INSTITUTO UNIVERSITÁRIO DE LISBOA

Mestrado em Telecomunicações e Informática

Segurança em Redes e Sistemas de Informação

Autores:

Silvia Barbosa de Sena, Nº 140691

João Carlos Rodrigues, Nº 85795

Filipe de Almeida Castanheira Marques Fernandes, Nº 104956

Alberto Joaquim Romão Jonatão, Nº 136359

Data: 20-10-2025

Título do trabalho:

Segurança de Redes Wi-Fi Residenciais: Avaliação de Vulnerabilidades e Boas Práticas

Docente:

Valderi Reis Quietinho Leithardt

José André Moura

Paul Andrew Crocker

GitHub:

https://github.com/FilipeFernandes10123/Wi-Fi-Project-

Resumo

Este projeto tem como objetivo proceder à análise da segurança de redes Wi-Fi em ambientes residenciais, abordando os protocolos Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Acess II – Extensible Authentication Protocol (WPA2) e Wi-Fi Protected Acess III (WPA3), bem como alguns conceitos básicos de criptografia, tanto a nível teórico como prático. Serão descritos o funcionamento de cada protocolo, a sua evolução ao longo do tempo e as principais vulnerabilidades conhecidas e associadas a cada um deles, complementando-se com exemplos de ataques reais e incidentes de segurança divulgados na comunicação social. Além disso, serão analisados os impactos das configurações inadequadas que podem ter na segurança das redes domésticas, destacando-se a importância de práticas corretas de configuração e manutenção.

Palavras-chave:

WPE, WPA, WPA2, WPA3 e criptografia.

Índice

Resumo....2
Glossário....4
Introdução....5
Segurança Wi-Fi: Criptografia e Evolução dos Protocolos....6
Criptografia....7
WPE....8
WPA....9
WPA2....11
WPA 3....13
Conclusões....14
Parte Prática....15
Ataque à rede WEP....15
Descrição de metodologia....16
Arquitetura....16
Descrição do ataque....17
Ataque Man-in-the-Middle....19
Etapas do Ataque....19
Descrição do Ataque....20
Resultados e Discussão dos testes efetuados....24
Conclusões e Sugestões para Trabalhos Futuros....24
Referências....25

Glossário

AES – Advanced Encryption Standard

AES-CCMP – Advanced Encryption Standard – Counter Mode with CBC-MAC

CBC – Cipher Block Chaining

CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CRC – Cyclic Redundancy Check

CTR – Counter Mode

EAP – Extensible Authentication Protocol

ECDHE – Elliptic Curve Diffie-Hellman Ephemeral

GCM – Galois/Counter Mode

HKDF – HMAC-based Key Derivation Function

KDF – Key Derivation Function

KRACK – Key Reinstallation Attack

MIC – Message Integrity Check

PSK – Pre-Shared Key

RADIUS – Remote Authentication Dial-In User Service

RC – Rivest Cipher

RSA – Rivest-Shamir-Adleman

RSN – Robust Security Network

SAE – Simultaneous Authentication of Equals

TKIP – Temporal Key Integrity Protocol

WPA – Wi-Fi Protected Access

WPA-PSK – Wi-Fi Protected Access – Pre-Shared Key

WPA2 – Wi-Fi Protected Acess II

WPA2-PSK – Wi-Fi Protected Acess II – Pre Shared Key

WPA2-EAP – Wi-Fi Protected Acess II – Extensible Authentication Protocol

WPA3 – Wi-Fi Protected Acess III

WEP – Wired Equivalent Privacy

WPS – Wi-Fi Protected Setup

Introdução

A generalização do Wi-Fi em ambientes residenciais trouxe grande conveniência, mas também uma superfície de ataque considerável, frequentemente agravada por configurações desatualizadas, palavras-passe fracas, Wi-Fi Protected Setup (WPS) ativo e firmware sem atualizações. Este trabalho procura avaliar a segurança de redes Wi-Fi domésticas e propor boas práticas de configuração e manutenção.

Os objetivos são: (i) descrever, de forma sucinta, a evolução de WEP → WPA → WPA2 → WPA3 e os respetivos mecanismos criptográficos; (ii) identificar vulnerabilidades típicas e erros de configuração que aumentam o risco; e (iii) apresentar recomendações operacionais adequadas ao utilizador comum.

A abordagem combina revisão dos protocolos, análise de vulnerabilidades publicamente documentadas e demonstrações controladas em ambiente laboratorial (apenas em redes locais), evidenciando o impacto de escolhas como o uso de WPA3, a desativação de Wi-Fi Protected Setup (WPS)e a adoção de palavras-passe robustas.

O relatório organiza-se assim: a secção “Segurança Wi-Fi: Criptografia e Evolução dos Protocolos” enquadra os conceitos e descreve WEP, WPA, WPA2 e WPA3; seguem-se resultados e discussão aplicada ao contexto residencial; por fim, as Conclusões sintetizam as principais lições e apresentam uma lista prática de recomendações para reforço da segurança em redes domésticas.

Segurança Wi-Fi: Criptografia e Evolução dos Protocolos

A segurança nas redes Wi-Fi evoluiu de mecanismos iniciais, concebidos para “privacidade equivalente ao cabo”, para soluções robustas que respondem a ataques práticos e a requisitos contemporâneos. Esta secção descreve, de forma contínua, os princípios criptográficos relevantes e a progressão histórica e técnica de WEP → WPA → WPA2 → WPA3, destacando objetivos, funcionamento, vulnerabilidades e recomendações de uso.

Criptografia

A segurança do Wi-Fi apoia-se em três ideias simples: confidencialidade (ninguém lê o que é enviado), integridade (as mensagens não são alteradas) e autenticação (só entra quem está autorizado). Para isso, os protocolos usam cifragem, códigos de integridade e métodos de autenticação.

Os métodos de criação de chaves de sessão apresentam os seguintes critérios específicos:
Acordo de chave (Diffie-Hellman / ECDHE), em que as duas partes envolvidas criam juntas uma chave secreta compartilhada, sem precisar transmiti-la diretamente para a rede. É uma das técnicas mais seguras e garante que, mesmo que os dados sejam capturados, não possam ser usados depois (sigilo de encaminhamento).
Transporte de chave (RSA), consiste em uma das partes gerar a chave de sessão e a enviar cifrada com a chave pública do outro usuário. O destinatário usa sua chave privada para descriptografar e obter a chave, sendo um método simples e rápido.
Segredo pré-compartilhado (PSK), a chave de sessão é obtida a partir de um segredo que ambos já possuem antes da comunicação, como uma senha, código ou token previamente definido.
Derivação de chave (KDF / HKDF), baseia-se em transformar um segredo inicial em uma nova chave, utilizando funções matemáticas que reforçam a segurança e evitam que duas sessões gerem a mesma chave.
Geração aleatória, onde a chave é criada automaticamente por um gerador de números aleatórios seguro e utilizada apenas durante a sessão ativa, assegurando unicidade e imprevisibilidade.

Existem dois tipos principais de cifras:
As cifras de fluxo que cifram os dados de forma contínua, processando-os de bit a bit ou byte a byte, gerando um fluxo contínuo de chaves (keystream) que é combinado com o texto original. Estas são rápidas e ideais para transmissões em tempo real, como por exemplo, o ChaCha20 amplamente utilizado e a Rivest Cipher 4 (RC4) que é considerada pouco segura.

As cifras de bloco que cifram com blocos de dados de tamanho fixo, geralmente de 128 bits. Cada bloco é cifrado individualmente ou em conjunto, de acordo com modo de operação adotado (CBC, GCM, CTR). Esse tipo de cifra é amplamente empregado em protocolos de segurança atuais, sendo o Advanced Encryption Standard (AES) o principal exemplo moderno, enquanto o Data Encryption Standard (DES) é uma tecnologia mais antiga e já desatualizada.

Os primeiros protocolos para segurar a confidencialidade dos dados em redes wireless, eram chamados WEP usaram RC4, uma cifra de fluxo rápida, mas fraca no modo como foi aplicada. As versões modernas (WPA2/WPA3) usam Advanced Encryption Standard (AES) em modo Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), também chamado AES-CCM, que combina encriptação com verificação de integridade numa única construção robusta. Para que a cifragem seja segura, cada mensagem precisa de um valor único (IV/nonce). O WEP usa IV de 24 bits (curto), o que leva a repetições e facilita ataques. Em WPA2/WPA3, o contador/nonce é longo e gerido pelo protocolo, reduzindo este risco.

O Cyclic Redundancy Check – 32 bits (CRC-32) do WEP apenas deteta erros acidentais, não é proteção criptográfica. Em WPA2/WPA3, a integridade é parte do CCMP (um MAC forte), o que impede alterações silenciosas às mensagens. Há dois modos principais: Pessoal (PSK), típico em casa, com uma palavra-passe única para a rede e empresarial (802.1X/EAP), onde cada utilizador se autêntica de forma individual via RADIUS. O WPA2 usa o 4-Way Handshake para derivar chaves de sessão; o WPA3-Personal substitui a PSK pelo SAE (Dragonfly), que resiste a ataques de dicionário offline e dá forward secrecy.

Na prática:
WEP: RC4 + IV curto + CRC → inseguro.
WPA (TKIP): mitigação transitória, hoje desaconselhado.
WPA2 (AES-CCMP): padrão mínimo atual, desde que atualizado.
WPA3 (SAE/OWE/192-bit): recomendado quando suportado pelos equipamentos.

WPE

A popularização do Wi-Fi exigiu mecanismos de segurança capazes de oferecer confidencialidade e integridade equivalentes ao cabo. O WEP foi a primeira resposta padronizada no âmbito do IEEE 802.11.

No final da década de 1990, o objetivo era disponibilizar um mecanismo simples, barato e universal para os chipsets emergentes de 802.11/802.11b (WIFI 2,4Ghz, até 11 Mb/s). O RC4 e o CRC-32 eram leves do ponto de vista computacional e a ideia de «privacidade equivalente ao

cabo» era considerada suficiente para a época. Constrangimentos regulatórios influenciaram, ainda, os tamanhos de chave (por exemplo, 40 bits), dando origem a designações como WEP-64 e, posteriormente, WEP-128.

O WEP cifra os dados do Wi-Fi utilizando a cifra de fluxo RC4. Para cada trama enviada, concatena um vetor de inicialização (IV) público de 24 bits com uma chave partilhada (40 ou 104 bits) para derivar a chave de sessão. Com essa chave, gera um keystream que é combinado com o payload através da operação XOR. Quem possui a mesma chave consegue reverter a operação e recuperar os dados. A integridade é verificada por um código de verificação (CRC-32), que deteta erros acidentais, mas não constitui um mecanismo criptográfico robusto. Devido à reduzida dimensão do IV, ocorre reutilização frequente em redes com tráfego elevado, assim, diferentes mensagens podem ser cifradas com o mesmo keystream, expondo correlações que atacantes exploram para inferir o conteúdo e, potencialmente, recuperar a chave.

As vulnerabilidades publicadas em 2001 precipitaram a evolução do padrão. O IEEE 802.11i (2004) definiu a RSN e tornou obrigatório o AES-CCMP, relegando o WEP (e, mais tarde, o TKIP) para compatibilidade legada. A partir daí, o WEP passou a ser considerado obsoleto e inseguro para qualquer cenário com requisitos mínimos de segurança. O WEP foi um marco inicial para a segurança em redes sem fios, mas as suas fragilidades estruturais tornaram-no inadequado.

Perante estas limitações, a indústria introduziu o WPA como medida transitória (com TKIP) e, de seguida, consolidou a segurança com o WPA2/IEEE 802.11i (baseado em AES-CCMP). Mais recentemente, o WPA3 reforçou o modelo com Simultaneous Authentication of Equals (SAE) e perfis de segurança alargados, tornando-se a referência atual. Na secção seguinte, analisam-se estes três estágios de evolução — WPA, WPA2 e WPA3 — destacando objetivos, mecanismos técnicos, benefícios e limitações.

WPA

O protocolo WPA foi concebido pela Wi-Fi Alliance como uma solução intermédia para colmatar deficiências evidenciadas no antecedente WEP. Este mecanismo de segurança para redes sem fios introduz-se com o objetivo de reforçar tanto os meios de autenticação como os de cifragem, implementando, entre outros, o protocolo Temporal Key Integrity Protocol (TKIP) para cifrar os dados transmitidos entre os dispositivos cliente e o ponto de acesso.

O WPA opera habitualmente em dois modos principais:

Modo Pessoal (WPA-PSK): utiliza uma “chave pré-partilhada” (PSK) que deve ser inserida manualmente em cada dispositivo da rede doméstica, permitindo a ligação dos dispositivos autorizados quando a palavra-passe correta for fornecida.
Modo Empresarial (WPA-Enterprise ou WPA-802.1X/EAP): desenhado para redes corporativas onde se exige um nível mais elevado de controlo e auditabilidade. Neste modo, cada utilizador é autenticado individualmente através de um servidor de autenticação (normalmente servindo o protocolo RADIUS) que valida as credenciais (nome de utilizador, palavra-passe ou certificado digital) antes de conceder acesso.

Em termos de evolução técnica, o WPA representou um avanço significativo em relação ao WEP, ao introduzir:
Gestão dinâmica de chaves (em substituição de chaves estáticas fixas em WEP).
Mensagens de integridade que ajudam a detectar modificações ou reinjeções de pacotes.
Compatibilidade com o framework de autenticação IEEE 802.1X/EAP, permitindo autenticações mais sofisticadas e individualizadas.
Contudo, apesar destas melhorias, o WPA não atingiu o nível de segurança que conseguiu o seu sucessor, WPA2. Por exemplo, o método base do WPA — TKIP — já era considerado menos robusto quando comparado com os algoritmos mais avançados introduzidos posteriormente.

Em termos de vulnerabilidades, o uso continuado do WPA é hoje desaconselhado em ambientes que exigem segurança forte, por razões como:
A partilha de uma única PSK em redes “pessoais” implica que todos os dispositivos utilizam a mesma chave, o que facilita tanto a divulgação acidental como a descoberta maliciosa da mesma.

O protocolo TKIP, utilizado no WPA original, foi alvo de ataques e é considerado obsoleto para novas redes.
A existência de modos mistos (WPA/WPA2) pode levar à utilização de métodos mais fracos com vista à compatibilidade com dispositivos antigos, o que reduz o nível global de segurança da rede.
De facto, a adoção do WPA-PSK foi em muitos casos apenas uma solução intermédia até à introdução plena do WPA2, que passou a requerer algoritmos mais fortes como o AES-CCMP para cifragem e integridade.

Em resumo, o WPA trouxe para o panorama das redes Wi-Fi melhorias importantes relativamente ao WEP, mas rapidamente se tornou ultrapassado face às exigências de segurança modernas. Em redes domésticas antigas ainda poderá encontrar-se, mas sempre que possível

deverá optar-se por protocolos mais recentes, como o WPA2 ou o Wi-Fi Protected Access III (WPA3), que corrigem as fraquezas identificadas no WPA e oferecem níveis de proteção mais elevados.

Imagem 1. Autenticação PSK do WPA2. O WPA e o WPA2 empregam o mesmo método de autenticação PSK.

WPA2

O WPA2 é um protocolo de segurança para redes sem fio que garante a proteção do tráfego da internet por meio de autenticação e criptografia forte de dados. Este emprega o AES para criptografar os dados transmitidos entre os dispositivos e o roteador, assegurando que somente usuários autorizados tenham acesso à rede.

O algoritmo AES é adotado no WPA2 para garantir a segurança dos dados transmitidos em redes Wi-Fi. Por se tratar de um sistema de criptografia simétrica, a mesma chave é usada tanto para a codificação quanto para a descodificação das informações. O AES opera no modo CCMP, que oferece confidencialidade, integridade e autenticação das comunicações. O modo Counter (CTR) realiza a criptografia dos dados, impedindo o acesso não autorizado ao seu conteúdo, enquanto o modo Cipher Block Chaining – Message Authentication Code (CBC-MAC) cria um código de autenticação, responsável por garantir que os pacotes transmitidos não tenham sido alterados durante a transmissão.

O WPA2 opera da mesma forma em dois modos como o WPA: o modo pessoal (WPA2-PSK), utilizado em redes domésticas através de uma senha compartilhada forte e complexa, inserida manualmente nos dispositivos para permitir o acesso à rede e o modo empresarial (WPA2-EAP),

indicado para redes corporativas que oferecem maior controlo e rastreabilidade sobre os usuários conectados. Neste modo, exigem autenticação individual para cada usuário através de um servidor RADIUS, que verifica as suas credenciais (nome de utilizador e palavra-passe), antes de conceder o acesso à rede.

Ao longo dos anos, o WPA2 marcou um avanço significativo em relação aos seus antecessores, WPA e WEP, ao proporcionar um nível de segurança mais elevado através da substituição do protocolo TKIP pelo algoritmo de criptografia AES. No entanto, foram identificadas algumas vulnerabilidades que possibilitaram alguns ataques, como o Key Reinstallation Attack (KRACK), um dos mais conhecidos e divulgado em 2017, que explorava falhas no processo de troca de chaves (4-way handshake), permitindo que os invasores intercetassem e alterassem dados do tráfego Wi-Fi, mesmo sem possuir a senha de rede.

Essa falha ocorre quando o invasor tenta forçar a reinstalação de chaves criptográficas, reutilizando parâmetros de segurança e comprometendo a confidencialidade da comunicação. Embora tenha sido uma das maiores falhas já identificadas no WPA2, foram realizadas atualizações de firmware e sistemas operativos para corrigir esse problema. A descoberta do KRACK incentivou à implementação de atualizações no padrão Wi-Fi e nas suas diversas aplicações, reforçando a necessidade de projetos mais seguros e de políticas de divulgação responsável de vulnerabilidades. Este incidente serviu também como impulso para o aperfeiçoamento das especificações técnicas e para a criação de protocolos mais modernos, como o WPA3, que introduziu melhorias significativas no processo de handshake e na proteção das comunicações sem fio.

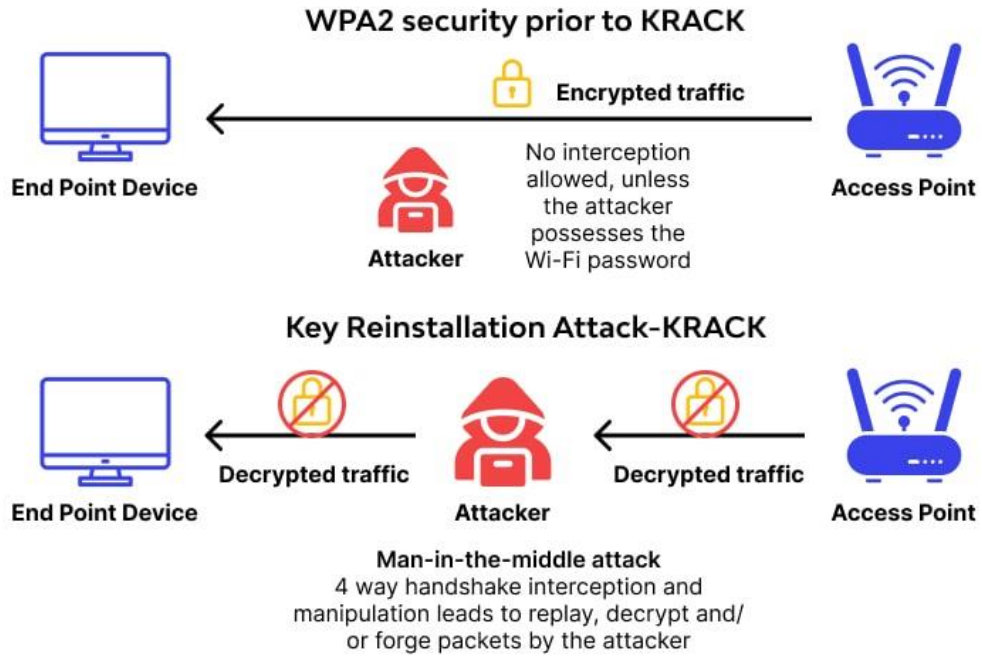


Imagem 2. Krack ataque ao WPA2

WPA 3

O WPA3 é um padrão de segurança desenvolvido pela Wi-Fi Alliance e apoiado por especificações IEEE, como o IEEE 802.11ax. Ele foi lançado em 2018 como uma evolução do WPA2, com foco em corrigir vulnerabilidades conhecidas e fortalecer a proteção de redes sem fio domésticas e corporativas.

O WPA3 funciona com base em três pilares principais:

Autenticação Simultânea de Iguais (SAE), substitui o handshake PSK do WPA2 por SAE, um protocolo baseado em prova de conhecimento zero. Isso significa que os dispositivos provam que conhecem a senha sem transmiti-la, dificultando ataques de dicionário offline.

Criptografia individualizada por sessão, cada conexão entre cliente e ponto de acesso recebe uma chave única, mesmo em redes públicas, garantindo que os dados não possam ser interceptados por outros usuários na mesma rede.

Forward Secrecy, utiliza o protocolo Dragonfly para garantir que sessões anteriores não possam ser descriptografadas mesmo que a chave atual seja comprometida.

Handshake Dragonfly: Substitui o handshake de quatro vias do WPA2, tornando ataques de força bruta offline muito mais difíceis.

Criptografia individual em redes abertas (Wi-Fi Enhanced Open): Mesmo em redes públicas sem senha, cada conexão é criptografada. O WPA3 tal como o anterior, também actua em dois modos, o modo pessoal: Para uso doméstico, com autenticação SAE, e o empresarial, com criptografia de 192 bits. Exemplo, Rede doméstica: Um vizinho mal-intencionado não consegue capturar o tráfego e tentar adivinhar a senha offline, pois o WPA3 exige interação direta com o roteador a cada tentativa.

Rede pública (café): Mesmo sem senha, cada cliente tem criptografia própria, evitando espionagem de tráfego entre usuários.

Apesar das melhorias, o WPA3 apresentou falhas logo após seu lançamento:

Dragonblood (2019): Pesquisadores da KU Leuven e da Universidade de Tel Aviv mostraram que o handshake Dragonfly podia ser explorado para ataques de dicionário e downgrade, permitindo roubo de senhas.

Ataques de canal lateral: Exploração de padrões de tempo e consumo de energia para inferir informações sobre a senha.

Problemas de implementação: Muitos ataques não exploram o protocolo em si, mas falhas em como fabricantes implementam o WPA3 nos roteadores.

Um atacante próximo a uma rede WPA3 pode forçar um downgrade para WPA2, explorando vulnerabilidades conhecidas do WPA2 e, assim, quebrar a segurança da rede.

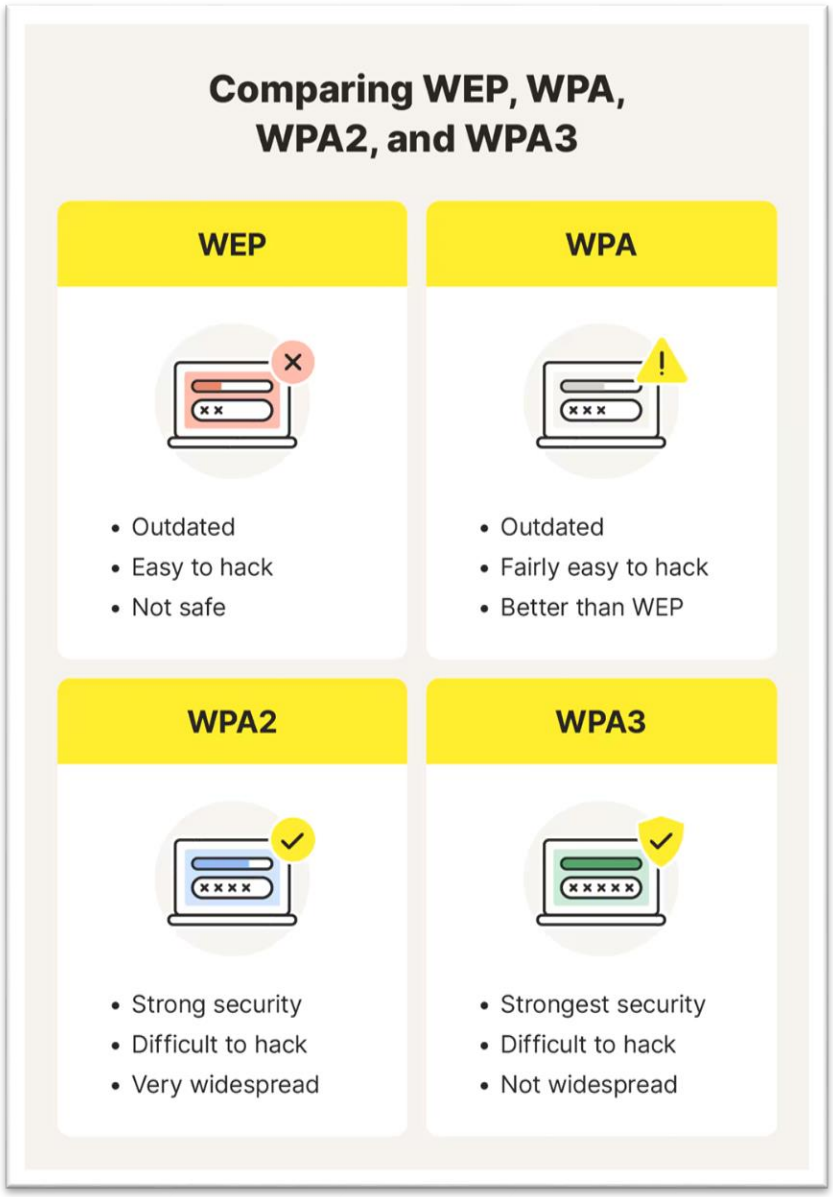


Imagem 3. Análise comparativa da criptografia utilizada nos protocolos

Conclusões

A evolução dos mecanismos de segurança em redes Wi-Fi reflete a necessidade constante de equilibrar conveniência e proteção num ambiente cada vez mais conectado. Desde o WEP, cuja fragilidade expôs rapidamente os riscos da cifragem inadequada, até ao atual WPA3, observa-se um esforço contínuo da indústria para reforçar a confidencialidade, a integridade e a autenticação das comunicações sem fios.

O WEP marcou o ponto de partida, mas revelou vulnerabilidades estruturais graves. O WPA surgiu como uma resposta transitória, introduzindo melhorias como o TKIP e o MIC, embora hoje se encontre obsoleto. O WPA2 consolidou a segurança ao adotar o AES-CCMP e ao tornar o 4-Way Handshake um padrão robusto, ainda que falhas como o ataque KRACK tenham demonstrado a importância de uma manutenção e atualização contínuas. Por fim, o WPA3 representa o estado da arte atual, com o protocolo SAE, criptografia individual em redes abertas e perfis de segurança de 192 bits, reduzindo substancialmente o impacto de ataques de força bruta e de dicionário offline.

Contudo, mesmo os protocolos mais recentes não estão imunes a falhas de implementação, configurações incorretas ou vulnerabilidades emergentes. A segurança efetiva de uma rede Wi-Fi depende, portanto, não apenas do protocolo utilizado, mas também da gestão segura de credenciais, da atualização regular do firmware e da correta configuração dos dispositivos.

Assim, este trabalho reforça a importância de compreender os princípios técnicos e as limitações inerentes a cada protocolo, de modo a aplicar boas práticas de configuração em ambientes domésticos e empresariais.

Na componente prática do trabalho, será realizada uma avaliação experimental de vulnerabilidades em ambiente controlado, incidindo sobre um dos protocolos estudados. O objetivo é demonstrar, de forma segura e ética, como determinadas fragilidades podem ser exploradas e, sobretudo, como podem ser mitigadas através de configurações adequadas e atualizações de segurança.

Parte Prática

Ataque à rede WEP

Esta fase do projeto descreve a execução de um ataque a uma rede protegida por criptografia WEP, realizado em ambiente controlado de laboratório para fins académicos e de demonstração. O objetivo foi analisar a vulnerabilidade do protocolo WEP e demonstrar como é possível comprometer a sua segurança utilizando ferramentas específicas.

O ataque foi conduzido seguindo as etapas apresentadas no guia disponível em WikiHow: How to Break WEP Encryption, adaptando os procedimentos ao contexto do laboratório.

Descrição de metodologia

O ataque foi realizado seguindo três etapas principais:

1. Configuração do ambiente: A interface de rede foi colocada em modo monitor para permitir a captura de pacotes.
2. Captura de tráfego: Utilizou-se airodump-ng para monitorar a rede WEP alvo e recolher vetores de inicialização (IVs). Para acelerar a coleta, foram injetados pacotes ARP com aireplay-ng.
3. Quebra da chave WEP: Após capturar um número suficiente de IVs, a ferramenta aircrack-ng foi usada para realizar o ataque estatístico e descobrir a chave.

Arquitetura

O ambiente foi configurado em laboratório, composto por:

- Attacker laptop: Kali Linux com placa de rede compatível com modo monitor.
- Router: Ponto de acesso com criptografia WEP.
- Victim laptop: Ligado ao router por wifi
- Android Smartphone: Used as a server.
- Topologia: Comunicação direta entre a máquina atacante e o ponto de acesso, sem dispositivos intermediários.

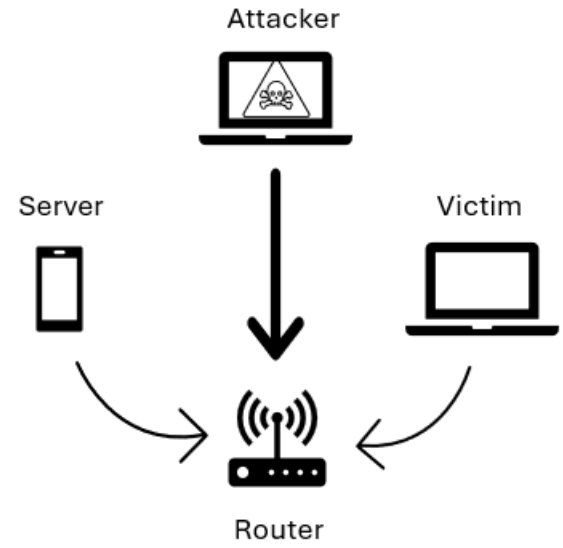


Imagem 3. Dispositivos usados no ataque.

Descrição do ataque

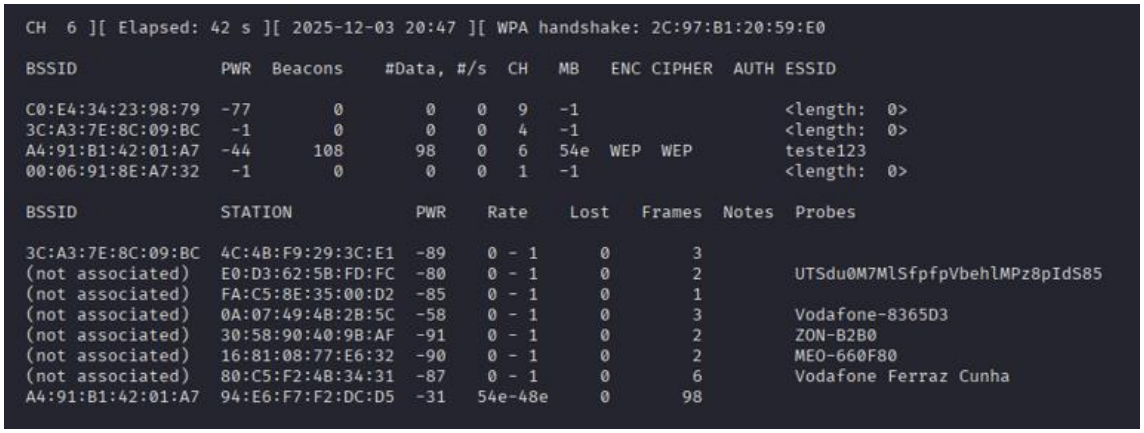
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 18:31:bf:20:29:e0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI>  mtu 1500
        unspec 40-9F-38-AD-2E-D5-00-90-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan1: flags=867<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC,ALLMULTI>  mtu 1500
        unspec 24-EC-99-BF-CB-8A-00-90-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 1083793  bytes 243344944 (232.0 MiB)
        RX errors 0  dropped 916025  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Foi identificado o nome do adaptador de rede. Para isso, foi utilizado o comando `ifconfig`. Esse comando exibiu todos os adaptadores de rede conectados ao computador. Através deste comando conseguimos indentificar que o nosso adaptador de rede era o wlan1.

Foi utilizado o comando Airmon-ng para colocar o adaptador de rede em modo monitor. Para isso, foi digitado o comando:

- `sudo airmon-ng start wlan1`

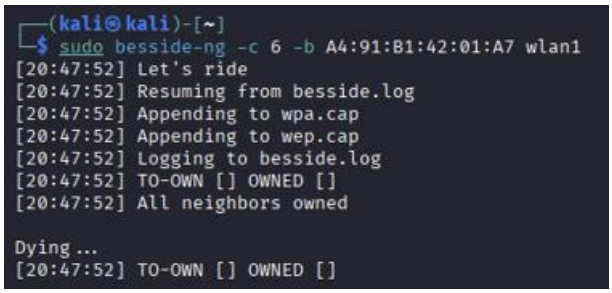
Este procedimento colocou o adaptador de rede em modo monitor.



Utilizou-se o comando Airodump-ng para procurar uma rede com WEP ativado. Para isso, foi digitado o comando:

- `sudo airodump-ng wlan1 --encrypt WEP`

Este procedimento permitiu procurar pacotes enviados com encriptação WEP. Caso fossem encontradas redes, estas seriam listadas com a indicação "WEP" na coluna "ENC" do resultado apresentado em cima.



Foi usado o Besside-ng para realizar o ataque à rede. Para isso, foi digitado o comando:

- `sudo besside-ng -c 6 -b A4:91:B1:42:01:A7 wlan1`

O parâmetro "número do canal" foi substituído pelo número do canal (6) obtido através do comando `airodump-ng`. O parâmetro "endereço BSSID" foi substituído pelo endereço MAC (`A4:91:B1:42:01:A7`) da rede identificado anteriormente.

Este procedimento iniciou um ataque à rede utilizando a ferramenta Besside-ng, que primeiro realizou injeção de pacotes e, em seguida, um flood na rede. Todos os dados recolhidos foram gravados num ficheiro com extensão .cap. O ataque teve uma duração aproximada de 10 minutos.

Foi utilizado o Aircrack-ng para obter a chave da rede. Para isso, foi digitado o comando:

- `sudo aircrack-ng ./wep.cap`

Este comando leu o ficheiro .cap que continha todos os dados recolhidos pela ferramenta Besside-ng. Após a execução, foi apresentada uma lista das redes encontradas, permitindo identificar a chave da rede alvo.

Ataque Man-in-the-Middle

Aqui descrevemos a execução de um ataque do tipo "man-in-the-middle" (MITM), realizado em ambiente não laboratorial, porém bastante controlado com fins académicos e de demonstração. O objetivo foi analisar a vulnerabilidade das comunicações em rede e demonstrar como é possível comprometer a integridade e a confidencialidade dos dados quando um atacante se coloca entre duas partes que acreditam estar a comunicar diretamente.

Etapas do Ataque

Seguimos as etapas apresentadas em guias técnicos de segurança informática, para conduzir o ataque, adaptando os procedimentos ao contexto do laboratório.

Durante a experiência, foram observados os seguintes aspetos:

- Interceção de tráfego.

- Manipulação de pacotes.

- Imitação de identidade.

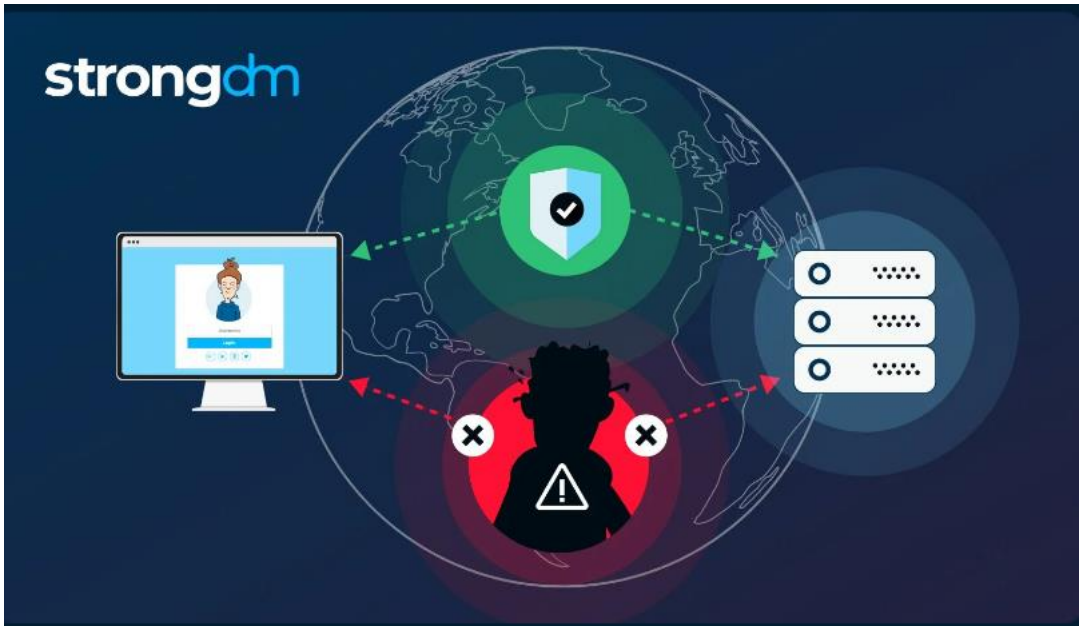
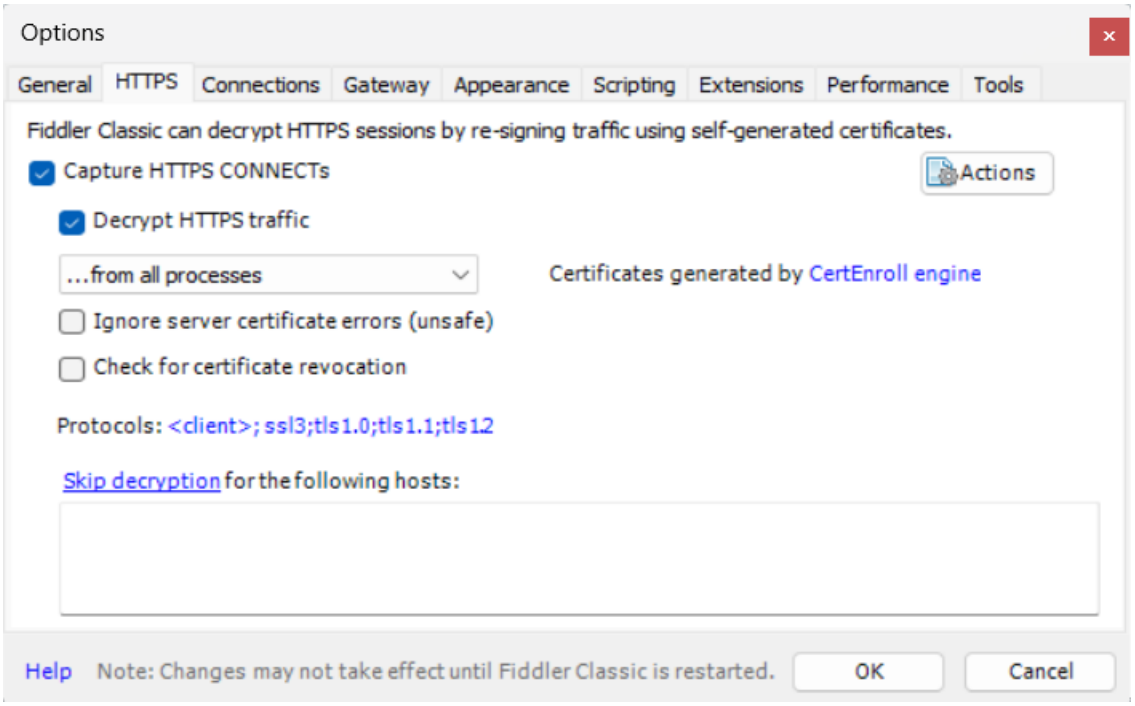
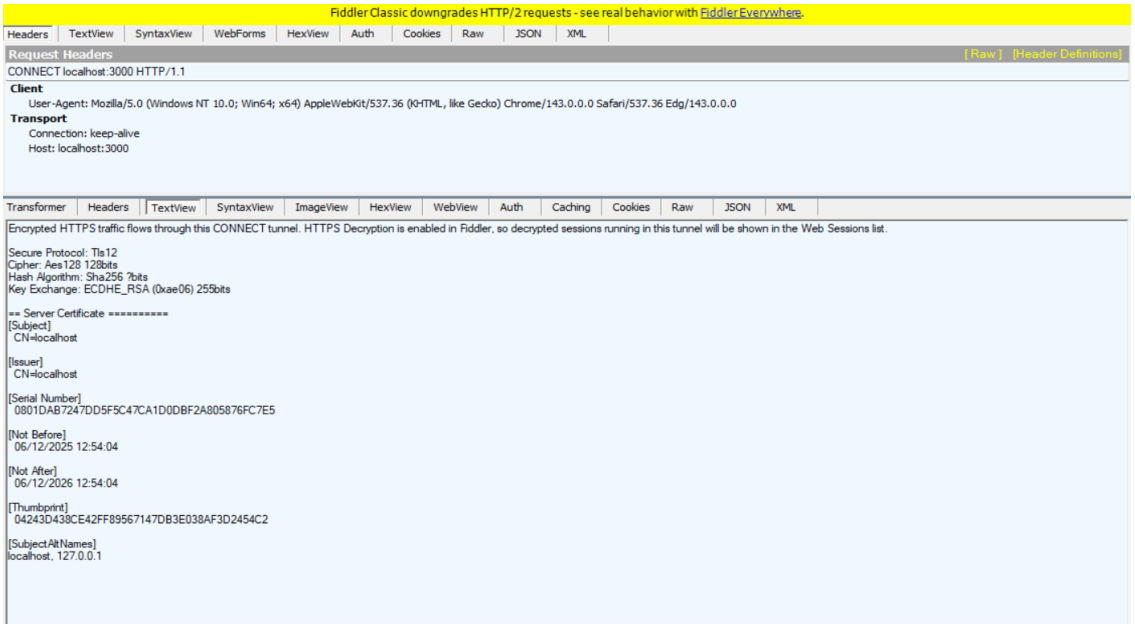


Imagem 4. Modelo ilustrativo de um ataque MITM

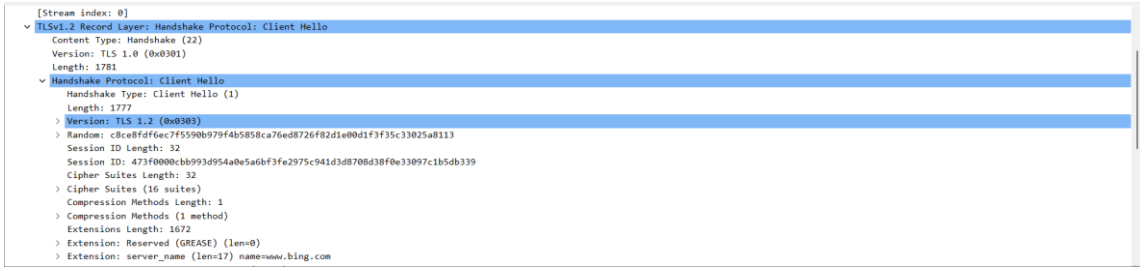
Descrição do Ataque



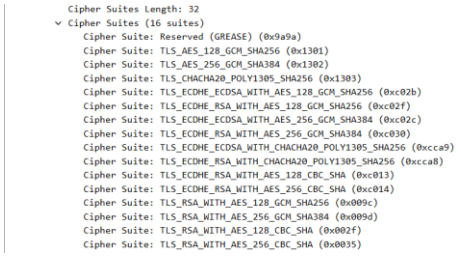
Configuração “Decrypt HTTPS traffic” janela de opções do Fiddler com a opção marcada.



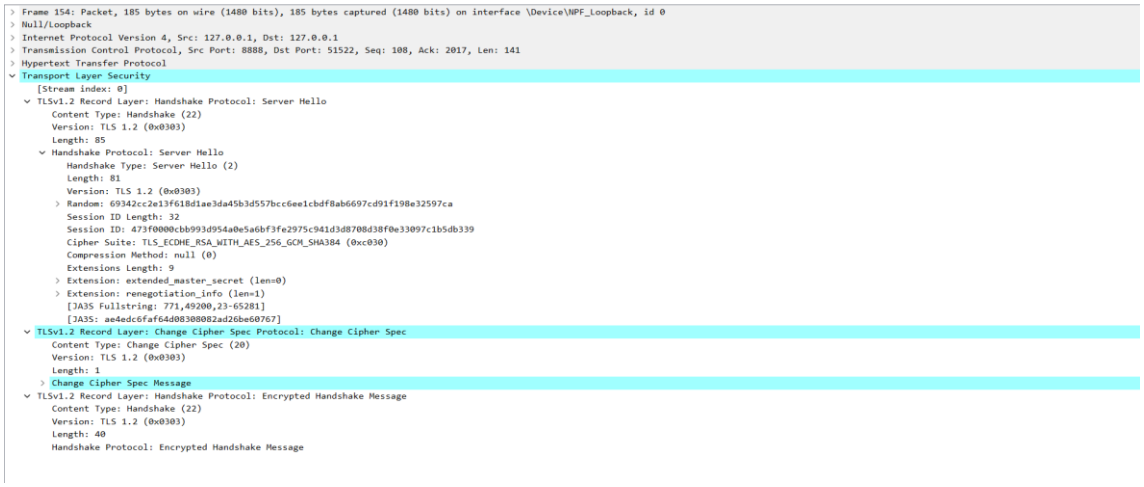
Tráfego HTTPS visível mostrando uma requisição HTTPS ao teu servidor, comheaders e conteúdo visível.Isto demonstra como o Fiddler consegue inspecionar tráfego quando o utilizador aceita o certificado falso.



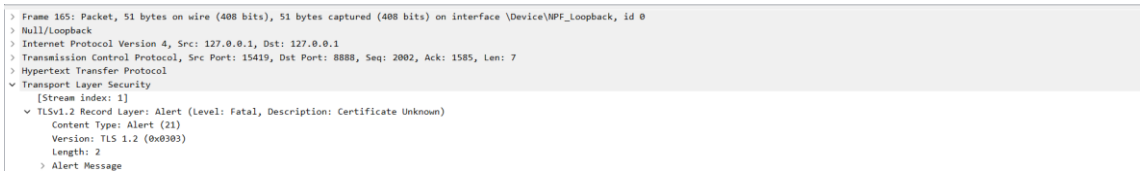
Mostra o pacote inicial do browser. Versões de TLS suportadas.



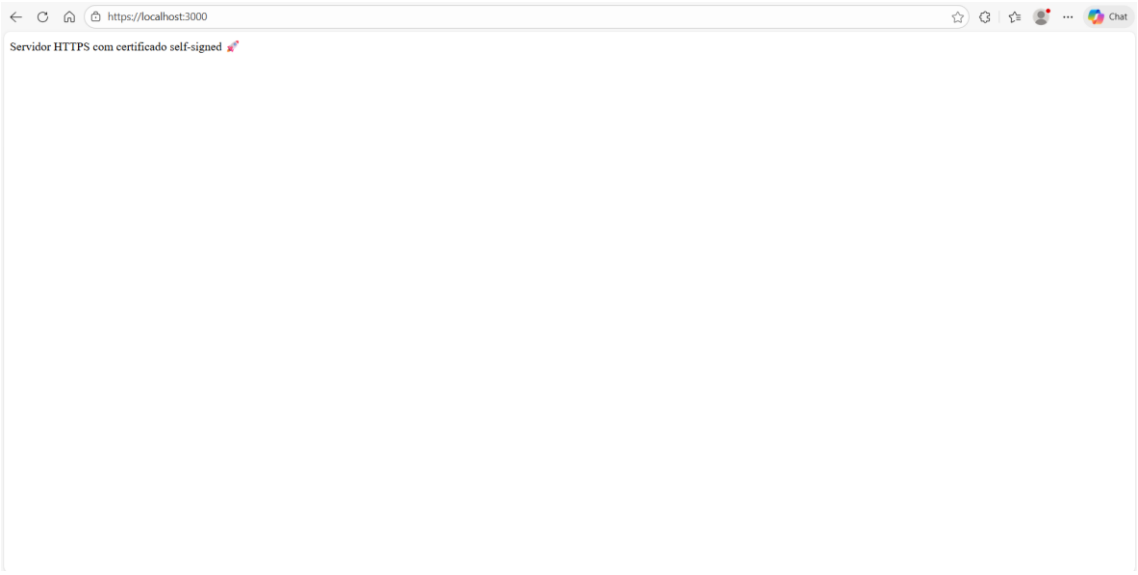
Mostra o pacote inicial do browser. Cipher suite selecionada.



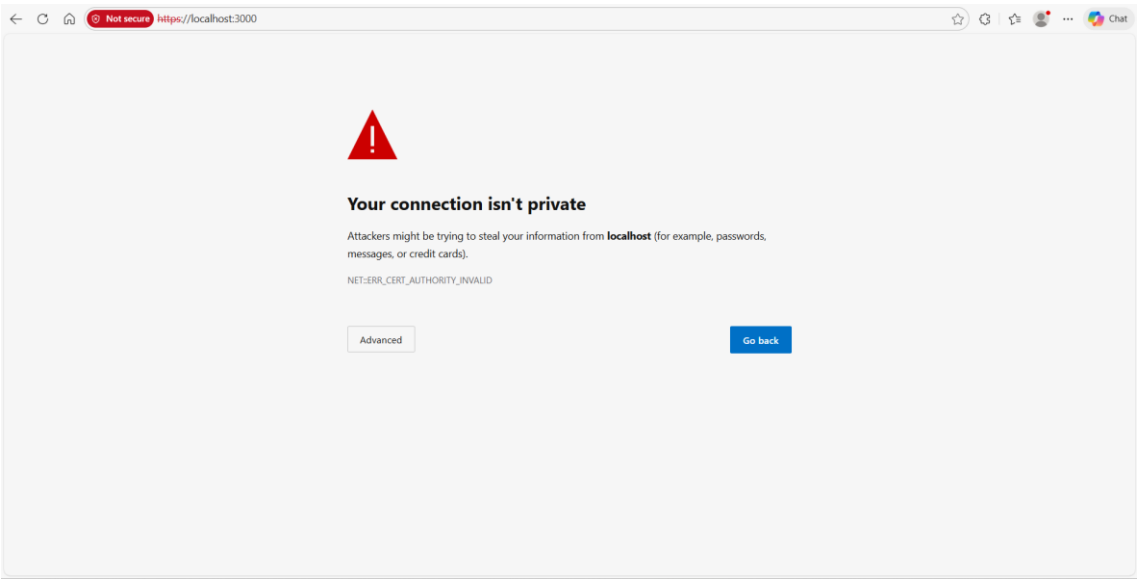
Mostra a resposta do servidor. Versão de TLS escolhida.



Alerta TLS (se rejeitares o certificado) Se o browser não aceitar o certificado, aparece um pacote “Alert”.



Página HTTPS carregada após aceitar o certificado imagem da tua página https://localhost:3000 a mostrar a mensagem “Servidor HTTPS com certificado self-signed



Aviso de certificado inválido imagem da página de aviso (“Your connection is not private” ou equivalente). Mostra que o browser bloqueia certificados não confiáveis.

Sessão HTTPS ativa (se aceitares o certificado) imagem mostrando pacotes TLS após o handshake.

Mostra que o conteúdo está encriptado (não consegues ver o GET/POST).

Este exercício evidenciou como ataques MITM podem comprometer sistemas que não utilizam mecanismos robustos de autenticação e encriptação, reforçando a importância da adoção de protocolos seguros como TLS/SSL e da utilização de certificados digitais válidos.

Resultados e Discussão dos testes efetuados

Durante os testes realizados, foi possível comprovar a vulnerabilidade do protocolo WEP e a eficácia das ferramentas utilizadas para comprometer a segurança da rede. Os principais resultados foram:

Ataque WEP

- Adaptador colocado em modo monitor com sucesso, permitindo captura de pacotes.
- Rede WEP identificada e IVs recolhidos com airodump-ng.
- Injeção de pacotes ARP acelerou a coleta de IVs.
- Em cerca de 10 minutos, o ficheiro .cap permitiu ao aircrack-ng descobrir a chave WEP.
- Confirma-se que o WEP é altamente vulnerável a ataques estatísticos.

Ataque MITM

- Interceção de tráfego HTTPS possível após aceitação de certificado falso no Fiddler.
- Quando rejeitado, o browser bloqueia a conexão e apresenta alertas TLS.
- Quando aceito, tráfego HTTPS pôde ser inspecionado, comprometendo a confidencialidade.
- Evidencia a importância da validação de certificados e da educação do utilizador.

Discussão:

Os resultados obtidos confirmam que:

- O protocolo WEP é obsoleto e inseguro, sendo facilmente quebrado com ferramentas amplamente disponíveis.
- A segurança das comunicações depende não apenas da tecnologia (TLS/SSL), mas também do comportamento do utilizador (aceitação de certificados).
- Em ambientes reais, ataques MITM podem ser mitigados com HSTS, certificados confiáveis e autenticação forte.

Conclusões e Sugestões para Trabalhos Futuros

Conclusões:

- O protocolo WEP não deve ser utilizado em redes modernas, pois sua vulnerabilidade permite que qualquer atacante com conhecimentos básicos comprometa a segurança.
- Ataques MITM continuam sendo uma ameaça relevante, especialmente quando os utilizadores ignoram alertas de segurança.
- A adoção de protocolos robustos (WPA2/WPA3) e boas práticas de gestão de certificados é essencial para garantir a integridade e confidencialidade das comunicações.

Sugestões para Trabalhos Futuros:

- Realizar testes com WPA, WPA2 e WPA3, analisando a resistência a ataques como Handshake Capture e KRACK.
- Explorar ferramentas de detecção de intrusão para identificar tentativas de MITM em tempo real.
- Implementar e avaliar mecanismos de HSTS e Certificate Pinning para mitigar ataques baseados em certificados falsos.
- Estudar o impacto da engenharia social na aceitação de certificados inválidos e propor estratégias de mitigação.

Referências

[1] N. Borisov, I. Goldberg, and D. Wagner, “Intercepting mobile communications: The insecurity of 802.11,” in Proc. ACM MobiCom, 2001.

[2] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4,” in Selected Areas in Cryptography (SAC 2001), 2001.

[3] IEEE, “IEEE 802.11i-2004 — MAC Security Enhancements,” 2004.

[4] NIST, “SP 800-38C: The CCM Mode for Authentication and Confidentiality,” 2008.

[5] M. Vanhoef and F. Piessens, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” in Proc. ACM CCS, 2017.

[6] Wi-Fi Alliance, “Wi-Fi CERTIFIED WPA3™ Security,” 2018.

[7] N. Borisov, I. Goldberg, and D. Wagner, “Intercepting mobile communications: The insecurity of 802.11,” in Proc. ACM MobiCom, 2001.

[8] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4,” in Selected Areas in Cryptography (SAC 2001), 2001.

[9] C. He and J. C. Mitchell, “Security Analysis and Improvements for IEEE 802.11i,” in Proc. Network and Distributed System Security Symposium (NDSS), 2005.

[10] Jisc Community, “WLAN Problems Arising from the Continued Use of WPA/TKIP,” Technical Report, 2009.

[11] B. Indira Reddy and V. Srikanth, “Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3),” Int. J. of Scientific Research in Computer Engineering and Information Technology, vol. 7, no. 5, 2019.

[12] IEEE, “IEEE 802.11-2020 — IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements,” 2020.

[13] M. Vanhoef e F. Piessens, “Dragonblood: Análise do Handshake Dragonfly do WPA3 e EAP-pwd,” em *Anais do Simpósio IEEE sobre Segurança e Privacidade*, San Francisco, CA, EUA, maio de 2020, pp. 517–533.

[14] Wi-Fi Alliance, “Wi-Fi CERTIFIED WPA3™ Segurança para redes pessoais e empresariais” .

[15] IEEE Transmitter, “Avanços no Wi-Fi e WiGig: Novas formas de usar as tecnologias do padrão IEEE 802.11,” IEEE, 2020.

[16] IEEE Spectrum, “Pesquisadores de segurança computacional acreditam que mais poderia ter sido feito pelo WPA3,” IEEE, 2019.

[17] D. J. Bernstein, *ChaCha20 Encryption and Decryption*, DevGlan.

[18] R. L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[19] J. Daemen and V. Rijmen, *Advanced Encryption Standard (AES)*, NIST FIPS PUB 197, Nov. 2001.

[20] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[21] T. Boylls, “How to Break WEP Encryption,” *wikiHow*, 2025. Disponível em: https://www.wikihow.com/Break-WEP-Encryption.

[22] Esri Support, “How to use Fiddler for e.g. ArcGIS Pro,” *Esri Knowledge Base*, Artigo ID: 000025158. Disponível em: https://support.esri.com/pt-br/knowledge-base/how-to-use-fiddler-for-e-g-arcgis-pro-000025158.