1.Proteção de redes Wireless

1.1 Segurança em redes sem fio (WAP)

Também conhecido como Ponto de Acesso sem Fio, é um dispositivo de rede que permite a conexão de dispositivos sem fio, como laptops, smartphones, tablets e outros dispositivos habilitados para Wi-Fi, a uma rede com fio. O WAP atua como uma ponte entre os dispositivos sem fio e a rede cabeada, permitindo a comunicação sem fio entre eles.

Funcionamento:

- **Conexão à rede com fio:** O WAP é conectado a uma rede cabeada através de um cabo Ethernet. Esse cabo é conectado a uma porta LAN (Local Area Network) do WAP, fornecendo conectividade à rede.
- **Criação de redes sem fio:** O WAP transmite um sinal de rádio para criar uma rede sem fio. Esse sinal é utilizado pelos dispositivos sem fio próximos para se conectarem ao WAP e obterem acesso à rede com fio.
- **SSID e autenticação:** O WAP possui um nome de rede, conhecido como SSID (Service Set Identifier), que identifica a rede sem fio. Quando os dispositivos sem fio estão dentro do alcance do WAP, eles detectam o SSID e podem se conectar à rede. O WAP pode exigir uma senha ou outras formas de autenticação para garantir que apenas dispositivos autorizados possam acessar a rede.
- **Comutação de pacotes:** O WAP é capaz de receber e transmitir pacotes de dados entre os dispositivos sem fio e a rede cabeada. Ele atua como uma espécie de "ponte" ou "gateway" que encaminha os pacotes de e para os dispositivos sem fio e a rede com fio.
- **Gerenciamento de conexões:** O WAP é responsável por gerenciar as conexões dos dispositivos sem fio. Ele pode permitir um número máximo de dispositivos conectados simultaneamente (chamado de limite de clientes) e garantir que a largura de banda seja distribuída de maneira adequada entre os dispositivos.
- **Segurança:** A segurança é uma consideração importante no funcionamento do WAP. É essencial que o WAP esteja configurado corretamente com criptografia forte (como WPA2 ou WPA3) para proteger as comunicações sem fio contra acessos não autorizados e ataques de intrusos.
- **Gestão e monitoramento:** O WAP pode ser gerenciado e monitorado remotamente por meio de interfaces de gerenciamento, como uma interface web ou um aplicativo. Isso permite que os administradores de rede controlem as configurações, monitorem o desempenho e apliquem atualizações de segurança no WAP.

1.2 Interferência de canal compartilhado

A Co-channel Interference (CCI) ou Interferência de Canal Compartilhado é um fenômeno que ocorre em redes sem fio, especialmente em redes Wi-Fi, quando

dois ou mais pontos de acesso sem fio (APs) operam no mesmo canal de frequência. Quando APs diferentes compartilham o mesmo canal, eles competem pelo espectro de rádio disponível, resultando em interferência mútua que pode afetar negativamente o desempenho e a confiabilidade da rede.

O fenômeno CCI é detalhado a seguir:

- **Canais de frequência:** As redes Wi-Fi operam em faixas de frequência não licenciadas, como as faixas de 2,4 GHz e 5 GHz. Cada faixa é dividida em canais, e os APs podem ser configurados para operar em um canal específico dentro dessas faixas.
- **Sobreposição:** Em ambas as faixas (2,4 GHz e 5 GHz), existem canais que se sobrepõem, o que significa que eles têm parte de sua largura de banda em comum. Por exemplo, nos canais de 2,4 GHz, os canais 1, 6 e 11 não se sobrepõem, mas outros canais têm sobreposição parcial.
- **Canais não sobrepostos e canais sobrepostos:** Os canais não sobrepostos são aqueles que não compartilham parte de sua largura de banda com outros canais adjacentes. Esses canais podem ser usados simultaneamente sem causar interferência um no outro. Já os canais sobrepostos são aqueles que compartilham parte de sua largura de banda, o que pode levar à interferência quando vários APs operam nesses canais ao mesmo tempo.
- **Concorrência por largura de banda:** Quando dois ou mais APs operam no mesmo canal sobreposto, eles competem pela mesma largura de banda, causando interferência. Essa interferência pode levar a perdas de pacotes, latência aumentada, redução da taxa de transferência e instabilidade na conexão de dispositivos sem fio.
- **Gerenciamento de canais:** Para reduzir a CCI, é importante realizar um planejamento adequado dos canais utilizados pelos APs. Administradores de rede devem configurar os APs para operarem em canais não sobrepostos sempre que possível e, quando necessário, escolher canais com menor interferência para minimizar os efeitos da CCI.
- **Controle de potência:** O controle de potência dos APs também pode ajudar a reduzir a CCI. Ao ajustar a potência de transmissão dos APs, é possível evitar que APs próximos operem em níveis muito altos de potência, o que pode agravar a interferência.

2.WPA2 e WPA3

WPA2 (***Wi-Fi Protected Access 2***) e ***WPA3*** (***Wi-Fi Protected Access 3***) são padrões de segurança utilizados em redes Wi-Fi para proteger a comunicação entre os dispositivos sem fio e o ponto de acesso (AP) ou roteador. Ambos foram desenvolvidos para substituir o padrão WEP (Wired Equivalent Privacy), que era inseguro e foi amplamente comprometido.

Veja como funciona o WPA2:

- **Autenticação:** O WPA2 utiliza o protocolo de autenticação 802.1X/EAP (Extensible Authentication Protocol) para autenticar os dispositivos na rede. Esse protocolo requer a apresentação de credenciais, como senhas, certificados ou outras formas de autenticação, antes que um dispositivo seja autorizado a se conectar à rede.
- **Criptografia:** O WPA2 utiliza o padrão de criptografia AES (Advanced Encryption Standard) para proteger a comunicação entre os dispositivos e o ponto de acesso. O AES é um algoritmo de criptografia forte e amplamente reconhecido por sua segurança.
- **Modos de operação:** O WPA2 oferece dois modos de operação: WPA2-Personal (ou WPA2-PSK) e WPA2-Enterprise. No modo WPA2-Personal, também conhecido como WPA2 com chave pré-compartilhada (PSK), todos os dispositivos compartilham uma senha comum para se conectar à rede. No modo WPA2-Enterprise, a autenticação é baseada em um servidor de autenticação externo, como um servidor RADIUS, tornando-o mais adequado para redes corporativas.

  Veja como funciona o WPA3:
- **Autenticação individualizada:** O WPA3 introduz o conceito de autenticação individualizada, onde cada dispositivo tem uma chave única para a autenticação, tornando mais difícil para atacantes obterem acesso à rede mesmo que conheçam a senha de autenticação.
- **Criptografia de 192 bits:** O WPA3 utiliza a criptografia de 192 bits do padrão SAE (Simultaneous Authentication of Equals) para proteger a autenticação entre o dispositivo e o ponto de acesso. Esse método de autenticação é mais seguro e resiliente a ataques de força bruta.
- **Proteção contra ataques de força bruta:** O WPA3 incorpora uma proteção contra ataques de força bruta para evitar tentativas repetidas de adivinhar a senha de autenticação.
- **Resistência contra ataques de dicionário:** O WPA3 também oferece maior resistência a ataques de dicionário, tornando mais difícil para os atacantes descobrirem senhas comuns usando listas de palavras.
- **Transições de segurança:** O WPA3 é projetado para ser retrocompatível com dispositivos mais antigos, permitindo que eles se conectem à rede com segurança, mesmo que não suportem os recursos mais avançados do WPA3.

O WPA3 traz aprimoramentos significativos em relação ao WPA2, tornando-o mais resistente a ataques e proporcionando uma camada adicional de segurança para redes Wi-Fi. À medida que a adoção do WPA3 cresce, é esperado que se torne o novo padrão de segurança preferencial para redes Wi-Fi em diversos ambientes, desde ambientes domésticos até redes empresariais e públicas.

3.Wi-Fi Protected Setup (WPS)

É um recurso criado para facilitar a configuração de redes Wi-Fi seguras, especialmente em ambientes domésticos e pequenos escritórios. Ele permite que os dispositivos se conectem à rede sem fio com segurança sem a necessidade de inserir a senha da rede manualmente.

Funcionamento:

- **Métodos de configuração:** O WPS oferece dois métodos de configuração: o método de botão de pressão (Push Button) e o método PIN (Personal Identification Number).
- **Método de botão de pressão:** Neste método, o usuário pressiona um botão físico no roteador ou no ponto de acesso (AP) e, em seguida, ativa a função WPS no dispositivo que deseja se conectar à rede Wi-Fi. Os dois dispositivos (roteador/AP e dispositivo cliente) trocam informações automaticamente, configurando a conexão sem fio de forma segura.
- **Método PIN:** Neste método, o usuário insere um PIN (número de identificação pessoal) de oito dígitos fornecido pelo roteador ou AP no dispositivo cliente. Esse PIN é usado para estabelecer a conexão Wi-Fi com segurança.
- **Temporização do PIN:** Para aumentar a segurança do método PIN, o WPS possui um recurso de bloqueio temporário. Após várias tentativas fracassadas de inserção do PIN, o WPS entra em um estado de bloqueio temporário, tornando mais difícil para um atacante tentar forçar a conexão através de ataques de força bruta.
- **Chaves de criptografia:** O WPS gera chaves de criptografia temporárias e exclusivas para a conexão entre o dispositivo cliente e o roteador/AP. Essas chaves são usadas para proteger a comunicação sem fio e são modificadas periodicamente para garantir a segurança contínua.
- **Ativação e desativação:** A maioria dos dispositivos roteadores e clientes possui suporte ao WPS. No entanto, por motivos de segurança, muitos fabricantes desativam o WPS por padrão em seus roteadores, pois alguns ataques demonstraram vulnerabilidades na implementação do WPS.
- **Segurança:** Embora o WPS tenha sido projetado para facilitar a configuração de redes Wi-Fi seguras, algumas implementações do WPS foram criticadas por suas vulnerabilidades de segurança. Isso inclui ataques conhecidos como "ataque de força bruta de PIN" e "ataque de registro externo". Como resultado, muitos especialistas em segurança recomendam desativar o WPS em roteadores e dispositivos que suportam esse recurso.

4.Engenharia social em Wi-Fi

Os seguintes ataques podem ser implementados em redes Wi-Fi para descobrir dados confidenciais:

4.1 Rogue Access Point

- **Criação da rede falsa:** O atacante configura o RAP para transmitir um sinal Wi-Fi com um SSID (nome da rede) similar ou idêntico ao da rede legítima. Isso faz com que dispositivos sem fio próximos detectem a rede falsa como uma opção de conexão.
- **Enganando dispositivos:** Quando os dispositivos sem fio tentam se conectar à rede, eles podem ser enganados a escolher o RAP em vez do ponto de acesso legítimo, especialmente se o sinal do RAP for mais forte ou estiver mais próximo dos dispositivos.
- **Captura de tráfego:** Uma vez que os dispositivos se conectam ao RAP, todo o tráfego da rede passa por ele. O atacante pode capturar e analisar o tráfego, incluindo informações confidenciais, senhas, dados de autenticação e outras comunicações sensíveis.
- **Ataques MitM:** O RAP também pode ser usado para realizar ataques Man-in-the-Middle (MITM), onde o atacante intercepta e manipula o tráfego entre os dispositivos e a rede legítima. Isso permite que o atacante veja, modifique ou injete dados no tráfego de rede.

4.2 Evil Twin

O ***Evil Twin*** (***Gêmeo Malicioso***) é uma forma específica de Rogue Access Point em que o atacante configura um ponto de acesso falso que se disfarça como o ponto de acesso legítimo de uma rede Wi-Fi conhecida. O funcionamento do Evil Twin é semelhante ao do Rogue Access Point, mas sua característica distintiva é a tentativa de enganar os usuários ao criarem uma rede com um SSID idêntico ou muito semelhante ao da rede legítima. Isso pode levar os usuários a se conectarem inadvertidamente ao Evil Twin sem perceberem que não estão conectados à rede real.