



 Stalker In The Middle

Laissez parler leurs paquets !

 Un moyen simple et efficace pour intercepter les paquets destinés à une autre machine et tester les faiblesses d’un réseau.

Etude d’opportunité et de faisabilité

Version 1.2

10/04/2013

Historique des révisions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Auteur** | **Relecteur** |
| 03/04/2013 | 1.0 | Document initial | Alban INQUEL | Christie BUNLON |
| 03/04/2013 | 1.0.1 | Mise à jour des objectifs et des risques | Nicolas CHATELAIN | Brice HOFFMANN |
| 08/04/2013 | 1.1 | Ajout du périmètre et de la mission | Alban INQUEL | Nicolas CHATELAIN |
| 10/04/2013 | 1.2 | Finalisation | Alban INQUEL | Nicolas CHATELAIN |

Sommaire

[Mission 4](#_Toc334801176)

[Objectifs 4](#_Toc334801177)

[Opportunité 4](#_Toc334801178)

[Contexte initial et historique 4](#_Toc334801179)

[Périmètre du projet 4](#_Toc334801180)

[Impact sur l’existant et vision à plus long terme 4](#_Toc334801181)

[Avantages, gains / Pertes 5](#_Toc334801182)

[Risques et actions en conséquence 5](#_Toc334801183)

[Etudes d’opportunité 5](#_Toc334801184)

[Etudes de faisabilité 5](#_Toc334801185)

[Aspects économiques ou matériels 5](#_Toc334801186)

[Budget prévisionnel 5](#_Toc334801187)

## Mission

## Interception de datagrammes destinés à une machine et affichage de leur contenu en temps réel.

## Objectifs

1. Pouvoir scanner l’intégralité du réseau avant le 15/04.
2. Pouvoir modifier la table ARP à distance avant le 22/04.
3. Pouvoir intercepter et rerouter les paquets avant le 29/04.
4. Création d’une interface graphique avant le 03/05.
5. Pouvoir obtenir les mots de passe transitant en clair avant le 06/05.
6. Pouvoir modifier les réponses DNS avant le 15/05.
7. Pouvoir intégrer les cookies de la « victime » automatiquement sur la machine attaquante avant le 23/05.
8. Affichage des pages web visitées avant le 30/05.
9. Pouvoir intercepter les transmissions VoIP avant le 05/06.
10. Pouvoir générer de faux certificats automatiquement avant le 13/06.

# Opportunité

## Contexte initial et historique

Ce projet se réalisera dans le cadre du projet industriel de semestre 4 SR de l’écoIe informatique IN’TECH INFO. C’est pour nous le moment de concrétiser l’enseignement que nous a apporté l’école dans le domaine des Systèmes et Réseaux. En effet, notre projet consiste à récupérer des informations, circulant sur le réseau afin de pouvoir en afficher le contenu. Pour ce faire, il faut maîtriser les différents concepts de fonctionnement du réseau de manière à définir le quoi et le comment des techniques que nous utiliserons durant ce semestre. Ce projet a été proposé par notre directeur Eric Lalitte, et intéressés par la sécurité réseau, nous avons décidé de le réaliser.

## Périmètre du projet

L’application SITM ne fonctionnera qu’en réseau local.

Lors de ce projet nous nous contenterons de traiter les protocoles suivants :

* HTTP, HTTPS
* FTP
* POP
* IMAP
* SMTP
* DNS
* VoIP
* TELNET

Afin de pouvoir intercepter les données envoyées par l’ordinateur victime au routeur nous utiliserons la technique de l’ARP Spoofing. Nous mettrons également en place une autre technique ayant le même objectif. Celle-ci utilisera la technique du DHCP Spoofing.

L’interception même et le reroutage des paquets s’effectueront grâce à la librairie Libpcap. C’est une librairie qui permet de capturer des paquets et de les analyser.

L’aspect graphique du logiciel sera développé à l’aide de la librairie perl Curses.

La solution permettant d’obtenir les mots de passe, contenus dans les paquets capturés grâce à Libpcap, sera codée en perl par nos soins.

La modification de requête DNS s’effectuera grâce à la librairie perl Net::DNS.

L’intégration de cookie sur la machine exécutant le programme se fera à l’aide du navigateur Firefox.

L’affichage des pages web visitées s’effectuera à l’aide de Webkit.

L’interception de communication VoIP se fera à l’aide de librairies Perl dont Net::RTP.

Pour pouvoir générer de faux certificats, nous utiliserons le logiciel openCA.

## Impact sur l’existant et vision à plus long terme

Le logiciel créé, est une solution potentiellement utilisable par les auditeurs de sécurité. Il permettra, lors d’un test d’intrusion, de vérifier l’intégrité du réseau d’une entreprise face aux attaques de type « man in the middle ». Une des évolutions possible de ce projet serait d’avoir la possibilité d’intercepter tous les protocoles connus circulant sur un réseau. L’étape supérieure serait d’enrichir de nouvelles fonctionnalités SITM, de manière à créer une sorte de « couteau suisse » de l’audit de sécurité.

## Avantages, gains / Pertes

**Avantages liés à la réussite du projet :**

* Logiciel de défense contre un type d’attaque.
* Reconnaissance de l’enseignement d’IN’TECH INFO lors du forum PI.
* Satisfaction du suiveur.
* Simplification d’utilisation de l’attaque ARP Poisoning.

**Pertes liées à l’échec du projet :**

* Projet raté pour le client

## Risques et actions en conséquence

**Risques techniques :**

* Manque de connaissances techniques pour travailler sur ce projet
  + Risque atténué :
    - Recherche sur internet de documentations, de tutoriels ou autre en rapport avec la technologie qui pose problème.
    - Demande de conseil au suiveur et à toute personne susceptible de pouvoir nous aider (intérieure comme extérieure à l’école).
    - Analyse de sources de programmes existants.
* Manque de matériel
  + Risque atténué :
    - Demande de matériel auprès de notre suiveur ou si impossibilité, utilisation de matériel personnel.
* Créer des problèmes sur le réseau
  + Risque refusé :
    - Les tests seront effectués sur un réseau local, destiné à ce seul usage.
* Manque de travail :
  + Risque atténué :
    - Bonne gestion du projet.
* Perte des données :
  + Risque atténué :
    - Données sauvegardées en local et à distance avec gestion des versions (Git).

**Risques externes :**

* Problèmes personnels des membres du projet :
  + Risque accepté :
    - Problèmes imprévisibles.

**Risques organisationnels :**

* Mauvaise préparation du forum PI
  + Risque atténué
    - Prise en compte, dans le planning, de l’organisation du forum PI.

**Risques de gestion :**

* Mauvaise gestion du temps de travail :
  + Risque atténué
    - Concertation lors de la création du planning en début de projet, pour un planning clair et précis.
* Mauvaise communication avec le suiveur :
  + Risque refusé
    - Réunions hebdomadaires prévues.

## Etudes d’opportunité

Il y a sur le marché, plusieurs logiciels « couteau suisse » de la sécurité informatique, permettant de lire les paquets destinés à une machine victime.

On peut nommer Cain & Abel ou encore Ettercap. Notre solution a un objectif final plus poussé dans le domaine d’attaque in the middle, puisque le but de ce projet est de visualiser en temps réel les pages visitées par l’utilisateur victime au sein d’un même réseau.

Il dispose également d’une fonctionnalité permettant de tromper l’utilisateur visitant des sites web dits « sécurisés » via HTTPS en redirigeant chaque site sécurisé en version non sécurisée.

Il dispose, en plus, d’un module de protection permettant de contrer les attaques du même genre sur le réseau. SITM est aussi un logiciel capable d’utiliser une fausse adresse MAC afin de rester le plus discret possible sur le réseau.

SITM est donc un logiciel d’attaque et de défense, apportant un plus dans le domaine technique et un confort visuel lors de son utilisation.

## Etudes de faisabilité

Les moyens nécessaires à la réussite du projet sont assez limités. Nous n’avons besoin que de trois ordinateurs, des câbles, un switch et un routeur.

Ce matériel devrait nous être prêté par IN’TECH INFO. Si l’école se trouve dans l’incapacité à nous prêter ce matériel, nous en utiliserons du personnel.