1.Ataques wireless

Um ataque de desautenticação em redes sem fio pode desconectar usuários de uma rede Wi-Fi sem aviso prévio, criando uma negação de serviço que impede a reconexão. Esse tipo de ataque explora vulnerabilidades nos quadros de gerenciamento do protocolo 802.11, que, em versões mais antigas, não eram protegidos por criptografia, permitindo que qualquer atacante próximo à rede os manipulasse. Quando um usuário tenta se conectar a um ponto de acesso Wi-Fi, seu dispositivo troca uma série de quadros de gerenciamento para estabelecer a conexão. No entanto, como esses quadros são enviados em texto claro, um invasor pode interceptá-los e forçar a desconexão de dispositivos da rede, enviando quadros falsificados de desautenticação.

Uma forma comum de realizar esse ataque envolve o uso de ferramentas como **airmon-ng** e **aireplay-ng**. Primeiramente, o atacante identifica o endereço MAC do ponto de acesso e dos dispositivos conectados. Em seguida, ele usa um comando específico para enviar quadros de desautenticação direcionados a um dispositivo específico ou a todos os dispositivos conectados ao roteador. Enquanto esses quadros continuarem sendo transmitidos, os dispositivos afetados não conseguirão se manter conectados à rede.

Os engenheiros do IEEE reconheceram esse problema e introduziram melhorias no protocolo 802.11ac e versões posteriores, que incluem a criptografia de quadros de gerenciamento. Com essa atualização, os quadros de desautenticação, associação e troca de canal passaram a ser protegidos, dificultando a exploração dessa vulnerabilidade. Entretanto, ainda existem quadros que permanecem em texto claro por necessidade operacional, como beacons e quadros de autenticação inicial, que devem ser visíveis para permitir a conexão inicial dos dispositivos.

Além dos ataques de desautenticação, outro método de negação de serviço em redes sem fio é o **jamming de radiofrequência** (RF jamming). **Esse ataque não afeta um único dispositivo, mas sim toda a rede, inundando a frequência com sinais de interferência**. O objetivo é reduzir a relação sinal-ruído, tornando impossível a comunicação entre os dispositivos e o ponto de acesso. Essa técnica pode ser implementada de várias maneiras, como a transmissão contínua de ruído, envio aleatório de pacotes ou a transmissão de um grande número de quadros legítimos para saturar a rede.

Interferências involuntárias também podem causar efeitos semelhantes ao jamming. Por exemplo, fornos de micro-ondas e lâmpadas fluorescentes podem interferir em redes de 2,4 GHz, dificultando a conexão dos dispositivos. No entanto, se a interferência não for causada por equipamentos domésticos, é possível que um atacante esteja deliberadamente transmitindo sinais para bloquear o Wi-Fi.

Para identificar e neutralizar um ataque de jamming, uma técnica conhecida como **fox hunting** pode ser utilizada. **Inspirada na prática de radioamadores, essa abordagem envolve o uso de antenas direcionais e atenuadores para localizar a origem do sinal interferente**. Conforme o investigador se aproxima da fonte do jamming, o sinal se torna mais forte, permitindo a triangulação precisa da sua localização.

A segurança em redes sem fio exige monitoramento contínuo e a adoção de padrões mais recentes de criptografia para proteger quadros de gerenciamento. Além disso, ferramentas de análise de espectro e equipamentos de rastreamento de sinal são essenciais para detectar e mitigar ataques de negação de serviço baseados em interferência de radiofrequência.