



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.

Version: 2.2

Contents

I	Foreword	2
II	Introduction	3
III	Goals	4
IV	General guidelines	5
V	Mandatory part	7
VI	Bonus part	9
VII	Submission and peer-evaluation	10

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,...

I figured you like Malcolm in the middle, but this project has actually nothing to do
with that.

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. This attack is possible using a vulnerability present in the the way the ARP protocol works and interacts in a network.

Chapter III

Goals

In this project aimed at introducing you to network security, you will discover in details 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.

The ARP protocol lies within the second layer of the complex but wonderful OSI model.



You should really start by reading the RFC 826 and 7042

Chapter IV

General guidelines

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:

- The whole project has to be done in a **virtual machine**.
- 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.
- 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.
 - inet_pton, inet_ntop.
 - if_nametoindex, sleep.
 - getuid, close.
 - sigaction, signal.
 - inet_addr.
 - gethostbyname.
 - getaddrinfo, freeaddrinfo.
 - getifaddrs, freeifaddrs.
 - htons, ntohs.
 - strerror / gai_strerror.
 - 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

- The executable must be named `ft_malcolm`.
- You must only manage a simple IPv4 address for the mandatory part.
- Your program should be able to exit when the user inputs `Ctrl+C`.
- 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.

When started, your program will have to wait for an ARP request sent on the broadcast by the target, requesting the source IP, before sending a single ARP reply to the target and exit. If everything went well, the arp table on the target should contain the associated ip and mac you provided as source.

Here is an example with a basic usage:

```
foo@debian:~/projetsecu42_1/sources$ sudo ./ft_malcolm 10.12.255.255 ff:bb:ff:ff:ee:ff 10.12.10.22 10:dd:b1:**:**  
Found available interface: eth0  
An ARP request has been broadcast.  
    mac address of request: 10:dd:**:**:**  
    IP address of request: 10:12:12:07  
Now sending an ARP reply to the target address with spoofed source, please wait...  
Sent an ARP reply packet, you may now check the arp table on the target.  
Exiting program...
```

In that example, the program sends an ARP Reply packet to the target (10.12.10.22) containing information on the source (10.12.255.255 and it's associated (spoofed) mac address) right after detecting that an ARP request has been sent over the network.

Example error handling:

```
foo@debian:~/projetsecu42_1/sources$ sudo ./ft_malcolm 10.11.11.11 aa:bb:cc:dd:ee:ff 10.11.11.1111 aa:bb:cc:dd:ee:ff  
ft_malcolm: unknown host or invalid IP address: (10.11.11.1111).
```

```
foo@debian:~/projetsecu42_1/sources$ sudo ./ft_malcolm 10.11.11.11 aa:bb:cc:dd:ee:ff 10.11.11.11 aaa:bb:cc:dd:ee:ff  
ft_malcolm: invalid mac address: (aaa:bb:cc:dd:ee:ff)
```



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.

Chapter VI

Bonus part

Find below a few ideas of interesting bonuses:

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



The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter VII

Submission and peer-evaluation

Turn in your assignment in your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Don't hesitate to double check the names of your folders and files to ensure they are correct.

You have to be in a VM with a Linux kernel > 3.14 . Note that grading was designed on a Debian 7.0 stable.