



ft\_malcolm

An introduction to Man in the Middle attacks

*Summary: This is the first project of a network security branch created by maabou-h.*

# Contents

<b>I</b>	<b>Foreword</b>	<b>2</b>
<b>II</b>	<b>Introduction</b>	<b>3</b>
<b>III</b>	<b>Goals</b>	<b>4</b>
<b>IV</b>	<b>General instructions</b>	<b>5</b>
<b>V</b>	<b>Mandatory part</b>	<b>6</b>
<b>VI</b>	<b>Bonus part</b>	<b>7</b>
<b>VII</b>	<b>Turn-in and peer-evaluation</b>	<b>8</b>

# Chapter I

## Foreword

Yes, no, maybe  
I don't know  
Can you repeat the question?  
You're not the boss of me now  
You're not the boss of me now  
You're not the boss of me now, and you're not so big  
You're not the boss of me now  
You're not the boss of me now  
You're not the boss of me now, and you're not so big  
You're not the boss of me now, and you're not so big Life is unfair, so i just stare at the  
stain on the wall where  
The tv'd been, but ever since we've moved in it's been empty  
Why i, why i'm in this room  
There is no point explaining  
You're not the boss of me now, and you're not so big  
You're not the boss of me now  
You're not the boss of me now  
You're not the boss of me now, and you're not so big  
Malcolm in the middle, and i confess  
I like this mess i've made so far  
Grade on a curve and you'll observe  
I'm right below the horizon  
Yes,...

This subject has nothing to do with Malcolm in the middle, but rather with Man in  
the middle!

# Chapter II

## Introduction

In this first project of network security, you will implement the Address Resolution Protocol spoofing/poisoning method, which is one of the most basic Man In The Middle attacks using a vulnerability present in the ARP protocol.

# Chapter III

## Goals

In this first project aimed at introducing you to network security, you will discover in detail what is the Address Resolution Protocol, that you may have seen during your days of piscine as ARP, and how it works. You will find that this implementation has several vulnerabilities and while protections and alternatives to arp might exist, it remains widely used and is unsafe and unprotected in most cases.



You should really start by reading the RFC 826 and 7042

# Chapter IV

## General instructions

- This project will be corrected by humans only. You're allowed to organise and name your files as you see fit, but you must follow the following rules
- You must use C and submit a Makefile
- You are allowed to use one global variable within your project.
- Your Makefile must compile the project and must contain the usual rules. It must recompile and re-link the program only if necessary.
- You have to handle errors carefully. In no way can your program quit in an unexpected manner (Segmentation fault, bus error, double free, etc).
- Within the mandatory part, you are allowed to use the following functions:
  - sendto, recvfrom
  - socket, setsockopt
  - getuid, close, signal
  - inet\_addr, gethostbyname, getifaddrs, freeifaddrs
  - htons, ntohs
  - printf and its family.
  - Your libft functions.
  - You are allowed to use other functions to complete the bonus part as long as their use is justified during your defense. Be smart.

# Chapter V

## Mandatory part

Your program must take the following four arguments:

source ip

source mac address

target ip

target mac address

Those parameters must always be given in that order.

Example usage:

```
$/ft_malcolm 10.11.254.254 aa:bb:cc:dd:ee:ff 10.11.12.18 42:42:42:42:42:42
```

You must only manage a simple IPv4 address for the mandatory part.

If the arguments provided do not follow that rule or are invalid, your program should exit and output some information.

How precise the information is will be up to you, but you are encouraged to provide details on the errors.

For this project, you will have to send an ARP reply containing the source ip and the mac you want to tell it belongs to to spoof the arp table of the target.

When run, your program will have to wait for an ARP request before sending a single ARP reply and exit.

If everything went well, the arp table on the target should contain the associated ip and mac you provided as source.



You are only allowed to spoof IPs that belong to you, such as your VM. Spoofing other IPs might result in problems and/or sanctions.

Your program should be able to exit when the user inputs Ctrl+C

# Chapter VI

## Bonus part



We will look at your bonuses if and only if your mandatory part is EXCELLENT. This means that you must complete the mandatory part, beginning to end, and your error management must be flawless, even in cases of twisted or bad usage. If that's not the case, your bonuses will be totally IGNORED.

Find below a few ideas of interesting bonuses:

- IPv6 management.
- Decimal notation for IPv4 addresses
- Verbose mode to print packet information
- Any other bonuses that provide extra functionalities to your program



# Chapter VII

## Turn-in and peer-evaluation

- Submit your work on your GiT repository as usual. Only the work on your repository will be graded.
- You have to be in a VM with a Linux kernel  $> 3.14$ . Note that grading was designed on a Debian 7.0 stable.