TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 16. Hacking Wireless Networks

Módulo 17. Hacking Mobile Applications

Módulo 18. IoT & OT Hacking

Módulo 19. Cloud Computing

Módulo 20. Cryptography

Conceitos de redes Wireless:

Uma rede sem fios refere-se a uma rede de computador que não está ligado por qualquer tipo de cabo. Em redes sem fio, a transmissão é possível através do sistema de transmissão de ondas de rádio. Isso geralmente ocorre na camada física da estrutura de rede. Mudanças fundamentais para a criação de redes de dados e de telecomunicações estão ocorrendo com a revolução da comunicação sem fio.

O Wi-Fi é desenvolvido em padrões 802.11 da IEEE, e é amplamente utilizado na comunicação sem fio. Ele fornece acesso sem fio para aplicações e dados através de uma rede de ondas de rádio.

CEHv12 (ANSI)

16.Hacking Wireless Networks

Vantagens

A instalação é fácil e rápida e elimina a fiação de cabos através de paredes e tetos.

É mais fácil para fornecer conectividade em áreas onde é difícil estabelecer uma ligação via cabo.

O acesso à rede pode ser de qualquer lugar dentro do alcance de um ponto de acesso.

Usando uma rede sem fio, vários membros podem acessar a Internet ao mesmo tempo sem ter que pagar ao provedor por várias contas.

Locais públicos, como aeroportos, bibliotecas, escolas, ou até mesmo lojas de café oferecem uma conexão com a Internet utilizando uma rede local sem fio.

Desvantagens

A segurança é um grande problema e pode-não atender às expectativas.

Com o aumento do número de computadores na rede a largura de banda diminui.

Padrões Wi-Fi mudam o que resulta na substituição de placas wireless e/ou pontos de acesso.

Alguns equipamentos eletrônicos podem interferir nas redes Wi-Fi.

Tipos de redes wireless

Os pontos de acesso são basicamente dois tipos:

1. Software access points
2. Hardware access points

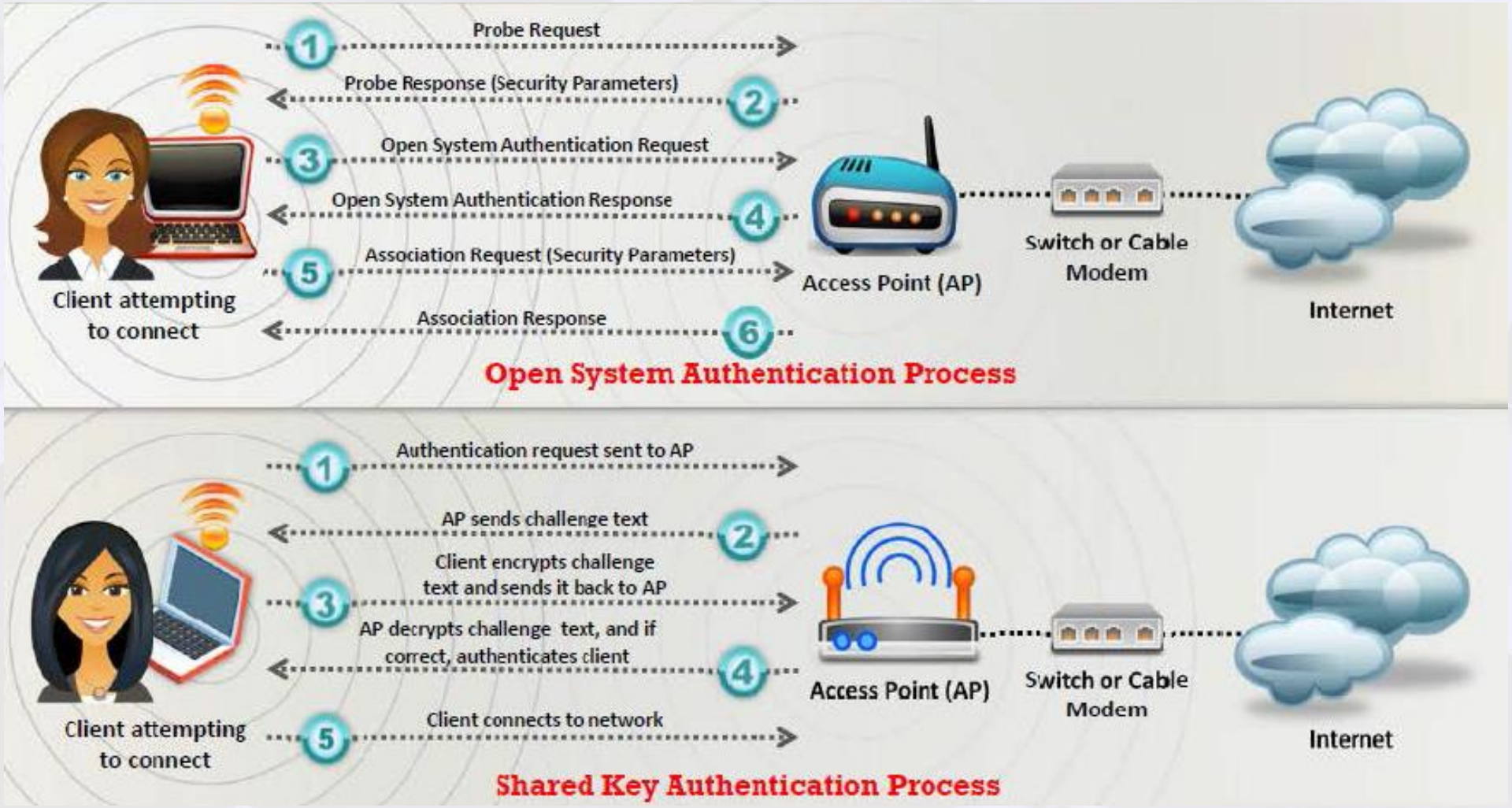
Software access point (SAPs) pode ser conectado à rede com fio, e executado em um computador equipado com uma placa de interface de rede sem fio.

Hardware access points (HAPs) oferecem amplo suporte para a maioria dos recursos sem fio. Com o apoio do software de rede adequado, os usuários da LAN sem fio podem compartilhar arquivos e impressoras situados na Lan cabeada e vice-versa.

Padrões Wireless

Amendments	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	OFDM	54	~100
802.16 (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.4		1 - 3	25

Métodos de Autenticação



Autenticação aberta

No processo de autenticação aberta, qualquer estação sem fio pode enviar um pedido de autenticação. Neste processo, uma estação pode enviar um frame de gerenciamento de autenticação que contém a identidade da estação de envio, para ser autenticado e conectado com outra estação sem fio.

A outra estação sem fio (AP) verifica o SSID do cliente e em resposta envia um frame de verificação de autenticação, se o SSID for correspondente. Uma vez que o frame de verificação atinge o cliente, o cliente se conecta a rede ou estação sem fio pretendida.

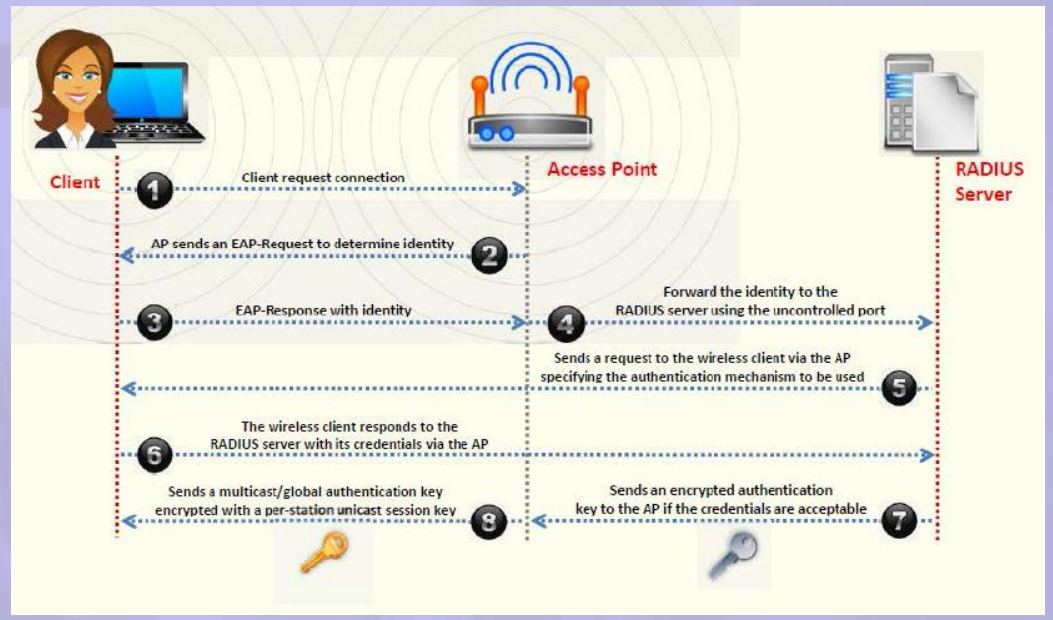
Autenticação de chave compartilhada

Neste processo cada estação sem fio assume ter recebido uma chave secreta compartilhada ao longo de um canal seguro que é distinto dos canais de comunicação de rede sem fio 802.11. As etapas a seguir ilustram como a conexão é estabelecida no processo de autenticação por chave compartilhada:

1. A estação envia um pedido de autenticação ao ponto de acesso.
2. O ponto de acesso envia o texto de desafio para a estação.
3. A estação criptografa o texto do desafio usando sua configuração de chave padrão de 64 bits ou 128 bits, e envia o texto cifrado para o ponto de acesso.
4. O ponto de acesso utiliza a sua chave WEP configurada (que corresponde à chave padrão da estação) para descriptografar o texto cifrado. O ponto de acesso compara o texto decifrado com o texto original desafio. Se o texto decifrado corresponde ao texto original, o ponto de acesso autentica a estação.
5. A estação de ligação à rede.

Autenticação 802.1x

O 802.1X fornece autenticação centralizada. Para a autenticação 802.1x para trabalhar em uma rede sem fio, o AP deve ser capaz de identificar com segurança o tráfego de um cliente sem fio particular. A identificação é realizada usando chaves de autenticação que são enviados para o AP e o cliente a partir do servidor Remote Authentication Dial User in Service (RADIUS). Quando um cliente chega dentro do alcance do AP, ocorre o seguinte processo:



1. O cliente envia uma solicitação de autenticação para o AP para estabelecer a conexão.

2. O AP envia o EAP-Request para a identificação de cliente.

3 O cliente responde com a sua identidade EAP-Response.

4. O AP envia a identidade para servidor RADIUS usando a porta não controlada.

5 O servidor RADIUS envia um pedido para a estação de rádio através do AP, especificando o mecanismo de autenticação a ser utilizado.

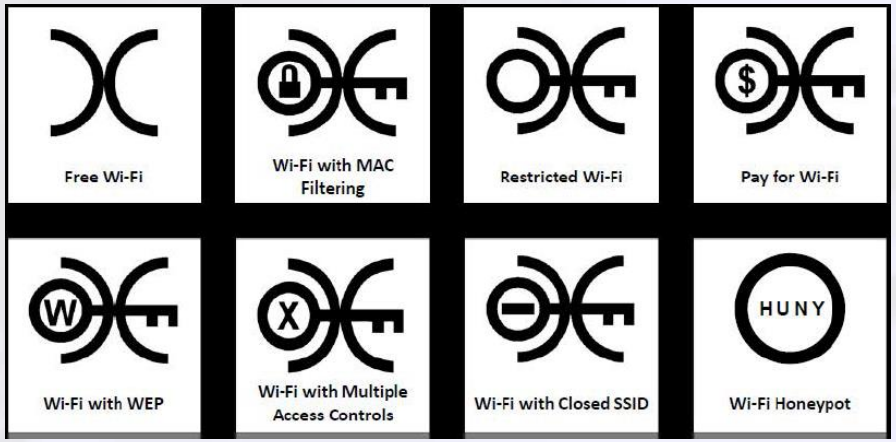
6. A estação responde ao servidor RADIUS com as suas credenciais através do AP.

7. Se as credenciais forem aceitáveis, o servidor RADIUS envia uma chave de autenticação criptografada para o AP.

8. O AP gera uma chave de autenticação multicast/global encriptada com uma chave de sessão unicast por estação, e a transmite para a estação.

Wi-Fi Chalking

WarChalking - Este termo vem de whackers que usam giz para colocar um símbolo especial em uma calçada ou outra superfície para indicar uma rede sem fio proxima que oferece acesso à Internet. Isto é um método usado para desenhar símbolos em lugares públicos para fazer propaganda de redes Wi-Fi abertas.

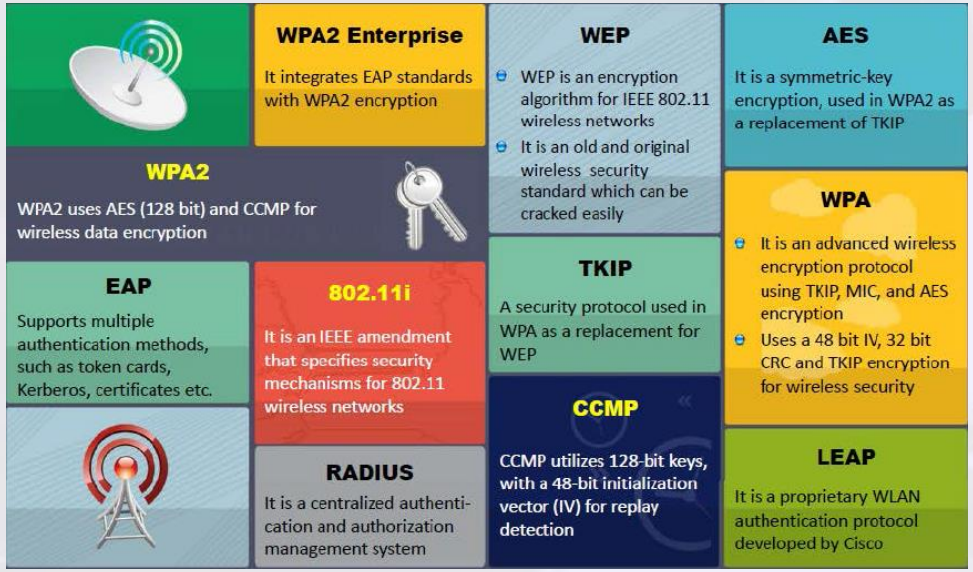


Warwalking - Para executar WarWalking, os atacantes andar por aí com laptops habilitados para detectar redes sem fio abertas. Nesta técnica, o atacante anda a pé para buscar as redes. A desvantagem dessa abordagem é a ausência de um ambiente computacional conveniente e a velocidade mais lenta do percurso.

WarFlying - WarFlying é uma atividade em que os atacantes voam com laptops para detectar redes sem fio abertas. Isso também é conhecido como warstorming. A desvantagem é o difícil acesso as redes abertas por causa do voo.

WarDriving - De acordo com www.wordspy.com, WarDriving é uma técnica que envolve a condução através de um bairro com um notebook e mapear casas e empresas que têm pontos de acesso sem fio.

Tipos de criptografia wireless



WEP: É um cliente de autenticação e protocolo de criptografia de dados e é um velho padrão de segurança sem fio que pode ser quebrado facilmente.

WPA: É um cliente de autenticação avançado e protocolo de criptografia de dados usando TKIP, MIC e criptografia AES. Ele usa uma criptografia de 48-bit IV (Inicialization Vector), 32-bit CRC e TKIP para a segurança sem fio.

WPA2: O WPA2 usa AES (128 bits) e CCMP para criptografia de dados.

WPA2 Enterprise: Ele integra normas EAP com criptografia WPA.

TKIP: Um protocolo de segurança utilizado no WPA como um substituto para WEP.

AES: É uma criptografia de chave simétrica, utilizado no WPA2 como um substituto do TKIP.

EAP: Utiliza vários métodos de autenticação! como cartões token, Kerberos, certificados, etc.

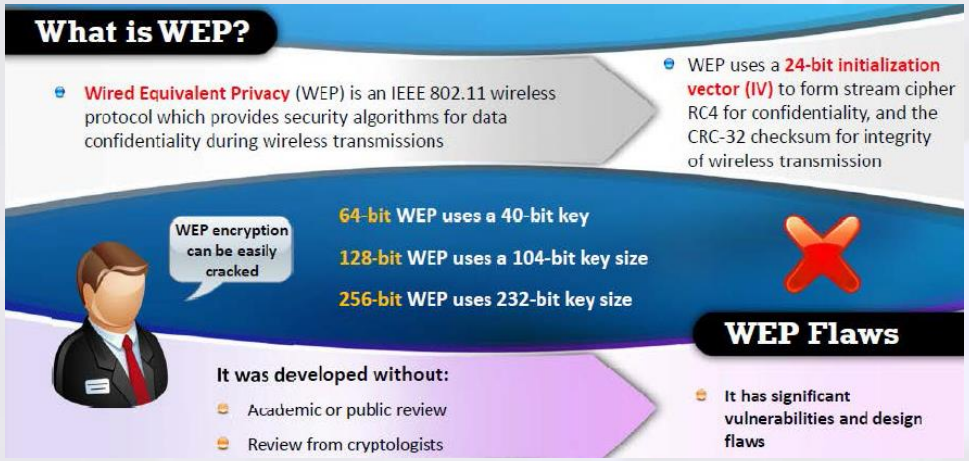
LEAP: Um protocolo de autenticação WLAN proprietário desenvolvido pela Cisco.

RADIUS: Um sistema de autenticação e gerenciamento de autorização centralizado.

802.11i: Um padrão IEEE que especifica mecanismos de segurança para redes sem fio 802.11.

CCMP: CCMP utiliza chaves de 128 bits, com um vector de inicialização de 8 bits para detecção replay.

WEP



Wired Equivalent Privacy (WEP) é o protocolo de criptografia mais antigo e mais fraco. Foi desenvolvido para garantir a segurança dos protocolos wireless. No entanto, é altamente vulnerável. Utiliza o Vetor de Inicialização (IV) de 24 bits para criar uma cifra de fluxo RC4 com Verificação Redundante Cíclica (CRC) para garantir confidencialidade e integridade.

- WEP padrão de 64 bits utiliza uma chave de 40 bits;
- WEP de 128 bits utiliza uma chave de 104 bits;
- WEP de 256 bits utiliza uma chave de 232 bits.

As autenticações utilizadas com WEP são autenticação de sistema aberto e autenticação de chave compartilhada.

Vetores de inicialização fracos (IV)

Um dos principais problemas com o WEP ocorre ao utilizar o vetor de inicialização. O valor IV é muito pequeno para proteger contra reutilização e repetição. O algoritmo RC4 utiliza o IV e chave para criar um fluxo utilizando um algoritmo de agendamento de chave. IVs fracos revelam informações. O WEP não possui nenhuma provisão interna para atualizar a chave.

WPA

A segurança da criptografia de dados foi aumentada no WPA como as mensagens são transmitidas através do Message Integrity Check (MIC), utilizando o Temporal Key Integrity Protocol (TKIP) para melhorar a criptografia de dados. O tráfego unicast muda a chave de criptografia depois de cada quadro usando o TKIP. A chave usada no TKIP muda com cada quadro, e é automaticamente coordenada entre o cliente e o ponto de acesso.

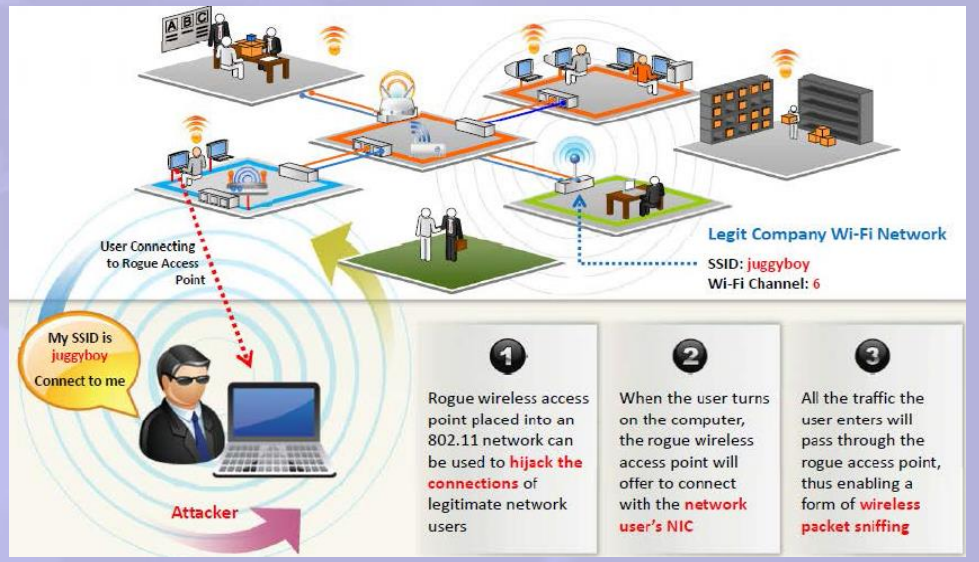
TKIP (Temporal Key Integrity Protocol): Utiliza a cifra de criptografia de fluxo RC4 com chaves de 128 bits e chaves de 64 bits para autenticação. O TKIP atenua a vulnerabilidade de derivação de chaves WEP por não reutilizar o mesmo vetor de inicialização.

Chave temporária de 128 bits: Sob o TKIP, o cliente inicia com uma "chave temporal" de 128 bits, que é então combinada com o endereço MAC do cliente e com um IV (Inicialization Vector) para criar uma chave que é utilizada para encriptar os dados através do RC4. Ele implementa um contador de sequência para se proteger contra ataques de repetição.

Ameaças de redes wireless

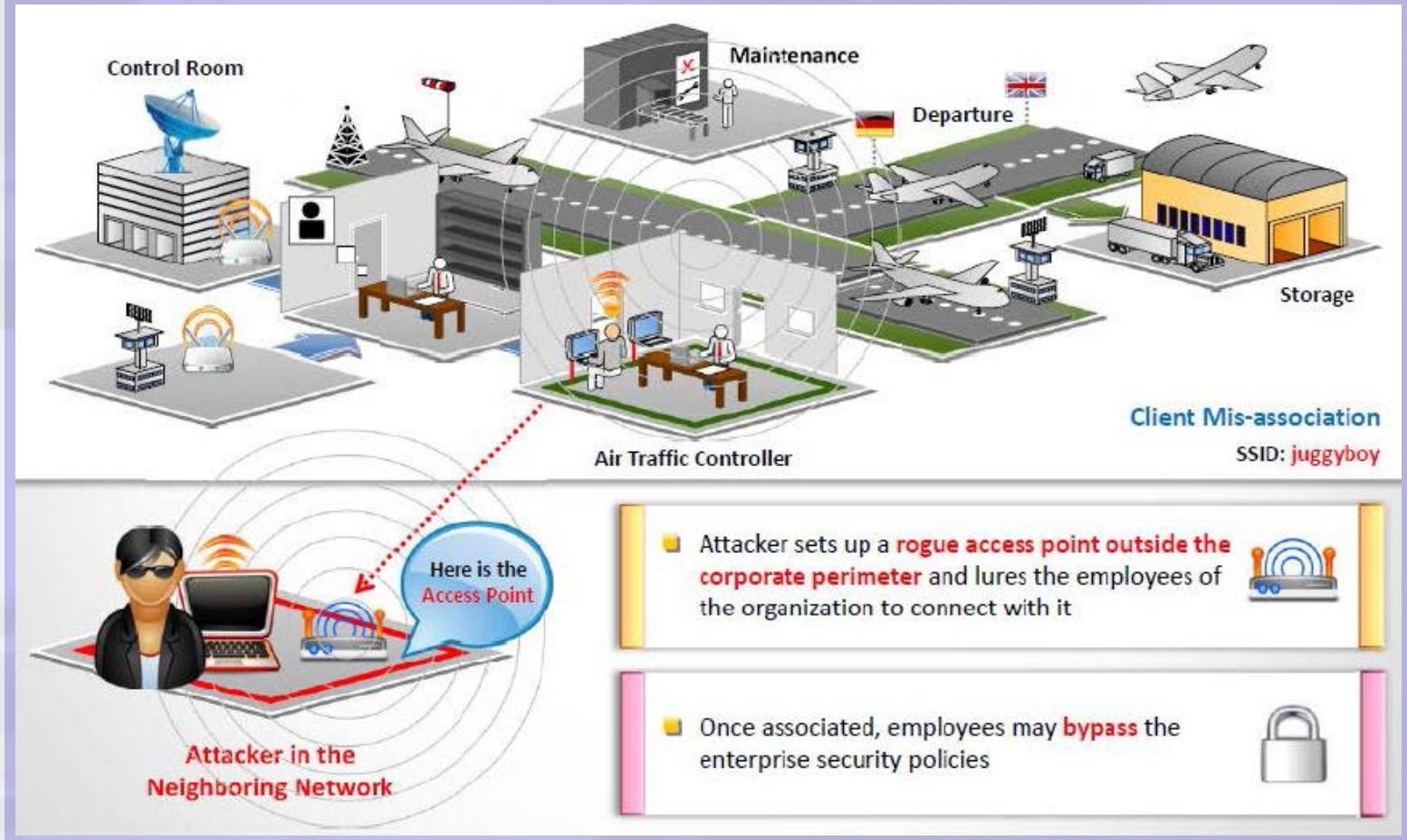
Wardriving - Em um ataque de wardriving, redes sem fio são detectadas através do envio de probe requests através de uma conexão ou ouvindo beacons. Uma vez que um ponto de penetração é descoberto, novos ataques podem ser lançados na rede local. Algumas das ferramentas que podem ser utilizadas para executar wardriving são KisMAC, NetStumbler e WaveStumber.

Cliente promíscuo - O cliente promíscuo oferece um sinal irresistivelmente forte intencionalmente para fins maliciosos. Cartões sem fio, muitas vezes olham para o sinal mais forte para se conectar a rede. Desta forma, o cliente promíscuo agarra a atenção dos utilizadores através do envio de sinais fortes.



Client Misassociation

Um hacker mal-intencionado pode utilizar este comportamento padrão e trazer seu próprio AP sem fio para a área física, onde você normalmente utiliza seu Wi-Fi. Se o sinal deste AP for melhor do que o do AP original, o software do laptop fará uma associação incorreta com o ponto de acesso falso (desonesto) fornecido pelo hacker (pensando que é o AP legítimo que você utilizou no passado). Este tipo de ataque é muito fácil de realizar em alguns grandes espaços abertos, como aeroportos, escritórios ou áreas públicas. Às vezes, esses tipos de ataques são chamados de **Honeypot AP Attacks** .

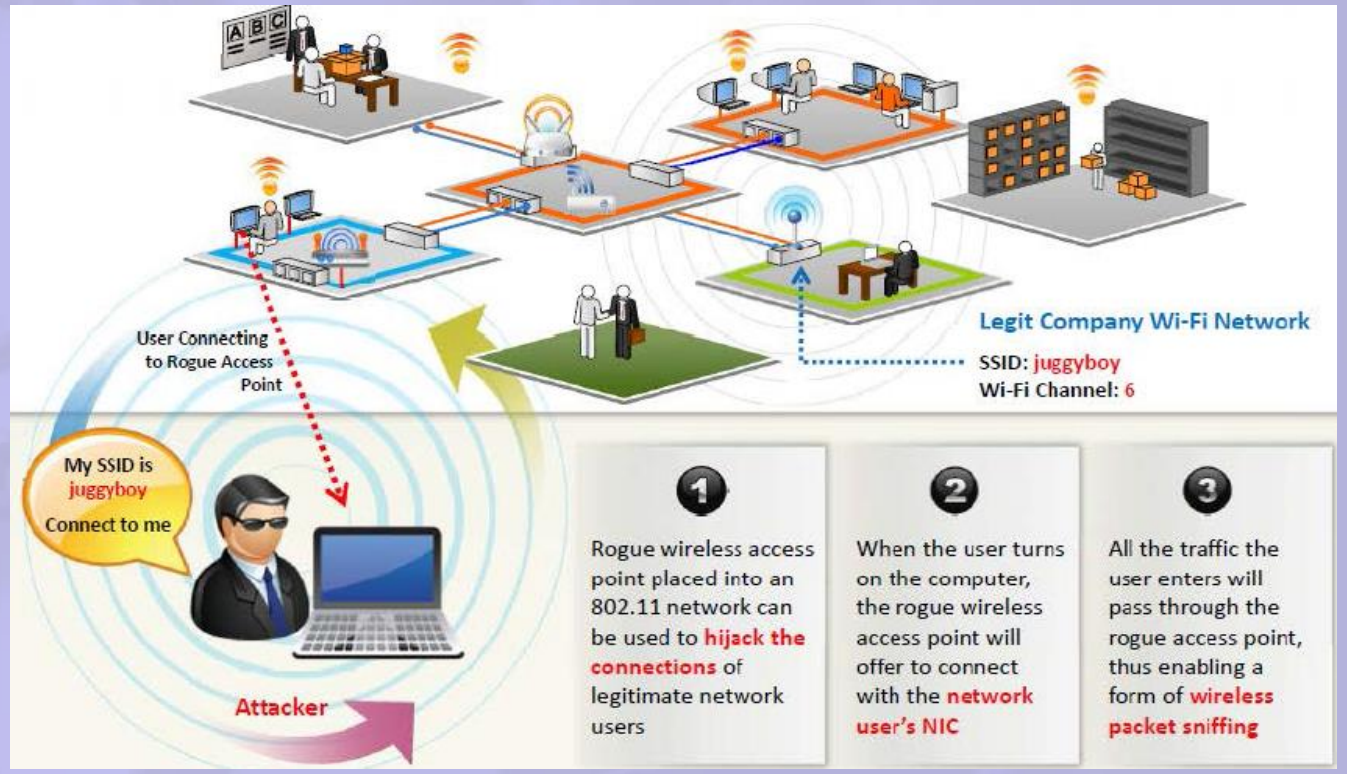


Rogue AP

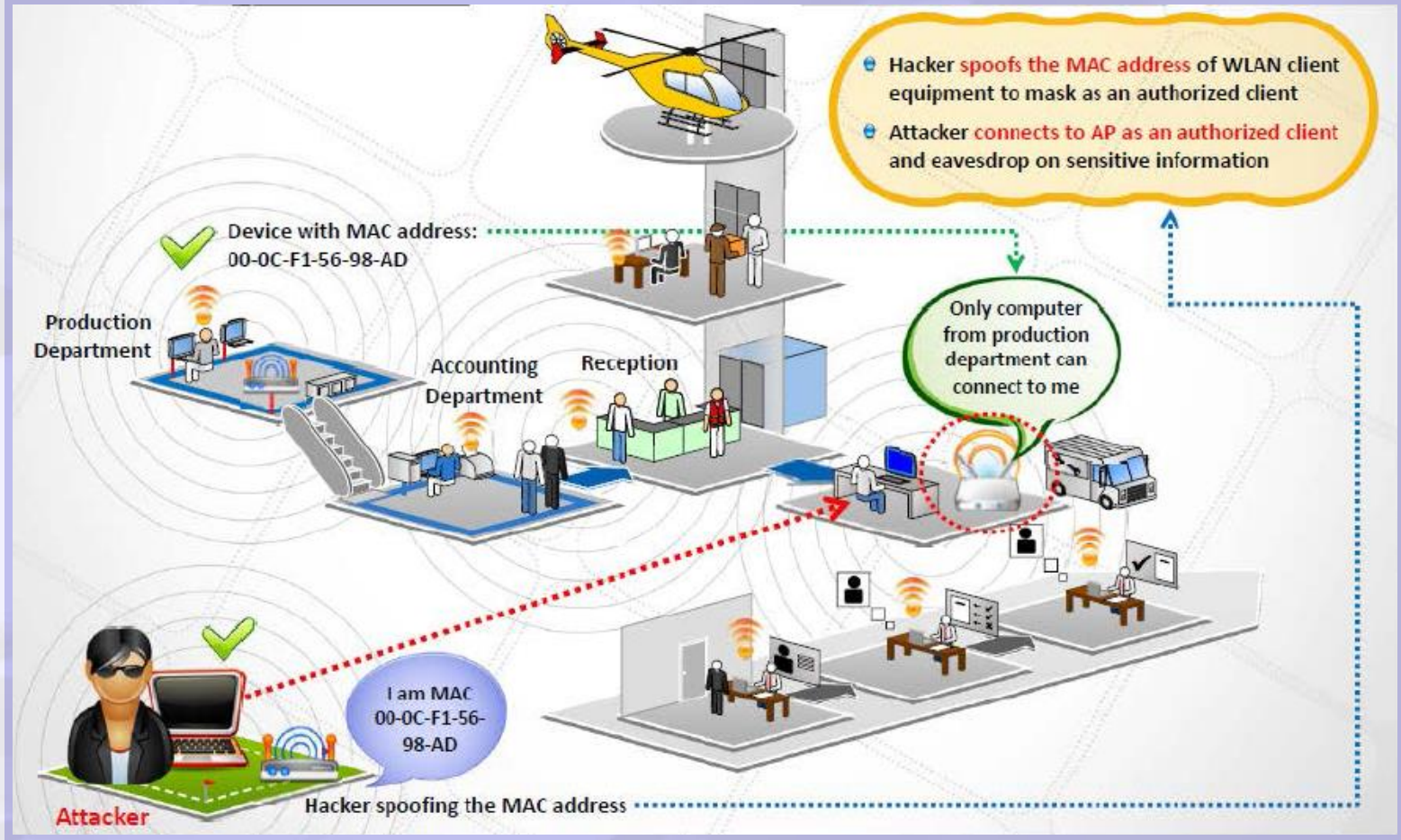
- Pontos de acesso não autorizados e seus clientes prejudicam a segurança de uma rede corporativa ao permitir o acesso irrestrito à rede por qualquer usuário ou cliente sem fio nas proximidades físicas. Pontos de acesso não autorizados também podem interferir na operação de sua rede corporativa

Pontos de acesso não autorizados podem causar os seguintes danos:

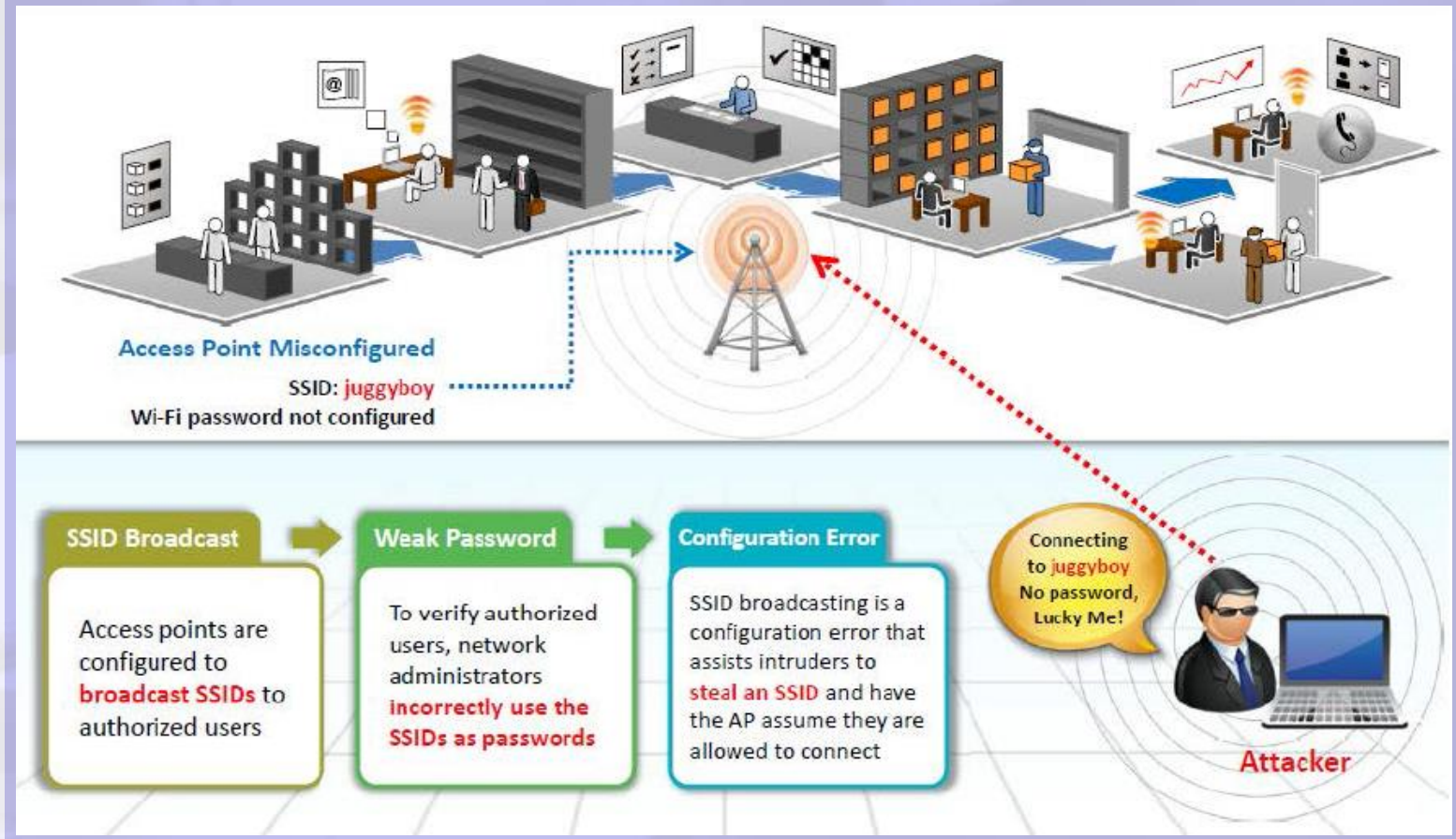
- Permitir que um hacker conduza um ataque man-in-the-middle. O invasor faz conexões independentes com as vítimas e repassa mensagens entre elas, fazendo-as acreditar que estão conversando diretamente entre si por meio de uma conexão privada, quando na verdade toda a conversa é controlada pelo invasor.
- Inundar a rede com dados inúteis, criando uma negação de serviço.
- Enviar SSIDs falsos anunciando recursos atraentes, como conectividade gratuita com a Internet. Depois que um usuário se conecta, o SSID falso é adicionado à configuração sem fio do cliente e o cliente começa a transmitir o SSID falso, infectando outros clientes. .
- Fornecer um canal para o roubo de informações da empresa.



MAC Spoofing



AP Misconfiguration



Metodologia

Wi-Fi Discovery

- **Método passivo** - Um invasor pode usar o modo passivo para detectar a existência de um AP fazendo o sniffing dos pacotes a partir das ondas de rádio, o que pode revelar o AP, SSID, e dispositivos que estão envolvidos.

- **Método ativo** - Neste método, o atacante envia uma probe request com o SSID para ver se o AP responde. Se o dispositivo wireless não têm o SSID, pode enviar a probe request com um SSID vazio. No caso de uma probe request com o SSID vazio, a maioria dos APs respondem com seu próprio SSID em uma probe de resposta.

GPS Mapping

Os invasores costumam criar mapas de redes Wi-Fi detectadas e criar um banco de dados com estatísticas recolhidas pelas ferramentas de descoberta de Wi-Fi como o Netsurveyor, NetStumbler, etc. O GPS é utilizado para rastrear a localização das redes Wi-Fi detectadas e as coordenadas enviadas para sites como o Wigle.

Análise de Tráfego Wireless

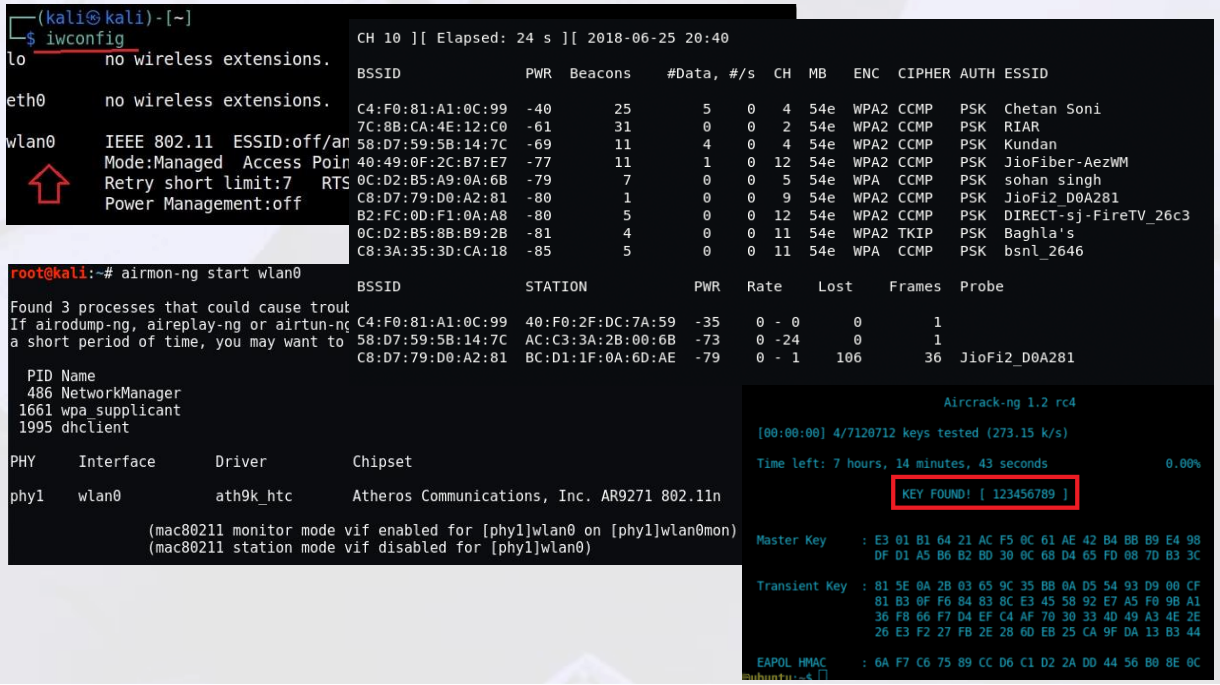
O tráfego wireless permite que atacantes identifiquem as vulnerabilidades e as vítimas sensíveis em uma rede wireless alvo. Isso ajuda na determinação da estratégia adequada para um ataque bem sucedido. Protocolos Wi-Fi são únicos na camada 2, e o tráfego através do ar não é serializado, o que torna fácil a analise de pacotes em redes wireless. Atacantes analisam uma rede sem fio para determinar:

- Broadcast SSID
- A presença de múltiplos pontos de acesso
- Possibilidade de recuperar SSIDs
- Método de autenticação SSL usado
- Algoritmos de criptografia de WLAN

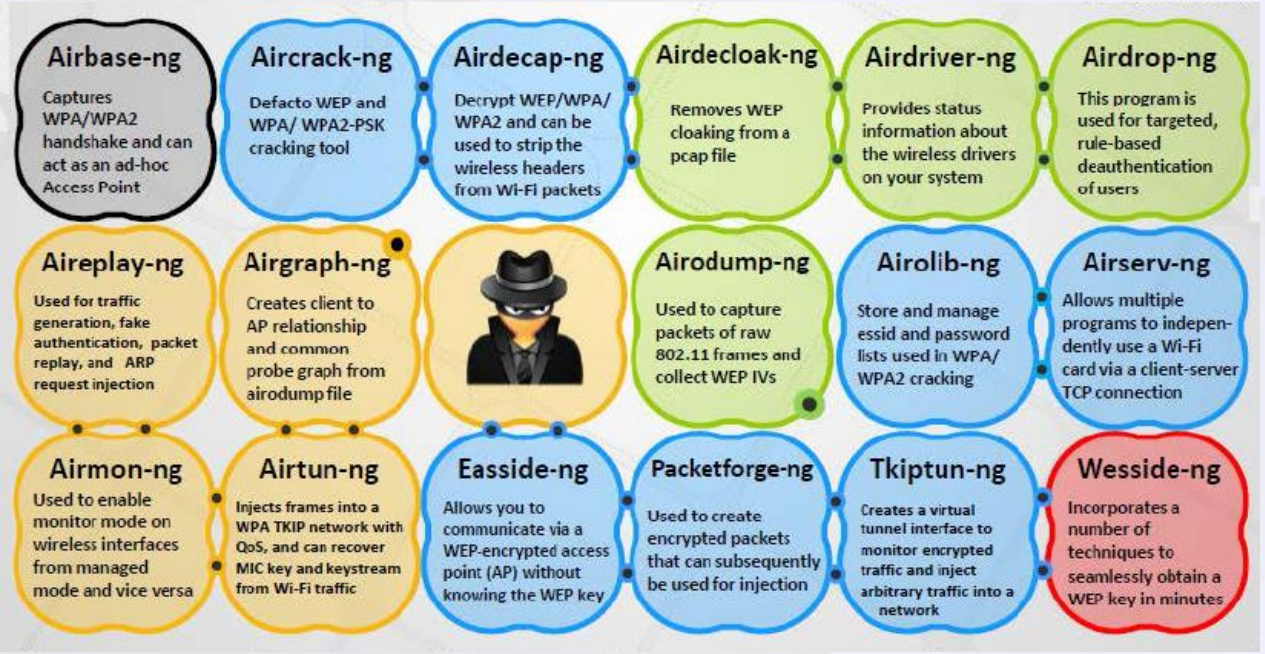
Realizar Ataques Wireless

Aircrack-ng é um conjunto de software de rede que consiste de um detector, sniffer de pacotes, cracker de WEP e WPA/WPA-PSK e ferramentas de análise de redes wireless 802.11.

Este programa é executado no Linux e Windows. Ele funciona com qualquer placa wireless cujo driver suporte o modo de monitoramento raw e possa fazer o sniffing no tráfego 802.11a, 802.11b e 802.11g.



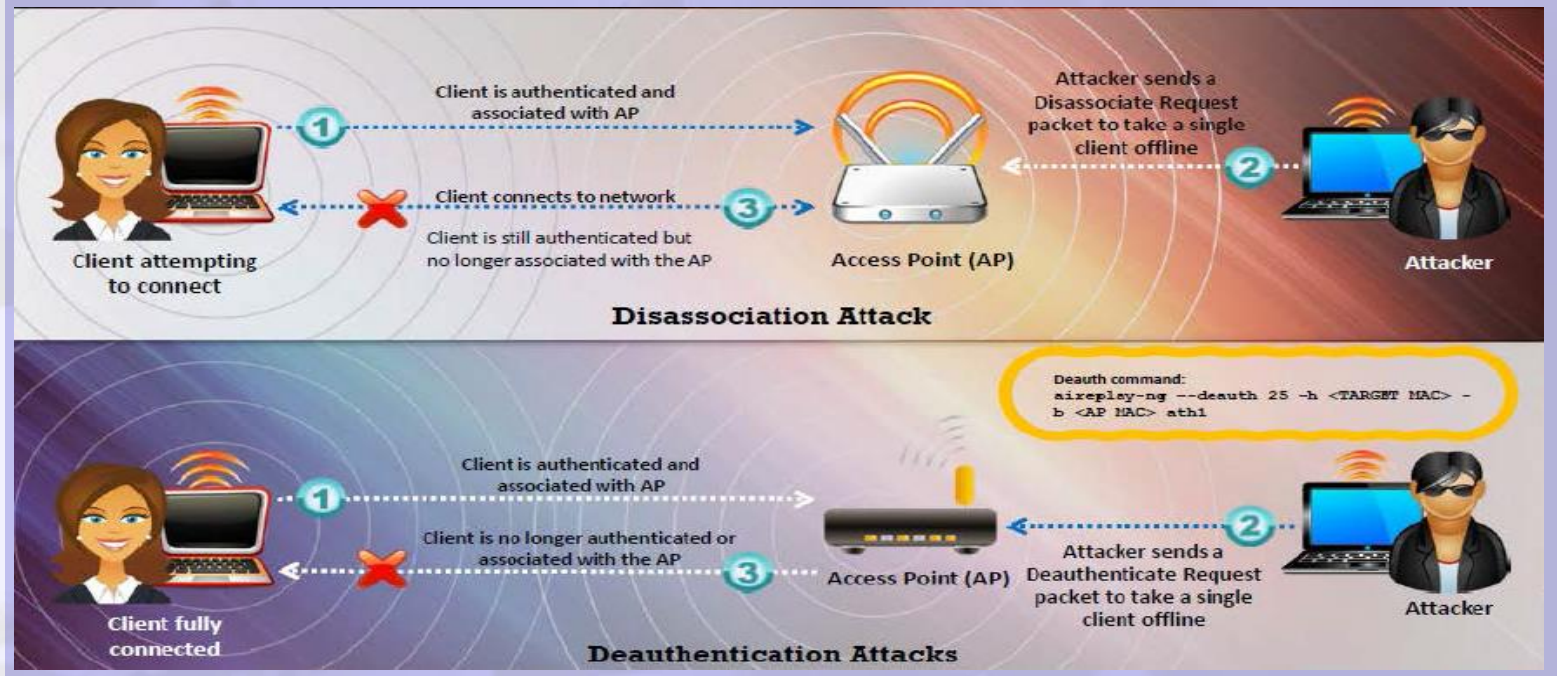
Suite Aircrack-ng



Deauth

Um ataque de desautenticação (DEAUTH) é um tipo de ataque man-in-the-middle (MITM) que visa a comunicação entre o roteador e o dispositivo. Desativando efetivamente o WiFi no dispositivo.

```
root@kali:~# aireplay-ng --deauth 0 -c 98:5F:D3:4A:B1:31 -a C4:E9:84:3F:26:04  wlan0mon
21:36:31  Waiting for beacon frame (BSSID: C4:E9:84:3F:26:04) on channel 1
21:36:31  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|51 ACKs]
21:36:32  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|52 ACKs]
21:36:32  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|47 ACKs]
21:36:33  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [20|49 ACKs]
21:36:33  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [24|48 ACKs]
21:36:34  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|52 ACKs]
21:36:34  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|53 ACKs]
21:36:35  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|53 ACKs]
21:36:36  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 6|48 ACKs]
21:36:36  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 4|45 ACKs]
21:36:37  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [28|46 ACKs]
21:36:37  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [58|46 ACKs]
21:36:38  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [61|53 ACKs]
21:36:38  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|54 ACKs]
21:36:39  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|48 ACKs]
21:36:39  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 0|54 ACKs]
21:36:40  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 4|50 ACKs]
21:36:40  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [ 1|54 ACKs]
21:36:41  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [42|43 ACKs]
21:36:41  Sending 64 directed DeAuth. STMAC: [98:5F:D3:4A:B1:31] [70|48 ACKs]
```



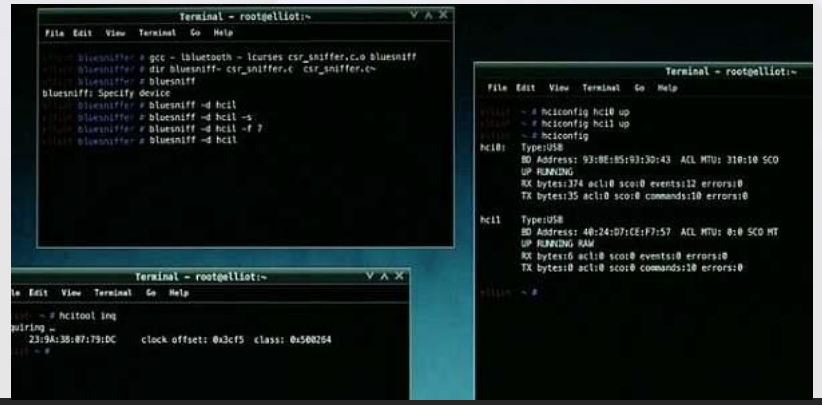
Técnicas de Bluetooth Hacking

Bluejacking

Bluejacking é o uso de Bluetooth para enviar mensagens para usuários sem o consentimento do destinatário, similar ao spam. Antes de qualquer comunicação Bluetooth, o dispositivo de inicialização deve fornecer um nome que será exibido na tela do destinatário. Como este nome é definido pelo usuário, ele pode ser configurado para ser uma mensagem irritante. O Bluejacking não causa qualquer dano ao dispositivo receptor.

BlueSniff

BlueSniff é código de prova de conceito para um utilitário Bluetooth wardriving. É útil para encontrar dispositivos Bluetooth escondidos e detectáveis.

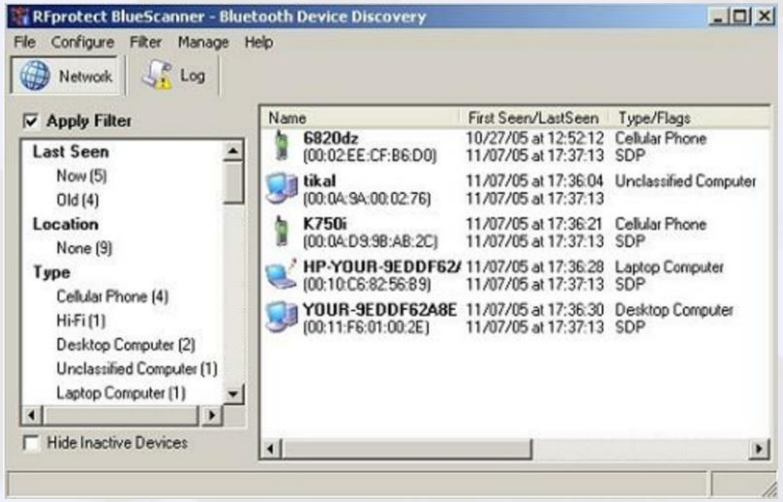


Bluesmacking

Um ataque Bluesmacking é quando um atacante envia um pacote de ping de grandes dimensões para o dispositivo da vítima.

Bluesnarfing

Bluesnarfing é um método de ganhar acesso aos dados confidenciais em um dispositivo compatível com Bluetooth. Se um atacante está dentro do alcance de um alvo, ele pode usar softwares para obter os dados armazenados no dispositivo da vítima.



Conceitos de redes Wireless:

Uma rede sem fios refere-se a uma rede de computador que não está ligado por qualquer tipo de cabo. Em redes sem fio, a transmissão é possível através do sistema de transmissão de ondas de rádio. Isso geralmente ocorre na camada física da estrutura de rede. Mudanças fundamentais para a criação de redes de dados e de telecomunicações estão ocorrendo com a revolução da comunicação sem fio.

O Wi-Fi é desenvolvido em padrões 802.11 da IEEE, e é amplamente utilizado na comunicação sem fio. Ele fornece acesso sem fio para aplicações e dados através de uma rede de ondas de rádio.

CEHv12 (ANSI)

16.Hacking Wireless Networks

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.