

(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)



(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**
- **Chapter 2: Requirements**
- **Chapter 3: Design & Planning**
- **Chapter 4: Implementation**
- **Chapter 5: Testing**
- **Chapter 6: Results**
- **Chapter 7: Advantages**
- **Chapter 8: Future visions**
- **Chapter 9: Conclusions**

Chapter 1: Introduction

Introduction:

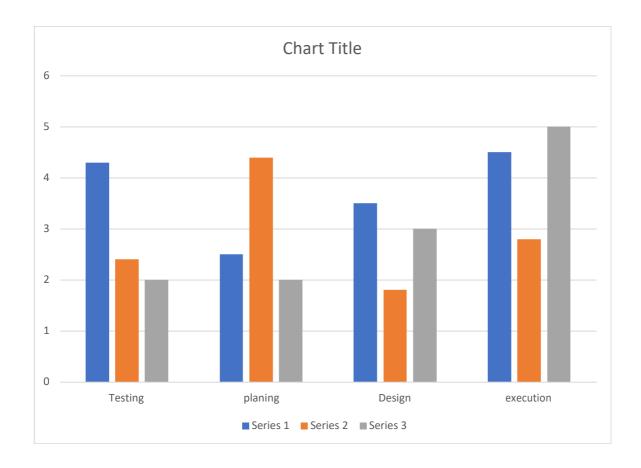
We are going to learn how to setup VoIP server in the Vmware, For that I'm going to use trixbox 2.8.0.4 ISO image. **Trixbox** is one of the most popular Asterisk-based distribution. Trixbox CE includes CentOS Linux, MySQL, and all the tools needed to run a business quality phone system. It give us GUI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

<u>Aim:</u>

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.

Organisation of Report:

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 Backend 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.



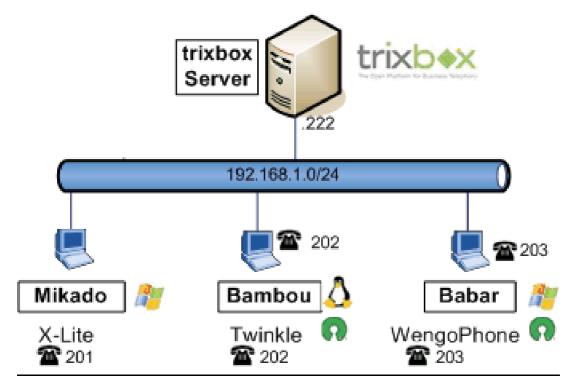
After installing VMware set up the virtual machine . install windows 7 os or another operating system.

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

	Admin Reports Panel Recordings Help
Setup Tools	System Status
Admin System Status	Notices
Module Admin	No email address for online update checks
Basic	show all
Extensions	
Feature Codes	Statistics
General Settings	Total active calls
Outbound Routes	Internal calls
Support	External calls
Trunks	Total active channels
Administrators	Connections
Inbound Call Control	

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

dmin	Reports		Recordings	Help	Apply Conf	guration Change
				Trop		Contract of the strength and
Add	an E	tensio	n			
Please	select vo	our Device	below then	click Subr	nit	
Device						
Device						
Device	Ger	eric SIP Devi	ce 🔻			
Submi	211					
Submi	U					

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 SIP Ext	ension	
Add Extension		
User Extension	12345678	
Display Name	secoceans	
Display Name CID Num Alias	secoceans	

Add the Device option

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

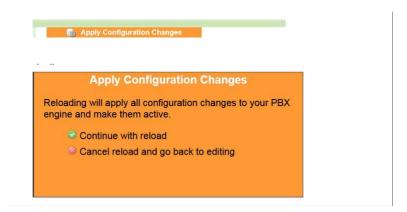
This device use	s sip technology.
secret	123
dtmfmode	rfc2833

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

	English
Add E	xtension
Techr	ology <1234567>
secod	eans <12345678>

.

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

🥖 Zoiper5	
✔ 1234567@192.168.1.88	0
Q	
Contacts	Recent
All Online Favorites	+
Click here to add	a new contact
📀 📾 🛋 🖒	

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

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

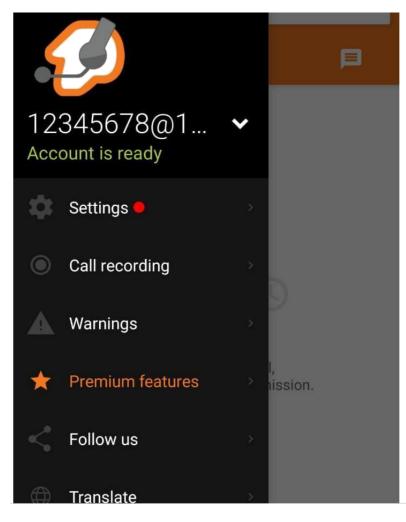
Enter 12345678@192.168.1.88 Pass- 123

Ę	Zoi Voip · Cha	Per t · Video	
Username @ F	PBX/VoIP pro	vider	
Password		k.	R
		and a set	
Cr	eate an acco	unt	
	Providers lis	t	
		with	

Enter the user number and IP and click on create account

Jsername @ PBX/VoIP provider	
12345678@192.168.1.88	
Password	
	Ø
For example K23Rdw32	

Zoiper is ready to use for make and receive call.



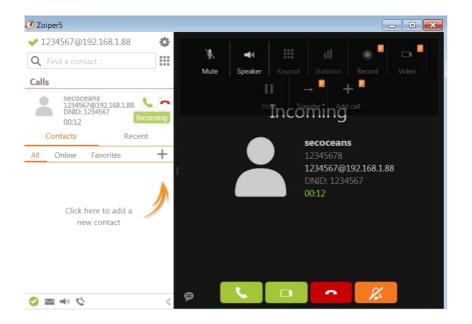
Both Zoiper account is ready to use.

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**.



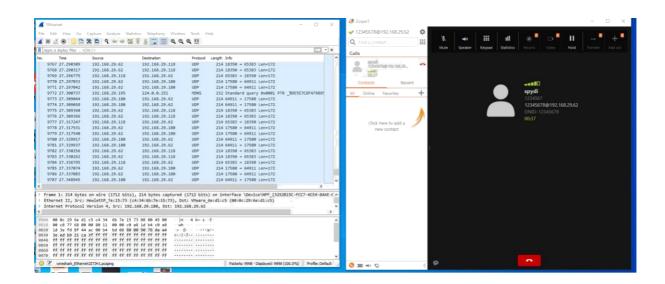
We configured the VoIP server on the local network , now we can make voice call, video call , or chat over the VoIP call.

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 !

	*Ethern																									-	-			×
le	Edit	View	Go	Сар	ture	Ar	nalyz	e	Statis	tics						Tools	He	lp												
	II (2)	۲		×	G	٩	۲	۲	SH I	-	<u></u>			Q,	0,0	2 11														
s	ipl																										Þ	<	-	+
	sip sipfra			5	Sourc	e ·					Desti	nation				Prote	col	Length	In	nfo										
6	sipira	orwald	52	100	192.	168.	29.	180		0	192.	168.	29.	62		SIP	SDP	948	Re	equest	: I	NVITE	sip:	1234	5670	192.	168.	29.62		
		0.8118		1	192.	168.	29.	180			192.	168.	29.	62		SIP.	SDP	948	R	equest	: 1	NVITE	sip:	1234	567@	192.	168.	29.62		
	13	0.8123	26	1	192.	168.	29.	62			192.	168.	29.	180		SIP		594	St	tatus:	40	1 Unau	thor	ized	11					
	14	0.8123	34	3	192.	168.	29.	62			192.	168.	29.	180		SIP		594	S	tatus:	40	1 Unau	thor	ized	11					
	15	0.8126	76	3	192.	168.	29.	180			192.	168.	29.	62		SIP		381	Re	equest	:: A	CK sip	:123	456	@192	.168	.29.	62;tr	5	
	16	0.8126	83	1	192.	168.	29.	180			192.	168.	29.	62		SIP		381	Re	equest	:: A	CK sip	:123	4567	@192	.168	.29.	62;tr	2	
	17	0.8159	83	- 3	192.	168.	29.	180			192.	168.	29.	62		SIP	SDP	1129	R	equest	: I	NVITE	sip:	1234	567@	192.	168.	29.62		
	18	0.8160	00	3	192.	168.	29.	180			192.	168.	29.	62		SIP,	SDP	1129	Re	equest	: I	NVITE	sip:	1234	567@	192.	168.	29.62	1	
	19	0.8168	25	1	192.	168.	29.	62			192.	168.	29.	180		SIP		535	5	tatus:	10	0 Tryi	ng							
	20	0.8168	37	1	192.	168.	29.	62			192.	168.	29.	180		SIP		535	5	tatus:	10	0 Tryi	ng							
	22	0.9615	99	3	192.	168.	29.	62			192.	168.	29.	118		SIP	SDP	1114	Re	equest	: I	NVITE	sip:	1234	567@	192.	168.	29.11	3.	
	23	0.9616	19	4	192.	168.	29.	62			192.	168.	29.	118		SIP,	SDP	1114	Re	equest	: 1	NVITE	sip:	1234	567@	192.	168.	29.11	3.	
	24	0.9619	40	1	192.	168.	29.	62			192.	168.	29.	180		SIP		551	S	tatus:	18	0 Ring	ing	1						
	25	0.9619	51	1	192.	168.	29.	62			192.	168.	29.	180		SIP		551	. 51	tatus:	18	0 Ring	ging	Ê.						
	27	1.1424	77	1	192.	168.	29.	118			192.	168.	29.	62		SIP		372	S	tatus:	10	0 Tryi	ng							
	30	1.4288	87	1	192.	168.	29.	118			192.	168.	29.	62		SIP		585	S	tatus:	18	0 Ring	ing	1						
	31	1.4292	70	1	192.	168.	29.	62			192.	168.	29.	180		SIP		551	St	tatus:	18	0 Ring	ing	1						
	32	1.4292	82	1	192.	168.	29.	62			192.	168.	29.	180		SIP		551	. 51	tatus:	18	0 Ring	ing	1						
	55	4.0553	93	1	192.	168.	29.	118			192.	168.	29.	62		SIP.	SDP	1002	St	tatus:	20	O OK (INVI	TE)	1					
	57	4.0559	82	1	192.	168.	29.	62			192.	168.	29.	118		SIP		507	Re	equest	: A	CK sip	:123	456	@192	.168	.29.	118:5	4	
	58	4.0559	93	1	192.	168.	29.	62			192.	168.	29.	118		SIP		507	R	equest	: A	CK sip	:123	4567	@192	.168	. 29.	118:5	4	
																								1	(Mictor)			,		
E		et II,	Src:	Hew	let	tP_7	e:1	5:7	3 (c	4:34	1:6b	:7e:	15:	73),	Dst:	VNwa	re_6					Device 9:6e:d			5281	SC-F	CC7-+	4CE4-		E
30		Øc 29							15 7							·4 k~	· s · · 8	E -												
1		a6 81																												
12		3e e8 73 69														22.45														
93 94		73 69														23 45 9, 62														
35		6f 72														DP 5														
36		0a 56														SIP														
37		50 20														.1 68														
-	1000.0		nitiation		mari	Meserve	2121										i i norma	kets: 4									78			7

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

	l 🧷		/ filte		-64/7,5	xi-/:	and the second second	٩	۲	8		1			Vol AN	P Ca ISI	lls														•	+
Ko.	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Time 0.00	20000 2049 22319 22349 22349 22349 22349 22349 2049 2049 2049 2049 2049 2049 2049 20	90 31 57 90 90 42 13 356 28 26 34 76 33 390 25 37		S ff	ourc e86 e86 e86 e86 e86 e86 e86 e86 e86 e86	1112 1112	0c:: ada f3a c48 0c:: 0c:: f3a .29 .29 .29 .29 .29 .29 .29 .29 .29 .29	cf1 :43: :19a 29f1 29f1 29f1 29f1 29f1 29f1 29f1 29f1	<pre>:fe :fe :fe :fe :fe :fe :fe :fe :fe :fe</pre>	:f8 Ifa :ca :ca :c3 :c3 :ca Ifa	f f f f f f f f		ISL LTE MT Os RTS SC SN UC FU NG H.J SIP	(2 Str IP Me IP3 mux SP TP IPP C SP Me AP SAP S225 Flow Stati	essage Operati essage vs istics	ions		•	1 1 1 1 1 1 1 1 1 1 1 1 1 5 5	y Info 62 Route 42 Route 50 Multi 50 Multi 30 Multi 10 Multi RTP Stree RTP Play 48 Reque 94 Statu 81 Reque 81 Reque 29 Reque 35 Statu 35 Statu	er Ad cast cast cast cast am Ar er est: est: est: est: est: est: est: est:	verti List List List List Invii Invii Invii 01 Un ACK s ACK s INVII INVII INVII INVII 00 Tr 00 Tr	semer ener ener si E si auth ip:1 E si E si ying ying	nt fro Repor Repor Repor Repor Repor P:1234 p:1234 p:1234 p:1234 p:1234	-t M M M M M M M M M M M M M M M M M M M	essa essa essa essa essa essa 0192 0.160 0.192 0.192	ge v2 ge v2 ge v2 ge v2 ge v2 ge v2 ge v2 ge v2 ge v2 ge v2 se se s	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
> Et	hern	et 1	I,	Src	: 1	lew	let	tP_	7e:1	5:7	3 (c4:	34:	6b :	7e:	15:7	3), 1		///wa	re_6e		n interf 1:c5 (00					528:	L5C-1	CC7-	4CE4-		
0000 0010 0020 0030 0040 0050 0050 0050	03 1d 20 2e 70	0c a6 3e 73 31 6f 0a	81 e8 69 36 72	b2 11 70 38 74	00 13 3a 2e 3d	00 c4 31 32 55	80 03 32 39 44	11 92 33 2e 50	00 bf 34 36 20	00 e6 35 32 53	c0 49 36 3b 49	73 a8 4e 37 74 50 32	1d 56 40 72 2f	b4 49 31 61 32	c0 54 39 6e 2e	a8 45 32 73 30	si .16	ip:123 58.29. t=UDP /ia: 5	450 62	NVIT 7@19 tran P/2.	E 2 5 0										,	

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

Source Address	Source Port	Destination Address	Destination Port	SSRC	Start Time	Duration	Payload	Packets	Lost	Min Delta (mc)	Mean Delta (ms)	Max Delta (ms)	Min Jitter	
92.168.29.62	17910	192,168,29,118	65383	0xf11ac4c		12.03	g711U	1202	-601 (-100.0%)		10.017323	39.950000	0.064927	0.27584
92.168.29.02	56105	192.168.29.62	17556	0x73c50d9e		12.03	g711U, Unassigned		-602 (-100.0%)		10.000673	39.896000	0.074749	0.2927
92.168.29.62	17556	192.168.29.180	56105	0x52ba345a		11.84		1183	-591 (-99.8%)		10.021017	611.708000	1.159509	10.938
92.168.29.118	65383	192.168.29.62	17910	0x7912f792		12.13	g711U, Unassigned			0.000000	20.008152	612.204000	10.417894	
	1776 ma/aarkat	. Ryte-cick for more aptions												

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/