**RAPPORT FINAL DE PROJET**

Sécurité et cryptographie

IFT606

Travail présenté à :

Mohammed Ouenzar

Marc Verreault

Présenté par:

Francis Gravel St-Pierre (11 140 669)

Simon Lévesque-Gobeil (11 166 187)

Alex Provencher (11 173 124)

Remise-le :

13 avril 2015

Faculté des Sciences

Université de Sherbrooke

Description

Le but de ce projet est d’explorer une attaque très connue en informatique : Le *man in the middle* attaque. Dans un premier temps, nous rechercherons une potentielle victime en utilisant un outil de recherche réseau. Par la suite, nous effectuerons un empoissonnement du réseau, avec le protocole ARP, dans le but de rediriger tous les paquets réseau de notre victime vers l’ordinateur de l’attaquant. Ensuite, nous utiliserons diverse technique pour afficher et/ou modifier, en temps réel, les paquets qui transigeront par l’ordinateur de l’attaquant. Cette attaque doit se faire de manière transparente pour la victime (protocole HTTP seulement). Le but ici est donc d’écouter le trafic de la victime, trouver de l’information utile (mot de passe, information privée, etc..) et d’altérer les paquets renvoyés par le serveur distant dans le but d’afficher du contenu modifié à l’usager.

Échéanciers et tâches

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **DESCRIPTION** | **SIMON**  **LÉVESQUE GOBEIL** | **ALEX PROVENCHER** | **FRANCIS GRAVEL ST-PIERRE** |
| **SEMAINE 1** | Recherche documentaire  choix des technologies  choix des librairies (ARP, Scan réseau, routing, etc.). | Recherche  Écriture du rapport initial | Recherche  Implémentation du bootstrap | Recherche  Création du système de gestion de versions  Écriture du rapport initial |
| **SEMAINE 2** | Implémentation de la découverte Réseau.  ARP poisoning | Développement  ARP poisoning | Développement  Découverte Réseau | Développement  ARP poisoning |
| **SEMAINE 3** | Routing des paquets  Affichage et modification en temps réel des paquets. | Développement  Routing des paquets | Développement  Affichage et modification | Développement  Affichage et modification |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **SEMAINE 4** | Production de documentation et de rapport  multiple test | Exécution de tests dans le but de se conformer aux exigences initiales du système | Exécution de tests dans le but de se conformer aux exigences initiales du système | Production de documents de références sur l’utilisation générale de la solution logicielle |

Nos réalisations

**la détection des adresses IP sur le réseau**

Le script fait un scan du réseau et détecte les clients connectés à celui-ci. Il affiche les informations au client pour que celui-ci choisisse la bonne victime. Notre script est aussi dans la capacité de détecter l’adresse IP de l’attaquant ainsi que l’adresse de la passerelle par défaut qui est aussi celle du routeur. Nous pouvons aussi avoir de l’information, dans certains cas spécifiques, sur le type de système d’exploitation qui est détecté par notre détection réseau.

**Empoisonnement ARP d’une cible**

Le protocole ARP est un protocole qui permet d’associer une adresse IP à une adresse MAC. En effet, le réseau a besoin d’une adresse MAC pour pouvoir envoyer de l’information à un autre ordinateur sur la couche 2 du modèle OSI. Le principe d’empoissonner le réseau est de substituer au routeur en envoyant de faux paquets ARP sur le réseau. Ainsi, la victime sur le réseau se fait bombarder de faux paquet ARP, ce qui fait en sorte que les tables ARP se font modifier et ainsi tout le trafic réseau est envoyé vers l’ordinateur de l’attaquant.

**Espionnage du trafic d’une cible**

Lorsque le trafic réseau est redirigé vers l’ordinateur de l’attaquant, il est alors facile de visionner le trafic et ainsi trouver de l’information intéressante. Lorsque la connexion de la victime n’est pas en protocole HTTPS, il est alors très facile d’intercepter ceux-ci.

**Interruption de la connexion au réseau d’une cible**

Puisque le trafic réseau de la victime passe par notre ordinateur, il est alors facile de l’interrompre complètement, ainsi rendant la connexion de la victime inutilisable.

Nos difficultés

**Compatibilité multiplateforme**

Nos différentes librairies utilisées au début n’étaient pas compatibles pour toutes les plateformes. Ayant dans l’équipe des personnes qui travaillaient sur Windows, Mac et Chromebook, il fallait utiliser les librairies qui étaient réellement multiplateformes.

**Difficulté à paralléliser les scripts**

Nous avons essayé au début d’utiliser des processus pour empoissonner différents IP en même temps, mais nous avions des problèmes de concurrence sur des fichiers des librairies que nous utilisions.

**Difficulté à tester**

Nous avions pris du temps avant d’avoir notre équipement réseau pour pouvoir faire nos tests. Ainsi, puisque nous ne pouvions utiliser les infrastructures de l’université, il était difficile de pouvoir tester nos différentes solutions.

Explication du script

* Script: mitm.py
* Langage: python
* Description: Envoi des requêtes ARP vers les victimes pour modifier son registre ARP
* Résultat: Tous les paquets des victimes passent maintenant par l’ordinateur de l’attaquant.

usage: mitm.py [— h] [— i] [— m MYIP] [— n NETIFACE] [— r ROUTERIP] [— x] [— y]  
optional arguments:  
 — h, --help show this help message and exit  
 -i, --interactive manually choose targets  
 -m MYIP, --myIp MYIP Manually specify your IP if not able to automatically  
 get it  
 -n NETIFACE, --netiface NETIFACE  
 Specify the interface to use by default wlan0  
 -r ROUTERIP, --routerIP ROUTERIP  
 Specify the IP for the router if not able to  
 automatically find it  
 -x, --ignoreHttp Don't redirect paquet from port 80 to the local  
 webserver  
 — y, --ignoreHttps Don't redirect paquet from port 443 to the local  
 webserver