Using Scapy for Man-in-the-Middle Attacks

Ana Rita Martinho
Department of Electrical and Computer Engineering
Faculty of Engineering of University of Porto
up201709727@fe.up.pt

Gonçalo Xavier
Department of Electrical and Computer Engineering
Faculty of Engineering of University of Porto
up201604506@fe.up.pt

Abstract—A Man-in-the-Middle(MITM) attack is a type of cyberattack where an attacker secretly relays and possibility alters the communication between 2 unsuspecting parties. Most recent cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks.

The goal of this project is to demonstrate, using scapy, why such measurements are needed. Scapy is a python module that enables a user to send, sniff and forge network packets, as such it provides easy methods to the types of functionalities needed to run a MITM attack.

4 different protocols were analyzed (FTP, SNMP, Telnet and SMTP).

I. INTRODUCTION

Here you should provide the context of this work and describe the problem you are solving.

II. RELATED WORK

You should identify and analyze related work here.

III. SOLUTION

Here you should describe the solution.

IV. EVALUATION

The evaluation results go here.

V. CONCLUSION

The conclusion goes here.

REFERENCES

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.