers de travail<sup>47</sup>  
 Créé par l'auteur

<sup>46</sup> Le mode Bridge considère la machine virtuelle comme une machine physique. Ce qui fait le routeur donnera à notre machine virtuelle une adresse IP différente de notre ordinateur qui l'émule

<sup>47</sup> Disponible sous « 3 Tableaux » avec le nom ArchitectureTechnologieBoard

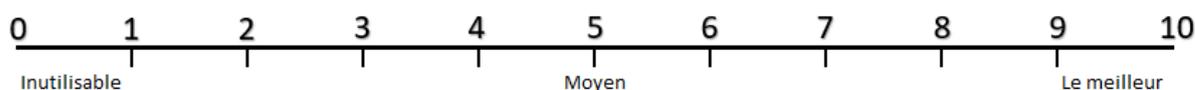
## 4. Cas pratiques

Lors de la phase de tests, nous analyserons plus en détail les applications conservées. Nous avons défini plusieurs cas pratiques afin de séparer les différentes expérimentations.

Avec l'aide des captures d'écran, nous ressortons les informations acquises lors de ces essais. Nous rédigeons un petit tutoriel pour chaque outil et ajoutons également des avis personnels sur l'utilisation de ce dernier.

Pour chaque cas pratique, nous créons un tableau contenant les critères de comparaison que nous jugeons importants. Dans la dernière phase que nous appellerons la phase de choix, nous intégrerons les analyses faites durant les tests afin de comparer les possibilités à disposition.

Les critères sont notés afin de donner une meilleure idée de la force de chaque produit. Nous utilisons le barème de 1 à 10 ci-dessous :



### 4.1. Récapitulation des applications

Nom	OS		Package			hors package
	NetHunter	Android root	NetHunterHome	Bugtroid	PenTest Tool List	
NMAP	X		X			
NMAP Android		X			X	
Zanti		X				
FING		X		X	X	
Pamn IP Scanner		X			X	
MITM	X		X			
Zanti		X				X
Metasploit DOS	X		X			
Loic		X		X	X	
AnDOSid		X		X	X	

Figure 38 : Applications retenues pour la phase de tests<sup>48</sup>  
Créé par l'auteur

<sup>48</sup> Le tableau est disponible sous « 3 Tableaux » sous le nom ApplicationsRecapitulationBoard

## 4.2. Découverte réseau

### 4.2.1. Applications retenues

- NMAP → Disponible sous NetHunter et l'Android rooté
- Fing → Disponible uniquement sous l'Android rooté
- Zanti → Disponible uniquement sous l'Android rooté
- Pamn IP Scanner → Disponible uniquement sous l'Android rooté

### 4.2.2. Critères de comparaison

Les critères retenus pour comparer les différents outils ci-dessous sont :

- Critère 1 : Efficacité de la réponse
  - Qualité du résultat de la recherche
  - Pondération : x3
- Critère 2 : Efficacité de la requête
  - Possibilité d'ajout de paramètre par l'utilisateur à la requête
  - Pondération x2
- Critère 3 : Ergonomie
  - La qualité du design et de l'utilisation de l'application
  - Pondération x1
- Critère 4 : Outils supplémentaires
  - Si l'application comporte des possibilités supplémentaires à un NMAP classique
  - Pondération x2
- Critère 5 : Rapidité
  - La rapidité du scan sur notre routeur NetGear
  - Pondération x1

### 4.2.3. NMAP NetHunter

Le NMAP Sous NetHunter fonctionne avec la ligne de commande Kali Linux. Via le package de NetHunter, nous trouvons une application appelée NMAP Scan qui nous permettra de générer une ligne de commande. Cette dernière une fois lancée réalise le NMAP et nous retourne ses résultats.

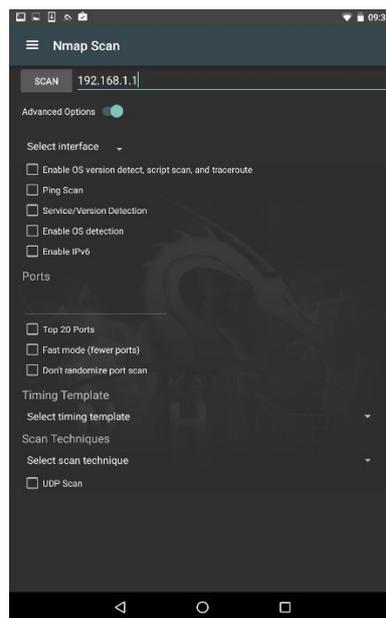


Figure 39 : NMAP sous NetHunter  
 Créée par l'auteur

Il est possible depuis l'invite de commande de créer sa propre requête NMAP sans passer par l'outil du package. Il est néanmoins plus facile de le faire directement depuis l'application. Par exemple, il est possible d'ajouter à l'adresse IP recherchée la marque du matériel. Si nous voulons savoir quelle adresse IP correspond à un ordinateur HP, nous pouvons cocher la case « Enable OS Detection ». Dans la ligne de commande, nous verrons apparaître un « -O » qui correspond à ce paramètre. Il existe beaucoup de possibilités avec la ligne de commande. Dans un premier temps, nous utilisons uniquement l'application mais avec l'habitude, il nous arrive d'entrer les commandes directement sur le prompt Kali Linux. Nous avons par ailleurs trouvé un site<sup>49</sup> qui relate tous les paramètres possibles du NMAP.

<sup>49</sup> Il est disponible sous ce lien : <http://tools.kali.org/information-gathering/nmap>

Le résultat apparaît dans la ligne de commande comme démontré sur la capture d'écran ci-dessous.

```

root@kali:/# nmap 192.168.1.1
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-06 07:48 UTC
Nmap scan report for internetbox.home (192.168.1.1)
Host is up (0.0034s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
49152/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 18.34 seconds
root@kali:/#
    
```

Figure 40 : Résultat requête NMAP sous NetHunter  
 Créé par l'auteur

Les résultats sont excellents comme nous pouvions nous y attendre avec NMAP. Nous avons scanné dans cet exemple notre routeur. Nous pouvons y voir la date, le temps de latence de l'hôte, le nombre de port ouvert, ainsi que le temps du scan. Le scan de notre routeur a pris 18,34 secondes. Il prend en moyenne 15 secondes pour effectuer son travail.

Il est possible de scanner plusieurs adresses IP en même temps. Pour se faire, nous devons ajouter une étoile sous la partie allouée aux machines de l'adresse IP. Dans notre cas, la commande serait :

```
nmap 192.168.1.*
```

En effet, étant en /24 sur notre réseau interne, la partie allouée aux machines correspond au dernier octet de notre adresse IP.

Lorsque nous scannons plusieurs adresses comme ci-dessus, nous avons automatiquement l'adresse MAC de chaque machine en retour.

L'ergonomie de l'application reste spartiate si nous utilisons que la ligne de commande. Si nous utilisons en revanche l'application, nous pouvons voir une application intuitive contenant plusieurs options citées dans la partie d'état de l'art.

Effacité Retour	Effacité Argument	Ergonomie	Outils supplémentaire	Rapidité
10	10	6	8	9
Le meilleur sur le marché	Ajout automatisé	Retour en ligne de commande	Advanced Options	~ 15 secondes

Tableau 6 : Résumé de l'analyse du NMAP de NetHunter

Résultat :

$$(10 * 3) + (10 * 2) + (6 * 1) + (8 * 2) + (9 * 1) = 81$$

#### 4.2.4. NMAP Android rooté

NMAP existe également sous l'Android rooté. Il fonctionne de la même manière que celui sous NetHunter. Il suffit de rentrer l'IP de la cible ainsi que les options NMAP tel que -O qui retourne les OS et ensuite appuyez sur le bouton NMAP. Il n'existe pas pour ce dernier la possibilité d'auto-générer des arguments comme il l'était possible pour le NMAP de NetHunter. Cela rend la tâche plus difficile à son utilisateur qui doit par conséquent connaître les différents raccourcis pour les arguments.

Au niveau efficacité, il s'agit du même NMAP que celui sous NetHunter. Il y a toutefois une différence notable au niveau du temps de recherche. Sous le NMAP d'Android, il est très rapide avec une moyenne de 5 secondes pour scanner notre routeur NetGear. Le design est en revanche un point négatif. Une fois le scan terminé, le résultat se trouve dans une textarea<sup>50</sup> qui est modifiable ce qui fait que lorsque nous appuyons sur le résultat, notre clavier virtuel s'ouvre. C'est fortement dommageable étant donné que le résultat du NMAP prend trois quarts de l'écran. Il est presque impossible de ne pas appuyer sur cette zone qui ouvrira notre clavier virtuel et rendra peu lisible le résultat.

<sup>50</sup> Zone contenant du texte qui peut être modifiable ou non-modifiable selon les paramètres que l'on lui donne.

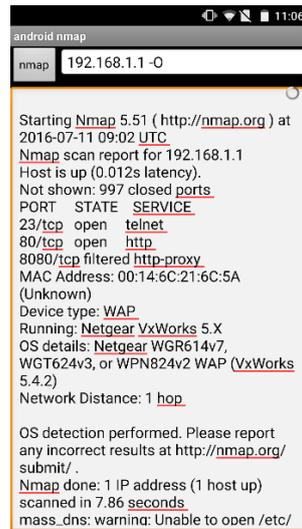


Figure 41 : NMAP sous l'android rooté (avec -O pour les OS)  
Crée par l'auteur

Il est également problématique de n'avoir aucun outil supplémentaire. Toutefois, l'application est gratuite et permet de réaliser un NMAP efficace et rapide.

Nous présentons ci-dessous le tableau contenant les différents critères susmentionnés pour le NMAP de l'Android rooté.

Efficacité Retour	Efficacité Argument	Ergonomie	Outils supplémentaire	Rapidité
10	7	3	0	10
Idem qu'un NMAP classique	Argument NMAP	Point faible de l'app	Aucun outil supplémentaire	~ 5 secondes

Tableau 7 : Résumé de l'analyse du NMAP d'Android

Résultat :

$$(10 * 3) + (7 * 2) + (3 * 1) + (0 * 2) + (10 * 1) = 57$$

#### 4.2.5. Fing

Fing réalise un scan efficace du réseau. Nous pouvons avec cette application Android mapper rapidement le réseau dans lequel se trouve l'appareil. En moyenne, un scan dure 8

secondes. Il est impossible toutefois d'ajouter des arguments comme dans un NMAP classique. Il y a plusieurs outils supplémentaires via le bouton paramètre en haut à droite de l'application. En cliquant sur un appareil après avoir effectué un scan, il est possible de réaliser un scan service afin de connaître les ports ouverts de la cible. Nous pouvons également réaliser un ping ou un traceroute sur l'appareil sélectionné.

Comme mentionné, il s'agit d'un scanner automatisé qui retourne l'IP des appareils du réseau, l'adresse MAC, le type d'appareil<sup>51</sup> et le nom de l'appareil. Fing se démarque par son design agréable et permet une prise en main rapide.

Effacité Retour	Effacité Argument	Ergonomie	Outils supplémentaire	Rapidité
4	0	10	5	10
Retour peu d'information	Aucun argument	Bonne prise en main	Outils basiques	~ 8 secondes

Tableau 8 : Résumé de l'analyse de Fing

Résultat :

$$(4 * 3) + (0 * 2) + (10 * 1) + (5 * 2) + (10 * 1) = 42$$

#### 4.2.6. Pamn IP Scanner

Pamn IP est la seule application payante<sup>52</sup> des 5 sélectionnées. Elle contient cependant d'excellentes options. Son coût est vite oublié car il propose un scan NMAP relativement rapide. Après plusieurs essais, nous avons eu un grand nombre de résultats après 5 secondes seulement. La possibilité d'avoir l'historique de nos scans est un point fort. Avec l'aide de cet historique, nous observons les résultats précédents ce qui nous évite de relancer un scan déjà effectué.

<sup>51</sup> Par exemple HTC, Intel. Il faut ajouter le package qui est proposé lors de l'installation de FING

<sup>52</sup> CHF 2.66

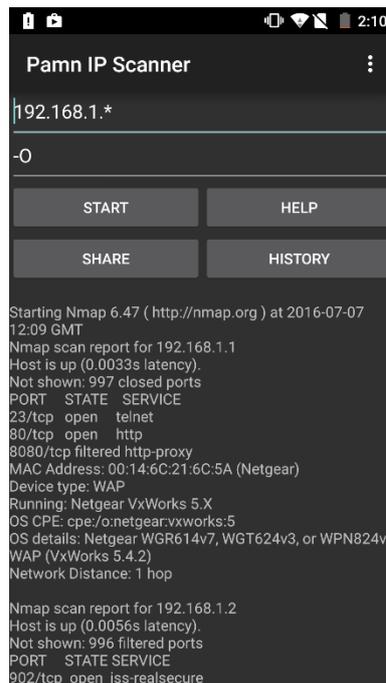


Figure 42 : Scan Pamn IP Scanner sur tous les appareils connectés au routeur  
Créé par l'auteur

L'application contient deux cases à remplir. La première contient l'IP de la ou les cibles et la seconde permet l'ajout d'argument NMAP. Dans cette deuxième case, les développeurs ont été performants en ajoutant le bouton help qui réalise un -h rapidement et offre la palette des arguments directement à l'utilisateur. Il existe la possibilité de réaliser un ping de la cible via le bouton en haut à droite.

Efficacité Retour	Efficacité Argument	Ergonomie	Outils supplémentaire	Rapidité
10	8	10	7	10
Retour NMAP	Argument NMAP	Très bon design	Historique et help	~ 5 secondes

Tableau 9 : Résumé de l'analyse de Pamn IP Scanner

Résultat :

$$(10 * 3) + (8 * 2) + (10 * 1) + (7 * 2) + (10 * 1) = 80$$

#### 4.2.7. Zanti Scan

Au démarrage de l'application, Zanti scan automatiquement le réseau dans lequel se situe l'appareil. Il retourne l'adresse IP, l'adresse MAC, le nombre de port ouverts sur la droite, et le type d'appareil. La qualité d'affichage permet d'avoir une vue d'ensemble rapide de l'architecture dans laquelle nous nous trouvons. En moyenne, son scan initial dure 10 secondes. Il est possible via l'icône de l'horloge avec la flèche dans le sens inverse de revoir l'historique de tous les réseaux scannés au préalable.

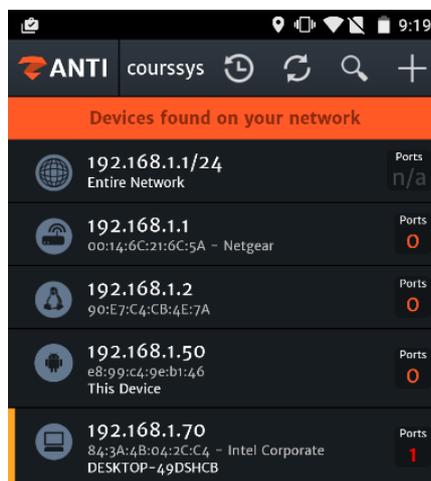


Figure 43 : Scan automatique de Zanti  
 Créé par l'auteur

Il est possible de cliquer sur un des appareils détectés mais également le réseau entier et de réaliser un second scan à l'intérieur de ce dernier. Il est possible dans ce second scan de choisir le type désiré, d'exécuter un script particulier ou encore d'activer le « Smart scanning » qui vérifie automatiquement les failles du réseau. Les développeurs ont prévu une zone de commentaires afin de pouvoir noter des informations particulières directement sur l'application.

Efficacité Retour	Efficacité Argument	Ergonomie	Outils supplémentaire	Rapidité
10	8	10	9	10
Retour NMAP	Manque argument classique	Ergonomie parfaite	Beaucoup de possibilité	~ 10 secondes

Tableau 10 : Résumé de l'analyse de Zanti Scan

Résultat :

$$(10 * 3) + (8 * 2) + (10 * 1) + (9 * 2) + (10 * 1) = 84$$

### Récapitulatif

	Efficacité Retour	Efficacité Argument	Ergonomie	Outils suppl.	Rapidité	Total
NetHunter NMAP	10	10	6	8	9	81
Android root NMAP	10	7	3	0	10	57
FING	4	0	10	5	10	42
Pamn IP Scanner	10	8	10	7	10	80
Zanti Scan	10	8	10	9	10	84

Tableau 11 : Récapitulatif des applications de découverte réseau

#### 4.2.8. Choix

Au final et pour résumer cette première analyse, nous pouvons remarquer que trois outils de découverte réseau se démarquent des autres.

- NetHunter NMAP
- Pamn IP Scanner
- Zanti Scan

Nous proposons après analyse et comparaison d'utiliser un de ces trois scanners pour la phase de découverte réseau.



Figure 44 : Liste des applications sélectionnées pour la phase de découverte réseau

### 4.3. Attaque Man In The Middle

#### 4.3.1. Applications retenues

- MITMF → Disponible uniquement sous NetHunter
- Zanti → Disponible uniquement sous Android rooté

#### 4.3.2. Critère de comparaison

Les critères retenus pour comparer les différents outils ci-dessous sont :

- Critère 1 : Mise en place
  - Le temps de mise en place de l'attaque ainsi que sa complexité
  - Pondération → 3x
- Critère 2 : Ergonomie
  - La qualité du design et de l'utilisation de l'application
  - Pondération → 2x
- Critère 3 : Outils supplémentaires
  - Si l'application comporte des outils supplémentaire et complémentaire au MITM
  - Pondération → 3x

### 4.3.3. MITMF

L'interface de MITMF sur NetHunter s'apparente à celle utilisée lors du NMAP. L'utilisateur est invité à sélectionner des cases à cocher qui construiront la requête sur la ligne de commande Kali. L'outil de NetHunter dispose de plusieurs onglets :

- General Settings
  - Interface
  - General Settings
  - ScreenShooter
- Responder Settings
- Inject Settings
- Spoof Settings
- MITMf configuration

Dans notre cas, le programme rencontre des problèmes avec certains plugins<sup>53</sup>. Aussi, nous conseillons d'entrer les informations directement depuis la ligne de commande Kali. Il faut ajouter après la commande mitm :

- L'interface
  - -i wlan0
- La cible
  - --target 192.168.1.110 (IP de la cible)
- La gateway
  - --Gateway 192.168.1.1 (IP du routeur)
- Type des paquets
  - --spoof --arp

---

<sup>53</sup> Certains arguments (plugins) posent problèmes lors de l'exécution de la commande

```
Last login: Mon Jul 11 11:24:06 UTC 2016 on pts/2
Linux kali 3.4.0-gcc51ee3-dirty #4 SMP PREEMPT Sat Dec 12 00:29:55 UTC 2015 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
--arpkali:~# mitmf -i wlan0 --target 192.168.1.50 --gateway 192.168.1.1 --spoo

[*) MITMf v0.9.7 online... initializing plugins
|_ Spoofer v0.6
|_ Sergio-Proxy v0.2.1 online
|_ SSLstrip v0.9 by Moxie Marlinspike online
|_ Net-Creds v1.0 online
|_ DNSCher v0.4 online
|_ SMBserver online (Impacket 9.13)

2016-07-11 11:38:40 [SMBserver] Config file parsed
2016-07-11 11:38:40 [SMBserver] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
2016-07-11 11:38:40 [SMBserver] Config file parsed
```

Figure 45 : Ligne de commande pour une attaque MITM avec NetHunter  
Créé par l'auteur

**mitmf -i wlan0 --target [IP cible] --gateway [IP Routeur Cible] --spoo --arp**

Après l'exécution de la commande, tous les gestes de la cible sur Internet seront rapportés sur la ligne de commande. Il est également le cas des mots de passe. Nous avons essayé de nous connecter comme précédemment sur le site de qoqa avec l'utilisateur « user1234 » et son mot de passe « ratonlaveur2 ». Nous avons pu en retirer ceci :

```
2016-07-11 11:39:39 192.168.1.50 [type:Chrome 37.0.0.0 os:Android Linux 5.0.1] Sending Request: stat
ic.qoqa.com
2016-07-11 11:39:46 192.168.1.50 POST Data (www.qoqa.ch):
name=user1234&password=ratonlaveur2&referrer=http%3A%2F%2Fwww.qoqa.ch%2F
2016-07-11 11:39:47 192.168.1.50 [type:Chrome 37.0.0.0 os:Android Linux 5.0.1] Sending Request: www.
qoqa.com
2016-07-11 11:39:47 192.168.1.50 [type:Chrome 37.0.0.0 os:Android Linux 5.0.1] Sending Request: www.
qoqa.ch
2016-07-11 11:39:48 192.168.1.50 [type:Chrome 37.0.0.0 os:Android Linux 5.0.1] Sending Request: stat
ic.qoqa.com
```

Figure 46 : MITM avec NetHunter  
Créé par l'auteur

MITMF fonctionne bien à partir du moment que nous l'utilisons directement depuis la ligne de commande. Il est facile à mettre en place surtout avec l'aide d'internet<sup>54</sup> qui permet d'avoir des exemples. Il est également possible de faire -h après MITMF dans la ligne de

<sup>54</sup> Sous « 2 Tutoriaux » il y a un document nommé MITMF qui apporte des informations sur ce sujet

commande afin d'avoir l'ensemble des raccourcis possibles. Il dispose de tous les outils que peut disposer un MITM hormis les plugins cités plus haut.

Mise en place	Ergonomie	Outils supplémentaire
10	6	8
Rapide et efficace	Ligne de commande	Beaucoup d'outils mais pas tous utilisés

Tableau 12 : Récapitulatif de l'analyse de MITMF

Résultat :

$$(10 * 3) + (6 * 2) + (8 * 3) = 66$$

#### 4.3.4. Zanti

Une fois l'application ouverte, Zanti propose automatiquement de réaliser un scan du réseau sur lequel se trouve notre appareil. Il retourne également les ports ouverts ainsi que l'adresse mac des cibles potentielles. Il est possible de réaliser un MITM aussi bien sur le réseau complet que sur une cible en particulier.

Afin de mettre en place l'attaque de l'homme du milieu, il suffit de choisir la cible et de presser sur le bouton Man in the Middle dans la rubrique Attack Actions. Dans l'interface du MITM, nous pouvons voir les faits et gestes de notre victime via la catégorie Logged Requests en appuyant sur view. C'est une interface diablement ergonomique qui nous est proposée. Lorsque la victime se déplace sur Internet, nous pouvons voir en un clin d'œil les informations de :

- Ses sessions
- Ses mots de passe
- Ses requêtes
- Ses users agents

Il existe comme démontré dans la phase d'état de l'art un grand nombre d'outils supplémentaires permettant de par exemple télécharger les .pdf que la victime télécharge ou encore remplacer les images de tous les sites internet.



Figure 47 : Interface Zanti  
Créé par l'auteur

C'est une application très intéressante et disposant d'un grand arsenal d'outils de pentest. Nous avons pu sniffer des mots de passe sur des sites internet tel que qoqa.ch en toute simplicité. Nous avons créé un faux compte sur le site de qoqa :

- Utilisateur : user1234
- Mot de passe : ratonlaveur2

Nous avons lancé notre MITM avec Zanti est voici le résultat après un login sur l'une de machine de tests.

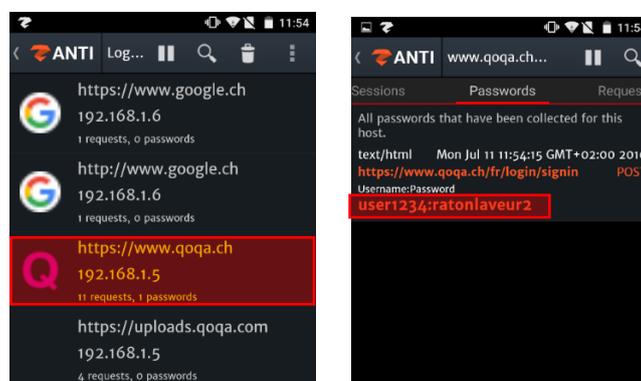


Figure 48 : Zanti permet d'avoir les mots de passe de la cible  
Créé par l'auteur

Etant donné que nous avons activé SSL Strip, la cible se connecte au site en http au lieu de https et par conséquent, nous pouvons observer le mot de passe en clair sur l'application. Comme mentionné plus haut, il est également possible de remplacer toutes les images par une image choisie. Nous avons testé cette possibilité sur le site du 20 minutes et voici le résultat :



Figure 49 : Replace image sur le site du 20 minutes  
Créé par l'auteur

Nous en arrivons à la conclusion que cette application contient énormément d'outils d'analyse réseau et de possibilité d'attaques. Son ergonomie est simplement efficace et facile à prendre en main. De plus, les résultats se font voir après quelques manipulations.

Mise en place	Ergonomie	Outils supplémentaire
10	10	10
Rapide et efficace	L'interface utilisateur est son plus grand point fort	Elle dispose d'un grand nombre d'outils

Tableau 13 : Récapitulatif de l'analyse de Zanti MITM

Résultat :

$$(10 * 3) + (10 * 2) + (10 * 3) = 80$$



#### 4.3.5. Récapitulatif

	Mise en place	Ergonomie	Outils suppl.	Total
NetHunter MITMF	10	6	8	66
Zanti	10	10	10	80

Tableau 14 : Récapitulatif des applications d'attaque Man In The Middle

#### 4.3.6. Choix

Il est intéressant d'avoir pu tester la version NetHunter du Man In The Middle qui propose un large panel de possibilités. Toutefois, nous conseillons l'application sous Android Zanti qui permet en plus de s'introduire, d'effectuer plusieurs actions sur le réseau de la victime.

Nous n'avons malheureusement pas été en mesure de proposer une troisième application vivable pour l'attaque Man In The Middle. Toutefois, nous estimons que les deux proposées sont efficaces et très intéressantes à utiliser.



Figure 50 : Application sélectionnée pour l'attaque Man In The Middle

## 4.4. Attaque DDoS

### 4.4.1. Applications retenues

- LOIC → Disponible uniquement sous l'Android rooté
- Metasploit DDoS → Disponible uniquement sous NetHunter
- AnDOSid → Disponible uniquement sous l'Android rooté

### 4.4.2. Critère de sélection

Les critères retenus pour comparer les différents outils ci-dessous sont :

- Critère 1 : Efficacité de l'attaque
  - Nombre de requêtes envoyées par seconde
  - Pondération : x3
- Critère 2 : Ergonomie
  - La qualité du design et de l'utilisation de l'application
  - Pondération x1
- Critère 3 : Outils supplémentaires
  - Quantité d'outils disponibles en plus de la simple attaque DDoS
  - Pondération x2
- Critère 4 : Mise en place de l'attaque
  - Temps de mise en place d'une attaque
  - Pondération x2
- Critère 5 : Exposition
  - L'attaquant peut être découvert ou non par la cible
  - Pondération x3

### 4.4.3. LOIC

LOIC fonctionne en trois étapes. La première consiste à entrer l'IP de la cible, la seconde contient les options d'attaques et la dernière partie concerne l'activation de l'attaque. Il est simple à mettre en place et offre la possibilité d'attaquer rapidement une cible à travers le monde entier.

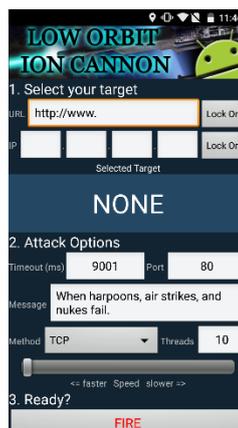


Figure 51 : Interface de LOIC  
Créé par l'auteur

Il y a à disposition une certaine quantité d'options telles que

- Timeout
  - Temps de repos entre chaque envoi
- Port
  - Port sur laquelle nous envoyons l'attaque
- Message
  - Message<sup>55</sup> disponible uniquement pour les méthodes UDP et TCP
- Méthode
  - Méthode d'inondation (TCP, UDP, http)
- Threads
  - Nombre de processus lancer simultanément

---

<sup>55</sup> Il est possible de le voir lorsque la cible réalise un wireShark de son réseau

59	3.178451	192.168.1.50	192.168.1.3	TCP	74	43374 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785272	TSecr=0	WS=64
60	3.178624	192.168.1.50	192.168.1.3	TCP	74	40638 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785272	TSecr=0	WS=64
61	3.179058	192.168.1.50	192.168.1.3	TCP	74	33894 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785272	TSecr=0	WS=64
62	3.495546	192.168.1.50	192.168.1.3	TCP	74	41864 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785309	TSecr=0	WS=64
63	3.500381	192.168.1.50	192.168.1.3	TCP	74	52300 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785313	TSecr=0	WS=64
64	3.500382	192.168.1.50	192.168.1.3	TCP	74	49326 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785313	TSecr=0	WS=64
65	3.559624	192.168.1.50	192.168.1.3	TCP	74	51311 → 80	[SYN]	Seq=0	Win=14600	Len=0	MSS=1460	SACK_PERM=1	TSval=785318	TSecr=0	WS=64

Figure 52 : Analyse wireshark d'une attaque DDoS TCP de LOIC  
Créé par l'auteur

Comme nous pouvons le remarquer, il est possible de connaître l'IP de l'attaquant est par conséquent, LOIC sous l'Android rooté ne dispose pas d'un système de protection pour l'attaquant.

L'application est rapidement prise en main. Son système d'étape lui permet d'être vite comprise par tous les utilisateurs. De plus, LOIC offre la possibilité de trouver l'IP d'un site internet directement en insérant ledit site.

Efficacité	Ergonomie	Outils supplémentaire	Mise en place	Exposition
6	8	8	10	0
15 paquets/sec 10 threads 500timeOut	Simple et facile à utiliser	Conversion URL/IP Attack options	Attaque DDoS en moins d'une minute	L'attaquant est exposé

Tableau 15 : Récapitulatif de l'analyse de LOIC

Résultat :

$$(6 * 3) + (8 * 1) + (8 * 2) + (10 * 2) + (0 * 3) = 62$$

#### 4.4.4. Metasploit DDoS

Il est possible de réaliser une attaque DDoS depuis Metasploit sur NetHunter. Nous démarrons la ligne de commande Kali Linux et rentrons dans Metasploit avec la requête msfconsole.

Ensuite, il faut utiliser `auxiliary/dos/tcp/synflood` avec la ligne de commande « `use auxiliary/dos/tcp/synflood` ». Une fois entrée dans le `synflood` qui nous permettra de réaliser l'attaque, nous devons indiquer l'interface<sup>56</sup> que nous utilisons avec la commande « `SET INTERFACE wlan0` ». Pour finir, nous avons modifié le `RHOST` qui correspond à l'IP de la cible. Dans notre cas, nous avons ajouté « `SET RHOST 192.168.1.70` ». Enfin, nous réalisons l'exploit avec « `exploit` » (Hacker, 2014).

3112	9.639820	211.166.14.196	192.168.1.3	TCP	54	59285	→ 80	[SYN]	Seq=0	Win=875	Len=0
3113	9.643027	211.166.14.196	192.168.1.3	TCP	54	62261	→ 80	[SYN]	Seq=0	Win=1044	Len=0
3114	9.646149	211.166.14.196	192.168.1.3	TCP	54	47299	→ 80	[SYN]	Seq=0	Win=1228	Len=0
3115	9.649318	211.166.14.196	192.168.1.3	TCP	54	34555	→ 80	[SYN]	Seq=0	Win=3157	Len=0
3116	9.653721	211.166.14.196	192.168.1.3	TCP	54	20575	→ 80	[SYN]	Seq=0	Win=1557	Len=0
3117	9.656193	211.166.14.196	192.168.1.3	TCP	54	23088	→ 80	[SYN]	Seq=0	Win=2665	Len=0
3118	9.659632	211.166.14.196	192.168.1.3	TCP	54	18371	→ 80	[SYN]	Seq=0	Win=3206	Len=0
3119	9.662833	211.166.14.196	192.168.1.3	TCP	54	49156	→ 80	[SYN]	Seq=0	Win=3956	Len=0

Figure 53 : Attaque DDoS avec Metasploit sous NetHunter  
 Créé par l'auteur

L'attaque DDoS avec ce moyen vient d'une adresse IP différente que celle de notre appareil sous NetHunter. On peut voir sur l'image ci-dessus que l'IP source est 211.166.14.196. Après avoir recherché sur internet, nous sommes en mesure de dire que cette adresse est une adresse venant de Chine. Il est par conséquent impossible pour la victime d'affirmer que c'est nous qui avons réalisé l'attaque.

### Details of 211.166.14.196

IP Address : 211.166.14.196

Location : China (95% accuracy)

Figure 54 : Situation de l'adresse IP 211.166.14.196  
<http://www.hcidata.info/host2ip.cgi>

Efficacité

Ergonomie

Outils

Mise en place

Exposition

<sup>56</sup> Il est possible de connaître l'interface à utiliser en réalisant un `ifconfig`

supplémentaire				
10	5	5	7	10
279 paquets/sec 500timeOut	Ligne de commande	Options en ligne de commande mais peu	Attaque DDoS en moins de 5 minutes	L'attaquant n'est pas exposé

Tableau 16 : Récapitulatif de l'analyse de Metasploit DDoS

Résultat :

$$(10 * 3) + (5 * 1) + (5 * 2) + (7 * 2) + (10 * 3) = 89$$

#### 4.4.5. AnDOSid

AnDOSid est moins performante que les deux applications précitées. Il n'est pas possible d'attaquer n'importe quelle IP. En effet, dans ce software, nous pouvons uniquement insérer l'adresse URL d'un site internet afin de mener une attaque DDoS sur ce dernier.

Il est important de savoir qu'une attaque DDoS n'est pas légale si nous n'avons pas l'accord du propriétaire. En France, l'année passée, un homme ayant pratiqué une attaque DDoS sur les sites internet du conseil régional de Lorraine risque 10 ans de prison et € 150'000.- d'amende. Il est par conséquent impossible pour nous de tester correctement ce package. Aussi, il nous est difficile de réaliser un tableau de critère complet.

Efficacité	Ergonomie	Outils supplémentaire	Mise en place	Exposition
?	7	3	10	?
	Simple et efficace	Taille des payload et timeout modifiable	Attaque DDoS en moins de 1 minutes	

Tableau 17 : Récapitulatif de l'analyse de AnDOSid

Résultat :

$$(0 * 3) + (7 * 1) + (3 * 2) + (10 * 2) + (0 * 3) = 29$$

#### 4.4.6. Récapitulatif

	Efficacité	Ergonomie	Outils suppl.	Mise en place	Exposition	Total
LOIC	6	8	8	10	0	62
Metasploit DDoS	10	5	5	7	10	89
AnDOSid	?	7	3	10	?	29

Tableau 18 : Récapitulatif des applications d'attaque DDoS

#### 4.4.7. Choix

L'efficacité du DDoS proposé par Metasploit sur le NetHunter est très efficace. Il envoie un grand nombre de paquets par seconde et inonde complètement la cible. Il y a une grande différence de paquets envoyés par seconde entre LOIC et Metasploit. On le voit rapidement avec le total de points. LOIC est certes plus ergonomique et plus facile à mettre en place mais ne cache pas son utilisateur ce qui est très mauvais pour un tel software.



Figure 55 : Application sélectionnée pour l'attaque DDoS

## 5. Conclusion

### 5.1. Outils conseillés

Nous avons testé et comparé les outils de la phase d'état de l'art et nous sommes à présent en mesure de proposer une solution de pentesting mobile. Nous utilisons notre expérience pour composer l'appareil suivant :

- OS
  - Installation de NetHunter sous une tablette de la gamme Nexus rooté

La combinaison root/NetHunter sur un même appareil offre la possibilité d'utiliser tous les outils présentés dans cette thèse. L'avantage de réaliser des tests d'intrusion avec une tablette présente un avantage certain qui est la taille de l'écran ainsi que du clavier virtuel. Il est beaucoup plus confortable de travailler sur une tablette que sur un smartphone.

Les deux packages de pentest présentés plus haut portant le nom de Bugtroid et Pentest Tools donnent la possibilité aux testeurs de trouver rapidement des solutions spécifiques. Il est important de ne pas les négliger car ils regroupent un très grand nombre d'applications permettant les tests d'intrusion via un Android rooté.

Au niveau des applications, nous avons sélectionné après analyse et comparaison :

- Découverte réseau
  - Zanti Scan → ANDROID
- Attaque MITMF
  - Zanti → ANDROID
- Attaque DDoS
  - Metasploit DDoS → NETHUNTER

Il existe encore beaucoup de possibilités non analysées sur NetHunter. La ligne de commande de Kali Linux est un outil formidable offrant des possibilités vastes et performantes.

## 5.2. Améliorations

La partie d'état de l'art a duré un long moment. Aussi, nous n'avons pas eu énormément de temps pour tester des applications et mettre en place des cas pratiques. Il existe encore plusieurs types d'attaque que nous aurions voulu mettre en pratique tels que :

- Man In The Middle via un port USB
- Mana Wireless Toolkit
- HID attacks
- Ainsi que toutes les possibilités qu'offre la ligne de commande de Kali Linux

Nous aurions désiré également réaliser des recherches vers des outils payants comme les prometteurs Pwn Pad et PWN Phone. Nous avons quadrillé le secteur des OS, packages et applications gratuites ou à bas coût mais il est logique de penser que ces produits payants valent la peine d'être testés. Le Pwn Pad est d'ailleurs décrit dans une vidéo du vendeur<sup>57</sup>. Il serait intéressant de pouvoir comparer leurs produits à notre proposition finale afin d'y voir nos lacunes par rapport à un appareil payant.

## 5.3. Pentest mobile et Pentest ordinateur

Le monde du pentest mobile est jeune mais déjà vaste. Certes, il n'est pas aussi étendu que le pentest sur des ordinateurs mais il possède un fort potentiel. A l'heure actuelle, il manque des outils afin de pouvoir le considérer comme complet. NetHunter possède un assortiment d'une dizaine d'applications. De son côté Kali Linux possède plus de 300 outils de tests d'intrusion (Security, 2013). La marge de progression de notre appareil mobile reste encore grande. Néanmoins, avec l'aide d'applications Android, nous pouvons nous rapprocher de ce que Kali Linux peut fournir en termes de pentesting.

Dans le futur, nous voyons les tests d'intrusion se réaliser sur des tablettes performantes proposant tout un panel d'outil rapidement accessible.

---

<sup>57</sup> <https://www.youtube.com/watch?v=RU-UATpfaUM>

## RÉFÉRENCES

- Abraham, A. (2016). *ajinabraham/Mobile-Security-Framework-MobSF*. Récupéré sur github: <https://github.com/ajinabraham/Mobile-Security-Framework-MobSF>
- Adduono, J. C. (2016, 04 26). *Kali NetHunter Documentation*. Récupéré sur Github: <https://github.com/offensive-security/kali-nethunter/wiki>
- Amadeo, R. (2016, 05 25). *Google to bring official Android support to the Raspberry PI 3*. Récupéré sur arstechnica: <http://arstechnica.com/gadgets/2016/05/google-to-bring-official-android-support-to-the-raspberry-pi-3/>
- Attaque DDoS*. (2015, 07 01). Récupéré sur melani.admin: <https://www.melani.admin.ch/melani/fr/home/themen/DDoSAttacken.html>
- Attaque man in the middle*. (s.d.). Récupéré sur futura-sciences: <http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/informatique-attaque-man-in-middle-10048/>
- Balt, T. (2016). *androidpit.fr*. Récupéré sur Qu'est-ce qu'une ROM Custom sur Android: <http://www.androidpit.fr/c-est-quoi-rom-custom-android>
- Bugroid Pentesting pro*. (2013, 11 30). Récupéré sur playboard: <http://playboard.me/android/apps/com.bugroid>
- Cherki, M. (2012, 02 15). *Figaro*. Récupéré sur 10 milliards d'appareils connectés à Internet en 2016: <http://www.lefigaro.fr/secteur/high-tech/2012/02/15/01007-20120215ARTFIG00682-10milliards-d-appareils-connectes-a-internet-en-2016.php>
- Cyanogenmod downloads*. (2016). Récupéré sur download Cyanogenmod: <https://download.cyanogenmod.org/>

*Devices.* (2014, 09 18). Récupéré sur wiki.cyanogenmod:  
<http://wiki.cyanogenmod.org/w/Devices>

*El\_FuerTos.* (2012, 06 01). *Root Android : rooter c'est quoi au juste ?* Récupéré sur cnetfrance.fr: <http://forums.cnetfrance.fr/topic/1170024-root-android--rooter-c-est-quoi-au-juste/>

Graff, P.-E. (2015). *clubic.* Récupéré sur Nexus 7 : La première tablette de Google par Asus: <http://www.clubic.com/tablette-internet-mid/article-507568-1-nexus-7.html>

Hacker, H. (2014, 05 27). *How to DDOS Attack Using Metasploit In Kali Linux.* Récupéré sur Youtube: <https://www.youtube.com/watch?v=yxAhrUAvjo0>

*How to use traceroute to identify network problems.* (2013, 01 19). Récupéré sur howtogeek: <http://www.howtogeek.com/134132/how-to-use-traceroute-to-identify-network-problems/>

*htc.* (s.d.). Récupéré sur VUE D'ENSEMBLE DES CARACTÉRISTIQUES: <http://www.htc.com/fr/smartphones/htc-one-m7/>

*Kali Linux NetHunter.* (2016). Récupéré sur kali: <https://www.kali.org/kali-linux-nethunter/>

*kenmaster.* (2016, 1 5). *Crack / piratage d'un réseau wifi.* Récupéré sur kenmaster: <http://kenmaster.unblog.fr/>

*NMAP Sécurité scanner.* (s.d.). Récupéré sur nmap: <https://nmap.org/>

*One Plus One.* (2016). Récupéré sur OnePlus: <https://oneplus.net/global/one>

*Pentest Tools List.* (s.d.). Récupéré sur play.google: <https://play.google.com/store/apps/details?id=com.itslap.pentesttools&hl=fr>

*Phmadore.* (2015). *hacked.* Retrieved from Penetration Testing: [https://hacked.com/wiki/Penetration\\_Testing](https://hacked.com/wiki/Penetration_Testing)

Polo. (2014, 06 20). *Facebook a été victime d'une attaque DDoS venant de Chine !* Récupéré sur tuxboard: <http://www.tuxboard.com/facebook-attaque-ddos-chine/>

Poulain, B. (2002, 06 23). *ping*. Récupéré sur linuxcertif: <http://www.linuxcertif.com/man/8/ping/>

*Procheckup*. (s.d.). Récupéré sur Penetration Testing: Black Box vs. White Box: <http://www.procheckup.com/services/black-box-vs-white-box-testing.aspx>

*Pwn Pad 2014*. (s.d.). Récupéré sur store.pwnieexpress: <https://store.pwnieexpress.com/product/pwn-pad-2014-penetration-testing-tablet/>

Revenssis. (2014, 02 16). *Revenssis Penetration Testing Suite*. Récupéré sur sourceforge: <https://sourceforge.net/projects/revenssis/>

Security, O. (2013). *Official Kali Linux Documentation*.

Upton, E. (2012). *Android 4.0 is coming !* Récupéré sur raspberrypi: <https://www.raspberrypi.org/blog/android-4-0-is-coming/>

Victor. (s.d.). *Android sur le Raspberry Pi*. Récupéré sur the-raspberry: <http://the-raspberry.com/android-sur-le-raspberry-pi>

*What is a DDoS Attack*. (2013). Récupéré sur digitalattackmap: <http://www.digitalattackmap.com/understanding-ddos/>

## Déclaration de l'auteur

Je déclare, par ce document, que j'ai effectué le travail de Bachelor ci-annexé seul, sans autre aide que celles dûment signalées dans les références, et que je n'ai utilisé que les sources expressément mentionnées. Je ne donnerai aucune copie de ce rapport à un tiers sans l'autorisation conjointe du RF et du professeur chargé du suivi du travail de Bachelor, y compris au partenaire de recherche appliquée avec lequel j'ai collaboré, à l'exception des personnes qui m'ont fourni les principales informations nécessaires à la rédaction de ce travail et que je cite ci-après : -.

Sierre, le 25 juillet 2016

Jérémie Vianin