FACULDADE PROFESSOR MIGUEL ÂNGELO DA SILVA SANTOS – FeMASS

CURSO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

ESTUDO SOBRE OS PRINCIPAIS CIBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

CAIO LUCAS LIMA ALMEIDA

MACAÉ

2025

FACULDADE PROFESSOR MIGUEL ÂNGELO DA SILVA SANTOS – FeMASS
CURSO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

CAIO LUCAS LIMA ALMEIDA

ESTUDO SOBRE OS PRINCIPAIS CIBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

Trabalho Final apresentado ao curso de graduação em Sistemas de Informação, da Faculdade Professor Miguel Ângelo da Silva Santos (FeMASS), para obtenção do grau de BACHAREL em Sistemas de Informação.

Orientador: Professor Lahir Bockorni

MACAÉ/RJ
2025

CAIO LUCAS LIMA ALMEIDA

ESTUDO SOBRE OS PRINCIPAIS CIBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado ao curso de graduação em Sistemas de Informação, da Faculdade Professor Miguel Ângelo da Silva Santos (FeMASS), para obtenção do grau de BACHAREL em Sistemas de Informação.

Aprovada em 7 de julho de 2025

BANCA EXAMINADORA

Prof. Lahir Bockorni

Faculdade Professor Miguel Ângelo da Silva Santos (FeMASS)

1º Examinador

Prof. Martinelli de Oliveira Paula

Faculdade Professor Miguel Ângelo da Silva Santos (FeMASS)

2º Examinador

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO II

CURSO DE GRADUAÇÃO EM SISTEMA DE INFORMAÇÃO – FeMASS

Data da defesa: 07 / 07 / 2025.

Aluno: CAIO LUCAS LIMA ALMEIDA

Orientador: LAHIR BOCKORNI

Coorientador: –

Banca Examinadora: (nomes completos)

Presidente (Orientador): LAHIR BOCKORNI

Examinador (1): MARTINELLI DE OLIVEIRA PAULA

Examinador (2):

Título do trabalho:

ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM ATIVO DE REDE EM AMBIENTES CORPORATIVOS

Local: CIDADE UNIVERSITÁRIA – BLOCO A Sala: 205

Hora de início: 20H05 Hora do Término:

Em sessão pública, após exposição de cerca de 25 minutos, o aluno foi arguido oralmente pelos membros da banca, tendo como resultado para seu Trabalho de Conclusão de Curso II:

(X) APROVADO.

( ) REPROVADO.

Nota obtida: 9.0

Na forma regulamentar foi lavrada a presente ata que é abaixo assinada pelos membros da banca, na ordem acima determinada, e pelo aluno:

Macaé, 07 de JULHO de 2025.

Presidente

Examinador (1):

Examinador (2):

Aluno: Caio Lucas Lima Almeida

Faculdade Prof. Miguel Ângelo da Silva Santos
Fabíola Coelho de Carvalho
Secretaria Acadêmica
Matrícula: 8540

DEDICATÓRIA

Dedico aos meus pais, em especial à minha mãe, por nunca desistir de me ensinar e me manter nos estudos.

AGRADECIMENTO

Agradeço ao professor, Lahir Bockorni, por seu ensinamento e por ter me instigado a buscar conhecimento na área de tecnologia.

EPÍGRAFE

"Software é como sexo: É melhor quando é de graça."

Linus Torvalds

RESUMO

Este trabalho tem como objetivo estudar os principais ciberataques em ativos de rede em ambientes corporativos**,** com ênfase em redes *wireless*. A pesquisa aborda de forma teórica os ataques mais comuns em redes Wi-fi empresariais, analisando suas metodologias e impactos. Além disso, são realizadas práticas de pós-exploração, no qual são aplicadas técnicas para comprometer dispositivos conectados a uma rede, demonstrando como atacantes podem explorar vulnerabilidades descobertas. Complementando o estudo, foi aplicada uma pesquisa de campo com estudantes da FeMASS, com o objetivo de avaliar o nível de conhecimento prático e a percepção de segurança em ambientes com redes Wi-fi. Através de um questionário, foi possível levantar dados relevantes sobre o comportamento dos usuários e sua exposição a ataques como *Evil Twin*, *Captive* Portal, WPA2, ARP *Poisoning*, ARP *Spoofing* e Força Bruta. Os resultados reforçam a importância da conscientização e da adoção de boas práticas de segurança no uso de redes sem fio, especialmente em contextos corporativos e acadêmicos.

Palavras-chave: Ciberataques. *Evil Twin*. *Captive* Portal. WPA2. ARP *Poisoning*.

ABSTRACT

This work aims to study the main cyberattacks targeting network assets in corporate environments, with an emphasis on wireless networks. The research presents a theoretical overview of the most common attacks on enterprise Wi-fi networks, analyzing their methodologies and impacts. In addition, post-exploitation practices were carried out, applying techniques to compromise devices connected to a network, demonstrating how attackers can exploit discovered vulnerabilities. Complementing the study, a field survey was conducted with students from FeMASS, aiming to assess their practical knowledge and security awareness when connecting to Wi-fi networks. Through a structured questionnaire, relevant data were collected regarding user behavior and their exposure to attacks such as Evil Twin, Captive Portal, WPA2, ARP Poisoning, ARP Spoofing, and Brute Force. The results reinforce the importance of awareness and the adoption of good security practices when using wireless networks, especially in corporate and academic contexts.

Key words: Cyberattacks. Evil Twin. Captive Portal. WPA2. ARP Poisoning.

LISTA DE FIGURAS

Figura 1 - *Wi-fi* e Ethernet 20
Figura 2 - OSI x TCP/IP 24
Figura 3 – Matriz 4x4 base e chave 30
Figura 4 - Expansão de chave e *AddRoundKey* 30
Figura 5 - *SubBytes* 31
Figura 6 - *ShiftRows* 31
Figura 7 - *MixColumns* 32
Figura 8 - 3DES funcionamento 33
Figura 9 - *Twofish* funcionamento 34
Figura 10 - *Blowfish* funcionamento 37
Figura 11 - RC4 funcionamento 38
Figura 12 - Equação y^2 = x^3 + ax + b representada em um gráfico 40
Figura 13 - Pontos P, Q, R 41
Figura 14 - Algoritmo de Criptografia ElGamal 42
Figura 15 - Tríade CIA 51
Figura 16 - Configuração do *Hostpad* 54
Figura 17 - Exibição de dois ESSIDs iguais, um legítimo e outro falso 55
Figura 18 - *Log* capturado pelo *hostapd-wpe* após a desautenticação 55
Figura 19 - Execução do *asleap* para quebra de credenciais 56
Figura 20 - Conexão realizada com sucesso utilizando as credenciais adquiridas 56
Figura 21 - Captura de *handshake* 58
Figura 22 - Ataque DDoS ao site focoemsec.com.br 60
Figura 23 - Listagem de dispositivos na rede usando *Ettercap* 61
Figura 24 - Interceptação do tráfego 62
Figura 25 - Uso do Hydra na prática 64

LISTA DE GRÁFICOS

Gráfico 1 - Qual a sua faixa etária? 46
Gráfico 2 - Qual a sua área de atuação? 47
Gráfico 3 - Conferência se a rede é legitima antes de se conectar 47
Gráfico 4 - Você já inseriu dados pessoais ao conectar em uma rede *Wi-fi*? 48
Gráfico 5 - Investiga o porquê de estar desconectando frequentemente? 33
Gráfico 6 - Frequência do uso de autenticação de dois fatores 49
Gráfico 7 - Teve uma conta invadida após se conectar a uma rede pública? 49
Gráfico 8 - Você utiliza ferramentas como VPN, antivírus ou monitoramento de rede ao se conectar a *Wi-fi* pública? 50

SUMÁRIO

1. INTRODUÇÃO **13**

2 OBJETIVOS **15**

1. OBJETIVO GERAL 15

2. OBJETIVOS ESPECÍFICOS 15

3 JUSTIFICATIVA **16**

4 METODOLOGIA DE PESQUISA **18**

5 REFERENCIAL TEÓRICO **19**

5.1 TIPOS DE REDES DE COMPUTADORES 19

5.2 TECNOLOGIA DE REDES LOCAIS A GLOBAIS 20

5.3 MODELOS DE REFERÊNCIA 21

5.4 SEGURANÇA DE REDES 24

5.5 PRINCÍPIOS BÁSICOS DA SEGURANÇA 25

5.6 PRINCÍPIOS BÁSICOS DO ATAQUE 26

5.7 CRIPTOGRAFIA 27

5.8 ALGORITMO DE CHAVE SIMÉTRICA 29

5.8.1 AES *29*

5.8.2 3DES *32*

5.8.3 Twofish *33*

5.8.4 Blowfish *35*

5.8.5 RC4 *37*

5.9 ALGORITMO DE CHAVE ASSIMÉTRICA 39

5.9.1 RSA *39*

5.9.2 ECC *40*

5.9.3 ElGamal *42*

5.10 MARCO CIVIL 43

5.11 LGPD 44

6 PESQUISA DE CAMPO **46**

6.1 COLETA DE DADOS 46

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS **51**

7.1 OBJETIVOS DOS ATAQUES EM REDES *WIRELESS* 52

7.1.1 Evil Twin *52*

7.1.2 Ataque de WPA Enterprise *53*

7.1.3 Ataque WPA2 *57*

7.1.4 Ataque DDoS *59*

7.2 PÓS-EXPLORAÇÃO EM REDES 60

7.2.1 ARP Poisoning - Interceptação de Login em um Ambiente de Testes *60*

7.2.2 Ataque de Força Bruta *63*

CONSIDERAÇÕES FINAIS **65**

REFERÊNCIAS 66

ANEXO A – DECLARAÇÃO DE CORREÇÃO GRAMATICAL **68**

ANEXO B – PARECER TÉCNICO **69**

1. INTRODUÇÃO

Para entender os desafios relacionados aos ciberataques é fundamental contextualizarmos o espaço cibernético. De acordo com o Barros *et. al* (2011), o espaço cibernético é um ambiente digital formado por dispositivos computacionais conectados a redes ou operando de forma independente, no qual dados são transmitidos, processados e armazenados, sendo que as atividades ofensivas nesse espaço podem comprometer seriamente a segurança nacional.

A segurança desse ambiente está relacionada aos princípios de confidencialidade, integridade e disponibilidade, como destacado por Fraga (2017). Esses princípios não se aplicam apenas a sistemas computacionais e informações digitais, mas abrangem todas as formas de proteção de dados, sendo essenciais para a segurança de computadores e sistemas. As normas de segurança da informação, como a série ISO/IEC 27000, evoluíram para estabelecer padrões internacionais que guiam a proteção dos dados e sistemas, garantindo uma abordagem estruturada para mitigar riscos cibernéticos.

A atuação internacional do Brasil em cibersegurança é coordenada por diversos órgãos governamentais e entidades especializadas. Em 2024, o Brasil instituiu o Grupo de Trabalho Temático para Definição de Parâmetros de Atuação Internacional do Brasil em Cibersegurança (GTT Internacional), conforme a Resolução CNCiber nº 4, de 25 de março de 2024. Esse grupo, composto por representantes de ministérios e entidades como o Ministério das Relações Exteriores e a Agência Nacional de Telecomunicações (Anatel), visa estabelecer diretrizes para a colaboração internacional, alinhando-se com os esforços globais para garantir a segurança cibernética e a proteção dos direitos fundamentais no ambiente digital (BRASIL, 2024).

Essas ameaças, definidas pela IBM como tentativas deliberadas de comprometer dados e sistemas por meio de ataques não autorizados, utilizam técnicas como *malware* (*software* malicioso para explorar vulnerabilidade e ter acesso não autorizado), *phishing* (fraude eletrônica) e *ransomware* (*malware* que faz criptografia dos arquivos da vítima e solicita pagamento para liberar a chave de descriptografia) para explorar vulnerabilidades de segurança. Com a crescente digitalização de empresas, governos e cidadãos, a proteção contra esses ataques tornou-se uma prioridade estratégica, vital para garantir a integridade dos sistemas e a segurança dos dados sensíveis (IBM, 2024).

Uma rede de computadores, conforme descrito por Tanenbaum; Feamster; Wetherall (2021), consiste em um conjunto de computadores autônomos interconectados por uma tecnologia específica, permitindo a troca de informações entre eles. Essas conexões podem ocorrer através de diferentes meios, como fios de cobre, fibras ópticas, micro-ondas,

infravermelho ou, até mesmo, satélites de comunicação. Redes podem variar em tamanho e forma, desde pequenas redes locais até redes globais interconectadas, como a *Internet*. A rede em si permite o compartilhamento de recursos e informações entre usuários e dispositivos, independentemente de sua localização geográfica.

A importância do estudo da prática de segurança para mitigação de ciberataques em ativos de rede é evidenciada por dados alarmantes sobre a crescente ameaça cibernética. De acordo com a pesquisa da CNN Brasil (2024), o Brasil, maior país da América Latina e um dos principais alvos globais de ataques *hackers*, registrou 357.422 incidentes no segundo semestre de 2023, um aumento de 8,86% em relação ao semestre anterior. Setores críticos como telecomunicações sem fio, transporte de cargas e processamento de dados enfrentam um crescente volume de ataques, com a telecomunicação sem fio experimentando um aumento dramático de 142,47% nos ataques. Este cenário ressalta a necessidade urgente de adotar práticas robustas de segurança cibernética para proteger redes e ativos essenciais, reduzindo vulnerabilidades e prevenindo danos significativos em um ambiente cada vez mais perigoso.

2 OBJETIVOS

1. Objetivo Geral

O presente Trabalho tem como objetivo geral analisar os principais ataques cibernéticos direcionados a redes *wireless* em ambientes corporativos, destacando suas técnicas e impactos. Além disso, busca-se aplicar práticas de pós-exploração em um ambiente controlado, bem como avaliar o nível de conscientização dos usuários por meio de um questionário, a fim de compreender as fragilidades e técnicas que contribuem para a vulnerabilidade das redes sem fio nas organizações.

2. Objetivos específicos

- Apresentar teoricamente ataques em redes *wireless* corporativos;
- Explorar ataques de pós-exploração tanto na teoria quanto na prática;
- Apresentar questionário via *google forms* sobre o conhecimento que os estudantes da FeMASS têm sobre ataques de *Pentest*.

3 JUSTIFICATIVA

É evidente que, na sociedade em rede aberta, sem barreiras ou delimitações, surgem novos desafios relacionados à cibersegurança. Isso acontece porque essas redes são construídas em estruturas colaborativas, baseadas em protocolos e tecnologias comuns, o que as torna vulneráveis a ataques. É de extrema importância reconhecer que os ciberataques visam comprometer três principais propriedades da informação: confidencialidade, integridade e disponibilidade. A confidencialidade se refere à proteção contra acessos não autorizados, garantindo que apenas pessoas autorizadas possam obter a informação. A integridade assegura que os dados permaneçam precisos e inalterados, preservando sua veracidade. Já a disponibilidade garante que os usuários autorizados possam acessar as informações e sistemas sempre que necessário, sem interrupções ou obstruções (Caldas, 2013).

Parte desses ataques ocorre por meio da prática de *Pentest* (*Penetration Test* – Teste de Intrusão), que visa identificar, enumerar e explorar vulnerabilidades utilizando técnicas baseadas em uma metodologia estruturada. Vale destacar que é comum haver confusão entre análise de vulnerabilidades e *Pentest*. O teste de segurança ou *Pentest*, busca identificar vulnerabilidades potenciais, frequentemente utilizando *scanners* customizados, como o BID (Bugtraq ID – Identificação de Vulnerabilidades), CAN/CVE (*Common Vulnerabilities and Exposures* – Vulnerabilidades e Exposições Comuns) e OSVDB (*Open Source Vulnerability Database* – Banco de Dados de Vulnerabilidades de Código Aberto). Por outro lado, a análise de vulnerabilidade não tem como objetivo testar ou explorar uma vulnerabilidade a ponto de confirmar se ela pode ser efetivamente utilizada como uma ameaça, por exemplo, para obter acesso a sistemas (Melo, 2017).

É importante destacar que os ataques frequentemente ocorrem em ambientes *Wireless*, que são sistemas de transmissão de dados flexíveis, alternativos às redes cabeadas. A *WLAN (Wireless Local Area Network)* ou rede local sem fio, utiliza ondas de rádio para estabelecer conexões de *internet* ou para interconectar dispositivos em uma rede local, em contraste com redes fixas como ADSL ou conexões de TV, que normalmente utilizam cabos físicos. O IEEE (*Institute of Electrical and Electronics Engineers*) é responsável pela criação e padronização dos protocolos e normas operacionais para essas redes. A configuração da rede sem fio envolve o uso de um SSID (*Service Set Identifier*) para identificar a rede e, se a criptografia estiver habilitada, o uso de uma chave WEP (*Wired Equivalent Privacy*) ou WPA (*Wi-fi Protected Access*) para proteger a comunicação (Macêdo, 2012).

Por outro lado, os ciberataques também desempenham um papel crucial na manutenção da segurança das empresas. Eles são essenciais para identificar falhas intrínsecas nas redes

testadas, permitindo que as organizações descubram vulnerabilidades que poderiam ser exploradas por atacantes. A partir dessas descobertas, é possível desenvolver e implementar mecanismos de defesa adequados e específicos para a corporação, fortalecendo assim a segurança geral da rede (Moreno, 2015).

Esse trabalho visa mostrar a necessidade de mitigar os ataques cibernéticos em um cenário cada vez mais digital e interconectado. O estudo aprofundado de redes *wireless* é crucial, pois essas redes, ao oferecerem flexibilidade e mobilidade, também introduzem vulnerabilidades específicas que podem ser exploradas por cibercriminosos. A inclusão do *Pentest* (teste de penetração) neste trabalho permite o estudo de ataques reais, identificando e explorando falhas antes que possam ser aproveitadas maliciosamente. Além disso, a análise de pós-exploração é vital para entender as consequências e a extensão dos ataques, fornecendo informações essenciais para a correção e proteção contínua dos sistemas. Portanto, abordar esse estudo fortalece o enfrentamento, neutralização ameaças cibernéticas e um ambiente de rede mais seguro (Kevin, 2022).

4 METODOLOGIA DE PESQUISA

Segundo Schwartzman (2001), a ciência pode ser entendida como um conjunto de conhecimentos acumulados e concorrentemente transformados, organizados de acordo com a lógica e métodos próprios de cada área. Nesse contexto, a pesquisa científica se estrutura de forma ordenada, podendo ser classificada quanto aos fins e quanto aos meios.

Quanto aos fins, objetivo deste estudo baseia-se em uma abordagem exploratória, ao buscar apresentar de forma clara o problema da segurança em redes *wireless* e a vulnerabilidade a ataques cibernéticos. Além disso, adota-se também uma abordagem explicativa, uma vez que os conceitos relacionados ao tema, como os protocolos de segurança, técnicas de ataque e pós-exploração, serão analisados em profundidade. Essa análise possibilitará uma compreensão mais detalhada dos desafios de segurança em redes sem fio.

Neste contexto, será adotado o método indutivo, no qual a observação de técnicas específicas de intrusão, como ataques direcionados a redes *wireless* e vulnerabilidades em protocolos de segurança, servirá como base para a identificação de padrões de ataque. A partir da análise de casos particulares, busca-se compreender melhor as fragilidades exploradas em diferentes contextos de rede, sem, no entanto, focar em estratégias de mitigação ou defesa (Cristiano, 2013).

A pesquisa adotará uma abordagem metodológica mista, combinando métodos qualitativos e quantitativos. A predominância qualitativa se justifica pela análise descritiva dos dados obtidos por meio de estudos de caso, simulações de ataques (*Pentest*) e análises técnicas de vulnerabilidades. Por outro lado, a dimensão quantitativa será incorporada com a aplicação de um questionário direcionado aos alunos da FeMASS, a fim de avaliar seu nível de conhecimento e conscientização sobre ciberataques. Essa combinação possibilita uma maior compreensão do fenômeno investigado.

Quanto aos meios os testes práticos serão realizados em ambiente controlado, utilizando o adaptador TP-LINK WN821N configurado em modo de monitoramento. Esse modo permite capturar pacotes de dados transmitidos pelas redes *Wi-fi*, sem a necessidade de conexão direta, o que é essencial para a coleta de dados e execução de simulações de ataques. O sistema operacional utilizado será o *Kali Linux*, amplamente reconhecido na área de segurança da informação, executado em máquina virtual por meio do *VirtualBox*. Essa configuração garante um ambiente seguro e isolado para a realização dos experimentos, permitindo a identificação e análise das vulnerabilidades presentes nas redes sem fio.

5 REFERENCIAL TEÓRICO

O presente referencial teórico tem como objetivo abordar os principais fundamentos que sustentam o funcionamento e a segurança das redes de computadores. Para isso, foram apresentados os diferentes tipos de redes e suas tecnologias, além dos modelos de referência que compõe sua comunicação. Foram apresentados os princípios básicos de segurança e os tipos de ataques que ameaçam a integridade e confidencialidade das informações. Por fim, são explorados os conceitos de criptografia, destacando os algoritmos de chave simétrica e de chave pública como mecanismos essenciais de proteção dos dados.

5.1 Tipos de redes de computadores

Segundo Tanenbaum (2021), há diversos tipos de redes de computadores, sendo que o autor dá ênfase às mais relevantes no contexto atual. As redes de banda larga se popularizaram significativamente com a democratização dos computadores, podendo ser acessadas por meio de cabos de cobre, cabos coaxiais ou fibra óptica.

As redes baseadas em fibra óptica foram fundamentais para expandir a conectividade a locais anteriormente inimagináveis, como veículos (carros, barcos e aviões), dispositivos móveis utilizados por entregadores de aplicativo, forças armadas e sistemas de transporte. Os *hotspots* sem fio, baseados no padrão IEEE 802.11, foram projetados para dispositivos portáteis e contribuíram para a popularização do acesso à *internet* em qualquer lugar. Com isso, houve uma mudança significativa nos hábitos de comunicação, como o abandono do SMS, cujas mensagens tinham um custo por envio, mesmo que baixo.

As redes de provedores de conteúdo atendem a crescente demanda por dados, utilizando amplamente a computação em nuvem. Muitos desses provedores adotam CDNs (*Content Delivery Networks*), que consistem em servidores distribuídos geograficamente para reduzir a latência, mantendo os dados mais próximos dos usuários finais. Quando o provedor de conteúdo e o provedor de serviços de *internet* (ISP - *Internet Service Provider*) não estão diretamente conectados, é comum recorrerem a uma rede de trânsito, que realiza o transporte do tráfego de ponta a ponta, geralmente mediante cobrança. Se houver troca significativa de dados entre as partes, pode-se optar por uma interconexão direta. Tradicionalmente, essas redes de trânsito são conhecidas como redes *backbone*.

As redes comerciais são amplamente utilizadas em empresas e universidades, permitindo o compartilhamento de recursos entre um grande número de computadores. Frequentemente, essas redes utilizam VPNs (*Virtual Private Networks*) para integrar filiais e

unidades distintas, criando uma rede lógica única, mesmo que os dispositivos estejam distribuídos em diferentes localizações físicas.

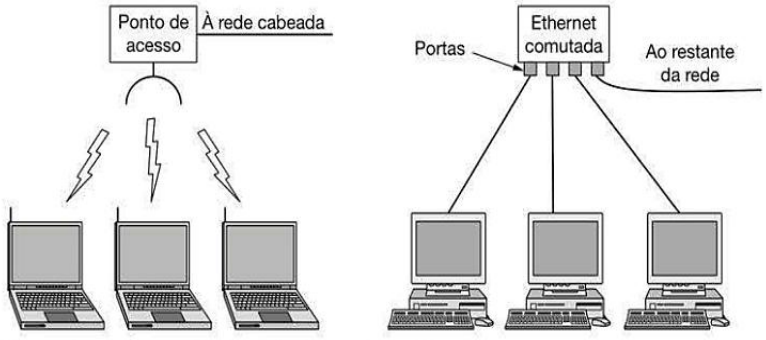
5.2 Tecnologia de redes locais a globais

As redes de computadores se organizam em diferentes escalas, de acordo com o seu alcance geográfico e aplicação. Redes pessoais ou PANs (*Personal Area Networks*) permitem que dispositivos se comuniquem em um alcance restrito à proximidade de uma pessoa. Exemplos comuns incluem a conexão entre um *smartphone* e um fone de ouvido *Bluetooth* ou entre um *notebook* e um mouse sem fio.

Uma rede local ou LAN (*Local Area Network*) é uma rede privada que opera em áreas restritas, como residências, escritórios ou fábricas. Essas redes são amplamente utilizadas para conectar computadores e dispositivos eletrônicos, permitindo o compartilhamento eficiente de recursos, como impressoras, arquivos e o acesso à *internet*. As LANs podem ser cabeadas, com velocidades variando de 100 Mbps a 40 Gbps, utilizando o padrão Ethernet (IEEE 802.3) ou sem fio, através do padrão IEEE 802.11 (*Wi-fi*), com taxas que vão de 11 Mbps (802.11b) até 7 Gbps (802.11ad).

Uma característica fundamental das LANs modernas é o uso de redes comutadas, nas quais *switches* são responsáveis por direcionar os pacotes de dados apenas aos dispositivos de destino, aumentando o desempenho e a segurança da rede em comparação com redes baseadas em *broadcast*. Além disso, é possível segmentar uma LAN física em diferentes LANs lógicas por meio de VLANs (*Virtual LANs*), o que proporciona maior organização, controle de tráfego e isolamento de segmentos da rede. Em redes sem fio, o acesso pode ser controlado por métodos de alocação estática ou dinâmica de tempo, dependendo da topologia e dos protocolos empregados.

Figura 1 - *Wi-fi* e Ethernet



Fonte: TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. Redes de Computadores (coedição Bookman e Pearson). [s.l.] Bookman Editora, 2021.

Embora, tecnicamente sejam LANs, as redes domésticas possuem características distintas. Seus dispositivos precisam ser de fácil instalação e manutenção. Além disso, apresentam riscos maiores de segurança, pois muitos dispositivos conectados, como câmeras e assistentes virtuais, podem comprometer diretamente a privacidade e segurança dos usuários. Essas redes evoluem organicamente com a adição de novos dispositivos, o que resulta em uma grande variedade tecnológica. Por questões de custo, muitos dos equipamentos utilizados priorizam o baixo preço, o que pode comprometer a robustez e a segurança da rede.

As redes metropolitanas ou MANs (*Metropolitan Area Networks*) cobrem áreas maiores como cidades inteiras. Um exemplo tradicional é a rede de TV a cabo, que evoluiu para também oferecer serviços de *internet* em banda larga por meio da utilização de partes não ocupadas do espectro de transmissão. Outro exemplo é a padronização do IEEE 802.16, voltada para o fornecimento de acesso à *internet* de alta velocidade sem fio em ambientes urbanos.

As redes de longa distância ou WANs (*Wide Area Networks*) abrangem grandes regiões geográficas, podendo cobrir países ou até continentes. Um exemplo típico de WAN é a *internet*, além da rede de telefonia celular. Em geral, essas redes são compostas por linhas de transmissão e elementos de comutação, sendo capazes de interligar diferentes redes locais através de enlaces de fibra óptica, cabos coaxiais, cobre ou sinais de rádio.

As redes interligadas são formadas pela conexão de diferentes tipos de redes, operadas de forma independente. Por exemplo, a interconexão entre uma LAN e uma WAN ou entre duas LANs de tecnologias distintas caracteriza uma rede interligada. Essa integração permite maior alcance e flexibilidade no tráfego de dados, sendo fundamental para o funcionamento da internet. Quando diferentes redes pagam para se interconectar ou utilizam tecnologias variadas (como cabeamento versus *wireless*), essa composição se enquadra no conceito de redes interligadas.

5.3 Modelos de referência

O projeto de protocolos em camadas é uma das abstrações mais importantes no desenvolvimento de redes de computadores. Essa abordagem permite dividir a complexidade da comunicação entre sistemas em níveis bem definidos, nos quais cada camada executa funções específicas e se comunica apenas com as camadas logo acima e abaixo. A ideia principal é definir claramente as responsabilidades de cada camada, bem como suas interfaces e os protocolos que regem a troca de dados entre entidades equivalentes em sistemas diferentes.

O modelo OSI (*Open Systems Interconnection*), desenvolvido pela ISO, é um modelo teórico amplamente utilizado como referência didática. Ele se baseia em três conceitos

fundamentais: serviços, interfaces e protocolos. Os serviços determinam o que uma camada oferece à camada superior; as interfaces descrevem como as camadas se comunicam internamente; e, os protocolos especificam como as camadas equivalentes em máquinas diferentes interagem.

O modelo OSI é dividido em sete camadas: física, enlace de dados, rede, transporte, sessão, apresentação e aplicação. Cada uma possui responsabilidades próprias, desde a transmissão de *bits* no meio físico até a interação com os *softwares* de aplicação do usuário. Isso inclui funções como roteamento, controle de erros, criptografia e gerenciamento de sessões. Essa separação permite um alto grau de modularidade e facilita a padronização de tecnologias, sendo especialmente útil para fins de estudo e compreensão da arquitetura de redes.

A camada física, a mais baixa do modelo OSI, é responsável pela transmissão dos *bits* brutos por meio de um canal físico de comunicação. Ela define características como voltagem, temporização de sinais, conectores, meios de transmissão e os aspectos mecânicos e elétricos da conexão. Essa camada trata, exclusivamente, da movimentação de dados em nível físico, sem considerar seu significado ou estrutura.

Logo acima, a camada de enlace de dados organiza os *bits* da camada física em unidades chamadas quadros, sendo responsável por detectar e, em alguns casos, corrigir erros que possam ocorrer durante a transmissão. Também realiza o controle de fluxo para que o transmissor não sobrecarregue o receptor, além de fornecer endereçamento físico por meio de endereços MAC.

A camada de rede tem como principal função o roteamento dos pacotes de dados entre redes distintas, determinando o melhor caminho que os dados devem seguir para chegar ao seu destino. Essa camada também se responsabiliza pelo endereçamento lógico (como os endereços IP), pela fragmentação de pacotes e pelo controle de congestionamento, quando necessário.

A camada de transporte garante que a comunicação entre as aplicações de origem e destino seja confiável e eficiente. Ela cuida da segmentação dos dados, da detecção de erros, da retransmissão de segmentos perdidos e do controle de fluxo entre os hosts finais. Protocolos como o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*) são exemplos típicos dessa camada.

Acima dela está a camada de sessão, cuja função é estabelecer, gerenciar e encerrar sessões de comunicação entre aplicações. Essa camada mantém o controle sobre quem transmite em determinado momento, permite a sincronização de diálogos e oferece mecanismos para retomada de sessões interrompidas.

A camada de apresentação é responsável por traduzir os dados entre o formato utilizado pela aplicação e aquele utilizado na transmissão. Além disso, ela pode realizar a compactação

dos dados, a criptografia e a conversão de padrões de codificação (como EBCDIC para ASCII), garantindo que diferentes sistemas compreendam os dados trocados.

No topo da pilha está a camada de aplicação, que oferece diretamente os serviços de rede aos usuários finais. Protocolos como HTTP, FTP, SMTP e DNS operam nessa camada, possibilitando navegação na *web*, envio de *e-mails*, transferência de arquivos e resolução de nomes de domínio. Essa camada é onde ocorre a real interação do usuário com a rede, por meio de softwares específicos.

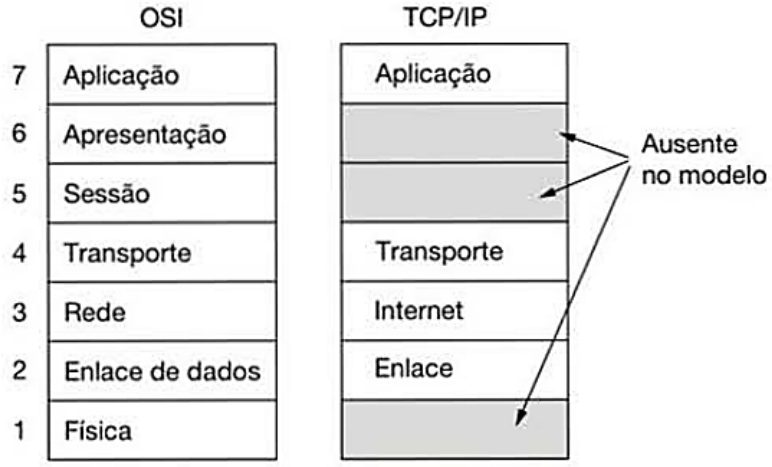
Já o modelo TCP/IP foi o pioneiro prático no desenvolvimento da comunicação entre redes de longa distância, sendo aplicado inicialmente na ARPANET, precursora da *internet* moderna. Diferente do OSI, esse modelo adota uma estrutura mais simples e funcional, composta por quatro camadas principais: enlace, *internet*, transporte e aplicação.

A camada de enlace, a mais baixa, trata da transmissão física e lógica de dados entre dispositivos, usando tecnologias como linhas seriais e redes Ethernet. A camada de *internet* define o formato dos pacotes IP (*Internet Protocol*) e utiliza também o ICMP (*Internet Control Message Protocol*), que auxilia no envio de mensagens de controle e diagnóstico. A principal função dessa camada é entregar os pacotes IP ao destino, sendo o roteamento um aspecto essencial para seu funcionamento. Já o controle de congestionamento, embora necessário, requer apoio das camadas superiores.

Acima dela, a camada de transporte garante uma comunicação confiável entre os processos de origem e destino nos *hosts*, sendo o TCP (*Transmission Control Protocol*) o principal protocolo utilizado. Ao contrário do OSI, o modelo TCP/IP não possui camadas específicas de sessão e apresentação, pois essas funções são normalmente tratadas diretamente pela aplicação. A camada de aplicação engloba todos os protocolos de alto nível, como TELNET, FTP e SMTP, que oferecem funcionalidades como acesso remoto, transferência de arquivos e envio de mensagens eletrônicas.

Abaixo, há uma imagem que apresenta as principais diferenças entre o modelo OSI e o modelo TCP/IP, comparando sua estrutura e as funções de cada camada para melhor compreensão.

Figura 2 - OSI x TCP/IP



Fonte: TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. Redes de Computadores (coedição *Bookman* e *Pearson*). [s.l.] Bookman Editora, 2021.

5.4 Segurança de redes

Visto que no início da existência das redes de computadores elas eram utilizadas, principalmente por pesquisadores, para envio de correio eletrônico e por algumas empresas para o compartilhamento de impressoras, a segurança não era uma preocupação central. É importante destacar que a prática de invasão de redes já existia muito antes do surgimento da *internet*. Um exemplo disso é o *phreaking*, que teve início no fim da década de 1950, quando pessoas exploravam falhas nos sistemas telefônicos para fazer chamadas gratuitas.

O caso mais conhecido envolveu John Draper, que descobriu que um apito de brinquedo, incluído nas caixas de cereal "*Cap'n Crunch",* no final dos anos 1960, emitia um som na frequência de 2600 Hz. Curiosamente, essa era a mesma frequência usada pela operadora AT&T para autorizar chamadas de longa distância. Utilizando o apito, Draper conseguia explorar essa vulnerabilidade para realizar chamadas sem custo.

A forma mais básica e eficaz de lidar com problemas de segurança em redes é seguir os princípios da tríade CIA, sigla para Confidencialidade, Integridade e Disponibilidade. A confidencialidade está relacionada à proteção das informações, impedindo o acesso por usuários não autorizados. A integridade garante que a informação recebida seja exatamente a mesma que foi enviada, sem modificações no caminho. Já a disponibilidade assegura que os sistemas e serviços estejam sempre acessíveis, evitando interrupções causadas por falhas, sobrecargas ou erros. Um exemplo clássico de ataque que compromete a disponibilidade é o ataque de negação de serviço, frequentemente direcionado a bancos, companhias aéreas e outros serviços essenciais.

5.5 Princípios básicos da segurança

Os princípios fundamentais da segurança da informação foram propostos em 1975, por Jerome Saltzer e Michael Schroeder. Eles definem diretrizes que ajudam a projetar sistemas mais seguros e confiáveis. O primeiro desses princípios é o da economia de mecanismos, que valoriza a simplicidade na construção dos sistemas. Quanto mais simples um sistema, menor a chance de conter falhas e mais fácil é seu entendimento pelos usuários. Isso reduz o risco de mau uso e limita as possíveis superfícies de ataque. Em outras palavras, funções desnecessárias devem ser removidas para evitar vulnerabilidades adicionais.

O princípio do padrão seguro (*default* seguro) estabelece que, ao definir quem pode acessar um recurso, é mais seguro negar o acesso por padrão e permitir apenas quando houver autorização explícita. Assim, a ausência de permissão deve significar bloqueio automático, reduzindo as chances de acesso indevido.

O princípio da mediação completa afirma que todo acesso a um recurso deve ser verificado, sem exceções. Isso implica que o sistema precisa ser capaz de identificar claramente quem está fazendo a solicitação e garantir que cada ação seja devidamente autorizada antes de ser executada.

O princípio da menor autoridade, conhecido pela sigla POLA (*Principle of Least Authority*), indica que cada componente ou processo deve ter apenas os privilégios mínimos necessários para cumprir sua função. Se um invasor comprometer esse componente, os danos serão limitados, pois ele não terá acesso a mais do que o estritamente necessário.

O princípio da separação de privilégios está relacionado ao POLA e sugere que é melhor dividir um sistema em partes menores, cada uma com permissões específicas, do que concentrar todos os privilégios em um único componente. Isso evita que a falha de um único ponto comprometa o sistema inteiro.

O princípio do mecanismo menos comum recomenda minimizar o compartilhamento de recursos entre usuários. Componentes utilizados por muitos usuários simultaneamente podem se tornar canais de vazamento de informações. Por exemplo, se uma funcionalidade for implementada diretamente no sistema operacional e compartilhada globalmente, é mais arriscado do que se ela estivesse isolada em uma biblioteca usada individualmente por cada processo.

O princípio do projeto aberto afirma que a segurança de um sistema não deve depender do sigilo do seu funcionamento. Esse princípio se baseia na ideia de que os algoritmos e estruturas de segurança devem ser públicos e revisáveis, como já estabelecido na criptografia

pelo princípio de Kerckhoffs. A chamada “segurança pela obscuridade” é uma prática frágil, pois assume que o adversário nunca entenderá o sistema, o que é uma falsa garantia.

Por fim, o princípio da aceitabilidade psicológica destaca que os mecanismos de segurança devem ser fáceis de usar e compreender. Se as medidas forem muito complexas, os usuários tendem a evitá-las ou ignorá-las, comprometendo a proteção do sistema. Além disso, é essencial que os usuários entendam o propósito das regras de segurança, aumentando sua adesão e colaboração com a proteção do ambiente.

5.6 Princípios básicos do ataque

A melhor maneira de entender como um ataque funciona é pensar como um invasor. A primeira fase é a de reconhecimento, que consiste em coletar o máximo de informações sobre o alvo. Se o ataque envolver spam ou engenharia social, por exemplo, o atacante pode investigar perfis *online* das vítimas para entender seus hábitos, preferências ou obter dados sensíveis. Em casos extremos, pode até procurar informações em documentos descartados fisicamente no lixo.

Sniffing e *Snooping* são técnicas usadas para interceptar o tráfego da rede. Quando os dados trafegam sem criptografia, torna-se fácil para o invasor capturar informações confidenciais. Mesmo quando há criptografia, o tráfego ainda pode revelar padrões úteis, como quem está se comunicando com quem, horários e endereços MAC. Para o atacante conseguir interceptar esses dados, é sinal de que princípios como a menor autoridade e a mediação completa não foram devidamente aplicados no ambiente.

Spoofing é uma técnica em que o invasor assume uma identidade falsa na rede, tentando se passar por outro dispositivo. Isso pode ser feito por meio da alteração do endereço de origem dos pacotes Ethernet ou IP, com o objetivo de burlar mecanismos de segurança ou realizar ataques como o de negação de serviço. Embora esse processo seja relativamente simples em protocolos básicos, ele encontra limitações em protocolos mais complexos, como o TCP. Por exemplo, ao tentar estabelecer uma conexão forjada, o atacante não recebe as respostas do servidor e, por isso, não consegue completar a comunicação. Mesmo assim, o *spoofing* representa uma quebra no princípio da mediação completa, pois, sem a verificação precisa da origem das solicitações, torna-se impossível controlá-las de forma eficaz.

Interrupção está ligada ao terceiro pilar da segurança da informação: a disponibilidade. Os ataques de negação de serviço (DoS) visam tornar sistemas e serviços indisponíveis, afetando bancos, empresas e até serviços públicos. Esses ataques evoluíram com o tempo, tornando-se mais complexos e difíceis de conter. Eles se aproveitam da falta de isolamento adequado entre os componentes do sistema, violando o princípio do mecanismo menos comum.

5.7 Criptografia

O primeiro princípio da criptografia garante que toda mensagem criptografada precisa conter algum tipo de informação extra que permita verificar sua validade. Isso significa que a mensagem deve ter dados redundantes, ou seja, informações que não são essenciais para o conteúdo, mas que ajudam a identificar se ela é legítima ou não.

Por exemplo, uma empresa chamada Encomenda Rápida que possui milhares de produtos e envia pedidos de forma automatizada. Os programadores dessa empresa decidem criar mensagens curtas para os pedidos. O nome do cliente ocupa dezesseis espaços e depois disso vem um pequeno bloco criptografado com as informações do produto. Esse bloco criptografado tem apenas três espaços e armazena a quantidade e o código do item. A chave usada para proteger esse bloco é secreta e conhecida apenas pelo cliente e pela empresa.

A ideia parece funcionar bem. Ninguém pode ler as mensagens se não tiver a chave certa. Mas existe uma falha grave. Suponha que um ex-funcionário da empresa, irritado após ser demitido, queira causar prejuízos. Ele ainda tem uma cópia parcial da lista de clientes e decide criar mensagens falsas com nomes reais. Como ele não tem acesso à chave, ele simplesmente preenche os últimos três espaços com valores aleatórios e envia centenas de pedidos para a empresa.

O sistema da empresa, ao receber esses pedidos, identifica o nome do cliente, procura a chave correspondente e tenta decifrar a mensagem. Como quase todas as combinações desses três espaços geram pedidos válidos, o sistema acredita que os pedidos são reais. Ele começa a preparar remessas estranhas, como trezentos *skates* ou seiscentas redes de descanso, pensando que o cliente tem um bom motivo para isso. O ex-funcionário, mesmo sem entender o conteúdo das mensagens, consegue causar transtornos.

Esse problema pode ser evitado com a inclusão de informações extras dentro da parte criptografada. Por exemplo, ao aumentar a parte criptografada de três para doze espaços, nove deles poderiam ter um valor fixo, como zeros ou um padrão acordado. Assim, mensagens falsas têm menos chance de passar pelo sistema. O atacante não consegue adivinhar os valores certos com facilidade e o sistema ignora as mensagens inválidas.

Esse tipo de proteção é muito útil contra quem tenta enganar o sistema, mas torna a vida mais fácil para quem quer espionar as mensagens. Por exemplo, se uma empresa concorrente da Encomenda Rápida intercepta os pedidos, ela pode verificar se uma mensagem é válida ou não. Isso ajuda a decifrar os dados com mais facilidade e entender, por exemplo, quais produtos estão sendo vendidos.

Existe um equilíbrio delicado nessa situação. A informação extra dificulta ataques que tentam bagunçar o sistema, mas facilita a ação de quem quer descobrir o conteúdo da comunicação. Por isso, é importante escolher bem o tipo de informação que será incluída.

Também é importante não usar sequências óbvias como zeros no começo ou no fim da mensagem. Isso pode tornar o trabalho do espião mais fácil, já que padrões simples ajudam a adivinhar partes da mensagem. Em vez disso, o ideal é usar um código de verificação, como um cálculo matemático aplicado ao conteúdo. Uma opção ainda mais segura é usar um tipo especial de código chamado *hash* criptográfico, que serve como uma assinatura única da mensagem. Esse tipo de verificação permite que o sistema reconheça mensagens falsas sem facilitar a quebra da proteção.

O segundo princípio da criptografia trata da importância de garantir que uma mensagem recebida seja realmente recente. Em outras palavras, o sistema precisa ter uma forma de verificar se aquela mensagem acabou de ser enviada e não é uma cópia antiga.

Esse cuidado é necessário porque, caso contrário, um invasor ativo pode capturar mensagens legítimas e reenviá-las várias vezes, como se fossem novas. Mesmo que não consiga entender o conteúdo, ele ainda pode causar transtornos ao sistema.

Por exemplo, imagine que um ex-funcionário mal-intencionado consiga ouvir a comunicação de uma empresa e repita mensagens de pedidos antigos que ainda são tecnicamente válidas. Isso poderia fazer com que o sistema da empresa reenviasse produtos ou registrasse ações repetidas, o que traria prejuízos.

Para evitar esse tipo de ataque, é preciso implementar algum mecanismo que torne cada mensagem única e válida apenas por um tempo limitado. Esse é o segundo princípio da criptografia: adotar uma forma eficaz de impedir ataques de repetição.

Uma solução simples seria adicionar um registro de data e hora em cada mensagem. Esse registro indicaria que a mensagem só deve ser aceita se tiver sido enviada nos últimos sessenta segundos. O sistema receptor manteria um histórico das mensagens recentes, rejeitando qualquer duplicata ou mensagem enviada fora desse intervalo.

Mensagens mais antigas seriam descartadas automaticamente, tornando inútil qualquer tentativa de reenvio após o prazo. Essa técnica exige que os relógios dos dois sistemas estejam razoavelmente sincronizados. Por isso, o tempo limite não pode ser curto demais, como cinco segundos, pois pequenas diferenças entre os relógios poderiam causar falhas na comunicação legítima.

Outras formas de proteger o sistema contra esse tipo de ataque, além do uso de registros de tempo, também são possíveis e serão explicadas mais à frente. O essencial é entender que

sem alguma forma de controle temporal, o sistema fica vulnerável a ataques baseados na repetição de mensagens válidas.

5.8 Algoritmo de chave simétrica

A criptografia de chave simétrica é um dos pilares fundamentais da segurança da informação, sendo amplamente empregada em contextos onde o desempenho e a confidencialidade são essenciais. Seu princípio básico é o uso de uma mesma chave para criptografar e descriptografar a informação. Isso significa que tanto o emissor quanto o receptor da mensagem devem possuir e manter em segredo a mesma chave. Essa característica torna a criptografia simétrica extremamente rápida e eficiente, especialmente para grandes volumes de dados, como arquivos ou transmissões contínuas.

Seu principal desafio está na distribuição segura da chave entre as partes, uma vez que, se essa chave for interceptada, toda a comunicação pode ser comprometida. No contexto de ciberataques, essa vulnerabilidade na distribuição é um ponto crítico que pode ser explorado por invasores, tornando fundamental a escolha de algoritmos robustos e modos de operação adequados.

No entanto, com o avanço das capacidades computacionais, sua chave de 56 bits tornou-se vulnerável a ataques de força bruta. Apesar dessa evolução, o DES e suas variantes foram aos poucos substituídos por algoritmos mais modernos, como o AES, especialmente após recomendações de órgãos como o NIST, que passou a considerar o DES obsoleto e inseguro para ambientes críticos.

5.8.1 AES

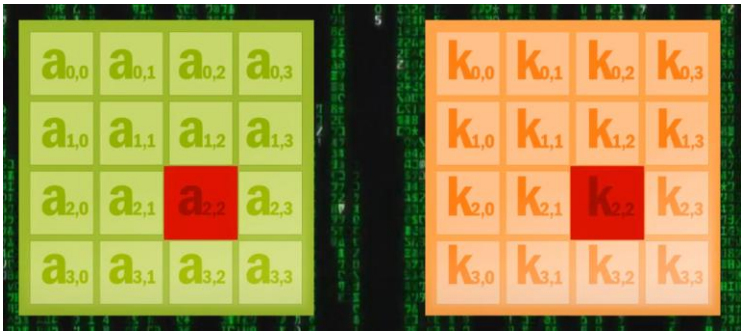
O AES, ou Advanced Encryption Standard, foi desenvolvido para substituir o DES como padrão de criptografia simétrica. Ele foi oficialmente adotado pelo NIST em 2001, após um processo seletivo rigoroso que avaliou diversas propostas internacionais, sendo a proposta vencedora chamada Rijndael, desenvolvida por dois criptógrafos belgas. O AES opera com blocos fixos de 128 bits e suporta chaves de 128, 192 ou 256 bits, com 10, 12 ou 14 rodadas de processamento, respectivamente na qual cada rodada tem 4 operações.

Diferente do DES, o AES utiliza uma estrutura de substituição-permutação, o que proporciona uma segurança mais robusta e uma eficiência computacional superior, tanto em software quanto em hardware. Uma das grandes vantagens do AES é sua resistência comprovada contra ataques conhecidos, como criptoanálise linear e diferencial. Até hoje, o AES permanece sem quebras práticas viáveis, sendo amplamente utilizado em padrões como

SSL/TLS, VPNs, Wi-Fi (WPA2 e WPA3) e em aplicações corporativas e governamentais. Seu uso é considerado seguro desde que combinado com práticas corretas de implementação, como o uso adequado de modos de operação e gerenciamento das chaves.

O funcionamento do algoritmo AES baseia-se na organização dos dados em uma matriz de 4 linhas por 4 colunas, totalizando 128 bits. Essa matriz é chamada de estado.

Figura 3 – Matriz 4x4 base e chave

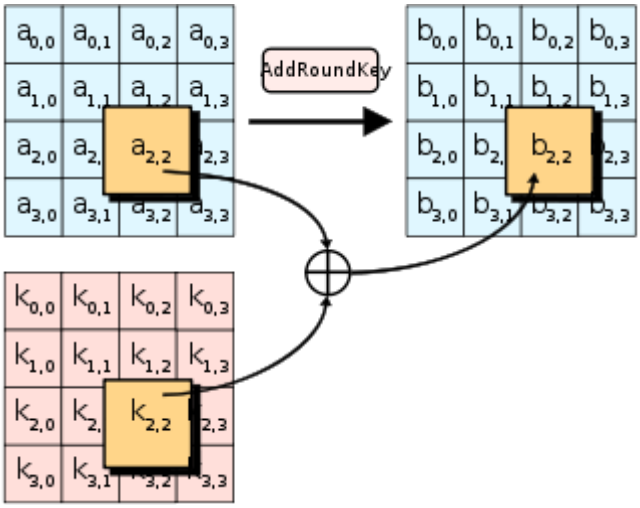


Fonte: https://www.youtube.com/watch?v=wiNndg-6_QQ

Cada bloco em destaque (em vermelho) representa uma subchave, que será usada ao longo das rodadas de transformação. O algoritmo AES realiza quatro operações principais em cada rodada: AddRoundKey, SubBytes, ShiftRows e MixColumns.

Na operação AddRoundKey, a subchave da rodada é combinada com o estado por meio de uma operação lógica chamada XOR (ou exclusivo). O XOR é uma operação booleana que retorna verdadeiro (1) apenas quando as duas entradas são diferentes. Por exemplo, se uma entrada for 1 e a outra for 0, o resultado será 1. Se ambas forem iguais, o resultado será 0. Essa operação garante que cada subchave altere o estado de maneira única. Cada rodada do AES possui sua própria subchave, e há uma subchave extra aplicada no início ou no fim do processo.

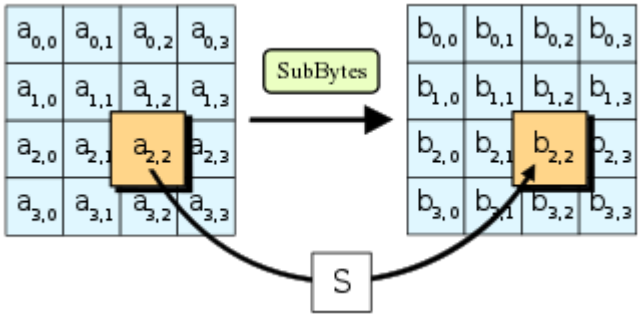
Figura 4 - Expansão de chave e *AddRoundKey*



Fonte: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Description_of_the_ciphers

A próxima operação é chamada SubBytes, na qual cada byte do estado passa por uma substituição não linear utilizando uma tabela chamada S-Box (Substitution Box). Essa tabela realiza uma substituição complexa, onde cada valor de entrada é substituído por um valor totalmente diferente. A função da S-Box é embaralhar os dados de forma segura, dificultando qualquer tentativa de previsão ou inversão da criptografia, mesmo com o uso de técnicas de força bruta. A operação em si é complexa do ponto de vista matemático, mas sua essência é substituir cada byte de forma que o novo valor seja imprevisível.

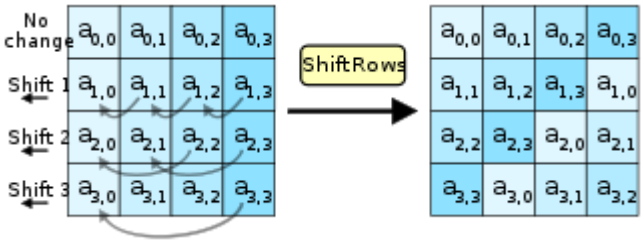
Figura 5 - *SubBytes*



Fonte: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Description_of_the_ciphers

Em seguida, a operação ShiftRows é aplicada. Essa operação realiza o deslocamento dos bytes de cada linha da matriz. É importante lembrar que os dados estão empilhados em colunas, e não dispostos da esquerda para a direita como geralmente lemos. A primeira linha permanece inalterada. A segunda linha é deslocada uma posição para a esquerda, com quebra circular, ou seja, o primeiro byte da linha é movido para o final. A terceira linha é deslocada duas posições para a esquerda, e a quarta linha, três posições. Esse deslocamento contribui para a difusão dos dados, espalhando os valores pela matriz e dificultando a reconstrução do conteúdo original.

Figura 6 - *ShiftRows*

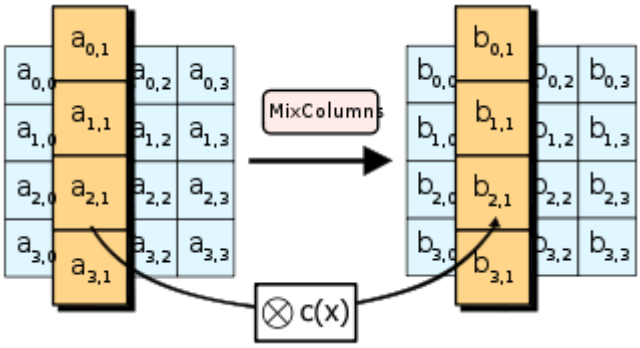


Fonte: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Description_of_the_ciphers

Por fim, temos a operação MixColumns, que é responsável por misturar os bytes de cada coluna da matriz de forma matemática. Essa mistura é feita por meio da multiplicação de cada coluna por uma matriz fixa, utilizando operações dentro de um campo finito conhecido como Galois Field GF(2^8). Essa multiplicação combina os quatro bytes de cada coluna para

gerar novos valores, de forma que uma pequena alteração em qualquer byte da coluna afeta todo o restante. O objetivo da MixColumns é aumentar ainda mais a difusão dos dados, dificultando a identificação de padrões e reforçando a segurança geral da criptografia.

Figura 7 - *MixColumns*



Fonte: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Description_of_the_ciphers

5.8.2 3DES

Em 1998, a Electronic Frontier Foundation demonstrou a vulnerabilidade do algoritmo DES ao construir uma máquina capaz de quebrar sua criptografia em menos de 24 horas. Como resposta, foi desenvolvido o Triple DES (3DES), que consiste em aplicar o algoritmo DES três vezes de forma sequencial, utilizando chaves diferentes para ampliar a segurança do processo criptográfico.

O funcionamento do 3DES baseia-se em três etapas sucessivas, alternando entre encriptação e decriptação, sendo conhecido como o modo EDE, sigla para Encrypt–Decrypt–Encrypt, ou seja, Criptografar–Descriptografar–Criptografar. Esse processo pode ser realizado com duas ou três chaves distintas.

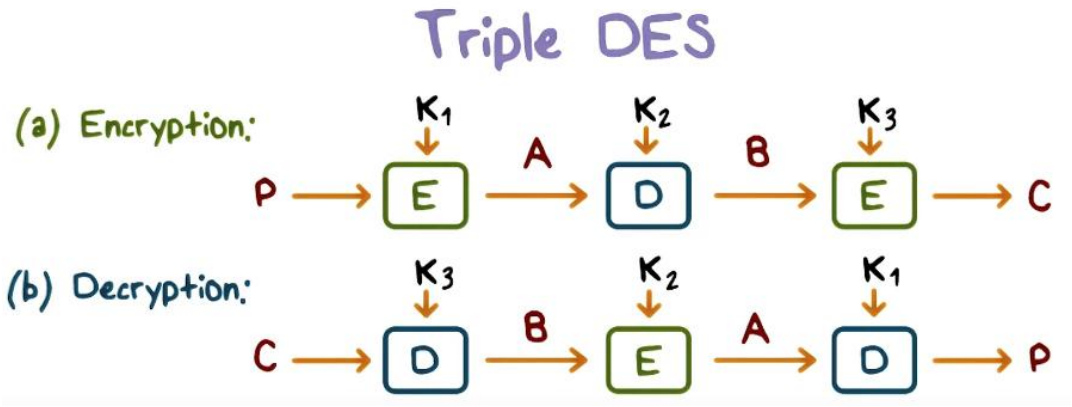
Quando são utilizadas três chaves diferentes (k1, k2 e k3), a encriptação é representada pela expressão matemática $C = E_{k3}(D_{k2}(E_{k1}(P)))$, na qual "E" representa a função de criptografia, "D" representa a função de decriptação e "P" é o texto original (plaintext).

A decriptação ocorre de forma inversa, seguindo a fórmula $P = D_{k1}(E_{k2}(D_{k3}(C)))$. Esse modo com três chaves distintas gera um espaço de chave de 168 bits, o que proporciona uma segurança ainda mais elevada.

Por outro lado, existe também uma versão utilizando apenas duas chaves, na qual k1 é igual a k3. Nesse caso, a operação de encriptação segue como $C = E_{k1}(D_{k2}(E_{k1}(P)))$, e a decriptação correspondente é $P = D_{k1}(E_{k2}(D_{k1}(C)))$. Esse modelo com duas chaves oferece uma segurança equivalente a 112 bits, considerado suficiente para muitos casos práticos. Além disso,

se k1 for igual a k2, o algoritmo passa a operar como o DES tradicional, podendo ser utilizado dessa forma para manter compatibilidade com sistemas legados.

Figura 8 - 3DES funcionamento



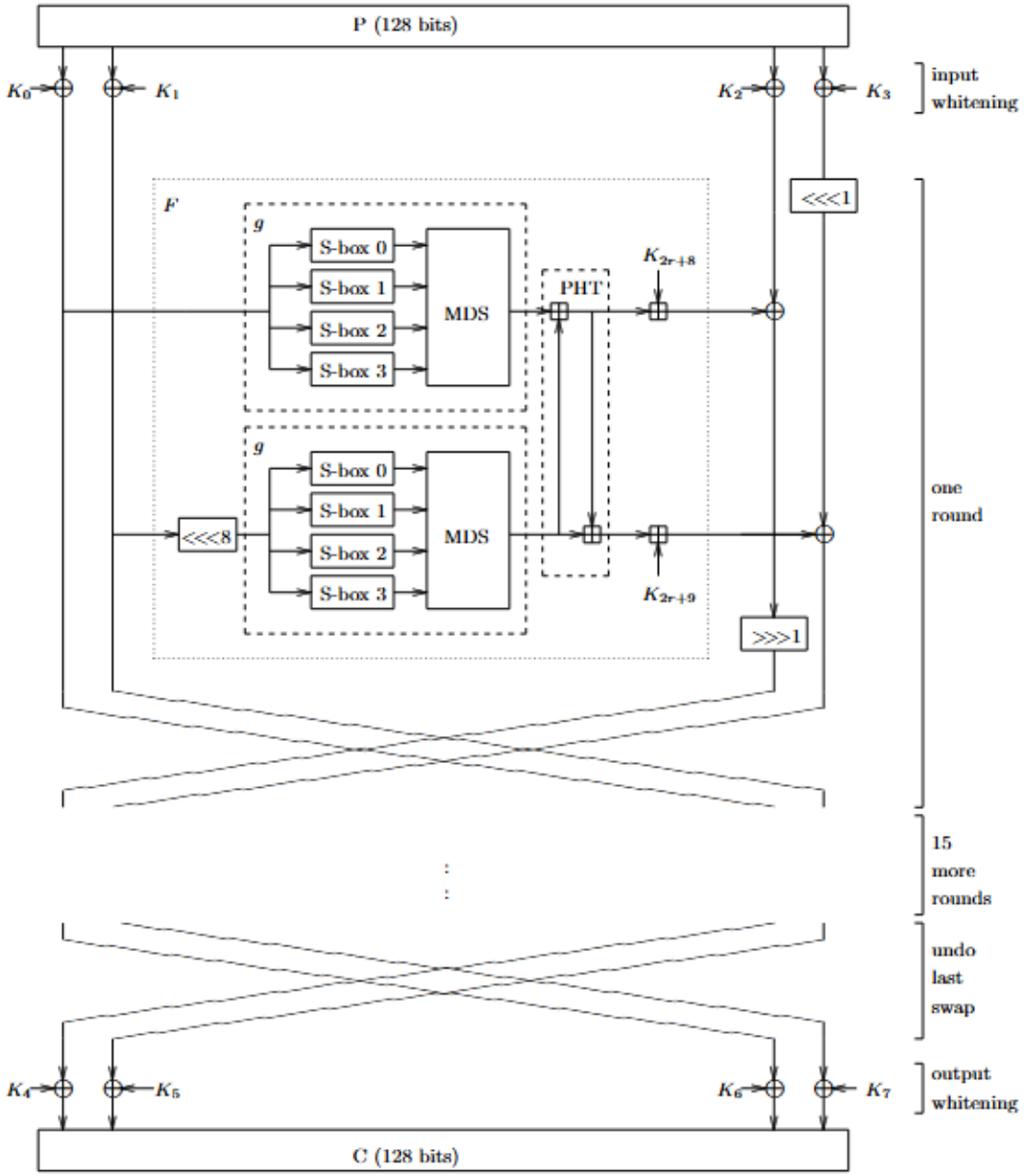
Fonte: https://www.youtube.com/watch?v=2O4dsChgcg8

A imagem acima representa graficamente as três etapas do 3DES, evidenciando o fluxo entre a entrada do texto em claro, a aplicação sequencial das chaves criptográficas e a obtenção do texto cifrado ao final do processo.

5.8.3 Twofish

O Twofish é um algoritmo de cifra de bloco simétrica desenvolvido por Bruce Schneier e sua equipe como um dos finalistas do concurso AES (Advanced Encryption Standard). Ele é baseado em uma estrutura de 16 rodadas, operando sobre blocos de 128 bits com chaves de até 256 bits. A figura abaixo representa a arquitetura geral do algoritmo.

Figura 9 - *Twofish* funcionamento



Fonte: https://www.karlin.mff.cuni.cz/~kozlik/udk_mat/twofish.pdf#page=5.67

A operação do Twofish inicia com uma etapa chamada input whitening, que consiste em uma operação de XOR entre os 128 bits do texto claro (dividido em quatro palavras de 32 bits) e quatro subchaves derivadas da chave principal (K_0, K_1, K_2, K_3). Após esse branqueamento de entrada, os dados passam por 16 rodadas de cifragem, cada uma realizando uma série de transformações complexas sobre os blocos.

Cada rodada do algoritmo atua sobre duas palavras (direita e esquerda), utilizando duas funções fundamentais chamadas F e g. A função g aplica quatro S-boxes (caixas de substituição não lineares), onde cada byte da palavra de 32 bits é substituído de acordo com valores definidos por tabelas que dependem da chave. Esses bytes transformados são combinados através de uma

multiplicação por uma matriz MDS (*Maximum Distance Separable*), que garante a difusão — ou seja, pequenas alterações nos dados de entrada geram grandes alterações na saída.

O resultado das duas funções g é então somado (operação de adição modular) com subchaves específicas daquela rodada (K_{8}+2i e K_{8}+2i+1), e passado por uma função PHT (Pseudo-Hadamard Transform), que promove ainda mais mistura entre os dados. Após isso, o resultado é usado para atualizar os blocos de dados por meio de operações de adição e XOR, além de deslocamentos circulares (shifts). Ao final de cada rodada, as palavras esquerda e direita são trocadas, exceto na última, onde a troca é revertida.

Depois das 16 rodadas, os dados passam por uma última etapa chamada output whitening, onde mais quatro subchaves (K_{4}, K_{5}, K_{6}, K_{7}) são aplicadas por meio de XOR aos blocos resultantes. O produto final é o texto cifrado de 128 bits. A descriptografia segue o mesmo processo, com as subchaves aplicadas em ordem reversa.

As principais características do Twofish incluem: suporte para tamanhos de chave variáveis (128, 192 e 256 bits), forte segurança contra ataques como criptoanálise linear e diferencial, além de eficiência tanto em hardware quanto em software. As operações nas S-boxes e na matriz MDS são as principais responsáveis pela confusão e difusão dos dados — pilares essenciais para a segurança de algoritmos de cifra de bloco. Apesar de o AES ter sido o algoritmo escolhido pelo NIST, o Twofish continua sendo considerado seguro e é utilizado em diversas aplicações criptográficas modernas.

5.8.4 Blowfish

Blowfish é um algoritmo de cifra de bloco com chave simétrica desenvolvido em 1993 por Bruce Schneier. Foi criado como uma alternativa mais segura e eficiente ao padrão de criptografia de dados da época, o DES (Data Encryption Standard), que já era considerado lento e vulnerável a ataques. O Blowfish opera sobre blocos de 64 bits e permite o uso de chaves variáveis com até 448 bits, oferecendo flexibilidade e robustez.

O funcionamento do Blowfish inicia-se com a geração das estruturas internas chamadas de P-array e S-boxes, que são tabelas utilizadas no processo de cifragem. Essas estruturas são inicialmente preenchidas com a representação hexadecimal da constante matemática pi, mas depois são modificadas com base na chave fornecida, garantindo que cada chave produza diferentes resultados. A P-array contém 18 subchaves e as S-boxes são quatro matrizes com 256 entradas cada.

A cifra divide o texto original de 64 bits em duas metades de 32 bits, denominadas L (left) e R (right). O algoritmo então executa 16 rodadas de processamento. Em cada rodada, a

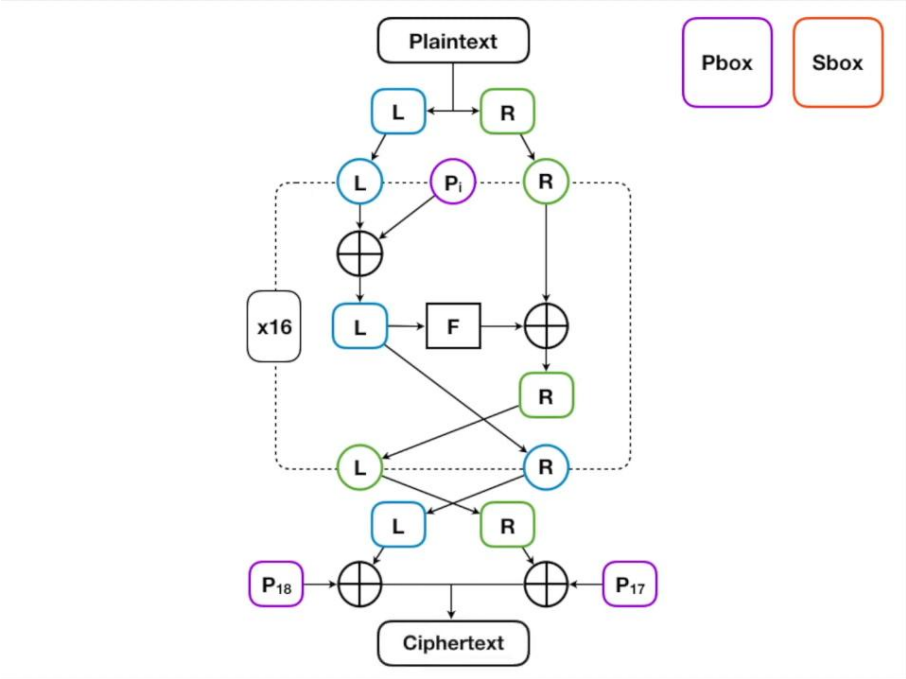
metade esquerda L é combinada com uma subchave da P-array por meio de uma operação XOR. Em seguida, a metade direita R é modificada com base no resultado de uma função não linear aplicada a L, chamada de função F. Essa função F divide o valor de L em quatro bytes, utilizando cada byte como índice para acessar as S-boxes. O valor obtido da primeira S-box é somado ao da segunda, o resultado passa por um XOR com o valor da terceira, e finalmente é somado ao valor da quarta S-box. O resultado final da função F é então combinado com R por meio de outra operação XOR.

Ao final de cada rodada, os valores de L e R são trocados. Após as 16 rodadas, uma última troca entre L e R é feita, seguida por duas operações XOR adicionais com as duas subchaves restantes da P-array. O resultado é a versão cifrada do texto original.

A descriptografia segue exatamente os mesmos passos do processo de criptografia, mas utilizando as subchaves da P-array em ordem inversa. Isso é possível devido à estrutura de Feistel empregada no Blowfish, que permite a reversibilidade do algoritmo sem alterar sua lógica.

Entre as principais vantagens do Blowfish estão sua alta taxa de criptografia, resistência a técnicas conhecidas de criptoanálise e o fato de ser um algoritmo de domínio público, sem patentes, o que o tornou popular em diversos sistemas e aplicações. Contudo, sua principal limitação está no tamanho do bloco de apenas 64 bits, o que pode ser problemático em aplicações modernas que processam grandes volumes de dados. Para contornar essa limitação, Bruce Schneier desenvolveu posteriormente o Twofish, uma evolução do Blowfish que utiliza blocos de 128 bits e participou como finalista no processo de seleção do novo padrão criptográfico promovido pelo NIST. Embora o AES (Advanced Encryption Standard) tenha sido o escolhido, o Twofish continua sendo considerado seguro e é utilizado até hoje em diversas aplicações.

Figura 10 - *Blowfish* funcionamento



Fonte: https://www.youtube.com/watch?v=gz8AV0bPaOU

A imagem acima ilustra a estrutura interna do algoritmo Blowfish, destacando a divisão do bloco em L e R, a aplicação da função F, as trocas entre os blocos e o uso das subchaves da P-array em cada rodada.

5.8.5 RC4

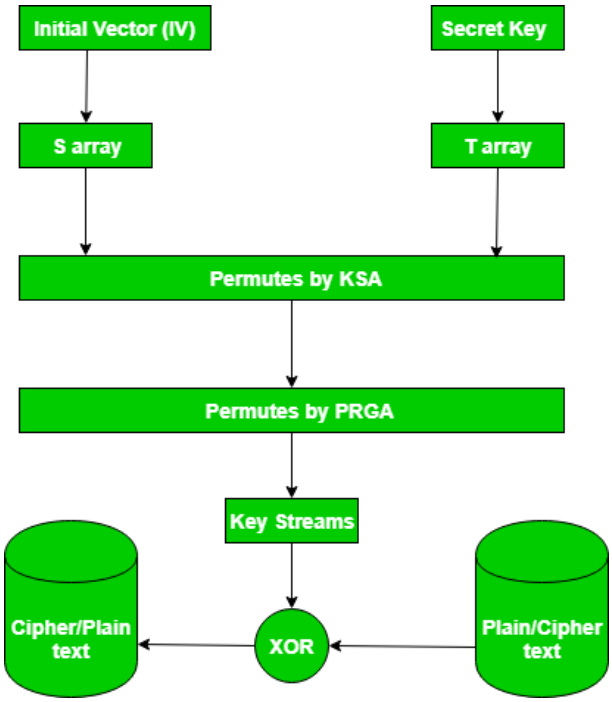
O RC4 (Rivest Cipher 4) é um algoritmo de cifra de fluxo com chave simétrica desenvolvido por Ron Rivest em 1987, sendo amplamente utilizado durante muitos anos por sua eficiência em software e hardware. O algoritmo opera byte a byte, utilizando uma chave de tamanho variável que pode conter de 1 até 256 bytes (8 a 2048 bits). A encriptação e a decriptação seguem o mesmo princípio: uma sequência pseudoaleatória de bytes (keystream) é gerada e combinada com os bytes do texto de entrada por meio da operação XOR, transformando o texto claro em texto cifrado, e vice-versa.

O funcionamento do RC4 pode ser dividido em duas fases: o algoritmo de agendamento da chave (Key Scheduling Algorithm – KSA) e o algoritmo gerador de pseudoaleatoriedade (Pseudo-Random Generation Algorithm – PRGA). Na fase KSA, o algoritmo inicializa um vetor de estado S de 256 bytes, com valores que vão de 0 a 255. Em seguida, um vetor auxiliar T também é construído, repetindo a chave fornecida até preencher as 256 posições. A partir disso, o vetor S é embaralhado por meio de permutações condicionadas pelos valores de T. Em cada iteração da KSA, um índice j é atualizado com a

equação j = (j + S[i] + T[i]) mod 256, e então os valores de S[i] e S[j] são trocados. Após 256 iterações, o vetor S está embaralhado com base na chave fornecida.

A fase PRGA é responsável por gerar o *keystream* utilizado na cifra. Inicialmente, os índices i e j são definidos como zero. A cada iteração, i é incrementado com i = (i + 1) mod 256, seguido da atualização de j como j = (j + S[i]) mod 256. Em seguida, ocorre a troca de S[i] e S[j], e um valor t é calculado com t = (S[i] + S[j]) mod 256. O byte S[t] então é extraído como o próximo byte do *keystream*, sendo combinado com o byte correspondente do texto de entrada através da operação XOR. Este processo se repete enquanto houver bytes a serem criptografados ou descriptografados.

Figura 11 - RC4 funcionamento



Fonte: https://www.geeksforgeeks.org/rc4-encryption-algorithm/

Apesar de sua simplicidade e performance, o RC4 apresenta vulnerabilidades significativas. A principal delas está nos primeiros bytes gerados após a fase KSA, que exibem padrões previsíveis e enviesados, permitindo ataques de análise estatística. Além disso, a repetição de chaves ou o uso de chaves fracas torna o algoritmo suscetível a ataques como o de Fluhrer, Mantin e Shamir (FMS), que comprometeram sua aplicação em protocolos como o WEP (Wired Equivalent Privacy). Por essas razões, o RC4 é considerado obsoleto, e seu uso é atualmente desaconselhado por entidades como o NIST e o IETF.

Em síntese, o RC4 foi um algoritmo amplamente adotado por décadas devido à sua facilidade de implementação e boa taxa de desempenho. No entanto, com a descoberta de falhas críticas em seu design, algoritmos mais robustos e modernos como o AES (em modo CTR ou

GCM) e o ChaCha20 passaram a ser recomendados para aplicações que exigem segurança criptográfica de longo prazo.

5.9 Algoritmo de chave assimétrica

5.9.1 RSA

O RSA *(Rivest–Shamir–Adleman)* é um dos algoritmos de criptografia assimétrica mais utilizados no mundo, criado em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman. Ele se destaca por utilizar um par de chaves distintas: uma pública, que pode ser compartilhada abertamente para cifrar mensagens, e uma privada, mantida em sigilo para descriptografá-las. A segurança do RSA repousa na dificuldade de fatorar números grandes, especificamente o produto de dois primos. Embora multiplicar seja simples, fatorar o resultado para encontrar os primos que o compõem é computacionalmente impraticável, garantindo assim que, mesmo com acesso à chave pública, um atacante não consiga derivar a chave privada.

Inicialmente, escolhem-se dois números primos grandes e distintos, representados por p e q. A partir desses valores, calcula-se N = p * q, que será utilizado como parte da chave pública e da chave privada. Também é necessário calcular phi(N) = (p - 1)(q - 1), que representa a função totiente de Euler aplicada a N. Em seguida, escolhe-se um número inteiro e, que fará parte da chave pública, de modo que e seja relativamente primo com phi(N), ou seja, o máximo divisor comum entre e e phi(N) seja igual a 1, respeitando a condição 1 < e < phi(N). Com os valores de “e” e phi(N) definidos, utiliza-se a congruência e * d ≡ 1 mod phi(N) para calcular d, que será o expoente da chave privada.

Após a geração das chaves, o remetente pode transformar a mensagem original em números, de acordo com uma tabela padronizada e pública que associa caracteres a valores numéricos, assegurando que todos os números possuam a mesma quantidade de dígitos. A mensagem numérica resultante é então dividida em blocos b, de maneira que cada bloco satisfaça a condição 1 ≤ b < N. Essa restrição garante que, ao aplicar a criptografia, cada bloco permaneça dentro do intervalo definido por N, permitindo a recuperação correta durante a descriptografia.

Com a chave pública (e, N), o processo de criptografia é realizado utilizando a congruência c ≡ b^e mod N, onde c representa o bloco cifrado. O destinatário, por sua vez, utiliza a chave privada (d, N) para realizar o processo inverso, aplicando a congruência b ≡ c^d mod N, recuperando assim o valor original do bloco. Por fim, todos os blocos recuperados são concatenados e convertidos de volta para caracteres com o auxílio da mesma tabela usada na

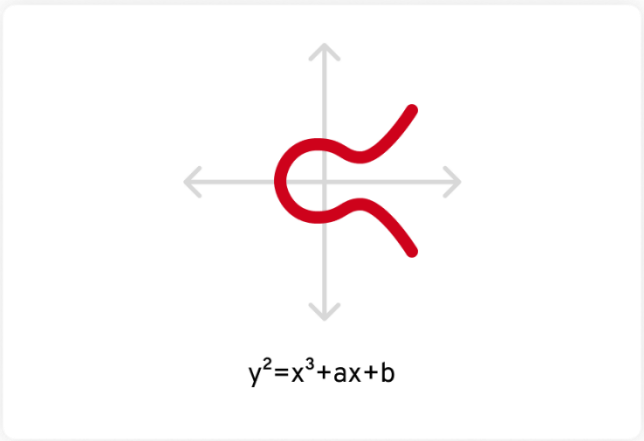
codificação, resultando na reconstrução da mensagem original. A robustez do RSA reside na complexidade de fatorar números muito grandes, o que torna o cálculo da chave privada praticamente inviável sem o conhecimento prévio dos primos p e q.

5.9.2 ECC

A criptografia de curva elíptica (ECC) é uma forma de criptografia de chave pública baseada na matemática das curvas elípticas. Ela fornece uma maneira segura de realizar operações criptográficas, como troca de chaves, assinaturas digitais e criptografia. A ECC é uma alternativa à criptografia Rivest-Shamir-Adleman (RSA), que foi publicada pela primeira vez em 1977.

A criptografia de curva elíptica (ECC) é um método de criptografia de chave pública que utiliza cálculos em curvas elípticas sobre campos finitos para garantir segurança com chaves menores, tornando-a mais eficiente que algoritmos tradicionais como o RSA. A estrutura matemática do ECC baseia-se na dificuldade do problema do logaritmo discreto em curvas elípticas, onde uma curva é definida por uma equação do tipo $y^2 = x^3 + ax + b$, sobre um campo finito.

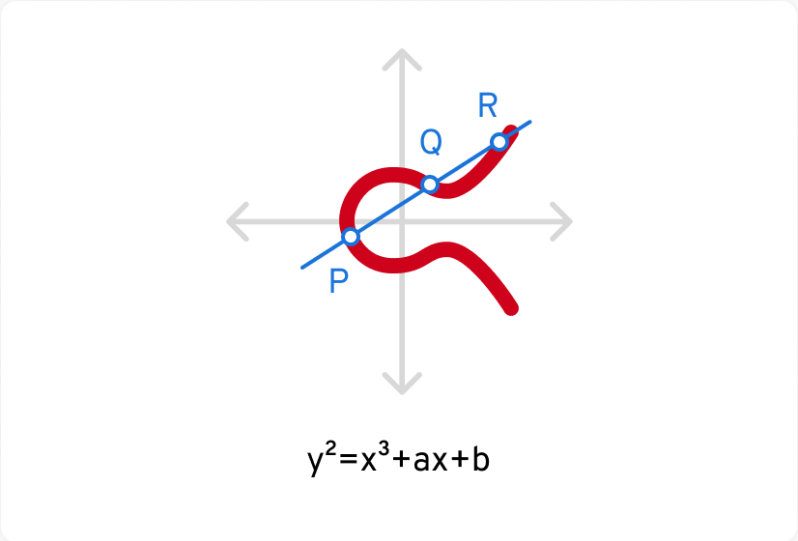
Figura 12 - Equação y^2 = x^3 + ax + b representada em um gráfico



Fonte: https://www.keepersecurity.com/blog/pt-br/2023/06/07/what-is-elliptic-curve-cryptography/

Para operar, o algoritmo requer que o emissor e o receptor concordem previamente em parâmetros de domínio, incluindo a curva (coeficientes a e b), o campo finito (geralmente um primo p), um ponto base G, sua ordem n e o cofator h.

Figura 13 - Pontos P, Q, R



Fonte: https://www.keepersecurity.com/blog/pt-br/2023/06/07/what-is-elliptic-curve-cryptography/

A chave privada é um número inteiro aleatório d, entre 1 e n – 1, enquanto a chave pública é o ponto Q obtido pela multiplicação escalar do ponto base pela chave privada, ou seja, Q = dG. A criptografia pode ser realizada usando esquemas como ECIES (Elliptic Curve Integrated Encryption Scheme), onde o emissor escolhe um número aleatório k e calcula primeiro o ponto R = kG. Em seguida, utiliza-se S = kQ (que equivale a kdG), para gerar uma chave simétrica temporária, utilizada para cifrar a mensagem real; o par R e o texto cifrado são então enviados ao destinatário. Ao receber R, o destinatário calcula novamente S = dR e, a partir desse valor, obtém a mesma chave simétrica para descriptografar a mensagem.

A segurança do ECC está diretamente relacionada à dificuldade computacional de resolver o logaritmo discreto elíptico (ECDLP). Ou seja, mesmo conhecendo G e Q, é praticamente inviável calcular d quando p e n possuem centenas de bits — por exemplo, uma curva de 256 bits oferece segurança equivalente a uma chave RSA de 3072 bits, mas com maior eficiência. Essa redução no tamanho das chaves resulta em requisitos menores de processamento e de armazenamento, o que torna o ECC ideal para aplicações em dispositivos com recursos limitados, como smartphones e sistemas de Internet das Coisas (IoT). Além disso, o ECC é amplamente utilizado em protocolos modernos, como TLS, assinaturas digitais (ECDSA) e acordos de chave como ECDH.

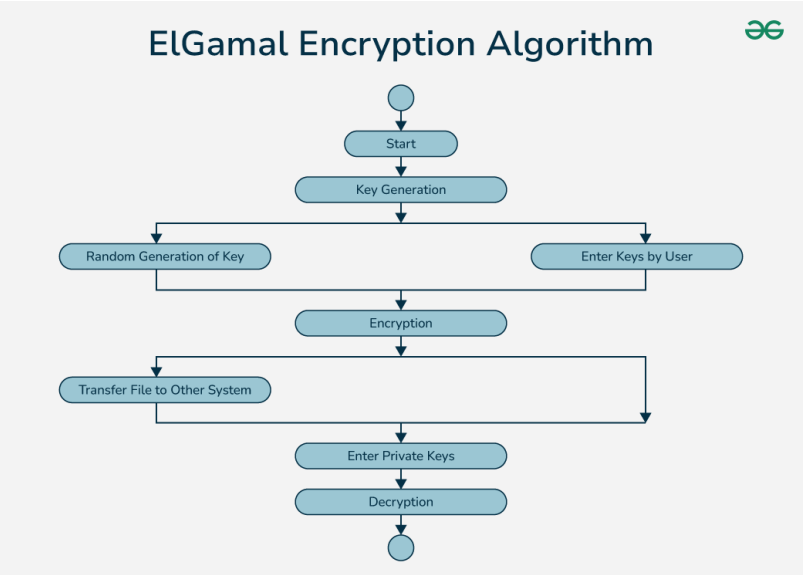
5.9.3 ElGamal

O algoritmo ElGamal é um sistema de criptografia assimétrica baseado no problema matemático do logaritmo discreto, considerado computacionalmente difícil de resolver. Ele opera em dois estágios principais: a geração de chaves e a criptografia/descriptografia. Inicialmente, o receptor escolhe um número primo grande p e uma raiz primitiva g desse número. Em seguida, seleciona um número aleatório x como chave privada, sendo x menor que p. A chave pública é gerada a partir do cálculo de $y = g^x \bmod p$, formando assim o trio (p, g, y) como chave pública e mantendo x em segredo como chave privada.

Para criptografar uma mensagem m, o emissor escolhe um número aleatório k, que também deve ser menor que p. Com isso, calcula-se dois valores: $a = g^k \bmod p$ e $b = (y^k \times m) \bmod p$. O par (a, b) representa o texto cifrado que será enviado ao receptor. A segurança do algoritmo está no fato de que, mesmo com acesso a a e b, é praticamente impossível obter a mensagem original sem o conhecimento da chave privada x, justamente devido à dificuldade de resolver o logaritmo discreto.

Para realizar a descriptografia, o receptor usa sua chave privada x para calcular $s = a^x \bmod p$, que é então invertido multiplicativamente em relação a p. Em seguida, recupera-se a mensagem original m com o cálculo de $m = (b \times s^{-1}) \bmod p$, onde s^{-1} é o inverso modular de s em relação a p. Dessa forma, a mensagem é restaurada com segurança. O ElGamal é utilizado em vários protocolos de segurança e sistemas de mensagens, especialmente por sua robustez contra ataques baseados em fatoração ou logaritmos discretos.

Figura 14 - Algoritmo de Criptografia ElGamal



Fonte: https://www.geeksforgeeks.org/computer-networks/elgamal-encryption-algorithm/

5.10 Marco Civil

O Marco Civil da Internet, instituído pela Lei nº 12.965/2014, é considerado a primeira legislação brasileira que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Ele foi construído com ampla participação social por meio de consultas públicas e audiências, sendo um exemplo de governança colaborativa que envolveu diferentes setores da sociedade civil, governo e especialistas da área de tecnologia e direito. Essa lei não trata apenas de aspectos técnicos, mas propõe uma visão democrática da internet, reconhecendo-a como um espaço essencial para o exercício da cidadania e para a promoção da liberdade de expressão.

Os princípios fundamentais do Marco Civil incluem a proteção da privacidade, a garantia da liberdade de expressão, a preservação da neutralidade da rede, a responsabilidade dos agentes conforme sua atuação, e a preservação da estabilidade, segurança e funcionalidade da rede. A neutralidade da rede, por exemplo, assegura que os dados sejam tratados de forma isonômica, sem discriminação por conteúdo, origem ou destino, impedindo que provedores favoreçam certos serviços ou aplicativos. Esse princípio é essencial para manter a internet aberta e acessível a todos, promovendo inovação e competitividade.

A importância dessa legislação está na sua função de assegurar os direitos dos usuários diante do crescimento acelerado da internet como ferramenta essencial na vida cotidiana. O Marco Civil garante que os dados pessoais dos usuários só possam ser armazenados ou tratados com consentimento, protegendo a privacidade e evitando abusos por parte de empresas ou do Estado. Ele também estabelece regras claras sobre a guarda de registros de conexão e acesso a aplicações, impondo limites à atuação dos provedores e garantindo transparência no tratamento das informações.

Na vida do cidadão, os impactos do Marco Civil são amplos e positivos. Ele fortalece o direito à privacidade, que muitas vezes é colocado em risco na era digital, e define parâmetros legais para o uso seguro da internet. Usuários passam a ter garantias contra a remoção arbitrária de conteúdos, podendo exercer sua liberdade de expressão com maior segurança jurídica. A exigência de consentimento para o uso de dados pessoais fortalece o controle dos indivíduos sobre suas próprias informações, reforçando os princípios democráticos em ambiente digital.

Em um contexto em que a internet é cada vez mais usada para transações comerciais, atividades educacionais, serviços públicos e interações sociais, o Marco Civil torna-se essencial para garantir que esse ambiente seja regido por normas justas, equitativas e transparentes. Sua existência representa um avanço no reconhecimento da cidadania digital e oferece uma base

sólida para a criação de outras legislações complementares, como a Lei Geral de Proteção de Dados (LGPD), que aprofunda os mecanismos de proteção à privacidade.

5.11 LGPD

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece o regime jurídico aplicável ao tratamento de dados pessoais em meios físicos e digitais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Com base em princípios como transparência, finalidade, necessidade, segurança e responsabilização, a LGPD estrutura-se como um importante instrumento regulatório diante do avanço tecnológico e da intensa circulação de dados na sociedade da informação. Sua entrada em vigor representou um divisor de águas nas relações entre titulares de dados e os agentes que realizam operações de tratamento, exigindo uma mudança cultural profunda tanto no setor público quanto no privado (TEFFÉ; VIOLA, 2020).

O primeiro aspecto relevante da LGPD refere-se à existência de uma base legal como pré-requisito para o tratamento de dados pessoais. A legislação prevê dez hipóteses legais para que esse tratamento seja considerado legítimo, entre elas o consentimento do titular, o cumprimento de obrigação legal, a execução de políticas públicas, a proteção da vida e da incolumidade física, e o exercício regular de direitos. O consentimento, por exemplo, deve ser obtido de forma livre, informada e inequívoca, podendo ser revogado a qualquer momento. No entanto, ele não é obrigatório em todas as situações, pois a LGPD admite outras bases legais conforme o contexto. Essa multiplicidade de bases legais impõe uma nova forma de gestão dos dados, que deve estar documentada e justificada, permitindo que o titular conheça os fundamentos jurídicos que sustentam o uso de suas informações. A ausência de base legal válida pode resultar na responsabilização do agente de tratamento e em sanções administrativas.

O segundo ponto central da LGPD é o princípio da finalidade, que determina que o tratamento de dados pessoais deve atender a propósitos legítimos, específicos e informados previamente ao titular. Esse princípio impede o tratamento de dados de forma genérica ou ilimitada, exigindo clareza quanto ao motivo da coleta, ao uso pretendido e à compatibilidade entre a finalidade informada e as atividades de tratamento realizadas. Com isso, busca-se assegurar a previsibilidade, a transparência e a confiança nas relações entre titulares e agentes de tratamento. Caso a finalidade original seja alterada, uma nova base legal deverá ser invocada, sendo necessário, em muitos casos, solicitar novamente o consentimento do titular. A clareza quanto à finalidade é também um fator essencial para o cumprimento do princípio da

autodeterminação informativa, pois permite que o titular exerça controle efetivo sobre seus dados.

O terceiro aspecto fundamental envolve os princípios da adequação e da necessidade, que atuam de forma complementar ao da finalidade. A adequação exige que o tratamento esteja de acordo com as finalidades informadas ao titular, ou seja, os dados coletados e utilizados devem estar compatíveis com os objetivos propostos. Já o princípio da necessidade estabelece que a coleta e o uso de dados devem se limitar ao mínimo necessário para a realização das finalidades pretendidas. Isso significa que é vedado o tratamento excessivo ou desproporcional, sendo imprescindível que as organizações façam uma avaliação criteriosa sobre quais dados são realmente essenciais para suas atividades. A aplicação rigorosa desses princípios contribui para reduzir riscos à privacidade, minimizar os impactos de eventuais incidentes de segurança e reforçar a confiança do titular no tratamento de seus dados.

Além desses princípios, a LGPD contempla uma série de direitos dos titulares, como o direito ao acesso, à retificação, à exclusão, à portabilidade, à revogação do consentimento e à oposição ao tratamento. A efetivação desses direitos é um desafio técnico e jurídico, que exige das instituições mecanismos claros, acessíveis e auditáveis de atendimento às requisições. Ao mesmo tempo, os agentes de tratamento devem observar o princípio da segurança, adotando medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou difusão.

A LGPD não apenas regulamenta a atividade econômica baseada em dados, mas também reafirma a centralidade da pessoa humana no ambiente digital. A proteção de dados pessoais, nesse sentido, passa a ser um elemento estruturante da cidadania contemporânea, impondo limites à lógica do controle, da vigilância e do lucro indiscriminado por meio da exploração de informações sensíveis. A adoção da LGPD exige, portanto, uma reformulação dos processos internos das organizações, a capacitação de profissionais, a criação de políticas de governança de dados e o desenvolvimento de uma cultura de proteção e respeito à privacidade.

6 PESQUISA DE CAMPO

Essa pesquisa tem como objetivo avaliar o nível de conhecimento prático e noção de segurança que os estudantes da FeMASS têm ao se conectar a redes wi-fi, principalmente em ambientes públicos e corporativos. Entre os ataques abordados, destacam-se: *Evil Twin*, *Captive* Portal, WPA2, ARP *Poisoning*, ARP *Spoofing* e Força Bruta.

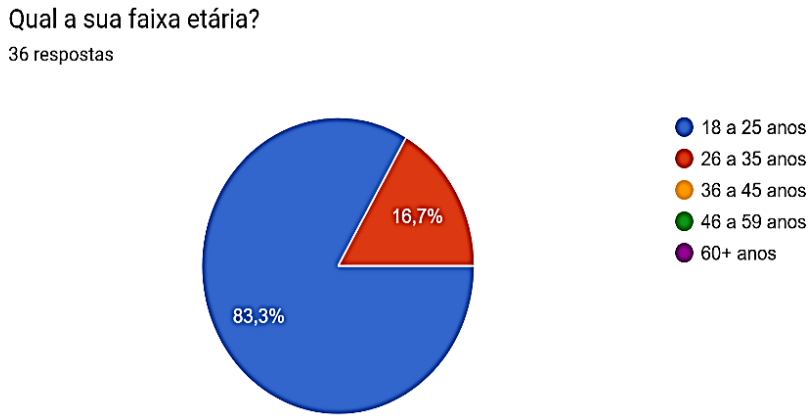
Buscou-se levantar dados quantitativos e qualitativos que reflitam o comportamento dos estudantes diante de situações que envolvem redes W*i-fi*, suas práticas de segurança e eventuais experiências anteriores com esse tipo de ameaça.

6.1 Coleta de dados

A coleta de dados foi feita a partir de um questionário *online*, desenvolvido no *Google Forms* e enviado para os estudantes da FeMASS através de grupos de mensagem no *WhatsApp*. A pesquisa constatou 36 participantes em um período de 09/04/2025 até 10/04/2025 com foco na identificação de hábitos de segurança digital e conhecimento prático sobre ataques em redes *Wi-fi*.

No Gráfico 1, é apresentada a faixa etária dos entrevistados, na qual pode se constatar que, na pesquisa, 100% se passa entre indivíduos de 18 anos a 35 anos de idade. Esse dado mostra que o público-alvo é composto por maior parte de jovens adultos e se alinha ao perfil dos estudantes da FeMASS mostrando seu comportamento e percepção sobre segurança em redes *Wi-fi*.

Gráfico 1 - Qual a sua faixa etária?

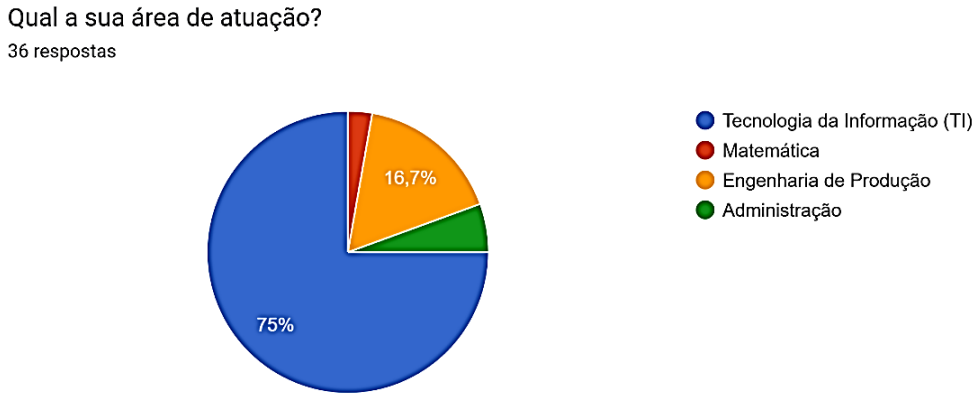


Fonte: Extraído do *Google Forms* (2025)

O Gráfico 2 revela que a maioria dos respondentes atua na área de Tecnologia da Informação (75%), seguida por Engenharia de Produção (16,7%), Administração (5,6%) e Matemática (2,8%). A diversidade de cursos representados amplia a validade da pesquisa,

embora a predominância de alunos de TI indique uma tendência maior ao conhecimento prévio sobre segurança digital.

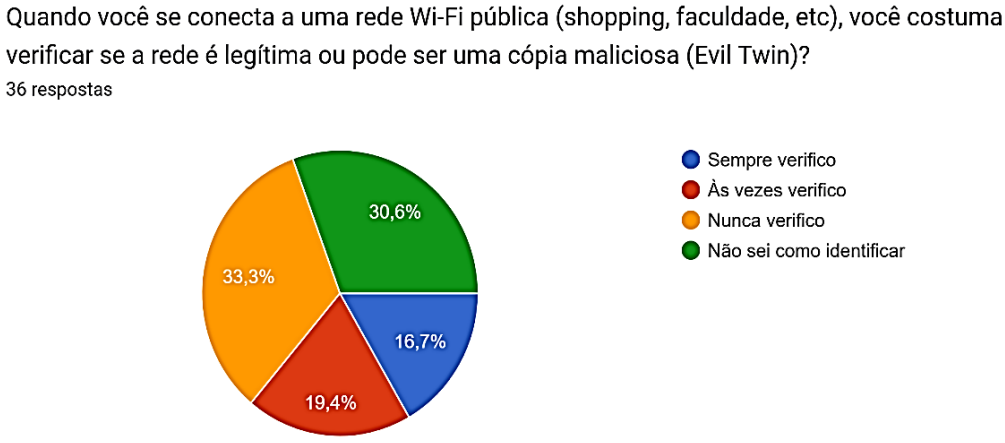
Gráfico 2 - Qual a sua área de atuação?



Fonte: Extraído do *Google Forms* (2025)

Quando questionados sobre o hábito de verificar se uma rede *Wi-fi* é legítima ou uma cópia maliciosa (*Evil Twin*), apenas 16,7% afirmaram sempre verificar, enquanto 19,4% disseram verificar às vezes. Um número preocupante de 33,3% nunca verifica, e 30,6% afirmaram não saber como identificar esse tipo de rede, evidenciando a falta de conhecimento na percepção de riscos em conexões sem fio.

Gráfico 3 - Conferência se a rede é legitima antes de se conectar

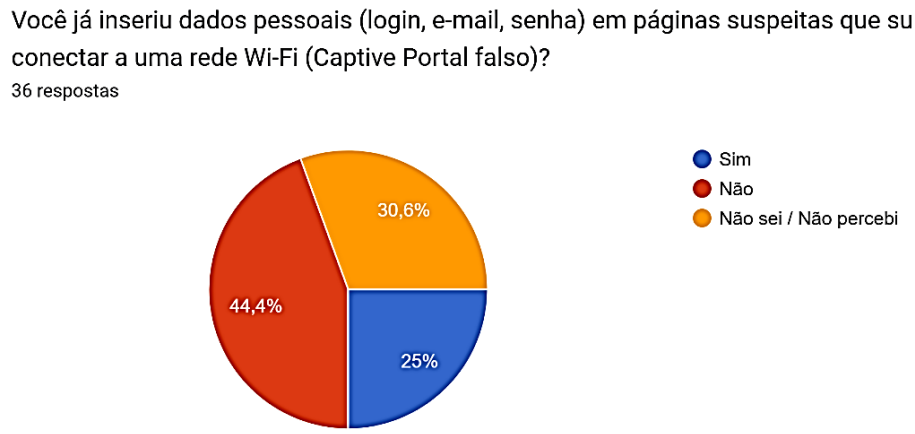


Fonte: Extraído do *Google Forms* (2025)

O Gráfico 4 aponta que 25% dos entrevistados já inseriram dados pessoais (como *login* e senha) em páginas suspeitas ao se conectarem a uma rede *Wi-fi*. 44,4% negaram essa prática, enquanto 30,6% não souberam dizer ou não perceberam. Esses dados reforçam a necessidade

de maior conscientização quanto ao uso de *Captive* Portal falsos, técnica comum de ataques como *Evil Twin*.

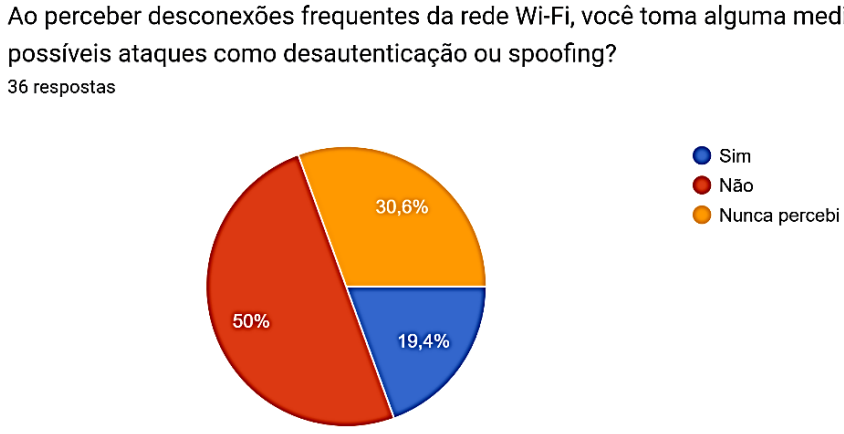
Gráfico 4 - Você já inseriu dados pessoais ao conectar em uma rede *Wi-fi?*



Fonte: Extraído do *Google Forms* (2025)

Frente a quedas repentinas de conexão (possivelmente causadas por ataques de desautenticação), apenas 19,4% dos respondentes afirmaram investigar o motivo, enquanto 50% não tomam nenhuma ação e 30,6% nunca perceberam tal situação. Isso mostra uma falta de reação frente a possíveis sinais de ataque, como os que ocorrem em redes WPA2 vulneráveis.

Gráfico 5 - Investiga o porquê de estar desconectando frequentemente?

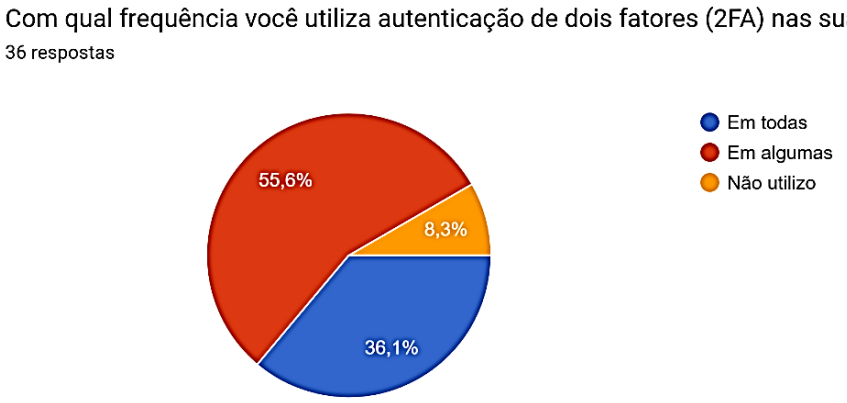


Fonte: Extraído do *Google Forms* (2025)

O uso de autenticação de dois fatores, importante proteção contra ataques de força bruta, foi relatado por 36,1% dos participantes em todas as contas, 55,6% em algumas e 8,3% não

utilizam esse recurso. Embora a maioria adote a prática em algum nível, ainda há necessidade significativa para reforço da segurança pessoal digital.

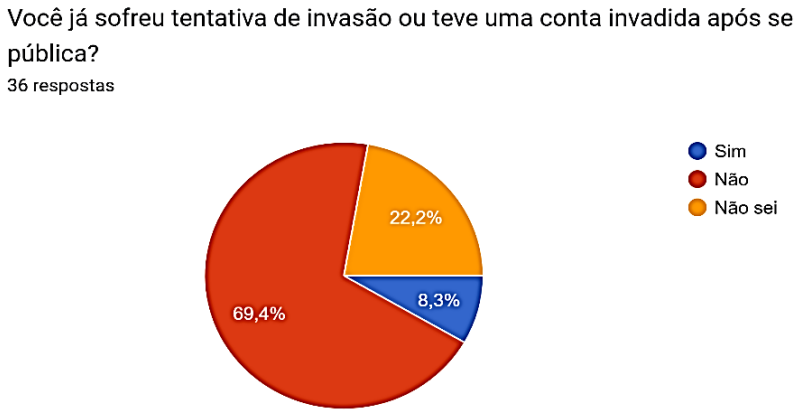
Gráfico 6 - Frequência do uso de autenticação de dois fatores



Fonte: Extraído do *Google Forms* (2025)

Segundo o Gráfico 7, 8,3% dos respondentes relataram que já tiveram contas invadidas após utilizar uma rede pública, enquanto 69,4% disseram que não e 22,2% não souberam responder. Ainda que a porcentagem de casos positivos seja baixa, ela é suficiente para mostrar que esse tipo de incidente realmente acontece e pode ter origem em falhas de segurança nas redes utilizadas.

Gráfico 7 - Teve uma conta invadida após se conectar a uma rede pública?

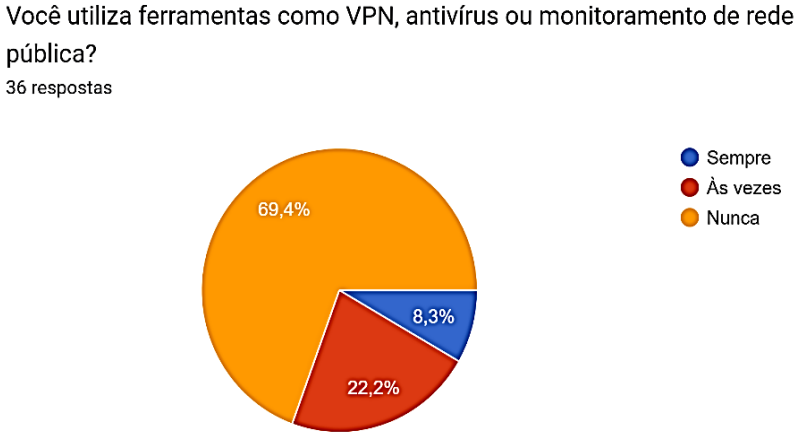


Fonte: Extraído do *Google Forms* (2025)

O Gráfico 8 mostra que apenas 8,3% dos entrevistados utilizam sempre ferramentas como VPN, antivírus ou monitoramento de rede ao se conectarem em redes públicas, 22,2%

usam às vezes e, a maioria, 69,4%, afirma nunca utilizar. Esse dado revela um alto nível de exposição a riscos cibernéticos, mesmo entre estudantes de áreas relacionadas à tecnologia.

Gráfico 8 - Você utiliza ferramentas como VPN, antivírus ou monitoramento de rede ao se conectar a *Wi-fi* pública?



Fonte: Extraído do *Google Forms* (2025)

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

A cibersegurança é fundamental para proteger redes *wireless*, especialmente em ambientes corporativos, contra ataques que exploram vulnerabilidades em seus protocolos e tecnologias. Redes sem fio, por sua natureza, são mais suscetíveis a interceptações e invasões não autorizadas, o que aumenta a necessidade de práticas de segurança robustas.

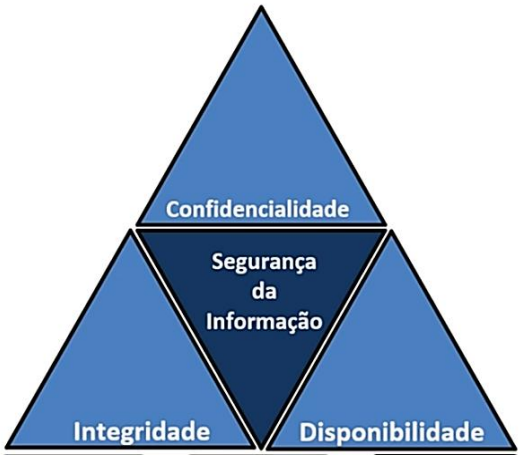
Em redes corporativas, no qual informações sensíveis circulam, garantir a integridade e confidencialidade dos dados é essencial para prevenir ataques como *Man in the Middle*, quebra de criptografia em WPA/WPA2 e outras ameaças avançadas. Além disso, a etapa de pós-exploração é crucial para identificar brechas, mitigar os danos e fortalecer as defesas futuras, assegurando que os ativos de rede sejam protegidos de ataques contínuos.

A confidencialidade refere-se à prevenção de acessos não autorizados às informações, garantindo que apenas indivíduos autorizados possam visualizá-las. Confidencialidade, integridade e disponibilidade são os pilares da segurança da informação.

A conectividade em uma rede global tem facilitado o roubo de grandes volumes de dados, incluindo informações altamente sensíveis, por parte de *hackers*. A integridade da informação assegura que os dados sejam precisos e autênticos, com ataques voltados para sabotagem de dados para fins criminosos, políticos ou até militares.

Além disso, os usuários esperam que seu direito à privacidade das informações seja preservado. Ataques à disponibilidade de sistemas visam impedir que usuários autorizados acessem os recursos necessários para realizar suas atividades. Os tópicos abordados são representados na figura 1 abaixo (Caldas, 2013).

Figura 15 - Tríade CIA



Fonte: https://blog.almeidamatheus.me/post/seguranca-da-informacao/

7.1 Objetivos dos ataques em redes *wireless*

Os ataques cibernéticos são motivados por uma variedade de fatores, sendo o lucro financeiro um dos mais comuns. A venda de dados roubados na *Dark Web* (*web* obscura) e a extorsão por meio de *ransomware* (vírus sequestra dados do dispositivo e criptografa eles) são exemplos claros dessa motivação. No entanto, outros fatores também impulsionam esse tipo de crime, como a espionagem cibernética, que visa obter informações estratégicas para fins políticos ou econômicos. Além disso, ataques cibernéticos podem ser utilizados para desestabilizar governos, empresas e infraestruturas críticas, causando danos significativos e interrupções nos serviços (BRASIL, 2022).

7.1.1 Evil Twin

O ataque *Evil Twin* (gêmeo malicioso) é uma técnica em redes *wireless* em que um atacante cria um ponto de acesso falso, mas com as mesmas configurações, nome de rede (SSID) e outros detalhes do ponto de acesso legítimo, com o objetivo de enganar usuários para que se conectem ao ponto malicioso. Este ataque se aproveita da facilidade de configuração e da confiança que os usuários têm nas redes conhecidas, especialmente, em locais públicos como cafeterias, aeroportos e até em ambientes corporativos. Quando os dispositivos se conectam ao ponto de acesso falso, o atacante consegue interceptar todo o tráfego entre o dispositivo da vítima e a *internet*, possibilitando a captura de dados confidenciais, como credenciais de *login*, informações financeiras e até conteúdo de mensagens (Oliveira, 2007).

A configuração de um *Evil Twin* é relativamente simples com as ferramentas de *hacking* disponíveis atualmente. O atacante pode monitorar o tráfego na área para identificar redes populares e, então, clonar a rede alvo. Uma vez que o usuário se conecta ao ponto falso, o atacante assume uma posição de *Man in the Middle* (MitM), capturando o tráfego ou até redirecionando o usuário para páginas falsas em que as vítimas podem ser induzidas a fornecer informações sensíveis, como senhas e dados pessoais. Em um ambiente corporativo, o uso de um *Evil Twin* pode resultar em comprometimento de sistemas internos, acesso a dados empresariais sensíveis e até facilitar movimentos de pós-exploração.

Para proteger uma rede contra ataques *Evil Twin*, é importante implementar métodos de autenticação e criptografia robustos, como o WPA3 e autenticação baseada em certificados, especialmente em redes empresariais. Além disso, instruir os usuários a verificarem sempre a legitimidade da rede antes de se conectarem pode ajudar a reduzir o risco. Outra abordagem eficiente é o uso de sistemas de detecção de intrusão (IDS) focados em *wireless*, que podem

monitorar o ambiente e alertar sobre a presença de pontos de acesso não autorizados, permitindo uma resposta rápida e eficaz contra essa ameaça.

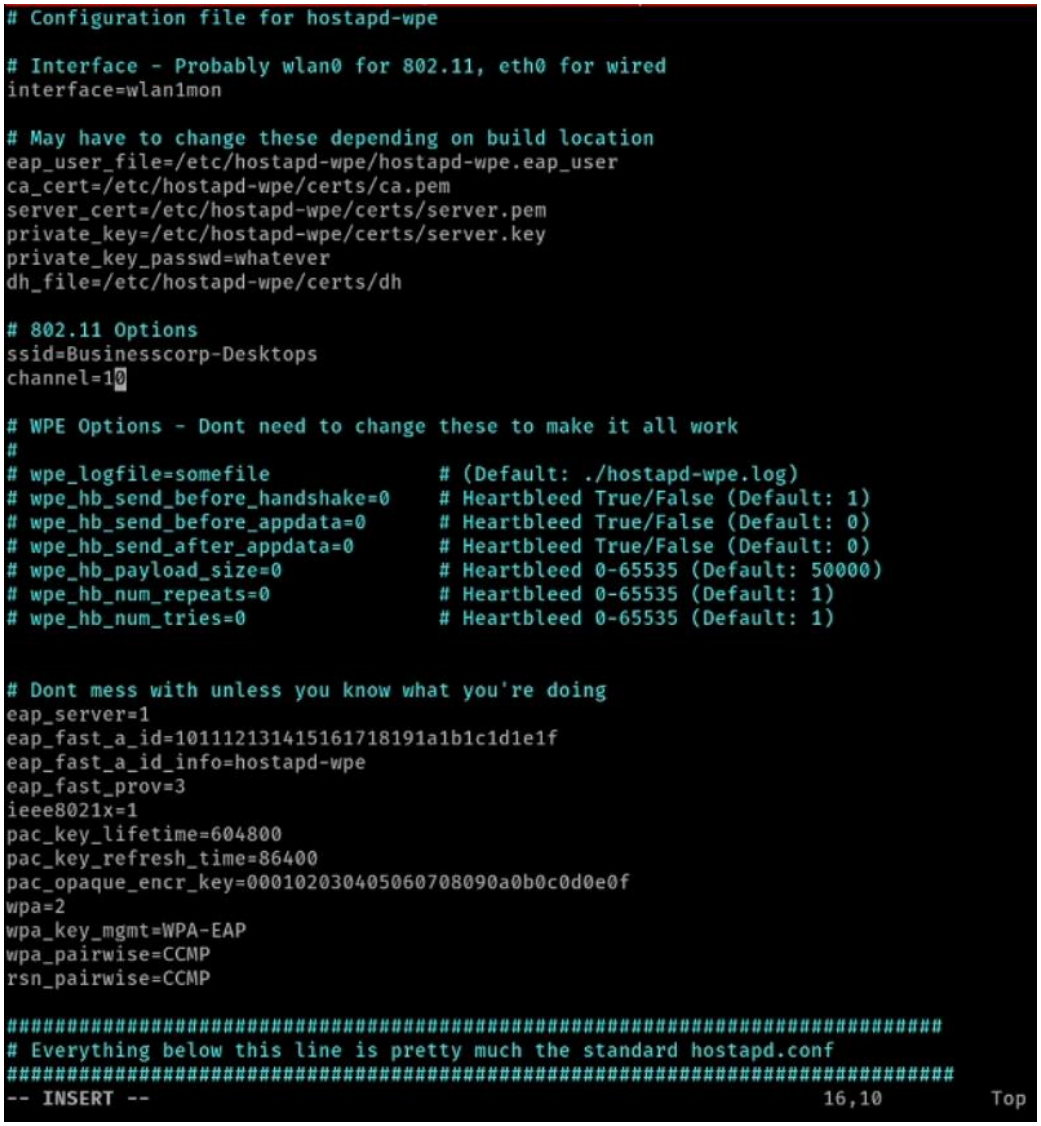
7.1.2 Ataque de WPA *Enterprise*

Este ataque explora a confiança que dispositivos conectados a uma rede WPA-*Enterprise* possuem no servidor RADIUS. Em vez de atacar diretamente o servidor legítimo, a estratégia consiste em configurar um servidor RADIUS falso, desautenticar os clientes da rede real e capturar suas credenciais quando tentam se reconectar automaticamente ao servidor malicioso.

O RADIUS (*Remote Authentication Dial-In User Service*) é um protocolo amplamente utilizado para autenticação, autorização e contabilização (AAA) de usuários em redes corporativas. Ele é comumente empregado em ambientes que utilizam o WPA-*Enterprise* para reforçar a segurança da conexão *wireless*, garantindo que apenas usuários autorizados possam acessar a rede. O processo envolve um servidor RADIUS que verifica as credenciais dos usuários antes de permitir o acesso.

Para realizar este ataque, foi utilizado o *hostapd*-wpe, uma versão modificada do *hostapd* que permite a interceptação de credenciais EAP (*Extensible Authentication Protocol*). Primeiro, configurou um ponto de acesso falso com o mesmo nome (SSID) da rede alvo, alterando parâmetros como SSID, canal e interface de rede.

Figura 16 - Configuração do *Hostpad*

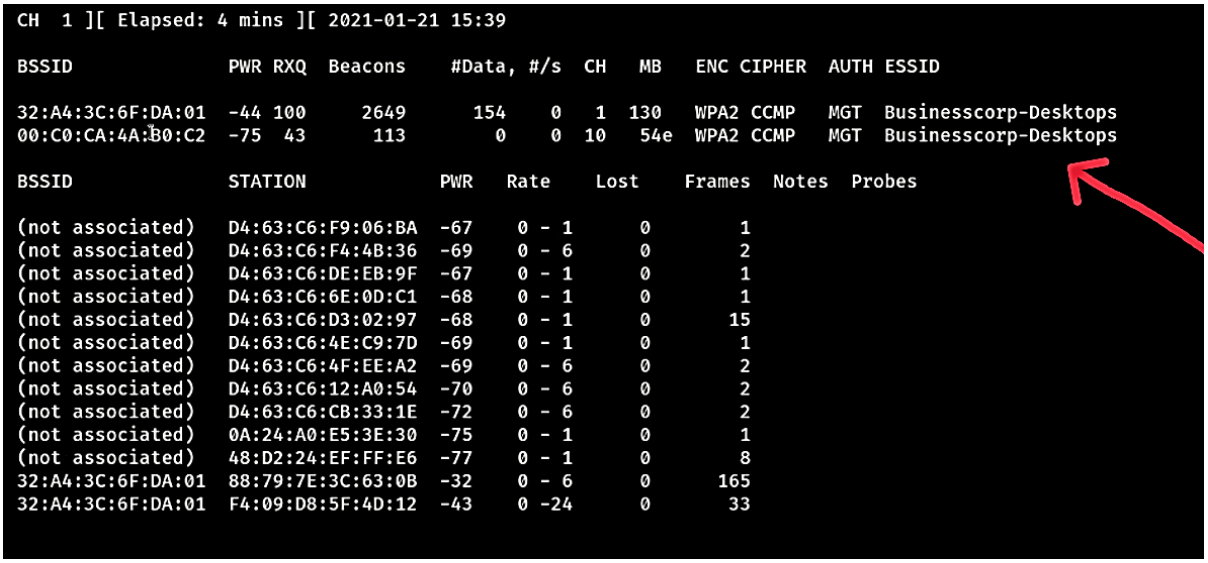


```
# Configuration file for hostapd-wpe

# Interface - Probably wlan0 for 802.11, eth0 for wired
interface=wlan1mon

# May have to change these depending on build location
eap_user_file=/etc/hostapd-wpe/hostapd-wpe.eap_user
ca_cert=/etc/hostapd-wpe/certs/ca.pem
server_cert=/etc/hostapd-wpe/certs/server.pem
private_key=/etc/hostapd-wpe/certs/server.key
private_key_passwd=whatever
dh_file=/etc/hostapd-wpe/certs/dh

# 802.11 Options
ssid=Businesscorp-Desktops
channel=10

# WPE Options - Dont need to change these to make it all work
#
# wpe_logfile=somefile              # (Default: ./hostapd-wpe.log)
# wpe_hb_send_before_handshake=0    # Heartbleed True/False (Default: 1)
# wpe_hb_send_before_appdata=0      # Heartbleed True/False (Default: 0)
# wpe_hb_send_after_appdata=0       # Heartbleed True/False (Default: 0)
# wpe_hb_payload_size=0             # Heartbleed 0-65535 (Default: 50000)
# wpe_hb_num_repeats=0              # Heartbleed 0-65535 (Default: 1)
# wpe_hb_num_tries=0                # Heartbleed 0-65535 (Default: 1)


# Dont mess with unless you know what you're doing
eap_server=1
eap_fast_a_id=101112131415161718191a1b1c1d1e1f
eap_fast_a_id_info=hostapd-wpe
eap_fast_prov=3
ieee8021x=1
pac_key_lifetime=604800
pac_key_refresh_time=86400
pac_opaque_encr_key=000102030405060708090a0b0c0d0e0f
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
rsn_pairwise=CCMP

##################################################################################
# Everything below this line is pretty much the standard hostapd.conf
##################################################################################
-- INSERT --                                                    16,10         Top
```

Fonte: https://desecsecurity.com/curso/Wi-fi-hacking

Após a configuração, os dispositivos próximos verão dois ESSIDs idênticos: um verdadeiro e outro falso, criado pelo atacante.

Figura 17 - Exibição de dois ESSIDs iguais, um legítimo e outro falso

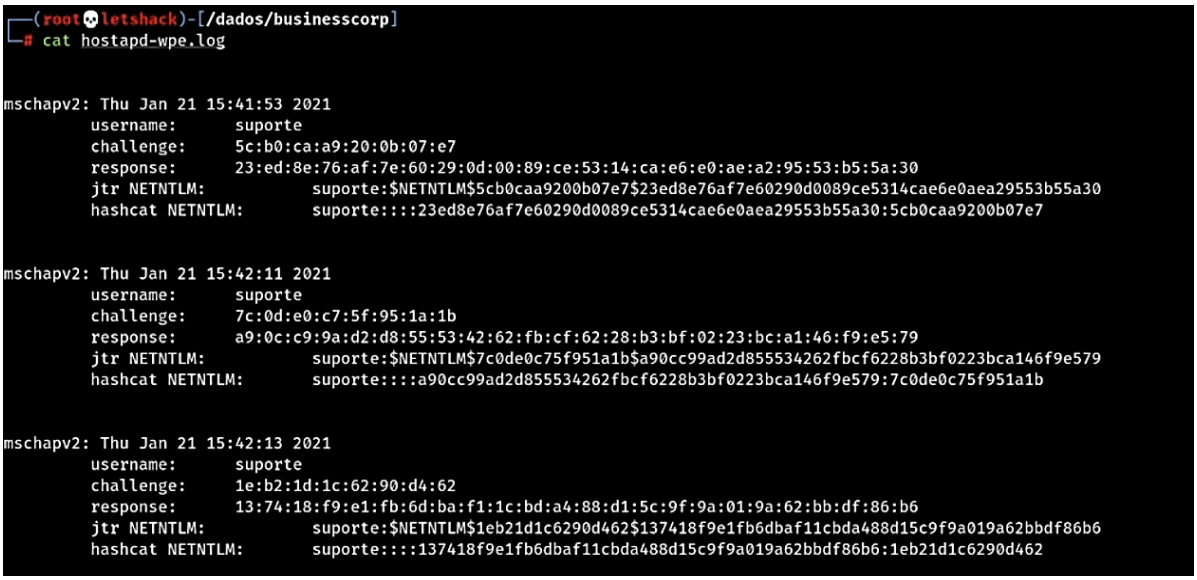


Fonte: https://desecsecurity.com/curso/Wi-fi-hacking

Para que os clientes se conectem ao ponto de acesso falso, é necessário desconectá-los da rede legítima. Isso pode ser feito utilizando o comando "aireplay-ng" para enviar pacotes de desautenticação à vítima, forçando-a a se reconectar.

aireplay-ng -0 0 -a <BSSID da rede alvo> -c <MAC da vítima> <interface>

Figura 18 - *Log* capturado pelo *hostapd-wpe* após a desautenticação



Fonte: https://desecsecurity.com/curso/Wi-fi-hacking

Após capturar as credenciais, utilizamos a ferramenta *asleap* para quebrar o *hash* e obter as senhas em texto claro. O ataque ocorre contra métodos de autenticação baseados em MS-CHAPv2, um protocolo vulnerável a ataques de dicionário e pré-computação.

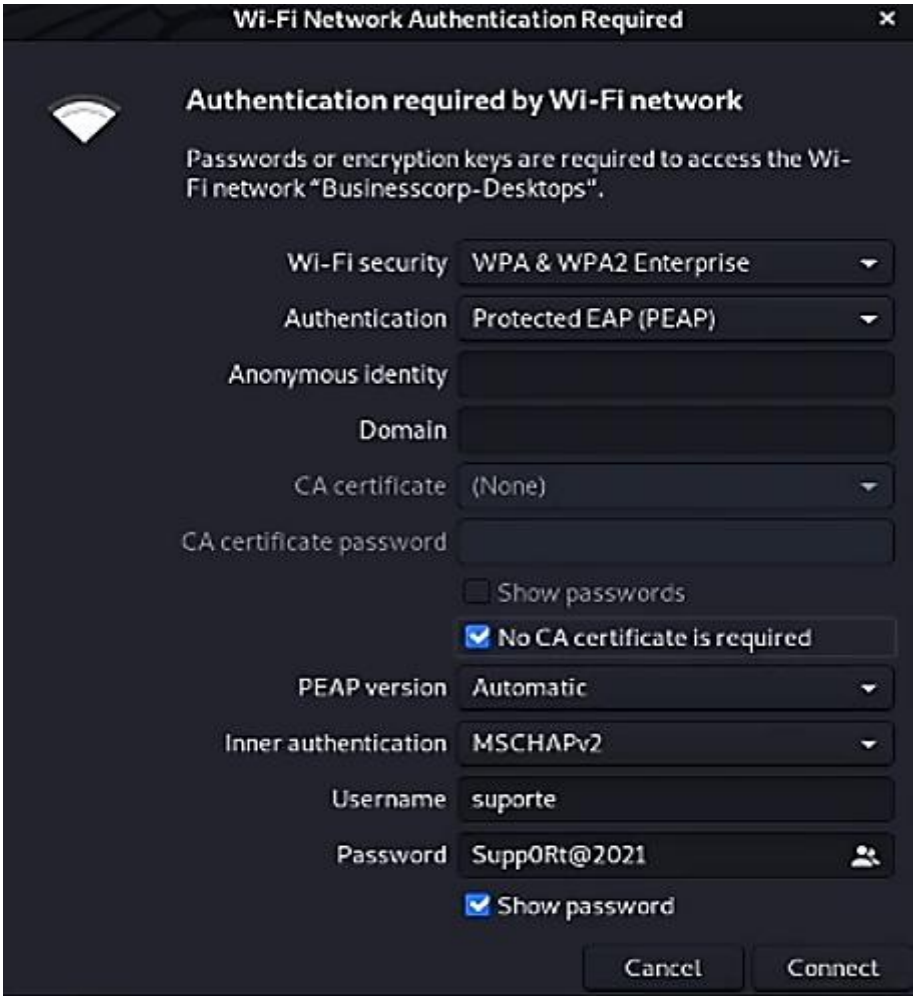
asleap -r hostapd-wpe.log -t <dicionário>

Figura 19 - Execução do *asleap* para quebra de credenciais

Fonte: https://desecsecurity.com/curso/Wi-fi-hacking

Uma vez que as credenciais foram recuperadas, é possível utilizá-las para se autenticar na rede legítima, comprometendo a segurança do ambiente corporativo.

Figura 20 - Conexão realizada com sucesso utilizando as credenciais adquiridas



Fonte: https://desecsecurity.com/curso/Wi-fi-hacking

Esse ataque demonstra a importância de utilizar métodos de autenticação mais robustos, como EAP-TLS, que não são vulneráveis a ataques baseados em dicionário ou força bruta.

7.1.3 Ataque WPA2

De acordo com Gunawan *et al.* (2018), o WPA2 (*Wi-fi Protected Access* 2) é um protocolo de segurança amplamente utilizado para proteger redes sem fio. Ele substituiu o antigo WEP (*Wired Equivalent Privacy*) e o WPA (*Wi-fi Protected Access*), oferecendo criptografia mais forte e autenticação mais segura. O WPA2 utiliza o protocolo AES (*Advanced Encryption Standard*) e o método de autenticação PSK (*Pre-Shared Key*) em redes domésticas ou 802.1X em redes empresariais. Um dos principais mecanismos de segurança do WPA2 é o *handshake* de quatro vias, um processo que garante que tanto o roteador (AP) quanto o dispositivo conectado compartilhem uma chave segura para criptografar os dados transmitidos.

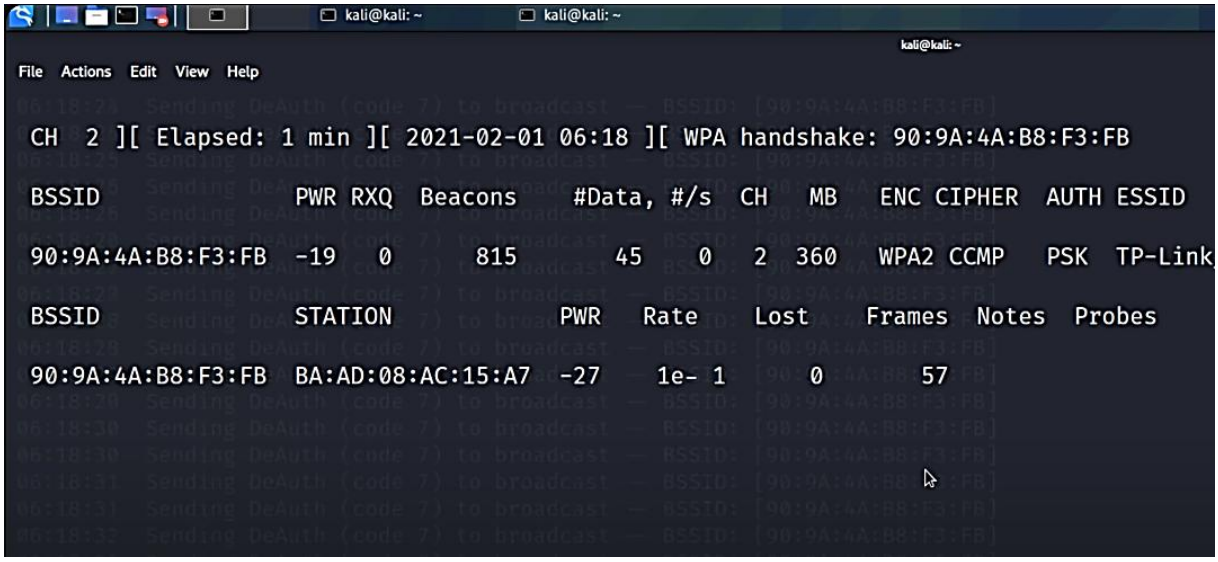
Apesar de ser considerado seguro, o WPA2 ainda pode ser comprometido, especialmente quando senhas fracas são utilizadas. Um dos métodos mais comuns de ataque consiste na captura do *handshake* de quatro vias, que ocorre quando um dispositivo se conecta ao ponto de acesso (AP). Para isso, uma ferramenta como airodump-ng pode ser utilizada para monitorar e capturar os pacotes de autenticação transmitidos entre o dispositivo e o roteador.

O ataque começa com o uso de aireplay-ng para enviar pacotes de desautenticação, forçando um dispositivo conectado a se desconectar do AP. Como a maioria dos dispositivos tenta se reconectar automaticamente, o airodump-ng pode capturar o *handshake* no momento da reconexão. Com esses dados em mãos, um atacante pode tentar quebrar a senha utilizando um ataque de dicionário com o aircrack-ng, testando uma grande quantidade de senhas até encontrar a correta.

Diferente de ataques baseados em *phishing*, como o realizado pelo Fluxion, que engana o usuário para que ele mesmo insira a senha, a abordagem com airodump-ng e aircrack-ng depende da força da senha utilizada na rede. Se a senha for simples e baseada em palavras comuns, o ataque pode ser bem-sucedido em poucas horas. No entanto, senhas longas e aleatórias tornam esse tipo de ataque extremamente difícil.

Para mitigar esses riscos, recomenda-se utilizar senhas complexas, implementar WPA3 sempre que possível e evitar conexões automáticas a redes *Wi-fi* desconhecidas. Além disso, empresas podem adotar métodos de autenticação mais robustos, como o 802.1X com RADIUS, para garantir uma camada extra de proteção nas redes corporativas.

Figura 21 - Captura de *handshake*



Fonte: https://desecsecurity.com/curso/Wi-fi-hacking

Ataque realizado em um ambiente de testes, foi utilizado o comando:

aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

Esse comando faz uso da ferramenta aireplay-ng, que integra o conjunto de ferramentas aircrack-ng, amplamente utilizadas em auditorias de segurança de redes sem fio. O parâmetro --deauth 0 envia pacotes de desautenticação de forma contínua, impedindo que o dispositivo alvo permaneça conectado ao ponto de acesso (AP) até que o ataque seja interrompido manualmente. A opção -a 90:9A:4A:B8:F3:FB especifica o endereço MAC do ponto de acesso a ser atacado. Já o argumento wlan0mon define a interface de rede que está operando no modo monitor, permitindo a interceptação dos pacotes transmitidos pela rede *Wi-fi*.

O objetivo desse ataque é fazer com que o dispositivo vítima perca a conexão com a rede sem fio, forçando-o a tentar se reconectar. Durante esse processo de reconexão, ocorre a troca do *handshake* de quatro vias entre o AP e o dispositivo cliente. Esse *handshake* contém informações essenciais para o processo de autenticação do protocolo WPA2 e, se capturado, pode ser utilizado em ataques *offline* com o objetivo de descobrir a senha da rede.

Para a captura do *handshake*, pode-se utilizar outra ferramenta do pacote aircrack-ng, como o airodump-ng, responsável por monitorar os pacotes transmitidos na rede e salvar as informações relevantes para análise posterior. Dessa forma, o ataque de desautenticação é frequentemente combinado com a captura de pacotes para garantir que o *handshake* seja obtido com sucesso.

7.1.4 Ataque DDoS

O ataque de negação de serviço distribuído (DDoS – *Distributed Denial of Service*) é uma das técnicas mais conhecidas e perigosas dentro do arsenal de um atacante, sendo amplamente utilizado para indisponibilizar sistemas, servidores e aplicações acessíveis pela internet. O objetivo principal de um DDoS é sobrecarregar os recursos computacionais do alvo, como processador, memória, largura de banda ou número de conexões simultâneas, até o ponto em que ele se torna incapaz de responder a requisições legítimas, tornando o serviço fora do ar para seus usuários.

Diferente de um ataque DoS tradicional, que parte de uma única máquina, o DDoS utiliza uma rede de dispositivos distribuídos — frequentemente infectados por malwares e controlados remotamente — conhecida como botnet. Cada nó da botnet envia requisições ou pacotes maliciosos ao servidor alvo de forma simultânea, multiplicando exponencialmente o volume de tráfego recebido. O ataque pode ser conduzido em diversas camadas do modelo OSI, sendo os mais comuns os ataques de camada 3/4 (como SYN *flood*, UDP *flood* e ICMP *flood*) e camada 7 (ataques HTTP que exploram recursos da aplicação web).

Um dos métodos mais simples, mas ainda eficazes, é o uso do comando hping3 com a opção --flood, que envia pacotes TCP, UDP ou ICMP de forma contínua, simulando múltiplas tentativas de conexão. Por exemplo, ao executar hping3 -S --flood -p 80 <IP do alvo>, o atacante envia pacotes SYN à porta 80 do servidor de forma ininterrupta, tentando abrir milhares de conexões simultâneas. Esse tipo de ataque, conhecido como SYN flood, explora a maneira como o protocolo TCP lida com o processo de estabelecimento de conexões, mantendo recursos alocados mesmo quando a conexão não é concluída.

Em nível de aplicação, ferramentas como o LOIC (*Low Orbit Ion Cannon*) ou o *GoldenEye* permitem que o atacante envie requisições HTTP massivas para sobrecarregar servidores web. Esses ataques são particularmente eficazes quando o site utiliza aplicações pesadas ou bases de dados, pois cada requisição exige mais processamento para ser atendida. Em ataques mais sofisticados, o tráfego pode ser embaralhado para dificultar a detecção por firewalls ou balanceadores de carga.

Os efeitos observados em ataques DDoS incluem lentidão extrema na navegação, erros de carregamento (como HTTP 503 - *Service Unavailable*), interrupções completas no serviço, ou até a queda total do servidor em casos de esgotamento dos recursos físicos. Em ambientes corporativos, tais interrupções podem causar prejuízos operacionais, financeiros e até reputacionais. Por isso, é fundamental que administradores de sistemas adotem estratégias de

mitigação como filtros de pacotes, limitação de conexões por IP, uso de serviços especializados (como Cloudflare, Akamai), detecção de tráfego anômalo e provisionamento escalável de recursos. Abaixo, apresenta-se uma imagem ilustrando um exemplo prático da execução de um ataque DDoS em ambiente controlado.

Figura 22 - Ataque DDoS ao site focoemsec.com.br

Fonte: https://www.youtube.com/watch?v=vwgKX6-YhU4

7.2 Pós-exploração em redes

A pós-exploração é a fase de um ataque em que o invasor, após obter acesso inicial ao sistema ou à rede, analisa o ambiente comprometido para explorar e expandir o controle sobre os recursos disponíveis. Durante essa etapa, o atacante busca identificar dados sensíveis, como credenciais, informações financeiras ou segredos comerciais, que possam ser extraídos ou utilizados para obter mais acesso. Em redes *wireless*, a pós-exploração pode envolver a execução de ferramentas de análise de tráfego, varredura de portas e protocolos para mapear outros dispositivos conectados e identificar vulnerabilidades adicionais. Essa fase é crucial para o atacante, pois permite consolidar o acesso, evadir detecções e maximizar o impacto do ataque. Para a defesa, entender a pós-exploração ajuda a desenvolver medidas de monitoramento e resposta, que limitam a movimentação do atacante dentro da rede e minimizam os danos.

7.2.1 ARP *Poisoning* - Interceptação de *Login* em um Ambiente de Testes

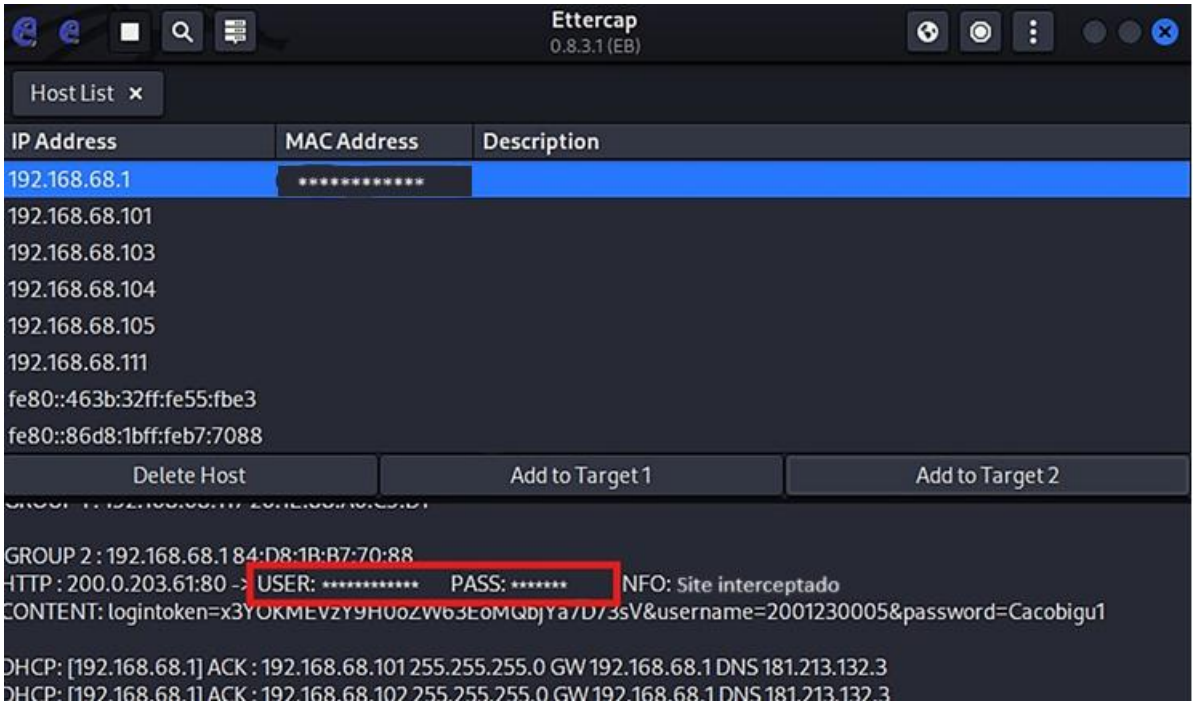
O ARP *Poisoning* é uma técnica de ataque baseada na exploração do protocolo *Address Resolution Protocol* (ARP), utilizado para mapear endereços IP para endereços MAC dentro de

redes locais. Conforme demonstrado por CERTBROS (2022), esse protocolo, por padrão, não possui mecanismos de autenticação, tornando-se vulnerável a ataques de falsificação. A técnica de envenenamento ARP é amplamente utilizada por atacantes para realizar ataques de *Man-in-the-Middle* (MitM), interceptando o tráfego de rede sem que os dispositivos envolvidos percebam a manipulação dos dados.

O ataque ocorre quando um invasor envia pacotes ARP falsificados para a rede, associando seu próprio endereço MAC ao IP do *gateway* ou de outro dispositivo alvo. Como consequência, o tráfego que deveria ser enviado diretamente ao roteador passa primeiro pelo atacante, que pode analisá-lo, modificá-lo ou até mesmo bloqueá-lo. Esse tipo de ataque é especialmente perigoso em redes que não utilizam criptografia para a comunicação de dados, como ocorre em conexões HTTP, onde informações sensíveis são transmitidas em texto claro.

O experimento foi conduzido em um ambiente de testes configurado para simular um cenário real de rede corporativa. Durante os testes, foi possível observar que a ausência de proteção contra ataques ARP *Poisoning* permitiu a interceptação e a captura de credenciais de *login* trafegando sem criptografia. Para a execução do ataque, foi utilizado o *Ettercap*, ferramenta amplamente empregada para a realização de ataques MitM. Essa ferramenta possibilitou o redirecionamento do tráfego de pacotes entre os dispositivos da rede, possibilitando o monitoramento das comunicações entre os usuários e o servidor de autenticação.

Figura 23 - Listagem de dispositivos na rede usando *Ettercap*

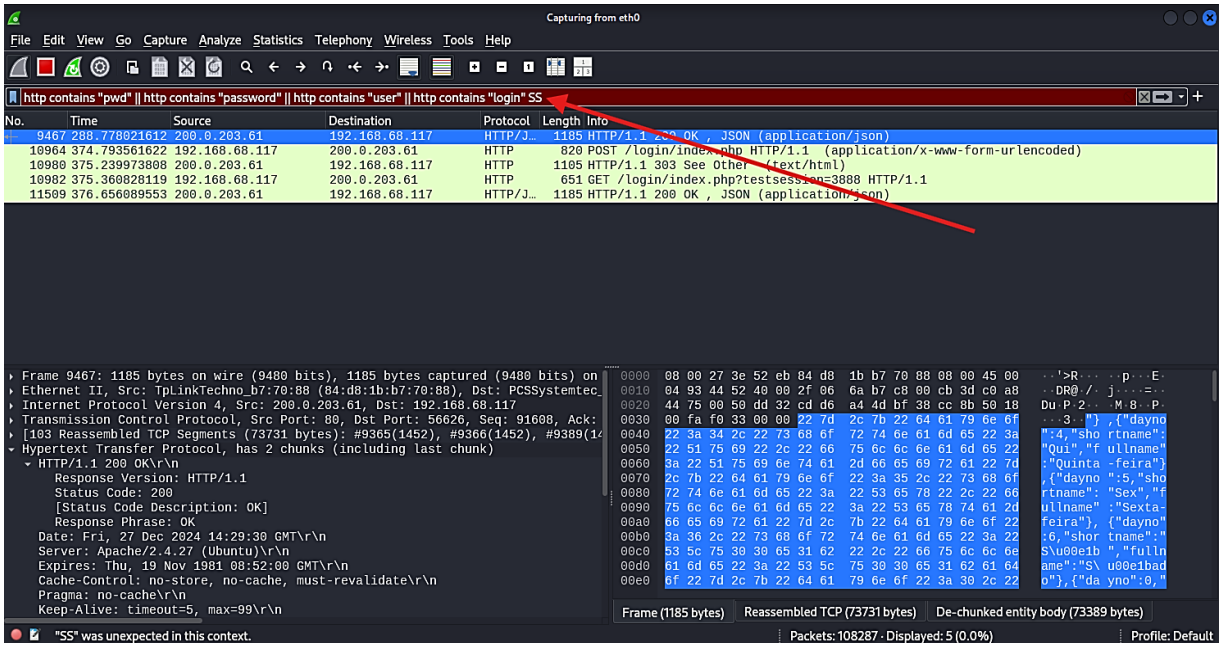


Fonte: Elaborada pelo autor (2025)

A captura e análise do tráfego foram realizadas com o *Wireshark*, um analisador de protocolos que permite inspecionar os pacotes transmitidos na rede em tempo real. Foi aplicado um filtro para identificar requisições contendo dados de autenticação enviados via HTTP, utilizando a seguinte regra de filtragem:

http contains "pwd" || http contains "password" || http contains "user" || http contains "login"

Figura 24 - Interceptação do tráfego



Fonte: Elaborada pelo autor (2025)

A análise revelou que credenciais estavam sendo transmitidas sem criptografia, tornando-as suscetíveis a interceptação por parte de um atacante posicionado na mesma rede. Esse experimento evidenciou a necessidade de implementação de protocolos de segurança, como HTTPS, que utiliza a criptografia TLS para proteger as comunicações entre cliente e servidor. Além disso, medidas como autenticação multifator (MFA), segmentação de redes e monitoramento ativo podem reduzir significativamente o risco de ataques do tipo ARP *Poisoning*.

A realização deste estudo permitiu reforçar a importância da segurança nas comunicações em redes locais, principalmente em ambientes que lidam com dados sensíveis. O uso de criptografia para proteger as credenciais dos usuários deve ser uma prioridade para qualquer organização que deseja garantir a integridade e a privacidade de suas informações. Sem a adoção dessas práticas, ataques de interceptação de tráfego continuarão sendo uma ameaça constante para redes desprotegidas.

7.2.2 Ataque de Força Bruta

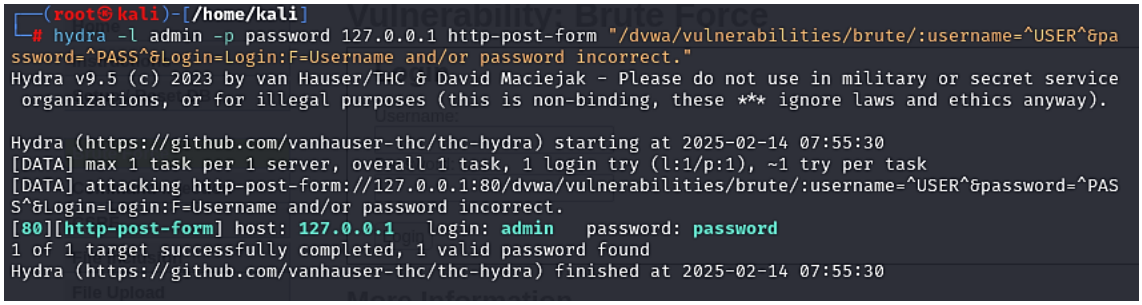
Os ataques de pós-exploração são uma fase crítica no comprometimento de um sistema, na qual o invasor busca consolidar e expandir seu acesso após a exploração inicial de uma vulnerabilidade. Um dos métodos mais comuns nesse estágio é o ataque de força bruta, que consiste na tentativa sistemática de diferentes combinações de usuário e senha até que uma credencial válida seja encontrada. Essa técnica é eficaz contra sistemas que não possuem proteções adequadas, como bloqueio temporário após múltiplas tentativas falhas, autenticação multifator (MFA) ou restrições de acesso baseadas em comportamento suspeito.

Dentro desse contexto, foi utilizado o *Damn Vulnerable Web Application* (DVWA), uma aplicação *web* propositalmente vulnerável desenvolvida para testes de segurança ofensiva. O DVWA permite a exploração de diferentes tipos de ataques, incluindo injeção de SQL, *Cross-Site Scripting* (XSS), falhas de autenticação e, principalmente, ataques de força bruta. Essa plataforma é amplamente utilizada em treinamentos de cibersegurança e simulações de ataques controlados, fornecendo um ambiente seguro para a experimentação de técnicas ofensivas sem infringir normas legais.

Para a realização do ataque de força bruta, foi utilizado o Hydra, uma das ferramentas mais eficazes para a automatização de tentativas de autenticação em diversos protocolos, como HTTP, SSH, FTP e SMTP. O Hydra permite testar múltiplas credenciais de forma rápida e eficiente, sendo amplamente empregado em auditorias de segurança para avaliar a robustez de sistemas de autenticação.

O ataque foi conduzido utilizando o Hydra com parâmetros específicos para explorar a vulnerabilidade do DVWA. O nome de usuário utilizado foi "admin" e a *wordlist* empregada foi a *rockyou.txt*, contendo diversas senhas comuns. O ataque foi realizado localmente no servidor (127.0.0.1), utilizando o método http-post-form, que permite a automação de tentativas de autenticação contra formulários *web*. O formulário de *login* do DVWA foi configurado para receber credenciais no formato username=^USER^&password=^PASS^&Login=Login, onde os valores ^USER^ e ^PASS^ foram substituídos automaticamente pelo Hydra durante as tentativas de força bruta. A resposta esperada para tentativas malsucedidas foi "Username and/or password incorrect.", permitindo ao Hydra identificar quando um *login* foi bem-sucedido.

Figura 25 - Uso do Hydra na prática



Fonte: Elaborado pelo autor (2025)

Após a execução do ataque, o Hydra percorreu milhares de combinações de credenciais até encontrar uma senha válida, demonstrando a vulnerabilidade do sistema quando não há mecanismos de proteção adequados. O sucesso do ataque reforça a necessidade de implementação de boas práticas de segurança para mitigar esse tipo de ameaça.

Entre as medidas recomendadas para evitar ataques de força bruta, destacam-se a autenticação multifator (MFA), que adiciona uma segunda camada de autenticação para impedir acessos não autorizados apenas com o uso de senha; a implementação de bloqueio temporário de conta após múltiplas tentativas malsucedidas, dificultando ataques automatizados; o uso de CAPTCHAs para evitar que *bots* realizem tentativas repetitivas de *login*; e a adoção de *rate limiting*, que restringe o número de tentativas permitidas dentro de um intervalo de tempo específico. Além disso, a criação de políticas de senha robustas, incentivando o uso de senhas longas e exclusivas, reduz significativamente o risco de exploração por ataques baseados em dicionários.

A simulação desse ataque no DVWA demonstrou, na prática, como sistemas sem proteções adequadas podem ser comprometidos por métodos automatizados. Esse estudo reforça a importância de políticas de segurança bem definidas para garantir a integridade dos sistemas e prevenir acessos não autorizados por meio de ataques de força bruta.

CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo analisar os principais ciberataques direcionados a ativos de rede em ambientes corporativos, com foco especial em redes wireless, considerando aspectos teóricos e práticos. Foi possível compreender que a crescente digitalização das organizações, associada à mobilidade proporcionada pelas redes sem fio, cria um ambiente propício à exploração de vulnerabilidades. Dentre os ataques abordados, destacam-se o *Evil Twin*, *Captive Portal*, ataques a WPA/WPA2, ARP *Poisoning*, ARP *Spoofing* e força bruta, todos capazes de comprometer a integridade, a confidencialidade e a disponibilidade das informações.

A análise teórica permitiu contextualizar os fundamentos da segurança da informação, os tipos de redes, os modelos de referência, os princípios dos ataques e os principais algoritmos criptográficos aplicáveis. Já a aplicação prática das técnicas de pós-exploração revelou, em ambiente controlado, como atacantes podem, a partir de uma brecha de segurança, executar ataques em camadas mais profundas do sistema, ampliando os danos potenciais. O estudo também demonstrou, através de um questionário aplicado a estudantes da FeMASS, que ainda há falhas significativas no conhecimento e nas práticas de segurança no uso de redes sem fio, mesmo entre usuários familiarizados com tecnologia.

Diante do cenário analisado, conclui-se que além da implementação de medidas técnicas de segurança, é essencial promover a educação contínua dos usuários, especialmente em ambientes acadêmicos e corporativos, onde a negligência com práticas básicas pode representar riscos sérios. O trabalho reforça a importância da integração entre teoria, prática e conscientização para mitigar os impactos dos ataques cibernéticos em redes wireless.

Como proposta para trabalhos futuros, destaca-se a realização de testes de invasão (pentest) em ambientes empresariais com autorização prévia, com o objetivo de identificar vulnerabilidades reais e propor medidas corretivas. Além disso, propõe-se o uso de técnicas de machine learning para detecção proativa de ataques, permitindo respostas mais ágeis e eficazes. Outra frente relevante seria a avaliação de vulnerabilidades em dispositivos IoT conectados a redes abertas, considerando o crescimento desse tipo de tecnologia em ambientes corporativos e residenciais.

Em termos de melhorias esperadas, sugere-se o desenvolvimento de ferramentas próprias para análise e mitigação de ameaças, além da criação de um laboratório dedicado ao estudo e treinamentos em segurança da informação, possibilitando práticas mais aprofundadas e realistas. Essas iniciativas visam fortalecer o preparo técnico e prático de profissionais da área, promovendo uma cultura contínua de segurança digital.

REFERÊNCIAS

BARROS, Otávio Santana Rêgo. GOMES, Ulisses de Mesquita. FREITAS, Whitney Lacerda de. **Desafios Estratégicos para a Segurança e Defesa Cibernética.** 1ª edição. Brasília: Secretaria de Assuntos Estratégicos, 2011.

BOTTI, Caio Fernandes. MARTINS, Daves Márcio Silva. **Análise comparativa entre ferramentas de ataque *Man in the Middle*.** Juiz de Fora: CES/JF, 2015. Disponível em: https://seer.uniacademia.edu.br/index.php/cesi/article/view/517/400. Acesso em: 19 de novembro de 2024.

BRASIL. **Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. Aumento de ataques às infraestruturas críticas.** Disponível em: https://www.gov.br/ctir/pt-br/assuntos/noticias/2022/aumento-de-ataques-as-infraestruturas-criticas. Acesso em: 17 de novembro de 2024.

_____. **Resolução CNCiber nº 4**, de 25 de março de 2024. Diário Oficial da União, Seção 1, n. 59, p. 7, 26 mar. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cnciber-n-4-de-25-de-marco-de-2024-550308382. Acesso em: 14 de setembro de 2024.

CALDAS, Alexandre. FREIRE, Vicente. **Cibersegurança:** das Preocupações à Ação. Instituto da Defesa Nacional, 2012. Disponível em: https://www.jstor.org/stable/resrep19122?seq=2. Acesso em: 14 de setembro de 2024.

CERTBROS. ***ARP Poisoning**: Man-in-the-Middle Attack*. YouTube, 2022. Disponível em: https://www.youtube.com/watch?v=A7nih6SANYs&list=LL&index=4&t=602s. Acesso em: 3 de janeiro de 2025.

CNN BRASIL. **Ataques *hackers* aumentam 8,8% no Brasil e país segue como 2º mais atacado do mundo.** CNN Brasil, 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/ataques-hackers-aumentam-88-no-brasil-e-pais-segue-como-2o-mais-atacado-do-mundo/. Acesso em: 14 de setembro de 2024.

CRISTIANO, Cleber. CESAR, Ernani. **Metodologia do trabalho científico**: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2ª edição. Rio Grande do Sul: Feevale, 2013.

CUNHA, André, *et al.* ***Man In The Middle***. Segurança de Sistemas e Redes, 2006.

FRAGA, Bruno. **Técnicas de Invasão.** São Paulo: Editora Labrador, 2019.

GUNAWAN, Teddy Surya. LIM, Muhammad Kasim. KARTIWI, Mira. MALIK, Noreha Abdul. ISMAIL, Nanang. ***Penetration testing using Kali Linux:** SQL Injection, XSS, WordPress, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science*, [S.l.], v. 12, n. 2, p. 729-737, nov. 2018.

IBM. ***Cyber Attack.*** Disponível em: https://www.ibm.com/br-pt/topics/cyber-attack. Acesso em: 14 de setembro de 2024.

KEVIN, Daniel. SILVA, Hyan. **Relatório de Análise de Vulnerabilidades.** 2022. Disponível em: https://gtifadba.com.br/wp-content/uploads/2023/04/Pentest-daniel-hyan.docx-1.pdf. Acesso em: 14 de setembro de 2024.

MACÊDO, Diego. **Redes Sem Fio *(Wireless):*** Fundamentos e Padrões**.** 2012. Disponível em: https://www.diegomacedo.com.br/redes-sem-fio-wireless-fundamentos-e-padroes/. Acesso em: 14 de setembro de 2024.

MARQUES, Anderson. **Modelo de Referência OSI**. 17 f. TCC – Tecnologia em Análise e Desenvolvimento de Sistemas, Instituto Federal do Pará, Tucumã, 2009. Disponível em: https://dom.maua.sp.gov.br/public/docs/5100781e-72f2-425d-82f2-be814305ee55.pdf. Acesso em: 20 de outubro de 2024.

MELO, Sandro. **Exploração de Vulnerabilidades em redes TCP/IP.** Rio de Janeiro: 3ª edição, 2017. Disponível em: https://www.amazon.com.br/Explora%C3%A7%C3%A3o-vulnerabilidade-Rede-TCP-IP/dp/8550800708. Acesso em: 14 de setembro de 2024.

MORENO, Daniel. **Introdução ao *Pentest*.** 2ª edição, São Paulo: Novatec, 2019.

OLIVEIRA, Alysson Nishiyama de. **Autenticação em redes *wireless* com certificação digital evitando "*evil twin*".** 100 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Faculdade de Ciências Exatas e de Tecnologia, UniCeub, Brasília, 2007. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/123456789/3179/2/9965560.pdf. Acesso em: 09 de novembro de 2024.

PINHEIRO, João Netto. OLIVEIRA, João Paulo Nascimento. VIEIRA, Paulo Roberto. **NMAP**. Faculdade Senac Goiás, Curso de Gestão de Tecnologia da Informação, Goiânia, 2018.

SCHWARTZMAN, S. **Um espaço para a ciência:** a formação da comunidade científica no Brasil. Brasília: Ministério de Ciência e Tecnologia Conselho Nacional de Desenvolvimento Cientifico e Tecnológico Centro de Estudos Estratégicos, 2001.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. **Redes de Computadores (coedição Bookman e Pearson)**. [s.l.] Bookman Editora, 2021.

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1–38, 9 maio 2020.

ANEXO A – DECLARAÇÃO DE CORREÇÃO GRAMATICAL

DECLARAÇÃO DE CORREÇÃO GRAMATICAL

Eu, Natalí de Oliveira Moreira, CPF nº 156.480.637-50, portadora da carteira de identidade nº 27.272.184-6, formada em Letras: Português e Literaturas, DECLARO, para os devidos fins, que realizei a correção ortográfica e gramatical do Trabalho de Conclusão de Curso do aluno Caio Lucas Lima Almeida, do curso de Sistemas de Informação, orientado pelo professor Lahir Bockorni.

(assinatura da revisora)

Data: 14 de junho de 2025

ANEXO B – PARECER TÉCNICO

Estado do Rio de Janeiro
Prefeitura Municipal de Macaé
Secretaria Municipal de Educação
Secretaria Executiva de Ensino Superior
Faculdade Professor Miguel Ângelo da Silva Santos – FeMASS

FeMASS

Recredenciamento: Parecer CEE-RJ nº 40 de 21/11/2023, homologado pela Portaria CEE-RJ nº 3914 de 21/11/2023, publicado no D.O /RJ nº 215, seção 1,pág. 23 de 23/11/2023

ANEXO I

PARECER TÉCNICO: TRABALHO DE CONCLUSÃO DE CURSO (TCC)

CURSO: ( ) ADMINISTRAÇÃO ( ) ENGENHARIA DE PRODUÇÃO (X) SISTEMAS DE INFORMAÇÃO
( ) MATEMÁTICA

ALUNO (A): CAIO LUCAS LIMA ALMEIDA

MATRÍCULA: 2021230005 DATA DA DEFESA: 07/07/2025

PROFESSOR ORIENTADOR:
LAHIN BOCKORNI

BANCA:
LAHIN BOCKORNI
MARINELLI DE OLIVEIRA PAULA

TÍTULO:
ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM AMBIENTE DE REDE EM AMBIENTES CORPORATIVOS

PARECER FINAL:
Em cumprimento ao Art. 9º, §5º da Deliberação nº____/17, atesto que o (a) aluno (a) acima referido (a):
(X) atendeu às solicitações/ajustes encaminhados pela banca para validação da versão final do TCC.
( ) não atendeu às solicitações/ajustes encaminhados pela banca para validação da versão final do TCC.

Encaminhe-se à Secretaria Acadêmica da FeMASS, para os registros, considerando o (a) aluno(a):
(X) APROVADO ( ) REPROVADO

Macaé, 09 de JULHO de 2025.

ASSINATURA DO PROFESSOR ORIENTADOR