-

 [go du projet]

 Stalker In The Middle

 Laissez parler leurs Packets

Un moyen simple et efficace pour comprendre comment une attaque man in the middle se déroule au sein d'un réseau, il permet aussi d'auditer ce réseau de façon à analyser ses failles. Stalker In The Middle permet aussi de s'en protéger

grâce à sa fonction de protection.

Spécifications

Version 1.0

03/04/2013

**Historique des révisions**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Auteur** | **Relecteur** |
| 03/04/2013 | 1.0 | Actions/réalisations,  documents de référence | Nicolas CHATELAIN | Alban  INQUEL |
| 03/04/2013 | 1.1 | Introduction | Alban INQUEL |  |
|  |  |  |  |  |
|  |  |  |  |  |

Veillez à la cohérence des dates et des numéros de versions dans ce tableau « Historique des révisions » mais également par rapport à la page de garde.

Table des matières

[1 Introduction 5](#_Toc352768778)

[1.1 Contexte initial, historique et vision 5](#_Toc352768779)

[1.2 Mission 5](#_Toc352768780)

[1.3 Objectifs 5](#_Toc352768781)

[1.4 Glossaire 5](#_Toc352768782)

[1.5 Documents de référence 5](#_Toc352768783)

[2 Description générale 6](#_Toc352768784)

[2.1 Acteurs et caractéristiques 6](#_Toc352768785)

[3 Caractéristiques du produit 6](#_Toc352768786)

[3.1 Description et priorité 6](#_Toc352768787)

[3.2 Actions / Réalisations par objectif 7](#_Toc352768788)

[3.2.1 Pouvoir scanner l’intégralité du réseau avant le 15/04. 7](#_Toc352768789)

[3.2.2 Pouvoir modifier la table ARP à distance avant le 22/04. 7](#_Toc352768790)

[3.2.3 Pouvoir intercepter et rerouter les paquets avant le 29/04 7](#_Toc352768791)

[3.2.4 Création d’une interface graphique avant le 03/05 7](#_Toc352768792)

[3.2.5 Pouvoir obtenir les mots de passe transitant en clair avant le 06/05 7](#_Toc352768793)

[3.2.6 Pouvoir modifier les réponses DNS avant le 15/05 7](#_Toc352768794)

[3.2.7 Pouvoir intégrer les cookies de la « victime » automatiquement sur la machine attaquante avant le 23/05. 7](#_Toc352768795)

[3.2.8 Affichage des pages web visitées avant le 30/05. 8](#_Toc352768796)

[3.2.9 Pouvoir intercepter les transmissions VoIP avant le 05/06. 8](#_Toc352768797)

[3.2.10 Pouvoir générer de faux certificats automatiquement avant le 13/06. 8](#_Toc352768798)

[4 Autres spécifications non fonctionnelles 8](#_Toc352768799)

[4.1 Environnement opérationnel 8](#_Toc352768800)

[4.2 Contraintes d’organisation et temporelles 8](#_Toc352768801)

[4.3 Contraintes de sécurité 8](#_Toc352768802)

[4.4 Documents pour les participants (ou clients ou abonnés…) 8](#_Toc352768803)

[4.5 Attributs de qualité 8](#_Toc352768804)

[4.6 Exigences de sécurité 9](#_Toc352768805)

[4.7 Exigences financières 9](#_Toc352768806)

# Introduction

## Contexte initial, historique et vision

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.

## 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 détecter les modifications de la table ARP avant le 25/04.
4. Pouvoir intercepter et rerouter les paquets avant le 29/04.
5. Création d’une interface graphique avant le 03/05.
6. Pouvoir obtenir les mots de passe transitant en clair avant le 06/05.
7. Pouvoir modifier les réponses DNS avant le 15/05.
8. Pouvoir intégrer les cookies de la « victime » automatiquement sur la machine attaquante avant le 23/05.
9. Affichage des pages web visitées avant le 30/05.
10. Pouvoir intercepter les transmissions VoIP avant le 05/06.
11. Pouvoir générer de faux certificats automatiquement avant le 13/06.

## Glossaire

Protocole : Norme de communication permettant d’établir une communication entre ordinateurs.

Adresse MAC : Identifiant unique et physique implanté dans la carte réseau.

ARP (Address Resolution Protocol) : Protocole permettant la résolution de l’adresse MAC à partir de l’adresse IP.

MITM (Man In The Middle) : Technique permettant l’interception des paquets destinés à un autre ordinateur en modifiant la table ARP de l’ordinateur victime.

## Documents de référence

Listez tous les documents, normes, rapports, sites Internet…, utiles à la compréhension du projet, identifiez leurs origines (règles de recherches documentaires), et indiquez leur emplacement. En cas de besoin, les documents peuvent être annexés.

Exemples :

* Résultats d'interviews des parties prenantes
* Enquêtes, sondages, questionnaires
* Cahier des charges
* Règles métier
* Lois et réglementations

|  |  |  |
| --- | --- | --- |
| Nom du document | Emplacement | Auteur |
| Documents avant-projet | GitHub SITM | Équipe SITM |
| Explication de l’attaque Man In The Middle | <http://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu> | NC |
| Explication ARP poisoning | <http://fr.wikipedia.org/wiki/ARP_poisoning> | NC |
| Explication DHCP poisoning | <http://www.hakipedia.com/index.php/DHCP_Rogue_Server> | NC |
| Explication protocole DHCP RFC 2131 | <http://tools.ietf.org/html/rfc2131> | NC |
| Explication protocole ARP RFC 826 | <http://www.ietf.org/rfc/rfc826.txt> | NC |
| Librairies Perl utilisées dans ce projet | <http://www.cpan.org/> | NC |
| Explication DNS RFC 1034 | <http://www.ietf.org/rfc/rfc1034.txt> | NC |

# Description générale

## Acteurs et caractéristiques

Il s’agit de lister toutes les personnes ou entités qui pourraient retirer un bénéfice (sous quelque forme que ce soit) à participer (sous quelque forme que ce soit) au PRP.

|  |  |  |
| --- | --- | --- |
| Acteurs | Caractéristiques | Attentes |
| Client | A un besoin demandant une solution | Une solution répondant à son besoin |
| Équipe SITM | Conceptrice de la solution | Acquisition de nouvelles compétences  Répondre à l’attente du client |

# Caractéristiques du produit

## Description et priorité

A la lecture du tableau que vous compléterez, le lecteur pourra avoir une vision globale de l’événement et de son déroulement, ou bien une vision globale des activités, services et cibles de la structure que vous allez créer (Club, Association, Entreprise).

Quelques exemples (très incomplets, à dessein) pour un événement :

|  |
| --- |
| Description Générale |

|  |  |  |
| --- | --- | --- |
| **Catégorie / Domaine** | **Item / Description** | **Priorité (H / M / F)** |
| **Cibles** | Client | Haute |
| Les personnes souhaitant tester la sécurité de leur infrastructure réseau | Moyenne |
| **Fonctionnalités** | Visualisation des pages web consultées en direct par l’utilisateur « victime » | Haute |
| Enregistrement des conversations VoIP de l’utilisateur « victime » | Haute |
| Visualisation des mots de passe, circulant en clair sur le réseau, d’une machine « victime » | Moyenne |
| Interface graphique | Moyenne |
| Détection des tentatives d’attaque de type Man In The Middle au sein d’un réseau | Moyenne |
| **Communication** | IN’TECHOES | Haute |
| Site web du groupe ESIEA | Faible |

## Actions / Réalisations par objectif

### Pouvoir scanner l’intégralité du réseau avant le 15/04.

* + Calculer la plage d’adresse du réseau local.
  + Envoyer de nombreux paquets ARP et ICMP à toutes les adresses IP.
  + Recevoir les réponses en écoutant les paquets et découvrir les adresses MAC du réseau.

### Pouvoir modifier la table ARP à distance avant le 22/04.

* + Envoyer un paquet de réponse ARP indiquant que l’adresse du routeur dispose maintenant de l’adresse MAC de l’ordinateur interceptant les paquets.
  + Vérifier la réception de paquets provenant de l’ordinateur victime.

### Pouvoir intercepter et rerouter les paquets avant le 29/04

* + Pouvoir lire et interpréter les paquets à l’aide de la librairie libpcap.
  + Modifier ou retransmettre les paquets à l’aide du FORWARDING.

### Création d’une interface graphique avant le 03/05

* + Utilisation de la librairie Curses pour créer l’interface en PERL.
  + Lier le programme initial à l’interface graphique.

### Pouvoir obtenir les mots de passe transitant en clair avant le 06/05

* + Étudier les différents protocoles et leurs systèmes d’authentification.
  + Réussir à extraire les identifiants en fonction du protocole utilisé.

### Pouvoir modifier les réponses DNS avant le 15/05

* + Être capable d’interpréter les paquets DNS, les modifier, puis enfin les retransmettre.

### Pouvoir intégrer les cookies de la « victime » automatiquement sur la machine attaquante avant le 23/05.

* + Étudier les solutions stables et acceptables afin d’intégrer les cookies sur un navigateur.
  + Implanter la solution.

### Affichage des pages web visitées avant le 30/05.

* + Intercepter et enregistrer les réponses HTTP.
  + Convertir la page web au format image.
  + Ouvrir les images finales.

### Pouvoir intercepter les transmissions VoIP avant le 05/06.

* + Etre capable de détecter lorsqu’un appel VoIP débute.
  + Enregistrer les conversations vocales dans un format audio.

### Pouvoir générer de faux certificats automatiquement avant le 13/06.

* + Détecter les transactions HTTPS.
  + Générer le faux certificat et l’envoyer à la victime.

# Autres spécifications non fonctionnelles

## Environnement opérationnel

Le projet est susceptible d’être développé dans les locaux d’IN’TECH INFO à Ivry-sur-Seine et à chaque endroit où un membre de l’équipe dispose d’une connexion Internet.

## Contraintes d’organisation et temporelles

Les sources du programme SITM doivent être modifiables simultanément, c’est pour cette raison que nous mettons en place un système de gestion de version en ligne, GitHub.

Il faut également pouvoir terminer les objectifs en temps et en heure, c’est une chose complexe car étant donné que nous implantons des fonctionnalités complexes et souvent nouvelles, nous ne pouvons pas bien estimer le temps requis.

## Contraintes de sécurité

Nous devons éviter lors de la phase de test d’utiliser le réseau IN’TECH INFO car SITM est un programme dangereux modifiant le routage des ordinateurs d’un réseau. Afin d’éviter ce problème, nous devrons mettre en place notre propre réseau local.

## Documents pour les participants (ou clients ou abonnés…)

Code source du programme & manuel d’utilisation du programme.

## Attributs de qualité

Le programme devra être fonctionnel sur la grande majorité des distributions Linux, devra être portable et ne devra pas utiliser un grand nombre de dépendances.

SITM doit être rapide, le programme doit avoir un minimum de temps de chargement, les attaques doivent pouvoir être lancer en quelques minutes.

SITM doit être stable, il doit être capable de gérer les erreurs provenant par exemple de paramètres invalides saisis par l’utilisateur.

SITM doit être performant, l’utilisateur doit avoir un choix entre plusieurs attaques, plusieurs méthodes de scans et devra être capable de traiter un grand nombre de paquet en un temps minimum.

Le programme devra disposer de nombreuses fonctionnalités configurables en fonction des besoins de l’utilisateur.

## Exigences de sécurité

Tous les tests de l’application doivent être faits dans un réseau privé afin que ces tests ne puissent pas interroger les ordinateurs et les routeurs IN’TECH INFO.