Man-in-the-Middle attack on WPA2-Enterprise networks.

Project for the Télécom SudParis course NET4104.

Nicolas Rocq, Benoit Marzelleau, Baptiste Sauvé,
Baptiste Legros, Tom Burellier

19 mars 2024

Contents

1 Introduction **1**
1.1 Contributors 1

2 Guidelines (in French) **1**
2.1 Sur la forme 1
2.2 Sur le fond 2

3 To-Do **3**

4 What is a Man In The Middle Attack **4**

5 Sources **4**
5.1 Pandoc 4

1 Introduction

In this project, we will explore a **MITM** (Man-in-the-Middle) attack on **WPA2-Enterprise** networks that **do not validate the CA** (Certificate Authority) certificate. This is exploiting the fact that the client does not validate the server's certificate, and the server does not validate the client's certificate. This is a common configuration in many enterprise networks, as it is easier to manage.

1.1 Contributors

- Nicolas Rocq[1]
- Benoit Marzelleau[2]
- Baptiste Sauvé[3]
- Baptiste Legros[4]
- Tom Burellier[5]

2 Guidelines (in French)

2.1 Sur la forme

Les groupes doivent être composés de 4 ou de 5 personnes, et peuvent être composés de personnes des deux groupes.

L'ensemble du développement devra se faire sur un dépôts Git unique par projet, hébergé sur Github, Gitlab.com ou GitlabEns ; Le coordinateur du module devra être ajouté au dépôt git dès la prochaine séance.

[1]https://github.com/Nishogi
[2]https://github.com/xanode
[3]https://github.com/Nepthales
[4]https://github.com/Direshaw
[5]https://github.com/Balmine

Nom d'utilisateur Github : rgrunbla Nom d'utilisateur Gitlab : rgrunbla Nom d'utilisateur GitlabEns : remy.grunblatt

Il est autorisé de réutiliser des ressources en lignes si celles-ci sont clairement identifiées, par exemple en spécifiant au niveau de chaque bloc de code la provenance de ces données (URL) et en plaçant ces URLs dans un fichier « sources.txt » à la racine du dépôt ;

L'ensemble des membres du groupe doivent participer à l'ensemble des tâches du projet, notamment :

Documentation ; Développement / Déploiement / Technique / … ; Écriture du rapport ; Présentation Vidéo ; Le rapport devra être rédigé en markdown, tracké dans Git dès le début du travail sur le projet, et compilé en PDF avec pandoc. Il devra comporter de 15 à 30 pages rédigées dans une police de type Arial, taille 11 ou 12 (ce ne sont pas des obligations), sans tenir compte des annexes qui ne comptent pas dans ce décompte (annexes dans lesquelles doivent figurer les extraits de code long, les photos, …) ;

La présentation finale durera 15 minutes (900 secondes) maximum, et prendra la forme d'une vidéo à m'envoyer avant le 2 mai 2024 à 23h59. Ces vidéos seront projetées lors de l'évaluation finale qui aura lieu le 3 mai 2024 à 10h, et seront évaluées par les pairs (c'est-à-dire vous) en utilisant une grille de notation en cours de conception, et qui sera envoyée prochainement.

2.2 Sur le fond

Le projet doit être centré sur les réseaux sans-fils : Bluetooth, BLE, Wi-Fi, Réseaux Cellulaire, Radios Logicielles, Capteurs, …

Le projet doit posséder au moins une des colorations suivantes :

Cybersécurité ; Simulation ou Modélisation ; Recherche et Développement ; Design / Audit ; Déploiement réel ou Maquettage / Prototype ; Le projet doit contenir une contribution originale et du travail : il n'est pas possible de juste copier trois bouts de codes déjà disponibles en ligne et les assembler pour que le projet soit considéré comme un succès. Pour rappel, 5 séances de 3h sont dédiées à ce projet, plus du travail à la maison, ce qui amène à un total de 4 semaines à temps complet pour une personne (35h / semaine) et un groupe de cinq personnes.

Le niveau d'encadrement est à décider à la prochaine séance :

Encadrement minimal : À part répondre à vos questions quand elles me sont addressées, je ne vais pas me pré-occuper du bon avancement de votre projet jusqu'à l'évaluation finale. Encadrement intermédiaire : Je fais le point à chaque séance programmée sur votre projet, en vous conseillant sur les choix à effectuer. Encadrement maximal : Une visio de 20 à 30 minutes est organisée chaque semaine jusqu'à la complétion du projet, et je vous impose un certain nombre de choix d'orientation, ou techniques qui devront être respectés. La prise de risque n'étant pas la même selon l'encadrement, la note finale tiendra compte de cet encadrement à un niveau de 4 points. Ainsi, selon le niveau d'encadrement, le groupe obtiendra :

4 / 4 points pour un encadrement minimal ; 2 / 4 points pour un encadrement intermédiaire ; 0 / 4 points pour un encadrement maximal. Cela veut dire qu'un projet avec un encadrement maximal obtiendra au maximum 16/20, un projet avec un encadrement intermédiaire obtiendra au maximum

18/20 et un projet avec un encadrement minimal obtiendra au maximum 20/20 (mais cela ne présume pas du minimum).

La présence reste obligatoire à l'ensemble des séances, quel que soit le type d'encadrement.

D'ici la fin de la prochaine séance, je souhaite donc un mail précisant, de manière construite, le projet que vous souhaitez réaliser avec :

Des informations sur les membres du groupe (nom, prénom, email) ; Un résumé détaillé de ce que vous comptez faire dans le projet (thématique, technologies, coloration, …) ; Le niveau d'encadrement souhaité ; L'URL du dépôt git qui sera utilisé pour l'ensemble du projet Ne vous précipitez pas pour m'envoyer ce mail, je validerai le principe de vos projets à la prochaine séance. Je reste à votre disposition pour répondre à vos questions sur le projet d'ici là, sur ce forum.

Si vous n'avez pas d'idée de projets, je pourrai en proposer autour du contenu du cours, mais ces projets seront donc nécessairement avec un mode d'encadrement maximal.

3 To-Do

- State of the art
- Program the card to impersonate an access controller
- Implement a MITM attack
- Have a testing environment
- Test
- Write the report

4 What is a Man In The Middle Attack

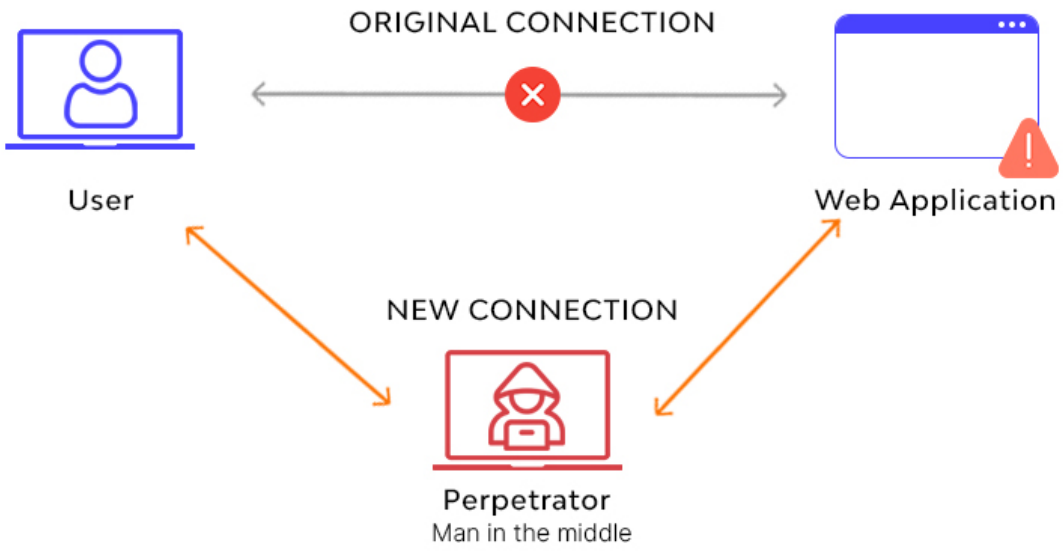

Figure 1: Man In The Middle

5 Sources

5.1 Pandoc

CI with pandoc - https://gitlab.com/pandoc/pandoc-ci-example