Cryptographie et sécurité

IFT-606

Rapport de projet - La Brulerie

Amandine Fouillet - 14 130 638
Frank Chassing - 14 153 710
Thomas Signeux - 14 126 590

April 11, 2015

Contents

Introduction

Avec la multiplication des objets connectés, notamment les smartphones et autres appareils mobiles, de nombreux réseaux publics ont vu le jour dans diverses endroits. Cependant, la sécurité de ces réseaux est parfois douteuse et il est aisé de s'y introduire, à l'insu de tous. Une fois sur ces réseaux, les possibiltés d'intrusions et de malveillances sont nombreuses.

Parmi ces intrusions, l'une d'elles peut être particulièrement efficace et dangereuse pour les personnes visées. Cette attaque s'appelle Man In The Middle.

Ce projet a pour but d'étudier cette faiblesse du réseau en développant une application capable de reproduire les principales attaques Man In the Middle mais également de pouvoir s'en protéger.

1 Description du projet et des objectifs

1.1 L'attaque Man In The Middle

L'attaque Man In The Middle a pour but d'intercepter les communications transitant entre deux machines, sans que ni l'une ni l'autre ne se doute que le canal de communication est compromis. L'attaquant a alors la possibilité de lire mais aussi de modifier les messages (dans une certaine mesure).

Il existe plusieurs techniques pour ce fair passer pour l'une ou l'autre de ces machines cibles.

- l'ARP Spoofing : attaque la plus fréquente, utilisée dans la partie pratique de ce projet. On force les communications à transiter par l'ordinateur de l'attaquant qui se fait alors passer pour le routeur (gateway) du réseau.
- le DNS Poisoning : le but de cette attaque est de faire correspondre l'adresse IP d'une machine controlée par un pirate à un nom réel et valide d'une machine publique. Pour cela, il altère le ou les serveur(s) DNS du réseau.
- l'annalyse du trafic : technique de sniffing permettant de visualiser les informations non chiffrées.
- le déni de service : empêcher le fonctionnement d'une machine pour en prender le contrôle.

1.2 Objectifs initiaux

L'objectif de ce projet est de mettre en place des scénarios d'attaques de piratage de réseaux et de proposer des moyens de défense. Dans un premier temps, nous explorerons l'actualité des attaques de réseaux publics. Puis nous présenterons le travail réalisé lors du projet. Suivrons les chapitres liés aux descriptions techniques du projet ainsi qu'un guide d'utilisation.

- Pouvoir identifier les ordinateurs connectés au routeur
- Couper l'ensemble des connexions au routeur afin de bénéficier d'une meilleure bande passante
- Limiter la connexion des personnes connectées au réseau
- Récupérer les informations transitant sur les réseau pour pouvoir les analyser et identifier les personnes se trouvant dans le bar
- Organiser une défense aux attaques précédentes
- Faire une vidéo de présentation

2 Présentation du travail réalisé

2.1 Attaque

Dans cette section, nous allons présenter nos applications d'attaques. Plusieurs scripts ont ainsi été déployés pour les réaliser. Le premier script vise à identifier les machines sur le réseau. Le second

2.1.1 Identification

2.1.2 Coupure

2.1.3 Sniffer

2.2 Défense

Dans cette section, nous allons présenter nos applications de défense. Afin de contrer les attaques ciblées sur une machine, nous avons déployé deux scripts. Le premier réalise une détection pour savoir si la machine est victime d'une attaque ARP spoofing. Le second script est une simple commande qui permet de contrer l'attaque de coupe de connexion.

2.2.1 Détection

2.2.2 Anti-coupure

3 Guide utilisateur

3.1 Interface principale

3.2 Attaquer

3.2.1 Couper et rétablir

3.2.2 Sniffer

3.3 Se défendre

3.3.1 Détecter une attaque

3.3.2 Activer une protection contre les coupures

4 Planification et organisation

4.1 Outils utilisés

4.2 Planification

5 Améliorations

Conclusion

List of Figures