SNIFFING VOIP CALLS USING A RASPBERRY PI

Table of Contents

1. Abstract	3
2. Literature Review	4
3. Introduction	5
3.1 VoIP Packets	5
4. Lab Configuration	7
4.1 Asterisk Configuration	8
1.2 Configuring Zoiper Softphone	14
5. Configuring Raspberry pi	17
5.1 Remote Log into Raspberry Pi's Full Operating System Using VNC Connect	24
5.2 Installing Required Packages	25
6. Sniffing VoIP calls using custom script over a Raspberry pi	26
7. Conclusion	31
8. References	32

1. Abstract

Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

Because of the bandwidth efficiency and low costs that VoIP technology can provide, businesses are migrating from traditional copper-wire telephone systems to VoIP systems to reduce their monthly phone costs. In 2008, 80% of all new Private branch exchange (PBX) lines installed internationally were VoIP[1].

The use of Voice Over Internet Protocol (VOIP) calls by criminals, have proved to be a hindrance in its investigations. The first use of VOIP calls was seen during the 26/11 terror attacks of 2008 and, since then, the practice has become alarmingly common among criminals, especially underworld elements who operate from outside the country[2].

This project aims at using the compactness and portability of raspberry pi for intercepting VoIP calls for investigative purposes.

2. Literature Review

As being an old concept, sufficient research is done on VoIP technology, security and forensics. Some of the relevant articles are cited here. Researcher Rakesh Arora have worked on understanding protocols and standards used in VoIP implementation[3] while Sohil Garg have worked on possible attacks on VoIP infrastructure[4]. Solutions have been proposed for the possible attacks vectors[5] by Santi Phithakkitnukoon, Enkh-Amgalan Baatarjav, Ram Dantu. Also efficient research has also been done on the forensic aspects of VoIP[6][7]. However, different researchers worked on enhancing security and forensics practice for VoIP attacks, no researcher has worked on sniffing VoIP call over a portable, robust, compact standalone device like a raspberry pi. This project focuses on the above mentioned untouched aspect in VoIP forensics.

3. Introduction

VoIP known as IP Telephony is the real-time transmission of voice signals to the Internet Protocol (IP) over the public Internet or a private data network. VoIP converts the voice signal from telephone into a digital signal that travels over the Internet. most important advantages of VoIP are that one can make a long distance phone call and bypass the toll charge. This integrated voice/data solution allows large organizations to carry voice applications over their existing data networks. Not only will this technological advancement have an impact on the large traditional telecommunications industry, it will alter the pricing and cost structures of traditional telephony (over a traditional public switched telephone network (PSTN - also known as a legacy networks). IP networks can carry 5 to 10 times the number of voice calls over the same bandwidth. However, through IP networks to transmit voice and other information, VoIP has inherited the security issues of Internet Protocol networks. As by default the Internet Protocol networks are not encrypted, the underlying VoIP calls are made in plain text. Though is a major security flaw, it is also a bone for a forensic expert as he can sniff and intercept the calls.

3.1 VoIP Packets

H.323

The procedures, elements and protocols specified by the H.323 standard that provides multimedia communication across packet-based networks. Multipoint multimedia or Point-to-point communication services is being provided by H.323 system when its four main elements Multipoint.

SIP

SIP (Session initiation protocol) is a communication protocol used for signalling and controlling multimedia communication sessions such as online gaming, instant messaging and various services. It is similar to web protocol HTTP since messages comprises of headers and a message body. SIP generally uses port 5060 as its default protocol for either TCP or UDP. SIP can be interpreted as the authorize protocol for voice, telephony and video over IP (VoIP) services.

Media Gateway Control Protocol

MGCP is a protocol for handling telephony and VoIP gateways from external network call control devices called Call Agents. The MGCP protocol assumes call control devices or Call

Agents, establish with each other to send commands to the they control. Call Agents also connect directly to IP Phones. The Media Gateways or IP Phones are run commands sent by the Call Agents. The figure shows the MGCP elements and call control actions.

RTP

RTP is using for real-time stream data transfer over the network. It allows data transfer to multiple destinations using IP and treated as primary protocol for audio/video transport within IP networks. RTP is used with a signalling protocol that assists in build-up connections across the network. The RTP protocol is useful for audio and video streaming. Two RTP sessions establishes for video streaming and each with different SSRC identifiers out of which one is useful for audio transmission whereas another for video transmission. Also, there is downside of RTP that it neither assures delivery of packets nor Quality of Service.

4. Lab Configuration

For the scope of this research, the following lab scenario is being considered:



Figure 1 Lab Configuration

• Router

TP Link AC750 Wireless Router

Network Address: 192.168.0.1

• VoIP Server (Asterisk)

Network: 192.168.0.100

• Windows 7 Home System

Network Address: 192.168.0.103

Zoiper Softphone 1

• Android 5.1.1 device

Network Address: 192.168.0.102

Zoiper Softphone 2

4.1 Asterisk Configuration

Asterisk is an open source framework for building communications applications. It powers IP PBX systems, VoIP gateways, conference servers and other custom solutions. It is used by small businesses, large businesses, call centre carriers and government agencies, worldwide. Asterisk is free and open source.

Today, there are more than one million Asterisk-based communications systems in use, in more than 170 countries. Asterisk is used by almost the entire Fortune 1000 list of customers. [9]

Asterisk ISO can be downloaded from here .

Setup

Begin with creating a virtual machine 3 GB RAM, 50 GB Hard Disk space and 1 processor CPU.

Later, move inside Settings -> Storage -> Controller: IDE -> Add Asterisk ISO image.

Now, move inside network settings and set the adapter to "Bridge Adapter".

Start the virtual machine, select option specified in screen shot.

Provide password for "Root" account.

Once configuration will be completed, the system will reboot. Once rebooted user will be greeted with following screen.

Here, account username is root. Password is one set in previous setting.

Look for the server IP Address.

Sniffing	VoIP	calls	using	Rasp	berry	рі
----------	------	-------	-------	------	-------	----

Last login: Ind Sep 19 14.57:42 on ttyl								
NOTICE! You have 2 notifications! Please log into the UI to see them! Current Network Configuration								
Interface MAC Address IP Addresses								
eth0 08:00:27:7C:25:B8 192.168.0.101								
Please note most tasks should be handled through the GUI. You can access the GUI by typing one of the above IPs in to your web browser. For support please visit: http://www.freepbx.org/support-and-professional-services								
This machine is not activated. Activating your system ensures that your machine is eligible for support and that it has the ability to install Commercial Modules.								
I If you already have a Deployment ID for this machine, simply run:								
fwconsole sysadmin activate deploymentid								
to assign that Deployment ID to this system. If this system is new, please go to Activation (which is on the System Admin page in the Web UI) and create a new Deployment there.								
[root@freepbx ~]#								

Figure 2 Server IP Address

Inside a web browser, traverse to the asterisk server IP address. User will be prompted to setup user account. Enter the required details.

÷	→ C° û	🛈 🔥 https://1	192.168.0.101/adm				♡ ☆	Jul\		@		🧈 »	
[]	FreePBX Support	ISymphonyV3 Panel	UCP										>
					Initial	Setup							
	Please provide the core s	ettings that will be used to a	administer and updat	e your system									- 1
					Administ	rator User							
	Username		admin										
	Password		•••••										
	Confirm Password		•••••										
					System Notif	cations Email							
	Notifications Email add	Iress	rameshsteve40	@gmail.com									
					System Id	entification							
	System Identifier		VoIP Server										
					System	Updates							
	Automatic Module Upd	lates	Enabled	Email Only	Disabled								
	Automatic Module Secu	arity Updates	Enabled	Email Only									
	Send Security Emails F	or Unsigned Modules	Enabled	Disabled									
	Check for Updates ever	у	Saturday		~	Between 4am and 8am						~	
									-	Se	etup Sy	stem	v

Figure 3 Setting User Account

After completing setup, move inside "FreePBX Administration".



Figure 4 FreePBX Administration

Activate FreePBX.

User must provide an email address.

Select language and time zone and hit submit.

÷	\rightarrow G	ŵ	(i) 🔒 https://19	2.168.0.101/admin	/config.php#			⊌	· ☆	III\ 🗊	۹	o 🔹	' 🧈 »	- ≡
[]	Admin	Applications	Connectivity	Dashboard	Reports	Settings	UCP						Q	\$
	Please	Select the def	fault locales o	of the PBX										
	Based or	your locale yo	ur language an	d timezone ha	ve been pr	re-selected.								
	Sound Pr	ompts Language 🤇	0	English									~	
	System L	anguage 😧		English (United	States)								~	
	Timezon	• •		Asia/Kolkata									~	
	Submit	_ <	ļ											
			0	FreePB	X g™	FreePBX is a regis: Sangoma Teo FreePBX 14.0.10.3 is li Copyright8	tered trademark of hnologies Inc. icensed under the 0 2007-2019	GPL SA	NG	MA				~

Figure 5 Language and Time Zone

In the next step, enable Sangoma Firewall.

Vighnesh Raje (@s3curityg33k)



Figure 6 Setting Smart Firewall

Trust the underlying network.

Select "Yes" for automatically configuring asterisk IP settings.



Figure 7 Automatically configuring IP Settings

User will be presented with a dashboard.

Vighnesh Raje (@s3curityg33k)

← → ♂ ·	ŵ	🛈 🔏 https://	192.168.0.101/admin	/config.php			⊠ ☆		9 📀	💶 🧈 »	- ≡
🔮 Admin	Applications	Connectivity	Dashboard	Reports	Settings	UCP		Appl	y Config	🔯 Q	*
	Sy	vstem Overvi	ew	C			FreePBX Feed	C			
Asterick	Weld FreePB (You can chang Summary	come to Fre X 14.0.10.3 'VoIP e this name in Ac S	ePBX server' ivanced Settings) ysInfo updated 1 seco	onds ago	 Farewell An An Open So Sangoma 7. The BETA Ro Performance Introducing 	drew ource Jou 6 Distro elease o ce Impro the Nev	rmey GA FFreePBX 15 vements in FreePBX VPBXact and FreePBX 1200 Appliances: More Capacity	for a Better Value			
Firewall Co MySQL Fail2Ban System Reg Web Server System Fire	nfiguration gistration r ewall	× × 0 ×	System Alerts No critical issues fo	bund	Why Getting Ch-ch-chang Workplace I Keeping the I Went on V You're Still U	g Traine ges to A Efficienc New W acation Jsing A I	Inside the Asterisk Feed Jon What's in your Data Center is Worthwhile striCon y: How Unified Communications can Help orkforce Engaged with Unified Communications and No One Noticed) Jusiness Communication System at Work?	0			
Mail Queue UCP Daem Xmpp Daer	≘ on mon	*			Asterisk 🔻	10 T	FreePBX Statistics	0			
Collecting	Anonymous Browser	Stats	I SIP ic: 5160	00	Uptime - CPU -						
Seldut bill	is porcior crimingrys	Show New			Memory -						
eth0	Live	e Network U Interface	sage e eth0	2	Network +	Use Cha	rs Online 🔶 Users Offline 🔿 Trunks Online 🌩 T: nnels In Use	runks Offline			Ŷ

Figure 8 Asterisk Dashboard

Let's now add Extensions. Go to Applications -> Extensions.

¢	\rightarrow G	û 🛈 🔒	https:// 192.168.0.101 /admin	/config.php		••	• ⊠ ☆	lii\ 🗊 🛛	9 📀	🛛 💶 🥔 »	≡
0	Admin	Applications Conne	ectivity Dashboard	Reports	Settings	CP				🔯 Q 📢	^ ک
	Asterisk Firewall Co MySQL Fali2Ban System Rej Web Serve System Firr	AMD Settings Announcements Appointment Reminder Broadcast Calendar Calendar Event Groups Call Flow Control Call Recording Callback CallerID Management Conferences Conferences Pro	erview FreePBX VolP Server' in Advanced Settings) Systinfo updated 1 secc System Alerts No critical issues for	C nds ago	Farewell Andrew An Open Source Sangoma 7,60 The BETA Releas Performance Im Introducing the I Why Getting Trai Ch-ch-tanges to Workplace Effici Keeping the Kee I Workplace IIII Shipper Shiper Shipper Shipper Shipper Shipper Shiper Shipper Shipper Shipper	FreePBX Journey tro GA of FreePBX 15 provements in FreePBX New PBXact and FreePBX 1200 A Inside the Ast ined on What's in your Data Cent o AstriCon ency: How Unified Communicatio vWorkforce Engaged with Unifie on (and No One Noticed) A Business Communication Syst	Feed ppliances: More Capacity for terisk Feed ter is Worthwhile ons can Help d Communications ter at Work?	Cra Better Value			
	Mail Queue UCP Daem Xmpp Daer Collecting . Default bin	Directory Extensions Follow Me IVR Languages Misc Applications Misc Destinations Paging and Intercom Park and Appounce	CHAN_SIP Is: 5160 ew 'k Usage řerface eth0	00 00	Asterisk + Uptime + CPU + Memory + Disk + Network +	FreePBX St Sep 19 20:09:07 Users Online: 0 Users Offline: 0 In Use: 0	tatistics	2 nks Offline			×

Figure 9 Adding Extensions

Under "Add Extensions", select "Add new CHAN_SIP Extension".

Vighnesh Raje (@s3curityg33k)

(-	→ C û	③ 192.168.0.1	01/admin/confi	ig.php?display=	extensions				🛛 1	*		∭\ ⊡	9	ی دی	1 🥵	» ≡
[]	Admin Applications	Connectivity	Dashboa	rd Repor	rts Settir	ngs	UCP								Ø] Q	\
	All Extensions Cu	stom Extensions	DAHDI E	xtensions	IAX2 Exten	isions	PJSIP Ex	tensions	Chan_SIF	Extensio	ns Vi	rtual Ext	ensions			
	+ Add Extension -	[#] Quick Create E	xtension	× Delete						Search			C		III •	
	+ Add New Custom Exte	ension Ex	tension	🔶 Nan	ne 🔶	cw	DND	FM/FM	CF	CFB	CFU	Туре		Actio	ins	
	+ Add New IAX2 Extensi	ion 50	0	rame	esh	Ø				D	D	sip		1	Û	
	+ Add New Chan_SIP Extens	tension	_	2												
	+ Add New Virtual Exter	nsion														
		* *	Free	DBX	FreePBX is	s a registered	i trademark of									
			let freedo	om ring™	Sang FreePBX 14.0. Co	oma Technol 13.4 is licens pyright® 200	ogies inc. ed under the GF 17-2019		SAN	JG(

Figure 10 Chan-SIP Extension

Provide with details like, User Extension, Display Name and Secret.

\leftarrow		ଟିଢି		🛈 🔏 https://19	2.168.0.101/ad					⊌ ☆	lii\	9	e	e ¹ &	<mark>,</mark> »	
0	Adr	min A	pplications	Connectivity	Dashboard	d Repor	ts Setti	ings UCF	2			Apply	Config		Q	\
_		General	Voicemail	Find Me/Fol	low Me	Advanced	Pin Sets	Other								- 1
		- Add Ext	ension													
		User Exte	nsion 📀			600										
		Display N	ame 🕜			suresh										_
		Outbound	i CID 😧													
	_	- Langua	ge													
		Language	Code 🕜			Defau	t							~		
	-	User Ma	anager Setti	ngs												
		Select Use	er Directory: 🛿	•		PBX In	ternal Direct	ory						~		
		Link to a l	Default User 🔞			Create	New User							~		
		Username	2 0			suresh						Jse Cust	om Usei	rname		
		Password	For New User	0		sureshe	00									
						Weak						×	Sub	mit	Re	set
															11	

Figure 11 User Details

Similarly, create second Extension.

Inside, Applications -> Extensions, we can view the created Extensions.

Vighnesh Raje (@s3curityg33k)

\leftarrow) C 🔓	 192.168.0.101 						• ⊠ ť		l	N	۹ () e	1 🦺 :	» ≡
[]	Admin Applications	Connectivity	Dashboard	eports Settin	gs l	JCP					Ар	ply Con	fig	3 Q	\$ ^
-	All Extensions Cu	stom Extensions	DAHDi Extensions	IAX2 Exten	sions	PJSIP Ext	ensions C	han_SIP	Extensior	is Vir	tual Exte	nsions			
	+ Add Extension +	7 Quick Create Ext	ension × Delet	te					Search			C		III •	_
		Exte	ension 🔶 M	Name 🔶	cw	DND	FM/FM	CF	CFB	CFU	Туре		Actio	ns	
		500	r	ramesh		0	0	0	0	0	sip		Ø 1	Ì	
		600	s	suresh		0	0	0	0	D	sip		Ø 1	Ì	
:	Showing 1 to 2 of 2 rows														
(
		XXX	FreePBX	FreePBX is Sango	a registered ma Technolo	trademark of gies Inc.	C								
			let freedom ring™	FreePBX 14.0.1 Cop	13.4 is license syright© 2007	ed under the GPL 7-2019	3/								

Figure 12 All Extensions

1.2 Configuring Zoiper Softphone

Zoiper is an on premise and cloud-based softphone solution that caters to service providers, call centres, VoIP integrators, mobile operators and businesses that require softphones independent of their service provider. [10]

Zoiper, the free softphone to make VoIP calls through your PBX or favourite SIP provider. Available for iPhone, Android, Windows Phone 8, Windows, Mac.

Zoiper can be downloaded from here.

The setup is demonstrated is on Windows 7 system.

Note: Here, we are considering the system to be on same network as that of VoIP server.

Install the downloaded Zoiper executable. After installation, launch the application. Provide with User Extension and password.

Note: Extension and password is the one added in Asterisk.



Figure 13 User Login

Provide the address of VoIP server along with port number.



Figure 14 Providing hostname

User can choose to skip Proxy settings.

The softphone software will automatically check for possible configurations.



Figure 15 Automatic Network Configuration

Contract

Contr

Zoiper has been successfully configured.

Figure 16 Zoiper Softphone

Following similar steps, configure Zoiper softphone inside android device.

5. Configuring Raspberry pi

For the scope of this project we will be working on Raspberry Pi Model 3.

The Raspberry Pi 3 Model B is the earliest model of the third-generation Raspberry Pi. It replaced the Raspberry Pi 2 Model B in February 2016. See also the Raspberry Pi 3 Model B+, the latest product in the Raspberry Pi 3 range. [11]

- Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
- 1GB RAM
- BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board
- 100 Base Ethernet
- 40-pin extended GPIO
- 4 USB 2 ports
- 4 Pole stereo output and composite video port
- Full size HDMI
- CSI camera port for connecting a Raspberry Pi camera
- DSI display port for connecting a Raspberry Pi touchscreen display
- Micro SD port for loading your operating system and storing data
- Upgraded switched Micro USB power source up to 2.5A

User must flash Kali Linux for ARM OS. Let's begin with downloading the kali image file from <u>here</u>.

Begin with formatting the SD Card, using SD card formatter.

SD Card Formatter		×
File Help		
Select card		
F:\-STRONTIUM		~
		<u>R</u> efresh
Card information		
Туре	SDHC	S)
Capacity	29.44 GB	
Formatting options		
Overwrite format		
CHS format size adju	ustment	
Volume label		
STRONTIUM		
		Format
SD Logo, SDHC	Logo and SDXC Logo are tradema	arks of SD-3C, LLC.

Figure 17 Formatting SD Card

After formatting the SD card, flash the image inside it. For that launch Balena Etcher software and follow the steps from the screen shot. Balena Etcher can be downloaded from https://www.balena.io/etcher/.

😚 Etcher		-
		3 Florefull
+ —		- 7
kali-linuexmon.img 5 GB	SDHC Card Change	Flash!
Change		
		balena
	Figure 18 Flashing OS in SD Card	
DC 18		

After flashing the SD card, insert SD card inside raspberry pi and power it on.

Now we will be connecting the raspberry pie with the network, so that latter we can SSH into the pie.

For that, inside your desktop go to Network Sharing centre and choose Wi-Fi.

💐 Network and Sharing Center				_		×	
🔶 🚽 🗸 🛧 💐 > Control Panel	Search Control Panel		٩,				
Control Panel Home	Control Panel Home View your basic network information and set up connections						
Change adapter settings	View your active networks	1					
Change advanced sharing settings	GUEST 2 Public network	Access type: Internet Connections: Wi-Fi (GUEST)					
	Unidentified network Public network	Access type: No network access Connections: <i>Center</i> Ethernet					
	Change your networking settings						
	Set up a new connection or network Set up a broadband, dial-up, or VPN connection	on; or set up a router or access point.					
	Troubleshoot problems Diagnose and repair network problems, or ge	t troubleshooting information.					
See also							
HomeGroup							
Infrared							
Intel® PROSet/Wireless Tools							
Internet Options Windows Firewall							
Windows FireWall							

Figure 19 Network Sharing

Now, go to Properties -> Sharing and check the "Allow other network users to connect" checkbox. In "Home networking connection" choose Ethernet. Click "OK" to save the settings.

Network and Sharing Center					- 0
← → × ↑ ₩ > Contro	Panel > All Control Panel Items > Netv	work and Sharing Center		~ (1)	earch Control Panel
	View your basis network i	eformation and set	up connection	2.	
Control Panel Home	di Wi-Fi Status	×	up connection	WI-FI Properties	×
Change adapter settings	General			Networking Sharing	
Change advanced sharing	Connection		Access type: I	Internet Connection Sharing	
settings	IPv4 Connectivity:	Internet	Connections: 📶 \	Allow other network users to conr	4.
	IPv6 Connectivity:	No network access	3.	computer's Internet connection	Select Ethernet
	Media State:	Enabled	Allow	Home networking connection:	
	Duration:	1 day 01:26:52	Connections: @ F	Ethernet	~
	Speed:	72.2 Mbps		Allow other network users to cont	rol or disable the
	Signal Quality:	atl		shared Internet connection	
	Details Winalass Presente	ac l			Settings
	there as Propertie				
	Activity		or set up a router		
	Sant	Received			
	1. Click on Properties	3.336,512,403	oubleshooting info		
		-,,			
See also		10000			
HomeGroup		ugitose			
Infrared		Close			
Intel® PROSet/Wireless Tool					OK Cancel
Internet Options					
Windows Firewall					
	Figure 20.	Allow network s	haring for Eth	ernet	
	Figure 20.	Allow network s	haring for Eth	ernet	
	Figure 20 .	Allow network s	haring for Eth	ernet	
ow, move to Et	Figure 20.	Allow network s	haring for Eth	ernet	
ow, move to Et	Figure 20.	Allow network s	haring for Eth	ernet	
ow, move to Et	Figure 20.	Allow network s	haring for Eth	ernet	1.1.1.1
ow, move to Et	Figure 20. nernet settings. ils" and notice the II	Allow network s Pv4 Address	haring for Eth	ernet 192.168.137.1 w	hich will act as
ow, move to Et	Figure 20. nernet settings. ils" and notice the II	Allow network s Pv4 Address	haring for Eth s. Here, its	ernet 192.168.137.1 w	hich will act as
ow, move to Et ow, go to "Deta ateway for our p	Figure 20. nernet settings. ils" and notice the II i.	Allow network s Pv4 Address	haring for Eth 5. Here, its	ernet 192.168.137.1 w	hich will act as
fow, move to Et fow, go to "Deta ateway for our p	Figure 20. nernet settings. ils" and notice the Il i.	Allow network s Pv4 Address	haring for Eth 5. Here, its	ernet 192.168.137.1 w	hich will act as
fow, move to Et fow, go to "Deta ateway for our p	Figure 20. nernet settings. ils" and notice the Il i.	Allow network s Pv4 Address	haring for Eth 5. Here, its	ernet 192.168.137.1 w	hich will act as
fow, move to Et fow, go to "Deta ateway for our p	Figure 20. hernet settings. ils" and notice the II i.	Allow network s Pv4 Address	haring for Eth s. Here, its	ernet 192.168.137.1 w	hich will act as
Tow, move to Et Tow, go to "Deta ateway for our p Network and Sharing Center $\Leftrightarrow \rightarrow \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	Figure 20. nernet settings. ils" and notice the II i.	Allow network s Pv4 Address	haring for Eth s. Here, its	ernet 192.168.137.1 w	hich will act as
Tow, move to Et Tow, go to "Deta ateway for our p Network and Sharing Center $\leftarrow \rightarrow \sim \uparrow \blacksquare \bigcirc \square$	Figure 20. hernet settings. ils" and notice the II i.	Allow network s	haring for Eth	ernet 192.168.137.1 w √೮	hich will act as

· → ~ ↑ 💐 > Cc	Ethernet Status	× •••• • • • • • • • • • • • • • • • •	Center	r	ٽ ~	Search Contro	I Panel	, P
Control Panel Home	General		nd si	Network Connection Details	1	×		
Change adapter settings Change advanced sharin settings	Connection IP-4 Connectivity: IP-6 Connectivity Media State: Duration: Speed: Details Activity Sent Sytes: 1,252 Bytes: 1,252 Properties Pro	No network access No network access Enabled 00:07:07 100.0 Mbps Received 2,210 Diagnose	nectic pr get	Network Connection Details: Property Connection-specific DNS S. Description Physical Address DHCP Enabled IPv4 Address IPv4 Address IPv4 Default Gateway IPv4 DNS Server NetBIOS over Tcpip Enabl Link-local IPv6 Address IPv6 DNS Servers	Value Realtek PCIe FE Family Co 50-9A-4C-85-65-86 No 192.168.137.1 255.255.255.0 Yee fe80:.49ab.6801.36c3.b5a57 fec0.0.0fff:.1%1 fec0.0.0fff:.1%1 fec0.0.0fff:.3%1	ntroller 2		
See also HomeGroup Infrared Intel® PROSet/Wireless T Internet Options Windows Firewall	pols	Close				Close		



Now for finding the IP address of raspberry pi, run advance in scanner on the IP range we found above (Ethernet settings).

<u></u> A	dvanced	IP Scanner			_	
<u>F</u> ile	<u>V</u> iew	<u>S</u> ettings <u>H</u> elp				
	Scan					
192.1	68.137.0	-192.168.137.255	Example: 192.16	18.0.1-100, 192.168.0.200	Search	Q
Resu	ults Fa	vorites				
	Status	Name	ÎP	Manufacturer	MAC address	С
> [DESKTOP-3C9APME	192.168.137.1	QUANTA COMPUTER I	A8:1E:84:AA:15:2A	
	-	kali.mshome.net	192.168.137.151	Raspberry Pi Foundati	B8:27:EB:56:CE:7E	
ļ		192.168.137.255	192.168.137.255	QUANTA COMPUTER I	A8:1E:84:AA:15:2A	- 1
<						>
3 alive	, 0 dead, 2	253 unknown				

Figure 22 Advance IP Scanner

SSH into the raspberry pi by using SSH client of user's choice.

Card a second		_	
MobaXterm		- 0	×
ierminal sessions view A server	loops games settings insicros riep ★ In the set of th	X server	U Exit
Quick connect			Ø
Vurk connect	SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Avs S3 WSL I Basic SSH settings Image: Terminal settings Image: Port 22 Image: Port 24 Image: Port		
UNKCOLDTERED VERSION * Please support	Figure 23 SSH Connection attempt		

Proceed by entering login credentials. The default user for raspbian OS is "pi" and password is "raspbian".

User will get a SSH terminal inside raspberry pi.



Figure 24 Raspberry pi terminal

Connect an additional USB Wi-Fi adapter to raspberry pi. After that user must configure the network settings. For that run the command:

\$ nmtui

User will be prompted with a text menu. Move to "Edit Connection" -> "Add Connection" -> "Wi-Fi". Provide details like SSID, Security Type, Password. Here static IP is configured.

192.168.137.151	- D	Х
Terminal Sessions View X server Tools Games Settings Macros Help		
🚇 🛧 🛝 🍕 🚖 🖳 🖳 ヤ 🖳 📥 🤃 🛛	X	U
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help	X server	Exit
Quick connect		Ø
Quick connect Image: Source of the so		
Remote monitoring		
Follow terminal folder		~
UNREGISTREED VERSION - Please support Mobaltern by subscribing to the professional edition here: https://nobautern.mobatek.net		

Figure 25 Configuring network settings

In similar manner, add another Wi-Fi connection.

Note: As static IP is set, the two Wi-Fi connections, even though have same SSID, must have different static IPs set.

Configure Wi-Fi adapter and USB Wi-Fi adapter with these connections respectively.

For checking network details, run the command:

\$ ifconfig



Figure 26 Network Details of Raspberry

5.1 Remote Log into Raspberry Pi's Full Operating System Using VNC Connect

VNC has been the best way to access any computer remotely on the same network. Recently, VNC Connect also came out to make it easy to access your Raspberry Pi from anywhere using a cloud connection. Once it's set up, you can access your Raspberry Pi's graphic interface from any other computer or smartphone using the VNC Viewer app.

VNC Connect comes packed in for free with the most recent versions of the Raspberry Pi operating system. [12]

VNC can be set up in few simple steps. Open up a terminal and run the following commands:

\$ sudo apt-get update

\$ sudo apt-get install realvnc-vnc-server realvnc-vnc-viewer

Once that's complete, type in

\$ sudo raspi-config

and press Enter. Scroll down to VNC and set it to Enabled.

Once that's finished downloading, you can set up VNC Connect:

- Head to the RealVNC Raspberry Pi sign up page and enter your email address in the sign up box.
- Follow the on-screen instructions to finish setting up your account with a password.
- Back on your Raspberry Pi, click the VNC icon in the top-right corner of the screen to open VNC. Then click the status menu and select Licensing.
- Enter the email address and password you created in step one.
- When prompted, select "Direct and cloud connectivity." Your Raspberry Pi is now accessible online.
- Download the VNC Viewer application on the computer you want to control the Raspberry Pi from, like the laptop or smartphone you'll have when you travel.

Open the VNC Viewer application and enter the credentials you created in step one.

Your Raspberry Pi will pop up as an option automatically. Select it to open up the connection. When prompted, enter your Raspberry Pi's username and password (by default this is the username "pi" and "toor" raspberry). Within a few second it'll connect. You're now able to log into your Raspberry Pi's graphic desktop from anywhere as long as your Raspberry Pi has internet access.

5.2 Installing Required Packages

The following packages need to be installed as the would be needed by our custom script.

Let's begin by install tcpdump.

Tcpdump is a common packet analyser that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software. [13]

\$ sudo apt-get install tcpdump -y

Now user needs to install Ettercap. We will be using Ettercap text only version for ARP Spoofing.

Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. [14]

\$ sudo apt-get install Ettercap-text-only -y

Next up, user needs to install python PyDrive library which will be useful for pushing files to the google drive.

PyDrive is a wrapper library of google-api-python-client that simplifies many common Google Drive API tasks. [15]

\$ pip install PyDrive

6. Sniffing VoIP calls using custom script over a Raspberry pi

Inside our lab configuration, we are considering that there are two softphones i.e. an android phone and another setup on a windows system. The two softphone users are communication with each other through VoIP call. The scope of this project is to intercept and analyse this call for investigative purpose.



Figure 27 Picturing the scenario

We have setup a raspberry pi inside the same network of that of the two softphones. The investigator connects to this raspberry pi using VNC Connect cloud service through a remote location.

The first step is to find the IP address of softphone, for that the investigator needs to run a nmap scan.

Once the IP address is known, the investigator needs to proceed by calling the custom python script which we have named as "sip_exploitation.py".

The scripts can be found at <u>https://github.com/s3curityg33k/VoIP-Sniffer</u>.

Sip_exploitation.py will ask for victim IP address. Enter the softphone IP address found through nmap scan.

192.168.137.165 (naspberrypi) - VNC Viewer			- 0	×
🛞 🌐 🛅 🗾 🗾 pi@raspberrypi: ~/Do 🛛 🚺 🏌 🎓	(را	23:44		
pi@raspberrypi: ~/Downloads		^ X		
File Edit Tabs Help				
<pre>pi@raspberrypi:~/Downloads \$ python sip_exploitation.py</pre>				
Enter victim IP Address 192.168.1.102				
			1	
		- 12		
		_		

Figure 28 Running exploit script

The script will then try to perform an ARP spoof on the victim using Ettercap API.



Figure 29 ARP poisoning

Consecutively, the script will also try to capture UDP packets belonging to the victim. Once the packet capture is completed the script will try to upload the pcap file on to google drive.



Figure 30 TCP dump

A web browser will be prompted asking to choose an account to which the script would be updated.

Note: Network congestion issues were seen when the script tried to upload the pcap on the drive. To avoid this, it is advisable to force shut the thread performing ARP spoofing once the packet capture is completed. For this press "Ctrl+C" on the terminal instance performing ARP spoofing.



Figure 31 Drive account

After this, the packet capture file would be uploaded on the drive.

Now the investigator can try to listen to the VoIP conversation taken place between the two softphone users on his remote system.

For this, the investigator first needs to download the packet capture file from the drive.



Figure 32 Uploaded packet capture

Open "test.pcap" inside wireshark.

For viewing all VoIP packets, apply the following filter "sip \parallel rtp".

🏹 Kali-	2019 (Snaj	pshot 1) [Running] - Orac	le VM VirtualBox					-	- 0	×
Appli	cations	Places Places	Wireshark 🔻		Sat 1	16:56		1 😼	ss (1))	Ĥ ▼
					test.	pcap			0	• •
	File	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tatistic	s Telephon <u>y W</u> ireless <u>T</u> oo	ls <u>H</u> elp				-	
			🖹 🕅 🔇 🔍 🔶 •			TT				
	sin								voressio	n +
	in orb								xp103310	
	No.	Time	Source	Destination	Protocol	Length Info				L A
		3 6.142826	192.168.1.102	192.168.1.101	SIP/SDP	799 Request: INVITE s	sip:600@192.168.1.101:5160;tr	ansport=U	DP	
		4 6.653164	192.168.1.102	192.168.1.101	SIP/SDP	799 Request: INVITE s	sip:600@192.168.1.101:5160;tr	ansport=U	DP	
		5 7.423083	192.108.1.102	192.108.1.101	SIP STD/SDD	799 Request: TNVITE	sip:6000102 168 1 101:5160;trar	sport=UDP		
_		7 7 922791	192.168.1.102	192.168.1.101	STP	808 Request: REGISTER	R sin:192.168.1.101:5160:trar	sport=UDP	(1	
		8 8.936332	192.168.1.102	192.168.1.101	SIP	808 Request: REGISTER	R sip:192.168.1.101:5160;tra	sport=UDP	(1	
_		9 9.645933	192.168.1.102	192.168.1.101	SIP/SDP	799 Request: INVITE s	sip:600@192.168.1.101:5160;tr	ansport=U	DP I	
M		11 10.937298	192.168.1.102	192.168.1.101	SIP	808 Request: REGISTER	R sip:192.168.1.101:5160;trar	sport=UDP	(1	
. 🖤		13 13.449315	192.168.1.102	192.168.1.101	SIP	719 Status: 200 OK				
		14 13.644790	192.168.1.102	192.168.1.101	SIP/SDP	799 Request: INVITE s	sip:600@192.168.1.101:5160;tr	ansport=U	DP	
		15 14.569175	192.168.1.102	192.168.1.101	SIP	719 Status: 200 OK				
		16 14.921297	192.168.1.102	192.168.1.101	SIP	808 Request: REGISTER	R sip:192.168.1.101:5160;trar	sport=UDP	(1	
		18 15.459580	192.168.1.102	192.168.1.101	SIP	719 Status: 200 OK				
		19 10.483583	192.108.1.102	192.108.1.101	SIP	719 Status: 200 OK				-
	Fra ▶ Fra	me 3: 799 bytes	s on wire (6392 bits)	, 799 bytes captured (6	392 bits)					4
	0000	00 c0 ca a9 7	1 a3 bc 3a ea 7c e8	d4 08 00 45 00 · · · · a		F.				
	0010	03 11 e4 8c 4	0 00 40 11 cf 33 c0	a8 01 66 c0 a8 ····@	·@· ·3···f					
A	0020	01 65 c8 f0 1	4 28 02 fd 54 05 49	4e 56 49 54 45 · e · · ·	(·· T·INVI	TE				
—	0030	20 73 69 70 3	a 36 30 30 40 31 39	32 2e 31 36 38 sip:	600 @192.1	.68				
:::	0040	2e 31 2e 31 3	0 31 3a 35 31 36 30	3b 74 72 61 6e .1.10	1:5 160;tr	an				
	0050	73 70 01 72 7 30 0d 0a 56 6	4 30 55 44 50 20 53 9 61 39 20 53 49 50	2f 32 2e 30 2f 0. Vi	-00 P SIP/	2.				
	0070	55 44 50 20 3	1 39 32 2e 31 36 38	2e 31 2e 31 30 UDP 1	92. 168.1.	10				
	0080	32 3a 35 31 3	4 34 30 3b 62 72 61	6e 63 68 3d 7a 2:514	40; branch	=z				
	0 7	Deal Time Transp	ort Drotocol, Drotocol			Dad	kata 266 Displayed 244 (04 0%)		Drafilo	▼ Dofault
		Reat-Time Transp	on Frotocol, Protocol			Pac	.xets. 500 · Displayed: 544 (94.0%)			Derault
							2 🙂 😼		T 👐 🚺 🕻	 Right Ctrl

Figure 33 VoIP packets

For viewing the call packets, go to Telephony -> VoIP Calls

Vighnesh Raje (@s3curityg33k)

쐽 Kal	i-2019	(Snapshot i	I) (Runni	ing] - Oracle \	/M VirtualBox											- ť	ס	×
File	Mach	ine View	Input	Devices H	Help													
Арр	licati	ons 🔻	Place	s 🔻 🗖 🛚	Wireshark 🔻				Sat	16:57				1	, #	_ x* =	» 🗎	
							1.		test	pcap						-		×
	Ei	ile <u>E</u> dit	View	<u>G</u> o <u>C</u> ap	oture <u>A</u> nalyz	e <u>S</u> tatistics	Telephony <u>W</u> ir	eless <u>T</u> ools	<u>H</u> elp									
			1 0	0	🗙 🏹	०, 🔹 🗭	.ə 🖛 🖬 🗐		् २ २									
		sip rtp												X		Express	ion	+
	No).	Time		Source		Destination		Protocol	Length Info								-
	L.C.	3	6.142	2826	192.168.	1.102	192.168.1.	101	SIP/SDP	799 Request	:: INVITE sip:60	00@192.16	8.1.101:	5160:tran	sport=	UDP		
P- 1		4	6.6					Wiresh	ark · VolP C	alls · test.pcap					S rt=	UDP		
<u> </u>		6	7.6	Start Tin T	Stop Time	Initial Speake	r From			То		Protoco	Duration	Dackets St	at rt=	UDP		
		7	7.9	6 142826	40.962996	192 168 1 102	<pre>csip:500@192</pre>	168 1 101-516	50:transnor	t=LIDP> <sip:600< td=""><td>@192 168 1 101-516</td><td></td><td>00.00.34</td><td>17 C</td><td></td><td>P (1</td><td></td><td></td></sip:600<>	@192 168 1 101-516		00.00.34	17 C		P (1		
		8	8.9	0.1-12020	40.502550	192.100.1.101		100.1.101.01	oo,cruinspor	(_0017_05)p.000	GISTING	01 511	00.00.54	· 1/ C.)P (1		
M		11	10.												=00)P (1		
L 🖷		13	13.				2									(-		
		14	13.				4.								rt=	UDP		
		15 16	14.												=UD	P (1		
		18	15.												0.0	. (2		

Figure 34 VoIP Conversation

Select the VoIP call and click on "Play Stream".

Here, the investigator will be able to hear the conversation that took place between the two suspects.



Figure 35 Playing VoIP call in RTP player

7. Conclusion

Outcome of this project work will assist forensic investigators in covertly sniffing and intercepting VoIP calls. This project will act as a basic guideline for the investigators and they can take help of findings of this project to speed up their investigation.

8. References

[1] Michael Dosch and Steve Church. "VoIP in the Broadcast Studio". Axia Audio. Archived from the original on October 7, 2011. Retrieved June 21, 2011.

[2] <u>https://indianexpress.com/article/cities/mumbai/criminals-making-voip-calls-cops-seek-</u> <u>dot-help/</u>

[3] Rakesh Arora. "Voice over IP: Protocols and Standards" dated November 23, 1999. http://www.cis.ohio-state.edu/~jain/cis788-99/voip_protocols/index.html

[4] Sohil Garg. "Enumerating and Breaking VoIP". <u>https://www.exploit-</u> db.com/docs/english/18136-paper-enumerating-and-breaking-voip.pdf

[5] Santi Phithakkitnukoon, Enkh-Amgalan Baatarjav, Ram Dantu. "VoIP Security – Attacks and Solutions" dated March 06, 2015. <u>https://www.researchgate.net/publication/220449868</u>

[6] Dharmin Suthar. "VoIP Penetration Testing and Forensics" dated April, 2018.

[7] Hardik Tandel, Dr. Parag Rughani. "Forensic Analysis of Asterisk-FreePBX based VoIP Server" dated June, 2018. <u>https://www.researchgate.net/publication/326046523</u>

[8] Yusuf Turk, Onur Demir, Sezer G⁻oren. "Real Time Wireless Packet Monitoring with Raspberry Pi Sniffer". <u>https://san.ee.ic.ac.uk/iscis2014/proceedings/27_turk.pdf</u>

[9] https://www.asterisk.org/get-started

[10] https://www.softwareadvice.com/voip/zoiper-profile/

[11] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

[12] <u>https://lifehacker.com/how-to-control-a-raspberry-pi-remotely-from-anywhere-in-</u> 1792892937

[13] https://www.tcpdump.org/manpages/tcpdump.1.html

[14] <u>https://en.wikipedia.org/wiki/Ettercap_(software)</u>

[15] https://pythonhosted.org/PyDrive/