République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par
Ouahiba BENNABI

Thème

Détection d'intrusions dans un système Android

Mémoire soutenu publiquement le 13/07/ 2016 devant le jury composé de :

M LAZRI Mourad
Maitre de conférences A, UMMTO, Président

M OUALLOUCHE Fethi
Maitre de conférences B, UMMTO, Encadreur

M KHADIR Wahab
2int, Co-Encadreur

M SEHAD Mounir
Maitre de conférences B, UMMTO, Examinateur

M HAMEG Slimane
Maitre assistant A, UMMTO, Examinateur

Remerciements

En premier lieu, je remercie Dieu le tout puissant de m'avoir accordé la volonté et la puissance pour réaliser ce travail.

Je tiens à exprimer mes sincères remerciements à mon promoteur Mr OUALLOUCHE de m'avoir guidé dans mon travail et de m'avoir aidé à trouver des solutions pour avancer.

J'exprime également mes remerciements à mon co-encadreur Mr KHADIR pour son aide, ses encouragements et son travail.

Je remercie également les membres du jury qui me feront l'honneur de juger mon travail.

Ainsi qu'à toutes les personnes qui m'ont apporté leur soutien et qui ont ainsi contribué à l'élaboration de ce mémoire.

Dédicaces

Je dédie ce modeste travail à ma famille pour leur aide et leurs encouragements

et à toutes personnes qui me sont chères.

Glossaire

ADSL: Asymmetric Digital Subscriber Line

API: Application Programming Interface

ARP: Adress Resolution Protocol

DHCP: Dynamic Host Configuration Protocol

DMZ: Dé-Militarized Zone

DNS: Domain Name System

DoS: Denial of Service

FTP: Foiled Twisted Pair

GPS: Global Positioning System

IDS: Intrusion Detection System

IP: Internet Protocol

IPS: Intrusion Prevention System

MAC: Medium Access Control

MITM: Man In The Middle

NAT: Network Adress Translation

OFDM: Orthogonal Frequency Division Multiplexing

OS: Operating System

OSI: Open Source Inder

Glossaire

PDA: Personal Digital Assistant

PCI: Peripheral Component Interconnect

SSID: Service Set Identifier

USB: Universal Serial Bus

WEP: Wired Equivalent Privacy

WECA: Wireless Ethernet Compatibility Alliance

WLAN: Wireless Local Area Network

Wi-Fi: Wireless Fidelity

WPA: Wireless Protocol Access

Sommaire

Introduction générale 1

Chapitre I : Généralités sur les réseaux sans fils

1. Historique 3
2. Définition des réseaux sans fil 3
3. Technologie Wi-Fi 3
   - 3.1. Définition du Wi-Fi 3
     - 3.1.1. Avantages du Wi-Fi 4
     - 3.1.2. Inconvénients du Wi-Fi 5
4. Les normes physiques du Wi-Fi 5
   - 4.1. La norme 802.11a 6
   - 4.2. La norme 802.11b 6
   - 4.3. La norme 802.11g 6
5. Les équipements Wi-Fi 6
   - 5.1. Carte réseaux Wi-Fi 6
   - 5.2. Routeurs 7
   - 5.3. Modems /Routeurs 8
   - 5.4. Points d'accès 8
6. Les couches du Wi-Fi 8
   - 6.1. La couche physique 9
   - 6.2. La couche liaison de données 9
7. Les techniques de transmission dans les réseaux sans fil 9
   - 7.1. Transmission par les ondes infrarouges 9
   - 7.2. Transmission par les ondes radio 9
8. Le système d'exploitation Android 10
   - 8.1. Architecture Android 11
     - 8.1.1. Linux kernel 12
     - 8.1.2. Librairies 12
     - 8.1.3. Application framework 12
     - 8.1.4. Applications 13
   - 8.2. Historique des versions d'Android 13
9. Discussion 14

Sommaire

Chapitre II : La sécurité informatique

1. Préambule 15
2. Définition de la sécurité 15
3. Les objectifs de la sécurité 15
   - 3.1. La disponibilité 15
   - 3.2. La confidentialité 15
   - 3.3. L'intégrité 16
   - 3.4. L'authentification 16
   - 3.5. Le contrôle d'accès 16
4. Les hackers 16
5. Types de hackers 16
   - 5.1. White hat 16
   - 5.2. Black hat 17
   - 5.3. Grey hat 17
6. Les phases du hacking 17
   - 6.1. La reconnaissance 18
   - 6.2. Scanning 18
   - 6.3. Gaining access 18
   - 6.4. Maintaining access 18
   - 6.5. Clearing tracks 19
7. Attaques et intrusions informatiques 19
   - 7.1. Les attaques informatiques 19
     - 7.1.1. Types d'attaques 19
       - a. ARP Spoofing 19
       - b. DNS Spoofing 20
       - c. Déni de service 20
       - d. Déni de service distribué : 21
       - e. Désauthentification 22
       - f. Sniffing : 22
       - g. Evil Twin 23
       - h. Man In The Middle 24
   - 7.2. Les intrusions informatiques 24

Sommaire

7.2.1. Types d'intrusions 25

a. Phishing 25

b. Trojans Android 25

c. Backdoor 25

d. Ingénierie sociale 26

8. Les méthodes de protections contre ses différentes attaques et intrusions 26

8.1. La cryptographie 26

8.2. Le pare-feu 28

8.3. Le proxy 29

8.4. Les systèmes de détection d'intrusions IDS 29

8.5. Les systèmes de prévention d'intrusions 30

8.6. La zone démilitarisée DMZ 30

9. Discussion 31

Chapitre III : Tests d'intrusions et outils de détection des intrusions

1. Préambule 32

2. Partie I : Test d'intrusion 33

2.1. Objectif d'un test d'intrusion : 33

2.2. Application 33

2.2.1. Présentation du projet 33

2.2.2. Principe du projet 34

2.2.3. Objectif de l'intrusion 34

2.2.4. Outils de développement 34

2.2.5. Technologie utilisée 35

2.2.6. Réalisation du test d'intrusion 36

a. Création du payload (Trojan Android) 36

b. Création du faux point d'accès 37

c. La désauthentification 39

3. Partie II 41

3.1. Les mesures de sécurité 41

3.1.1. L'Antivirus 41

a. Principe de fonctionnement 41

Sommaire

3.1.2. Reverse engineering 41
3.2. Application 42
3.3. Outils utilisés 42
3.4. Réalisation 42
3.4.1. L'antivirus Kaspersky 43
3.4.2. Reverse engineering 50
4. Discussion 59

Conclusion générale 60

Bibliographie 61

I. Mise en place d'une machine virtuelle :

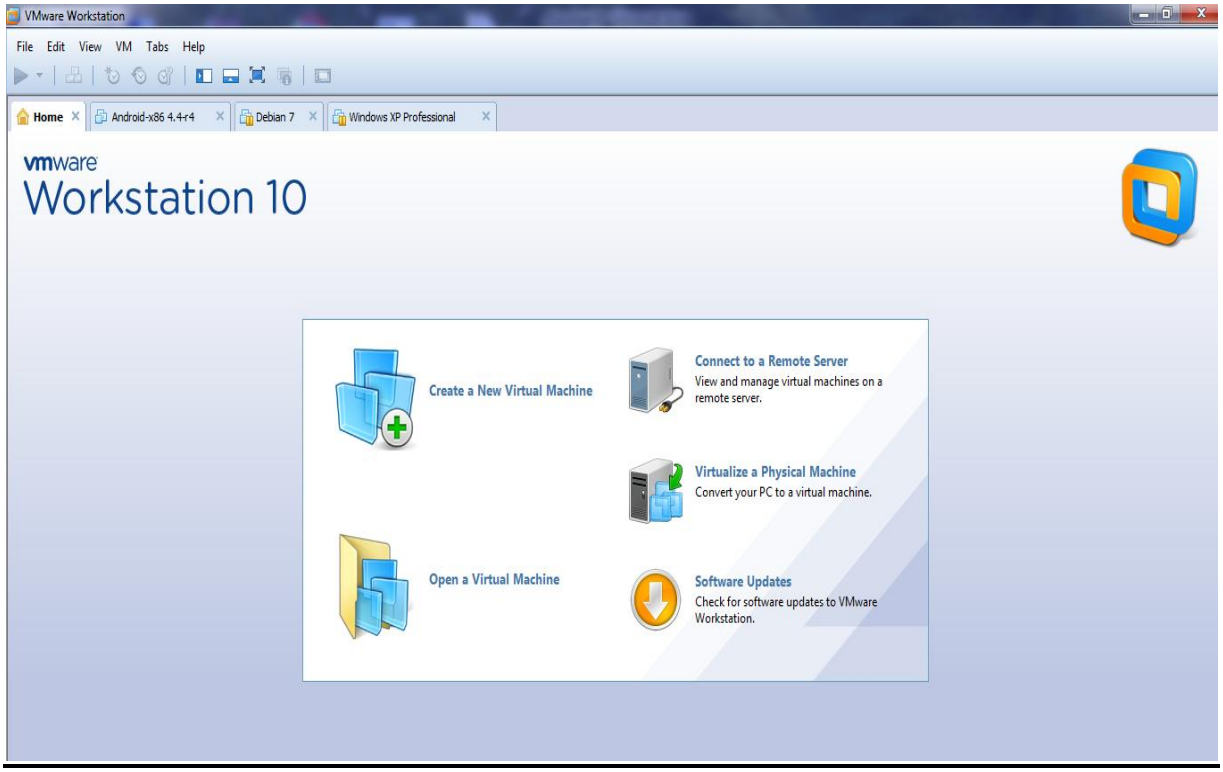
La virtualisation est une technique consistant à faire fonctionner en même temps, sur un seul ordinateur, plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts, à l'aide d'un logiciel de virtualisation appelé VMware Workstation.

➢ VMware Workstation 10 :

C'est la version station de travail du logiciel. Permet la création d'une ou plusieurs machines virtuelles au sein d'un système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

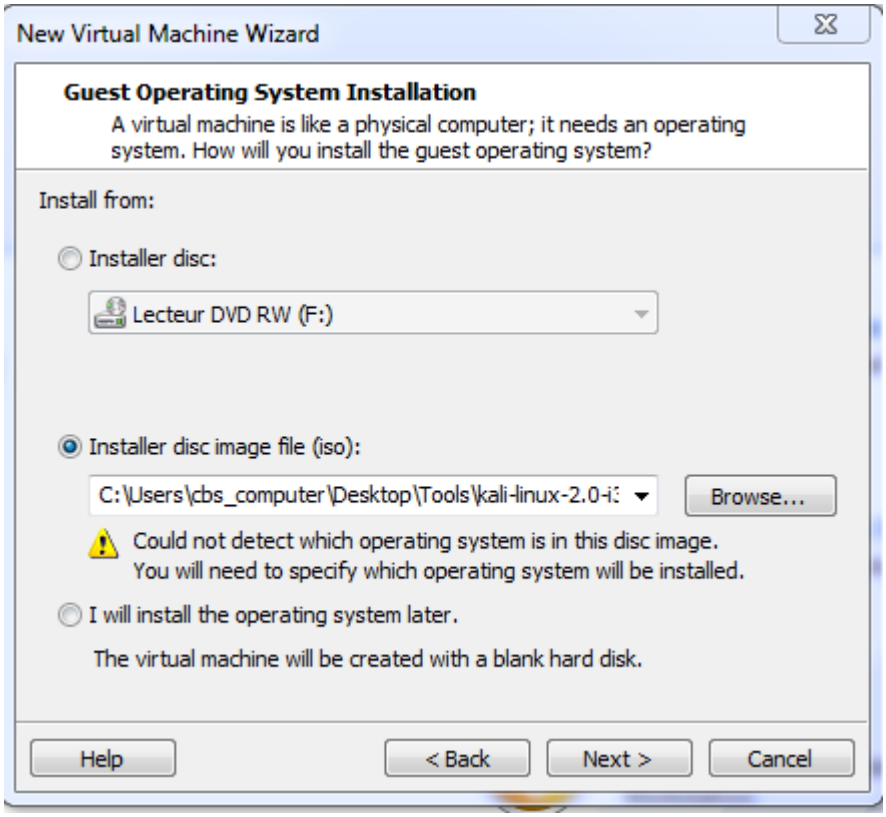
➢ Istallation de kali linux 2.0 sur la VMware Workstation 10 :

1. Lancer le programme VMware Workstation 10 et cliquer dans le menu présenté sur l'interface ci-dessous, sur create a new Virtuel Machine (créer une nouvelle machine virtuelle).

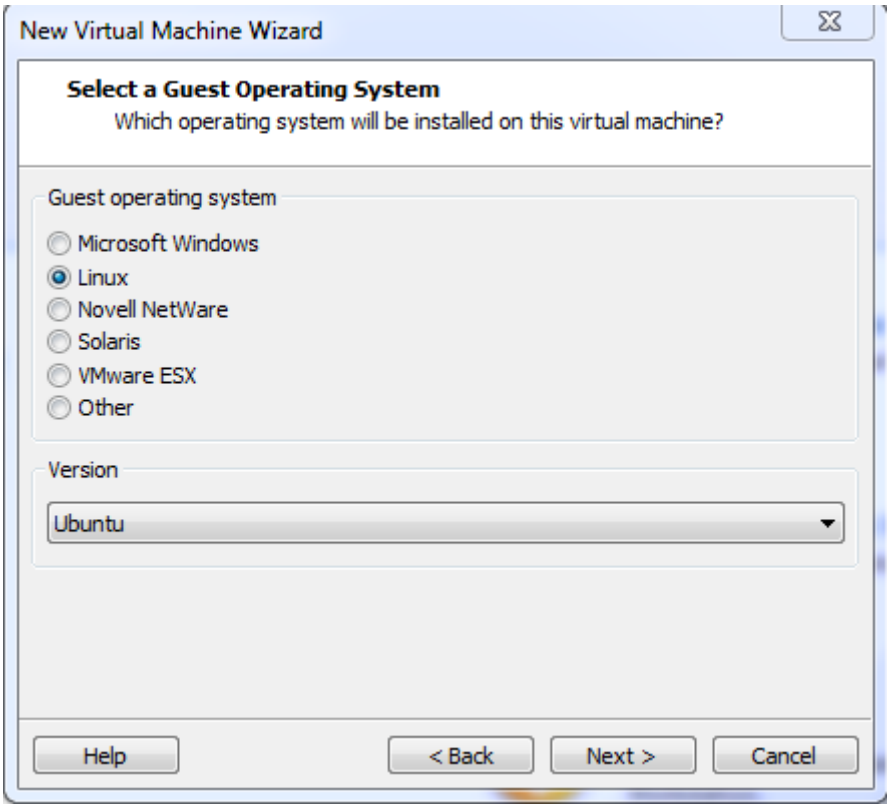


2. Sélectionner le premier choix « Typical (recommended) ».

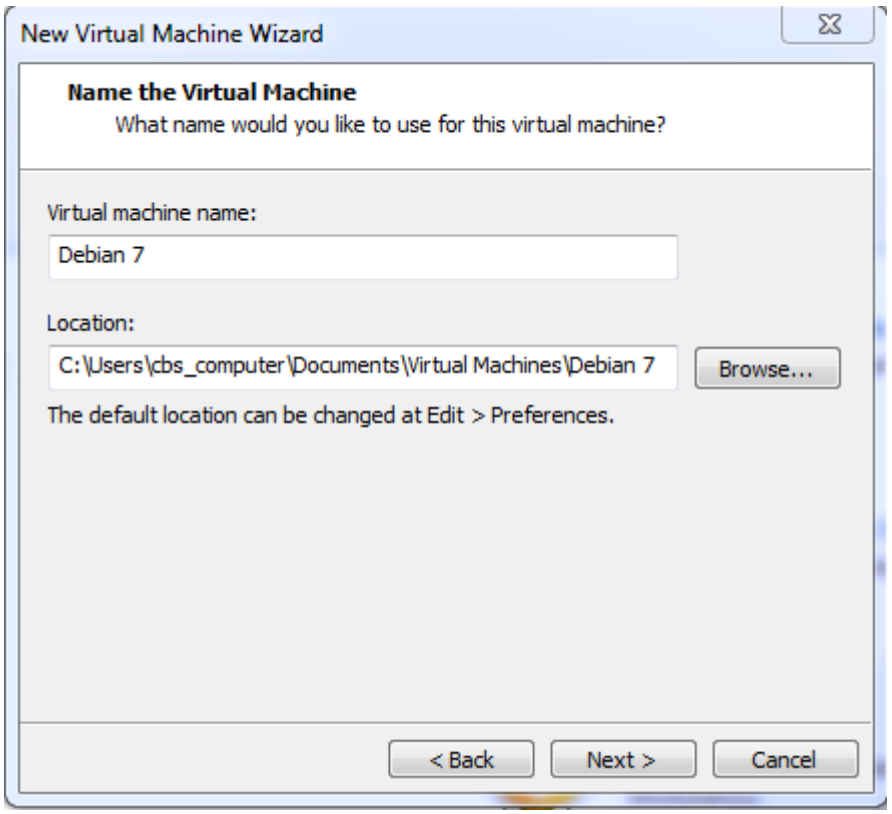
3. Choisir l'option « installer un fichier image ISO » et télécharger l'image existante sur la machin physique, puis cliquer sur Next.



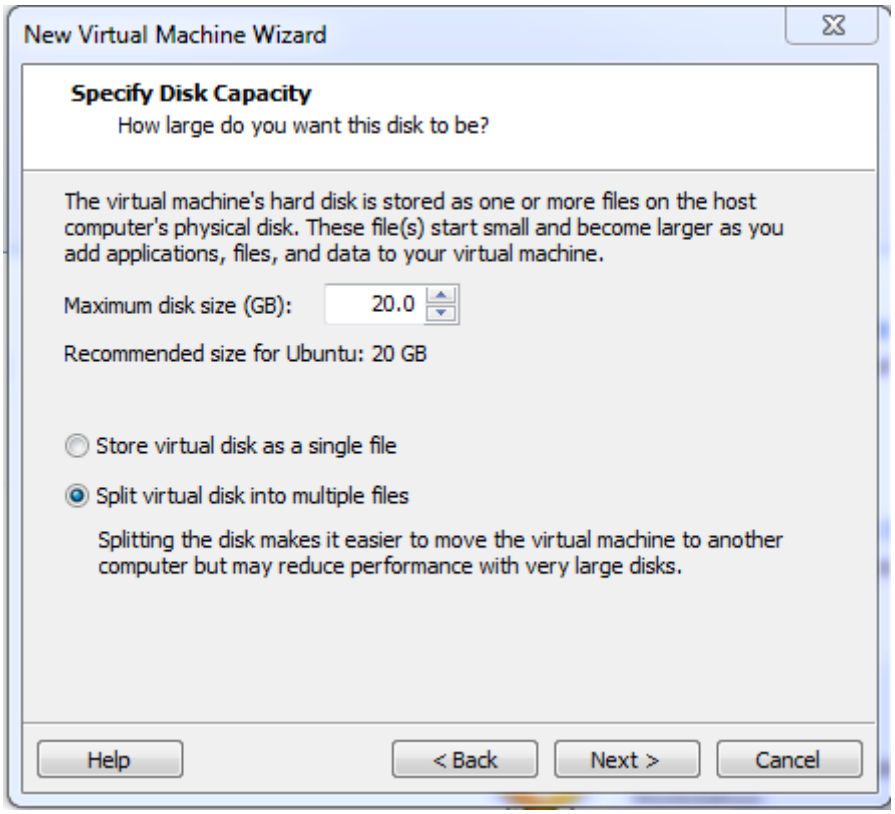
4. Choisir le système d'exploitation Linux puis cliquer sur Next.



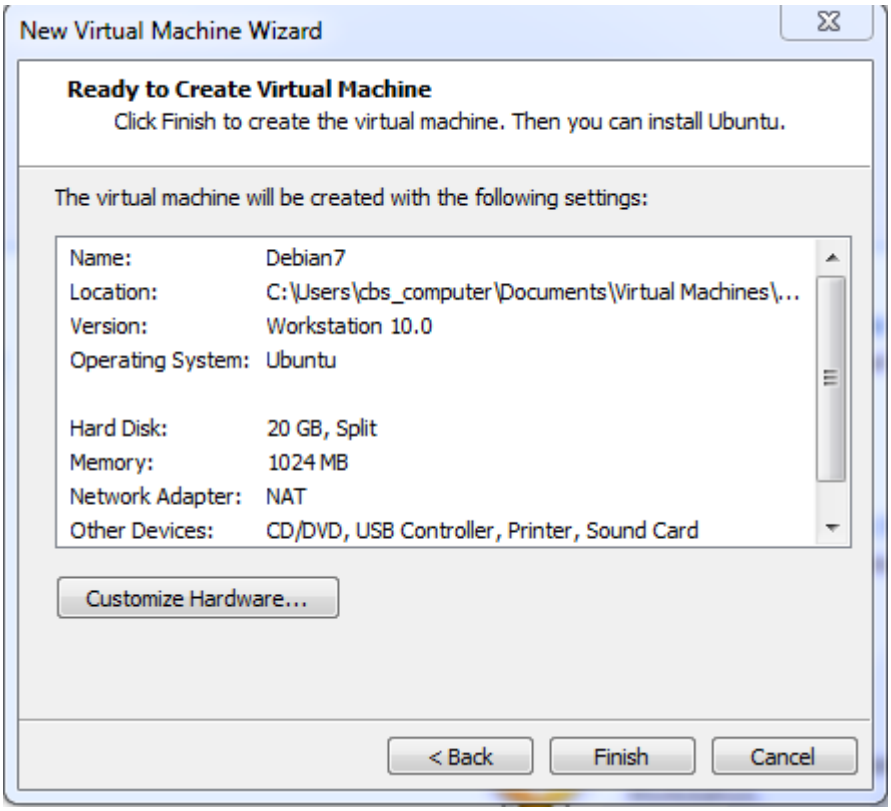
5. Donner un nom à la nouvelle machine créée puis cliquer sur Next.



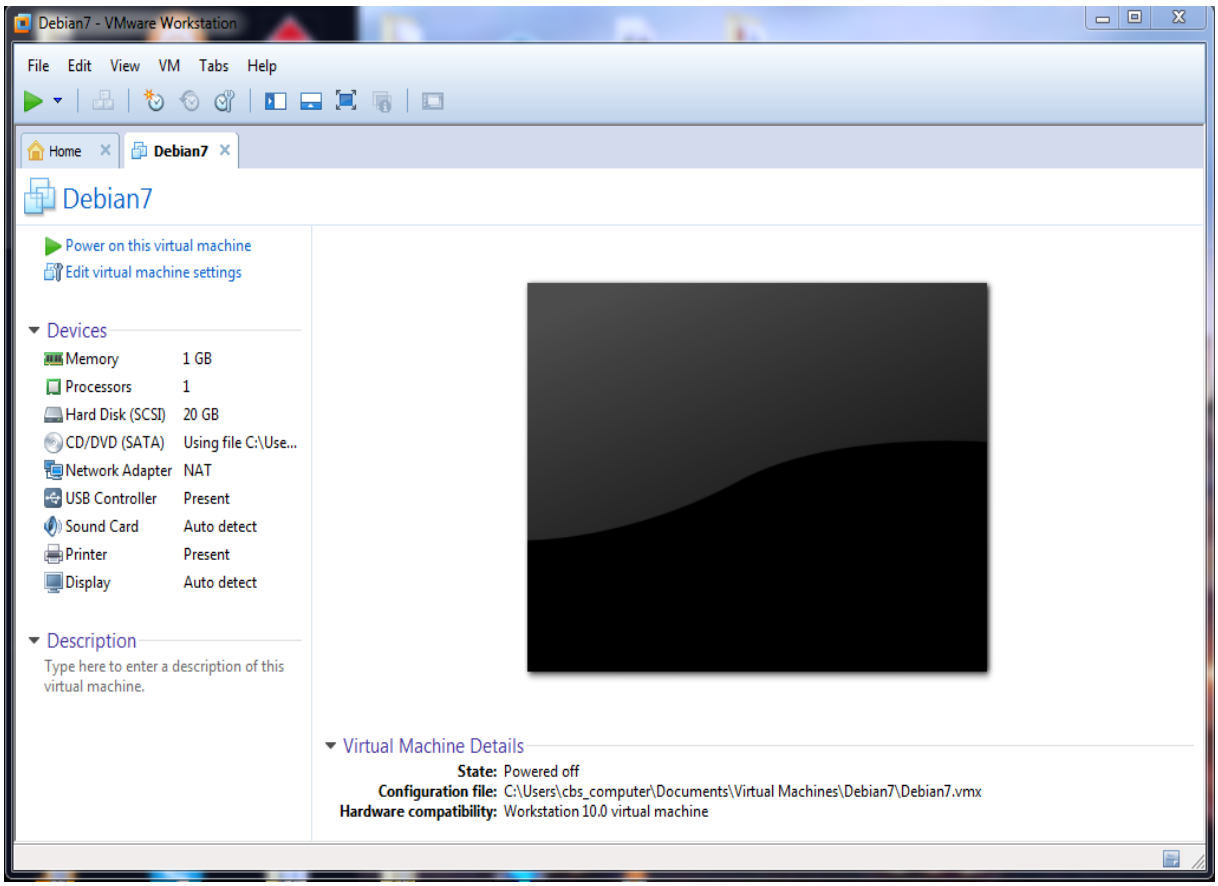
6. Choisir une capacité pour le disque, 20GB recommandé.



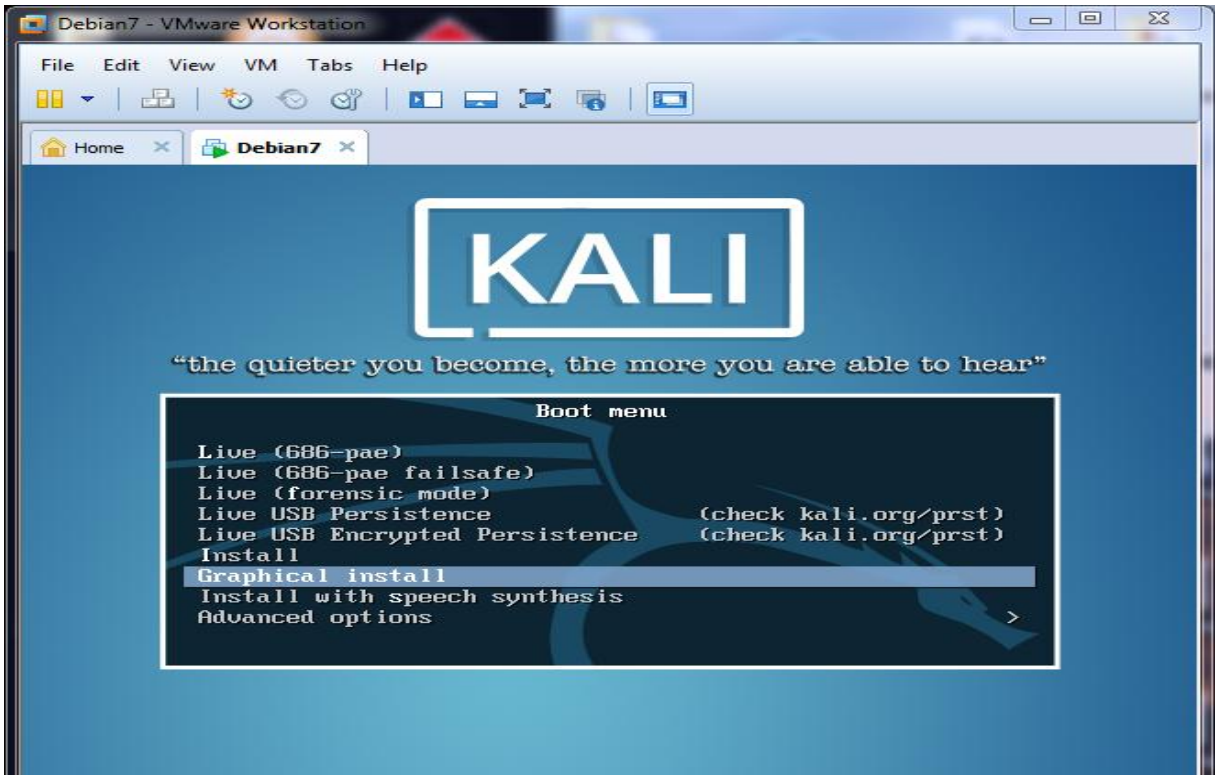
7. Cliquer sur « Finish ».



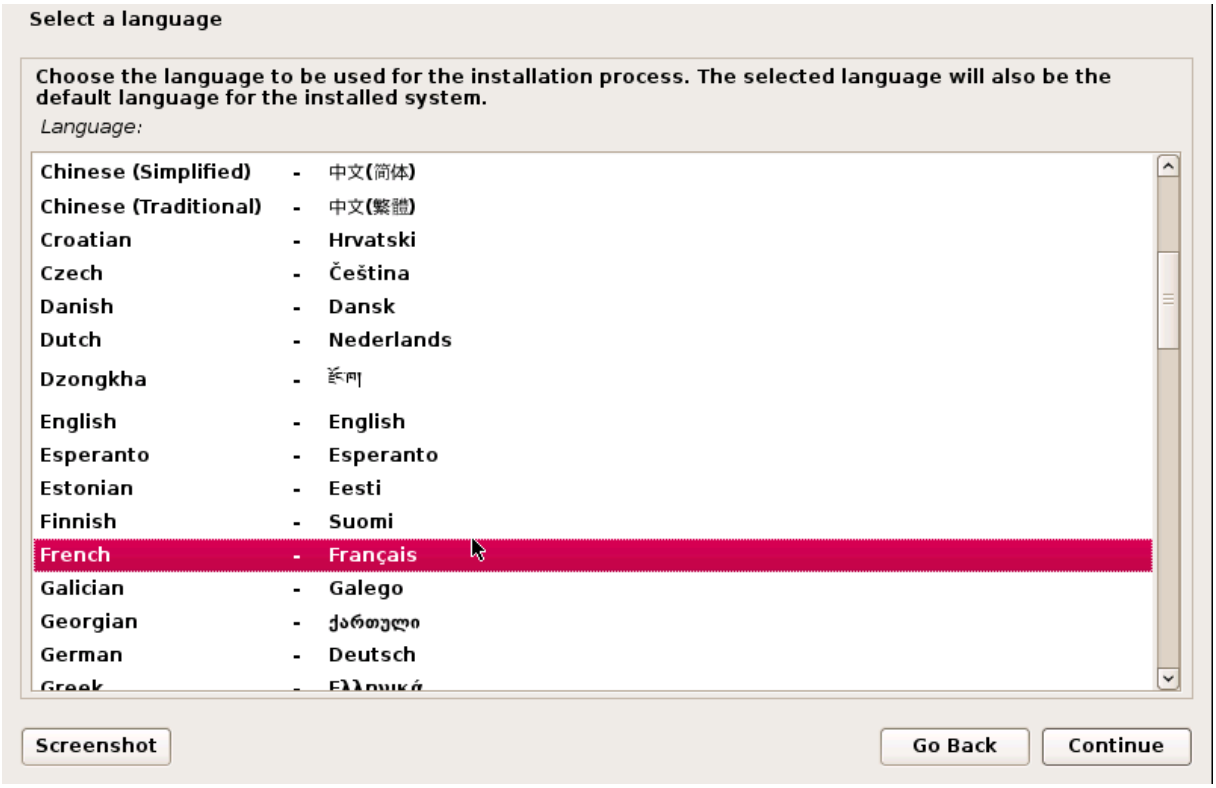
8. Cliquer sur « Power on this virtual machine » pour commencer l'installation de Kali Linux.



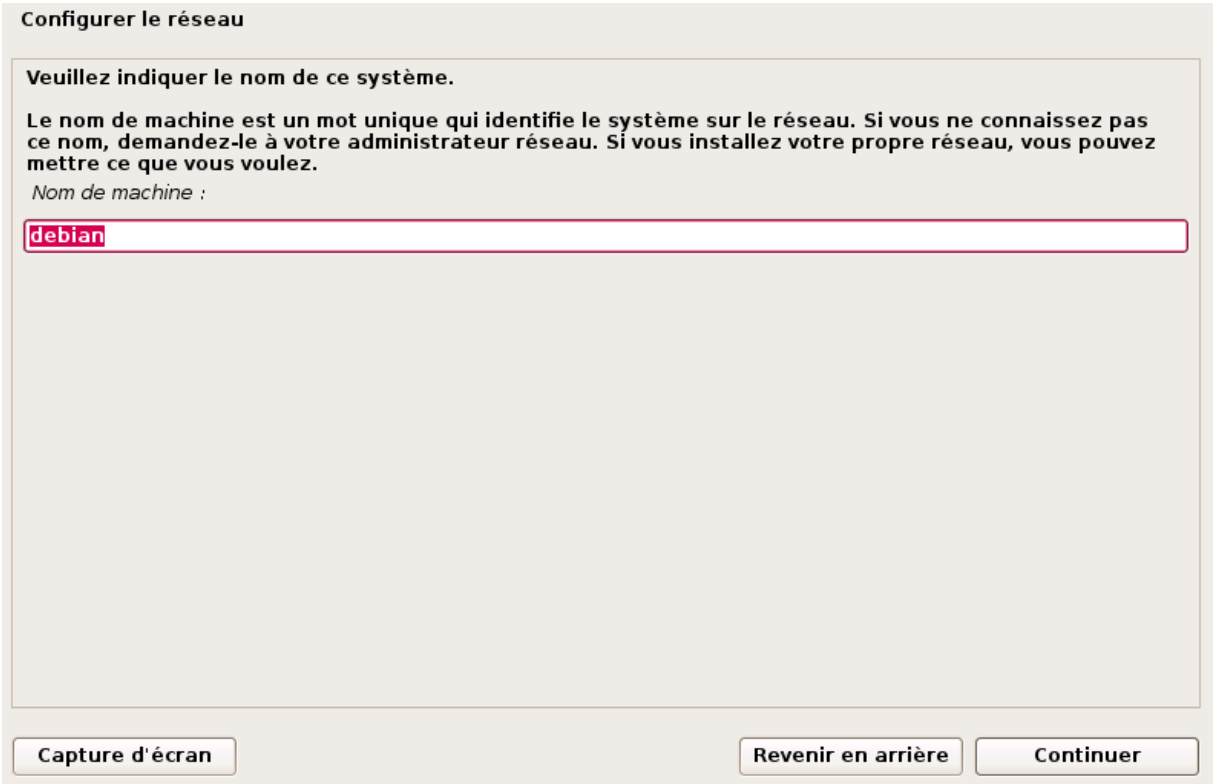
9. Choisir « Graphical install » puis appuyer sur entrée pour démarrer.



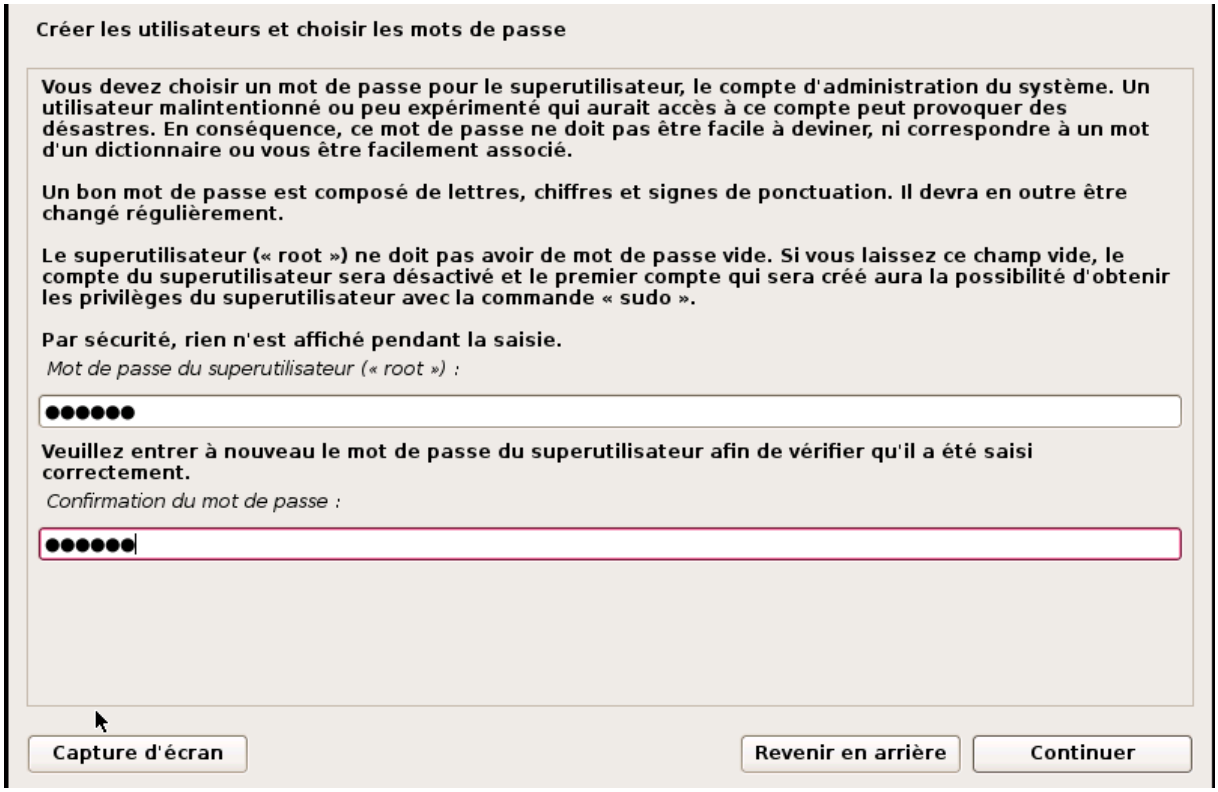
10. Choisir la langue d'installation puis continuer.



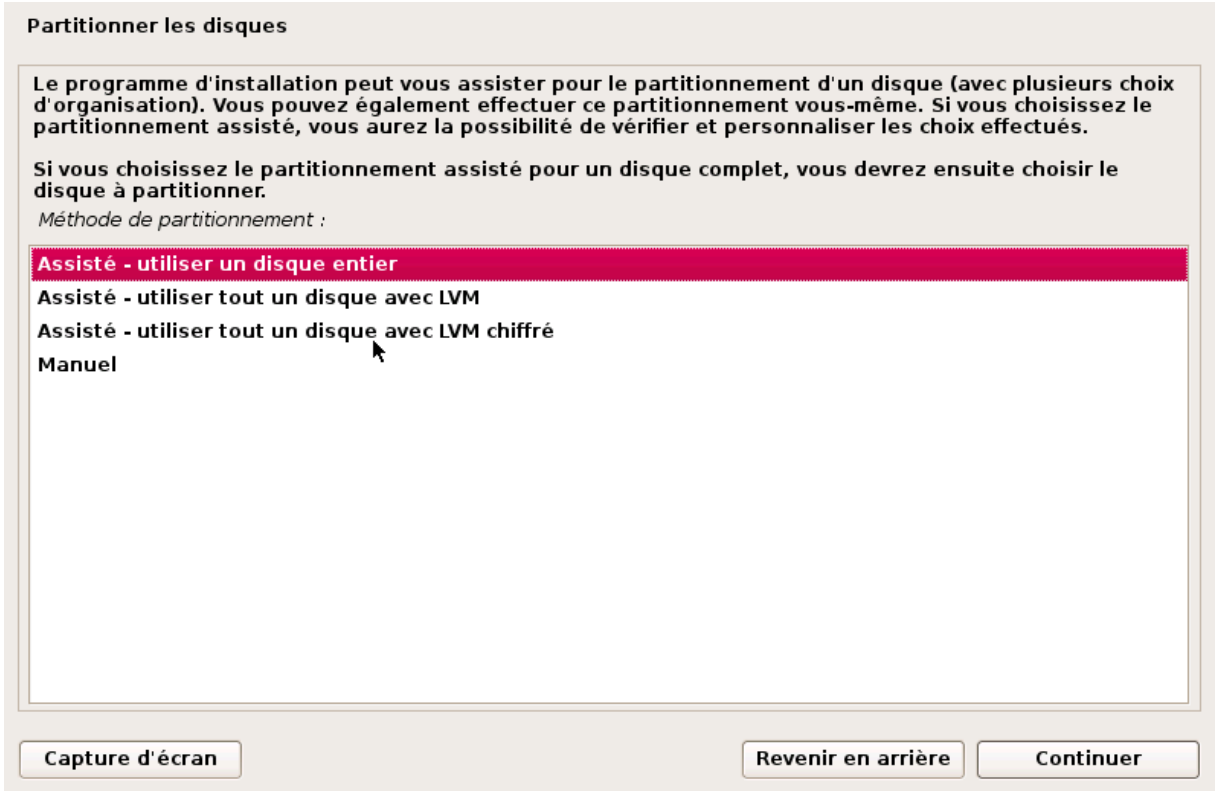
11. Donner un nom à la machine, puis cliquer sur Next.



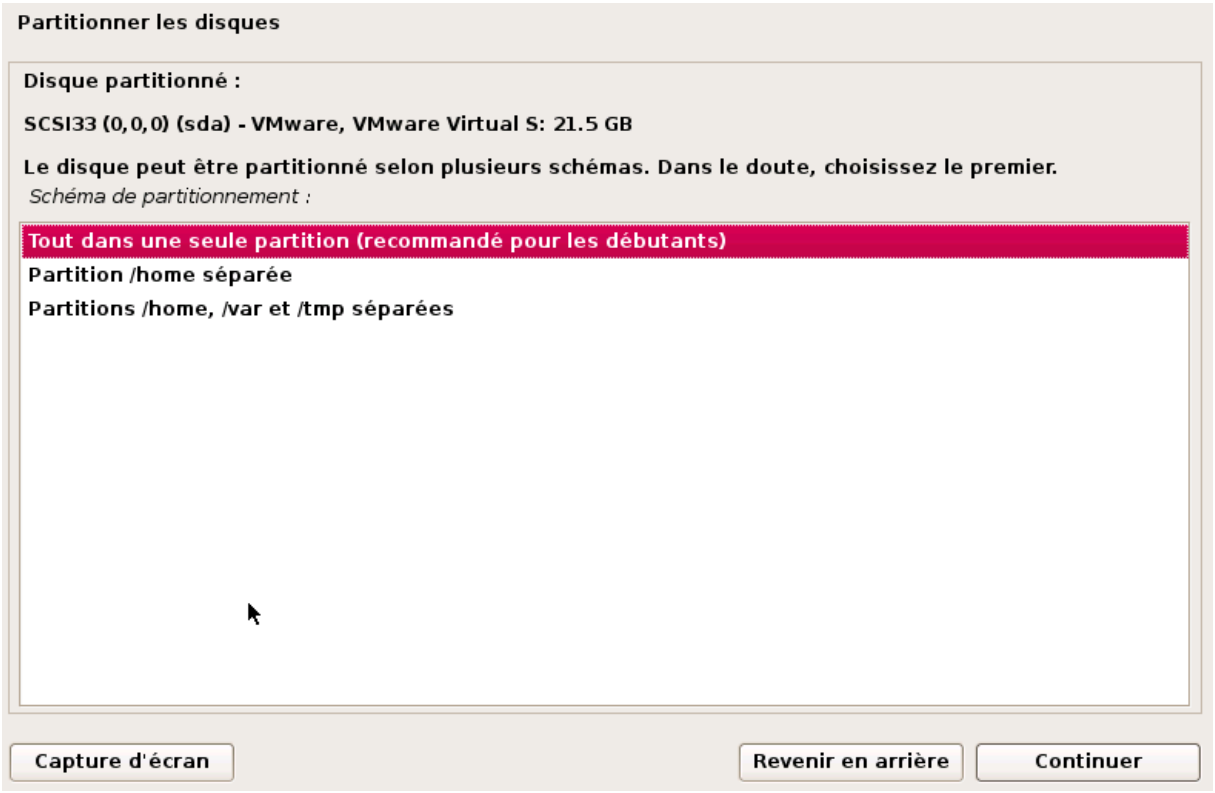
12. Entrer un mot de passe pour le compte administrateur « root ».



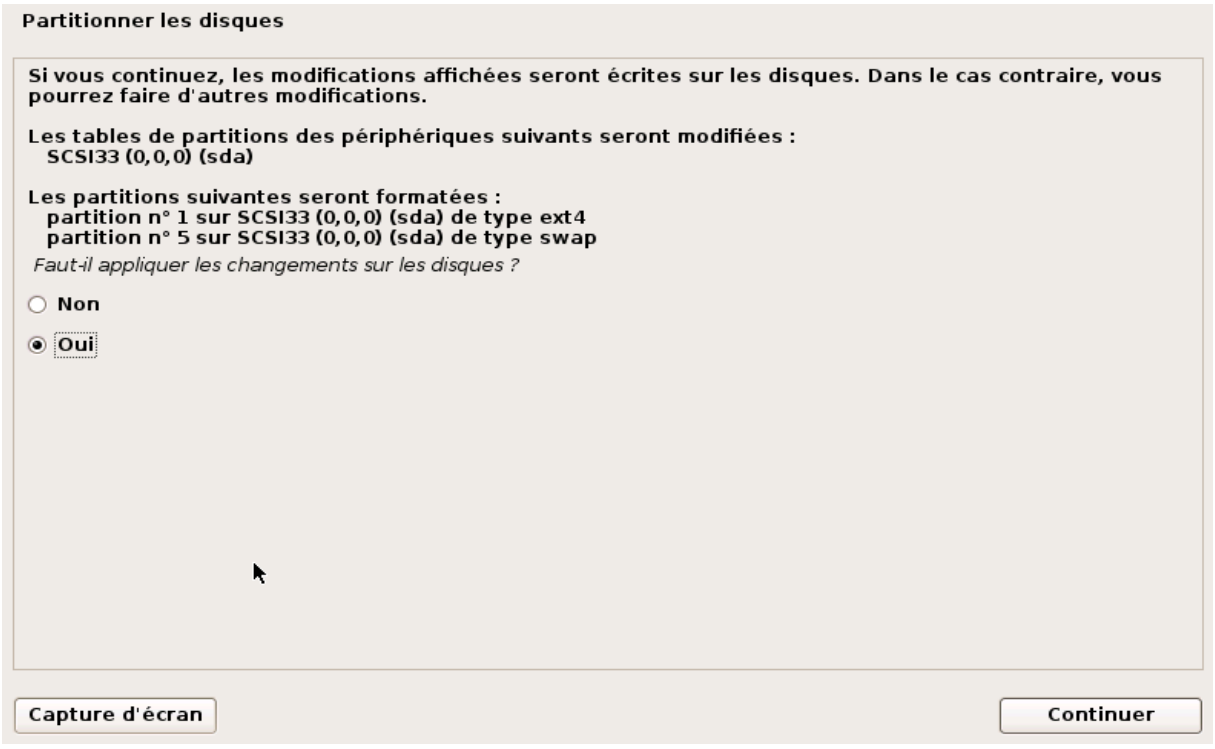
13. Utiliser un disque entier, puis cliquer sur Continuer.



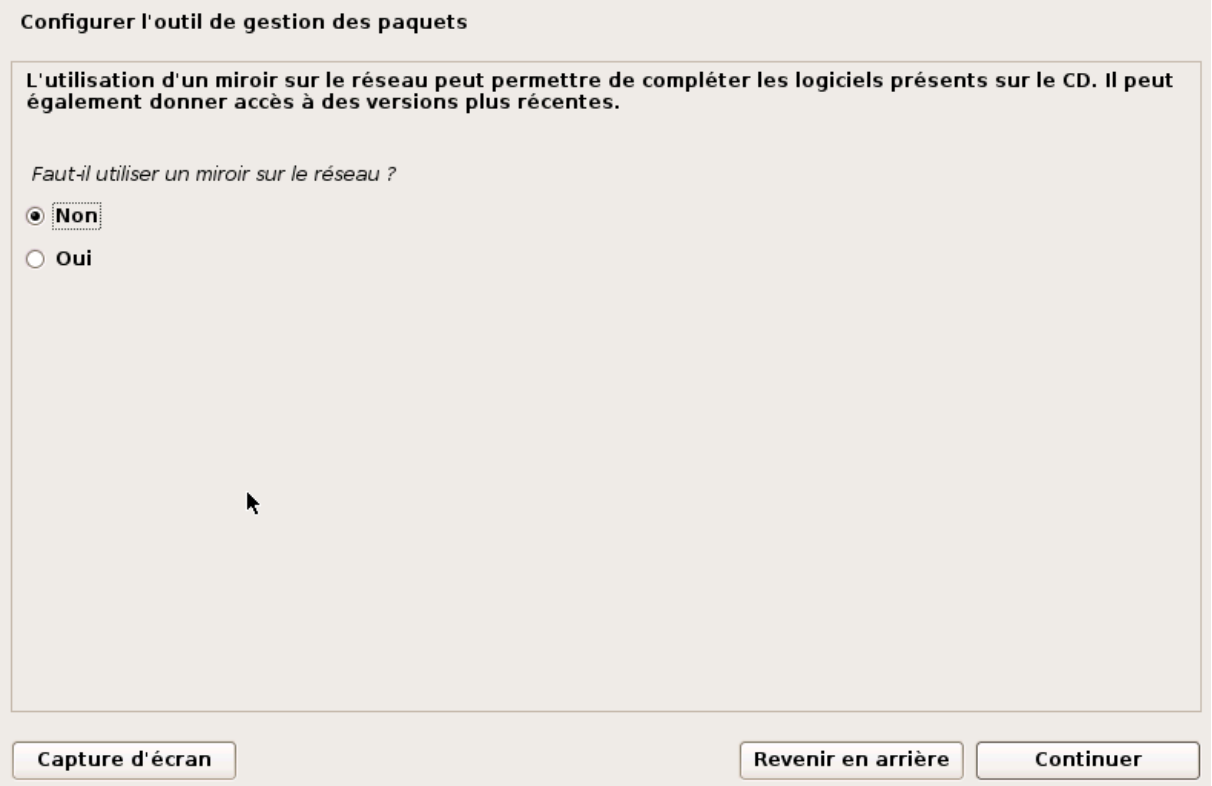
14. Choisir « Tout dans une seule partition » qui est recommandé, puis cliquer sur Continuer.



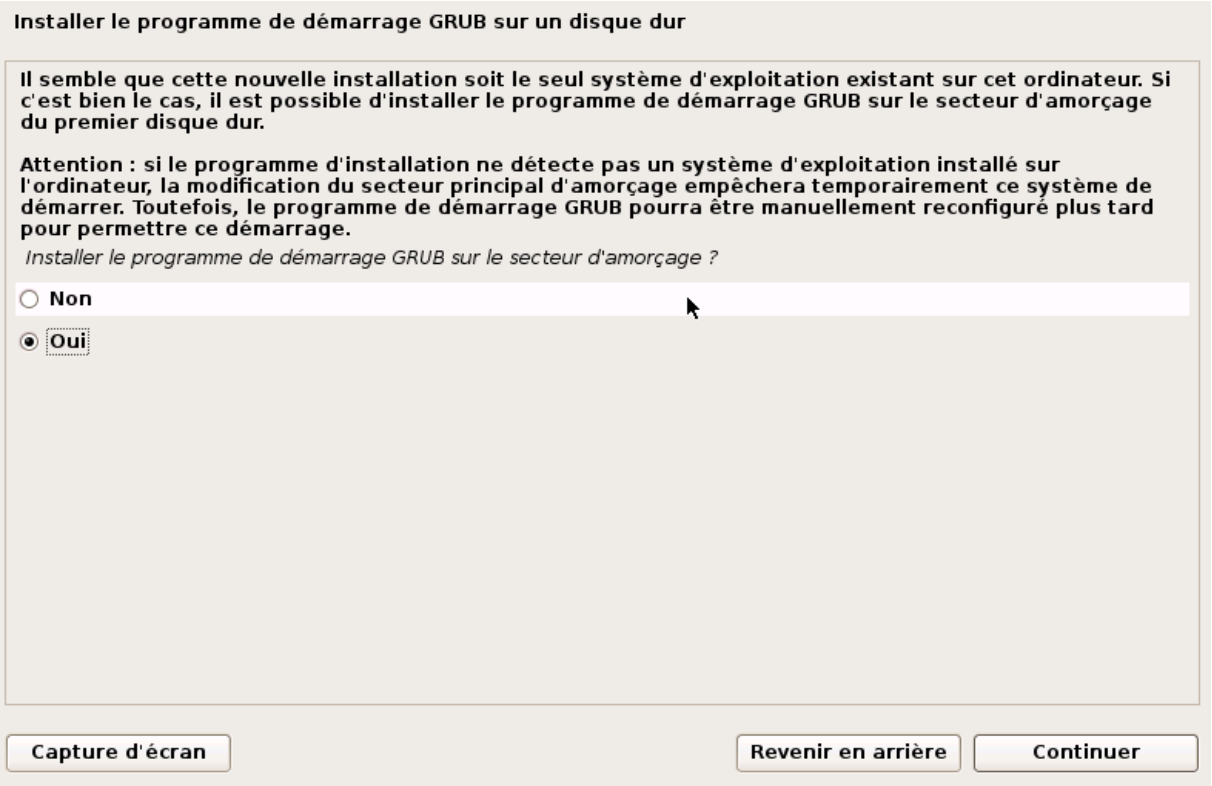
15. Une possibilité de réviser les changements avant de continuer cette opération irréversible. Cliquer sur Continuer.



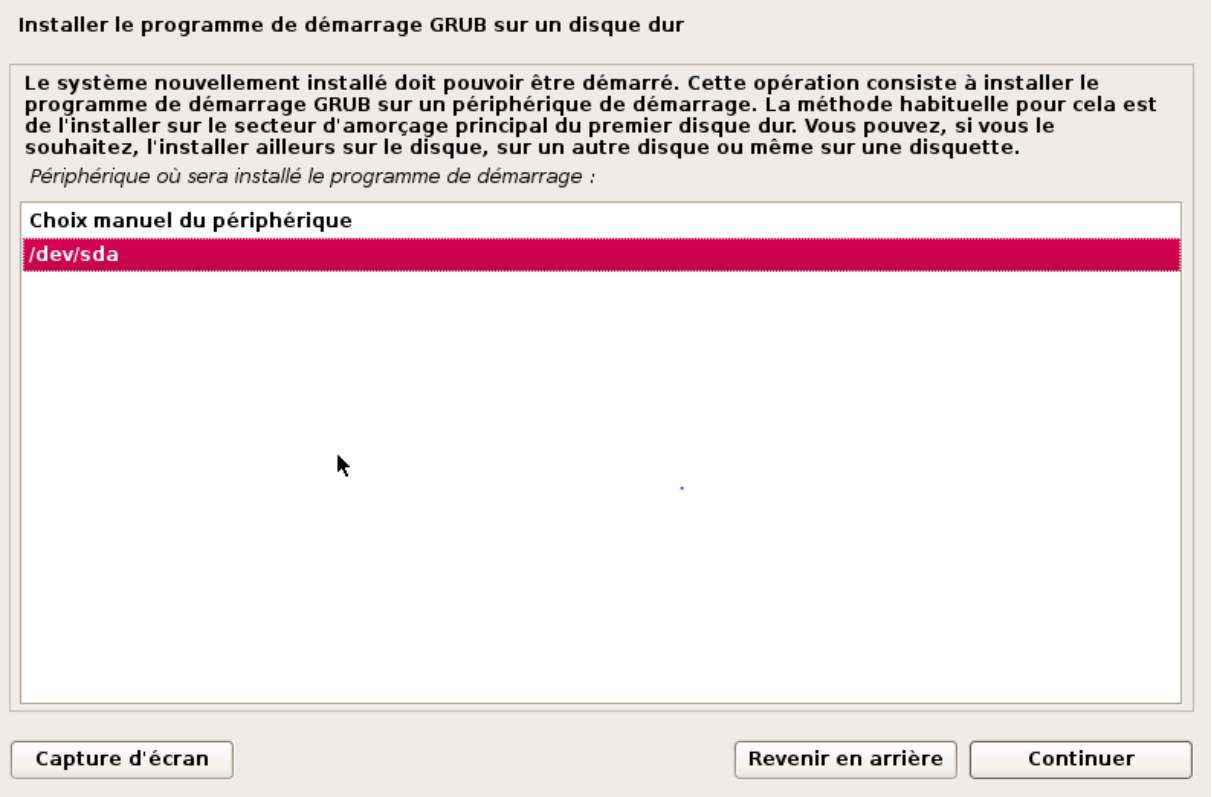
16. Choisir « Non », puis cliquer sur Continuer.



17. Choisir « Oui » pour installer le GRUB qui donne à l'utilisateur la possibilité de démarrer plusieurs programmes, puis cliquer sur Continuer.

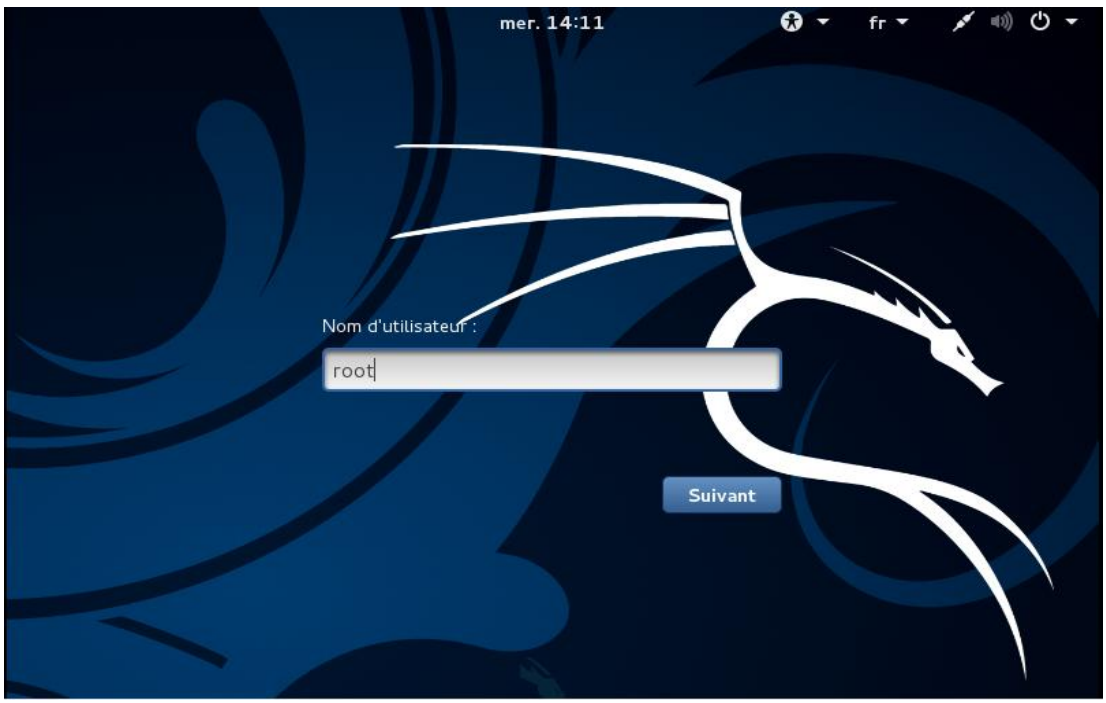


18. Cliquer sur Continuer.

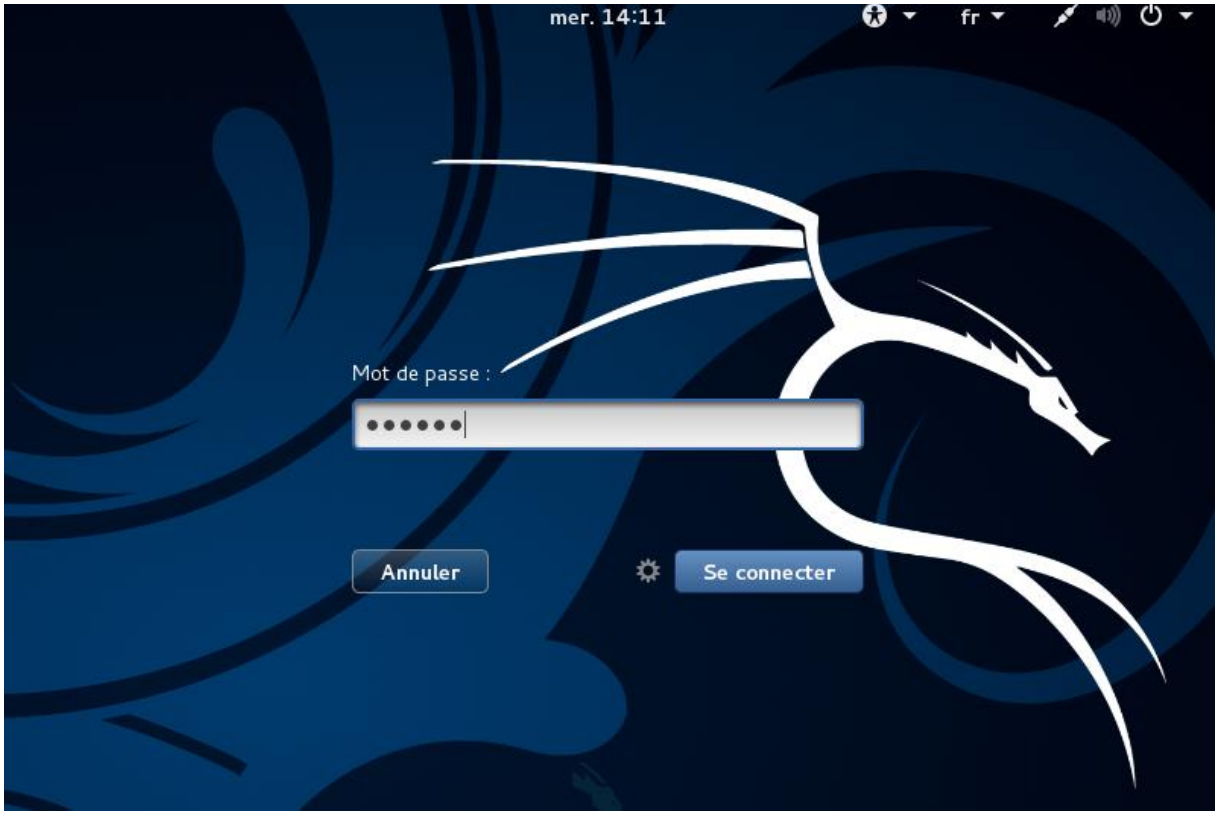


19. Reste seulement à cliquer sur Continuer et kali linux va démarrer automatiquement.

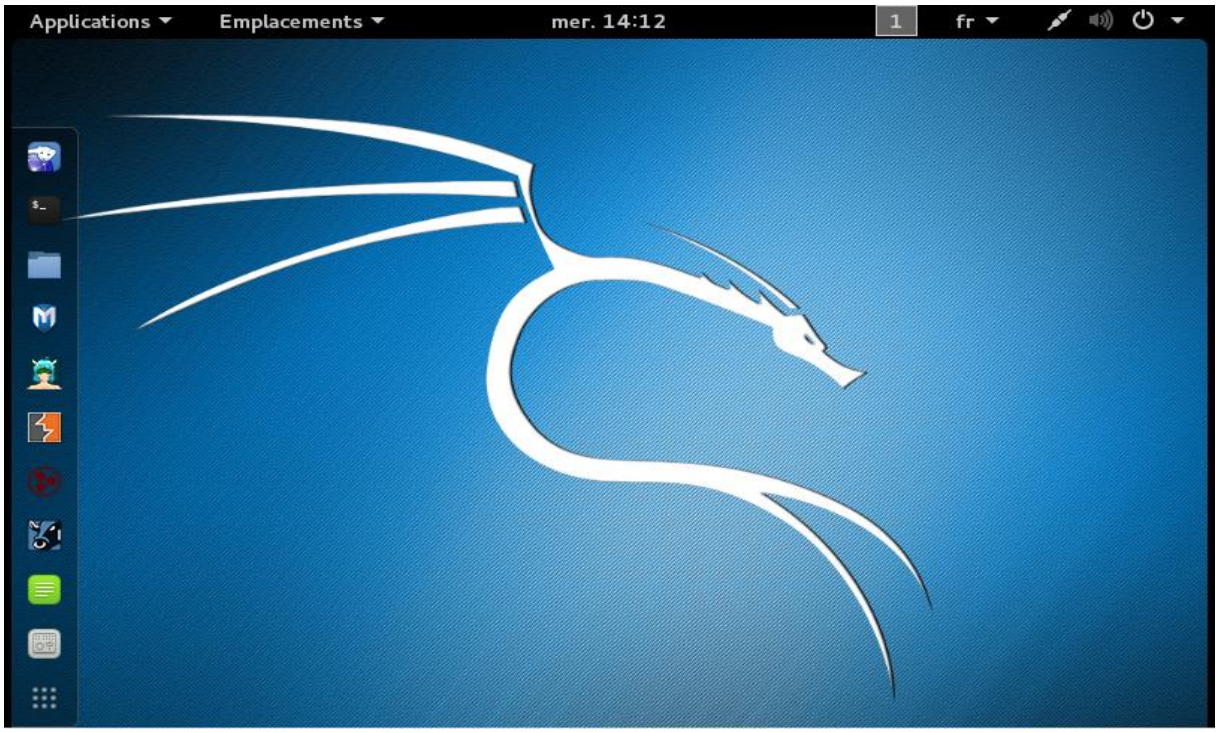
20. Après le démarrage de kali linux 2.0, il ne reste qu'à saisir le nom d'utilisateur.



21. Puis saisir le mot de passe pout y accéder.



Voici maintenant le bureau de kali linux 2.0



Liste des figures

Chapitre I : Généralités sur les réseaux sans fil

Figure 1 : Carte réseau sans fil....7

Figure 2 : Routeur....7

Figure 3 : Modem/Routeur....8

Figure 4 : Architecture Android 11

Chapitre II : La sécurité informatique

Figure 5 : Les phases du hacking 17

Figure 6 : ARP spoofing.... 20

Figure 7 : Attaque DoS 21

Figure 8 : L'attaque DDos.... 21

Figure 9: Désauthentification.... 22

Figure 10 : L'attaque sniffing 23

Figure 11: Evil Twin 23

Figure 12: Attaque Man In The Middle.... 24

Figure.13 : La cryptographie symétrique 27

Figure.14 : La cryptographie asymétrique 27

Figure.15 : Le fonctionnement d'un pare-feu.... 28

Figure.16 : Le fonctionnement d'un proxy 29

Figure.17 : Architecture DMZ.... 30

Liste des figures

Chapitre III : Tests d'intrusion et outils de détection des intrusions

Figure 18 : Icone du Trojan sur le bureau 36

Figure 19 : Ouverture d'un port sur msfconsole 37

Figure 20 : Activation du service web 38

Figure 21 : Création du point d'accès « 2intpartners » 38

Figure 22 : Configuration de l'interface at0 38

Figure 23: Déconnection des utilisateurs du point d'accès légitime 39

Figure 24: La page phishing de l'application à télécharger 39

Figure 25 : Console Meterpreter sur Metasploit 40

Figure 26 : Téléchargement de Kaspersky pour Android 43

Figure 27 : Activation d'un administrateur de l'appareil 44

Figure 28 : Détection des virus 45

Figure 29 : Résultats du scan Kaspersky 46

Figure 30 : Détection afin de désinstaller le virus 47

Figure 31 : Désinstallation de l'application 48

Figure 32 : Smartphone protégé 49

Figure 33 : Télécharger l'outil dex2jar 50

Figure 34 : Modification de l'extension en .zip 50

Figure 35 : Extraction du fichier classes.dex 51

Figure 36 : Les différents choix disponibles 51

Figure 37 : Conversion du fichier « .dex » en «. jar » 52

Figure 38 : Résultat de la commande de conversion 52

Liste des figures

Figure 39 : Menu principale de l'application APK-Multi-Tool 53

Figure 40 : Décompression et décompilation du fichier .APK..... 53

Figure 41 : Contenu du dossier Android.APK par APK-Multi-Tool 54

Figure 42 : Contenu du fichier AndroidManifest.xml 54

Figure 43 : Java Decompiler 55

Figure 44 : Ouverture de Java Decompiler 55

Figure 45 : Ouverture du fichier .JAR crée précédemment par l'outil Dex2Jar 56

Figure 46 : Ouverture du fichier classes.jar 56

Figure 47 : Contenu de la class MainActivity 57

Figure 48 : Contenu de la class Payload et extraction de l'adresse IP du hacker..... 58

INTRODUCTION

La transmission d'informations et le souci d'assurer la confidentialité de celles-ci est devenue un point primordial et une problématique essentielle que ce soit pour les entreprises, ou pour les individus toujours plus nombreux à se connectés sur Internet [1]. La sécurité informatique est donc aujourd'hui devenue vitale [2]. Il est donc important de définir une politique de sécurité et de veiller à son respect.

Lancé en 2007, Android est devenu en quelques années le système d'exploitation le plus répandu sur les plateformes mobiles de type Smartphone et tablette [3]. Puisque chaque année ce système s'améliore et apporte de nouvelles fonctionnalités aux utilisateurs.

L'utilisation des Smartphones a changée au cours du temps. En effet, actuellement nous utilisons les Smartphones pour différents domaines (images, audio, vidéos). Par conséquent, les données stockés sont très importantes et ne doivent pas être aux mains de personnes mal intentionnées.

Le système d'exploitation Android suscite l'intérêt des hackers qui voient dans ce système une cible potentielle d'attaque au même niveau que les ordinateurs de bureau à cause de la diversité des données et services [3]. Il devient alors nécessaire d'effectuer des tests d'intrusions afin de découvrir les failles existante et développer des outils de détection de ces attaques afin les détecter.

Dans le cas de notre projet de fin d'études, nous nous intéresserons à la détection d'intrusions sous un système Android. A cet effet, nous commençons par effectuer un test d'intrusions sur un Smartphones dans lequel nous allons nous introduire grâce à une fausse application. Ensuite nous allons détecter cette intrusion et installer un Antivirus pour empêcher d'éventuelles intrusions.

Nous avons scindé le présent mémoire en trois chapitres :

Dans le premier chapitre, nous allons présenter des généralités sur les réseaux sans fil ainsi que le système d'exploitation Android.

Le deuxième chapitre sera consacré à la sécurité informatique et les différentes attaques et intrusions qui peuvent avoir lieux.

Dans le troisième chapitre, nous allons présenter notre application et les outils de sécurité utilisés.

Enfin, nous allons terminer notre mémoire par une conclusion et une bibliographie.

1. Historique :

Les réseaux sans fil ont été créés en 1945 pour améliorer les communications de l'armée américaine pendant la deuxième guerre mondiale puisque ce type de réseau est caractérisé par son spectre qui est largement étendu. Après leur création, des entreprises commerciales ont commencé à exploiter cette technologie.

En 1971, la technologie sans fil à connu un véritable essor par AlohNet qui est un projet consacré par l'université de Hawaii [4]. Ce projet a permis à sept ordinateurs de communiquer depuis les différentes îles en utilisant un concentrateur central Oahu.

Par conséquent, les recherches qui ont été faites sur AlohNet ont posé les bases de la première génération de réseaux sans fil qui régissaient sur la plage de fréquences 901-928 MHz utilisée notamment par les militaires [4]. Cette phase de progrès des réseaux sans fil n'a connu que peu d'utilisateurs à cause de son faible débit.

2. Définition des réseaux sans fil :

Un réseau sans fil (Wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux périphériques (ordinateur, PDA, imprimante, routeur, etc.) peuvent communiquer sans liaison filaire mais plutôt par les ondes radioélectriques (hertziennes). Ce type de réseaux permet aux utilisateurs de se déplacer dans un certain périmètre de couverture sans perdre le signal.

Les réseaux sans fil offrent aussi la facilité de relier des équipements distants d'une dizaine de mètres à quelques kilomètres [5] et leur installation est très facile et ne demande pas beaucoup d'aménagements des infrastructures existantes.

3. Technologie Wi-Fi :

3.1. Définition du Wi-Fi :

Le Wi-Fi (contraction de Wireless Fidelity) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Wi-Fi correspond initialement au nom

donné à la certification délivrée par la WECA (Wireless Ethernet Compatibility Alliance), organisme ayant pour mission de spécifier l'interopérabilité entre les matériels répondant à la norme 802.11 [5].

Cette technologie permet de relier plusieurs appareils informatiques (ordinateurs, routeurs, …) à une liaison haut débit (11Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert [5].

3.1.1 Avantages du Wi-Fi :

a. La mobilité :

Le Wi-Fi offre la possibilité aux utilisateurs de rester connectés en se déplaçant sur un périmètre géographique plus ou moins étendu.

b. La facilité :

Un réseau Wi-Fi bien configuré permet de se connecter très facilement, à condition, bien sûr, de posséder une autorisation. Il suffit généralement de se trouver dans la zone de couverture pour être connecté.

c. La souplesse d'installation :

La souplesse d'installation du Wi-Fi permet d'adapter facilement la zone d'action en fonction des besoins. Si le point d'accès est trop faible, on ajoute des répéteurs pour étendre la couverture.

d. Le coût :

La plupart des éléments du réseau Wi-Fi (point d'accès, répéteurs, antennes…) peuvent être simplement posés. L'installation peut donc parfois se faire sans le moindre outillage, ce qui réduit les coûts de main-d'œuvre. Le budget de fonctionnement est similaire à un réseau filaire.

e. L'évolutivité :

La facilité d'extension ou de restriction du réseau permet d'avoir toujours une couverture Wi-Fi correspondant aux besoins réels.

3.1.2. Inconvénients du Wi-Fi :

a. La qualité et la continuité du signal :

Un réseau Wi-Fi bien installé et bien configuré est généralement fiable et d'une qualité constante. Cependant, il suffit parfois de peu pour perturber le signal : un radar de gendarmerie ou un émetteur Bluetooth, par exemple.

b. La sécurité :

Le Wi-Fi étant un réseau sans fil, il est possible de s'y connecter sans intervention matérielle. Cela veut dire qu'il faut particulièrement étudier la sécurisation du réseau si l'on veut éviter la présence d'indésirables ou la fuite d'informations.

c. La complexité de gestion :

Le premier problème auquel l'administrateur réseau est confronté, est la diversité des compétences nécessaires à la mise en œuvre d'un réseau Wi-Fi. Il faut prendre en considération les problèmes de transmission radio, un éventuel audit du site, l'intégration de l'existant (réseau câblé, mais peut être aussi les quelques ilots Wi-Fi déjà en place), le respect de régulation, le support effectif des standards actuels et à venir, l'administration de ce futur réseau, le monitoring du trafic, etc.

4. Les normes physiques du Wi-Fi :

Les normes physiques correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents débits en fonction de la portée.

4.1. La norme 802.11a :

La norme 802.11a permet d'obtenir un haut débit de 54 Mbits/s, pour une portée d'environ une trentaine de mètres seulement [5]. Cette norme s'appuie sur un codage du type OFDM (Orthogonal Frequency Division Multiplexing) sur la bande de fréquence 5 GHz.

4.2. La norme 802.11b :

La norme 802.11b permet d'obtenir un débit de 11 Mbits/s, pour une portée d'environ une cinquantaine de mètres en intérieur et jusqu'à deux cent mètres en extérieur. Elle utilise la bande des 2,4 GHz [5].

4.3. La norme 802.11g :

La norme 802.11g permet d'obtenir un débit de 54 Mbits/s, pour une portée équivalente à celle de la norme 802.11b [5]. Cette norme s'appuie sur un codage OFDM sur la bande de fréquence 2,4 GHz. La norme est compatible avec la norme 802.11b, ce qui signifie que des matériels conformes à celles-ci peuvent fonctionner en 802.11b.

5. Les équipements Wi-Fi :

Il existe plusieurs types d'équipements Wi-Fi, parmi lesquels on peut situer :

5.1. Carte réseaux Wi-Fi :

Une carte réseau (Network Interface Card) constitue l'interface entre l'ordinateur et le câble du réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau. Elle peut être incluse dans la carte mère ou on peut la trouver sous forme d'une carte PCI ou d'une clé USB. Chaque carte réseau dispose d'une adresse MAC ou adresse physique unique qui lui est affectée par le constructeur.

Figure .1 : Carte réseau sans fil

5.2. Routeurs :

Centre névralgique de toute installation, connectés à un modem haut débit, le routeur transforme la connexion Internet filaire en connexion sans fil. La plupart des routeurs font office de borne sans fil offrant l'accès Internet à tous les ordinateurs. Ils disposent également de ports Ethernet (en générale quatre) pour raccorder physiquement les postes les plus proches et certains offrent une sécurité pour le réseau en étant dotés de firewall et de limitation d'accès.

Figure .2 : Routeur

5.3. Modems /Routeurs :

Un modem/routeur Wi-Fi intègre un modem câble ou ADSL (Asymmetric Digital Subscriber Line). C'est une solution « tout en un » idéal pour les petites entreprises qui souhaitent raccorder quelques postes à Internet. Cet équipement sert alors à partager la connexion Internet entre les différents utilisateurs du réseau. Il est également équipé d'un serveur DHCP qui attribue une adresse IP à chaque poste client et d'un firewall qui assure la translation (NAT) entre les adresses IP locales et l'Internet et protège le réseau des attaques extérieures. Au niveau de la connectique, un modem/routeur Wi-Fi offre généralement les mêmes options qu'un routeur Wi-Fi.

Figure .3 : Modem/Routeur

5.4. Points d'accès :

Le point d'accès est l'un des éléments essentiels de l'architecture Wi-Fi [6], qui permet la communication entre les clients Wi-Fi. Ils peuvent en outre être reliés à un réseau filaire tel qu'un réseau local.

Les points d'accès sont caractérisés par le fait qu'il ne nécessite pas un ordinateur pour fonctionner. Ils sont totalement autonomes, leur configuration se fait via un ordinateur relié au réseau sur lequel se trouve le point d'accès. Bien entendu, il peut être relié à l'ordinateur par câble, mais cela n'est pas nécessaire.

6. Les couches du Wi-Fi :

Le standard 802.11 couvre les deux premières couches du modèle OSI, à savoir la couche physique et la couche liaison de données.

6.1. La couche physique :

Elle gère la communication avec l'interface physique afin de faire transiter ou de récupérer les données sur le support de transmission, en fournissant des moyens électriques (un bit doit être représenté par une tension de 5V), mécaniques (forme du connecteur, topologie…) fonctionnels ou procéduraux nécessaire à l'activation et à la désactivation des connexions physiques.

6.2. La couche liaison de données :

Cette couche s'occupe de la bonne transmission de données entre des machines reliées par un même support, cette couche détecte et corrige les erreurs de transmission, synchronise les données et contrôle le flux afin d'éviter l'engorgement du récepteur.

7. Les techniques de transmission dans les réseaux sans fil :

Il existe principalement deux méthodes pour la transmission dans les réseaux sans fil :

7.1. Transmission par les ondes infrarouges :

La transmission par les ondes infrarouges nécessite que les appareils soient en face l'un des autres et aucun obstacle ne sépare l'émetteur du récepteur (car la transmission est directionnelle). Cette technique est utilisée pour créer des petits réseaux de quelques dizaines de mètres (exemple de télécommande) [7].

7.2. Transmission par les ondes radio :

La transmission par les ondes radios est utilisée pour la création des réseaux sans fil qui ont plusieurs kilomètres. Les ondes radios ont l'avantage de ne pas être arrêtées par les obstacles car elles sont émises d'une manière omnidirectionnelle. Le problème de cette technique est les perturbations extérieures qui peuvent affecter la communication à cause de l'utilisation de la même fréquence par exemple.

8. Le système d'exploitation Android :

Tout a débuté avec une société américaine du nom d'Android, fondée en 2003. Celle-ci a été rachetée par Google en 2005 [8]. L'objectif premier était de développer un système d'exploitation qui permettrait aux utilisateurs d'interagir avec ce dernier.

Le système a été lancé en Juin 2007, et depuis il ne cesse d'évoluer pour satisfaire les besoins des utilisateurs. En 2015, Android est le système d'exploitation le plus utilisé dans le monde avec plus de 80% de parts de marché dans les Smartphones [8].

Android est un système d'exploitation open source. Conçu pour les Smartphones, les tablettes, les terminaux mobiles puis il s'est diversifié dans les objets connectés et ordinateurs comme les télévisions.

Ce système d'exploitation est fondé sur un noyau Linux, qui est le gros point fort d'Android puisque il est libre donc il offre beaucoup d'avantages parmi lesquels on peut citer la possibilité de consulter le code source à tout moment, le télécharger…, l'évolutivité du système puisqu'il est facilement portable d'un appareil à un autre, par ailleurs son fonctionnement même assure la possibilité de combiner des fonctionnalités (par exemple, la combinaison de l'appareil photo avec la géo localisation, pour définir des lieux associés à vos clichés). En dernier, la facilité de développement, car plusieurs APIs sont fournies en vue d'accélérer le développement, il est donc préférable d'apprendre à programmer sur ce système que sur un OS propriétaire [9].

8.1. Architecture Android :

Le système d'exploitation Android se compose de 4 couches principales, comme le montre le schéma suivant:

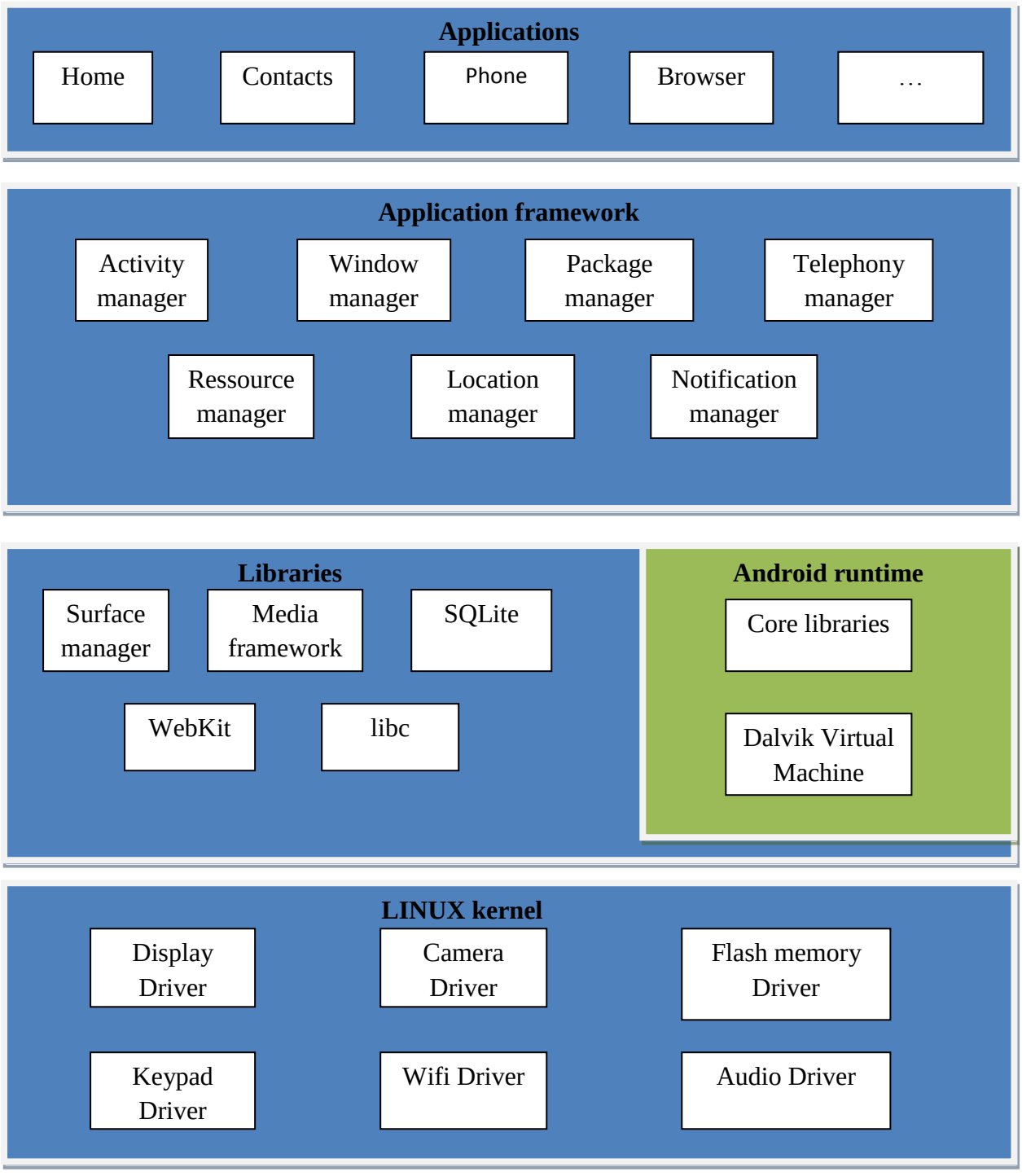


Figure .4 : Architecture Android [9]

8.1.1. Linux kernel :

Android se base sur un kernel (noyau) Linux version 2.6 conçu spécialement pour l'environnement mobile [8], qui se charge des services de base tels que la gestion des processus, la gestion de la mémoire, gestion du matériel (écran, clavier…), la gestion des capteurs (appareil photo, GPS…).

Cette couche fait en sorte qu'Android soit compatible avec tant de supports différents, elle est la seule couche qui gère le matériel, quand un constructeur veut ajouter un matériel qui n'est pas pris en compte par défaut par Android, il doit travailler sur le kernel et non pas sur les couches au-dessus.

8.1.2. Librairies :

C'est la couche des bibliothèques principales du système qui sont écrites en C et/ou C++. Elles fournissent des services essentiels tels que la gestion de l'affichage 2D et 3D, un moteur de base de données SQLite, la lecture et l'enregistrement audio et vidéo, un moteur de navigateur Web…

Directement sur cette couche vient se greffer le runtime Android, qui comprend la machine virtuelle Java et ses bibliothèques. Cette machine virtuelle, développée spécifiquement pour Android, porte le nom de Dalvik Virtual machine. Conçue pour fonctionner dans un environnement embarqué limité en ressources, elle utilise un format d'exécutable compressé (.dex), afin de minimiser l'empreinte mémoire [8].

8.1.3. Application framework :

En fournissant une plateforme de développement ouverte, Android offre aux développeurs la possibilité de créer des applications extrêmement riches et innovantes. Les développeurs sont libres de profiter du matériel périphérique, les informations de localisation d'accès, exécuter les services d'arrière-plan, définir des alarmes, ajouter des notifications de la barre d'état, etc.

8.1.4. Applications :

C'est la dernière couche, la seule finalement dont l'utilisateur aura à se préoccuper. Ces applications sont celles fournies par défaut, comme l'application d'accueil, gestionnaire de contacts, agenda, le navigateur web, l'application de téléphone, ainsi que celles qui seront installées plus tard par l'utilisateur. Elles sont sous forme de paquets .apk, qui permettent une installation et une désinstallation facile.

8.2. Historique des versions d'Android :

Le système d'exploitation Android connait un grand succès grâce à son évolution depuis son apparition, pour satisfaire les besoins des utilisateurs.

Date de sortie	Version	Nom	Sécurité
11 novembre 2007	1.0	/	
26 octobre 2009	2.0	Eclair	
22 février 2011	3.x.x	Honeycomb	
19 octobre 2011	4.0.x	Ice Cream Sandwich	Reconnaissance faciale (Face Unlock)
24 juillet 2013	4.3.x	Jelly Bean	protection par blocage en cas de perte ou vol
3 novembre 2014	5.0.x	Lollipop	
9 mars 2015	5.1.x	Lollipop	protection par blocage en cas de perte ou vol
5 octobre 2015	6.0	Marshmallow	support natif du capteur d'empreinte digitale

Tableau .1 : Les différentes versions d'Android

9. Discussion

Le réseau sans fil présente l'avantage d'être mobile, procure la facilité de se connecter au réseau, la souplesse d'installation, l'évolutivité puisqu'il est facile de faire une extension ou une restriction au réseau.

L'avènement du système d'exploitation Android a permis le développement de l'utilisation des Smartphones et tablettes. En effet, plusieurs applications actuellement fonctionnent avec ce système d'exploitation. Ce dernier présente beaucoup d'avantages puisqu'il offre la possibilité aux constructeurs d'apporter leur touche à l'application et la facilité de programmation. C'est un système open source, donc il est gratuit et aussi souple. Toutefois, comme tout système d'exploitation, Android fait face à des attaques.

1. Préambule :

Aujourd'hui, la majorité des foyers possèdent un accès à Internet et il est possible de se connecter avec le bout du monde où que l'on soit pour garder le contact avec ses proches ou travailler à distance… etc. Une réelle avancée technologique dans un monde où tout doit aller si vite, mais un véritable problème de fond en ce qui concerne la sécurité des données et de la vie privée de chacun.

Pour faire face à ce genre de situation, nous allons voir dans ce chapitre L'importance de la mise en place d'une politique de sécurité, l'identité des hackers, les différentes attaques et intrusions et quelques méthodes de protection pour mieux se défendre.

2. Définition de la sécurité :

La sécurité informatique est l'ensemble des techniques et méthodes conçues et mises en œuvre pour minimiser les vulnérabilités d'un système contre les menaces accidentelles ou intentionnelles.

3. Les objectifs de la sécurité :

Dans la sécurité informatique, on cherche à réaliser les fonctions suivantes :

3.1. La disponibilité :

L'objectif de cette fonction est de garantir l'accès à l'information et aux services de façon permanente qu'aux personnes (ou et ordinateurs) autorisées.

3.2. La confidentialité :

Consiste à assure que l'information est accessible seulement par les personnes autorisées à avoir l'accès.

3.3. L'intégrité :

Elle garantit la fiabilité d'une ressource ou d'une donnée en termes de prévention contre des changements non autorisés. L'information ne peut être modifiée que par les personnes autorisées.

3.4. L'authentification :

Elle consiste à assurer que seules les personnes autorisées aient l'accès aux ressources.

3.5. Le contrôle d'accès :

Il utilise l'identité authentifiée des entités ou des informations fiables pour déterminer leur droit d'accès à une ressource. Il peut enregistrer sous forme de trace d'audit et signaler toute tentative non autorisée d'accès. Il peut mettre en jeu les listes maintenues par des centres ou par l'entité accédée : des mots de passe, des jetons utilisés pour distribuer les droits d'accès.

4. Les hackers :

Les hackers sont des individus intelligents avec d'excellentes compétences en informatiques [2]. Chaque hacker a un but différents des autres, pour certains hackers, le hacking est juste un loisir, pour d'autres c'est pour acquérir un savoir ou faire des choses illégales et d'autres hackers le font avec mauvaise intention comme par exemple voler des données d'entreprise, avoir des mots de passe, avoir des informations confidentielles, etc.

5. Types de hackers :

Il existe de nombreux types de hackers catégorisés selon leur expérience et leurs motivations, parmi lesquels on peut citer :

5.1. White hat :

Un white hat est un individu qui possède des compétences d'un hacker, mais qu'il utilise pour des fins défensives. Le but d'un white hat est d'aider à améliorer des systèmes et technologies informatiques et de découvrir les vulnérabilités pas encore connues, sans en tirer profit de manière illicite.

5.2. Black hat :

Un black hat désigne généralement, les hackers révoltés contre le système, qui frôlent les limites de la loi, ou les dépassent carrément. Ils pénètrent par effraction dans les systèmes, dans un intérêt qui n'est pas celui du propriétaire du réseau ou du système, mais plutôt personnel, voire financier [2]. Un tel hacker peut détruire, voler et vendre des informations.

5.3. Grey hat :

Un grey hat est un peu un hybride du white hat et du black hat. C'est un hacker compétent, qui agit parfois avec l'esprit d'un white hat mais avec une philosophie de divulgation différente [2]. Son intention n'est pas mauvaise même s'il commet cependant occasionnellement un délit.

Par curiosité, par exemple il tentera de s'infiltrer dans un système. Une fois la faille trouvée, il n'endommagera pas le système, et préviendra généralement le propriétaire. Cependant ceci reste illégal dans la plupart des pays.

6. Les phases du hacking :

Le hacking réfère à l'exploitation des vulnérabilités des systèmes et compromettre les politiques de sécurité pour avoir un accès non autorisé ou non approprié aux ressources des ces systèmes. Pour se faire, le hacker passe par cinq phases distinctes.

Figure .5 : Les phases du hacking

6.1. La reconnaissance :

La reconnaissance est la phase préparatoire, où le hacker cherche à acquérir le maximum d'informations possible à propos de sa cible avant de lancer une attaque. Cette étape permet au hacker d'établir des stratégies sur son attaque pour qu'elle soit efficace.

On distingue deux types de reconnaissance :

- **La reconnaissance passive :**
  Elle permet au hacker d'acquérir des informations sans se déplacer ou interagir avec la cible.
- **La reconnaissance active :**
  Elle permet au hacker d'acquérir des informations directement en étant sur place.

6.2. Scanner : (Scanning)

La phase scanning réfère à la phase pré-attaque où le hacker scanne le réseau pour avoir des informations spécifiques sur la base des informations collectées durant la phase reconnaissance, telles que des adresses IP, Les systèmes d'exploitation, l'architecture du système, les applications installées.

6.3. Gagner l'accès : (Gaining access)

C'est la phase où le hacker obtient l'accès, soit au système, soit aux applications ou au réseau.

Après avoir obtenu cet accès, le hacker peut maintenant lancer des attaques.

6.4. Maintenir l'accès : (Maintaining access) :

C'est la phase où le hacker essaye de maintenir son accès administrateur obtenu dans la phase précédente. Le hacker peut bloquer les autres hackers d'avoir le même accès en sécurisant cet accès avec des backdoors, il peut envoyer, télécharger ou manipuler les données présentes sur le système et il peut aussi utiliser le système compromis pour lancer d'autres attaques.

6.5. Effacer les traces : (Clearing tracks)

C'est la dernière phase du hacking, où le hacker efface ses traces en effaçant les fichiers contaminés, les messages d'erreurs qui peuvent avoir été générés par le processus d'attaque etc, pour accéder au système en continu sans être repéré.

7. Attaques et intrusions informatiques :

7.1. Les attaques informatiques :

Une attaque informatique est une action malveillante qui consiste à tenter de contrôler les fonctions et les mesures de sécurité d'un système informatique, détruire, endommager ou altérer son fonctionnement normal.

7.1.1. Types d'attaques :

a. ARP Spoofing :

L'ARP spoofing est une technique utilisée pour attaquer un réseau local [1], dont l'objectif est de permettre de trouver l'adresse IP d'une machine connaissant l'adresse physique de sa carte réseau. Cette attaque consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet ARP falsifié indiquant que l'ARP (adresse MAC) de l'autre machine a changé, l'adresse ARP fournie étant celle du hacker. Les deux machines cibles vont ainsi mettre à jour leur table ARP, de cette manière, à chaque fois qu'une des deux machines communiquera avec la machine distante, les paquets seront envoyés au hacker qui les transmettra de manière transparente à la machine destinatrice.

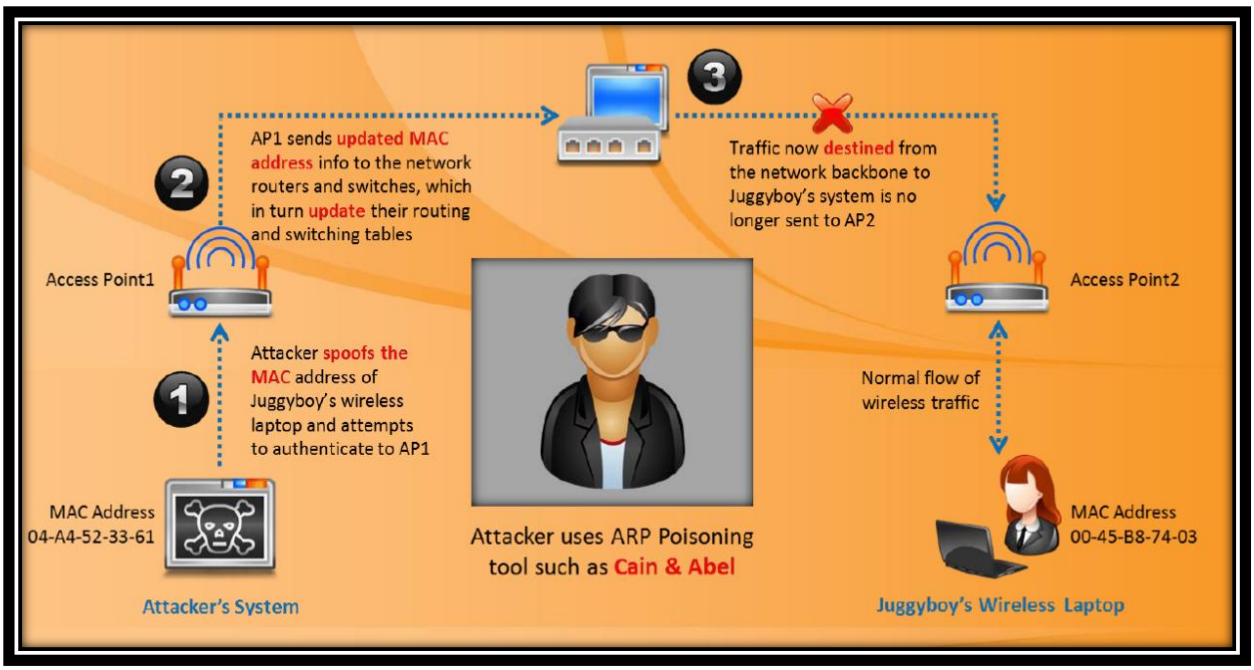


Figure .6 : ARP spoofing [10]

b. DNS Spoofing :

Le DNS spoofing appelé également DNS poisonning est une technique qui consiste à usurper l'identité d'un serveur DNS déjà connu pour rediriger des machines vers un faux site semblable au site authentique contrôlé par le hacker. L'objectif de cette attaque est de fournir de fausses informations et récupérer toutes les données envoyées par la victime au vrai site.

c. Déni de service :

L'attaque Déni de service (en anglais Denial of Service « DoS ») est une attaque qui consiste à envoyer des paquets IP depuis la machine malveillante au système ou au réseau cible, ce qui empêche alors ses utilisateurs de ne plus accéder aux ressources de ce système.

C'est une technique qui est simple à réaliser puisque le hacker n'a généralement pas besoin de mots de passe ou d'autres moyens d'accès. Une telle attaque peut paralyser un service ou un réseau complet.

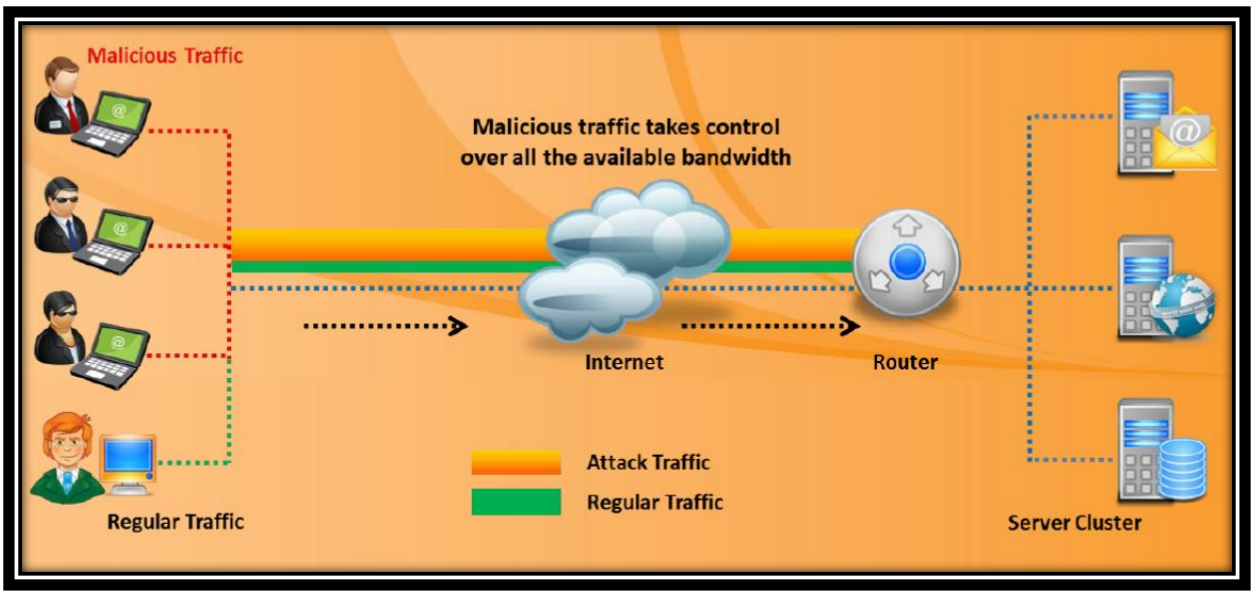


Figure .7 : Attaque DoS [10]

d. Déni de service distribué :

L'attaque déni de service distribué (DDoS) est un type d'attaque DoS où plusieurs machines compromises sont utilisées pour envoyer simultanément une multitude de requêtes à un système cible afin de causer son instabilité ou son indisponibilité. Les attaques DDoS sont souvent effectuées par des machines contrôlées et infectées par des Trojans [2].

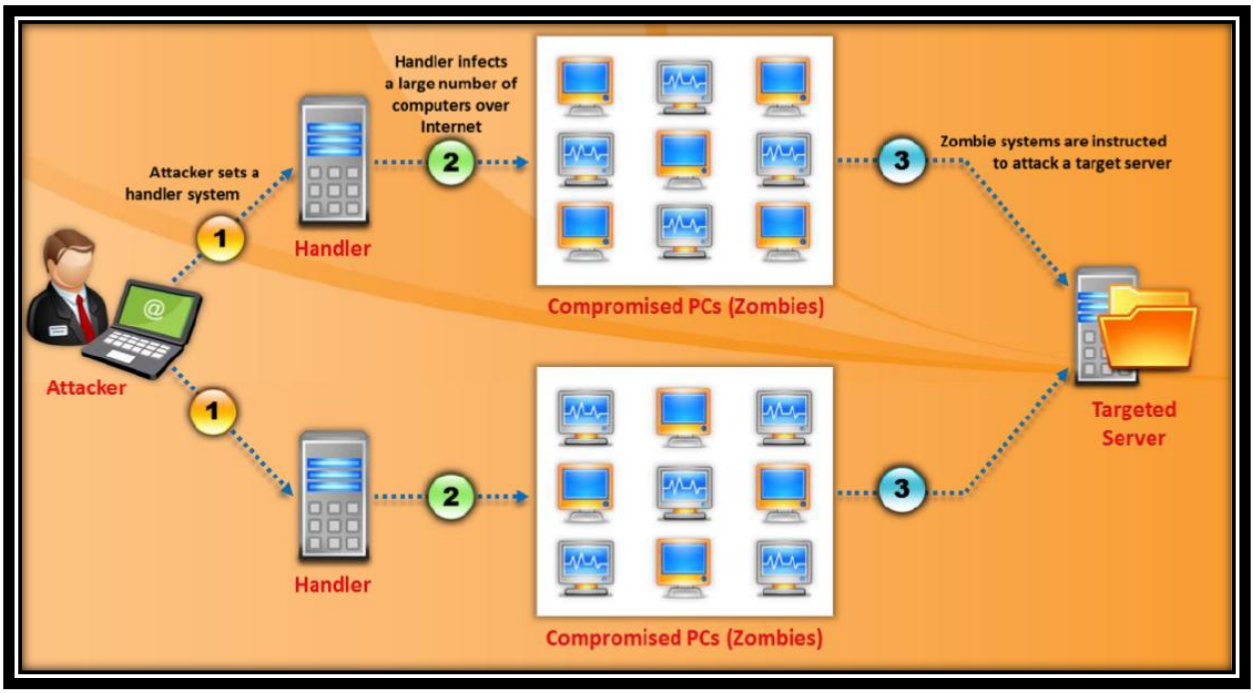


Figure .8 : L'attaque DDos [10]

e. Désauthentification :

La désauthentification est probablement la technique la plus employée et la plus connue des attaques DoS contre les réseaux Wi-Fi [7]. Le hacker envoie, au point d'accès auquel l'utilisateur est connecté, des paquets de demandes de désauthentification pour déconnecter l'utilisateur de ce point d'accès, comme le montre la figure suivante :

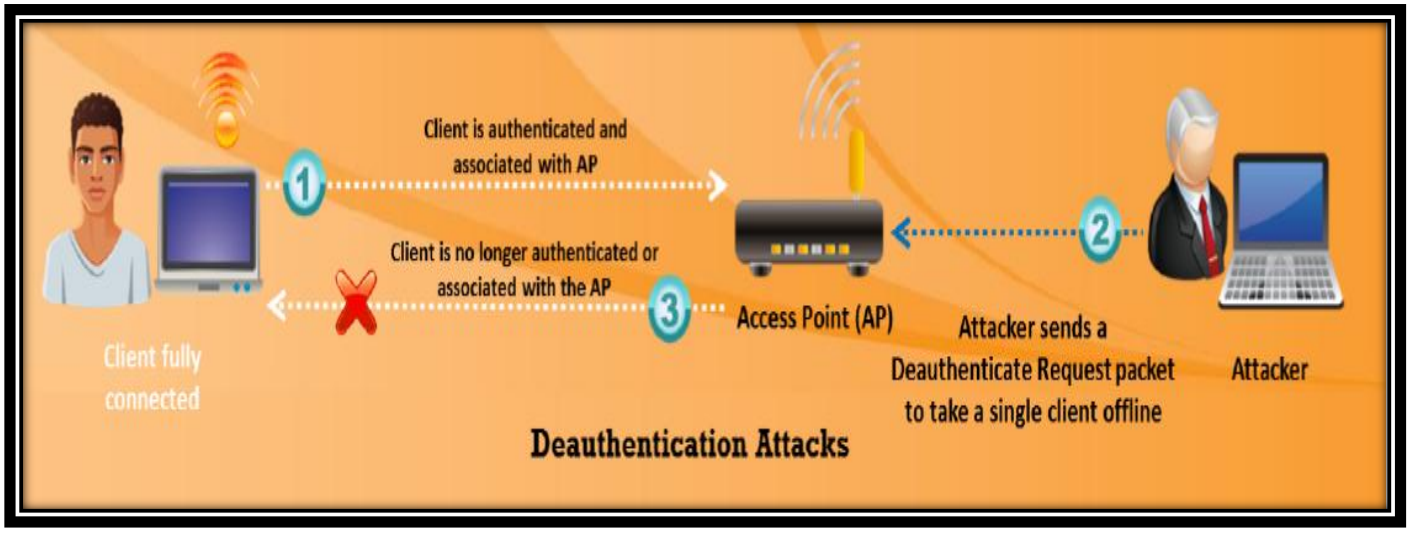


Figure .9 : Attaque de désauthentification [10]

f. Sniffing :

L'attaque sniffing (écoute du réseau) est une technique qui consiste à analyser le trafic réseau, pour récolter illégalement des informations secrètes (ex : mots de passe). Grace à un logiciel appelé « sniffer » (renifler de paquets), le hacker pourra intercepter tout les paquets transitant sur le réseau. Par exemple, lors d'une connexion grâce à telnet, le mot de passe de l'utilisateur va transiter en clair sur le réseau. Il est aussi possible de savoir à tout moment quelles pages web utilisent les personnes connectées au réseau, les mails envoyés ou reçus. Mais cette technique permet aussi de détecter des failles sur un système.

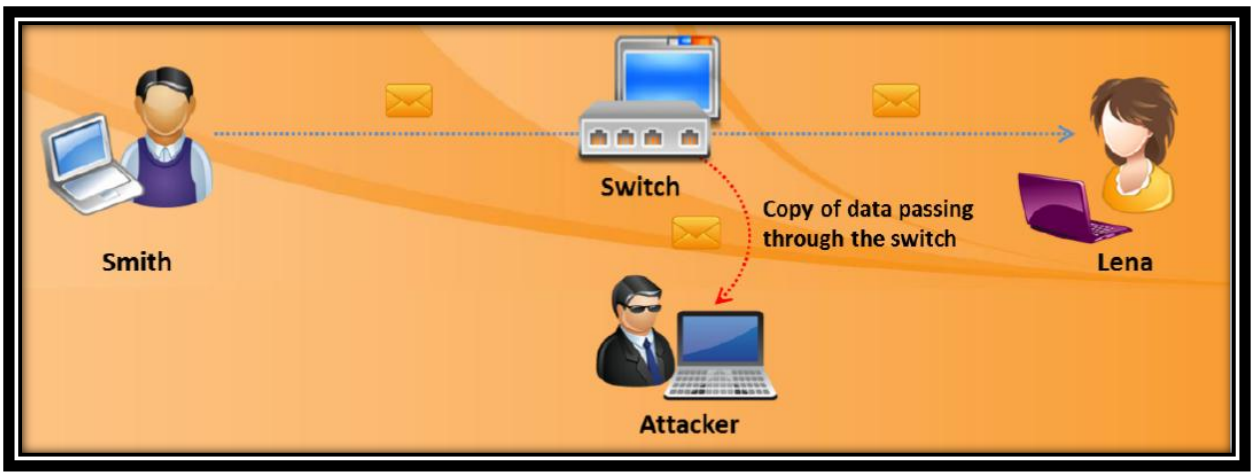


Figure .10 : L'attaque sniffing [10]

g. Evil Twin :

Jumeau maléfique (en français) désigne un faux point d'accès Wi-Fi qui a été mis en place par un hacker, qui porte le même SSID (nom) et qui se trouve au même endroit que le véritable point d'accès pour lequel il s'est fait passer. Ensuite, le hacker redirige les accès sur un serveur web qu'il contrôle pour récupérer les identifiants de connexion, ensuite, il pourra écouter l'ensemble des données qui transitent sur le réseau.

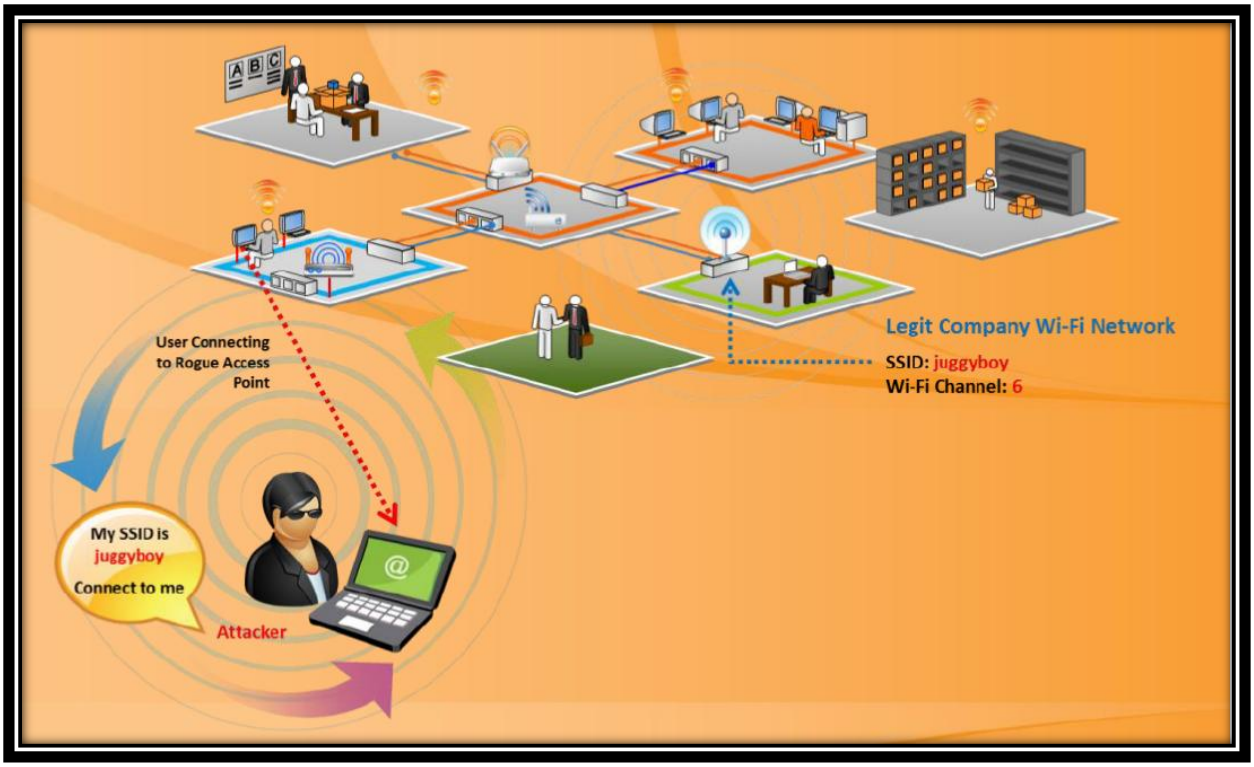


Figure .11 : Evil Twin [10]

h. Man In The Middle

L'attaque Man In The Middle (MITM) ou homme du milieu (en français), est une attaque qui nécessite au moins trois machines dont l'une d'elle est celle du hacker. Le hacker (la machine malveillante) se place alors au milieu d'une communication pour intercepter ou modifier les échanges et se faire passer pour l'une des entités.

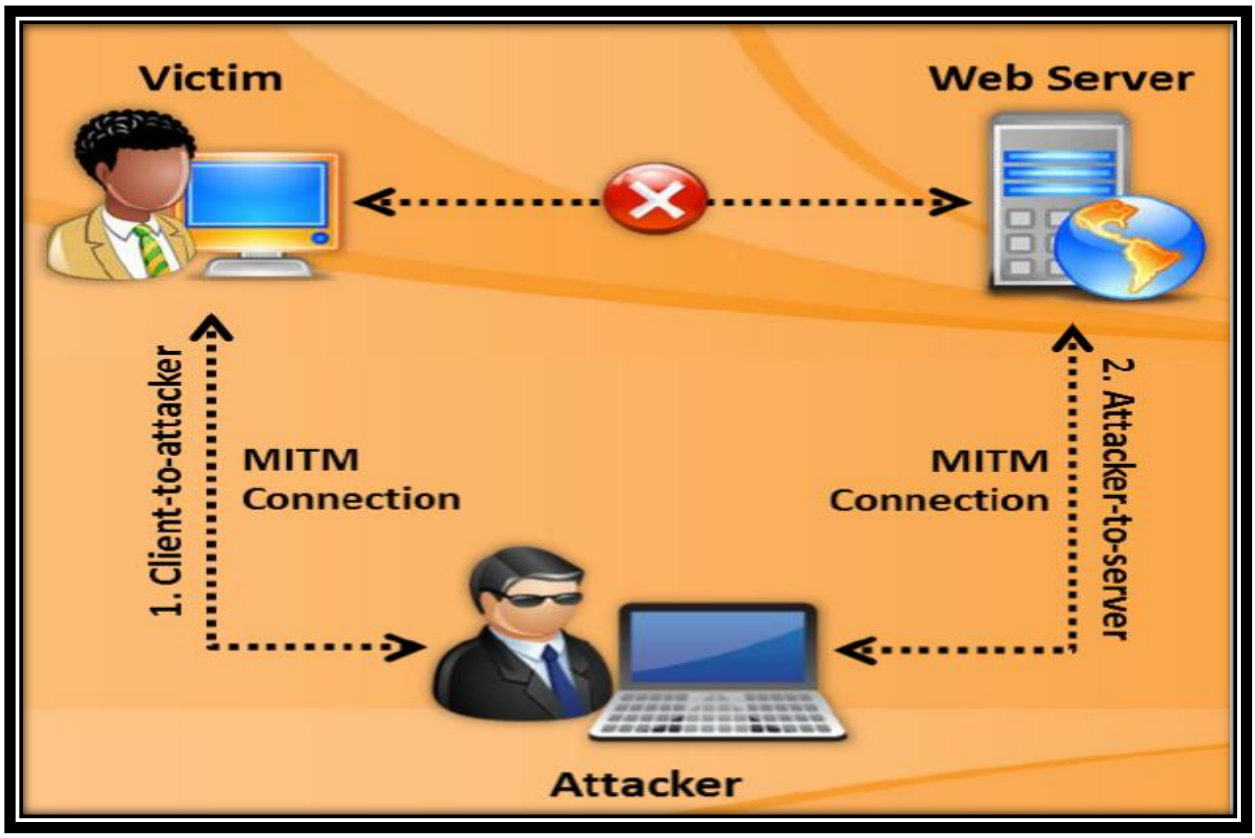


Figure .12: Attaque Man In The Middle [10]

7.2. Les intrusions informatiques :

Une intrusion informatique est une opération qui consiste à accéder, sans autorisation aux données d'un système informatique ou d'un réseau en contournant ou en désamorçant les dispositifs de sécurité mis en place, pour modifier ou voler des informations confidentielles ou détruire les données du système.

7.2.1. Types d'intrusions :

a. Phishing :

Phishing (en français Hameçonnage) est une technique frauduleuse utilisée par les hackers pour obtenir des renseignements personnels dans le but de réaliser une usurpation d'identité. Cette technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte bancaire, date de naissance, etc. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques [7].

b. Trojans Android:

Un trojan ou cheval de Troie est un programme (code) malveillant mais qui a l'apparence d'une application qu'on peut utiliser en toute sécurité.

Les applications qui fonctionnent sur nos Smartphones et tablettes, viennent généralement de sources fiables comme Google Play Store, l'Appstore ou quelques autres magasins virtuels [2]. Les utilisateurs vont juste aller à un magasin d'applications, ils cherchent une application, ils la téléchargent et ils l'installent. Ces magasins permettent généralement toute application à être inclue dans leur catalogue sans faire aucune sorte de validation de ce que le logiciel fait en réalité.

c. Backdoor :

Backdoor ou porte débordée est une fonctionnalité d'un programme permettant d'avoir un accès secret au système. Ce genre de fonctionnalité est souvent ajouté à un logiciel par l'éditeur [7], afin de lui permettre de surveiller l'activité du logiciel, ou de prendre contrôle en cas de sollicitation. Généralement, les hackers, une fois entrés dans le système, créent une porte débordée afin de pouvoir y avoir accès à n'importe quel moment.

d. Ingénierie sociale :

L'ingénierie sociale (en anglais social engineering) est un ensemble de méthodes et de techniques permettant d'obtenir l'accès à un système d'information ou à des informations confidentielles auprès du personnel d'une entreprise en vue d'une intrusion future. L e hacker exploitera les vulnérabilités humaines et sa connaissance de la cible, de ses clients ainsi que de ses fournisseurs en utilisant : la manipulation, la supercherie et l'influence. Pour son exploitation, le hacker pourra utiliser tout média à sa disposition : téléphone, email, messagerie instantanée, réseaux sociaux, etc.

8. Les méthodes de protections contre ses différentes attaques et intrusions :

8.1. La cryptographie :

La cryptographie est l'étude des méthodes permettant de transformer un texte compréhensible en un texte incompréhensible, dans le but de cacher leurs contenus, empêcher leur modification ou leur utilisation illégale. Cette opération permet donc de préserver la confidentialité des données et de garantir leur intégrité et leur authenticité.

Il existe deux types de cryptographie : la cryptographie symétrique et la cryptographie asymétrique.

- **La cryptographie symétrique :**

La cryptographie symétrique ou encore appelée cryptographie à clé privée repose sur l'utilisation d'une même clé pour crypter et décrypter le message. La clé est connue uniquement de l'expéditeur et du destinataire donc cette technique présente un inconvénient majeur lors de la transmission de cette clé d'une entité à une autre puisqu'elle pourrait être interceptée.

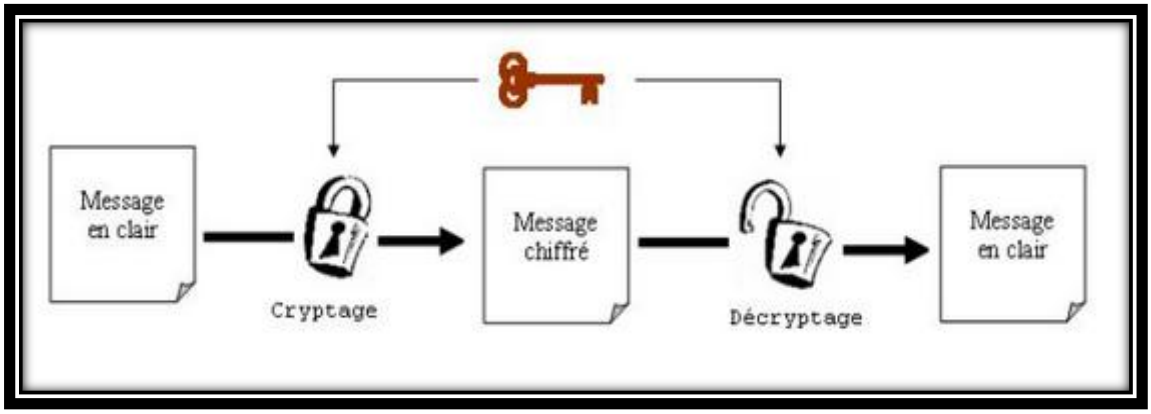


Figure.13 : La cryptographie symétrique

➢ La cryptographie asymétrique :

La cryptographie asymétrique ou encore appelée cryptographie à clé publique repose sur l'utilisation de deux clé différentes. Une clé privée qui n'est connue que de son propriétaire et une autre publique qui est accessible par tout le monde.

Les deux clés privée et publique sont liées par l'algorithme de cryptage utilisé de telle sorte qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. L'avantage de cette technique est de résoudre le problème de l'envoi de clé privée sur le réseau.

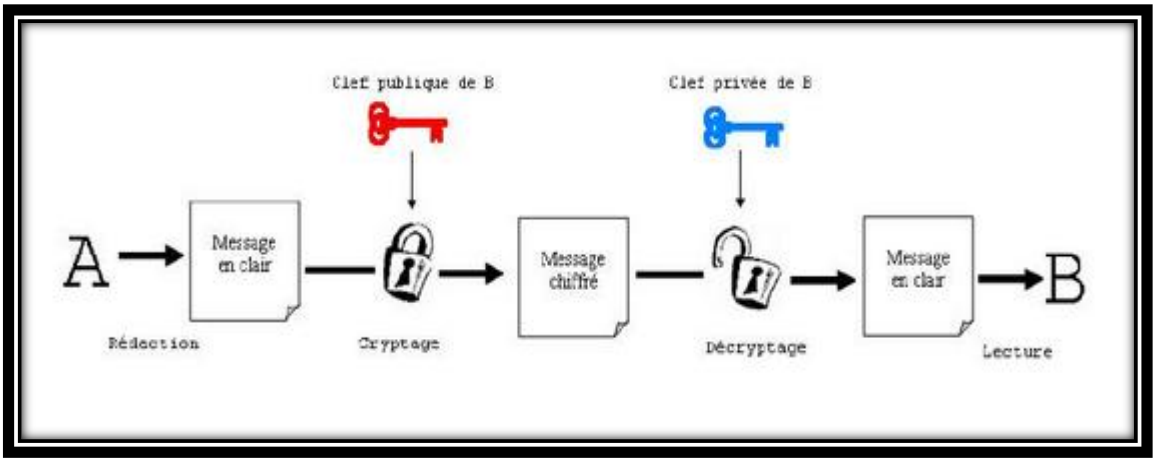


Figure.14 : La cryptographie asymétrique

8.2. Le pare-feu :

Un pare-feu ou Firewall (en anglais) est un composant matériel ou logiciel qui contrôle le trafic entrant ou sortant selon la politique de sécurité mise en œuvre.

Un pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines connectées aux réseaux, il s'agit ainsi d'une passerelle filtrante. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'autres part, d'éviter la fuite non contrôlée d'informations vers l'extérieur. Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau.

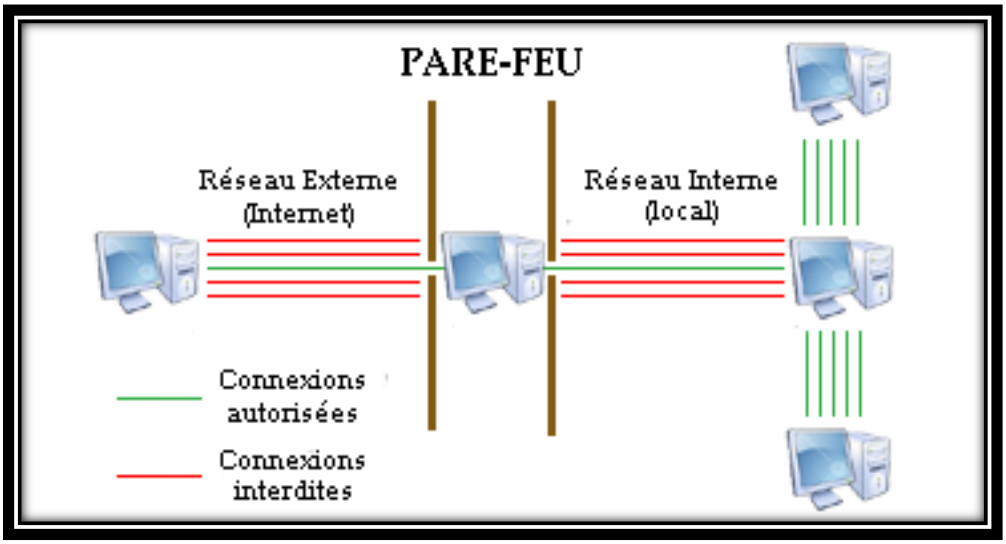


Figure.15 : Le fonctionnement d'un pare-feu

8.3. Le proxy :

Un proxy est un composant logiciel qui joue le rôle d'intermédiaire entre les ordinateurs d'un réseau local et Internet pour faciliter ou surveiller leurs échanges.

Le principe de fonctionnement basique d'un serveur proxy est assez simple [11]. Il s'agit d'un serveur prédestiné par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

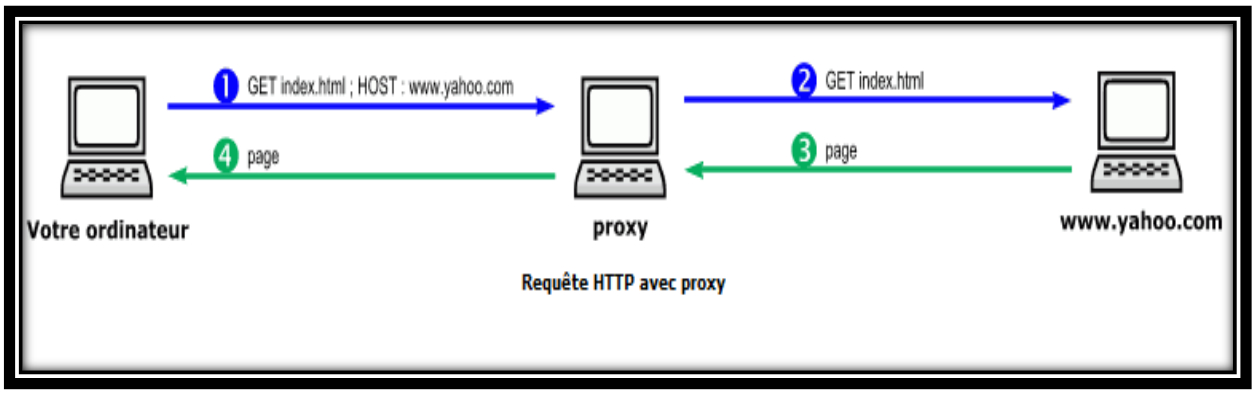


Figure.16 : Le fonctionnement d'un proxy

8.4. Les systèmes de détection d'intrusions IDS :

IDS (Intrusion Detection Système) est un ensemble de composants logiciels et/ ou matériels permettant de repérer des activités anormales ou suspectes d'un réseau ou d'un hôte donné, permettant ainsi d'avoir une action de prévention sur les risques d'intrusion et prendre les mesures de protection qui s'imposent.

8.5. Les systèmes de prévention d'intrusions :

IPS (Intrusion Prevention Système) est un IDS étendu qui agit et qui a pour principale différence d'intercepter les paquets intrus, il est donc un IDS actif [11]. Il est conçu pour identifier les attaques potentielles et exécuter de façon autonome une contre mesure pour les empêcher, sans affecter le système d'exploitation.

8.6. La zone démilitarisée DMZ :

DMZ (De-Militarized Zone) est un segment du réseau local contenant plusieurs machines comprises entre le réseau local et le réseau externe (ex : Internet). La DMZ permet à des machines du réseau interne d'accéder à Internet et/ou de publier des divers services (serveur web, serveur FTP, serveur de messagerie, etc) sur Internet sous le contrôle d'un pare-feu externe. En cas de compromission d'une machine de la DMZ, l'accès au réseau local est encore contrôlé par un pare-feu interne.

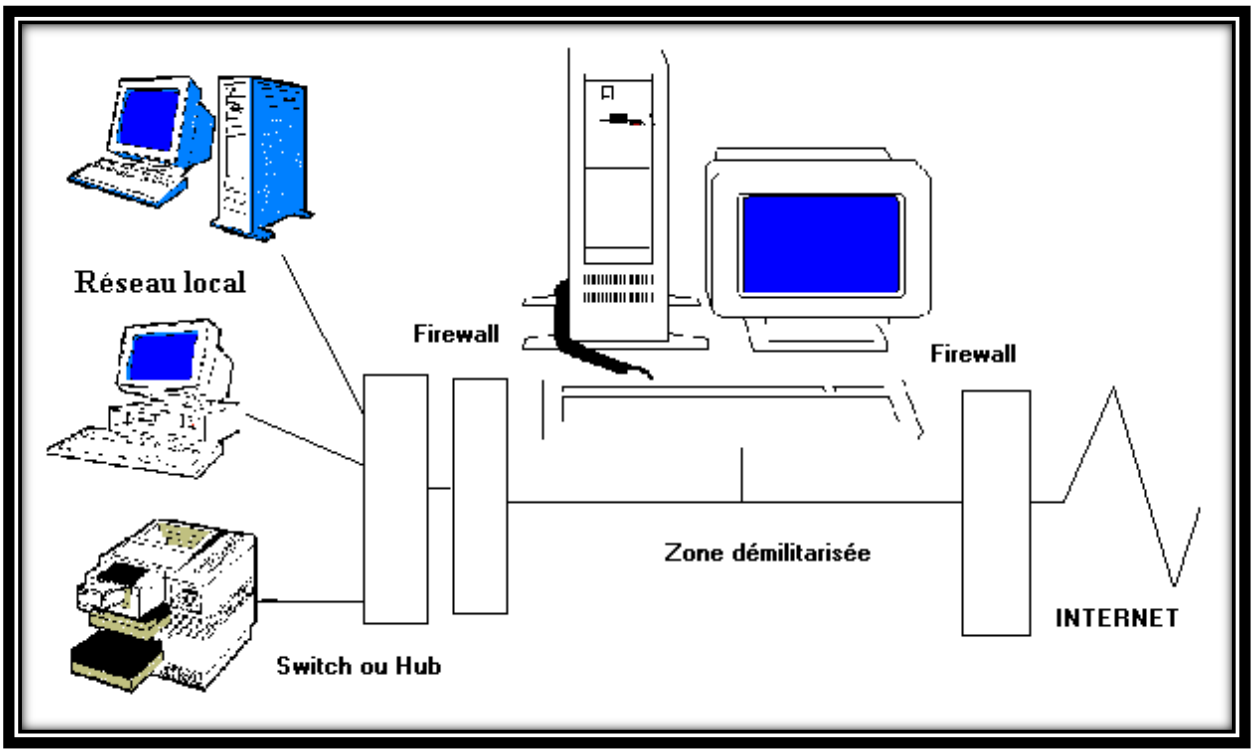


Figure.17 : Architecture DMZ

9. Discussion :

Il nous est paru évident que les attaques réseaux reposent sur un ensemble de faiblesses de sécurité touchant différents domaines, tel que les protocoles réseaux et les systèmes d'exploitations. Par conséquent, de nombreux mécanismes on été conçus pour tester les vulnérabilités des systèmes, détecter, prévenir et réagir contre les attaque informatiques.

Il est donc nécessaire d'effectuer des tests d'intrusion afin de détecter les failles du système et d'établir des mesures de sécurité.

1. Préambule

La sécurisation des différents appareils (Smartphones, tablettes,…etc) utilisant le système d'exploitation Android est aujourd'hui une des préoccupations majeurs des responsables informatiques et des développeurs de logiciels. En effet, un système d'exploitation qui ne peut pas faire face aux différentes attaques sera délaissé par les utilisateurs et par les développeurs d'applications.

Dans le but de sécuriser un appareil sous Android, nous devons au préalable effectuer des tests d'intrusions. Ces tests vont nous permettre de connaitre les failles de sécurité. Ensuite, nous allons utiliser des outils pour détecter une éventuelle intrusion.

Ce chapitre est scindé en deux parties. Dans la première, nous allons présenter les différents tests d'intrusion effectués. Tandis que dans la deuxième, nous allons exposer les outils permettant de détecter une éventuelle intrusion.

2. Partie I : Test d'intrusion

Un test d'intrusion (« penetration test» ou « pentest» en anglais) est une méthode d'évaluation de la sécurité d'un système ou d'un réseau informatique. Cette méthode consiste généralement à simuler une attaque pour trouver des vulnérabilités exploitables en vue de proposer un plan d'actions permettant d'améliorer la sécurité d'un système.

2.1. Objectif du test d'intrusion :

L'objectif d'un test d'intrusion est alors multiple et peu varier selon les contextes :

- Lister un ensemble d'informations, trouvées d'une manière ou d'une autre, et qui peuvent être sensibles ou critiques.
- Dresser une liste des vulnérabilités ou faiblesses du système de sécurité pouvant être exploitées.
- Tester l'efficacité des systèmes de détection d'intrusion et la réactivité de l'équipe de sécurité, et parfois des utilisateurs (social engineering)
- Effectuer un rapport et une présentation finale de son avancement et de ses découvertes au client
- Donner des pistes et conseiller sur les méthodes de résolution et de correction des vulnérabilités découvertes.

2.2. Application :

La phase application vient nous éclaircir les notions théoriques acquises dans le chapitre précédent sur les différentes intrusions informatiques qui peuvent avoir lieu et nous permettre d'aboutir à la finalité de notre projet.

2.2.1. Présentation du projet :

Ce projet est consacré à la réalisation et à la mise en œuvre de notre application sur les tests d'intrusions. Dans cette partie, on va commencer d'abord par expliquer le principe de notre projet et l'objectif de l'intrusion, puis on va citer les outils de développement et la technologie utilisée pour l'intrusion.

Enfin, nous passerons à la réalisation des tests d'intrusion par l'élaboration des captures d'écrans pour les résultats.

2.2.2. Principe du projet :

Le principe de notre projet est de parvenir à nous introduire dans un Smartphone sous Android que nous contrôlerons avec la suite d'outils de kali linux.

2.2.3. Objectif de l'intrusion :

L'objectif de cette intrusion est de réussir à convaincre une victime d'installer sur son Smartphone ou sa tablette une fausse application de Djaweb (Idoomobile) sans se rendre compte qu'il s'agit réellement d'un Trojan Android. Ce Trojan nous permettra d'ouvrir un backdoor dans le Smartphone victime afin de s'introduire et de nous assurer un accès direct et un contrôle total de la victime.

Pour que la victime installe l'application, nous allons créer un faux point d'accès et nous allons déconnecter ou désauthentifier la victime du point d'accès réel.

Ensuite, une fois la victime connectée au faux point d'accès, elle sera redirigée vers la fausse page (page Phishing) de l'application et il ne reste plus qu'à cliquer sur soumettre pour installer cette application.

2.2.4. Outils de développement :

➢ Metasploit Framework (msf) :

Ensemble d'outils et de composants logiciels conçus pour faciliter la réalisation des tests d'intrusion. Parmi ces outils :

- **Msfconsole :** Interface qui permet un accès efficace à la quasi-totalité des options disponibles sur Metasploit Framework. Cet outil peut réaliser plusieurs fonctions en même temps, tel que : lancer des attaques, scanner en masse un ensemble du réseau, etc.
- **Meterpreter :** Extension de Metasploit Framework qui nous permet de compromettre d'avantage une cible.
- **Msfvenom :** Générateur standard des payloads de metasploit.

➢ Aircrack-ng :

Aircrack-ng est un outil de sécurité Wi-Fi. Il permet de casser les clés WEP et WPA-PSK à partir de paquets capturés sur le réseau. Il regroupe plusieurs formes d'attaques connues pour l'intrusion sur un réseau. C'est en fait une boîte à outils pour l'audit de réseaux sans fil. Parmi ces outils :

- **Airmon-ng :** C'est un script qui permet d'activer/désactiver le mode moniteur d'une carte Wi-Fi. Dans ce mode, la carte Wi-Fi se place en « observateur » du réseau.
- **Airbase-ng :** C'est un script qui permet de créer des points d'accès Wi-Fi.

➢ Mdk3 :

Mdk3 est un programme indispensable pour l'analyse des réseaux Wi-Fi. Il a de nombreuses fonctionnalités dont la plupart sont agressives vis-à-vis du réseau cible, parmi lesquelles on peut citer la désauthatification, trouver un SSID caché, trouver une adresse MAC, faire croire à la cible que le WPA est buggé et le forcer à repasser en WEP, etc. Son but est purement intrusif.

2.2.5. Technologie utilisée :

Dans ce projet nous avons utilisé la technologie de virtualisation constituant à faire fonctionner plusieurs systèmes sur une même machine physique.

Cette technologie présente plusieurs intérêts :

- Economie d'électricité, de temps et d'argent.
- Installation, tests, développements et possibilité de recommencer sans endommager le système d'exploitation hôte.
- Possibilité d'installer plusieurs systèmes d'exploitation (Windows, Linux) sur une même machine physique.

Dans le cas de notre application, nous avons utilisé :

- Un ordinateur portable avec le système d'exploitation Windows 7, d'une fréquence d'horloge de 2,3 GHz et de 4Go de RAM. Sur lequel nous avons installé une machine virtuelle nommée Debian 7 avec le système d'exploitation Kali Linux, de 1GB de mémoire et d'un disque dur d'une capacité de 20GB.

- Un Smartphone sous Android.

2.2.6. Réalisation du test d'intrusion :

Maintenant, nous allons entamer la partie réalisation, dans laquelle nous allons arborer les différentes procédures à suivre pour effectuer notre test d'intrusion et quelques captures d'écrans des résultats.

a. Création du payload (Trojan Android) :

Nous allons créer un payload (Trojan Android) avec la commande à l'aide des outils suivants, qu'on va nommer « Android ».

- **Msfconsole :** Interface qui permet un accès efficace à la quasi-totalité des options disponibles sur Metasploit Framework. Cet outil peut réaliser plusieurs fonctions en même temps, tel que : lancer des attaques, scanner en masse un ensemble du réseau, etc.
- **Meterpreter :** Extension de Metasploit Framework qui nous permet de compromettre d'avantage une cible.
- **Msfvenom :** Générateur standard des payloads de metasploit.

La figure ci dessous confirme la création du Trojan sur le bureau.

Figure .18 : Icone du Trojan sur le bureau

Après avoir ouvert msfconsole, on ouvre le port 4444 par exemple, afin de réceptionner les connexions inverses.

Figure .19 : Ouverture d'un port sur msfconsole

b. Création du faux point d'accès :

Evil Twin :

Un hacker utilise le scénario « Evil Twin », cette technique consiste à crée d'abord un faux point d'accès sans fil et se faire passer pour un point d'accès légitime, qui déclenche ensuite une attaque par déni de service contre ce point d'accès légitime, ou crée des interférences autour de ce dernier, ce qui déconnecte alors les utilisateurs légitimes. Ces derniers sont ensuite invités à inspecter les réseaux disponibles.

Une fois déconnecté du point d'accès légitime, les ordinateurs et périphériques hors ligne se reconnectent automatiquement au jumeau maléfique, permettant au hacker d'intercepter tout le trafic via ce dispositif.

Pour créer ce point d'accès, on suit les étapes suivantes :

1) Nous commençons par l'installation du serveur DHCP avec la commande suivante : **apt-get install isc-dhcp-server**
2) On copie le fichier **dhcp.conf** dans le répertoire **/etc/dhcp/dhcp.conf**
3) Juste après la configuration du serveur DHCP, nous allons utiliser **/var/www/html** comme un répertoire dans lequel nous allons stocker les fichiers web.
   Par la suite, nous utilisons la commande **rm *** pour supprimer les fichiers existant, une fois ces fichiers supprimés, nous allons copier les fichiers de la page web phishing vers ce dossier.

4) Nous utilisons la commande **/etc/init.d/apache2** pour activer le service web (apache2).

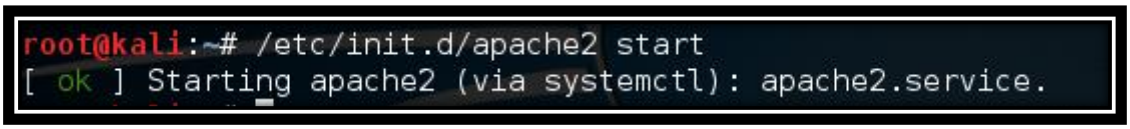


Figure .20 : Activation du service web

5) Nous ouvrons une nouvelle console puis on tape la commande **airmon-ng** pour détecter notre interface Wi-Fi.

6) Une fois que notre interface est détectée, nous allons utiliser cette dernière pour activer notre mode moniteur.

7) Dans cette étape, nous allons utiliser la commande **airbase-ng** pour créer un point d'accès qui porte l'identifiant « 2intpartners ».

Figure .21 : Création du point d'accès « 2intpartners »

8) Avant de démarrer le serveur, nous devons configurer l'interface at0 :

Figure .22 : Configuration de l'interface at0

9) Maintenant, il faut configurer le pare-feu iptables pour autoriser le transfert d'une interface à l'autre.

c. La désauthentification :

10) Après avoir crée le faux point d'accès, nous allons désauthentifier l'utilisateur du véritable point d'accès en utilisant **mdk3**

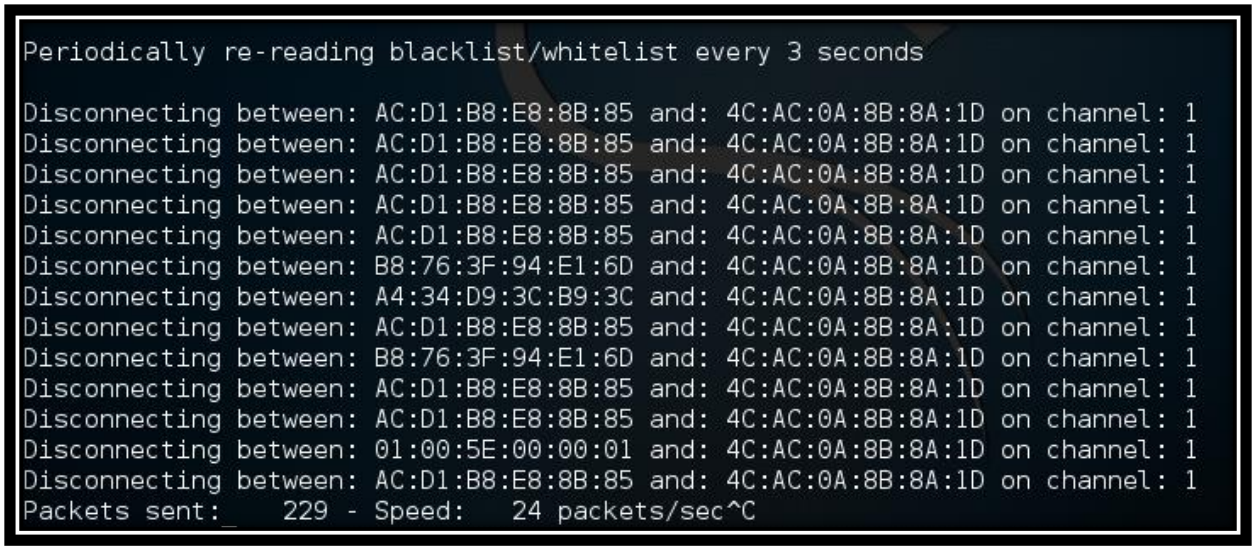


Figure .23: Déconnection des utilisateurs du point d'accès légitime

11) Une fois que l'utilisateur est déconnecté du point d'accès, il va se connecté au faut point d'accès créé et il sera redirigé vers la page phishing qui permet à l'utilisateur de télécharger l'application (le Trojan) en cliquant sur soumettre.

Figure .24: La page phishing de l'application à télécharger

12) Après que l'utilisateur a installé et ouvert l'application, nous reçevront une connexion inverse qui nous permet de nous introduire dans son Smartphone.

Figure .25 : Console Meterpreter sur Metasploit

3. Partie II

3.1. Les mesures de sécurité :

3.1.1. L'Antivirus :

Les Antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants dont les virus informatiques. Ces logiciels surveillent la présence de virus et éventuellement de nettoyer, supprimer ou mettre en quarantaine les fichiers infectés.

a. Principe de fonctionnement :

La détection des virus se fait selon deux principes, une détection par signature et une détection comportementale.

- **Détection par signature :**

L'Antivirus scanne la machine à la recherche de caractéristiques ou de signatures de programmes malveillants connus. Il le fait en se référant à un dictionnaire de logiciels malveillants connus, si quelque chose sur la machine correspond à un modèle dans le dictionnaire, le programme tente de le neutraliser. L'approche dictionnaire nécessite des mises à jour, pour se protéger contre de nouveaux logiciels malveillants. L'Antivirus peut seulement protéger contre ce qu'il reconnait comme dangereux.

- **Détection comportementale :**

L'Antivirus ne cherche pas à identifier les programmes malveillants connus, mais surveille le comportement des logiciels installés sur l'ordinateur. Quand un programme agit étrangement, comme par exemple en tentant d'accéder à un fichier protégé ou à modifier un autre programme, un logiciel Antivirus basé sur la détection comportementale repère l'activité suspecte et nous avertit. Cette approche offre une protection contre des types de logiciels malveillants qui n'existent pas encore dans aucun dictionnaire.

3.1.2. Reverse engineering :

En général, on définit le reverse engineering (rétro-ingénierie ou ingénierie inverse en français) par le fait de décompiler un programme, c'est à dire que l'on traduit Un langage compréhensible par une machine en un langage lisible et compréhensible par un être humain en utilisant des outils de décompilation.

Dans la pratique, le reverse engineering représente l'étude et l'analyse d'un système pour en déduire son fonctionnement interne, en examinant pas à pas les résultats de son exécution.

3.2. Application :

Pour arriver à la finalité de notre projet, nous allons nous intéresser à la sécurité du Smartphone victime par la mise en œuvre d'une solution de sécurité contre l'intrusion réalisée dans la première partie.

3.3. Outils utilisés :

Dans cette partie, nous allons utiliser les outils suivants :

- Kaspersky
- APK-Multi-Tool
- Dex2jar-2.0
- Java decompiler

3.4. Réalisation :

Le but du test d'intrusion réalisé dans la première partie était de télécharger une application qui est réellement un Trojan. Pour faire face à ce genre d'intrusion, on va procéder à l'installation d'un antivirus qui va nous permettre de détecter les virus dans le Smartphone puis, on va utiliser l'ingénierie inverse pour décompiler le fichier (.apk) ou l'application pour extraire l'adresse IP du hacker

3.4.1. L'antivirus Kaspersky :

1) Nous commençons par télécharger l'antivirus Kaspersky sur le site officiel qui permet de détecter et de supprimer des virus existant :

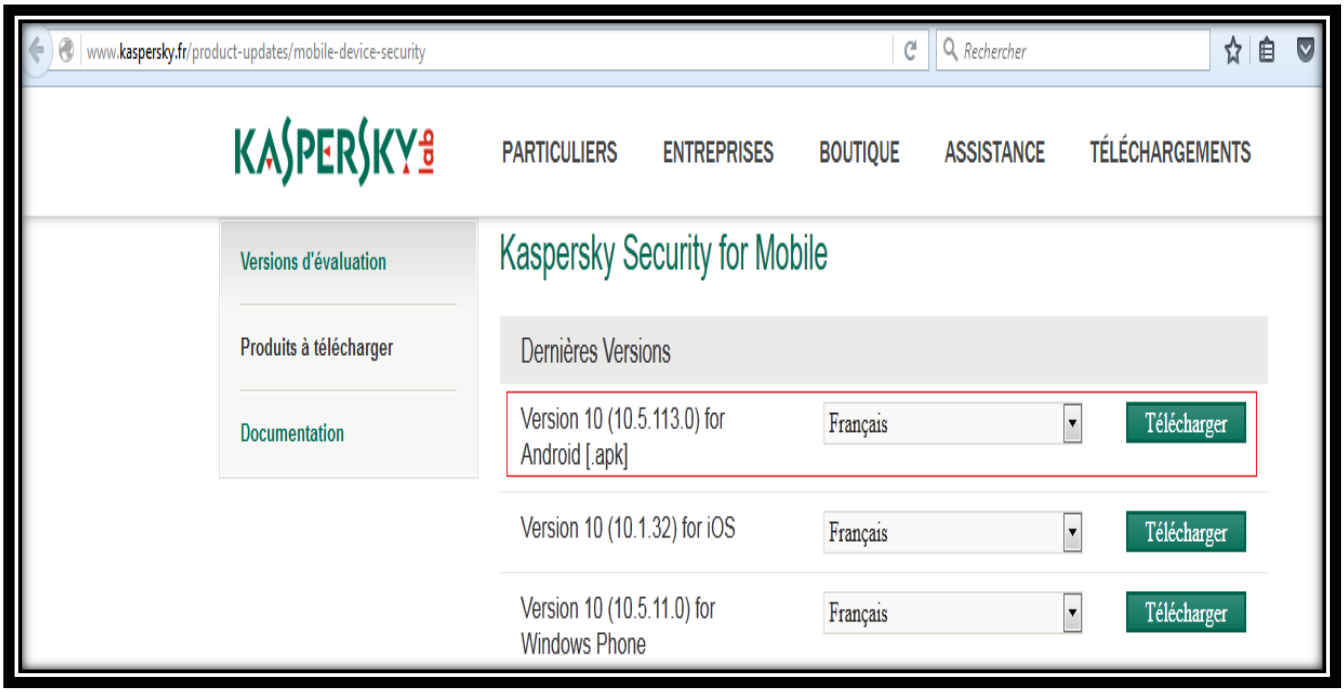


Figure .26 : Téléchargement de Kaspersky pour Android

2) Puis nous cliquons sur activer :

Figure .27 : Activation d'un administrateur de l'appareil

3) Kaspersky détecte les virus existant dans le Smartphone :

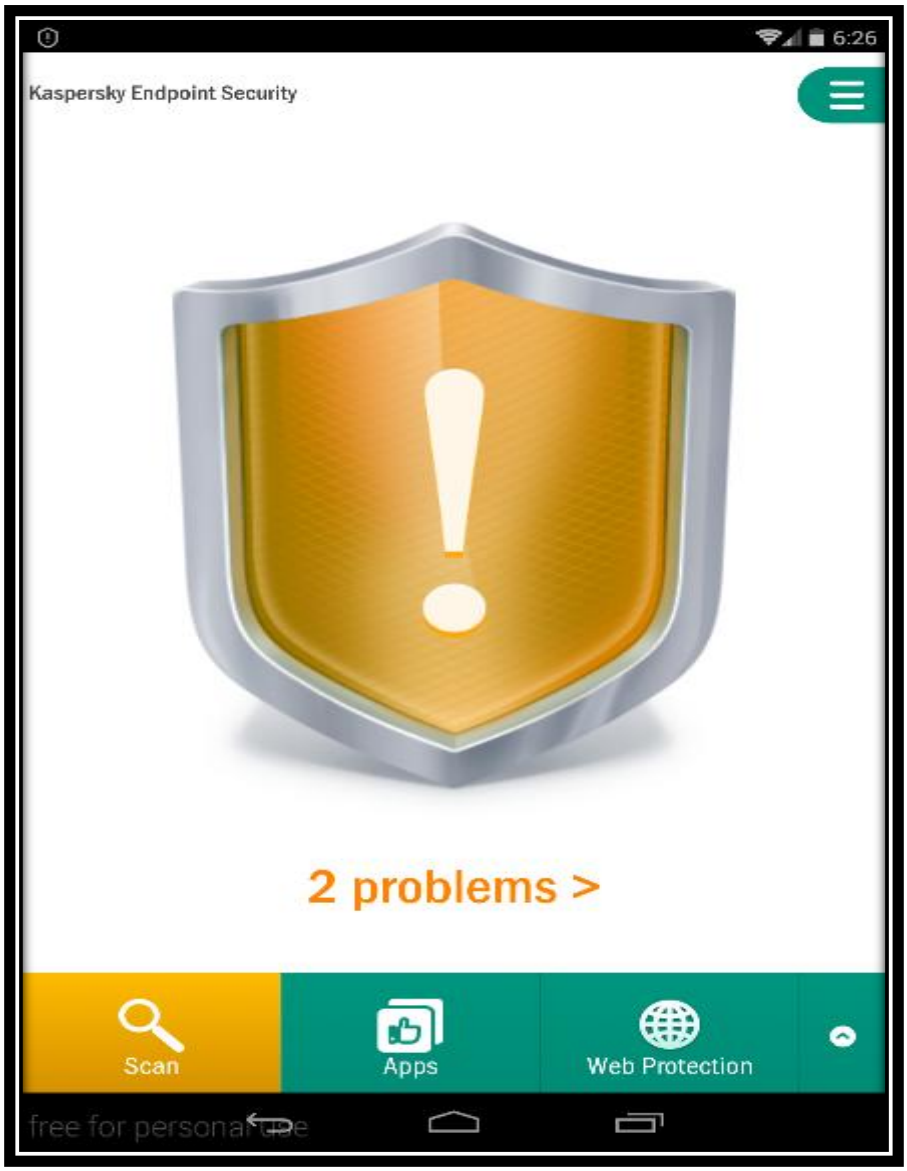


Figure .28 : Détection des virus

4) Fin et résultats du scan :

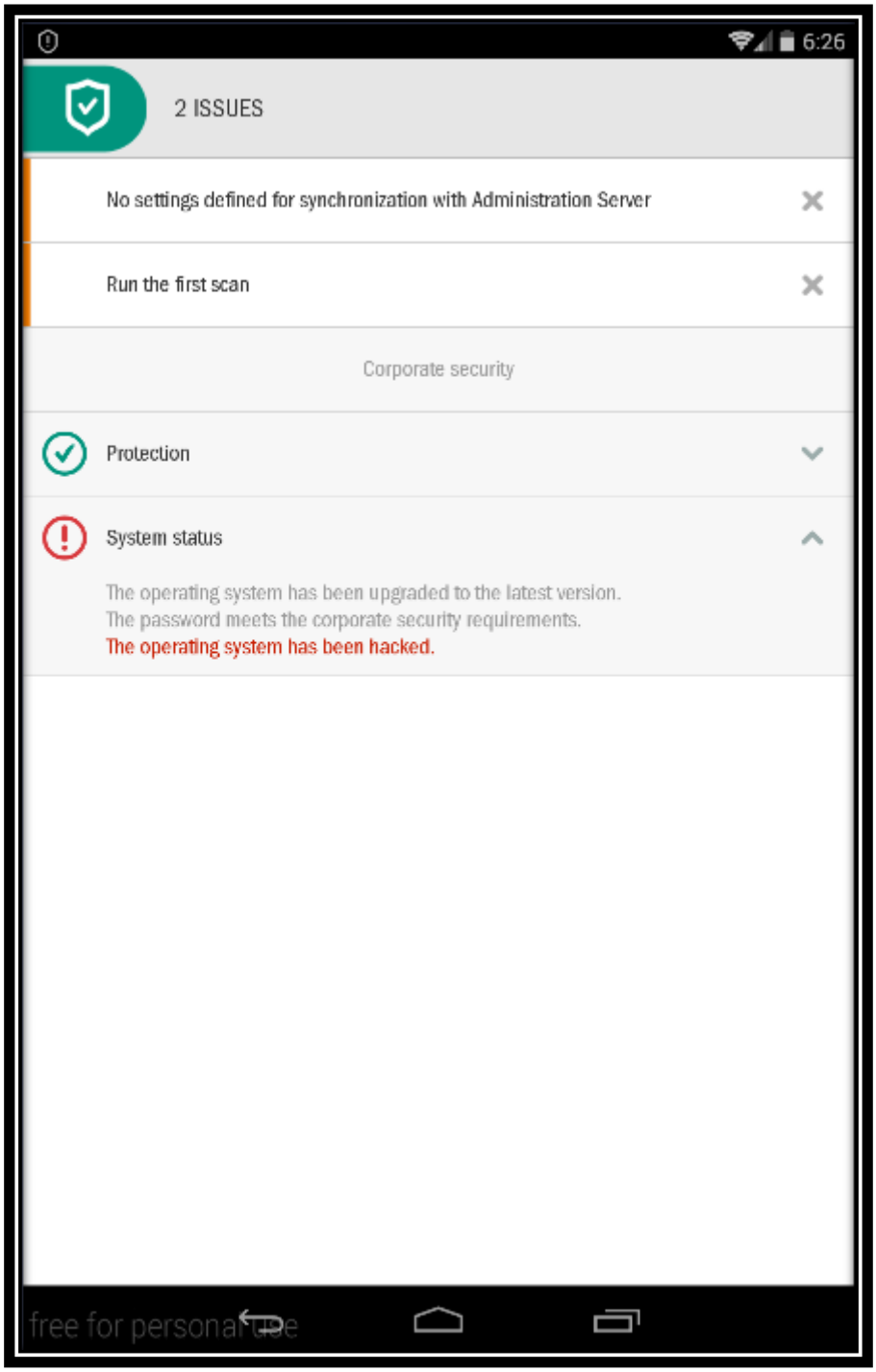


Figure .29 : Résultats du scan Kaspersky

5) Maintenant, nous cliquons sur supprimer, pour désinstaller l'application :

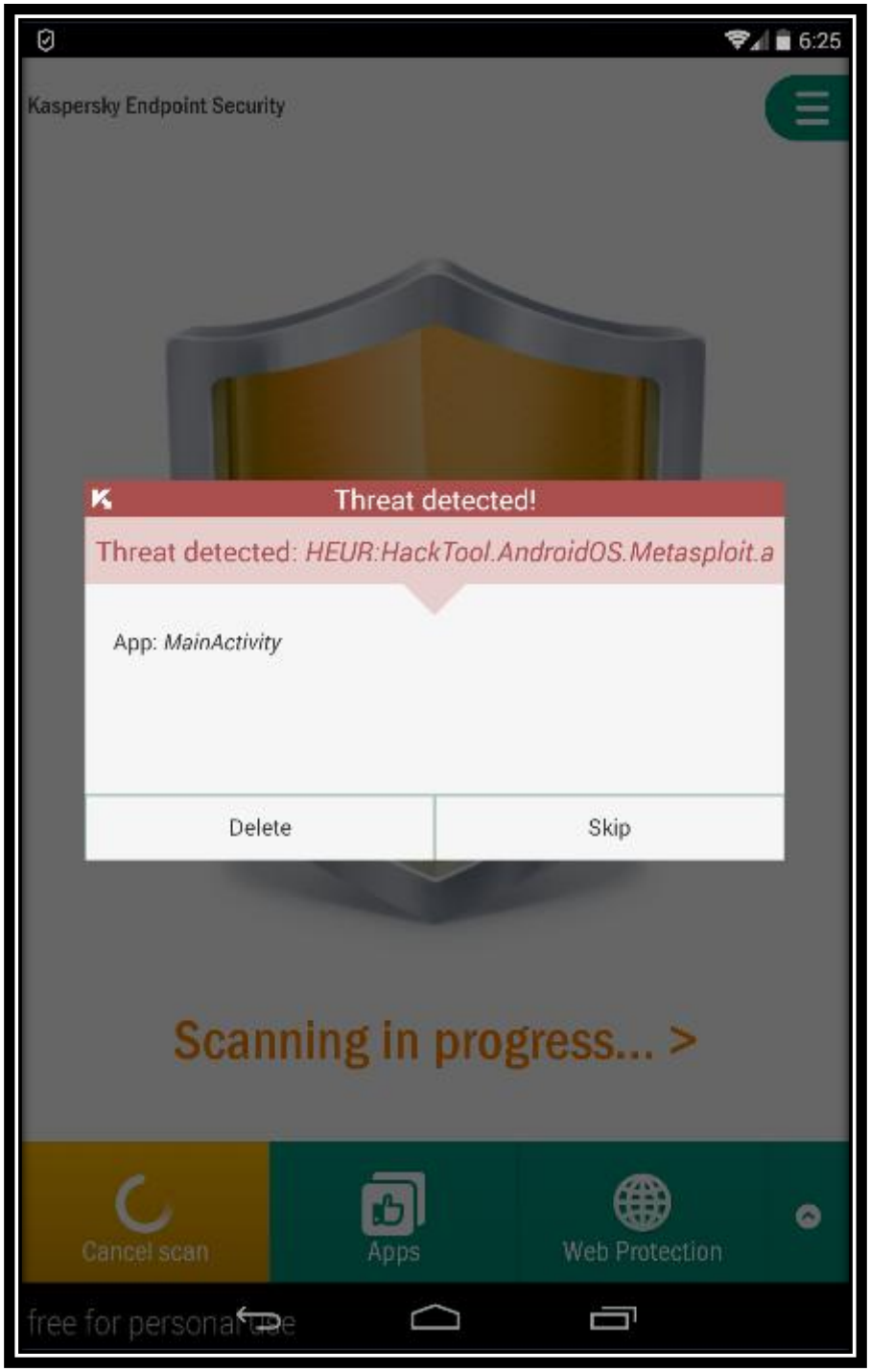


Figure .30 : Détection afin de désinstaller le virus

6) Nous cliquons sur ok pour désinstaller l'application :

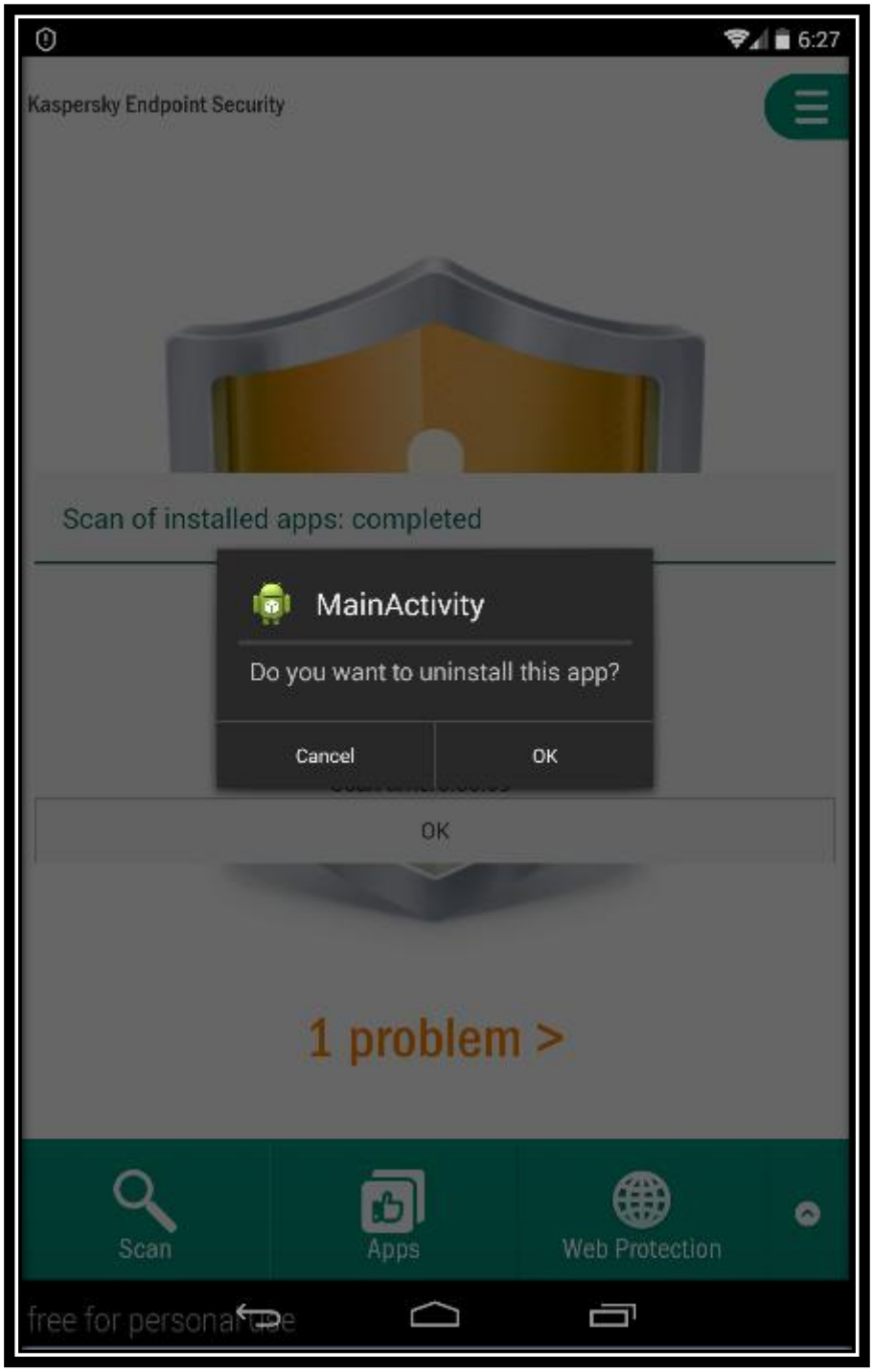


Figure .31 : Désinstallation de l'application

7) Le smartphone est maintenant protégé :

Figure .32 : Smartphone protégé

3.4.2. Reverse engineering :

1) Nous allons commencer par télécharger l'outil dex2jar qui permet de convertir les formats Android qui ont l'extension .dex en format Java. class :

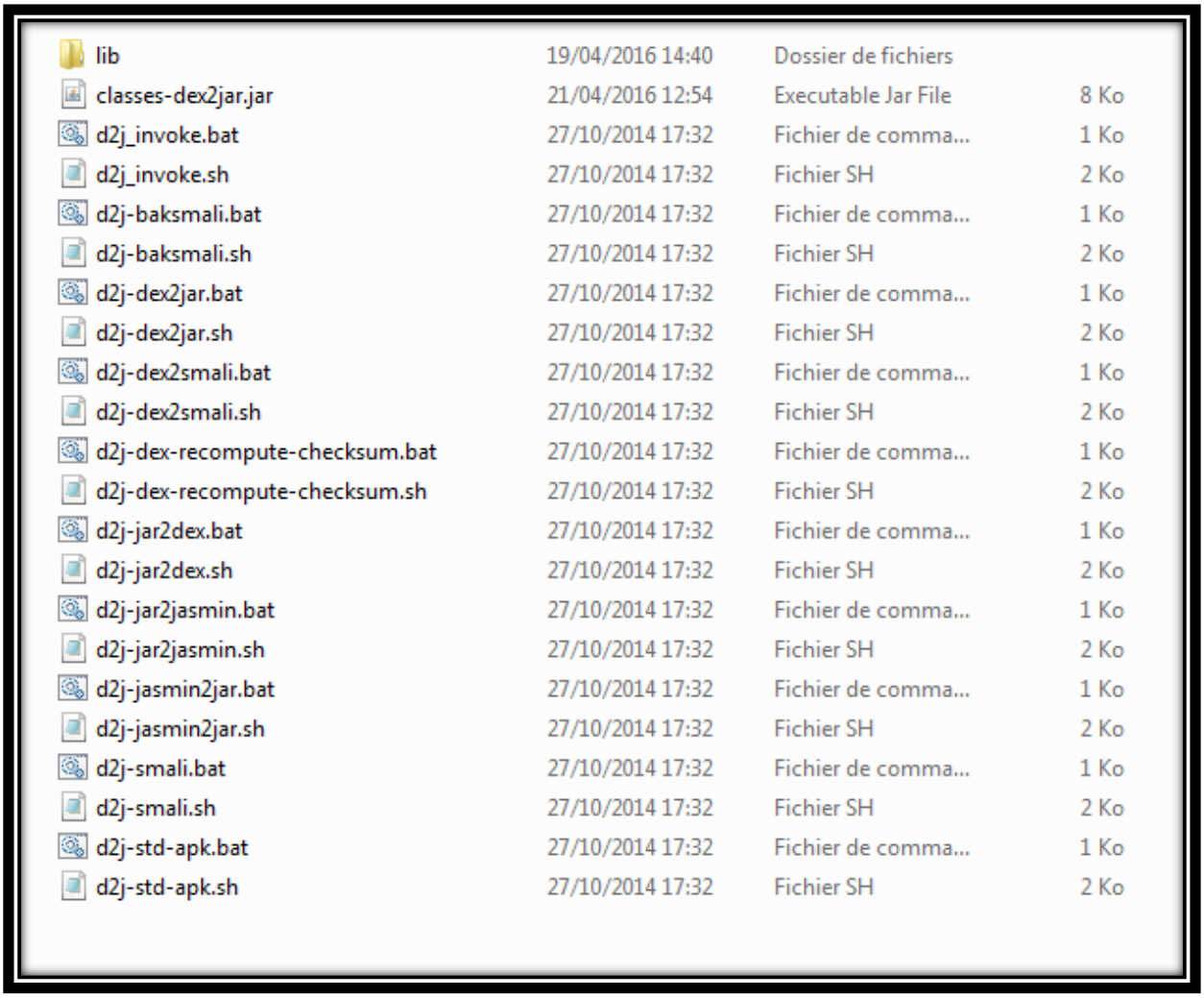


Figure .33 : Télécharger l'outil dex2jar

2) Nous copions le Trojan dans un fichier, puis nous modifions l'extension qui était .**apk** en **.zip**, car l'extension apk n'est pas prise en charge par aucun outil de décompilation :

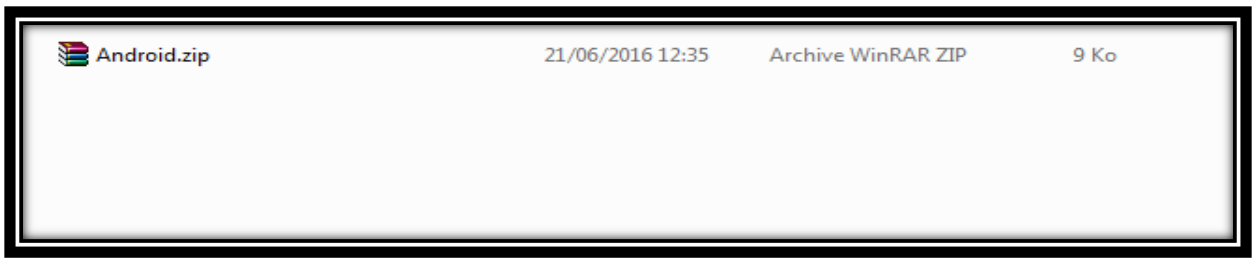
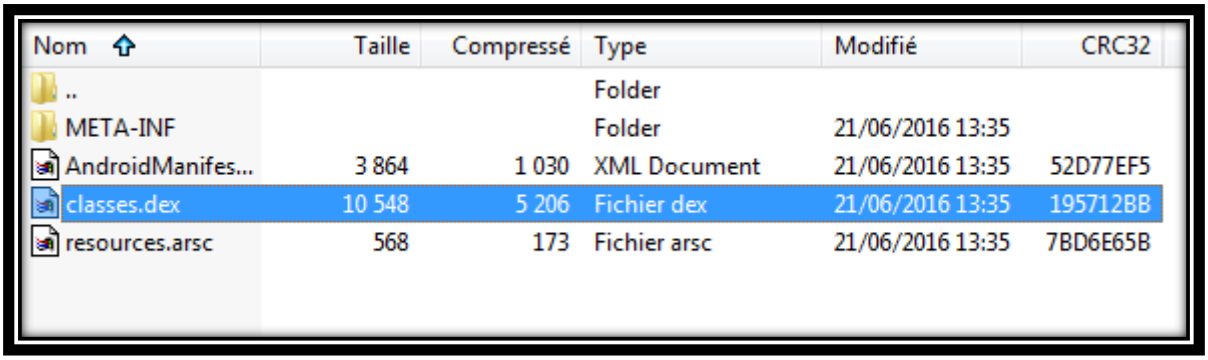


Figure .34 : Modification de l'extension en .zip

3) Nous double cliquons sur le fichier **.zip** et nous allons extraire le fichier **classes.dex** qui est essentiellement la totalité de la logique d'application. C'est le code d'une application donnée écrit en Java, puis compilée à des fichiers de classe **:**



Nom	Taille	Compressé	Type	Modifié	CRC32
..			Folder		
META-INF			Folder	21/06/2016 13:35	
AndroidManifes...	3 864	1 030	XML Document	21/06/2016 13:35	52D77EF5
classes.dex	10 548	5 206	Fichier dex	21/06/2016 13:35	195712BB
resources.arsc	568	173	Fichier arsc	21/06/2016 13:35	7BD6E65B

Figure .35 : Extraction du fichier classes.dex

4) Nous exécutons la commande dex2jar pour voir les différentes options :

```
C:\Users\cbs_computer\Desktop\Tools\dex2jar-2.0>d2j-dex2jar.bat
d2j-dex2jar -- convert dex to jar
usage: d2j-dex2jar [options] <file0> [file1 ... fileN]
options:
 -d,--debug-info                translate debug info
 -e,--exception-file <file>     detail exception file, default is $current_dir/[fi
                                le-name]-error.zip
 -f,--force                     force overwrite
 -h,--help                      Print this help message
 -n,--not-handle-exception      not handle any exception throwed by dex2jar
 -nc,--no-code
 -o,--output <out-jar-file>     output .jar file, default is $current_dir/[file-na
                                me]-dex2jar.jar
 -os,--optmize-synchronized     optmize-synchronized
 -p,--print-ir                  print ir to Syste.out
 -r,--reuse-reg                 reuse regiter while generate java .class file
 -s                             same with --topological-sort/-ts
 -ts,--topological-sort         sort block by topological, that will generate more
                                 readable code, default enabled
version: reader-2.0, translator-2.0, ir-2.0
```

Figure .36 : Les différents choix disponibles

5) Nous exécutons la commande qui nous permet de convertir le fichier **.dex** en fichier **.jar**, puis nous cliquons sur entrer :

Figure .37 : Conversion du fichier « .dex » en «. Jar »

6) Puis nous aurons le résultat suivant :

Figure .38 : Résultat de la commande de conversion

7) Maintenant, nous allons executer APK-Multi-Tool qui est un outil de décompilation, et nous allons décompiler le fichier **.apk** en choisissant l'option 17 « Batch Decompile apk Files » **:**

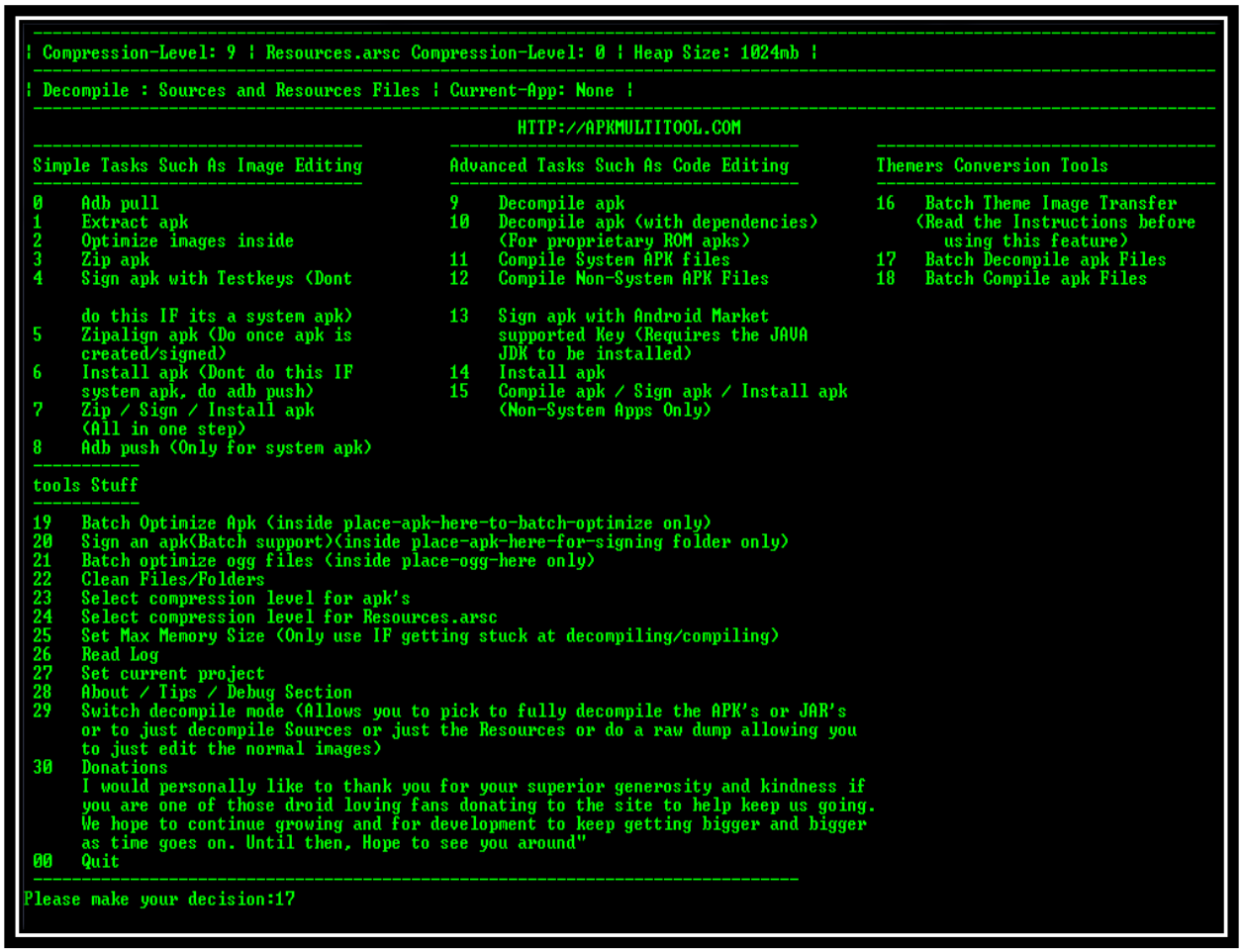


Figure .39 : Menu principale de l'application APK-Multi-Tool

8) Nous aurons le résultat suivant qui est le processus de décompilation d'un fichier (application) .APK :

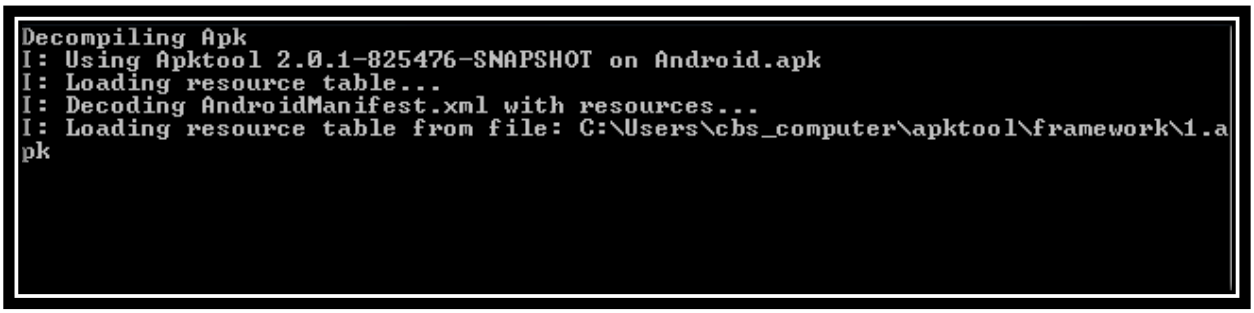


Figure .40 : Décompression et décompilation du fichier .APK

9) A présent nous allons nous rendre dans le chemin «..\APK-Multi-Tool\projects\Android.apk » où nous pouvons trouver les fichiers (applications) APK décompilés par l'application APK Multi Tool sous forme de dossier portant le nom du fichier (application) décompilé.

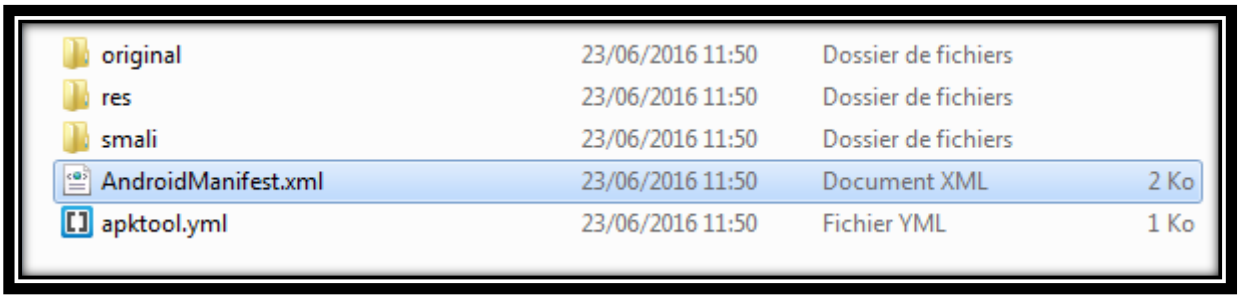


Figure .41 : Contenu du dossier Android.APK par APK-Multi-Tool

10) Nous ouvrons le fichier AndroidManifest.xml, qui est un fichier qui contient des informations sur le package, le nom de l'application, etc :

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.metasploit.stage"
platformBuildVersionCode="10" platformBuildVersionName="2.3.3">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COURSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <application android:label="@string/app_name">
        <activity android:label="@string/app_name" android:name=".MainActivity"
android:theme="@android:style/Theme.NoDisplay">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Figure .42 : Contenu du fichier AndroidManifest.xml

11) Nous ouvrons Java Decompiler, qui permet de décompiler et d'analyser le code Java :

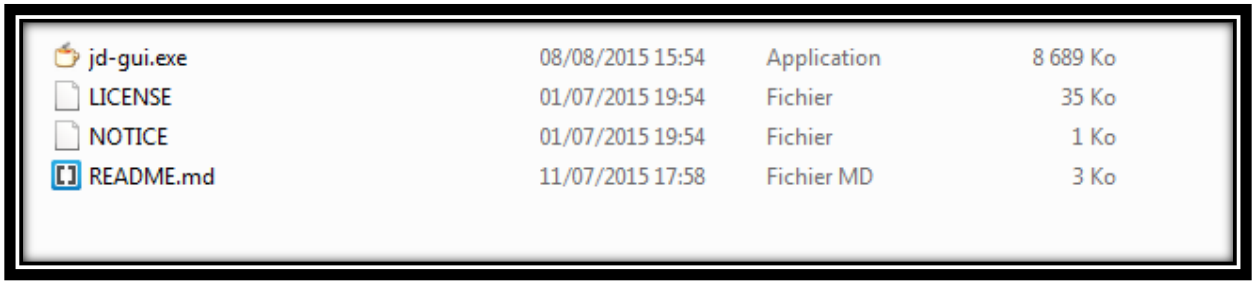


Figure .43 : Java Decompiler

12) Nous double cliquons sur **jd-gui.exe** afin d'exécuter l'application :

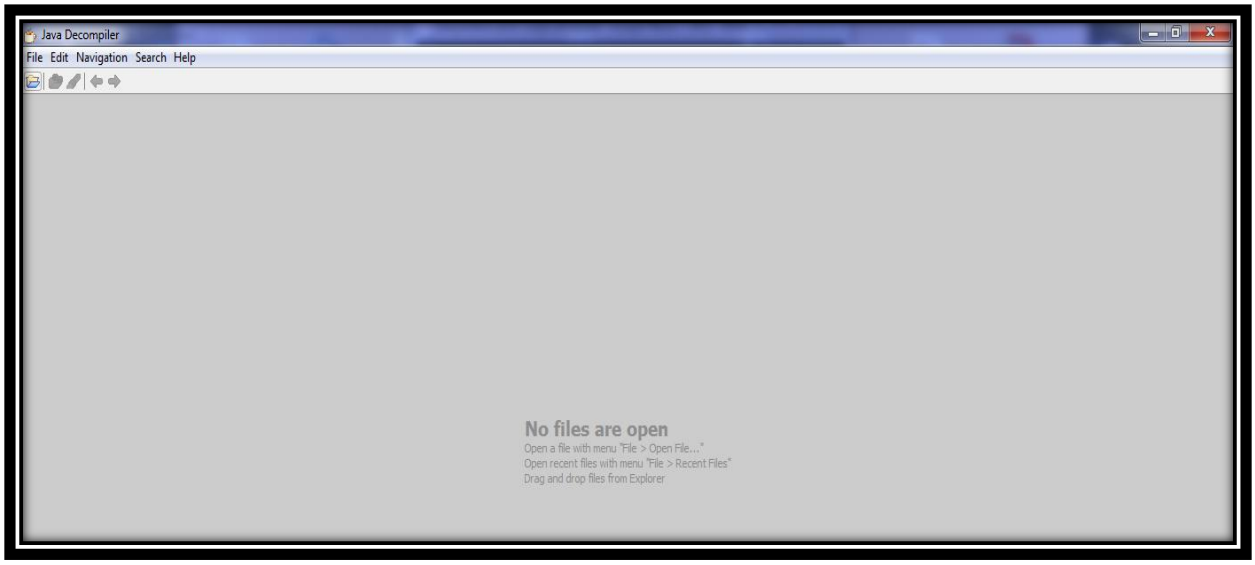


Figure .44 : Ouverture de Java Decompiler

13) Nous cliquons sur **File,** puis **Open file,** nous cliquons sur le fichier **classes.jar** précédemment converti par dex2jar, puis ouvrir :

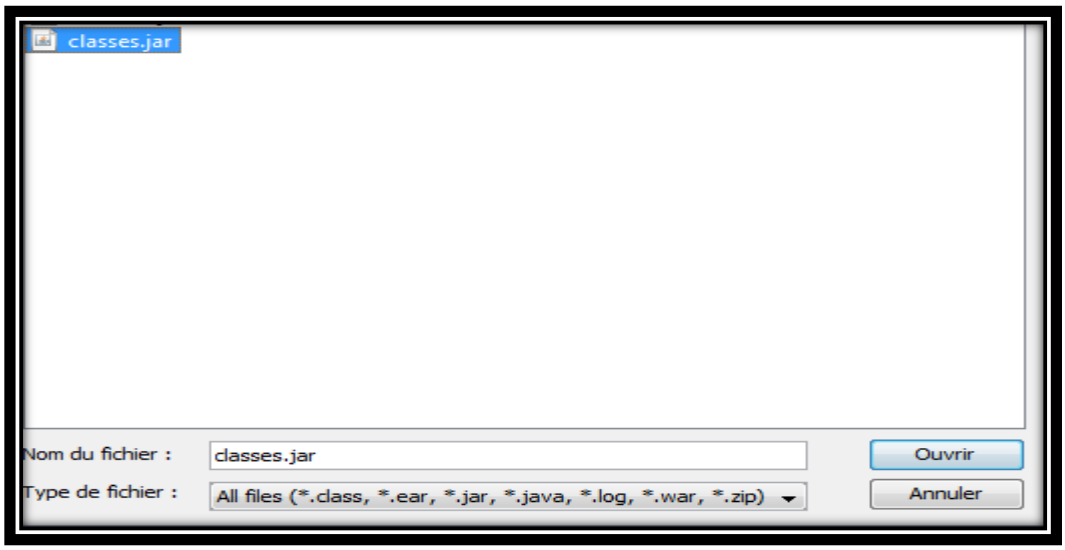


Figure .45 : Ouverture du fichier .JAR crée précédemment par l'outil Dex2Jar

14) Après l'ouverture du fichier classes.jar nous pouvons naviguer sur les différentes classes qui sont écrit en Java :

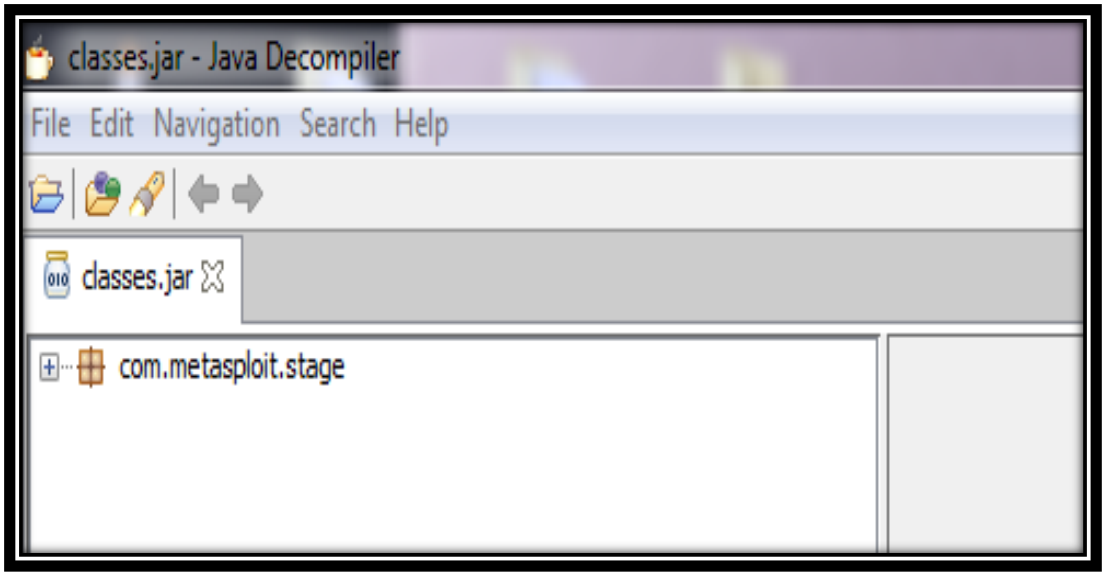


Figure .46 : Ouverture du fichier classes.jar

15) A présent pour trouver l'adresse source de la personne ayant crée ce virus et qui va nous permettre de l'identifier, nous cliquons sur **MainActivity.class** qui est le processus principal de l'application et permet l'exécution d'autres classes dans le même fichier, après ça nous trouvrons « Payload.start » qui exécute une classe Payload qui est probablement un virus :

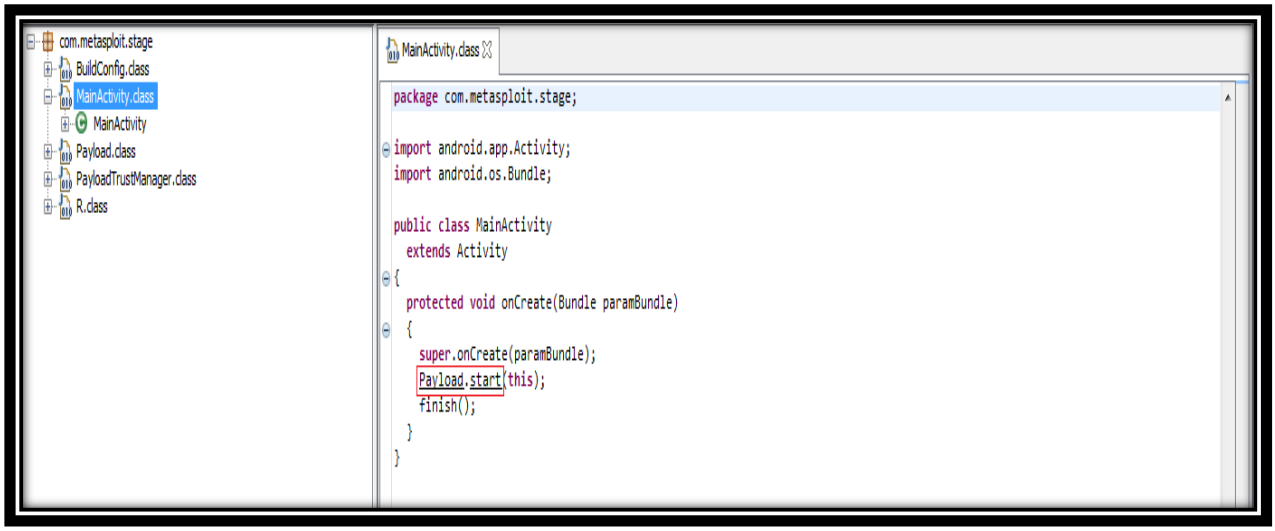


Figure .47 : Contenu de la class MainActivity

16) On clique sur **Payload.class** afin de lire le contenu de cette classe et de trouver plus d'informations. Après cela nous verrons que l'adresse IP source est affichée « tcp://192.168.1.6:4444 » ce qui va nous permettre d'identifier la personne. Dans le cas de notre exemple, nous avons trouvé une adresse IP locale. Pour localiser la personne détentrice de cette adresse, nous allons vérifier les adresses attribuées par le routeur ou bien l'administrateur Réseau.

Toutefois, dans le cas où nous trouvons une adresse IP d'un site malveillant. Par exemple : montrojan.no-ip.org, dans ce cas no-ip.org est un DNS dynamique …. Dans ce cas, on peut l'inclure dans la base de données de l'antivirus utilisé comme étant un site malveillant.

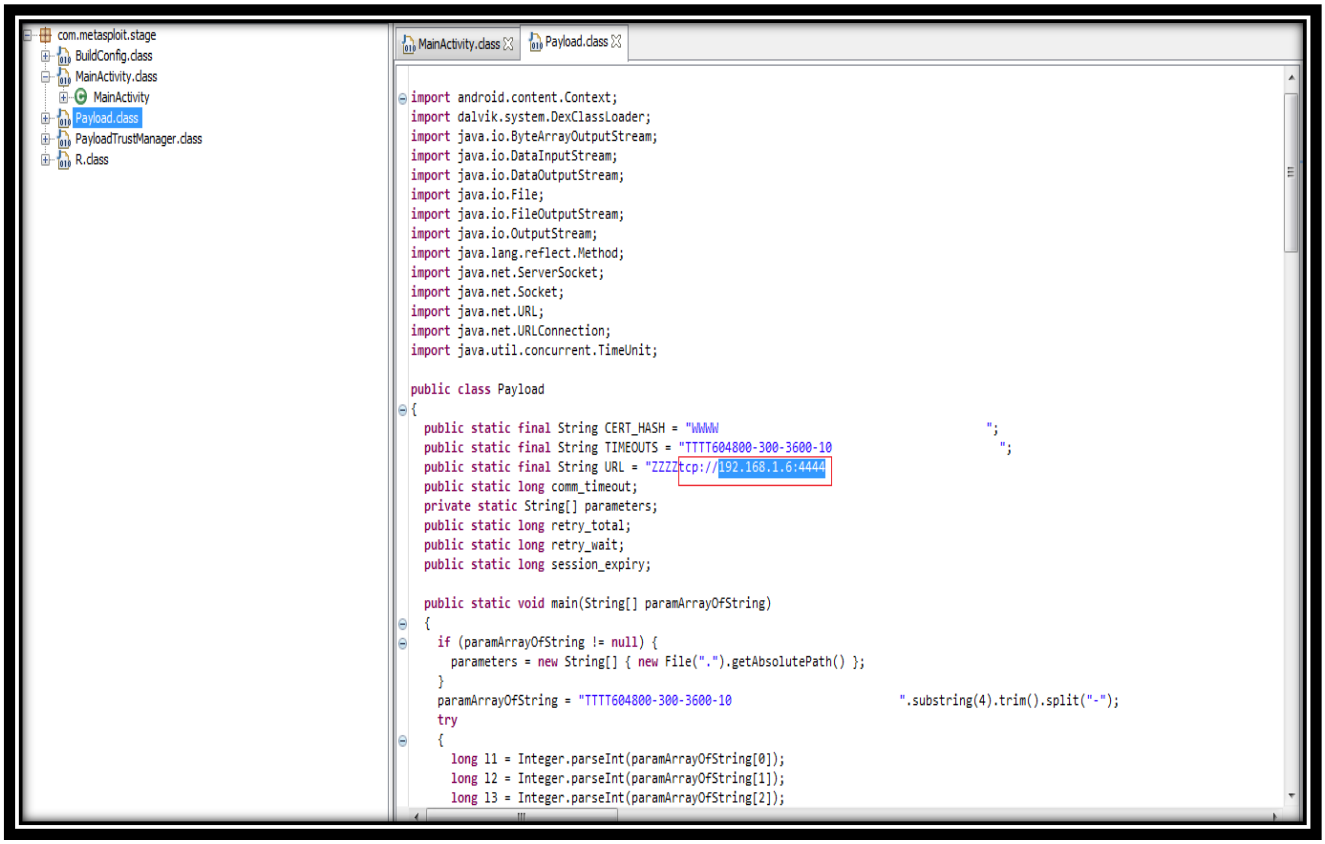


Figure .48 : Contenu de la class Payload et extraction de l'adresse IP du hacker

4. Discussion

Pour effectuer le test d'intrusion, nous avons crée un Trojan, puis nous avons créé un faux point d'accès et nous avons déconnecté l'utilisateur du point d'accès légitime. Une fois que l'utilisateur va se connecter au faux point d'accès, il sera redirigé vers une fausse page, il installe l'application qui est en réalité un Trojan, et nous pourrons ainsi nous introduire dans son Smartphone. Pour faire face à cette intrusion, nous avons utilisé en premier lieu l'antivirus Kaspersky mis-à-jour. Ce dernier nous a permis de détecter et de supprimer le virus que nous avons créé au départ. Toutefois, dans le cas de la non disponibilité d'un antivirus puissant, nous pouvons utiliser l'ingénierie inverse qui consiste à décompiler le fichier (le virus) et à la fin nous aurons l'adresse IP du hacker et nous pouvons ainsi l'identifier. En effet, dans le cas de notre exemple, on a pu détecter l'adresse IP de la machine malveillante.

CONCLUSION

Actuellement la majorité des appareils de communication (Smartphones et tablettes) utilisent le système d'exploitation Android. Dans ce mémoire nous avons présenté et mis en œuvre deux outils de sécurisation de ce système d'exploitation. Pour cela nous avons simulé une intrusion. Celle-ci, consiste à inciter l'utilisateur de télécharger une application qui est en réalité un Trojan. Pour cela, nous avons créé ce Trojan et nous avons créé aussi un faux point d'accès, puis nous avons déconnecté l'utilisateur du point d'accès légitime. Dès que la victime se connecte au faux point d'accès et qu'elle essaye de se connecter à un site donné, elle sera redirigée vers une fausse page qui lui propose d'installer une application sur son Smartphone, l'utilisateur va cliquer sur soumettre, il va télécharger et installer l'application (le Trojan) et ainsi on pourra s'introduire et prendre le control sur cet appareil.

Pour se faire, nous avons crée une machine virtuelle avec un système d'exploitation Kali Linux et nous avons utilisé les différents outils de ce dernier. Puis, nous avons appliqué deux outils de sécurisation, un Antivirus Kaspersky mis à jour qui va détecter et supprimer le virus proposé et un autre outil qui est l'ingénierie inverse qui consiste à décompilé le fichier (le Trojan) et à la fin nous aurons l'adresse IP de l'intrus avec laquelle nous pourrons l'identifier.

Le test d'intrusion qu'on a effectué n'est pas le seul dans ce domaine. Donc et en guise de perspectives, nous proposons de simuler d'autres tes d'intrusion afin de découvrir d'autres failles ainsi mettre en place des outils de sécurisation pour faire face à ce genre d'intrusions.

Bibliographie

[1] : Jean-François PILLOU, Jean-Philippe BAY, « Tout sur la sécurité informatique », 2ème édition, Edition Dunod, Paris, 2009.

[2] : ACISSI, « Sécurité informatique Ethical Hacking », 3ème édition, Edition ENI, Septembre 2012.

[3] : Radoniaina ANDRIATSIMANDEFITRA RATSISAHANANA, « Caractérisation et détection de malware Android basées sur les flux d'information », thèse de doctorat, SUPELEC, Ecole Doctorale MATISSE 2015.

[4] : Thinhinane Ammari, Djamila Attab, « Etude et application des outils de sécurité d'un réseau Wi-Fi », Mémoire de fin d'études de Master Réseau et Télécommunication, UMMTO 2015.

[5] : Fabrice LEMAINQUE, « Tout sur les réseaux sans fil », Edition Dunod, Paris, 2009.

[6] : Laurence SOYER, Mise en place du Wi-Fi, Edition ENI, avril 2005.

[7] : Djemah Massicilia, « Test d'intrusion interne avec une mise en place d'une solution de sécurité », Mémoire de fin d'études de Master Réseau et Télécommunication, UMMTO 2015.

[8] : Frédéric Brault, « Hackez Google Androide », Edition Eyrolles, 2009.

[9] : Khaoula MRABET, Nessrine TRABELSI, « Application de messagerie simple sur Android », rapport de projet de VAP RSM, TELECOM Sud Paris 2011.

[10]: Ec- Council, Ethical Hacking and Countermeasures, version 8 2011.

[11]: DELFOUF Nardjes, DJEBARI Nabila, « Mise en place d'un système de sécurité basé sur le serveur d'authentification TACACS+ », Mémoire de fin d'études de Master Réseau et Télécommunication, UMMTO 2015.