Our vision of security in VoIP/UC

17th of April, 2012

KAMAILIO WORLD
CONFERENCE & EXHIBITION
BERLIN - GERMANY, APRIL 16-17, 2013

Quobis®
leading your ITinerary

About Quobis

- Working in UC since 2006
- Focus on VoIP since 2008
- Addressing SP and enterprise markets
- HQ in Vigo (Spain)
- Authors of QoffeeSIP

Presentation

- NOT a common VoIP security presentation, you all know that stuff ;-)

  - State of security through not typical examples.
  - Our new toy: Bluebox-ng.
  - Our modest opinion.

Antón Román
CTO
@antonroman
anton.roman@quobis.com

Jesús Perez
Security Engineer
@jesusprubio
jesus.perez@quobis.com

Some things we are going to talk about

- Why do we receive attacks?

- How is money related to VoIP attacks?

- What things can we pay for?

Security in 2013. Introduction

Some years ago ...

- Skilled Individuals
- Ethics
- Knowledge

Today...

- Mafias
- Automated tools
- $$$$$$

Security in 2013. All can be bought

TRAFICO

CLICK FRAUD

MARKETPLACES

IFRAMES/WEBINJECTS

PROXYS/SOCKS/ACCOUNTS

BINDERS/CRYPTERS

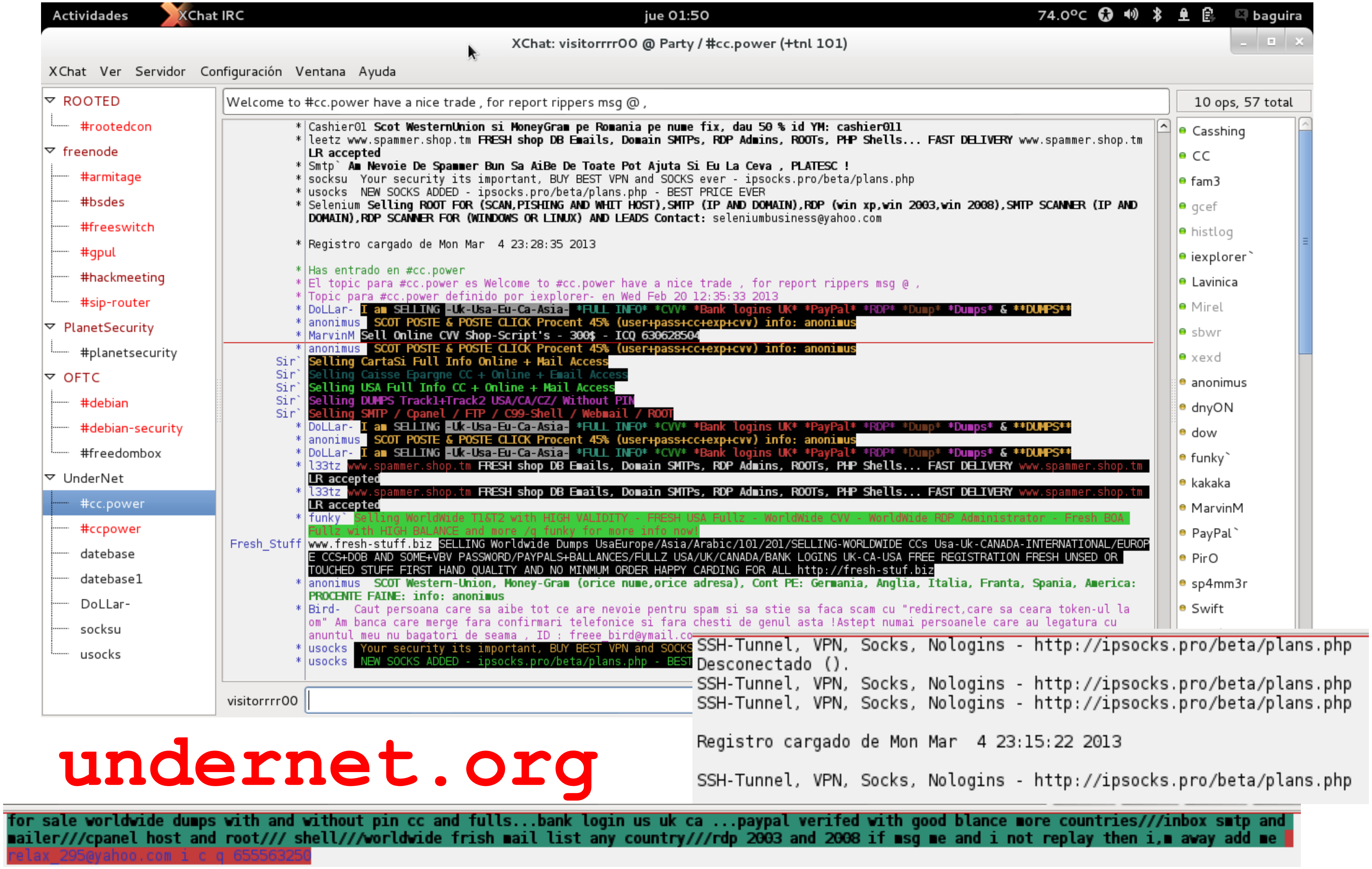
VPS

VPN

PROGRAMACIÓN

CRIMEWARE

Security in 2013. All can be bought



Welcome to #cc.power have a nice trade , for report rippers msg @ ,

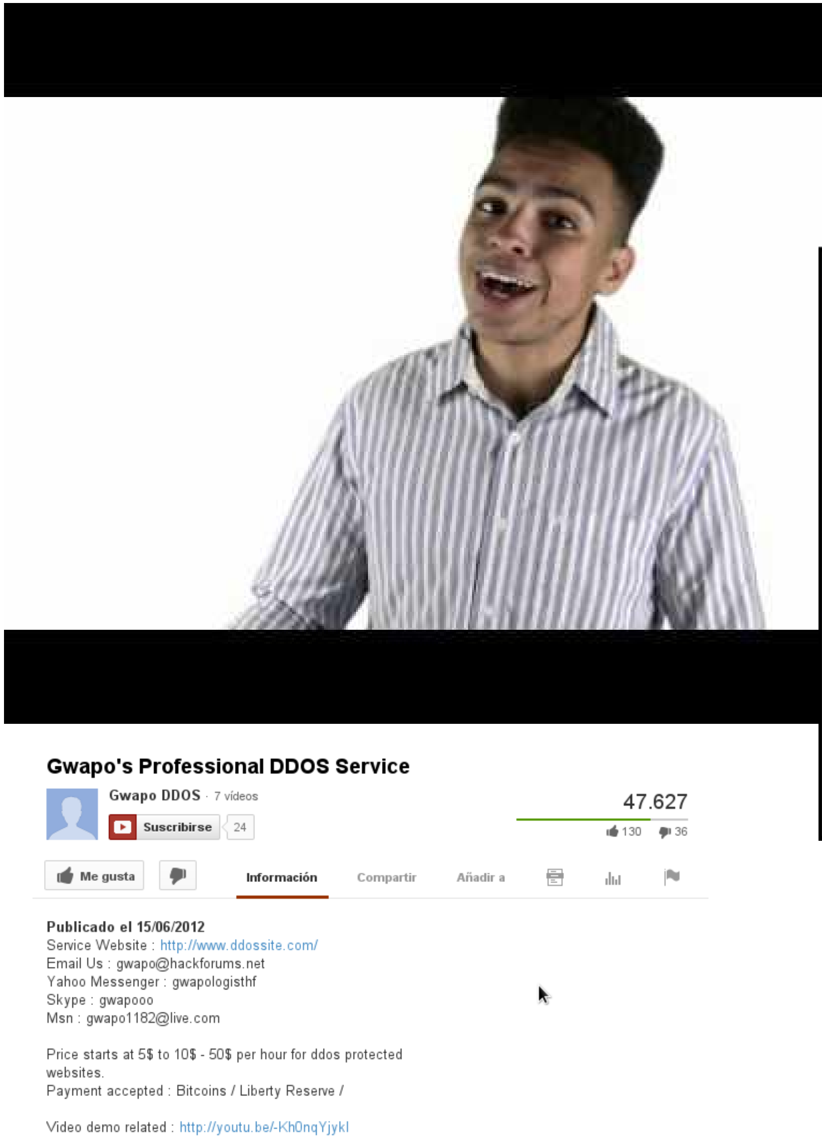
```
         * Cashier01 Scot WesternUnion si MoneyGram pe Romania pe nume fix, dau 50 % id YM: cashier011
         * leetz www.spammer.shop.tm FRESH shop DB Emails, Domain SMTPs, RDP Admins, ROOTs, PHP Shells... FAST DELIVERY www.spammer.shop.tm
           LR accepted
         * Smtp` Am Nevoie De Spammer Bun Sa AiBe De Toate Pot Ajuta Si Eu La Ceva , PLATESC !
         * socksu  Your security its important, BUY BEST VPN and SOCKS ever - ipsocks.pro/beta/plans.php
         * usocks  NEW SOCKS ADDED - ipsocks.pro/beta/plans.php - BEST PRICE EVER
         * Selenium Selling ROOT FOR (SCAN,PISHING AND WHIT HOST),SMTP (IP AND DOMAIN),RDP (win xp,win 2003,win 2008),SMTP SCANNER (IP AND
           DOMAIN),RDP SCANNER FOR (WINDOWS OR LINUX) AND LEADS Contact: seleniumbusiness@yahoo.com

         * Registro cargado de Mon Mar  4 23:28:35 2013

         * Has entrado en #cc.power
         * El topic para #cc.power es Welcome to #cc.power have a nice trade , for report rippers msg @ ,
         * Topic para #cc.power definido por iexplorer- en Wed Feb 20 12:35:33 2013
         * DoLLar- I am SELLING -Uk-Usa-Eu-Ca-Asia- *FULL INFO* *CVV* *Bank logins UK* *PayPal* *RDP* *Dump* *Dumps* & **DUMPS**
         * anonimus  SCOT POSTE & POSTE CLICK Procent 45% (user+pass+cc+exp+cvv) info: anonimus
         * MarvinM Sell Online CVV Shop-Script's - 300$ - ICQ 630628504
         * anonimus  SCOT POSTE & POSTE CLICK Procent 45% (user+pass+cc+exp+cvv) info: anonimus
      Sir` Selling CartaSi Full Info Online + Mail Access
      Sir` Selling Caisse Epargne CC + Online + Email Access
      Sir` Selling USA Full Info CC + Online + Mail Access
      Sir` Selling DUMPS Track1+Track2 USA/CA/CZ/ Without PIN
      Sir` Selling SMTP / Cpanel / FTP / C99-Shell / Webmail / ROOT
         * DoLLar- I am SELLING -Uk-Usa-Eu-Ca-Asia- *FULL INFO* *CVV* *Bank logins UK* *PayPal* *RDP* *Dump* *Dumps* & **DUMPS**
         * anonimus  SCOT POSTE & POSTE CLICK Procent 45% (user+pass+cc+exp+cvv) info: anonimus
         * DoLLar- I am SELLING -Uk-Usa-Eu-Ca-Asia- *FULL INFO* *CVV* *Bank logins UK* *PayPal* *RDP* *Dump* *Dumps* & **DUMPS**
         * l33tz www.spammer.shop.tm FRESH shop DB Emails, Domain SMTPs, RDP Admins, ROOTs, PHP Shells... FAST DELIVERY www.spammer.shop.tm
           LR accepted
         * l33tz www.spammer.shop.tm FRESH shop DB Emails, Domain SMTPs, RDP Admins, ROOTs, PHP Shells... FAST DELIVERY www.spammer.shop.tm
           LR accepted
         * funky` Selling WorldWide T1&T2 with HIGH VALIDITY - FRESH USA Fullz - WorldWide CVV - WorldWide RDP Administrator - Fresh BOA
           Fullz with HIGH BALANCE and more /q funky for more info now!
Fresh_Stuff www.fresh-stuff.biz SELLING Worldwide Dumps UsaEurope/Asia/Arabic/101/201/SELLING-WORLDWIDE CCs Usa-Uk-CANADA-INTERNATIONAL/EUROP
           E CCS+DOB AND SOME+VBV PASSWORD/PAYPALS+BALLANCES/FULLZ USA/UK/CANADA/BANK LOGINS UK-CA-USA FREE REGISTRATION FRESH UNSED OR
           TOUCHED STUFF FIRST HAND QUALITY AND NO MINMUM ORDER HAPPY CARDING FOR ALL http://fresh-stuf.biz
         * anonimus  SCOT Western-Union, Money-Gram (orice nume,orice adresa), Cont PE: Germania, Anglia, Italia, Franta, Spania, America:
           PROCENTE FAINE: info: anonimus
         * Bird-  Caut persoana care sa aibe tot ce are nevoie pentru spam si sa stie sa faca scam cu "redirect,care sa ceara token-ul la
           om" Am banca care merge fara confirmari telefonice si fara chesti de genul asta !Astept numai persoanele care au legatura cu
           anuntul meu nu bagatori de seama , ID : freee_bird@ymail.co
         * usocks  Your security its important, BUY BEST VPN and SOCKS
         * usocks  NEW SOCKS ADDED - ipsocks.pro/beta/plans.php - BEST
```

```
SSH-Tunnel, VPN, Socks, Nologins - http://ipsocks.pro/beta/plans.php
Desconectado ().
SSH-Tunnel, VPN, Socks, Nologins - http://ipsocks.pro/beta/plans.php
SSH-Tunnel, VPN, Socks, Nologins - http://ipsocks.pro/beta/plans.php

Registro cargado de Mon Mar  4 23:15:22 2013

SSH-Tunnel, VPN, Socks, Nologins - http://ipsocks.pro/beta/plans.php
```

undernet.org

```
for sale worldwide dumps with and without pin cc and fulls...bank login us uk ca ...paypal verifed with good blance more countries///inbox smtp and
mailer///cpanel host and root/// shell///worldwide frish mail list any country///rdp 2003 and 2008 if msg me and i not replay then i,m away add me
relax_295@yahoo.com i c q 655563250
```

Security in 2013. Or ordered ...

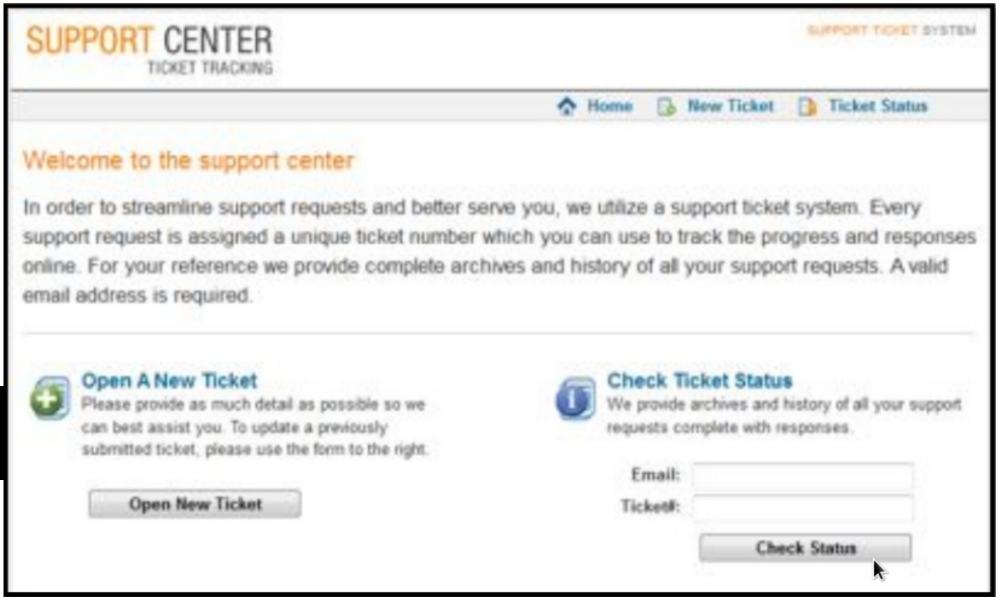


Gwapo's Professional DDOS Service

Publicado el 15/06/2012
Service Website : http://www.ddossite.com/
Email Us : gwapo@hackforums.net
Yahoo Messenger : gwapologisthf
Skype : gwapooo
Msn : gwapo1182@live.com

Price starts at 5$ to 10$ - 50$ per hour for ddos protected websites.
Payment accepted : Bitcoins / Liberty Reserve /

Video demo related : http://youtu.be/-Kh0nqYjykl



SUPPORT CENTER
TICKET TRACKING

Welcome to the support center

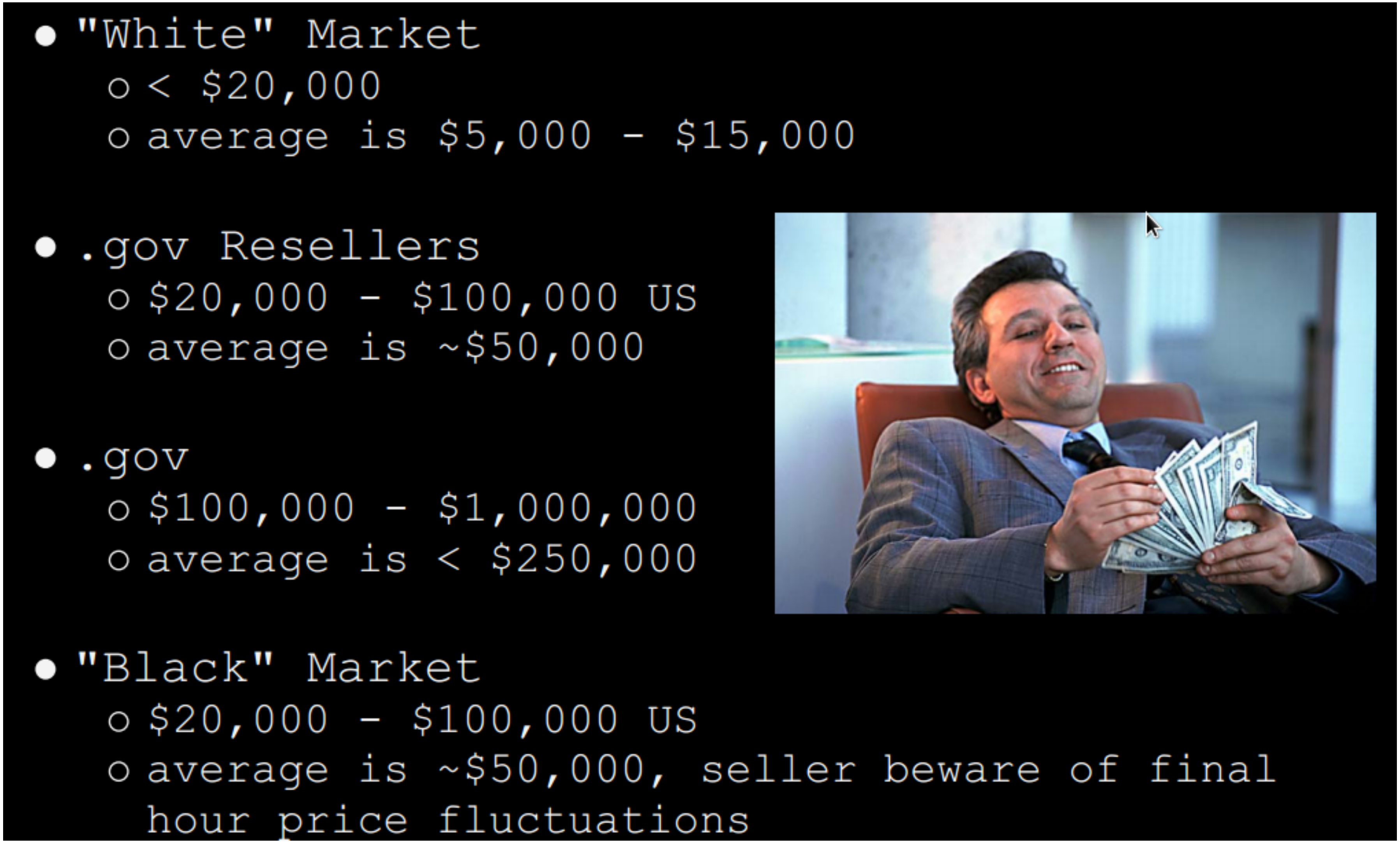
In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required.

Open A New Ticket
Please provide as much detail as possible so we can best assist you. To update a previously submitted ticket, please use the form to the right.

Check Ticket Status
We provide archives and history of all your support requests complete with responses.

Email:
Ticket#:

Security in 2013. 0-days prices



- "White" Market
  - < $20,000
  - average is $5,000 - $15,000
- .gov Resellers
  - $20,000 - $100,000 US
  - average is ~$50,000
- .gov
  - $100,000 - $1,000,000
  - average is < $250,000
- "Black" Market
  - $20,000 - $100,000 US
  - average is ~$50,000, seller beware of final hour price fluctuations

Security in 2013. Hacktivism

Threats. Cloudtag

Flood

Unauthenticated calls

DDoS

Fuzzing

Footprinting

0-days

Shodan

Fingerprinting

Web vulns

DMTF

Google dorks

Vishing

TFTP

Spoofing

Teardown

SPIT

Brute-force

Insecure passwords

Cracking

Malware

Botnet

Register hijacking

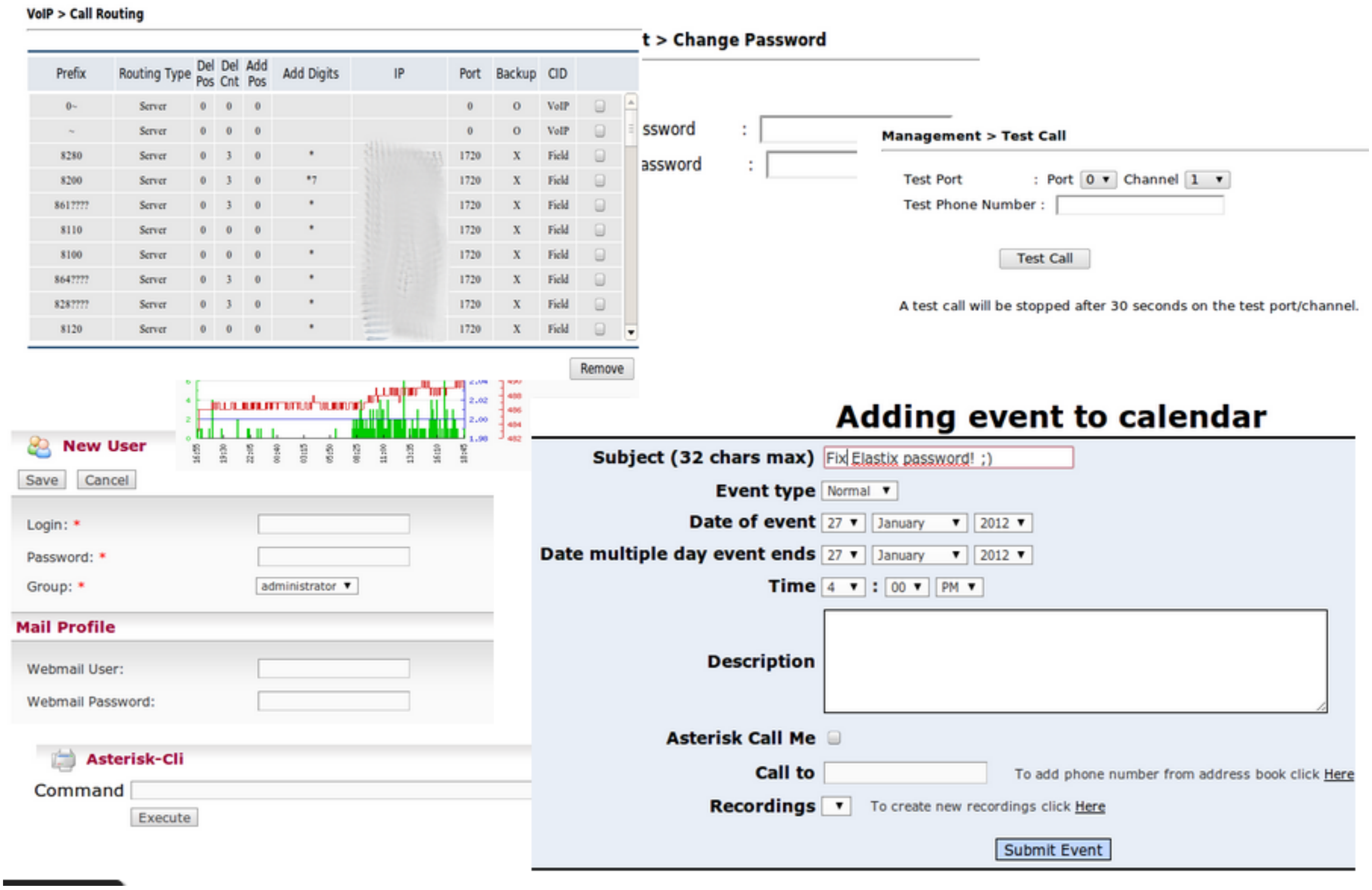
OccupyPhones

Eavesdropping

Communication manipulation

VLAN hopping

Threats. Shodan



VoIP > Call Routing

Prefix	Routing Type	Del Pos	Del Cnt	Add Pos	Add Digits	IP	Port	Backup	CID	
0~	Server	0	0	0			0	O	VoIP	□
~	Server	0	0	0			0	O	VoIP	□
8280	Server	0	3	0	*	[redacted]	1720	X	Field	□
8200	Server	0	3	0	*7	[redacted]	1720	X	Field	□
861????	Server	0	3	0	*	[redacted]	1720	X	Field	□
8110	Server	0	0	0	*	[redacted]	1720	X	Field	□
8100	Server	0	0	0	*	[redacted]	1720	X	Field	□
864????	Server	0	3	0	*	[redacted]	1720	X	Field	□
828????	Server	0	3	0	*	[redacted]	1720	X	Field	□
8120	Server	0	0	0	*	[redacted]	1720	X	Field	□

Remove

t > Change Password

ssword :

assword :

Management > Test Call

Test Port : Port 0 ▾ Channel 1 ▾

Test Phone Number :

Test Call

A test call will be stopped after 30 seconds on the test port/channel.

New User

Save Cancel

Login: *

Password: *

Group: * administrator ▾

Mail Profile

Webmail User:

Webmail Password:

Asterisk-Cli

Command

Execute

Adding event to calendar

Subject (32 chars max)	Fix Elastix password! ;)
Event type	Normal ▾
Date of event	27 ▾ January ▾ 2012 ▾
Date multiple day event ends	27 ▾ January ▾ 2012 ▾
Time	4 ▾ : 00 ▾ PM ▾
Description	
Asterisk Call Me	□
Call to	To add phone number from address book click Here
Recordings	▾ To create new recordings click Here

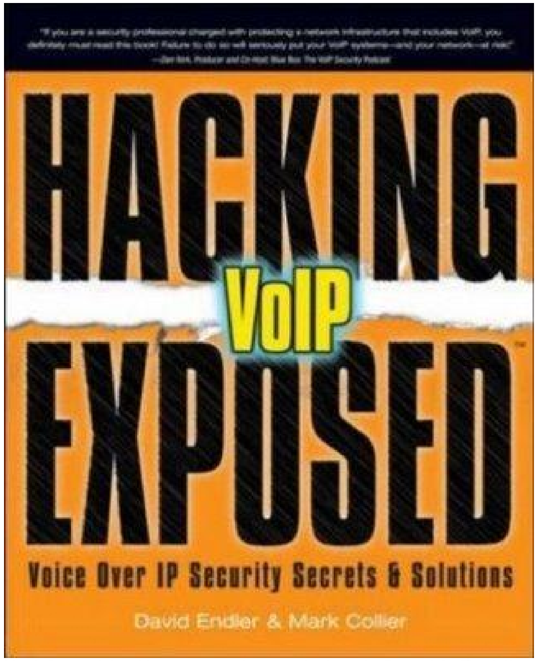
Submit Event

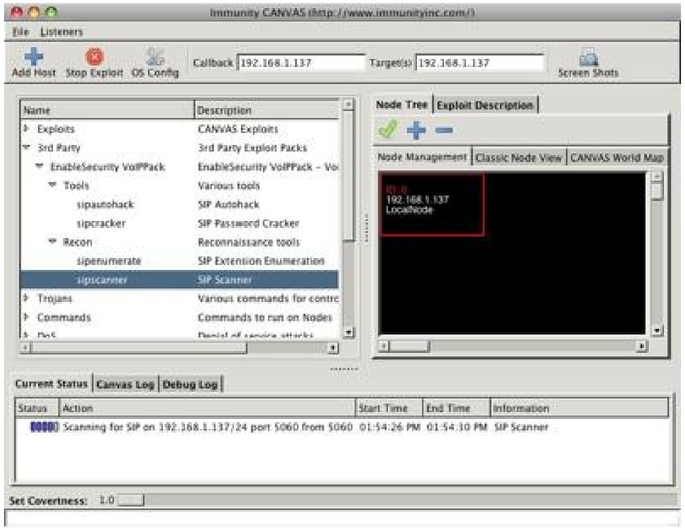
Tools.

SIPp

VoIPER

SiVuS
(SiP Vulnerability Scanner)


"If you are a security professional charged with protecting a network infrastructure that includes VoIP, you definitely must read this book! Failure to do so will seriously put your VoIP systems—and your network—at risk!"
—Dan York, Producer and Co-Host, Blue Box: The VoIP Security Podcast
HACKING VoIP EXPOSED
Voice Over IP Security Secrets & Solutions
David Endler & Mark Collier



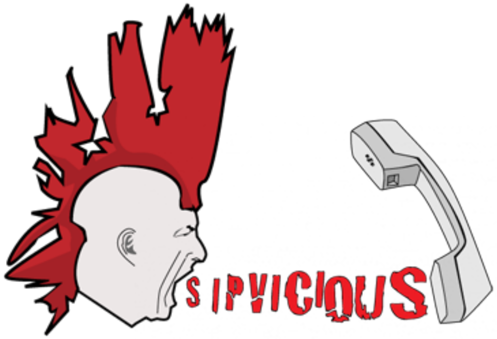
Callback 192.168.1.137 Target(s) 192.168.1.137

Name	Description
Exploits	CANVAS Exploits
3rd Party	3rd Party Exploit Packs
EnableSecurity VoIPPack	EnableSecurity VoIPPack - Vo
Tools	Various tools
sipautohack	SIP Autohack
sipcracker	SIP Password Cracker
Recon	Reconnaissance tools
sipenumerate	SIP Extension Enumeration
sipscanner	SIP Scanner
Trojans	Various commands for contro
Commands	Commands to run on Nodes
DoS	Denial of service attacks

0 0
192.168.1.137
LocalNode

Status	Action	Start Time	End Time	Information
	Scanning for SIP on 192.168.1.137/24 port 5060 from 5060	01:54:26 PM	01:54:30 PM	SIP Scanner

Set Covertness: 1.0



UCSniff

metasploit®

Some thoughts ...

- Classic vector still works too often => they are used massively by bad guys.
- No modern tools. *
- In general, poor security culture.
- New vectors are going to appear => we should be ready.
- VoIP/UC technologies are mature now => we have to push in infosec terms too.

* Except VoIPPack for Inmunity Canvas, but $$$$
Metasploit SIP support isn't serious at all

Bluebox-ng. A step ahead!

- A next generation UC/VoIP security tool. It has been written in CoffeeScript using Node.js powers and using code from CoffeeSIP

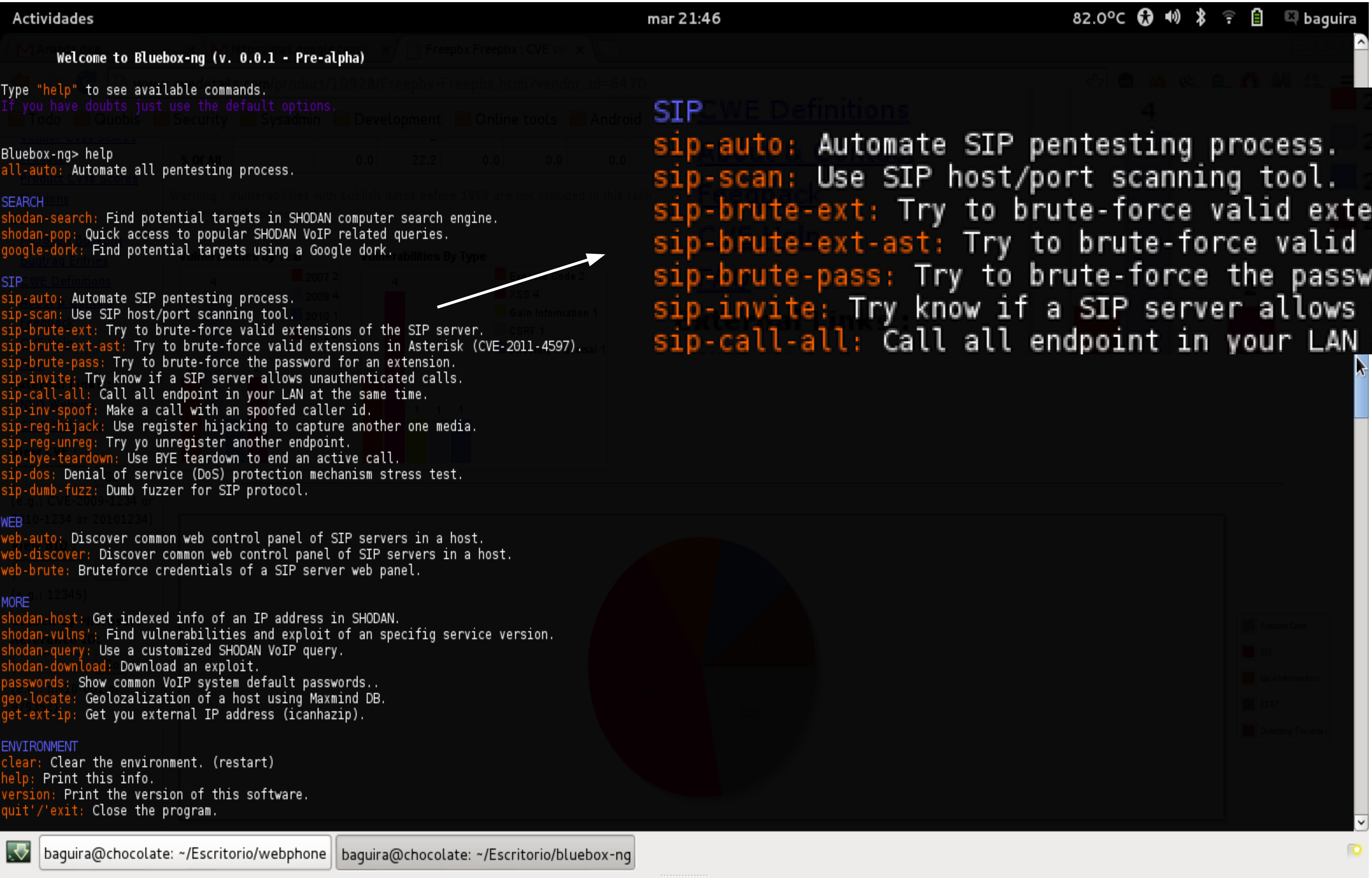
- Our "2 cents" to help to improve infosec culture in VoIP/UC environments.

- Thanks to:
  - @pamojarpan
  - @pepeluxx

Bluebox-ng. Features

- **Automatic pentesting process (VoIP, web and service vulns)**
- **SIP (RFC 3261) and extensions compliant**
- **TLS and IPv6 support**
- **SIP over websockets (and WSS) support (draft-ietf-sipcore-sip-websocket-08)**
- **REGISTER, OPTIONS, INVITE, MESSAGE, SUBSCRIBE, PUBLISH, OK, ACK, CANCEL, BYE, Ringing and Busy Here requests support**
- **Extension and password brute-force through different methods (REGISTER, INVITE, SUBSCRIBE, PUBLISH, etc.)**
- **DNS VoIP related SRV registers discovery**
- **SHODAN and Google Dorks**
- **SIP common vulns modules: scan, extension brute-force, Asterisk extension brute-force (CVE-2011-4597), invite attack, call all LAN endpoints, invite spoofing, registering hijacking, unregistering, bye teardown**
- **SIP DoS/DDoS audit**
- **Common UC related servers web management panels discovery and brute-force.**
- **Automatic exploit searching (Exploit DB, PacketStorm, Metasploit)**
- **Automatic vulnerability searching (CVE, OSVDB)**
- **Geo-localization using WPS (Wifi Positioning System) or IP address (Maxmind database)**
- **Coloured output**
- **Command completion**

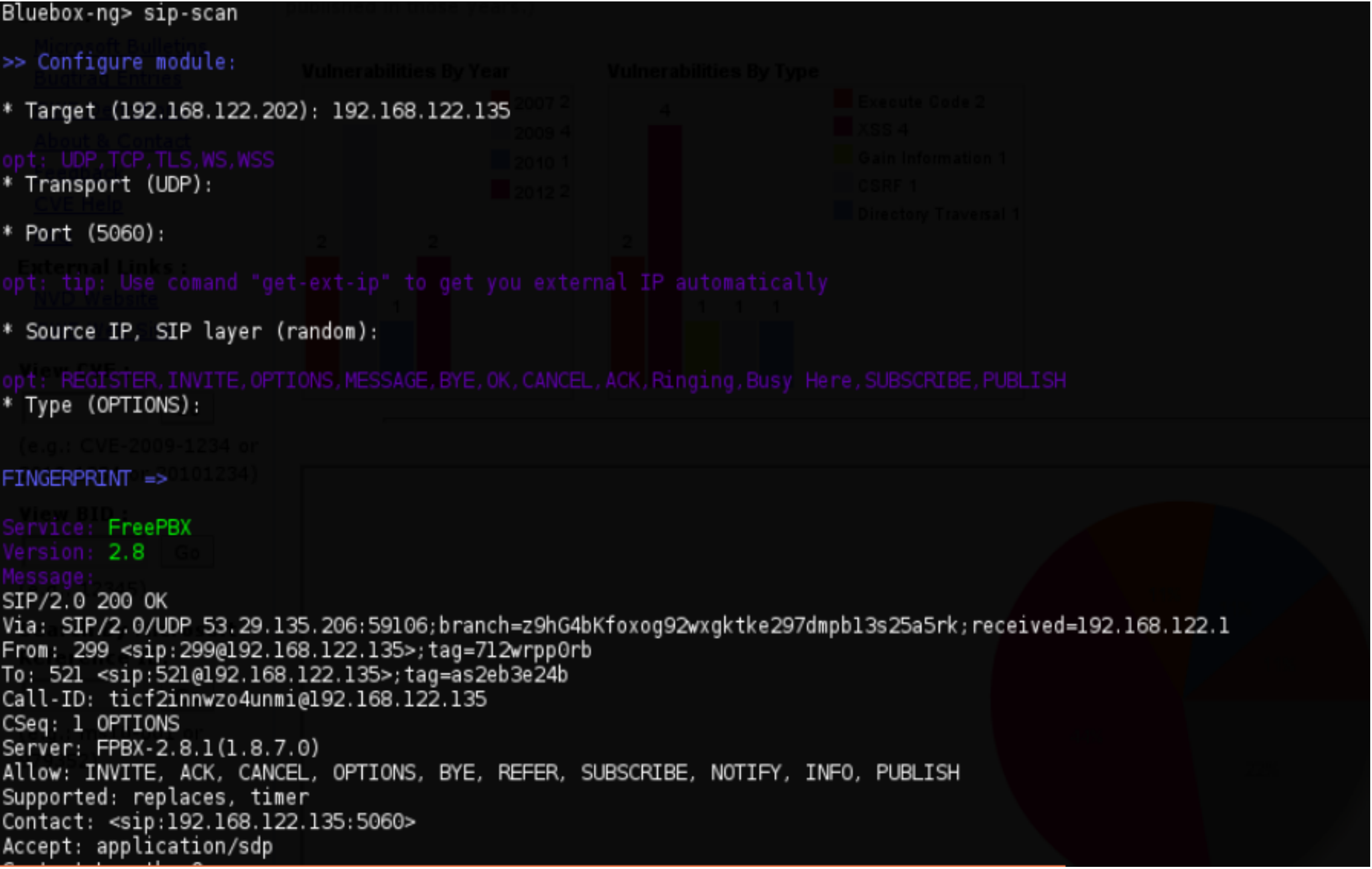
Demo. Bluebox-ng 1


Actividades
mar 21:46
82.0ºC
baguira
baguira@chocolate: ~/Escritorio/webphone
baguira@chocolate: ~/Escritorio/bluebox-ng

```
        Welcome to Bluebox-ng (v. 0.0.1 - Pre-alpha)

Type "help" to see available commands.
If you have doubts just use the default options.

Bluebox-ng> help
all-auto: Automate all pentesting process.

SEARCH
shodan-search: Find potential targets in SHODAN computer search engine.
shodan-pop: Quick access to popular SHODAN VoIP related queries.
google-dork: Find potential targets using a Google dork.

SIP
sip-auto: Automate SIP pentesting process.
sip-scan: Use SIP host/port scanning tool.
sip-brute-ext: Try to brute-force valid extensions of the SIP server.
sip-brute-ext-ast: Try to brute-force valid extensions in Asterisk (CVE-2011-4597).
sip-brute-pass: Try to brute-force the password for an extension.
sip-invite: Try know if a SIP server allows unauthenticated calls.
sip-call-all: Call all endpoint in your LAN at the same time.
sip-inv-spoof: Make a call with an spoofed caller id.
sip-reg-hijack: Use register hijacking to capture another one media.
sip-reg-unreg: Try yo unregister another endpoint.
sip-bye-teardown: Use BYE teardown to end an active call.
sip-dos: Denial of service (DoS) protection mechanism stress test.
sip-dumb-fuzz: Dumb fuzzer for SIP protocol.

WEB
web-auto: Discover common web control panel of SIP servers in a host.
web-discover: Discover common web control panel of SIP servers in a host.
web-brute: Bruteforce credentials of a SIP server web panel.

MORE
shodan-host: Get indexed info of an IP address in SHODAN.
shodan-vulns': Find vulnerabilities and exploit of an specifig service version.
shodan-query: Use a customized SHODAN VoIP query.
shodan-download: Download an exploit.
passwords: Show common VoIP system default passwords..
geo-locate: Geolozalization of a host using Maxmind DB.
get-ext-ip: Get you external IP address (icanhazip).

ENVIRONMENT
clear: Clear the environment. (restart)
help: Print this info.
version: Print the version of this software.
quit'/'exit: Close the program.
```

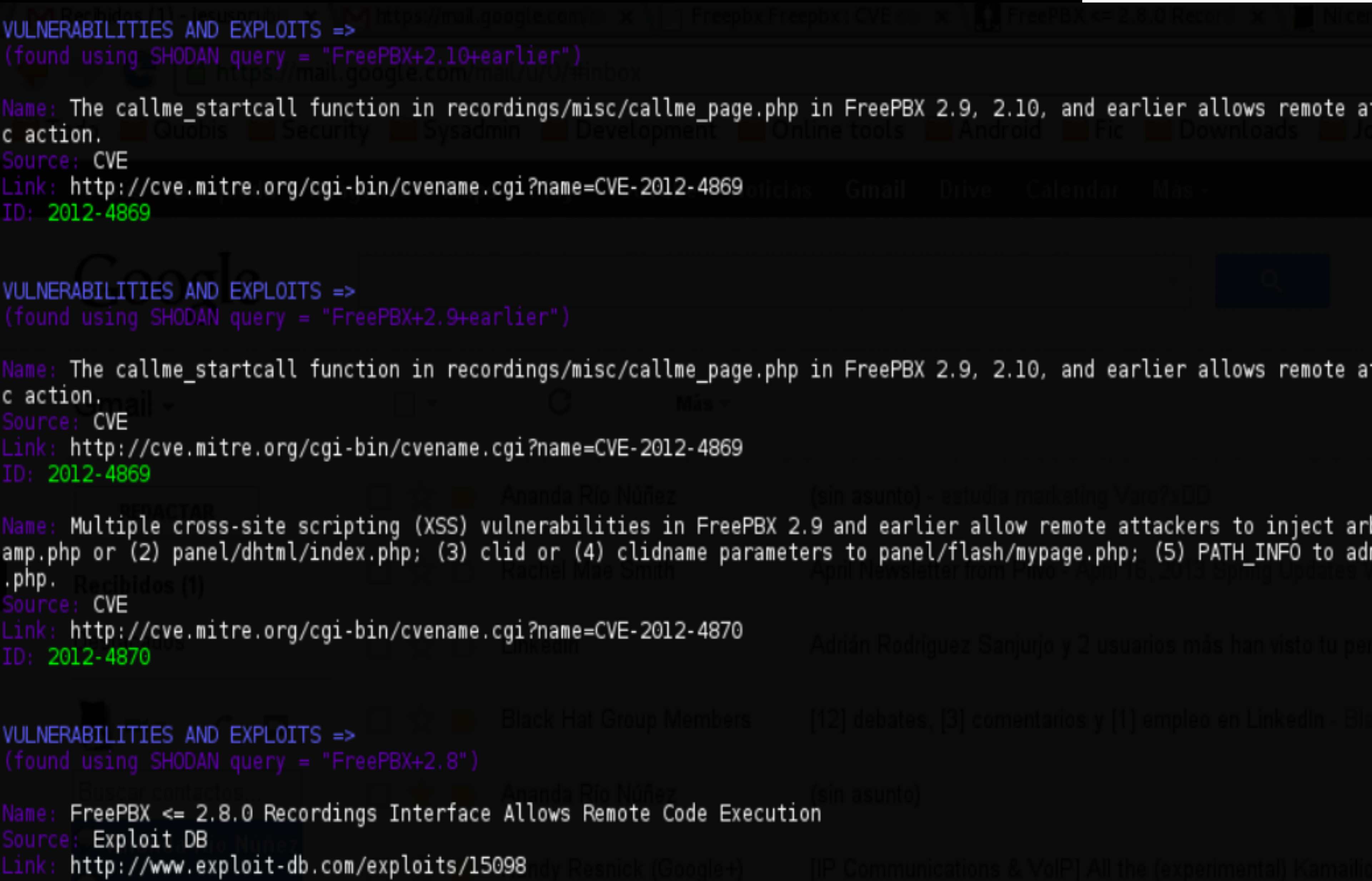
```
SIP
sip-auto: Automate SIP pentesting process.
sip-scan: Use SIP host/port scanning tool.
sip-brute-ext: Try to brute-force valid exte
sip-brute-ext-ast: Try to brute-force valid
sip-brute-pass: Try to brute-force the passw
sip-invite: Try know if a SIP server allows
sip-call-all: Call all endpoint in your LAN
```

Demo. Bluebox-ng 2



```
Bluebox-ng> sip-scan

>> Configure module:

* Target (192.168.122.202): 192.168.122.135

opt: UDP,TCP,TLS,WS,WSS
* Transport (UDP):

* Port (5060):

opt: tip: Use comand "get-ext-ip" to get you external IP automatically

* Source IP, SIP layer (random):

opt: REGISTER,INVITE,OPTIONS,MESSAGE,BYE,OK,CANCEL,ACK,Ringing,Busy Here,SUBSCRIBE,PUBLISH
* Type (OPTIONS):

FINGERPRINT =>

Service: FreePBX
Version: 2.8
Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 53.29.135.206:59106;branch=z9hG4bKfoxog92wxgktke297dmpbl3s25a5rk;received=192.168.122.1
From: 299 <sip:299@192.168.122.135>;tag=712wrpp0rb
To: 521 <sip:521@192.168.122.135>;tag=as2eb3e24b
Call-ID: ticf2innwzo4unmi@192.168.122.135
CSeq: 1 OPTIONS
Server: FPBX-2.8.1(1.8.7.0)
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
Contact: <sip:192.168.122.135:5060>
Accept: application/sdp
```

Demo. Bluebox-ng 3



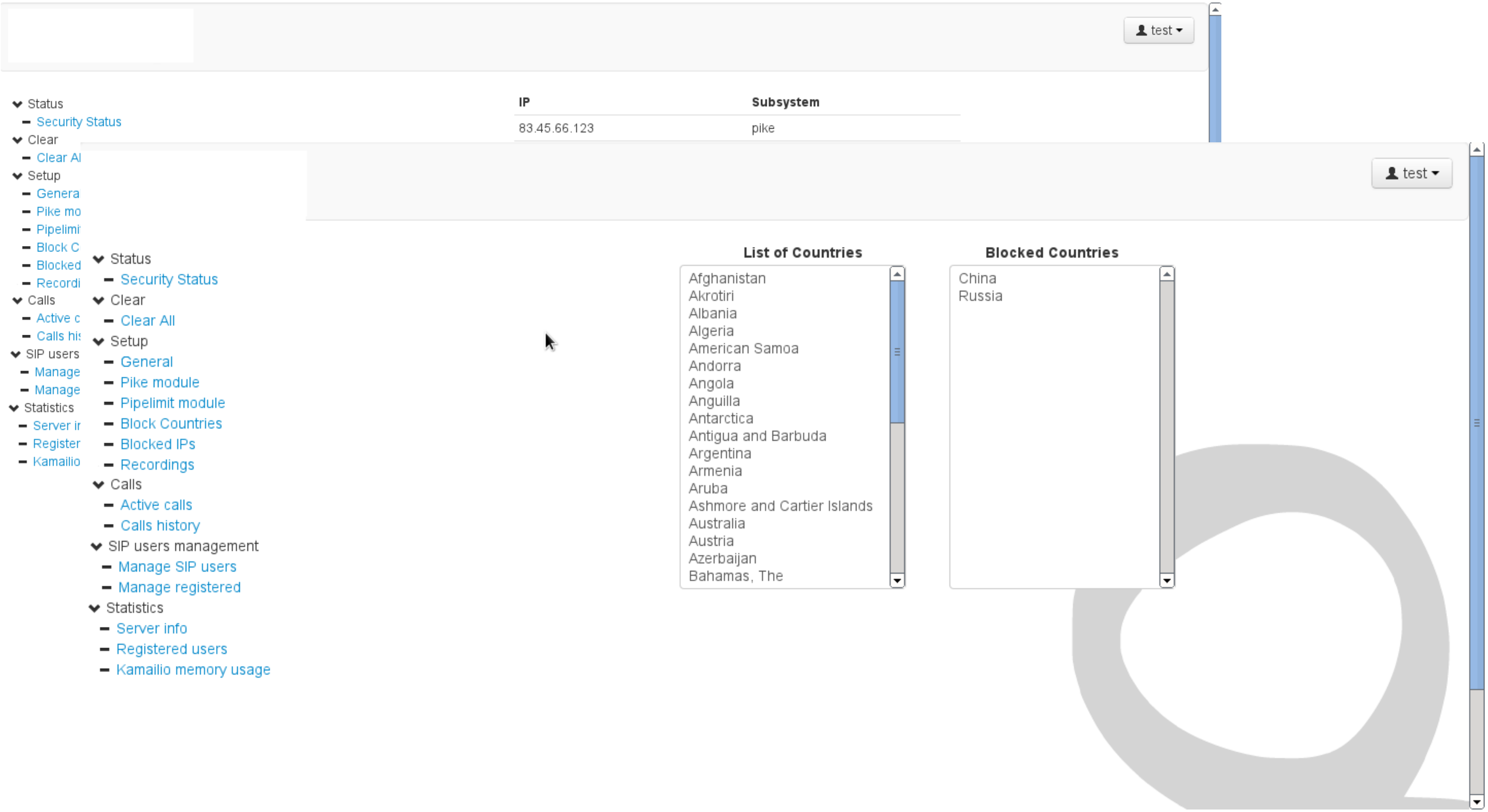
```
VULNERABILITIES AND EXPLOITS =>
(found using SHODAN query = "FreePBX+2.10+earlier")

Name: The callme_startcall function in recordings/misc/callme_page.php in FreePBX 2.9, 2.10, and earlier allows remote at
c action.
Source: CVE
Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4869
ID: 2012-4869


VULNERABILITIES AND EXPLOITS =>
(found using SHODAN query = "FreePBX+2.9+earlier")

Name: The callme_startcall function in recordings/misc/callme_page.php in FreePBX 2.9, 2.10, and earlier allows remote at
c action.
Source: CVE
Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4869
ID: 2012-4869

Name: Multiple cross-site scripting (XSS) vulnerabilities in FreePBX 2.9 and earlier allow remote attackers to inject arb
amp.php or (2) panel/dhtml/index.php; (3) clid or (4) clidname parameters to panel/flash/mypage.php; (5) PATH_INFO to adm
.php.
Source: CVE
Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4870
ID: 2012-4870


VULNERABILITIES AND EXPLOITS =>
(found using SHODAN query = "FreePBX+2.8")

Name: FreePBX <= 2.8.0 Recordings Interface Allows Remote Code Execution
Source: Exploit DB
Link: http://www.exploit-db.com/exploits/15098
```

Demo. Bluebox-ng roadmap

- Tor support
- More SIP modules
- SIP fuzzing (SIP Torture RFC)
- Eavesdropping
- CouchDB support (sessions)
- H.323 and IAX support
- Web common panels post-explotation (Pepelux research)
- A bit of command Kung Fu post-explotation
- RTP fuzzing.
- Advanced SIP fuzzing with Peach
- Reports generation
- Graphical user interface
- Windows support
- Include it in Debian.
- Include it in Kali GNU/Linux
- Team/multi-user support
- Complete documentation
- ...
- Any suggestion/piece of code ;) is appreciated

Countermeasurements. What we use

Do you accept VAF? ;) (VoIP Application Firewall)



IP	Subsystem
83.45.66.123	pike

List of Countries

Afghanistan
Akrotiri
Albania
Algeria
American Samoa
Andorra
Angola
Anguilla
Antarctica
Antigua and Barbuda
Argentina
Armenia
Aruba
Ashmore and Cartier Islands
Australia
Austria
Azerbaijan
Bahamas, The

Blocked Countries

China
Russia

Kamailio + Pike Module + Fail2Ban + Fixed ACL in Firewalls

References

- Manu Quintans & Frank Ruiz - "All Your Crimeware Are Belong To Us!" [RootedCON 2012]
- David Barroso - "Extorsiones mediante DDoS"
- Pedram Amini - "Mostrame la guita! Adventures in buying vulnerabilities" [Ekoparty 2009]
- Mark Collier & David Endler - "Hacking VoIP Exposed"
- Quobis Whitepaper - "Riegos actuales de la VoIP"
- http://nicerosniunos.blogspot.com.es/
- Quobis Labs - http://www.quobis.com/
- Planet Quobis - http://planet.quobis.com/

Questions?

¿?

Thanks!

Antón Román
CTO
@antonroman
anton.roman@quobis.com

Jesús Perez
Security Engineer
@jesusprubio
jesus.perez@quobis.com