

Presentation of the master's thesis by explaining the generally recognized steps of scientific research followed to prepare this thesis.

Prepared by

ALI MMADI, PhD student - Midocean University





Research Skills (2)

Task 1

ALI MMADI

PhD student - Midocean University

www.midocean.ae

INTRODUCTION

Hello, my name is **Ali Mmadi**, an engineer and researcher in networks and **cybersecurity**. Today, as part of the Research Skills 2 course, I am going to present my Master's thesis entitled: "**Mastering the Securing of VoIP and Network Services under Linux.**" This work was carried out at the Higher Institute IS-IESI of Madagascar, under the supervision of **Doctor Zoaritsihoarana Fitiavana Avo Tongalafatra**.

In this presentation, I will explain how I applied the main steps of scientific research to design, carry out, and validate this project.



Step 1: Identifying the problem and formulating the research question

I started with a concrete observation: in companies, particularly those that use **VoIP** for their internal communications, there are often **serious security flaws**. These vulnerabilities can lead to **eavesdropping, denial-of-service attacks, or even intrusions into servers**.

My main issue was therefore the following: "How can we control and secure Voice over IP and network services in a Linux environment to ensure the confidentiality and integrity of communications?"

Literature review and state of the art

In the second step, I conducted a literature review . I consulted several academic and technical resources on:

- ☐ **VoIP transport protocols (RTP, RTCP, SIP, H323);**
- ☐ **Possible types of attacks such as sniffing, spoofing, or SPIT;**
- ☐ **VoIP security standards such as SRTP and TLS;**
- ☐ **And finally, open-source tools used for security like Snort and Fail2ban.**

This analysis allowed me to define the theoretical framework and situate my research within the context of network cybersecurity.

Step 3: Formulation of objectives and hypotheses

After identifying the problem and reviewing existing work, I formulated two main objectives:

- 1) **“Implement a functional and secure VoIP solution based on Asterisk on Linux”.**
- 2) **“Test and demonstrate common attacks to propose effective countermeasures”.**

My research hypothesis was that using a **stable and well-configured Linux system**, with integrated security tools, would help **strengthen the protection of VoIP communications**.

Research methodology

For the methodology, I adopted an **experimental and demonstrative approach**.

- **I first installed and configured a Debian 12 server, chosen for its stability and security.**
- **Then, I installed Asterisk, the open-source IP telephony software, and configured several softphones (X-Lite, 3CXPhone, Ekiga).**
- **Next, I set up SSH and FTP services for secure connections and transfers. Afterwards,**
I simulated different types of attacks:
 - **Eavesdropping attack,**
 - **Man-In-The-Middle attack,**
 - **DoS (Denial of Service) attack,**
 - **And brute-force attacks on SIP passwords.**

Finally, I applied countermeasures: iptables firewall, SRTP encryption, monitoring with Snort, and automatic detection with Fail2ban.

Results and analysis

The results obtained confirmed my hypotheses. After implementing the countermeasures, the tests showed a significant **reduction in vulnerabilities**:

- **Communications were encrypted and could not be deciphered by sniffing.**
- **DoS attacks were blocked by the firewall and Fail2ban.**
- **And real-time monitoring with Snort allowed for the detection of any suspicious activity.**

The VoIP system thus operated in a **secure, stable, and reliable manner**, even under heavy loads.

Discussion and limitations of the research

This study allowed me to better understand the relationship between **network security, communication protocols**, and operating systems. The main limitations were related to the **experimentation time** and the absence of a real **corporate environment**.

For future work, I recommend extending the research to **secure videoconferencing** and the integration of **Cloud VoIP** solutions with **multi-factor authentication**.

Conclusion and scientific contribution

In conclusion, this thesis made it possible **to design and validate a complete** VoIP security solution on Linux. This project strengthened my skills in:

- ✓ **system and network security,**
- ✓ **threat analysis,**
- ✓ **configuration of Asterisk and open-source tools.**

On the scientific level, I applied all the recognized **steps of the research process:**

observation, problem formulation, hypothesis, experimentation, validation, and conclusion.

Thank you for your attention.

Bibliographic reference

- 1) Ali Mmadi. (2019-2020). Mastery of VoIP security and network services under Linux. Final year thesis, IS-IESI Madagascar, supervised by Dr. Zoaritsihoarana Fitiavana Avo Tongalafatra.
- 2) **Keller, J., & Wright, R. (2020).** *VoIP Security: Protecting Your Asterisk PBX and SIP Networks*. Packt Publishing.
- 3) **Rosenberg, J., Schulzrinne, H., Camarillo, G. et al. (2002).** *SIP: Session Initiation Protocol (RFC 3261)*.
- 4) Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th Edition)...



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

