Airmon-ng

Descrição

Este script pode ser usado para habilitar Modo Monitor em interfaces de placas wireless. Ele também pode ser usado para desligar (parar) tais interfaces. Digitar o comando **airmon-ng** sem parâmetros mostrará o estado da interface (status).

Uso

```
airmon-ng <start|stop> <interface> [canal]
```

Onde:

- <start|stop> indica se você quer iniciar (start) ou parar (stop) a interface. (Obrigatório)
- <interface> especifica a interface. (Obrigatório)
- [canal] opcionalmente configura a placa para o canal especificado.

Exemplos de Uso

Usos Típicos

Para iniciar wlan0 em modo monitor: **airmon-ng start wlan0**

Para iniciar wlan0 em modo monitor no canal 8: **airmon-ng start wlan0 8**

Para parar wlan0: **airmon-ng stop wlan0**

Para verificar o estado da interface (status): **airmon-ng**

Airodump-ng

Descrição

Airodump-ng é usado para captura de pacotes de frames brutos 802.11 e é particularmente apropriado para coletar IVs (Vetores de Inicialização) WEP com intuito de usá-los com o aircrack-ng. Se você tem um receptor GPS conectado ao computador, airodump-ng é capaz de registrar as coordenadas dos Access Points encontrados.

Suplementarmente, airodump-ng cria um arquivo de texto (também chamado de "dump") contendo os detalhes de todos os Access Points e clientes vistos.

Uso

Antes de executar o airodump-ng, inicie o script airmon-ng para listar as interfaces wireless detectadas.

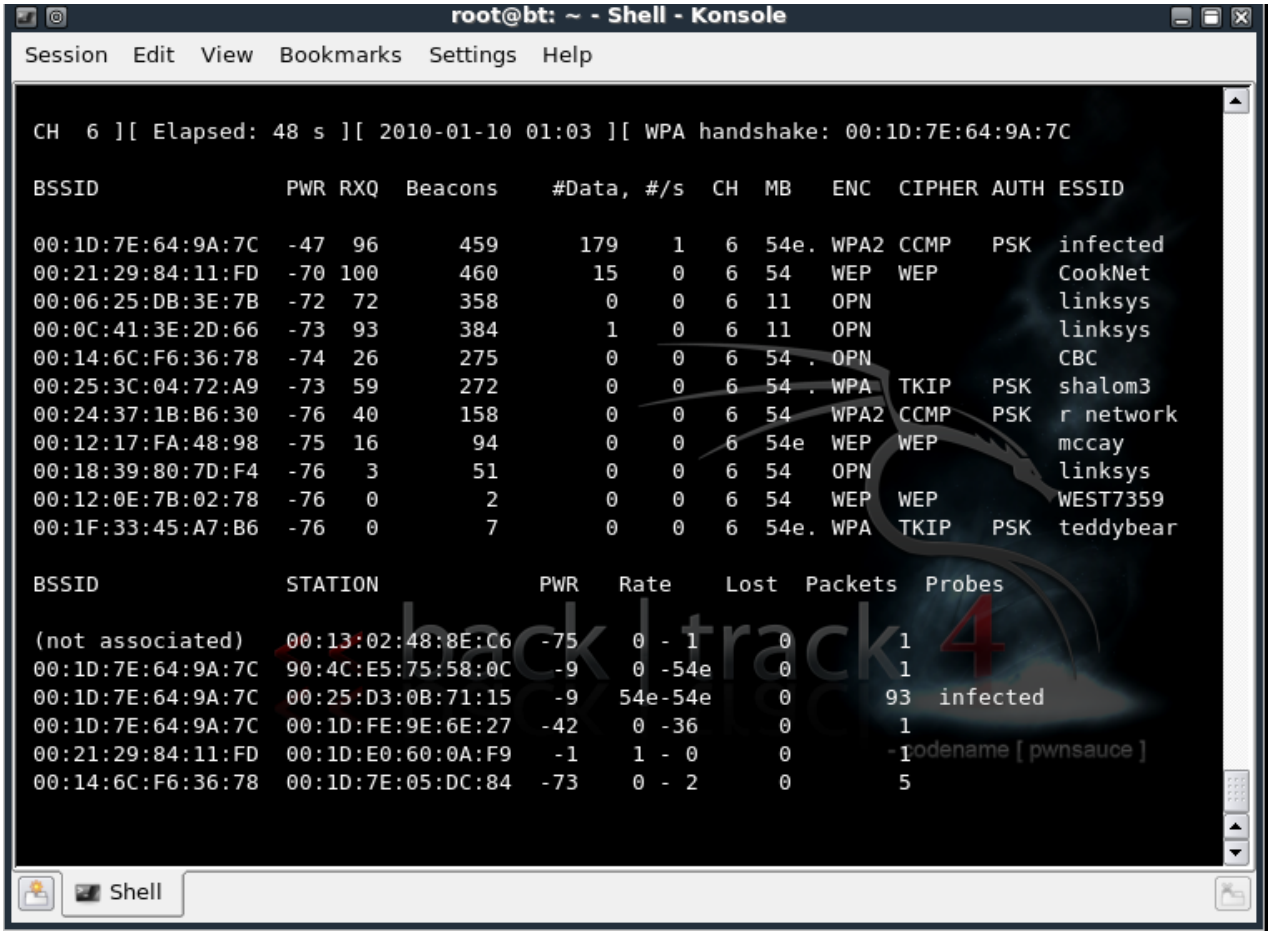
```
uso: airodump-ng <opções> <interface>[,<interface>,...]

Opções:
   --ivs             : Salva somente IVs capturados
   --gpsd            : Usa GPSd
   --write    <prefix> : Prefixo do arquivo dump
   -w                : mesmo que --write
   --beacons         : Grava todos os beacons em arquivo dump
   --update     <secs> : Mostra atraso de atualização em segundos
   --showack         : Apresenta as estatísticas ack/cts/rts
   -h                : Esconde estações conhecidas pelo --showack
   -f         <msecs> : Tempo em milisegundos entre canais alternando (saltos)
   --berlin     <secs> : Tempo antes da remoção do AP/cliente
                         da tela quando nenhum pacote a mais
                         for recebido (Padrão: 120 segundos).
   -r          <file> : Lê pacotes do arquivo especificado.

Opções de filtro:
   --encrypt   <suite> : Filtra APs pela criptografia (cifra)
   --netmask <netmask> : Filtra APs pela máscara de sub-rede
   --bssid     <bssid> : Filtra APs pelo BSSID
   -a                  : Filtra clientes não-associados

Por padrão, airodump-ng salta em canais 2.4GHz.
Você pode fazê-lo capturar em outro(s)/específico(s) canal(is) usando:
   --channel <channels>: Captura em canais específicos
   --band <abg>        : Banda na qual o airodump-ng deve saltar (a, b ou g)
   --cswitch  <method> : Configura o método de alternação dos canais
                0    : FIFO (padrão)
                1    : Round Robin
                2    : Salta no último
   -s                  : mesmo que --cswitch
   --help              : Mostra esta tela de uso do programa
```

Você pode converter arquivos .cap / .dump para o formato .ivs ou mesclá-los.

Dicas de Uso

Qual o significado dos campos apresentados pelo airodump-ng ?

Airodump-ng mostrará uma lista de Access Points detectados, e também uma lista de clientes conectados (“estações”). Aqui está um exemplo de uma captura de tela:



A primeira linha mostra o canal atual, tempo de execução decorrido, data atual e opcionalmente se um “aperto de mão” (handshake) WPA/WPA2 foi detectado. No exemplo acima, “WPA handshake: 00:1D:7E:64:9A:7C” indica que um *handshake* WPA/WPA2 foi capturado com sucesso para o BSSID.

Campo	Descrição
BSSID	Endereço MAC do Access Point. Na seção Client (Cliente), um BSSID com “(not associated)” significa que o cliente não está associado com qualquer AP.

Campo	Descrição
	Nesse192.168.100.76 estado desassociado, ele está procurando por um AP para conectar-se.
PWR	Nível de sinal apresentado pela placa. Seu significado depende do driver, mas quanto maior o sinal mais perto você fica do AP ou estação. Se o BSSID PWR for -1, então o driver não suporta relatório do nível de sinal. Se o PWR for -1 para um número limitado de estações, então isso é para um pacote que veio de um AP para o cliente mas as transmissões do cliente estão fora do alcance da sua placa. O que significa que você está escutando somente metade da comunicação. Se todos os clientes tiverem PWR como -1, então o driver não suporta relatório do nível de sinal.
RXQ	Qualidade de Recepção, medida pela porcentagem de pacotes (quadros de dados e de gerenciamento) recebidos com sucesso nos últimos 10 segundos. Ver nota abaixo para explicação mais detalhada.
Beacons	Número de pacotes de aviso enviados pelo AP. Cada Access Point manda por volta de 10 beacons por segundo na velocidade mais baixa (1M), então geralmente eles podem ser pegos de bem longe.
# Data	Número de pacotes de dados capturados (se WEP, contagem única de IVs), incluindo pacotes de difusão de dados.
#/s	Número de pacotes de dados por segundo medidos nos últimos 10 segundos.
CH	Número do Canal (capturados a partir dos pacotes beacon). Nota: às vezes pacotes de outros canais são capturados mesmo se o airodump-ng não estiver saltando canais, por causa da interferência de rádio.
MB	Velocidade máxima suportada pelo AP. Se MB = 11, é 802.11b; se MB = 22 é 802.11b+ e velocidades maiores são 802.11g. O ponto (após 54 acima) indica que preâmbulo curto - short preamble - é suportado.
ENC	Algoritmo de criptografia em uso. OPN = sem criptografia, “WEP?” = WEP ou maior (não há dados suficientes para escolher entre WEP e WPA/WPA2), WEP (sem o ponto de interrogação) indica WEP estático ou dinâmico, e WPA ou WPA2 se TKIP ou CCMP estiver presente.
CIPHER	A cifra detectada. Um desses: CCMP, WRAP, TKIP, WEP, WEP40 ou WEP104. Não é regra, mas TKIP é tipicamente usado com WPA e CCMP é tipicamente usado com WPA2. WEP40 é mostrado quando o índice da chave é maior que 0. O padrão define que o índice pode ser 0-3 para 40bit e deve ser 0 para 104bit.
AUTH	O protocolo de autenticação usado. Um desses: MGT (WPA/WPA2 usando um servidor de autenticação separado), SKA (Chave compartilhada para WEP), PSK (Chave pré-compartilhada para WPA/WPA2), ou OPN (Aberto para WEP).
ESSID	O tão chamado “SSID”, que pode estar vazio, se o esconder SSID estiver ativado. Nesse caso, airodump-ng tentará recuperar o SSID de respostas de sondagem (probe responses) e pedidos de associação (association requests).

Campo	Descrição
STATION	Endereço MAC de cada estação associada ou estações procurando por um AP para se conectarem. Clientes não associados no momento possuem um BSSID com “(not associated)”.
Lost	O número de pacotes de dados perdidos nos últimos 10 segundos, baseado no número de sequência. Ver nota abaixo para uma explicação mais detalhada.
Packets	O número de pacotes de dados enviados por um cliente.
Probes	Os ESSIDs sondados pelo cliente. Estas são as redes que o cliente está tentando se conectar se não estiver conectado no momento.

Aireplay-ng

Descrição

Aireplay-ng é usado para injetar frames.
A função principal é gerar tráfego para uso posterior no aircrack-ng para quebrar chaves WEP e WPA-PSK. Existem ataques diferentes que podem causar desautenticações com o propósito de capturar dados de *handshake* WPA, autenticações falsas, repetição de pacote interativo, injeção de ARP Request forjados e reinjeção de ARP Request. Com a ferramenta packetforge-ng é possível criar frames arbitrários.

A maioria dos drivers precisam ser de 'patch' para poder realizar injeção de pacotes, não esqueça de ler Instalando drivers.

Uso dos ataques

Atualmente são implementados múltiplos ataques diferentes:

- **Ataque 0: Desautenticação**
- Ataque 1: Autenticação Falsa
- Ataque 2: Replay (Repetição) de Pacote Interativo
- Ataque 3: Ataque de Replay de ARP Request
- Ataque 4: Ataque KoreK chopchop
- Ataque 5: Ataque de fragmentação
- Ataque 9: Teste de Injeção

Uso

Esta seção fornece uma visão geral. Nem todas as opções podem ser usadas em todos os ataques. Veja os detalhes do ataque específico para detalhes relevantes.
Uso:

```
aireplay-ng <opções> <replay interface>
```

Para todos os ataques, com exceção da desautenticação e autenticação falsa, você pode usar os seguintes filtros para limitar quais pacotes serão apresentados no ataque em particular. A opção de filtro mais comumente usada é a “-b” para selecionar um Access Point (AP) específico. Para uso normal, o “-b” é o único que você usa.
Opções de Filtro:

- -b bssid : Endereço MAC, Access Point
- -d dmac : Endereço MAC, Destino
- -s smac : Endereço MAC, Origem
- -m len : tamanho mínimo do pacote
- -n len : tamanho máximo do pacote
- -u type : controle de frame, tipo campo
- -v subt : controle de frame, subtipo campo
- -t tods : controle de frame, Para DS bit
- -f fromds : controle de frame, De DS bit
- -w iswep : controle de frame, WEP bit

Quando repetindo (injetando) pacotes, as opções a seguir podem ser usadas. Tenha em mente que nem todas as opções são relevantes para cada ataque. A documentação do ataque fornece exemplos das opções relevantes.

Opções de Replay:
- -x nbpps : número de pacotes por segundo
- -p fctrl : configurar a palavra do controle de frame (hex)
- -a bssid : configurar o endereço MAC do Access Point
- -c dmac : configurar Destino Endereço MAC
- -h smac : configurar Origem Endereço MAC
- -e essid : ataque de autenticação falsa : configurar SSID do AP alvo
- -j : ataque ARP Replau : injetar pacotes FromDS
- -g value : mudar tamanho do ring buffer (padrão: 8)
- -k IP : configurar o IP de destino em fragmentos
- -l IP : configurar o IP da origem em fragmentos
- -o npckts : número de pacotes por burst/rajada (-1)
- -q sec : segundos entre keep-alives (-1)
- -y prga : fluxo de chave para autenticação de chave compatilhada

Os ataques podem obter pacotes para repetir (replay) de duas origens. A primeira sendo um fluxo ativo de pacotes da sua placa wireless. A segunda sendo de um arquivo pcap. Formato Pcap padrão (Packet CAPture ou CAPtura de Pacote, associado à biblioteca libpcap http://www.tcpdump.org), é reconhecida pela maioria das ferramentas open-source e comerciais de análise e captura de tráfego. Leitura de arquivo é geralmente uma característica despercebida do arieplay-ng. Isso permite que você leia pacotes de outras sessões de captura ou, quase sempre, vários ataques geram arquivos pcap para fácil reutilização.

Opções da Origem:

- -i iface : captura pacotes desta interface
- -r file : extrai pacotes deste arquivo pcap

Isso é como você especifica em qual modo (ataque) o programa irá operar. Dependendo do modo nem todas as opções acima são aplicáveis.
Modos de Ataque (Números ainda podem ser usados):

- - -deauth count : desautenticar 1 ou todas as estações (-0)
- - -fakeauth delay : autenticação falsa com AP (-1)
- - -interactive : seleção de frame interativo (-2)
- - -arpreplay : replay de ARP Request padrão (-3)
- - -chopchop : decifrar/fatiar(chopchop) pacote WEP (-4)
- - -fragment : gera fluxo de chaves válido (-5)
- - -test : teste de injeção (-9)

Uso

Ataque de desassociação:
aireplay-ng -0 N -a XX:XX:XX:XX:XX:XX -c YY:YY:YY:YY:YY:YY interface

-0: Indica que vamos fazer um ataque do tipo "0" o de desassociação de cliente.

N: É um número. Indicamos quantos pacotes de desassociação serão enviados.

-a XX:XX:XX:XX:XX:XX: “-a” Indica o MAC do AP.

-c YY:YY:YY:YY:YY:YY: "-c" Indica o MAC do cliente.

Aircrack-ng

Descrição

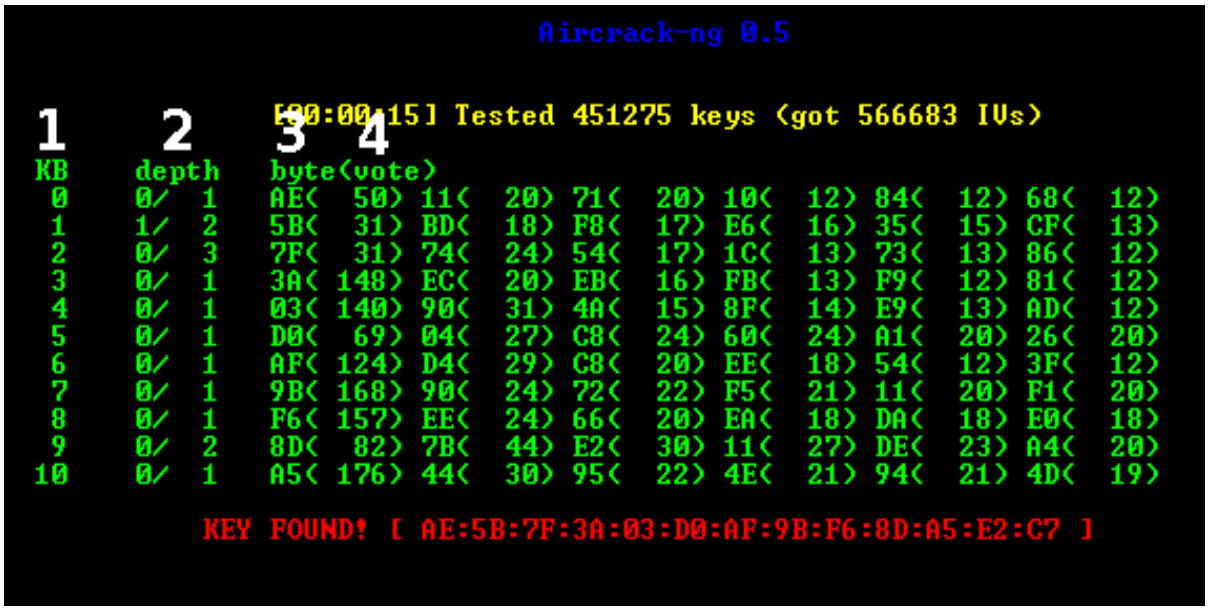
Aircrack-ng é um programa para quebrar chaves WEP e WPA/WPA2-PSK do IEEE 802.11.

Aircrack-ng pode recuperar a chave WEP, uma vez que um número suficiente de pacotes criptografados sejam capturados com o airodump-ng. Esta parte do pacote Aircrack-ng determina a chave WEP usando dois métodos fundamentais. O primeiro método é por abordagem PTW (Pyshkin, Tews, Weinmann). A principal vantagem da abordagem PTW é que pouquíssimos pacotes de dados são necessários para quebrar a chave WEP. O segundo método é o método FMS/KoreK. O método FMS/KoreK incorpora vários ataques estatísticos para descobrir a chave WEP e usa esses ataques em combinação com força-bruta.

Adicionalmente, o programa oferece um método de dicionário para determinar a chave WEP. Para quebrar chaves pré-compartilhadas WPA/WPA2, somente o método de dicionário é utilizado.

Captura de Tela

LEGENDA
1 = Byte da chave
2 = Profundidade da procura da chave atual
3 = Byte que os IVs vazaram
4 = Votos indicando que este byte está correto



Como funciona?

O primeiro método é o método PTW (Pyshkin, Tews, Weinmann). O método PTW está completamente descrito no artigo encontrado neste web site. Em 2005, Andreas Klein apresentou uma outra análise da cifra de fluxo RC4. Klein mostrou que há mais relações entre o fluxo de chave RC4 e a chave do que nas relações encontradas por Fluhrer, Mantin, e Shamir, e essas podem ser utilizadas em conjunto para quebrar o WEP. O método PTW faz extensão do ataque do Klein e otimiza-o para uso contra o WEP. Ele basicamente usa técnicas FMS melhoradas, descritas na seção seguinte. Uma restrição importante em particular é que somente funciona com pacotes ARP Request/Reply e não pode ser empregado contra outro tráfego.

O segundo método é o método FMS/Korek, o qual incorpora múltiplas técnicas.

Os Documentos de Técnicas, na página de links, lista vários trabalhos e artigos que descrevem essas técnicas detalhadamente e a matemática por detrás delas.

Neste método várias técnicas são combinadas para quebrar a chave WEP:

- Ataques FMS (Fluhrer, Mantin, Shamir) - técnicas estatísticas
- Ataques Korek - técnicas estatísticas
- Força-Bruta

Quando usar técnicas estatísticas para quebrar a chave WEP, cada byte da chave é manipulada individualmente. Usando matemática estatística, a possibilidade de um certo byte na chave ser adivinhado corretamente sobe para 15% quando o Vetor de Inicialização (IV) correto é capturado para um byte de chave específico. Essencialmente, certos IVs “vazam” a chave WEP secreta para bytes de chaves específicos. Esta é a base fundamental das técnicas de estatística.

Por meio do uso de uma série de testes estatísticos chamados de ataques FMS e Korek, votos são acumulados para chaves prováveis para cada byte de chave da chave WEP secreta. Ataques diferentes têm um número diferente de votos associados a eles, já que a probabilidade de cada ataque render a resposta certa varia matematicamente. Quanto mais votos um valor particular de chave em potencial acumular, mais provável será de estar correto. Para cada byte de chave, a tela mostra a provável chave secreta e o número de votos que acumulou até o momento. Nem precisa dizer, a chave secreta com o maior

número de votos tem maior probabilidade de estar correta, mas não é garantido. Aircrack-ng testará em seqüência a chave para confirmá-la.

Observando um exemplo tornará isso mais claro. Na captura de tela acima, você pode ver que no byte de chave 0, o byte 0xAE coletou alguns votos, 50 nesse caso. Então, matematicamente, é mais provável que a chave comece com AE do que com 11 (o segundo na mesma linha), que é quase metade da probabilidade. Isso explica por quê quanto mais dados são disponibilizados, maiores são as chances de o aircrack-ng determinar a chave WEP secreta.

Entretanto, a abordagem estatística só pode ser levá-lo até aqui. A idéia é chegar até esse ponto com estatística e então usar força-bruta para terminar o trabalho. Aircrack-ng usa força-bruta nas chaves mais prováveis, na verdade, para determinar a chave WEP secreta.

Aqui é onde o fator de correção entra. Basicamente o fator de correção diz ao aircrack-ng como fazer força-bruta de modo mais amplo. É como arremessar uma bola em um campo e dizer a alguém que a bola está em algum lugar entre 0 e 10 metros de distância. Contra dizer que a bola está em algum lugar entre 0 e 100 metros de distância. O cenário de 100 metros levará mais tempo para procurar a bola do que o de 10 metros, mas você terá mais chances de encontrar a bola com a procura mais ampla. É uma troca entre a duração do tempo e a propabilidade de encontrar a chave WEP secreta.

Por exemplo, se você dizer ao aircrack-ng para usar um fator de correção 2, ele vai usar os votos do byte mais provável, e verificar todas as outras possibilidades que são, pelo menos, metade da possibilidade desse byte em uma base de força-bruta. Quanto maior for o fator de correção, mais possibilidades o aircrack-ng tentará em uma base de força-bruta.

Tenha em mente que quanto maior for o fator de correção, aumenta tremendamente o número de chaves secretas a tentar, e conseqüentemente o tempo restante também aumenta. Portanto, com mais dados disponíveis, a necessidade de força-bruta - que requer muito tempo e muito da CPU - pode ser minimizada.

No final, é tudo só matemática “simples” e força-bruta!

Para quebrar chaves WEP, um método de dicionário é incluído também. Para WEP, você pode usar ou o método estatístico descrito acima ou o método de dicionário, não os dois

ao mesmo tempo. Com o método de dicionário, você primeiro cria um arquivo ou com chaves ASCII ou com chaves hexadecimais. Um único arquivo só pode conter um tipo, e não uma mistura dos dois. Ele é então utilizado como entrada no aircrack-ng, e o programa testa cada chave para determinar se está correta ou não.

As técnicas e abordagens acima não funcionam para chaves pré-compartilhadas WPA/WPA2. O único jeito de quebrar essas chaves pré-compatilhadas é por meio de um ataque de dicionário. Essa capacidade está incluída também no aircrack-ng.

Com chaves pré-compartilhadas, o cliente e o Access Point estabelecem material de chaveamento para ser usado no início de suas comunicações, quando o cliente primeiro associa com o Access Point. Há um “aperto de mão de quatro vias”, mais conhecido como four-way handshake, entre o cliente e o Access Point. Airodump-ng pode capturar esse four-way handshake. Utilizando entrada de uma lista de palavras(wordlist) providenciada, o aircrack-ng duplica o four-way handshake para determinar se uma entrada em particular da lista de palavras iguala-se aos resultados do four-way handshake. Se igualarem, então a chave pré-compartilhada foi identificada com êxito.

Deve-se notar que este processo é muito intensivo computacionalmente, e na prática, chaves pré-compartilhadas incomuns ou muito longas são improváveis de se determinar. Uma lista de palavras de qualidade te dará os melhores resultados. Outro caminho é usar uma ferramenta, como John The Ripper, para gerar advinhações de senhas, que servem no aircrack-ng.

Explicação do Campo de Profundidade e Fator de Correção

A melhor explicação é um exemplo. Nós observaremos um byte específico. Todos os bytes são processados da mesma maneira.

Você tem os votos como na captura de tela abaixo. Para o primeiro byte, eles se parecem com isso:

```
AE(50) 11(20) 71(20) 10(12) 84(12)
```

AE, 11, 71, 10 e 84 formam a possível chave secreta para o byte de chave 0. Os números em parênteses são os votos que cada chave secreta possível acumulou até o momento.

Agora se você decidir usar um fator de correção 3, o aircrack-ng pega o voto do byte mais possível, no caso o byte AE(50), e o divide por 3:

```
50 / 3 = 16.666666
```

Aircrack-ng testará (força-bruta) todas as chaves possíveis com um voto maior que 16.6666, resultando em

```
AE, 11, 71
```

sendo testados, então nós temos uma profundidade total de três:

```
0 / 3     AE(50) 11(20) 71(20) 10(12) 84(12)
```

Quando o aircrack-ng está testando chaves com AE, ele mostra 0 / 3, se tiver todas as chaves testadas com aquele byte, ele muda para o próximo (11 nesse caso) e apresenta:

```
1 / 3     11(20) 71(20) 10(12) 84(12)
```

Resumindo:

Antes…

```
0 / 3     AE(50) 11(20) 71(20) 10(12) 84(12)
```

depois…

```
1 / 3     11(20) 71(20) 10(12) 84(12) ??(??)
```

E por aí vai…

```
2 / 3     71(20) 10(12) 84(12) ??(??) ??(??)
```

Uso

```
aircrack-ng [opções] <arquivo(s) capturado(s)>
```

Você pode especificar vários arquivos de entrada (em formato .cap ou .ivs). Você pode também executar ambos airodump-ng e aircrack-ng ao mesmo tempo: aircrack-ng fará atualização automática quando novos IVs estiverem disponíveis.

Aqui está um resumo de todas as opções disponíveis:

Opção	Parâmetro	Descrição
-a	modo	Força modo de ataque (1 = WEP estático, 2 = WPA/WPA2-PSK).
-e	essid	Se usado, todos os IVs de redes com o mesmo ESSID serão utilizados. Essa opção é também requisitada para quebrar WPA/WPA2-PSK se o ESSID não está em broadcast (escondido).
-b	bssid	Seleciona a rede alvo baseada no endereço MAC do Access Point.
-p	número de CPUs	Em sistemas SMP: número de CPUs a utilizar.
-q	*nenhum*	Habilita modo quieto (não mostra status até que a chave seja encontrada, ou não).
-c	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres alfa-

Opção	Parâmetro	Descrição
		numéricos somente (0x20 - 0x7F).
-t	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres hexadecimais codificados em binários.
-h	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres numéricos (0x30-0x39). Essas chaves são usadas por padrão na maioria dos Fritz!BOXes.
-d	início	[Quebra WEP] Configura o início da chave WEP (em hexadecimal), para propósitos de depuração.
-m	endereço MAC	[Quebra WEP] Endereço MAC para filtrar pacotes de dados WEP. Alternativamente, especifique **-m ff:ff:ff:ff:ff:ff** para usar cada um e todos IVs, independente da rede.
-n	número de bits	[Quebra WEP] Especifica o tamanho da chave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. O valor padrão é 128.
-i	índice	[Quebra WEP] Apenas mantém os IVs que têm esse índice de chave (1 a 4). O comportamento padrão é ignorar o índice de chave (key index).
-f	fator de correção	[Quebra WEP] Por padrão, esse parâmetro é ajustado pra 2 para WEP de 104-bit e pra 5 para WEP de 40-bit. Especifique um valor mais alto para aumentar o nível de força-bruta: quebra da chave levará mais tempo, mas terá mais probabilidade de êxito.
-k	Korek	[Quebra WEP] Existem 17 ataques estatísticos Korek. Às vezes um ataque cria um enorme falso-positivo que previne a chave de ser encontrada, mesmo com muitos IVs. Tente -k 1, -k 2, ... -k 17 para desabilitar cada ataque seletivamente.
-x/-x0	*nenhum*	[Quebra WEP] Disabilita força-bruta dos últimos bytes de chave.
-x1	*nenhum*	[Quebra WEP] Habilita força-bruta do último byte de chave. (padrão)
-x2	*nenhum*	[Quebra WEP] Habilita força-bruta dos últimos 2 bytes de chave.
-X	*nenhum*	[Quebra WEP] Disabilita multi-processamento da força-bruta (somente SMP).
-y	*nenhum*	[Quebra WEP] Este é um ataque de força-bruta único, experimental, que apenas deve ser usado quando o modo de ataque padrão falhar com mais de um milhão de IVs.
-w	palavras	[Quebra WPA] Caminho de uma lista de palavras - wordlist, ou “-” sem as aspas para padronizar em (stdin).
-z	*nenhum*	Inicia com o método PTW de quebra de chaves WEP.

Exemplos de Uso

WEP

O caso mais simples é quebrar uma chave WEP. Se você quer tentar isso por si próprio.

```
aircrack-ng 128bit.ivs
```

Onde:

- **128bit.ivs** é o nome do arquivo contendo IVs.

O programa responde:

```
Opening 128bit.ivs
Read 684002 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:04:57:9B                            WEP (684002 IVs)

Choosing first network as target.
```

Se existirem várias redes contidas no arquivo, então você tem a opção de selecionar qual rede você quer. Por padrão, o aircrack-ng assume a criptografia de 128 bits.

O processo de quebrar começa, e uma vez quebrado, aqui está como a tela se parece:

```
   Aircrack-ng 0.7 r130

   [00:00:10] Tested 77 keys (got 684002 IVs)

 KB    depth   byte(vote)
  0    0/  1   AE( 199) 29(  27) 2D(  13) 7C(  12) FE(  12)
FF(   6) 39(   5) 2C(   3) 00(   0) 08(   0)
  1    0/  3   66(  41) F1(  33) 4C(  23) 00(  19) 9F(  19)
C7(  18) 64(   9) 7A(   9) 7B(   9) F6(   9)
  2    0/  2   5C(  89) 52(  60) E3(  22) 10(  20) F3(  18)
8B(  15) 8E(  15) 14(  13) D2(  11) 47(  10)
  3    0/  1   FD( 375) 81(  40) 1D(  26) 99(  26) D2(  23)
33(  20) 2C(  19) 05(  17) 0B(  17) 35(  17)
  4    0/  2   24( 130) 87( 110) 7B(  32) 4F(  25) D7(  20)
F4(  18) 17(  15) 8A(  15) CE(  15) E1(  15)
  5    0/  1   E3( 222) 4F(  46) 40(  45) 7F(  28) DB(  27)
E0(  27) 5B(  25) 71(  25) 8A(  25) 65(  23)
  6    0/  1   92( 208) 63(  58) 54(  51) 64(  35) 51(  26)
53(  25) 75(  20) 0E(  18) 7D(  18) D9(  18)
  7    0/  1   A9( 220) B8(  51) 4B(  41) 1B(  39) 3B(  23)
9B(  23) FA(  23) 63(  22) 2D(  19) 1A(  17)
  8    0/  1   14(1106) C1( 118) 04(  41) 13(  30) 43(  28)
99(  25) 79(  20) B1(  17) 86(  15) 97(  15)
  9    0/  1   39( 540) 08(  95) E4(  87) E2(  79) E5(  59)
0A(  44) CC(  35) 02(  32) C7(  31) 6C(  30)
 10    0/  1   D4( 372) 9E(  68) A0(  64) 9F(  55) DB(  51)
38(  40) 9D(  40) 52(  39) A1(  38) 54(  36)
 11    0/  1   27( 334) BC(  58) F1(  44) BE(  42) 79(  39)
3B(  37) E1(  34) E2(  34) 31(  33) BF(  33)

           KEY FOUND! [ AE:66:5C:FD:24:E3:92:A9:14:39:D4:27:4B ]
```

Essa chave pode então ser usada para conectar-se à rede.

A seguir, nós observamos a quebra de WEP com um dicionário. Para conseguir fazer isso nós precisamos de arquivos de dicionário com chaves ASCII ou hexadecimais para testá-las. Lembre-se: um único arquivo só pode ter chaves ou ASCII ou hexadecimais nele, não ambos.

Chaves WEP podem ser inseridas em haxadecimal ou ASCII. A tabela a seguir descreve quantos caracteres de cada tipo são necessários nos seus arquivos.

Tamanho da chave WEP em bits	Caracteres Hexadecimais	Caracteres ASCII
64	10	5
128	26	13
152	32	16
256	58	29

Exemplo de chave ASCII de 64 bits: “ABCDE”
Exemplo de chave hexadecimal de 64 bits: “12:34:56:78:90” (Note o “:” a cada dois caracteres.)
Exemplo de chave ASCII de 128 bits: “ABCDEABCDEABC”
Exemplo de chave hexadecimal de 128 bits: “12:34:56:78:90:12:34:56:78:90:12:34:56”

Para quebrar uma chave WEP de 64 bits por dicionário:

```
aircrack-ng -w h:hex.txt,ascii.txt -a 1 -n 64 -e teddy wep10-01.cap
```

Onde:

- **-w h:hex.txt,ascii.txt** é a lista de arquivos a usar. Para arquivos contendo valores hexadecimais, você precisa colocar um “h:” na frente do nome do arquivo.
- **-a 1** informa que a chave é WEP
- **-n 64** informa que a chave tem 64 bits. Altere isso para o tamanho de chave que se ajusta aos arquivos de dicionário.
- **-e teddy** é para selecionar opcionalmente o Access Point. Você poderia também usar a opção “-b” para escolher baseado no endereço MAC.
- **wep10-01.cap** é o nome do arquivo contendo os dados. Pode ser o pacote completo ou um arquivo contendo apenas IVs. Precisa conter um mínimo de quatro IVs.
-

Aqui está um exemplo do resultado final:

```
                                                Aircrack-ng 0.7 r247
```

```
                              [00:00:00] Tested 2 keys (got 13 IVs)

 KB    depth   byte(vote)
  0    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  1    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  2    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  3    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
  4    0/  0   00(   0) 00(   0) 00(   0) 00(   0) 00(   0)
00(   0) 00(   0) 00(   0) 00(   0) 00(   0)

                         KEY FOUND! [ 12:34:56:78:90 ]
      Probability: 100%
```

Vamos dar uma olhada em um exemplo de ataque PTW. Lembre-se que esse método requer pacotes ARP Request/Reply como entrada. Precisa ser o pacote completo, e não somente os IVs. Isso significa que a opção “– ivs” não pode ser utilizada quando estiver executando o airodump-ng. De mesmo modo, somente funciona para criptografia WEP de 64 e 128 bits.

Digite o seguinte comando:

```
aircrack-ng -z ptw*.cap
```

Onde:

- **-z** significa usar a metodologia PTW para quebrar a chave WEP.
- **ptw*.cap** são os arquivos capturados a serem usados.

O sistema responde:

```
Opening ptw-01.cap
Read 171721 packets.

#  BSSID              ESSID                     Encryption
1  00:14:6C:7E:40:80  teddy                     WEP (30680 IVs)
Choosing first network as target.
```

Então:

```
          Aircrack-ng 0.9
          [00:01:18] Tested 0/140000 keys (got 30680 IVs)
KB    depth   byte(vote)
 0    0/  1   12( 170) 35( 152) AA( 146) 17( 145) 86( 143)
F0( 143) AE( 142) C5( 142) D4( 142) 50( 140)
 1    0/  1   34( 163) BB( 160) CF( 147) 59( 146) 39( 143)
47( 142) 42( 139) 3D( 137) 7F( 137) 18( 136)
 2    0/  1   56( 162) E9( 147) 1E( 146) 32( 146) 6E( 145)
79( 143) E7( 142) EB( 142) 75( 141) 31( 140)
 3    0/  1   78( 158) 13( 156) 01( 152) 5F( 151) 28( 149)
59( 145) FC( 145) 7E( 143) 76( 142) 92( 142)
 4    0/  1   90( 183) 8B( 156) D7( 148) E0( 146) 18( 145)
33( 145) 96( 144) 2B( 143) 88( 143) 41( 141)

   KEY FOUND! [ 12:34:56:78:90 ]
     Decrypted correctly: 100%
```

WPA

Agora vamos para quebra de frases-senha (passphrases) WPA/WPA2. Aircrack-ng pode quebrar ambos os tipos.

```
aircrack-ng -w password.lst *.cap
```

Onde:

- **-w password.lst** é o nome do arquivo de senha. Lembre-se de especificar o caminho completo se o arquivo não estiver localizado no mesmo diretório.
- ***.cap** é o nome do grupo de arquivos contendo os pacotes capturados. Observe que neste caso nós usamos o curinga '*' para incluir vários arquivos.

O programa responde:

```
Opening wpa2.eapol.cap
Opening wpa.cap
Read 18 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)
2  00:0D:93:EB:B0:8C  test                      WPA (1 handshake)

Index number of target network ?
```

Note que neste caso, já que existem múltiplas redes, nós precisamos selecionar qual rede atacar. Nós selecionamos a número 2. O programa então responde:

```
                                Aircrack-ng 0.7 r130


                    [00:00:03] 230 keys tested (73.41 k/s)


                            KEY FOUND! [ biscotte ]


    Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85
D6
                     39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24
EE
```

```
    Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2
49
                     73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE
08
                     AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67
97
                     D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62
CD

    EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60
BD
```

Agora você tem a frase-chave (passphrase) e pode conectar-se à rede.

Airbase-ng

Um dos ataques mais eficientes e de grande potencial a clientes de uma WLAN, é o que envolve o uso de pontos de acesso piratas, conhecidos como Rogue Access Point (Rogue APs).

Geralmente esse tipo de ataque acontece quando em um determinado local, uma determinada rede wireless tem seu sinal enfraquecido, o então atacante cria uma rede wireless com o mesmo SSID e BSSID e compartilha a conexão com a internet através de um 3G, por exemplo, ou até mesmo da própria rede a ser pirateada, onde se utiliza uma antena de maior ganho para alcançar o sinal e posteriormente distribuir.

Como o AP é a máquina do atacante o mesmo utiliza-se de software do tipo sniffer, para capturar informações dos clientes associados ao AP pirata.

Outro ataque é o chamado Caffe Latte que será descrito mais abaixo.

Caffe Latte

O ataque Caffe Latte é direcionado a clientes de redes sem fio, e não aos Access points. Ele é assim denominado porque pode ser conduzido enquanto um cliente de uma rede protegida pelo WEP está tomando um café com leite usando seu notebook.

O conceito do ataque é bem simples. Os notebooks de clientes de redes que usam o WEP guardam em seu chaveiro a chave da rede. A chave não é enviada para o Access point, porém ela é utilizada para encriptar o desafio enviado por ele.

O ataque então consiste de criar um access point falso com o endereço MAC e o nome ESSID do access point que o cliente conhece. O sistema operacional do notebook do cliente o reconhece e tenta conectar a ele automaticamente. Um desafio é enviado e o cliente o encripta utilizando a chave legítima (de onde vários bytes do RC4 podem ser obtidos pois o desafio foi criado pelo atacante). O access point falso aceita o cliente (mesmo sem verificar a chave) e utiliza pacotes ARP enviados pelo mesmo para realizar injeção e captura de pacotes como seria feito com um ataque convencional. Tendo os pacotes basta usar o mesmo aircrack-ng para obter a chave. Todo o ataque leva menos de 6 minutos.

Como usar:

```
airbase-ng -c 9 -e SSID -L -W 1 wlan0
```

Onde:

- -c 9 canal
- -e SSID
- -L especifica o tipo de ataque caffe latte
- -W 1 força o beacons para especificar WEP
- wlan0 especifica a interface wlan0

O sistema responde:

```
 15:08:31  Created tap interface at0
15:13:38  Got 140 bytes keystream: 00:0F:B5:88:AC:82
15:13:38  SKA from 00:0F:B5:88:AC:82
15:13:38  Client 00:0F:B5:88:AC:82 associated to ESSID: "teddy"
```

Uma outra tela execute:

```
airodump-ng -c 9 wlan0
```

Onde:

- -c 9 canal
- wlan0 especifica a interface

Tela confirmando o início do ataque:

```
H  9 ][ Elapsed: 9 mins ][ 2008-03-12 15:13 ][ 140 bytes keystream:
00:C0:CA:19:F9:65

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

```
 00:C0:CA:19:F9:65   87  92     5310        0    0   9  54  WEP
WEP     SKA  teddy

 BSSID              STATION            PWR   Rate  Lost  Packets
Probes

 00:C0:CA:19:F9:65  00:0F:B5:88:AC:82   83   0- 1     0     4096
teddy
```

Como alternativa, use a opção "-F <file nome do prefixo>” no airbase-ng para escrever diretamente um arquivo de captura em vez de usar airodump-ng.