GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

University of Polytechnic

(Greater Noida, Uttar Pradesh)

Final Project (DPCS9999) Report on VOIP HACKING LAB

By

AAMIR RIZWAN

(Admission NO: 19GPTC4060002)

In partial fulfilment of requirements for the award of the degree

Diploma in Computer Science & Engineering

(Under the guidance of Er. Nutan Gussain)

GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that Aamir Rizwan (19GPTC4060002) student of Diploma in Computer Science & Engineering, 6th Semester, Department of Computer Science of Galgotias University, has pursued the Major Project titled "VOIP HACKING LAB" under the supervision of Assistance Professor Er. Nutan Gussain and their report has been submitted in partial fulfilment of requirements for the award of the degree, Diploma in Computer Science & Engineering by Galgotias University in the Year2021.

Er. Nutan Gussain

(Assistance Professor)

Acknowledgment

I express my sincere regard and indebtedness to my project internal guide and Er. Nutan Gussain, for his valuable time, guidance, encouragement, support and cooperation throughout the duration of our project. I would sincerely like to thank IT Department for giving me the opportunity to work on enhancing my technical skills while undergoing this project. This project was done under the guidance Er. Nutan Gussain. This project helped in understanding the various parameters which are involved in the development of a VOIP HACKING LAB and the working and integration frontend along with the backend to create a fully functional VOIP Hacking Lab .

I would like to thank Er. Nutan Gussain (Assistance Professor) and whole of department for their constant support.

AAMIR RIZWAN
Admission no : 19GPTC4060002
Enrollment No : 19014060002

Abstract

The main objective of the VOIP HACKING LAB is to Learn how to listen a live call from another device. For monitoring the call this can help police force to monitor criminals as well as this can use for teaching in university for networking topic and forensic. This lab can help to check network security and end point security.

INDEX

Chapter 1: Introduction

Introduction:

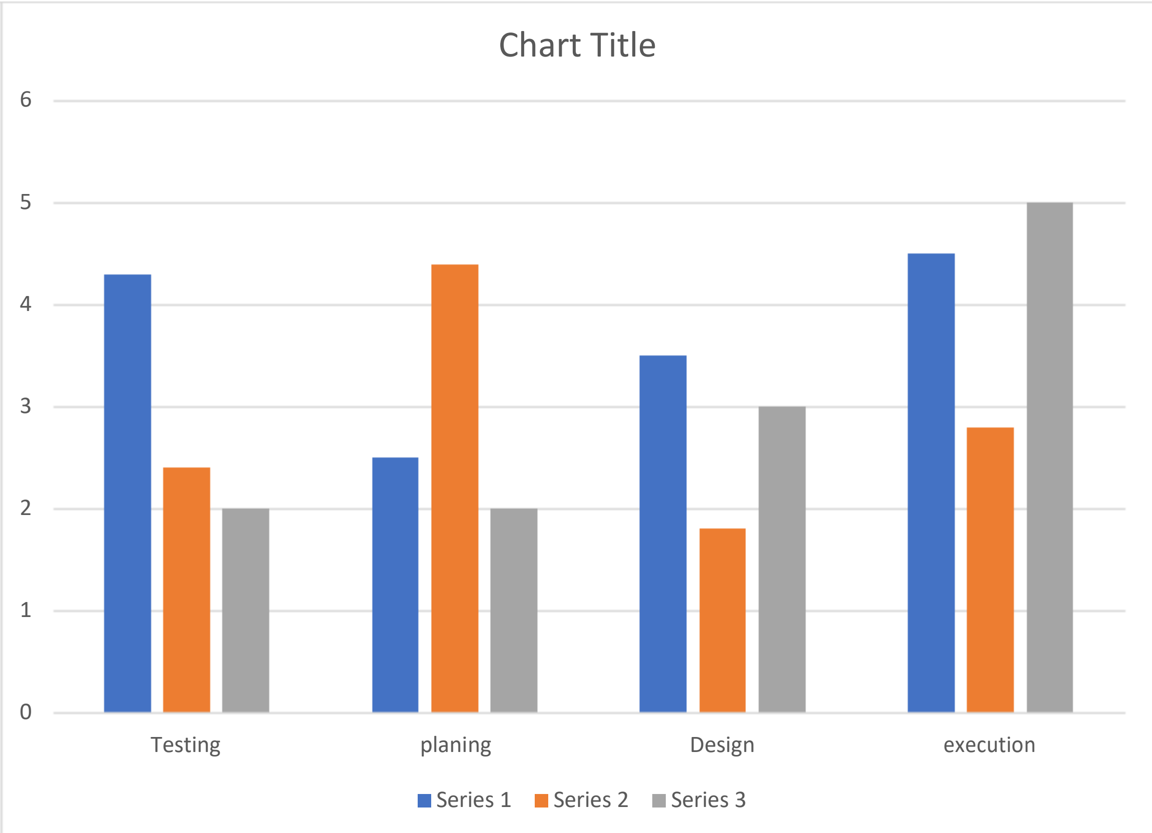
We are going to learn how to setup VoIP server in the Vmware, For that I'm going to use trixbox 2.8.0.4 ISO image. **Trixbox** is one of the most popular Asterisk-based distribution. Trixbox CE includes CentOS Linux, MySQL, and all the tools needed to run a business quality phone system. It give us GUI interface to make configuration and to operate easy. It allow the user to to setup a voice over IP phone system and other necessary application.

We need 3 device 1) trixbox 2) windows caller 3) android receiver.

Aim:

Our proposed "AN VOIP HACKING LAB" are built for the act of Monitoring the live call over the internet. Creating records of everything user speak on a call. These are used to quietly monitor user call activity while user use there normal call . this lab are used for legitimate purposes like f monitoring the user call by police force but can be misused by cyber criminals to steal user data.

Project Work Schedule:



The planning phase is quite easy because there are several certified, tested and managed by big multinational's antivirus software are out there, so basic understanding about how they made are quite easy to find..

The most difficult is the setting a virtual env for the program to run.

<u>Organisation of Report</u>:

INTRODUCTION

This section includes the overall view of the project i.e. the basic problem definition and the general overview of the problem which describes the problem in layman terms. it also specifies the software used and the proposed solution strategy.

SOFTWARE REQUIREMENTS SPECIFICATION

This section includes the Software and hardware requirements for the smooth running of the application.

DESIGN & PLANNING

This section consists of the Software Development Life Cycle model.it also contains technical diagrams like the Data Flow Diagram and the Entity Relationship diagram.

IMPLEMENTATION DETAILS

This section describes the different technologies used for the entire development process of the Front-end as well as the Back-end development of the application.

RESULTS AND DISCUSSION

This section has screenshot so fall the implementation i.e. user interface and their description.

SUMMARY AND CONCLUSION

This section has screenshots of all the implementation i.e. user interface and their description.

Question arises why Trixbox?

TrixBox is a telephone system based on the popular open source Asterisk PBX (Private Branch eXchange) Software. TrixBox allows an individual or organization to setup a telephone system with traditional telephone networks as well as Internet based telephony or VoIP (Voice over Internet Protocol).

trixbox is an open telephony platform utilizing the best of the open source telephony tools into one easy-to-install package. Based on an enhanced LAAMP (Linux, Apache, Asterisk, mySQL, PHP) the trixbox dashboard provides easy to use web-based interfaces to setup, manage, maintain, and support an complete IP PBX system.

Chapter 2: Requirements

Hardware Requirements:

- Pc with a 500GB or more space free for user.
- Pc with 4GB of RAM.
- Pentium 4 or higher.
- 1 caller phone
- 1 receiver phone / windows
- 1 attacker pc / windows
-

Software Requirements:

- OS (supported os are: windows, linux, Debian, fedora, mint, arch linux)
- Wireshark
- Zoiper

Chapter 3: Design & Planning

GETTING STARTED

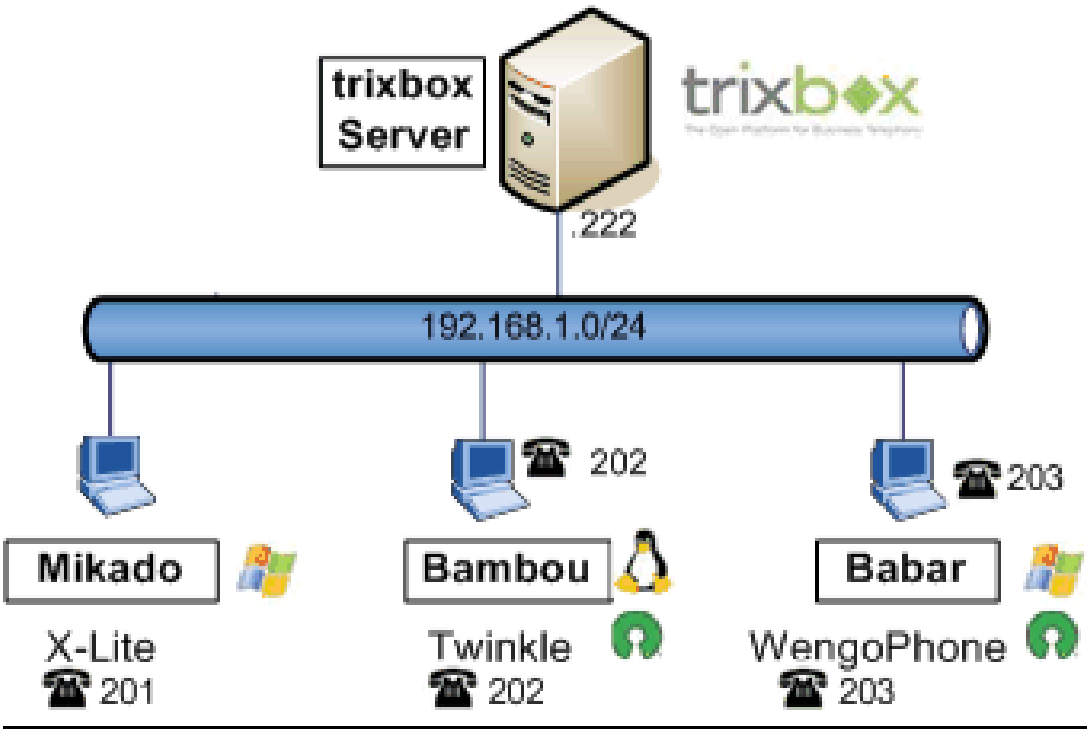
Install VMware for virtual setup of lab.

After installing VMware set up the virtual machine . install windows 7 os or another operating system.

Install trixbox in VMware machine set up the network mode as windows 7 machine (bridge connection)

Now install android machine in VMware set up the network connection in bridge connection.

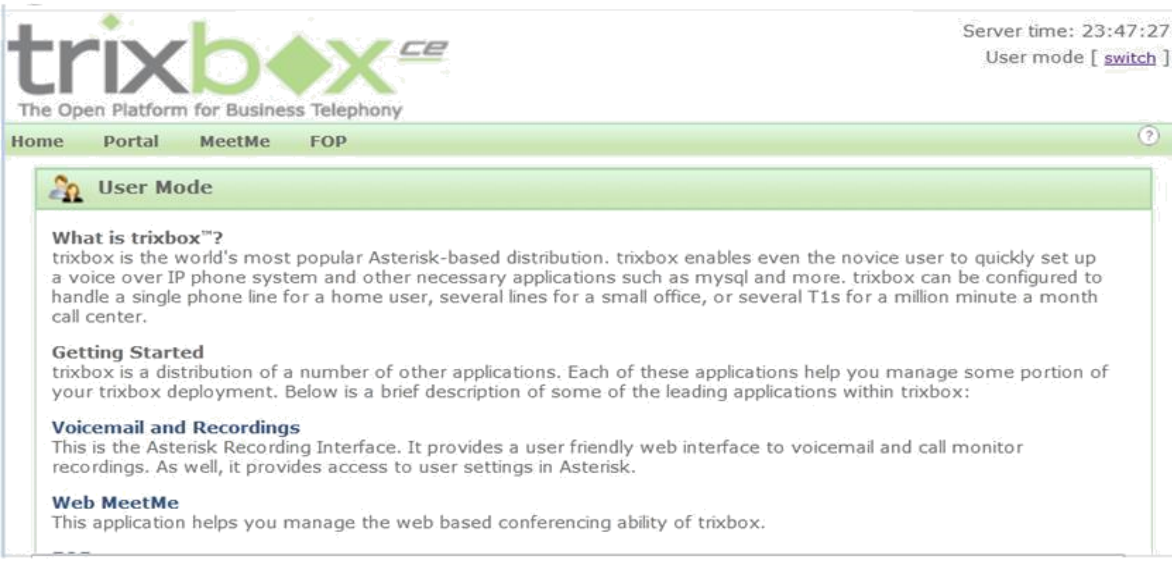
Architecture:



Chapter 4: Implementation

implementation:

After installing the trixbox in vmware we need to configure the trixbox.



Now we need to create the user account by assigning the extension number for that we need to switch the user mode to admin mode by click the top right corner.

when we click on switch for admin mode we need to enter the credential the by default credential is **username-maint** and **pass- password** enter credential to get into the admin mode. when you login the admin mode a dialogue box will popup for registration we don't need to register just close it.This is the trixbox admin interface. now click on now click on **PBX option** and select **PBX setting** option from the menu.

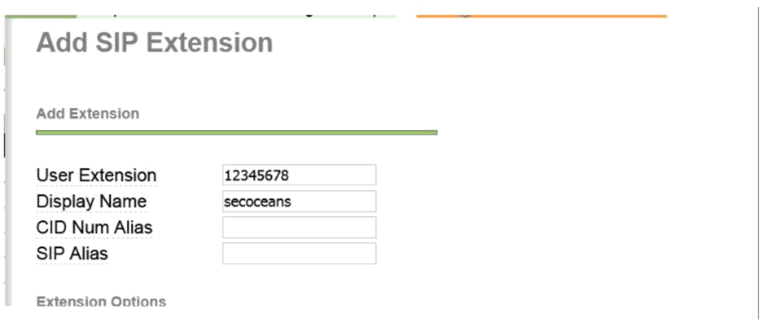
Now click on extension that highlighted in below image

now we need to create the extension inside the server select device **generic SIP device** and click on submit.

After device setup add the extension

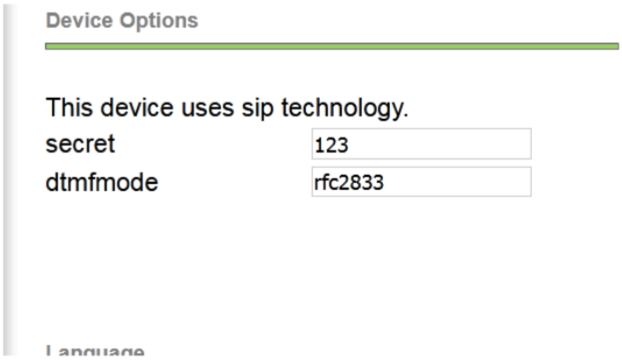
user extension: any 7-8 digit number (later on we will use as a phone number to make a call)

Display Name: any user name we can give

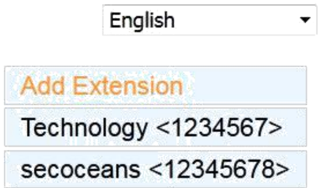


Add the Device option

secret 123 and dtmfmode: default (rfc2833) Click on submit.



Same as add one more extension, we can add multiple extension we this time we need only two extension.

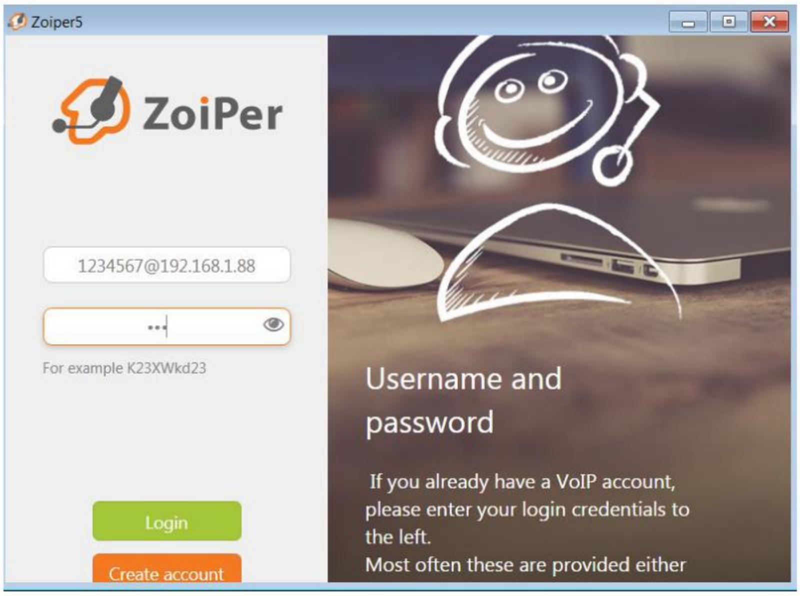


We add the extension for caller and receiver one is Secoceans and 2nd is Technology with number. Now we need to save the configuration for that click on yellow option **apply configuration changes**. again it will show a yellow popup click on **Continue with reload**. Extension is successfully added.

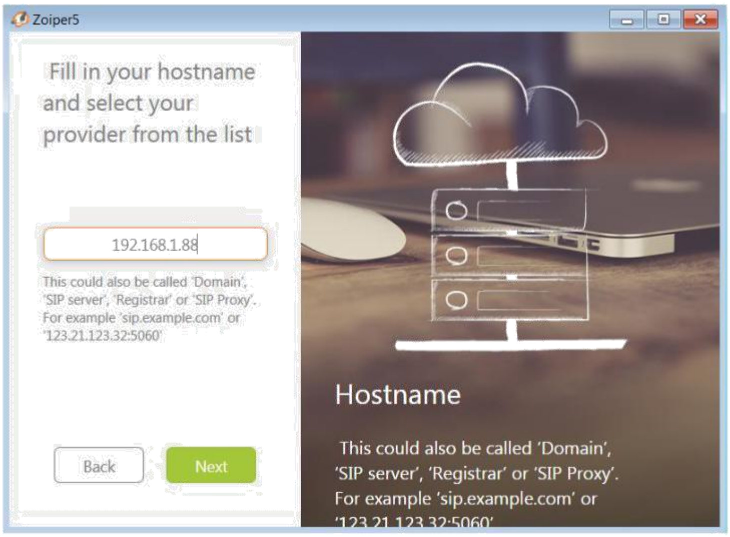
Now download the **ZOIPER** application for making and receiving call.

One it installed it will show a popup click on free account then next after that enter the credential:

extension number@server ip **1234567@192.168.1.88** and password 123 click on login.



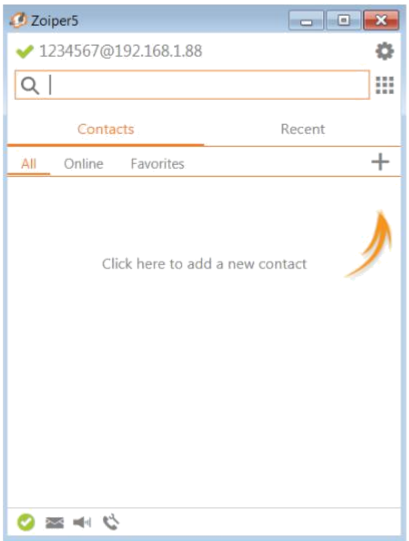
It will detect the server IP automatic click on next.



Skip the Authentication and outbound proxy

Account 1: **Username: Technology Phone number 1234567 password 123**

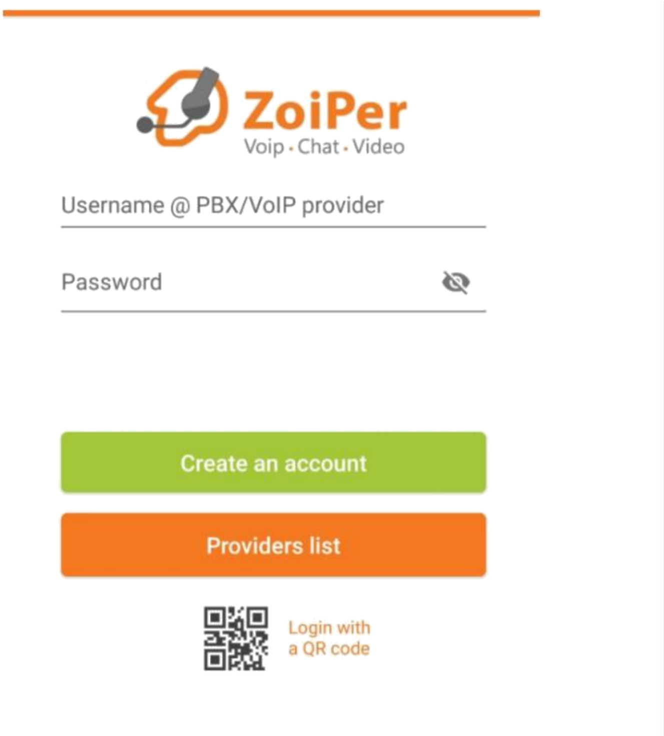
Now Zoiper is ready to make or receive call in the system



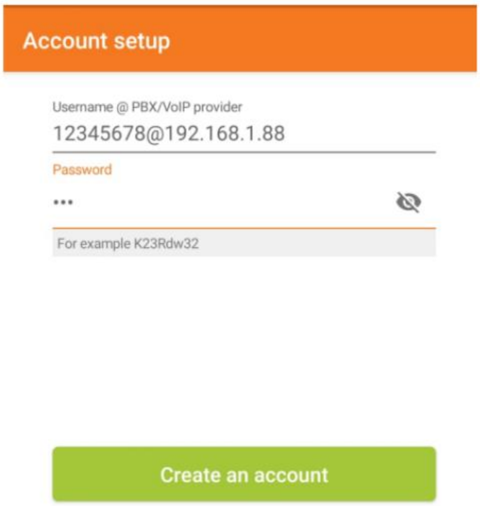
Install zoiper in the phone and configure it as we configured in the system.

Use Account 2: Username: Secoceans phone number: 12345678 password:123

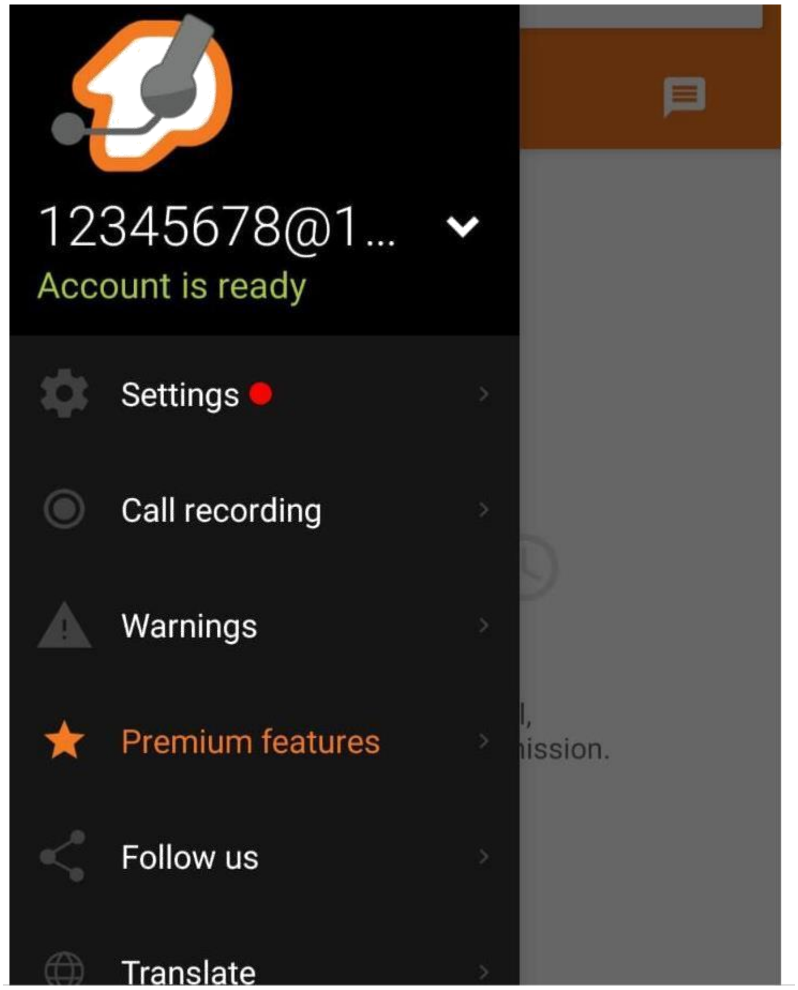
Enter **12345678@192.168.1.88 Pass- 123**



Enter the user number and IP and click on create account



Zoiper is ready to use for make and receive call.

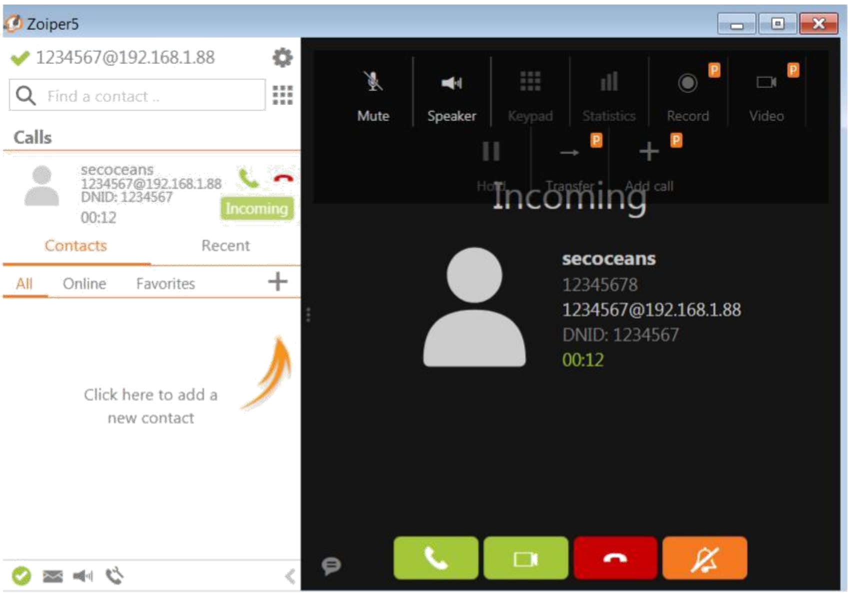


Both Zoiper account is ready to use.

Lets make call from account technology 12345678 –> secoceans 1234567

calling from account 1 Technology 12345678 (from android phone) –> account 2 secoceans.

secoceans is geting an incoming call on the system as shown in the given image. Click on an answer for accepting a call from **technology**.



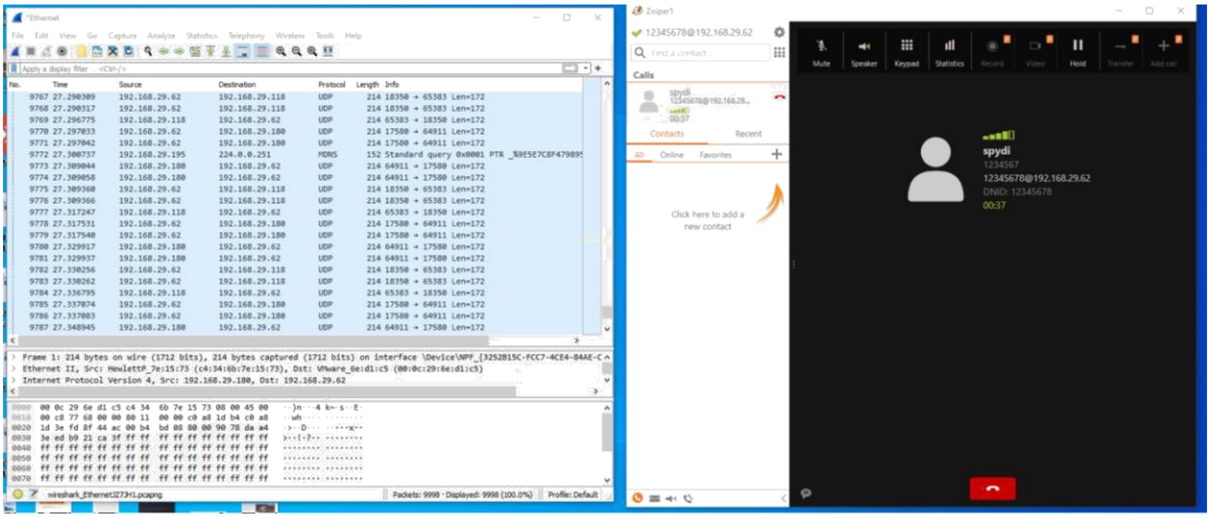
We configured the VoIP server on the local network , now we can make voice call, video call , or chat over the VoIP call.

Chapter 5: Testing

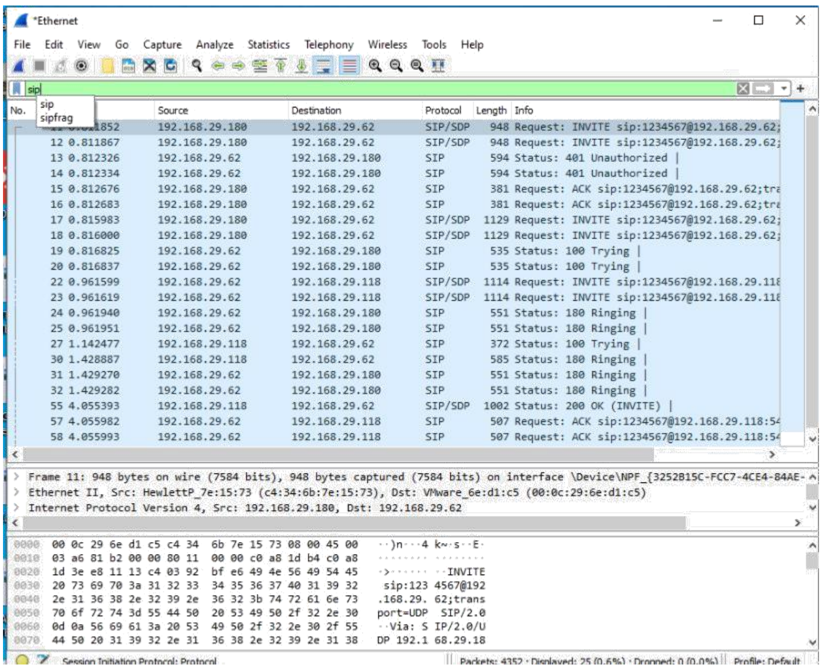
HACKING VoIP

Now we have to hack the VoIP call using Wireshark. Attacker have to inside the caller or receiver network . and connected to the victim network and start monitor network traffic using Wireshark.

Now start **wireshark** when 2 victim are on call and capture the data sip rtp packets.

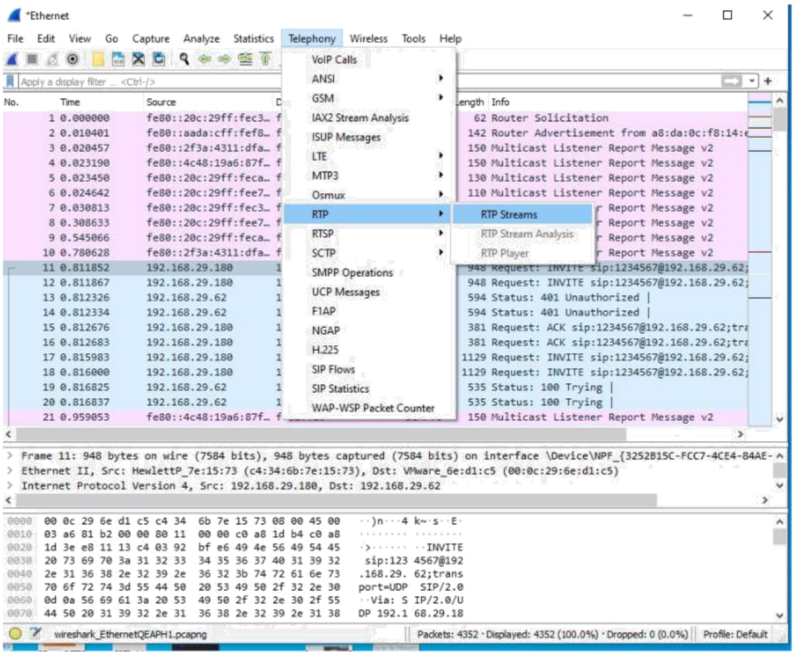


Search for sip rtp packets !

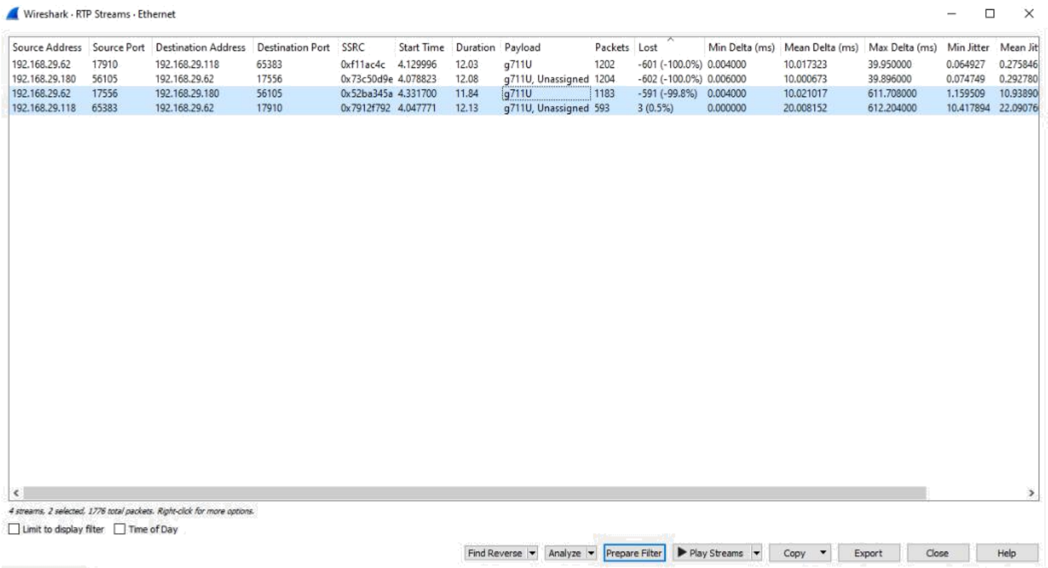


Here we can se lots of packets of sip that’s confirm this is voip call packets. Now go to

Telephony select RTP AND THEN select RTP stream



Now select which packet you want listen. And click on play streams



Now RTP player pop up and start playing the the streams Enjoy……….

VOIP call hacked and attacker listen all the call packets

Chapter 7: Advantages

- Monitoring the activities of a particular person.
- Track call records
- Easy to Maintain Best Practices.
- Faster Access
- Ethical Hacking

As well as serving the interests of law enforcement agents, voip hacking can help police maintain protect valuable bandwidth and ensure optimum use of networked resources by monitoring criminal activity online. Parents can even use them to check their children's call activities.

Chapter 8: Future Vision

Our future vision towards our VOIP hacking lab is to make it available for police / and to university so that it can work for research environment . (want to make it opensource and use it on your own risk) (made for security research and to learn the logging vulnerability in devices.)

Chapter 8: Conclusion

VOIP Hacking Lab is for Research use and it can used by Defense force for the legal purpose. It is very handy setup to set and use anywhere with some resource using virtual environment. It is open source anyone can use there skill and pentest the VOIP Network.

References

Trixbox:

https://sourceforge.net/projects/asteriskathome/

vmwre:

https://www.vmware.com/in.html

Zoiper:

https://www.zoiper.com/