Trabalho de Conclusão de Curso

Avaliação de Risco em Redes 802.11n: Uma abordagem baseada em Árvores de Ataque

Paloma da Silva Lacerda dos Santos
psls@ic.ufal.br

Orientador:
Prof. Dr. Almir Pereira Guimarães

Maceió, Abril de 2024

Paloma da Silva Lacerda dos Santos

Avaliação de Risco em Redes 802.11n: Uma abordagem baseada em Árvores de Ataque

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação do Instituto de Computação da Universidade Federal de Alagoas.

Orientador:

Prof. Dr. Almir Pereira Guimarães

Maceió, Abril de 2024

Paloma da Silva Lacerda dos Santos

Avaliação de Riscos e Redes 802.11n: uma abordagem baseada em árvores de ataque.

Este Trabalho de Conclusão de Curso (TCC) foi julgado adequado para obtenção do Título de Bacharel em Ciência da Computação e aprovado em sua forma final pelo Instituto de Computação da Universidade Federal de Alagoas.
Maceió, _03_ de _abril_ de 2024.

_____

Professora Dra. Roberta Vilhena Vieira Lopes.
Coordenador do Curso de Ciência da Computação

Banca Examinadora:

_____

Prof. ALMIR PEREIRA GUIMARÃES, Dr.
Orientador
Instituto de Computação

_____

Prof. PETRÚCIO ANTÔNIO MEDEIROS BARROS, Me.
Universidade Federal de Alagoas
Instituto de Computação

_____

Prof. RÔMULO OLIVEIRA, Me.
Universidade Federal de Alagoas
Campus Arapiraca

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária: Helena Cristina Pimentel do Vale – CRB4 - 661

S237a Santos, Paloma da Silva Lacerda dos.
Avaliação de risco em redes 802.11n : uma abordagem baseada em árvores de ataque / Paloma da Silva Lacerda dos Santos. – 2024.
69 f.: il.

Orientador: Almir Pereira Guimarães
Monografia (Trabalho de Conclusão de Curso em Ciências da Computação) – Universidade Federal de Alagoas, Instituto de Computação. Graduação em Ciência da Computação. Maceió, 2024.

Bibliografia: f. 67-69.

1. Avaliação de risco. 2. Redes Wi-Fi (IEEE 802.11). 3. Modelagem de ameaças. 4. Segurança de redes. 5. Árvores de ataque. I. Título.

CDU: 004.77

Agradecimentos

Gostaria de agradecer primeiramente a Deus, por ter permitido que minhas ambições durante esses anos de curso fossem alcançadas.

Aos meus pais, Maisa e Lacerda, pelo sacrifício realizado diariamente desde o meu nascimento para garantir uma educação de qualidade para mim e minha irmã, e por todo o apoio fornecido não apenas durante a graduação, mas em todas as áreas da minha vida.

À minha irmã, Luana, por seu apoio e compreensão ao longo de todos esses anos, incentivando-me nos momentos difíceis e compartilhando minhas alegrias.

Agradeço ao meu namorado, Rodrigo, pelo constante incentivo e apoio em cada etapa da graduação que passamos juntos, por sempre acreditar na minha capacidade e estar ao meu lado nas dificuldades.

Agradeço aos meus amigos que esse curso me proporcionou conhecer, Gabriel (Gabiru), Yanka (Raissa), Elias (Lias), Vinicius (Vine) , Pedro(Pedu) e Túlio (Tulin), por me acompanharem desde o primeiro dia de aula e me incentivarem nos momentos mais trabalhosos da graduação, pelos momentos de descontração tanto dentro quanto fora da sala de aula, pelos almoços no RU e CETEC, pelas fofocas compartilhadas, pelos concelhos divididos e acima de tudo por me mostrarem que a graduação não é apenas estudo e que é preciso um equilíbrio entre tudo.

Às meninas do curso, em especial a Carol, Nathalia, Esther, Ully, Kamila e Lilian, pelo apoio mútuo e companheirismo ao longo da jornada acadêmica.

Gostaria de agradecer ao meu orientador Almir Guimarães, pelos ensinamentos e pelo tempo que estivemos trabalhando juntos no decorrer desse trabalho.

Também expresso minha gratidão a todos os professores do Instituto de Computação, em especial à professora Roberta, pela atenção e orientação dedicadas a mim desde o início da graduação.

Agradeço ao corpo técnico do Instituto de Computação, em especial a Ana Ferreira por sempre ajudar nas maiores emergências, pelos conselhos e conversas compartilhadas nos corredores. Agradeço também a Tia Lúcia por sempre cuidar de todos os alunos e do Instituto com tanta dedicação.

Agradeço também todos aqueles que não mencionei, mas que se fizeram presente em algum momento durante esses anos, estão guardados na memória com afeto.

Por fim, agradeço à banca examinadora pelo tempo dedicado à leitura, questionamentos e sugestões oferecidas.

"Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes"

– King, *Marthin Luther*

Paloma Lacerda

Resumo

Com o avanço da tecnologia e a crescente integração das redes wi-fi em diversos aspectos da vida moderna, desde ambientes domésticos até ambientes corporativos e públicos, surge um desafio crítico: garantir a segurança dessas redes. O padrão IEEE 802.11, amplamente utilizado em redes wi-fi, enfrenta uma variedade de ameaças cibernéticas que podem comprometer a integridade, confidencialidade e disponibilidade dos dados transmitidos. Nesse contexto, este estudo propõe uma avaliação abrangente de risco, tanto quantitativa quanto qualitativa, com o objetivo de identificar e analisar essas ameaças. O problema central reside na necessidade de estimar os danos associados a cada ameaça, visando orientar a implementação de medidas de segurança eficazes para proteger as redes wi-fi e os dados dos usuários.

Os objetivos deste trabalho incluem compreender a natureza das ameaças em redes wi-fi, calculando parâmetros associados a estas ameaças e fornecer *insights* para profissionais de segurança na tomada de decisões informadas. A abordagem metodológica empregada consiste na construção de árvores de ataque, utilizando métricas comportamentais associadas ao sistema. Foram consideradas variáveis como a notabilidade, habilidade técnica, custo e impacto das ameaças, baseadas no nível de exposição dos sistemas alvo. Os resultados obtidos fornecem uma visão detalhada do risco associado às ameaças em redes wi-fi, permitindo uma compreensão mais profunda dos desafios de segurança enfrentados por organizações e usuários individuais.

Palavras-chave: Avaliação de Risco, Redes wi-fi, IEEE 802.11, Modelagem de ameaças, Segurança de redes, Árvores de ataque, Negação de serviço, Eavesdrop, EvilTwin

Abstract

With the advancement of technology and the increasing integration of wi-fi networks in various aspects of modern life, from domestic to corporate and public environments, a critical challenge has arisen: guaranteeing the security of these networks. The IEEE 802.11 standard, widely used in wi-fi networks, faces a variety of cyber threats that can compromise the integrity, confidentiality and availability of transmitted data. In this context, this study proposes a comprehensive risk assessment, both quantitative and qualitative, with the aim of identifying and analyzing these threats. The central problem lies in the need to estimate the damage associated with each threat, in order to guide the implementation of effective security measures to protect Wi-Fi networks and user data.

The objectives of this work include understanding the nature of threats in Wi-Fi networks, calculating parameters associated with these threats and providing *insights* for security professionals to make informed decisions. The methodological approach employed consists of constructing attack trees using behavioral metrics associated with the system. Variables such as notability, technical skill, cost and impact of the threats were considered, based on the level of exposure of the target systems. The results obtained provide a detailed view of the risk associated with threats in Wi-Fi networks, allowing for a deeper understanding of the security challenges faced by these systems.

Key-words: Risk assessment, wi-fi networks, IEEE 802.11, Threat modeling, Attack trees, Network security, Denial of service, Eavesdrop, EvilTwin

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ARPANET	Advanced Research Projects Agency Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IP	Internet Protocol address
ICMP	Internet Control Message Protocol
GPS	Global Positioning System
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
WI-FI	Wireless Fi-delity
PAN	Personal Area Network
LAN	Local Area Network
MAN	Main Area Network
WAN	Wide Area Network
LTE	Long Term Evolution
SGSI	Sistema de Gerenciamento da Segurança da Informação
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OSI	Modelo de interconexão de sistemas abertos
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
MSDU	MAC Service Data Unit
MIMO	Multiple-input multiple-output
AP	Access Point
OFDM	Orthogonal Frequency Division Multiplexing
DSSS	Direct Sequence Spread Spectrum
ISM	Industrial, Scientific e Medical
GSM	Sistema Global para Comunicações Móveis
MAC	Controle de Acesso ao Meio
MTU	Maximum Transmission Unit

Conteúdo

1

Introdução

1.1 Contextualização e Motivação

Embora o tema das redes de computadores possa inicialmente parecer restrito a profissionais especializados, atualmente, essas redes permeiam quase todos os aspectos de nossa vida cotidiana. Desde a navegação na Internet, transações financeiras eletrônicas, compras online, redes sociais, o uso constante do GPS e muitos outros (Mendes, 2016). As redes de computadores desempenham um papel essencial e ubíquo em nossas atividades diárias.

Mendes (2016) afirma ainda que ao longo da evolução histórica, as redes de computadores foram inicialmente concebidas para otimizar as comunicações em ambientes militares e centros de pesquisa acadêmica que ficou conhecida posteriormente como ARPANET. Ela tinha como objetivo original permitir que os fornecedores do governo do Estados Unidos compartilhassem caros e escassos recursos computacionais, como o compartilhamento de arquivos e programas e troca de mensagens via Email. Dessa forma, à medida que pesquisas avançaram, foram desenvolvidos protocolos de comunicação que ficaram conhecidos como o modelo de referência TCP/IP e assim viabilizando a troca de dados entre redes distintas, independentemente de seus fabricantes. Esse progresso extrapolou as aplicações originais, estendendo o alcance e a utilidade das redes para diversos propósitos.

Wrightson (2014) destaca que com a expansão e difusão da Internet em escala global, surgiu a necessidade de uma rede que ultrapassasse as limitações físicas, permitindo que as pessoas se conectassem sem depender de cabos, fitas ou outros suportes. Dessa demanda, emergiu a comunicação sem fio, mais conhecida como *Wireless Fidelity* - wi-fi que da mesma forma que a rede cabeada, também surgiram protocolos de comunicação para viabilizar sua comunicação. No entanto, a sua acessibilidade e simplicidade, tanto em ambientes residenciais quanto empresariais, resultaram em uma disseminação rápida que trouxe consigo desafios significativos de

segurança. Devido à facilidade de instalação, muitos usuários em redes sem fio negligenciam precauções adicionais, uma prática que se estende até mesmo às empresas, onde a falta de conhecimento técnico adequado por parte dos administradores sobre os padrões e protocolos de segurança para essas redes se torna evidente.

Se faz necessário que as redes sem fio se tornem mais seguras e confiáveis, sempre sendo implementas por pessoas com conhecimento técnico e com um nível alto de segurança (Giavaroto, 2013). Apenas dessa maneira ela deixará de ser um alvo fácil para pessoas mal-intencionadas. À vista disso, esse trabalho irá analisar e orientar na implementação da segurança das redes wi-fi que adotam o padrão IEEE 802.11n. Para tanto, foram identificadas as principais vulnerabilidades em redes sem fio e desenvolvido um modelo baseado em árvore de ataque para representar as principais ameaças à segurança nesse contexto.

1.2 Relevância

O uso crescente de redes wi-fi (IEEE 802.11) em ambientes corporativos e residenciais destaca a importância crítica da segurança nesse contexto. Atualmente, enfrentamos desafios significativos relacionados segurança em redes sem fio. Segundo a empresa norte-americana NETCOUT, o Brasil é líder pelo 10ª ano consecutivo em ataques DDOS, desses ataques, 33.846 mil são relacionados a telecomunicação sem fio (Jorge Marin, TecMundo, 2023). Este trabalho busca em auxiliar no preenchimento dessa lacuna, oferecendo uma avaliação de risco quantitativa modelada com árvores de ataque. A relevância prática desse estudo reside na capacidade de fornecer *insights*[1] valiosos para profissionais de segurança, permitindo a quantificação de vulnerabilidades e classificação delas para que dessa forma, seja possível implementar medidas de proteção adequadas levando em consideração o ambiente do usuário. Além disso, contribui para o corpo teórico da segurança em redes wi-fi, apresentando uma abordagem não convencional para estimar o impacto de ameaças específicas. Com a ubiquidade das redes sem fio, os resultados deste estudo são de interesse direto para profissionais, pesquisadores e estudantes envolvidos na área de segurança da informação.

1.3 Objetivos

Este trabalho tem como objetivo realizar uma avaliação de risco quantitativo e qualitativo em redes wi-fi que utilizam o padrão IEEE 802.11n. A abordagem adotada baseia-se na modelagem de árvores de ataque, visando estimar o impacto de ameaças em ambientes determinados.

[1] Insight, nada mais é que a compreensão de uma causa e efeito específicos dentro de um contexto específico.

Pretende-se orientar a implementação eficaz de medidas de proteção, considerando as vulnerabilidades mais críticas e relevantes no ambiente em questão.

1.3.1 Objetivos específicos

Este trabalho possui os seguintes objetivos específicos:

- Identificar as vulnerabilidades comuns em redes sem fio.
- Desenvolver um modelo de árvore de ataque para representar as principais ameaças à segurança em redes 802.11n.
- Obter o grau de risco, viabilidade, custo, probabilidade de ocorrência e impacto que tais ataques podem acarretar em sistemas vulneráveis.
- Recomendar o aprimoramento da segurança em redes sem fio com base nos resultados obtidos.

1.4 Estrutura do Trabalho

Nesta seção será apresentada a organização desta monografia. Após este capítulo de introdução, o trabalho está estruturado em mais 5 capítulos.

No segundo capítulo é abordado o referencial teórico que fundamentará a motivação desta monografia, apresentando os principais conceitos da área e a importância da aplicação de segurança nas redes wi-fi, além de dar uma visão básica de como funciona a comunicação entre os diversos protocolos de rede IEEE 802.11.

No terceiro capítulo é destacado os trabalhos relacionados na área. Busca-se contextualizar o atual trabalho em relação ao conhecimento existente, identificando lacunas, tendências e abordagens adotadas por outros pesquisadores.

No quarto capítulo é apresentada a metodologia do trabalho desenvolvido.

No quinto capítulo é feito uma breve discussão a cerca dos resultados obtidos e relevância do mesmo.

Por fim, no sexto capítulo é apresentado as considerações finais, limitações e trabalhos futuros, dessa forma concluindo esse trabalho.

2

Fundamentação Teórica

A fim de ter uma melhor compreensão do tema apresentado, este capítulo dispõe dos referenciais teóricos obtidos através de uma revisão bibliográfica dos conceitos e técnicas existentes no estado da arte.

2.1 Redes de Computadores

Nas duas primeiras décadas de sua existência, os sistemas computacionais eram predominantemente centralizados, frequentemente instalados em salas espaçosas, muitas vezes com paredes de vidro, permitindo aos visitantes observar admirados aquele imponente "cérebro eletrônico", afirma Tenenbaum (2021). O conceito tradicional de um centro de computação, onde os usuários levavam seus trabalhos para processamento, tornou-se obsoleto diz Tenenbaum (2021). Agora, os centros de dados, com uma grande quantidade de servidores de Internet, são comuns. O antigo modelo de um único computador atendendo todas as necessidades da organização foi substituído por uma rede de computadores interconectados, onde o processamento é distribuído entre vários sistemas.

2.1.1 Características das redes

De acordo com Tenenbaum (2021) para entendermos como os dispositivos em uma rede se comunicam entre si, se faz necessário entender quais são os elementos das redes de computadores e sua importância. Tenenbaum (2021) destaca dois elementos fundamentais que formam a arquitetura dessas redes, as camadas e protocolos.

Protocolos de rede

De acordo com Tenenbaum (2021), um protocolo é um conjunto de diretrizes que regulamenta tanto o formato quanto o conteúdo dos pacotes ou mensagens trocados entre entidades em uma

camada específica da rede. Essas entidades utilizam os protocolos para efetivar as definições de serviço estabelecidas.

Os protocolos de rede compartilham um conjunto comum de objetivos que visam garantir o bom funcionamento e a eficiência das comunicações em uma rede, afirma Tenenbaum (2021). Um desses objetivos é a confiabilidade, que se refere à capacidade da rede de se recuperar de erros, defeitos ou falhas, garantindo assim a continuidade das operações mesmo em situações adversas. Tenenbaum (2021) destaca que outro objetivo importante é a alocação de recursos, que envolve o compartilhamento equitativo e eficiente de recursos como largura de banda e tempo de processamento entre os diversos usuários e dispositivos conectados à rede. Além disso, segundo Tenenbaum (2021), os protocolos de rede devem ser projetados com capacidade de evolução, permitindo a implantação incremental de melhorias ao longo do tempo para acompanhar o avanço da tecnologia e as mudanças nas necessidades dos usuários. Tenenbaum (2021) diz ainda que segurança é um aspecto fundamental, visando proteger a rede contra diferentes tipos de ataques, como acesso não autorizado e interceptação de dados, por meio da implementação de mecanismos de autenticação, criptografia e detecção de intrusões. Esses objetivos em conjunto garantem o funcionamento eficaz e seguro das redes de computadores.

Camadas dos Protocolos

Segundo Tenenbaum (2021), a maioria das redes é organizada como uma pilha de camadas sobrepostas, onde cada camada possui um número, nome, conteúdo e função variáveis, podendo diferir de uma rede para outra. Apesar das variações, o principal objetivo de cada camada é fornecer serviços específicos para as camadas superiores, desvinculando-as dos detalhes técnicos de implementação dos serviços oferecidos. Dessa forma, um serviço consiste em um conjunto de operações que uma camada oferece à camada situada acima dela, definindo as operações que a camada está apta a realizar em nome de seus usuários, mas sem especificar a forma como essas operações são executadas afirma Tenenbaum (2021). Esse serviço estabelece uma interface entre duas camadas, com a camada inferior atuando como fornecedora do serviço e a camada superior como usuária do serviço.

2.1.2 Modelos de referência

Segundo Tenenbaum (2021) o projeto de protocolo em camadas é uma das abstrações-chave no desenvolvimento de redes. É essencial definir a funcionalidade de cada camada e as interações entre elas. Dois modelos predominantes nesse contexto são o modelo de referência TCP/IP e o modelo de referência OSI, conforme ressaltado por Tenenbaum (2021). Estes modelos oferecem estruturas bem definidas para organizar as camadas e facilitar o entendimento das comunicações em rede.

Modelo de referência OSI

O modelo de referência OSI *(Open Systems Interconnection)*, segundo Tenenbaum (2021) trata de um modelo que irá se preocupar com a interconexão de sistemas abertos, ou seja, sistemas abertos à comunicação com outros sistemas, tendo sete camadas como principal característica. Veja a Figura 2.1 para mais detalhes.

Tenenbaum (2021) diz ainda que o modelo OSI tem três conceitos fundamentais:

- Serviços: Refere-se às funcionalidades fornecidas por uma camada para a camada imediatamente superior, sem abordar os detalhes sobre como as entidades superiores a acessam ou como ela é implementada.
- Interfaces: São os pontos de conexão entre as camadas adjacentes do modelo OSI. As interfaces definem como as camadas se comunicam entre si, estabelecendo os padrões e protocolos para a troca de dados e controle
- Protocolos: São conjuntos de regras e convenções que governam a comunicação entre entidades em uma mesma camada. Os protocolos especificam o formato e o significado dos pacotes de dados trocados, garantindo a interoperabilidade entre os sistemas.

Uma das principais contribuições do modelo OSI é a clara distinção entre esses três conceitos, afirma Tenenbaum (2021).

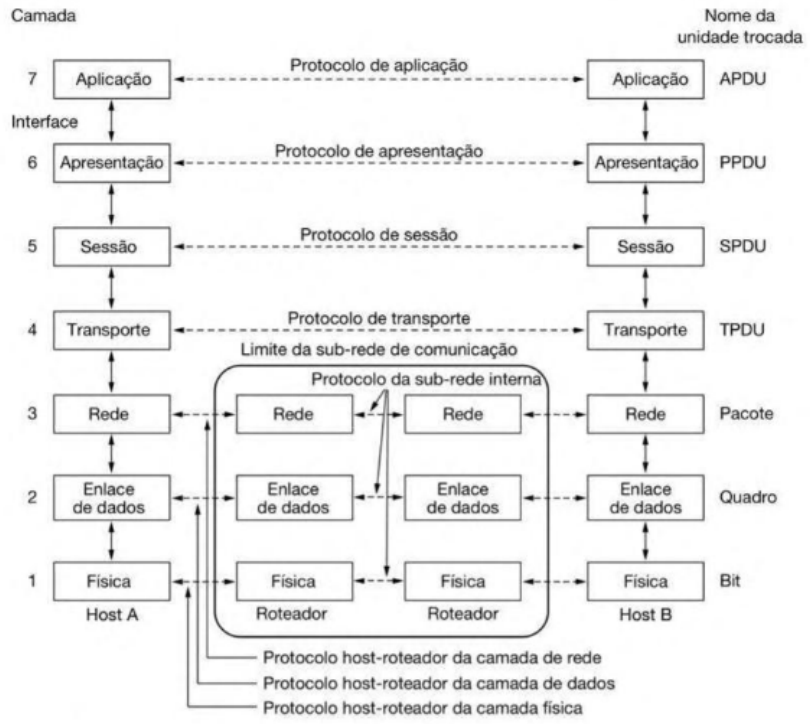

Figura 2.1: Modelo de referência OSI
Fonte: Tenenbaum (2021)

Modelo de referência TCP/IP

Tenenbaum (2021) destaca que o modelo TCP/IP foi o primeiro modelo criado e utilizado pela ARPANET, uma das pioneiras redes de computadores descentralizadas. Tenenbaum (2021) diz ainda que gradualmente, centenas de universidades públicas e repartições foram conectadas à ARPANET, inicialmente utilizando linhas telefônicas dedicadas. No entanto, com o advento das redes de rádio e satélite, surgiram problemas de interoperabilidade entre os protocolos existentes e essas novas tecnologias, o que levou à necessidade de uma nova arquitetura de referência. De acordo com Tenenbaum (2021), desde o início a capacidade de interconectar várias redes de forma homogênea foi um dos principais objetivos do projeto. Essa arquitetura ficou conhecida como modelo de referência TCP/IP, devido aos seus dois principais protocolos.

Tenenbaum (2021) destaca também que o modelo TCP/IP consiste em uma pilha de protocolos organizados em quatro camadas distintas, cada uma com suas funções específicas, diferentemente do modelo OSI que possui sete camadas. Veja a Figura 2.2.

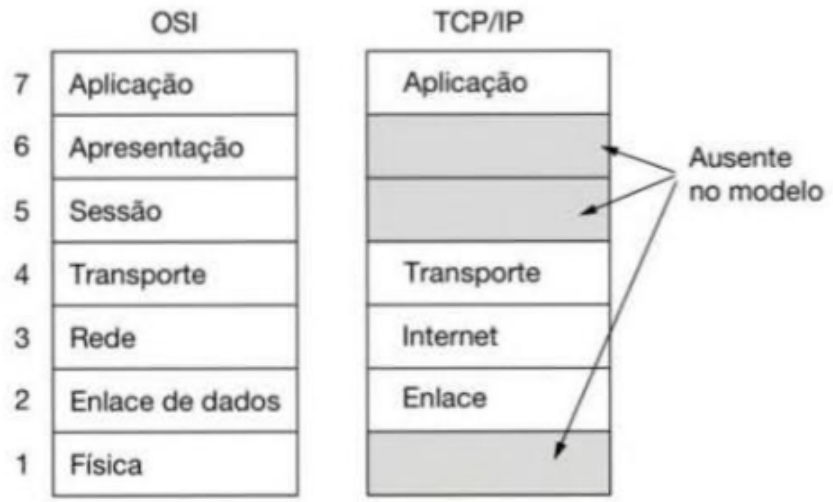

Figura 2.2: Modelo de referência TCP/IP
Fonte: Tenenbaum (2021)

2.1.3 Tipos de redes de computadores

As redes de computadores podem ter diferentes categorias em que podem ser classificadas com base em sua abrangência geográfica, finalidade e topologia afirma Tenenbaum (2021). Essas categorias incluem as Redes Pessoais (PAN), Redes Locais (LAN), Redes Metropolitanas (MAN) e as Redes de Longa Distância (WAN).

Redes Pessoais (PAN)

Por definição, as redes pessoais, ou PANs *(Personal Area Networks)*, permitem que dispositivos comuniquem-se dentro do alcance de uma pessoa, afirma Tenenbaum (2021).

A maioria dos computadores possui monitor, teclado, mouse e impressora conectados. Sem o uso de tecnologia sem fio, essa conexão é feita com cabos. No entanto, Tenenbaum (2021) diz que algumas empresas colaboraram para desenvolver uma rede sem fio de curto alcance chamada *Bluetooth*, a fim de conectar esses componentes sem necessidade de fios.

De forma simplificada, segundo Tenenbaum (2021) as redes *Bluetooth* seguem o paradigma mestre-escravo, ou seja, o dispositivo principal, geralmente o computador, atua como mestre, comunicando-se com dispositivos como mouse e teclado, que desempenham o papel de escravos. O mestre controla aspectos como endereços a serem usados, tempos de transmissão, frequências disponíveis, entre outros.

Redes locais (LAN)

Uma rede local, também conhecida como LAN *(Local Area Network)*, é uma infraestrutura de rede privada que opera dentro e nas proximidades de um único edifício, como uma residência, um escritório ou uma fábrica, destaca Tenenbaum (2021). Elas são amplamente utilizadas para interconectar computadores pessoais e dispositivos eletrônicos, permitindo que compartilhem recursos, como impressoras, armazenamento de arquivos e acesso à Internet, além de facilitar a troca de informações entre os dispositivos conectados. Tenenbaum (2021) afirma também que as LANs são caracterizadas por alta velocidade de comunicação e baixo custo de implantação, o que as torna uma solução ideal para ambientes locais onde a colaboração e o compartilhamento de recursos são essenciais para a eficiência operacional.

Tenenbaum (2021) ressalta também que as LANs sem fio estão em alta demanda nos dias de hoje, tornando-se especialmente populares em residências e em prédios de escritórios mais antigos, bem como em outros locais onde a instalação de cabos é complexa. Nesses sistemas, cada computador é equipado com um rádio modem e uma antena, que são utilizados para a comunicação com outros dispositivos. Tipicamente, cada computador estabelece conexão com um dispositivo conhecido como ponto de acesso (AP), roteador sem fio ou estação-base. Tenenbaum (2021) destaca que existe um padrão para as comunicações LANs sem fio, chamado IEEE 802.11, popularmente conhecido como wi-fi.

As LANs com fio, segundo Tenenbaum (2021) empregam uma variedade de tecnologias de transmissão para conectar dispositivos, sendo os meios físicos mais comuns o cobre, o cabo coaxial e a fibra óptica. Cada um desses modos de transmissão oferece vantagens e desvantagens específicas em termos de largura de banda, alcance e resistência a interferências. Além disso, Tenenbaum (2021) destaca também que as LANs são projetadas para serem restritas em tamanho, o que significa que o tempo necessário para a transmissão de dados, mesmo no pior cenário, é limitado e conhecido com antecedência. Isso garante uma comunicação mais eficiente e previsível dentro da rede.

Redes metropolitanas (MAN)

Uma rede metropolitana, também conhecida como MAN *(Metropolitan Area Network)*, é segundo Tenenbaum (2021) uma infraestrutura de rede que abrange uma área geográfica extensa, geralmente uma cidade ou região metropolitana. Um exemplo bem conhecido de MAN é a rede de televisão a cabo. Tenenbaum (2021) ressalta que esses sistemas evoluíram a partir de antigos sistemas de antenas comunitárias, originalmente utilizados em áreas com recepção fraca do sinal de televisão via ar. As redes metropolitanas são projetadas para fornecer conectividade de alta velocidade e confiável para uma grande quantidade de usuários dentro de uma área geográfica específica, facilitando a transmissão de dados, voz e vídeo entre diferentes locais urbanos, diz Tenenbaum (2021).

Tenenbaum (2021) destaca ainda que a televisão a cabo não é a única forma de MAN. Avanços recentes na tecnologia para acesso à Internet de alta velocidade sem fio resultaram em outra MAN, padronizada como IEEE 802.16 e popularmente conhecida como *WiMAX*. Além disso, outras tecnologias sem fio, como LTE *(Long Term Evolution)* e 5G, também têm contribuído significativamente nesse contexto.

Redes a longa distância (WAN)

As WAN *(Wide Area Network)* ou rede de longa distância, é uma infraestrutura de comunicação que se estende por uma vasta área geográfica, muitas vezes abrangendo um país ou continentes, afirma Tenenbaum (2021). As WANs desempenham um papel crucial na interconexão de organizações, permitindo a comunicação eficiente e o compartilhamento de recursos em escala global. Tenenbaum (2021), destaca também que elas podem ser implementadas como redes privadas, atendendo a uma organização específica, como no caso de uma WAN corporativa, ou como serviços comerciais oferecidos por provedores de telecomunicações, como é o caso das redes de trânsito. Ainda segundo Tenenbaum (2021), essas redes desempenham um papel fundamental na conectividade global, facilitando a comunicação entre diferentes locais geográficos e impulsionando a colaboração e o compartilhamento de informações em larga escala.

2.2 Redes sem fio

A popularidade das redes sem fio, em particular as redes wi-Fi, vem se tornando mais presente em lugares do nosso cotidiano, como conferências, aeroportos, hotéis e shoppings; De acordo com Kurose (2022), o número de assinantes de telefones móveis no mundo inteiro aumentou de 34 milhões em 1993 para quase 8,3 bilhões em 2019 e, agora, ultrapassa o número de pessoas no planeta.

Boris Bellalta (2015) afirma que as redes sem fio são uma rede de comunicação sem cabo por onde a transmissão de dados é realizada através de ondas, podendo ser dividas em vários tipos

de redes. Há algumas vantagens no uso dessas redes, ainda segundo Boris Bellalta (2015) algumas delas são a mobilidade, facilidade de implementação, flexibilidade e interoperabilidade. Segundo Kurose (2022), graças a essas vantagens mais recentemente, *smartphones*, *tablets* e *laptops* têm se conectado sem fio à internet por meio de redes celulares ou wi-fi. Além disso, cada vez mais dispositivos, como consoles de jogos, termostatos, sistemas de segurança residencial, eletrodomésticos, relógios, óculos inteligentes, carros, sistemas de controle de tráfego e outros, estão sendo conectados sem fio à internet.

2.2.1 Fundamentos das redes sem fio

Segundo de Oliveira Rufino (2019), os fatores externos causam mais problemas nas redes sem fio do que nas redes convencionais. Isso acontece porque não há proteção para o ambiente onde as informações são transmitidas. Contudo, de Oliveira Rufino (2019) destaca que apesar das redes sem fio não possuírem proteção física, elas têm a vantagem de poder alcançar áreas de difícil acesso para redes com fio com facilidade.

Tenenbaum (2021) faz uma análise sobre os tipos de redes para usuários móveis e redes sem fio, destacando sua interação com as redes maiores, geralmente com conexões cabeadas. É importante destacar que, conforme mencionado por Tenenbaum (2021), existem ambientes de rede em que os dispositivos estão conectados sem fio, mas não estão em constante movimento, como é o caso das redes residenciais sem fio ou redes de escritórios com computadores fixos. Além disso, há formas limitadas de mobilidade que não envolvem conexões sem fio, como quando alguém utiliza um notebook em casa, desliga-o e o leva para o escritório, onde o conecta à rede por meio de cabos. Para esses casos, Tenenbaum (2021) as classificou como computação móvel.

Dessa forma, vale ressaltar que segundo Tenenbaum (2021), embora as redes sem fio e a computação móvel sejam frequentemente mencionadas juntas, elas não são a mesma coisa. É importante entender a diferença entre as redes sem fio que são fixas e as que são móveis. Veja a Tabela 2.1 para mais informações.

Sem Fio	**Móvel**	**Aplicações típicas**
Não	Não	Computadores desktop em escritórios
Não	Sim	Um notebook usado em um quarto de hotel
Sim	Não	Redes em edifícios que não dispõem de fiação
Sim	Sim	Assistente de registro de estoque em uma loja

Tabela 2.1: Aplicações das Redes móveis e Sem fio
Fonte: Tenenbaum (2021)

2.2.2 Elementos das redes sem fio

Tenenbaum (2021) afirma que os elementos incluem todos os dispositivos necessários para

estabelecer, manter e gerenciar a conectividade sem fio entre diferentes dispositivos ou nós na rede. Dessa forma, segundo Kurose (2022), podemos destacar os seguintes elementos que compõem as redes sem fio:

- Hospedeiros sem fio: Equipamentos de sistemas finais que executam aplicações. Esse hospedeiro pode ser um notebook, smartfone ou computador de mesa, podendo ser móveis ou não, afirma Kurose (2022).
- Estação-base: Kurose (2022) destaca que as estações-bases serão responsáveis pelo envio e recebimento de dados de e para um hospedeiro sem fio que está associado a ela. Uma estação-base frequentemente será responsável pela coordenação da transmissão de vários hospedeiros sem fio com os quais está associada. Como por exemplo, torres celulares e pontos de acessos. Na Figura 2.3, a estação base está conectada a uma rede maior (por exemplo, a Internet, rede corporativa ou residencial), funcionando como um ponto de conexão entre o dispositivo sem fio e o resto do mundo com o qual o dispositivo se comunica.
- Links sem fio: Um hospedeiro se conecta a uma estação-base ou a outro hospedeiro sem fio por meio dos links de comunicação sem fio. Tecnologias diferentes de links sem fio têm taxas de transmissão diversas e podem transmitir a distâncias variadas, diz Kurose (2022). Na Figura 2.3, os links sem fio conectam *hosts* localizados na borda da rede à infraestrutura de rede maior. Kurose (2022) ressalta que os links sem fio também são às vezes utilizados dentro de uma rede para conectar roteadores, *switches* e outros equipamentos de rede.
- Infraestrutura de rede: Segundo Kurose (2022), esta é a rede maior com a qual um dispositivo sem fio pode desejar se comunicar.

Ver a Figura 2.3 para visualizar os elementos supracitados.

2.2.3 Elementos dos protocolos das redes sem fio

Segundo de Oliveira Rufino (2019) os principais elementos que compõem os protocolos das redes sem fio são:

- Frequências: de Oliveira Rufino (2019) define que as frequências serão sinais de radio frequência utilizados pelos mais variados tipos de serviços, que vão desde as infraestruturas comerciais até as de uso militar ou de rádio amador. Ele destaca ainda que quando falamos de frequência de rádio, devemos ter em mente que será propagado no espaço por algum centímetros ou por vários quilômetros, sendo a distância percorrida diretamente ligada às frequências do sinal. Desse modo, de Oliveira Rufino (2019) ressalta que quanto mais alta a frequência, menor será a distância alcançada.

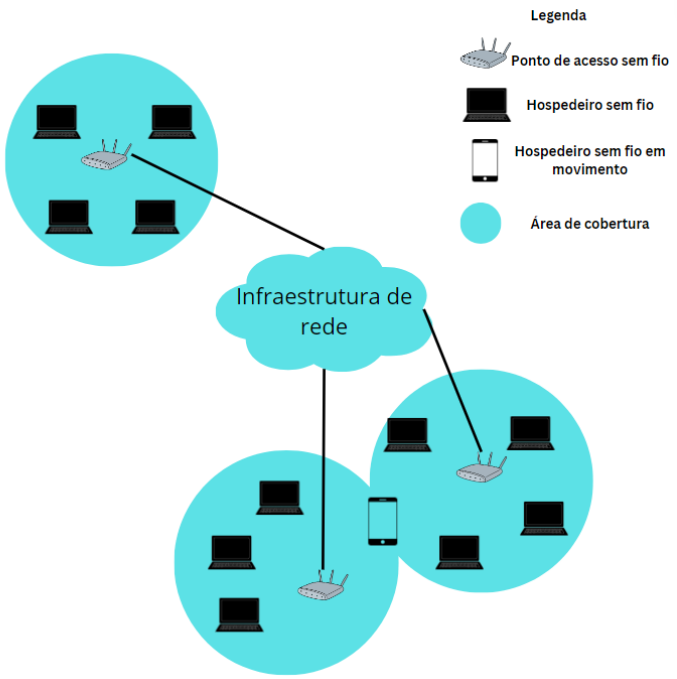

Figura 2.3: Elementos de uma rede sem fio
Fonte: Elaborada pelo Autor

- Canais: de Oliveira Rufino (2019) afirma que para definir canais precisamos entender que espectro de radiofrequência é organizado em faixas designadas para diferentes tipos de serviços, de acordo com padrões internacionais e regulamentações governamentais. Cada faixa é subdividida em canais, que são frequências menores permitindo a transmissão simultânea de sinais distintos.

- Spread Spectrum: De acordo com de Oliveira Rufino (2019) foi inicialmente criada para uso militar e tem a função de distribuir o sinal de maneira uniforme em toda a faixa de frequência. Mesmo que consuma mais largura de banda, essa tecnologia oferece maior segurança para a transmissão de informações e é menos suscetível a ruídos e interferências do que outras tecnologias que utilizam frequências fixas. Em um sistema de frequência uniforme, um ruído em uma frequência específica afetará apenas a transmissão nessa frequência, não prejudicando toda a faixa. Isso significa que o sinal só precisa ser retransmitido quando necessário. No entanto, como o sinal ocupa toda a faixa, pode ser facilmente detectado. Se o receptor não estiver ciente do padrão de variação de frequência, qualquer sinal recebido será interpretado como ruído. Atualmente, essa é a principal forma de comunicação usada em redes sem fio, conforme destacado por de Oliveira Rufino (2019).

- Bandas de radiofrequência públicas: Segundo de Oliveira Rufino (2019), os padrões internacionais estabeleceram três faixas de frequência de rádio reservadas para uso em ati-

vidades industriais, científicas e médicas (ISM). Estas faixas podem ser utilizadas sem a necessidade de uma licença governamental. Essas faixas são: de 902 a 928 (MHz) *megahertz* ; de 2,4 a 2,485 (GHz) *gigahertz* (ou de 2,4 a 2,5 GHz no Brasil); e de 5,150 a 5,825 GHz.

- Frequências licenciadas: Algumas soluções de redes sem fio optam por faixas de radiofrequência menos sujeitas à interferência e com maior alcance. de Oliveira Rufino (2019) destaca que para utilizá-las, é necessário que o fornecedor da solução obtenha autorização da agência reguladora e, geralmente, pague uma taxa. de Oliveira Rufino (2019) trás alguns exemplos como o padrão 802.16a (WiMax) que usa a faixa de 2 a 11 GHz, alcançando até 50 km a velocidades de 10 a 70 Mb e os provedores de serviço de telefonia móvel no padrão GSM que usam a faixa de 1,8 GHz no Brasil, enquanto em países como Canadá, México e Estados Unidos, a faixa é de 1,9 GHz.

2.2.4 Padrão IEEE 802.11

Kurose (2022), destaca que embora muitas tecnologias e padrões para redes locais sem fio tenham sido desenvolvidos na década de 1990, uma classe específica de padrões claramente se destacou como a vencedora: o IEEE 802.11 wireless LAN, também conhecido como wi-fi.

De acordo com a atualização de 2020, conforme destacado por Kurose (2022), existem vários padrões 802.11. Os padrões 802.11 b, g, n, ac e ax representam gerações sucessivas da tecnologia 802.11, projetadas para redes locais sem fio (WLANs), comumente cobrindo distâncias de até 70 metros em ambientes domésticos, de escritório ou empresariais. Além disso, conforme mencionado por Kurose (2022), os padrões 802.11 n, ac e ax foram recentemente designados como *wi-fi* 4, 5 e 6, respectivamente, em uma clara concorrência com as designações de redes celulares 4G e 5G. Já os padrões 802.11 af e ah foram desenvolvidos para operar em distâncias maiores e são direcionados para aplicações relacionadas à Internet das Coisas, redes de sensores e medição.

Kurose (2022), ressalva ainda que os diferentes padrões 802.11 b, g, n, ac, ax compartilham algumas características comuns, incluindo o formato de quadro 802.11 e são retro compatíveis, o que significa, por exemplo, que um dispositivo móvel capaz apenas de 802.11 g ainda pode interagir com uma estação base mais recente de 802.11 ac ou 802.11 ax.

Os padrões 802.11n, 802.11ac e 802.11ax, conforme ressaltado por Kurose (2022), utilizam antenas de entrada múltipla e saída múltipla (MIMO), ou seja, duas ou mais antenas no lado de envio e duas ou mais antenas no lado de recepção que estão transmitindo/recebendo sinais diferentes. Kurose (2022) afirma também que as estações base 802.11ac e 802.11 ax podem transmitir para várias estações simultaneamente e utilizam antenas inteligentes para adaptativamente realizar *beamforming* que nada mais é que uma técnica que envolve o direcionamento intencional de sinais de rádio em uma direção específica, ao invés de irradiá-los em todas as

direções igualmente. Isso reduz a interferência e aumenta a distância alcançada a uma determinada taxa de dados.

Kurose (2022), afirma que esses dispositivos podem operar em duas faixas de frequência distintas: 2,4–2,485 GHz (conhecida como faixa de 2,4 GHz) e 5,1–5,8 GHz (conhecida como faixa de 5 GHz).

Tabela 2.2 trás uma comparação entre o histórico de padrões 802.11.

Padrão	**Velocidade**	**Frequência**	**Distância**	**Ano**
802.11b	5.5 Mbp/s e 11 Mbps	2.4GHz	30 m	1999
802.11g	Até 54Mbp/s	2.4GHz	30 m	2003
802.11n	Até 450Mbps/s	2.4GHz e 5GHz	70 m	2009
802.11ac	Até 6,93 Gb/s	5GHz	70 m	2013
802.11ax	Até 9,6 Gb/s	2.4Ghz e 5GHz	70 m	2020
802.11af	Até 560Mbps/s	Até 790 MHz (TV)	1 km	2014
802.11ah	Até 347Mbps/s	900 MHz	1 km	2017

Tabela 2.2: Comparação dos padrões 802.11
Fonte: Kurose (2022)

2.2.5 Tipos de redes IEEE 802.11

de Oliveira Rufino (2019), destaca que em termos organizacionais, o padrão IEEE 802.11 define dois modos distintos de operação: *Ad-Hoc* e infraestrutura.

Ad-Hoc

As redes *Ad-hoc* representam uma categoria de redes sem fio que se distinguem pela ausência da necessidade de um ponto de acesso central para a comunicação entre dispositivos conectados, destaca de Oliveira Rufino (2019). Em vez disso, todos os dispositivos na rede assumem a função de roteadores, encaminhando informações diretamente entre si. Conforme ressaltado ainda por de Oliveira Rufino (2019), esse modo de operação torna-se particularmente relevante em cenários nos quais a presença de um ponto de acesso convencional não está disponível.Essa abordagem *ad-hoc* oferece uma solução flexível para situações específicas, como a necessidade de estabelecer uma comunicação temporária para a troca de arquivos ou a realização de uma comunicação rápida em ambientes dinâmicos. Ao dispensar a dependência de uma infraestrutura centralizada, as redes *ad-hoc* demonstram sua utilidade em contextos nos quais a mobilidade e a flexibilidade são prioritárias. Ver a Figura 2.4.

Infraestrutura

de Oliveira Rufino (2019) afirma que as redes de infraestruturas diferente das *Ad-hoc*, irão precisar de um equipamento central de rede que irá ser utilizado para rotear as informações

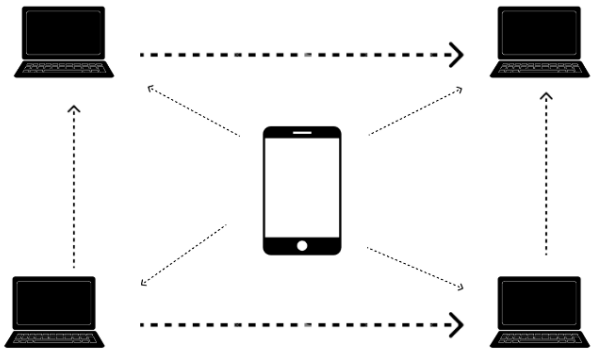

Figura 2.4: Topologia Redes Ad-Hoc
Fonte: Elaborada pelo Autor

da rede. de Oliveira Rufino (2019) ressalta que o ponto de acesso único será compartilhado por vários clientes, resultando na centralização de todas as configurações de segurança em um único ponto.. Dessa forma, torna-se possível controlar todos os recursos de segurança como autorização, controle de banda, filtro de pacotes e vários outros em um único ponto centralizado. Normalmente nesse tipo de abordagem as estações irão precisar de menos esforço para cobrir uma mesma área. Ver a Figura 2.5

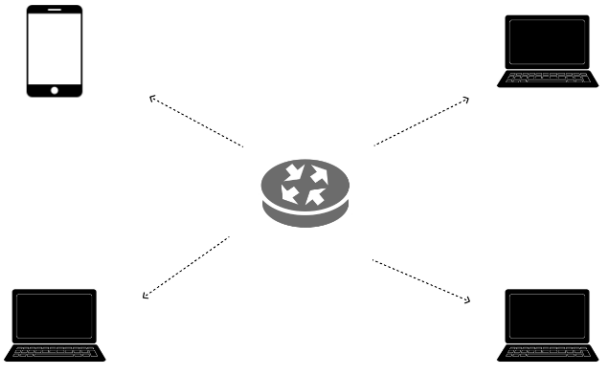

Figura 2.5: Topologia Redes Infraestrutura
Fonte: Elaborada pelo Autor

2.2.6 Principais características das redes IEEE 802.11

Conforme observado por de Oliveira Rufino (2019), alguns conceitos são exclusivos das redes sem fio, enquanto outros foram adaptadas das redes cabeadas convencionais, já que esses padrões fundamentaram o modelo *Wi-Fi*. No entanto, a maioria desses conceitos são específicas para redes sem fio, devido às suas características distintas, particularmente nas camadas mais próximas do hardware, isto é, nas camadas 2 e 3 do modelo OSI, em comparação com as redes convencionais.

Canais e associações nas redes IEEE 802.11

De acordo com Kurose (2022), no padrão 802.11 é necessário que cada estação sem fio se associe a um Ponto de Acesso (AP) antes de poder enviar ou receber dados na camada de rede. Esse processo de associação é essencial para estabelecer uma conexão efetiva entre os dispositivos sem fio e a rede. Além disso, ao instalar um Ponto de Acesso (AP), o administrador de rede deve atribuir um Identificador de Conjunto de Serviço (SSID), que é uma identificação única da rede sem fio, composta por uma ou duas palavras significativas para os usuários. Segundo Kurose (2022), essa identificação facilita que os dispositivos sem fio reconheçam e se conectem à rede desejada. Adicionalmente, o administrador também precisa atribuir um número de canal ao AP, que determina a frequência de operação da rede sem fio. A escolha adequada do canal é importante para evitar interferências e garantir uma comunicação eficiente entre os dispositivos conectados ao AP.

Em concordância com Kurose (2022), vale destacar também o conceito de *Wi-fi Jungle* ou "selva Wi-Fi". Se trata de um termo utilizado para descrever uma situação em que uma estação sem fio, como um dispositivo móvel ou computador, recebe sinais de dois ou mais Pontos de Acesso (APs) em uma mesma área física. Essa situação é comumente observada em ambientes urbanos densamente povoados, como cafés, áreas comerciais ou residenciais, ressalta Kurose (2022). Por exemplo, em um café em uma cidade bem populada, um dispositivo móvel pode detectar o sinal não apenas do Ponto de Acesso fornecido pelo próprio café, mas também de APs localizados em apartamentos ou estabelecimentos próximos. Cada um desses APs geralmente está configurado em uma rede *Wi-Fi* independente, com seu próprio Identificador de Conjunto de Serviço (SSID) e canal de comunicação. A presença de múltiplos APs em uma mesma área cria um *Wi-fi Jungle* , onde as estações sem fio podem enfrentar desafios relacionados à interferência de sinais, à qualidade da conexão e à segurança da rede. A compreensão desse fenômeno é fundamental para o planejamento e a implementação de redes sem fio mais eficientes e confiáveis em ambientes urbanos.

De acordo com Kurose (2022), para o acesso à Internet por meio de dispositivos sem fio a associação desses dispositivos a um Ponto de Acesso (AP) específico é crucial. Esta associação é necessária porque cada dispositivo sem fio precisa estar conectado a uma sub-rede para acessar a Internet. Ao se associar a um AP, o dispositivo sem fio estabelece uma conexão virtual com ele, garantindo assim a comunicação eficiente com a rede. Como resultado, apenas o AP ao qual o dispositivo está associado enviará e receberá dados para ele, e todo o tráfego de dados do dispositivo para a Internet passará por esse AP específico. Segundo, Kurose (2022) essa configuração permite uma transmissão segura e confiável de dados entre o dispositivo sem fio e a rede, assegurando uma conexão estável e sem interrupções para o usuário.

Contudo, para que essa associação aconteça, o padrão IEEE 802.11 requer que o AP mande periodicamente *beacon frames*[1] que contenham o SSID e o endereço MAC do AP, afirma Ku-

[1]Responsável por transmitir informações sobre a rede, sendo emitida periodicamente pelos pontos de acesso.

rose (2022). O seu dispositivo sem fio, ciente de que os APs estão enviando quadros de *beacon*, faz uma varredura nos canais, buscando quadros de *beacon* de quaisquer APs que possam estar disponíveis. Kurose (2022) destaca que normalmente, o dispositivo escolhe o AP cujo quadro de beacon é recebido com a maior intensidade de sinal.

Escaneamento passivo e ativo

De acordo com Kurose (2022) o processo de escanear canais e ouvir quadros de *beacon* é conhecido como escaneamento passivo, veja a Figura 2.6. Um dispositivo sem fio também pode realizar escaneamento ativo, afirma Kurose (2022), transmitindo um quadro de sondagem que será recebido por todos os APs dentro do alcance do dispositivo sem fio, como mostrado na Figura 2.7. Os APs respondem ao quadro de solicitação de sondagem com um quadro de resposta de sondagem e a partir dai o dispositivo sem fio então pode escolher o AP com o qual se associar entre os APs que responderam.

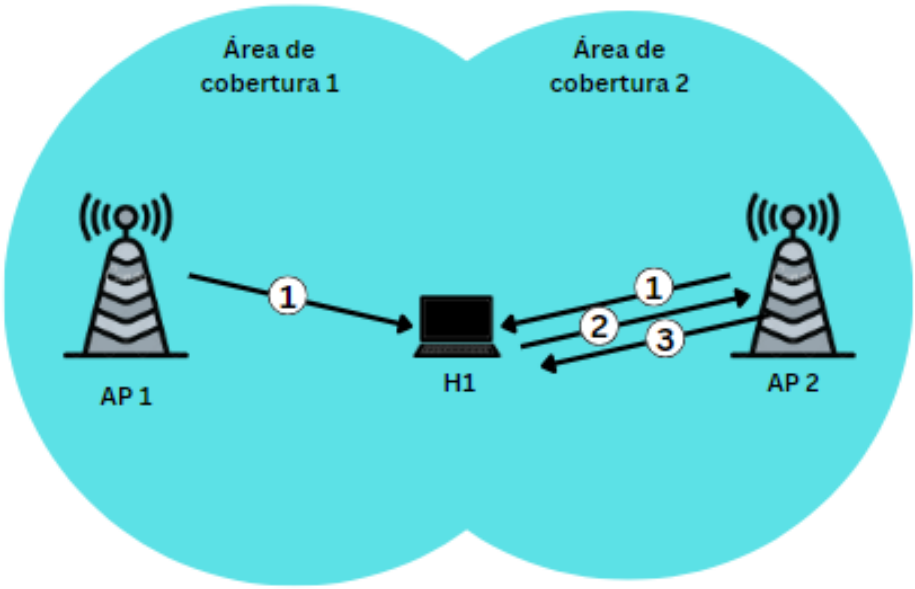

Figura 2.6: Estrutura do Escanemaneto Passivo
Fonte: Kurose (2022)

Autenticação nas redes IEEE 802.11

Para estabelecer uma conexão com um Ponto de Acesso (AP) específico e se associar adequadamente, um dispositivo sem fio pode precisar se autenticar perante o AP, afirma Kurose (2022). As *LANs* sem fio IEEE 802.11 oferecem diversas opções para autenticação e acesso. Kurose

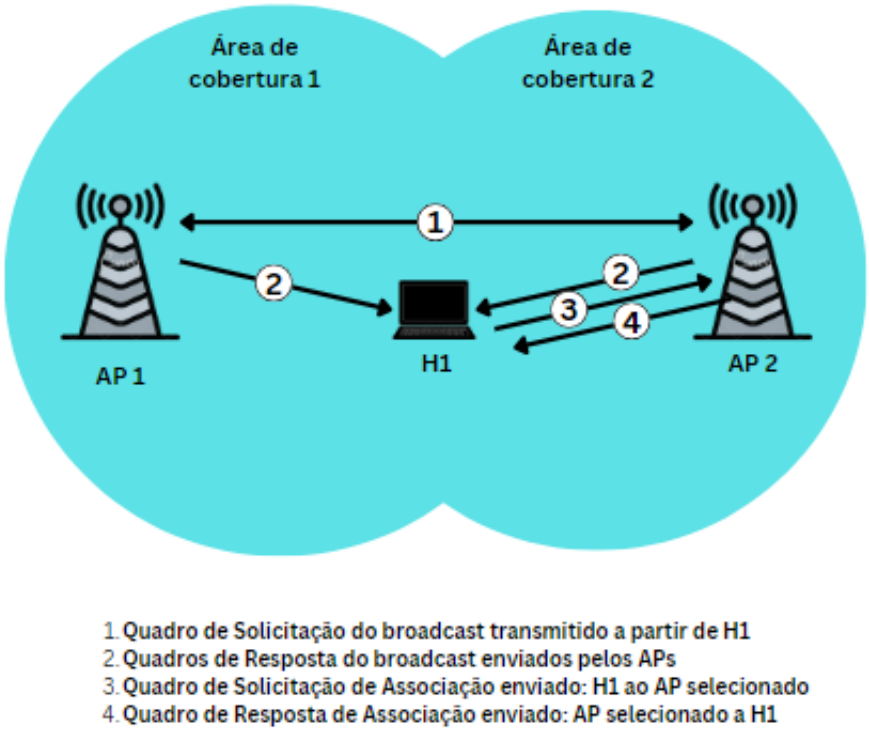

Figura 2.7: Estrutura do Escanemaneto Ativo
Fonte: Kurose (2022)

(2022) ressalta que uma estratégia comum, adotada por muitas empresas, é permitir o acesso à rede sem fio com base no endereço MAC do dispositivo. Outra abordagem, frequentemente encontrada em cafeterias e espaços públicos, envolve o uso de nomes de usuário e senhas. Em ambos os casos, o AP geralmente estabelece comunicação com um servidor de autenticação, facilitando a troca de informações entre o dispositivo sem fio e o servidor de autenticação através de protocolos, destaca Kurose (2022). Essa separação entre o AP e o servidor de autenticação permite que um único servidor atenda a múltiplos APs, garantindo uma gestão mais eficiente e centralizada.

Segundo Tenenbaum (2021), as redes 802.11 podem ser configuradas como abertas, permitindo que qualquer usuário as utilize. No entanto, ele ressalta que, quando a autenticação é habilitada, existem diversos padrões de segurança disponíveis para autenticar essas redes 802.11. Esses padrões incluem o WEP *(Wired Equivalent Privacy)*, WPA *(Wi-Fi Protected Access)*, WPA2 *(Wi-Fi Protected Access 2)* e o mais recente *WPA3 (Wi-Fi Protected Access 3)*.

1. WEP: A autenticação ocorre com uma chave previamente compartilhada antes da associação. No entanto, segundo Tenenbaum (2021) seu uso é desencorajado devido a falhas de projeto que tornam o WEP vulnerável a ataques. Tenenbaum (2021) destaca também que atualmente, existe software disponível gratuitamente para descobrir senhas WEP, o que enfatiza ainda mais a fragilidade desse protocolo de segurança.

2. WPA: Segundo Kurose (2022), o WPA surgiu em 2003 através da *wi-fi Alliance* com o objetivo de corrigir as vulnerabilidades do WEP. Esse protocolo utiliza o TKIP *(Temporal Key Integrity Protocol)* para garantir a segurança das comunicações sem fio. Comparado ao WEP, o WPA teve uma melhoria significativa ao introduzir verificações de integridade das mensagens, o que impediu ataques que permitiam a um usuário descobrir chaves de criptografia após analisar o fluxo de mensagens criptografadas por um período de tempo.

3. WPA2: Tenenbaum (2021) destaca que com o WPA2, o Ponto de Acesso (PA) pode estabelecer comunicação com um servidor de autenticação, que mantém um banco de dados de nomes de usuários e senhas, para verificar se a estação tem permissão para acessar a rede. Alternativamente, pode ser configurada uma chave previamente compartilhada, conhecida como *passphrase*, que serve como senha de rede. Além disso, Kurose (2022) ressalta que essa autenticação utiliza o protocolo de criptografia AES *(Advanced Encryption Standard)* para fornecer uma segurança mais robusta em comparação com o TKIP do WPA.

4. WPA3: Lançado em 2018, é a mais recente iteração do padrão de segurança Wi-Fi, afirma Kurose (2022). Foi desenvolvido para fornecer segurança aprimorada e proteção contra ataques de força bruta, utilizando protocolos mais avançados de criptografia e autenticação. Kurose (2022) afirma ainda que o WPA3 também introduz recursos como criptografia individualizada para cada dispositivo conectado à rede, aumentando ainda mais a segurança.

O protocolo MAC IEEE 802.11

Kurose (2022) ressalva que uma vez associada com um AP, uma estação sem fio pode começar a enviar e receber quadros de dados de e para um AP. Porém, para várias estações poderem transmitir quadros de dados ao mesmo tempo sobre o mesmo canal é necessário um protocolo de acesso múltiplo para coordenar as transmissões e esse é o principal objetivo do Controle de Acesso ao Meio (MAC). De acordo com Kurose (2022), existem três classes de protocolos de acesso múltiplo: particionamento de canal, acesso aleatório e por turnos. Ainda segundo Kurose (2022), inspirados pelo grande sucesso do Ethernet e seu protocolo de acesso aleatório, os projetistas do IEEE 802.11 escolheram um protocolo de acesso aleatório para as LANs sem fio 802.11.

Esse protocolo de acesso aleatório é chamado de CSMA, ou CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*, ressalva Kurose (2022). Como o CSMA/CD usado no Ethernet, o "CSMA"em CSMA/CA significa "acesso múltiplo com detecção de portadora", significa que cada dispositivo verifica se o canal está livre antes de enviar dados e espera se estiver ocupado. Ainda segundo Kurose (2022), mesmo que tanto o Ethernet quanto o 802.11 usem acesso aleatório com detecção de portadora, eles têm diferenças importantes. Primeiro, o

802.11 usa técnicas para evitar colisão em vez de detecção de colisão. Segundo, devido às altas taxas de erros de bits nos canais sem fio, o 802.11 (diferente do Ethernet) usa um método de retransmissão/reconhecimento (ARQ) na camada de enlace para garantir a entrega correta dos dados.

2.2.7 Desafios na segurança em redes IEEE 802.11

Segundo Kurose (2022) a segurança desempenha um papel crucial nas redes sem fio devido à vulnerabilidade a que estão sujeitas. Em tais redes, os ataques podem ser realizados por um invasor posicionando um dispositivo receptor dentro do alcance de transmissão do remetente, permitindo a interceptação de quadros de comunicação, afirma Kurose (2022). Essa capacidade de interceptação pode comprometer a integridade e a confidencialidade dos dados transmitidos, destacando a importância de estratégias robustas de segurança para mitigar essas ameaças.

Kurose (2022) destaca ainda duas preocupações críticas de segurança às quais uma rede IEEE 802.11 está sujeita.

1. Autenticação mútua: Segundo, Kurose (2022) antes que um dispositivo móvel possa se conectar completamente a um ponto de acesso e enviar datagramas para *hosts* remotos, a rede normalmente desejará autenticar primeiro o dispositivo - para verificar a identidade do dispositivo móvel que está se conectando à rede e verificar os privilégios de acesso desse dispositivo. Da mesma forma, o dispositivo móvel desejará autenticar a rede à qual está se conectando - para garantir que a rede à qual está se juntando seja realmente a rede à qual deseja se conectar. Essa autenticação bilateral é conhecida como autenticação mútua.

2. Criptografia: Dado que os quadros 802.11 serão trocados por meio de um canal sem fio que pode ser interceptado e manipulado por possíveis malfeitores, é importante criptografar os quadros de nível de link que transportam dados de nível de usuário trocados entre o dispositivo móvel e o ponto de acesso (AP), afirma Kurose (2022). Na prática, os padrões de segurança WEP, WPA, WPA2 e WPA3 são responsáveis por realizar a criptografia necessária. A depender do método escolhido, o dispositivo móvel e o AP precisarão derivar as chaves de criptografia e descriptografia simétricas a serem utilizadas.

De acordo com Tenenbaum (2021), uma parcela significativa das vulnerabilidades de segurança pode ser atribuída aos fabricantes de pontos de acesso, os quais frequentemente priorizam a facilidade de uso de seus produtos para os usuários finais. Tipicamente, ao retirar o dispositivo da embalagem e conectá-lo à tomada de energia, ele começa a operar imediatamente, quase sempre sem a implementação de medidas de segurança adequadas, expondo informações confidenciais a qualquer indivíduo dentro do alcance do sinal de rádio. Além disso, segundo Tenenbaum (2021), se o dispositivo estiver conectado a uma rede *Ethernet*, todo o tráfego dessa

rede será repentinamente visível para quem estiver nas proximidades. Tenenbaum (2021) destaca ainda a infraestrutura de rede sem fio, por sua natureza, oferece uma oportunidade única para o espionagem de dados, uma vez que permite o acesso a informações sensíveis sem exigir grande esforço. Diante disso, torna-se evidente que a segurança em sistemas sem fio é de extrema importância.

2.2.8 Ataques as redes IEEE 802.11

Os ataques em redes sem fio podem ser classificados em ataques passivos e ataques ativos afirma Thant (2019). Os ataques passivos não envolvem a alteração de recursos e representam principalmente uma ameaça à confidencialidade dos dados. Um ataque passivo ocorre quando alguém escuta ou intercepta o tráfego de rede. Ainda segundo, Thant (2019) os ataques ativos envolvem a alteração de recursos e exigem que o agressor gaste energia para executar o ataque. Alguns dos ataques em redes sem fio incluem sondagem e descoberta de rede, ataques de negação de serviço (DoS), falsificação, ataques de *man-in-the-middle*, entre outros. Thant (2019) afirma também que a maioria dos ataques é direcionada às camadas física e de enlace.
No escopo dessa pesquisa iremos ressaltar os ataques:

2.2.9 Ataques de negação de serviço

Um ataque de negação de serviço (DOS) ocorre quando qualquer recurso do sistema não está disponível para os usuários da rede, afirma Agrawal (2018). Um ataque de negação de serviço sobrecarrega o sistema remoto com tanto tráfego que ele não consegue lidar com as solicitações normais e válidas feitas por outros sistemas da rede. Agrawal (2018) destaca ainda que esses ataques não são facilmente detectáveis, pois o computador remoto não consegue distinguir facilmente entre as solicitações e o tráfego enviados pelas máquinas que realizam o ataque de negação de serviço e aqueles enviados por meios válidos. Além disso, ainda segundo Agrawal (2018), um DOS pode ocorrer devido a uma alta demanda legítima. Agrawal (2018) destaca que os ataques de negação de serviço podem ser classificados de acordo com o modelo OSI da seguinte maneira:

- Ataques de negação de serviço na camada de aplicação: Agrawal (2018) afirma que o atacante tenta explorar uma vulnerabilidade de um protocolo de aplicação, como DNS (envenenamento de cache) e HTTP (estouro de pilha e buffer). Isso é alcançado enviando grandes quantidades de solicitações legítimas para uma aplicação.

- Ataques na camada de transporte e inter-redes: Um ataque de negação de serviço na camada de transporte envolve o envio de muitas solicitações de conexão para um *host* afirma Agrawal (2018). É muito eficaz e extremamente difícil de rastrear até o atacante devido às técnicas de falsificação de IP utilizadas. Um ataque de negação de serviço na

camada de rede é alcançado pelo envio de uma grande quantidade de dados para uma rede sem fio.

- Ataques de negação de serviço na camada de acesso à mídia: Agrawal (2018) destaca que as redes sem fio são particularmente vulneráveis a ataques de nível MAC devido ao uso de um meio compartilhado. Um atacante pode transmitir pacotes usando um endereço MAC de origem falsificado de um ponto de acesso. O destinatário desses quadros falsificados não tem como saber se são solicitações legítimas ou ilegítimas e irá processá-las. Agrawal (2018) destaca dois principais ataques na camada MAC são: ataque de inundação de autenticação/associação ou ataques de inundação de desautenticação/desassociação.

- Ataques de negação de serviço na camada física: Ainda segundo Agrawal (2018), os dois principais ataques são *jamming* e interferência. Perturbar uma rede sem fio com sinais de ruído pode reduzir a taxa de transferência da rede. A interferência com outros transmissores de rádio é outra possibilidade para prejudicar o desempenho de uma rede sem fio.

Vale ressaltar que ainda segundo Agrawal (2018) um ataque de negação de serviço (DoS) é executado de um único ponto de origem, sobrecarregando um sistema alvo com solicitações maliciosas para torná-lo inacessível. Em contraste, um ataque distribuído de negação de serviço (DDoS) envolve múltiplos pontos de origem *(botnets)*[2] , coordenados para atacar simultaneamente o alvo, aumentando a eficácia e dificultando a mitigação.

2.2.10 Ataque Syn-Flood

A inundação *SYN*, ou ataque de porta entreaberta, é um tipo de ataque de negação de serviço (DoS) com a intenção de deixar um servidor ou ponto de acesso indisponível para o tráfego legítimo ao consumir todos os seus recursos disponíveis, afirma CloudFlare (2021). Ao enviar pacotes de solicitação de conexão inicial *SYN* repetidamente, o invasor consegue sobrecarregar as portas disponíveis na máquina do servidor visado, fazendo com que o dispositivo atingido responda lentamente ou pare totalmente de responder ao tráfego legítimo.

CloudFlare (2021) mostra que para realizar esse ataque, o atacante irá explorar o processo de handshake de uma conexão TCP. Que em condições normais irá ser realizada da seguinte forma:

- Primeiramente, o cliente envia um pacote *SYN* ao servidor para iniciar a conexão.

- Em seguida, o servidor responde ao pacote inicial com um pacote *SYN/ACK* para confirmar a comunicação.

[2]Rede de dispositivos comprometidos que são controlados remotamente por um atacante para realizar atividades maliciosas

- Por fim, o cliente devolve um pacote *ACK* para confirmar o recebimento do pacote do servidor. Após concluir essa sequência de envios e recebimentos de pacotes, a conexão TCP é aberta e consegue enviar e receber dados.

Para deixar o serviço indisponível, CloudFlare (2021) ressalva que o invasor se aproveita do fato de que, após ter recebido o pacote inicial *SYN*, o servidor irá responder com um ou mais pacotes *SYN/ACK* e esperar a etapa final do *handshake*. Ele irá enviar um grande volume de pacotes *SYN* no servidor alvo, muitas vezes esse envio terá endereços de *IPs* falsificados. Após isso, o servidor responderá a cada solicitação de conexão, mantendo uma porta aberta temporariamente em antecipação a uma resposta que nunca chegará. Com cada novo pacote *SYN* enviado, uma nova conexão de porta é temporariamente estabelecida pelo servidor por um período definido. Após o esgotamento de todas as portas disponíveis, o servidor ficará incapaz de operar normalmente. Veja a Figura 2.8 para mais detalhes.

CloudFlare (2021) ressalva que existe a possibilidade desse ataque ser criado com o uso de botnets. A probabilidade de rastrear o ataque até sua origem é pequena quando esse modo de ataque é feito, diz CloudFlare (2021). Para obter um nível extra de dissimulação, o invasor também pode fazer com que cada dispositivo distribuído falsifique os endereços *IP* dos quais envia pacotes.

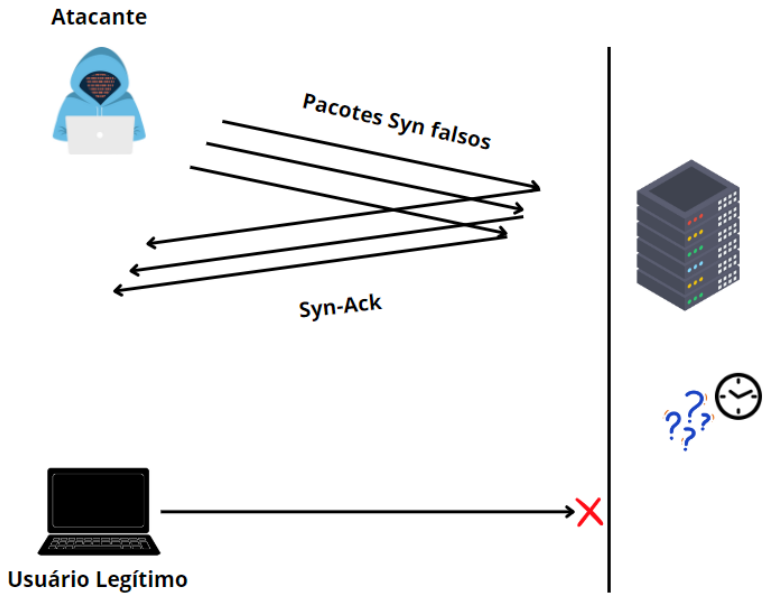

Figura 2.8: Ataque Syn-Flood
Fonte: Elaborada pelo Autor

2.2.11 Ataque Auth-Flood

O ataque de inundação por autenticação *Authentication Request Flood* terá como seu objetivo final a indisponibilidade do serviço, conforme descreve Agrawal (2018). Após a identificação

do Ponto de acesso alvo, um invasor irá transmitir quadros de solicitação de autenticação com endereços MAC falsificados que tentam se autenticar no AP, conforme explicado na Seção 2.2.6. O invasor inunda o AP com esses quadros para esgotar seus recursos de processamento e memória, destaca Agrawal (2018).Em resposta aos quadros de solicitação de autenticação, o AP precisa alocar memória para manter informações sobre cada nova estação que se autentica com êxito. Dessa forma, um AP sob ataque não poderá permitir que clientes legítimos se conectem à rede sem fio pois não haverá espaço disponível, destaca Agrawal (2018).

Para esse ataque também existe a possibilidade de ser criado com o uso de botnets. O atacante obterá os mesmos benefícios citados no ataque Syn-Flood.

2.2.12 Ataque Assr-Flood

O ataque de inundação por solicitação de associação *(Association Request Flood)* também terá como objetivo indisponibilizar o *AP*, afetando diretamente a disponibilidade do serviço afirma Agrawal (2018). Por padrão, o *AP* insere os dados fornecidos por uma estação em sua "Solicitação de Associação"em uma tabela conhecida como tabela de associação, que é mantida na memória do *AP*. Quando essa tabela atinge seu limite, o *AP* recusa outras tentativas de associação de clientes. Conforme mencionado por Agrawal (2018), após esse ponto, o invasor pode autenticar várias estações inexistentes usando endereços *MAC* ou *IPs* que parecem legítimos, mas foram gerados aleatoriamente. Em seguida, o atacante envia uma série de solicitações de associação falsificadas, levando a tabela de associação a transbordar e recusar novas solicitações. Se não houver uma lista de controle de acesso para filtragem de endereços *MAC* ou *IPs*, os ataques de autenticação e associação se tornam consideravelmente mais fáceis de serem lançados por um invasor. Destacando que um *AP* não aceitará uma solicitação de associação enviada por uma estação não autenticada.

Para esse ataque também existe a possibilidade de ser criado com o uso de botnets. O atacante obterá os mesmos benefícios citados no ataque Syn-Flood e Auth-Flood.

2.2.13 Ataque Eavesdrop

Fortinet (2022) afirma que o principal objetivo do *eavesdrop*, também conhecido como escuta, é a coleta, deleção ou interceptação dos dados, assim violando diretamente a confidencialidade das informações. Networks (2022) ressalva que um *eavesdrop* casual faz a varredura passiva e é capaz de simplesmente usar qualquer rádio cliente IEEE 802.11 para ouvir os quadros de *beacon* IEEE 802.11. Esses quadros são enviados continuamente pelo AP. Algumas das informações encontradas nos quadros de *beacon* incluem o identificador do conjunto de serviços (SSID), endereços MAC, taxas de dados compatíveis e outros recursos do conjunto de serviços básicos (BSS). Networks (2022) ressalta ainda que um analisador de protocolo WLAN deve ser usado como uma ferramenta de diagnóstico. No entanto, um invasor pode usar um analisador

como um dispositivo de escuta malicioso para monitoramento não autorizado de trocas de quadros 802.11. Embora todas as informações da camada 2 estejam sempre disponíveis, todas as informações das camadas 3 a 7 podem ser expostas se a criptografia WPA2/WPA3 não estiver em vigor. Todas as comunicações em texto claro, como senhas de e-mail, FTP e Telnet, podem ser capturadas se não houver criptografia. Além disso, todas as transmissões de quadros 802.11 não criptografados podem ser remontadas nas camadas superiores do modelo OSI. As mensagens de e-mail podem ser remontadas e, portanto, lidas por um atacante.

Conforme destacado por Fortinet (2022), o *eavesdrop* pode acarretar sérias consequências, incluindo perdas financeiras substanciais. Pois os invasores podem explorar o acesso obtido para adquirir informações confidenciais, como dados corporativos, segredos comerciais ou senhas de usuários, visando lucros indevidos. Além disso, há o risco de roubo de identidade, já que os invasores podem capturar as credenciais dos usuários na rede. Veja a Figura 2.9.

Existem algumas variantes desse ataque, são elas:

- Man-in-the-Middle (MITM): O ataque MITM terá como objetivo interceptar e possivelmente alterar a comunicação entre duas partes sem o conhecimento dos usuários, afirma James (2023). O invasor pode interferir de maneira passiva realizando a interceptação de informações sem que a vítima perceba, ou de forma ativa, modificando o conteúdo das mensagens ou se passando pela pessoa ou sistema envolvido na comunicação.

- Ataque de repetição: Datta (2023) destaca que também é conhecida como *Replay Attack*, trata-se de uma técnica na qual um atacante intercepta ou retransmite dados que foram previamente transmitidos entre partes legítimas. O principal objetivo é enganar o sistema para que ele aceite a retransmissão dos dados como legítima, ou seja, ele irá apenas retransmitir passivamente os dados já existentes na rede sem modifica-los.

2.2.14 Ataque Evil Twin

Ter acesso à internet por meio do próprio notebook em locais como aeroportos, shoppings, cafés ou bares pode parecer uma tarefa simples. No entanto, pontos públicos de conexão Wi-Fi apresentam vulnerabilidades que atraem a atenção de *hackers*, aumentando o risco de roubo de informações pessoais, destaca HSC Brasil (2020). Com o objetivo de explorar essa vulnerabilidade surgiu o ataque *Evil Twin*, variação do *Rogue Access*. HSC Brasil (2020) afirma que é popularmente conhecido como gêmeo malvado, nesse ataque o invasor irá ter como objetivo a coleta de informações sem o conhecimento do usuário final, fazendo-o acreditar que o dispositivo em que está se conectando é real, quando na verdade o usuário estará se conectando a um servidor malicioso que pode monitorar e obter os dados digitais desse usuário. HSC Brasil (2020) mostra que para a realização desse ataque, inicialmente o invasor terá que configurar o seu (SSID) *Service Set Identifier* com o mesmo nome do ponto de acesso alvo, após isso ele

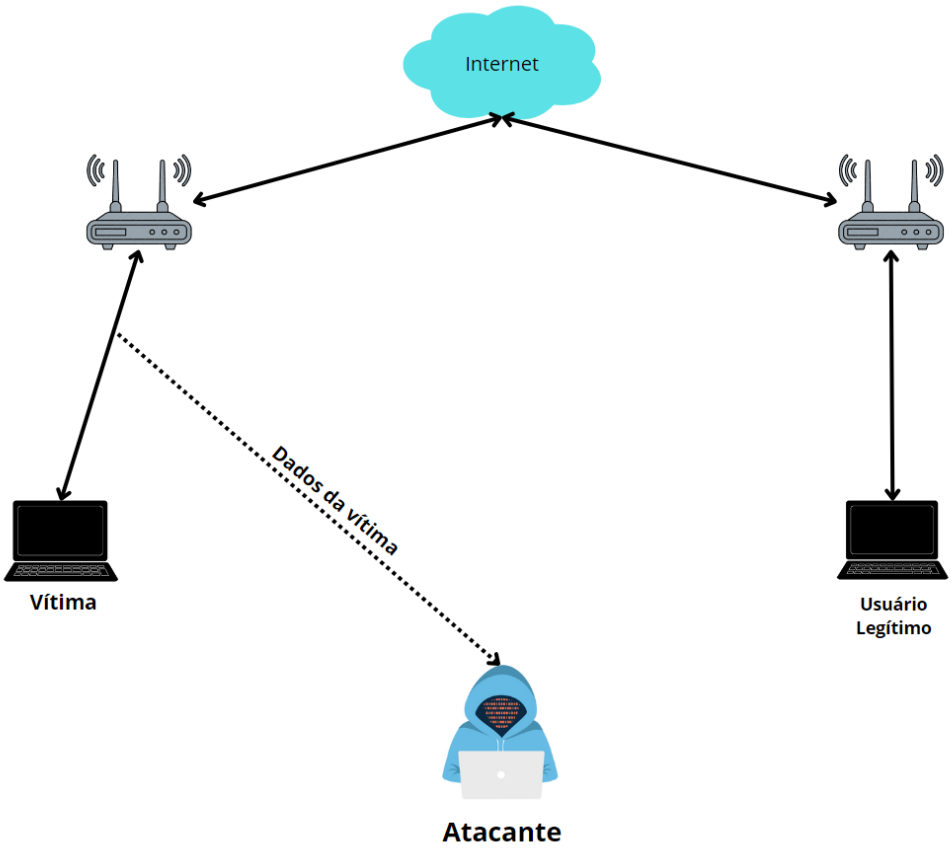

Figura 2.9: Ataque Eavesdrop
Fonte: Elaborada pelo Autor

deverá interromper ou desabilitar o sinal do ponto de acesso legítimo, ele poderá fazer isso criando uma interferência com os sinais de radiofrequências (RF) que o seu ponto de acesso falso está transmitindo, fazendo-o ser maior que o legítimo, desse modo os usuários conectados irão perder suas conexões com o *AP* verdadeiro e se reconectarão ao *AP* invasor, permitindo assim que ele passe a receber todo o tráfego que passa pela rede para seu dispositivo ilegítimo. Veja a Figura 2.10.

2.3 Segurança da informação

A segurança da informação representa um dos maiores desafios tecnológicos da atualidade, conforme apontado por Oliveira (2018). Embora conectar uma ampla gama de dispositivos à internet possa não ser um obstáculo para a indústria ou empresas, a verdadeira preocupação reside na garantia da segurança desses dispositivos. Oliveira (2018) ressalta que, embora a tecnologia avance diariamente, é crucial reconhecer que os criminosos também se especializam e se atualizam constantemente. Como resultado, observa-se um aumento contínuo nos crimes

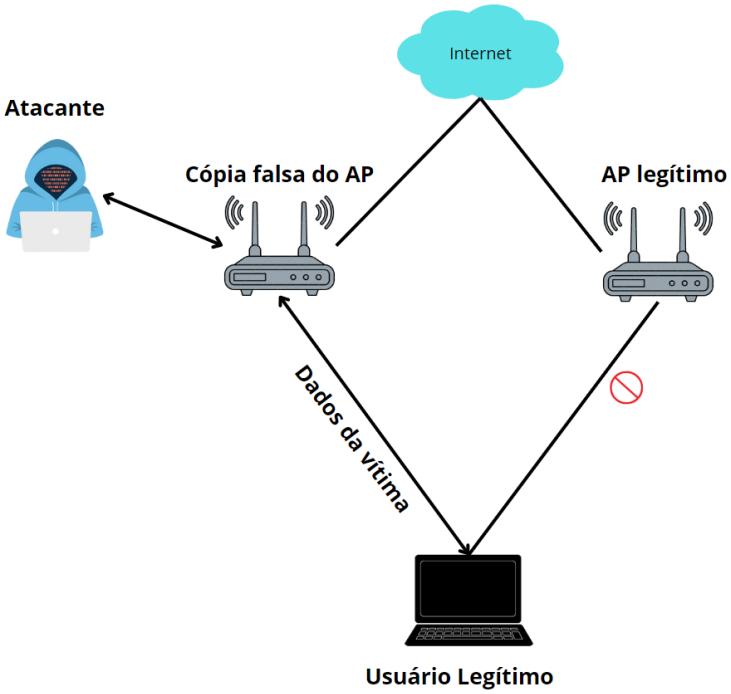

Figura 2.10: Ataque Evil Twin
Fonte: Elaborada pelo Autor

cibernéticos, fraudes e outras formas de ataques que ocorrem por meio da internet, apesar dos avanços em segurança já existentes atualmente.

Segundo Oliveira (2018), a maior vulnerabilidade de qualquer sistema de segurança reside no fator humano, que muitas vezes subestima os riscos ou simplesmente não considera a possibilidade de ser alvo de um ataque. Portanto, Oliveira (2018) destaca que para garantir a segurança de um sistema ou dispositivo, é crucial adotar medidas para minimizar os riscos ao máximo possível. Isso inclui manter os softwares sempre atualizados, estar atento às vulnerabilidades descobertas nos sistemas, realizar backups regulares e armazená-los em locais separados do equipamento principal.

Hintezbergen (2018) diz que a segurança da informação tem por objetivo a preservação da confidencialidade, integridade e disponibilidade da informação. Dessa forma, podemos dizer que a segurança da informação tem por objetivo proteger os ativos [1] responsáveis por transmitir, armazenar ou processar informações. Ainda de acordo com Hintezbergen (2018), a segurança da informação é alcançada através da implementação de um conjunto de controles, que estende-se a políticas, processos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados quando necessário, para assim assegurar que os objetivos específicos de segurança sejam atendidos. A abordagem de processo para gestão da segurança da informação apresentada na ISO27002 (2022), que nada mais é que um código de boas práticas que trás um conjunto de

[1] Ativo é qualquer coisa que agrega valor para a organização

controles necessário para implementação da SGSI, inclui a importância de:

- Compreender requisitos de segurança e a necessidade de estabelecer políticas e objetivos para a segurança da informação.
- Implementar e operar controles para gerenciar riscos de segurança da informação da organização no contexto de riscos gerais de negócio da organização.
- Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação.
- Melhoria contínua baseada em medições objetivas

2.3.1 Fundamentos da segurança da informação

Antes de adentrarmos no conceito de segurança da informação, é crucial compreender a natureza dos dados e informações, afirma Oliveira (2018).

Conforme destacado por Oliveira (2018), os dados constituem-se como conjuntos de códigos e caracteres que, por si só, ainda não possuem significado ou contexto específico. Esses dados podem se tornar informações quando são submetidos a processamentos e análises que lhes conferem significado e utilidade para os usuários ou sistemas. Assim, podemos estabelecer a seguinte distinção fundamental:

- Dado: Segundo Oliveira (2018), os dados representam os elementos brutos, como números, letras e símbolos, que carecem de contexto e interpretação imediata.
- Informação: Refere-se aos dados que foram processados, organizados e contextualizados de forma a fornecer significado e relevância para determinado fim ou propósito, afirma Oliveira (2018).

Conforme Oliveira (2018) retrata, essa distinção entre dado e informação é crucial para compreendermos a importância da segurança da informação, uma vez que esta se destina a proteger não apenas os dados em sua forma bruta, mas também as informações derivadas desses dados após processamento e análise.

2.3.2 Tríade da segurança CID

A tríade da segurança da informação é um conceito fundamental que serve como alicerce para todas as medidas e práticas de proteção de dados e sistemas. Essa tríade, representada pela sigla CID (Confidencialidade, Integridade e Disponibilidade), encapsula os três principais objetivos da segurança da informação, cada um desempenhando um papel essencial na preservação e proteção das informações sensíveis, destaca Oliveira (2018). Veja a Figura 2.11.

- Confidencialidade: Hintezbergen (2018) afirma que será garantia que a informação não será disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados.
- Integridade: De acordo com Hintezbergen (2018) diz respeito à garantia de que as informações sejam precisas, completas e confiáveis ao longo do tempo.
- Disponibilidade: Segundo Hintezbergen (2018) é a certeza que a informação estará acessível e utilizável sob demanda por uma entidade autorizada. Isso inclui proteger os sistemas contra falhas, ataques cibernéticos ou eventos adversos que possam interromper ou impedir o acesso legítimo às informações.

Hintezbergen (2018) afirma que o nível de segurança requerido para executar esses princípios é diferente em cada empresa ou estabelecimento, pois cada um terá sua própria combinação de objetivos e requisitos de negócios e segurança. O autor destaca também que todos os controles de segurança, mecanismos e proteção são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidos pela capacidade potencial de comprometer um ou todos os princípios do triângulo CIA.

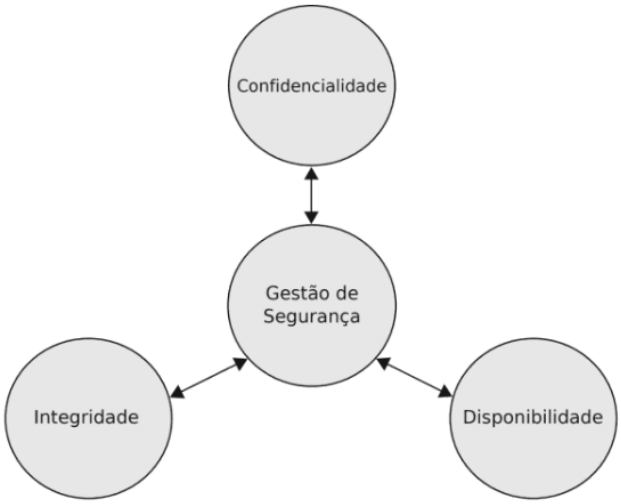

Figura 2.11: Tríade CID da segurança da informação
Fonte: Hintezbergen (2018)

2.3.3 Criminosos Cibernéticos e suas classificações

De acordo com Oliveira (2018), por trás de qualquer tipo de crime cibernético está um indivíduo. Dependendo da natureza do delito cometido, esse criminoso pode ser classificado de diversas maneiras. No entanto, é importante ressaltar que não há uma hierarquia entre os criminosos cibernéticos; o que existe é um indivíduo que utiliza um computador ou dispositivo para cometer atividades criminosas no ambiente virtual. Oliveira (2018) classifica-os como:

1. Hacker: Segundo Oliveira (2018), um *hacker* é definido como um indivíduo que possui um vasto conhecimento em tecnologia e que o utiliza em benefício próprio, independentemente de estar cometendo um crime.

2. Cracker: De acordo com Oliveira (2018), os *crackers* são cibercriminosos cujo principal objetivo é causar danos. Ao contrário dos *hackers*, que usam suas habilidades para benefício próprio, os *crackers* buscam obter informações sensíveis, como números de cartão de crédito, para realizar compras fraudulentas. Caso não obtenham sucesso, podem optar por destruir dados, formatando discos rígidos ou criptografando informações e exigindo resgate para descriptografá-las.

3. Script Kiddie: Oliveira (2018) destaca que o *Script Kiddie* é um tipo de atacante que possui conhecimento limitado em programação e segurança, mas utiliza *scripts* ou ferramentas prontas para realizar ataques cibernéticos. Esses indivíduos geralmente não possuem habilidades avançadas de programação ou compreensão profunda dos sistemas que estão atacando. Em vez disso, eles confiam em *scripts* e ferramentas desenvolvidas por outros, muitas vezes sem entender completamente como funcionam.

4. Lammer: Segundo Oliveira (2018), o *Lammer* será um indivíduo inexperiente e pouco habilidoso que tenta se envolver em atividades de *hacking* ou *cracking*. Ao contrário dos *script kiddies*, que possuem conhecimento limitado, mas utilizam *scripts* e ferramentas prontas para realizar ataques, os *Lammer* são caracterizados por sua falta de habilidade e compreensão básica dos conceitos de segurança cibernética.

5. Ciberterrorista : De acordo com Oliveira (2018) será o tipo de cibercriminoso que fará o ciberterrorismo, que refere-se a ataques coordenados por indivíduos ou grupos com o objetivo de derrubar infraestruturas críticas, como redes elétricas, satélites ou aeroportos, utilizando técnicas avançadas de *hacking*. Esses ataques são planejados de forma sincronizada e visam causar interrupções graves na vida cotidiana e na segurança nacional. Os ciberterrorista exploram vulnerabilidades em sistemas de infraestrutura para alcançar seus objetivos, representando uma séria ameaça à segurança global.

2.3.4 Gerenciamento de risco

Para que a segurança seja implementada de maneira eficaz é necessário inicialmente definir estratégias, ou seja, precisamos identificar o que estamos protegendo e do que estamos protegendo e a metodologia que usamos para nos ajudar a obter algum conhecimento sobre isso é chamada de Gerenciamento de Risco, afirma Hintezbergen (2018). Para realiza-la, primeiramente precisamos definir o que é risco. Dessa maneira, Hintezbergen (2018) afirma que risco é

a possibilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios.

Segundo Hintezbergen (2018), por definição, o Gerenciamento de riscos compreende no processo de planejar, organizar, conduzir e controlar as atividades de uma organização, visando minimizar os efeitos do risco sobre o capital e lucro de uma organização.

Hintezbergen (2018) ressalta que os riscos enfrentados pelas organizações podem ter origens variadas, podendo surgir da incerteza do mercado financeiro, falhas de projeto, obrigações legais, riscos de crédito, acidentes, eventos naturais ou desastres, além de ataques deliberados por adversários. Para lidar com esses desafios, foram desenvolvidos diversos padrões de gerenciamento de riscos, incluindo aqueles propostos pelo *Project Management Institute* (PMI), *National Institute of Standards and Technology* (NIST) e padrões ISO. Neste contexto, este trabalho concentrará sua análise no padrão proposto pelo NIST, D. Gallagher (2012).

Conforme destacado por Hintezbergen (2018), as estratégias de gestão de riscos abrangem uma variedade de abordagens, que incluem: mitigar o impacto negativo do risco por meio de medidas preventivas ou de contingência ou aceitar parcial ou totalmente as consequências de um risco específico. O autor ressalta ainda que o gerenciamento de riscos é um processo contínuo e abrangente, que permeia todos os aspectos das operações organizacionais.

Conforme afirmado por Hintezbergen (2018), o gerenciamento de riscos é um processo complexo que engloba duas medidas essenciais: a Avaliação de Risco e a Análise do Risco. A Figura 2.12 ilustra detalhadamente essa estrutura.

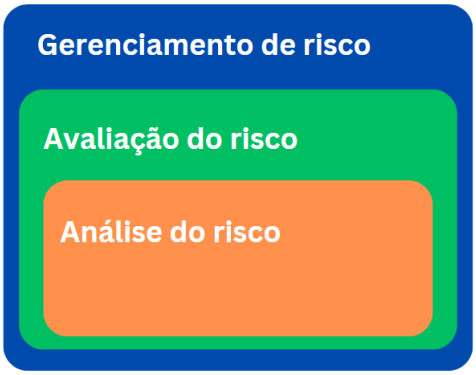

Figura 2.12: Estrutura da Gestão de Risco
Fonte: Guard (2023)

2.3.5 Avaliação do risco

A avaliação do risco será um dos primeiros processos no gerenciamento do risco. D. Gallagher (2012) afirma que as organizações irão usa-la para determinar a extensão das potenciais ameaças e o risco associado a um ativo. Ao final desse processo, será possível identificar controles apropriados para reduzir ou eliminar riscos durante a fase de mitigação. D. Gallagher

(2012) enfatiza ainda que a avaliação da probabilidade de um evento adverso futuro demanda uma análise conjunta das ameaças a um ativo, considerando as vulnerabilidades existentes e os controles já implementados para tal ativo. Quanto ao impacto, este está relacionado à magnitude do dano que poderia ser provocado pela exploração de uma vulnerabilidade por uma ameaça. O nível de impacto é governado pelos potenciais efeitos na missão organizacional e, consequentemente, gera um valor relativo para os ativos e recursos afetados. Ainda de acordo com D. Gallagher (2012) o processo para conduzir uma avaliação do risco, deverá ser dividida em 9 passos. É possível entender por meio da Figura 2.13.

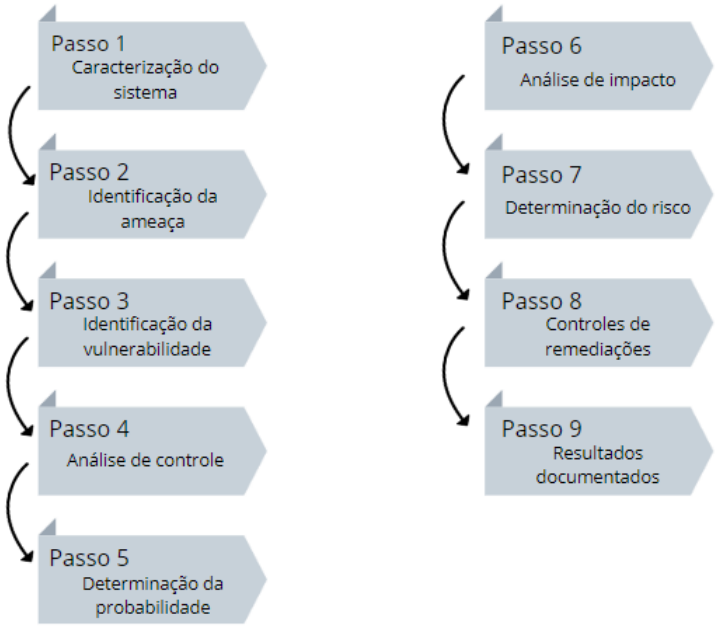

Figura 2.13: Avaliação de Risco - Fluxograma
Fonte: Elaborada pelo Autor

Caracterização do sistema

Para D. Gallagher (2012), o passo inicial e crucial na avaliação de riscos é a definição do escopo, que envolve um mapeamento abrangente dos recursos e informações que constituem o sistema ou infraestrutura em análise. A caracterização minuciosa do sistema não apenas delineia o escopo para o esforço de avaliação, mas também autorizações necessárias, fornecendo informações vitais, como detalhes sobre software, hardware e conectividade. Essa abordagem meticulosa na delimitação do escopo possibilita uma identificação precisa dos riscos inerentes a essa área específica. A coleta de informações do sistema pode ser realizada por meio de questionários, entrevistas, revisão de documentos ou o emprego de ferramentas de varredura. Ao concluir esta etapa, obtemos uma visão abrangente do ambiente e a delimitação clara dos limites do sistema ou infraestrutura em análise.

Identificação da ameaça

Para uma compreensão eficaz desta etapa, é crucial distinguir os conceitos de ameaça, vulnerabilidade, agentes de ameaças e fontes de ameaças. De acordo com D. Gallagher (2012), uma ameaça representa a possibilidade de uma fonte específica explorar com êxito uma vulnerabilidade determinada. D. Gallagher (2012) afirma também que:

- Vulnerabilidade: Um ponto fraco em um sistema ou infraestrutura que pode ser explorado por um invasor para realizar um ataque bem-sucedido.
- Agentes de ameaças: Indivíduos ou grupos que causam intencionalmente danos a dispositivos e sistemas digitais.
- Fonte de ameaças: O método utilizado para explorar intencionalmente uma vulnerabilidade.

É crucial destacar que, de acordo com D. Gallagher (2012), uma fonte de ameaça não representa um risco por si só; ela só se torna relevante quando há uma vulnerabilidade que um atacante pode explorar. Portanto, ao determinar a probabilidade de uma ameaça, é necessário considerar tanto as fontes de ameaças quanto as vulnerabilidades potenciais. O objetivo desta etapa é identificar as possíveis fontes de ameaças e criar uma lista abrangente dessas fontes, aplicáveis ao sistema ou infraestrutura em avaliação, enfatiza D. Gallagher (2012).

D. Gallagher (2012), classifica as fontes de ameaças mais comuns entre naturais: são aquelas causadas por eventos da natureza como, terremotos, tornados, avalanches e etc; humanas: são ameaças que são causadas por ações humanas, sendo elas com intenção efetiva ou não; ambiental: são aquelas causadas por ações do ambiente em que o sistema ou infraestrutura está, tais como falta de energia a longo prazo, poluição, vazamento de líquidos e etc.

Ainda de acordo com D. Gallagher (2012), no quesito ameaças humanas, é necessário ter em mente que se uma pessoa tem recursos adequados e a motivação para realizar um potencial ataque, isso a tornará uma perigosa fonte de ameaça com uma alta chance de que esse indivíduo realize um ataque. É necessário a realização de um estudo para classificar as potenciais motivações que uma pessoa possa ter contra o ambiente. Essa informação será de grande valor para a organização no que se refere ao mapeamento de possíveis agentes de ameaças expõe D. Gallagher (2012). Logo, para evitar riscos, realizar uma coleta de informações sobre o histórico de vazamentos de dados e violações de segurança será de grande importância na identificação de maiores potenciais de ataques e na identificação de novas vulnerabilidades.

Ao final dessa etapa teremos uma lista de possíveis fontes de ameaças que poderá ser usada para explorar potenciais vulnerabilidades.

Análise de controle

O foco primordial desta fase reside na análise dos controles planejados ou já implementados pela organização, diz D. Gallagher (2012), visando minimizar ou eliminar a probabilidade de exploração de ameaças por meio de vulnerabilidades e consequentemente reduzir os riscos. D. Gallagher (2012) propõe ainda uma série de passos para a implementação desses controles.

D. Gallagher (2012) afirma que os Métodos de Controle abrangem medidas de segurança que utilizam abordagens técnicas e não técnicas. Ainda segundo o autor, os controles técnicos são aqueles integrados ao hardware, software ou firmware do sistema, como sistemas de autenticação ou detectores de intrusos. Por outro lado, os controles não técnicos envolvem aspectos gerenciais e operacionais, como segurança ambiental e políticas de segurança.

As Categorias de Controle, aplicáveis a ambos os métodos técnicos e não técnicos, são classificadas como preventivas ou detectivas, afirma D. Gallagher (2012). Ainda de acordo com ele, os controles preventivos têm como objetivo inibir tentativas de violação da política de segurança, incluindo recursos como controle de acesso, autenticação e criptografia. Enquanto isso, os controles detectivos buscam alertar sobre possíveis tentativas de violação das políticas de segurança, empregando recursos como sistemas de detecção de intrusão e *checksums*[2] .

Determinação da probabilidade

Segundo Eclipse (2022), para determinar uma classificação geral de probabilidade que indicarão as verdadeiras chances de uma potencial vulnerabilidade ser explorada no ambiente, é necessário levar em consideração a fonte da ameaça, motivação e capacidade, natureza da vulnerabilidade e se existe atualmente no escopo do ambiente controles implementados. Eclipse (2022) explica ainda que essa probabilidade pode ser classificada como: alta, média ou baixa a depender da situação. Consulte a Tabela 2.3 para mais detalhes.

Nível	**Definição**
Alto	A fonte da ameaça está com uma motivação alta e suficientemente capaz de realizar o ataque, os controles implementados são ineficazes.
Médio	A fonte da ameaça está motivada e é capaz de realizar o ataque, mas os controles de segurança estão bem configurados e impede a exploração efetiva da vulnerabilidade.
Baixo	A fonte da ameaça não está muito motivada ou capacitada, os controles de segurança estão bem posicionados para impedir que a vulnerabilidade seja explorada.

Tabela 2.3: Classificação de níveis da probabilidade
Fonte: Eclipse (2022)

[2]procedimento de verificação da autenticidade e integridade de um determinado arquivo

Análise de impacto

Nessa fase, iremos mensurar o nível de impacto negativo que um ataque bem sucedido terá em uma determinada vulnerabilidade, afirma D. Gallagher (2012). Um impacto negativo será aquele que poderá causar perda ou degradação de qualquer uma ou a combinação dos pilares da segurança (confidencialidade, integridade ou disponibilidade), destaca D. Gallagher (2012). Segundo, Tucker (2012) a avaliação do impacto pode ser conduzida tanto de forma quantitativa quanto qualitativa. Tucker (2012) afirma ainda que a análise quantitativa de riscos atribui uma probabilidade à ocorrência dos perigos identificados e determina seu impacto ou consequência, muitas vezes resultando em um valor específico, como a expectativa de perda ou custo associado. Já a análise qualitativa de riscos, assemelhando-se à avaliação de riscos ou à análise de vulnerabilidades, direciona menos atenção à probabilidade, concentrando-se na análise de ameaças de maneira análoga à identificação de perigos, vulnerabilidades, consequências ou controles. Ao fim dessa fase teremos uma magnitude do impacto que poderá ser classificada como alta, média ou baixa.

Determinação do risco

O propósito desta etapa consiste em avaliar o nível de risco associado ao ambiente, diz D. Gallagher (2012). Ainda de acordo com D. Gallagher (2012), a determinação do risco para um determinado par de ameaça/vulnerabilidade pode ser expressa como uma função de:

- A probabilidade de uma fonte específica de ameaça tentar explorar uma vulnerabilidade específica.
- A magnitude do impacto, caso uma fonte de ameaça seja bem-sucedida na exploração da vulnerabilidade.
- A eficácia dos controles de segurança planejados ou já implementados para reduzir ou eliminar o risco.

D. Gallagher (2012) diz que para quantificar o risco, desenvolver uma escala e uma matriz de níveis de risco é de grande ajuda. Isso proporcionará uma visão abrangente e estruturada para a tomada de decisões quanto às medidas a serem adotadas. Essa matriz, consiste em uma tabela orientada por duas dimensões: probabilidade e impacto.

Controles de remediações

Nesta fase de acordo com D. Gallagher (2012), são apresentados os controles destinados a mitigar e eliminar os riscos identificados. O principal objetivo é reduzir o nível de risco no ambiente, marcando assim o início do processo de mitigação dos riscos previamente avaliados e identificados. D. Gallagher (2012) afirma ainda que a implementação de todos os controles

recomendados pode não ser viável em termos de custo-benefício. Portanto, cada caso será avaliado individualmente nesse contexto. Ao final deste processo, serão fornecidas recomendações de controles específicos e possíveis soluções alternativas para efetivar a mitigação dos riscos identificados.

Documentação

Como mencionado por D. Gallagher (2012) ao encerrar a etapa de avaliação de riscos, que inclui a identificação das fontes de ameaças, vulnerabilidades, riscos avaliados e os controles recomendados, é imperativo consolidar essas informações em um relatório oficial. Ainda de acordo com D. Gallagher (2012), este documento servirá como um registro abrangente, detalhando todas as descobertas e as estratégias propostas para lidar com os riscos identificados. O relatório não apenas documenta os resultados da avaliação, mas também fornece um guia claro para as próximas etapas no processo de gestão de riscos. Ele se torna uma ferramenta valiosa para comunicar efetivamente os *insights* obtidos, facilitando a tomada de decisões informadas e a implementação eficiente de medidas de segurança apropriadas.

2.3.6 Análise de risco

Hintezbergen (2018) define a análise de risco como um processo para compreender a natureza do risco a fim de determinar seu nível, proporcionando uma base estimativa para que possam ser tomadas decisões de tratamento para ele. D. Gallagher (2012) afirma que juntas, as abordagens de avaliação e análise do risco formam a abordagem analítica dos riscos. As organizações determinam o nível de detalhe e a forma como as ameaças serão analisadas, incluindo o nível de granularidade para descrever eventos de ameaças ou cenários de ameaças, afirma D. Gallagher (2012). Abordagens de análise diferentes podem levar a diferentes níveis de detalhe na caracterização de eventos adversos para os quais as probabilidades são determinadas.

Tucker (2012) diz que para prosseguir de maneira lógica para realizar a análise, primeiramente é necessário prosseguir com algumas tarefas fundamentais:

1. Identificar os ativos que precisam de proteção;
2. Identificar os riscos ou ameaças que podem afetar os ativos identificados;
3. Determinar a probabilidade de ocorrência dos riscos identificados;
4. Determinar o impacto, monetário quando possível, que a empresa irá sofrer se a perda efetivamente acontecer;

2.3.7 Risco vs Viabilidade de um ataque

Conforme destacado por Hintezbergen (2018) o risco de um ataque é uma medida que avalia a possibilidade de um evento prejudicial ocorrer, juntamente com a magnitude de suas consequências. Em um contexto de segurança cibernética, conforme Hintezbergen (2018) destaca, o risco de um ataque representa a probabilidade de que um ataque ocorra e o impacto que esse ataque terá no ambiente afetado. Esse conceito leva em consideração diversos fatores. R. Ingoldsby (2021) destaca alguns, como a probabilidade do ataque ser bem-sucedido, o impacto que terá nos sistemas e dados, e o custo associado à mitigação ou reparação dos danos causados pelo ataque. Quanto maior o risco de um ataque, maior a probabilidade de ocorrerem consequências adversas e maiores os danos potenciais que ele pode causar.

Já quando falamos da viabilidade, R. Ingoldsby (2021) afirma que a viabilidade de um ataque refere-se à capacidade de um atacante de executar com sucesso um determinado tipo de ataque. Essa medida leva em conta diversos fatores, como a facilidade de realização do ataque, os recursos necessários para executá-lo, a exposição das vulnerabilidades nos sistemas alvo e a probabilidade de evasão das medidas de segurança existentes, destaca R. Ingoldsby (2021). Em outras palavras, a viabilidade de um ataque avalia se um atacante possui os meios e oportunidades para explorar com sucesso uma vulnerabilidade específica nos sistemas de um alvo. Quanto maior a viabilidade de um ataque, mais provável é que ele seja executado com sucesso pelos atacantes.

Segundo R. Ingoldsby (2021), o risco de um ataque está relacionado à probabilidade e ao impacto das consequências adversas desse ataque, enquanto a viabilidade de um ataque está relacionada à capacidade dos atacantes de explorar com sucesso as vulnerabilidades nos sistemas alvo. R. Ingoldsby (2021) destaca também que ambos os conceitos são fundamentais para entender e gerenciar a segurança cibernética de uma organização.

2.4 Modelagem de ameaças

A modelagem de ameaças é um procedimento sistemático e analítico empregado para identificar e avaliar potenciais vulnerabilidades em um sistema, decorrentes de decisões de projeto menos favoráveis afirma Coles (2021). O autor destaca também que seu propósito primordial reside na detecção precoce dessas vulnerabilidades, permitindo a implementação de medidas corretivas de forma proativa. Coles (2021) afirma que durante o processo de modelagem de ameaças, o sistema é examinado como uma entidade composta por diversos componentes, cujas interações com o ambiente externo e os agentes externos são minuciosamente consideradas. A partir dessa análise, são exploradas possíveis falhas nos componentes e interações, bem como os potenciais cenários em que essas falhas podem ocorrer ou serem exploradas.

Conforme mencionado por Coles (2021), esse procedimento acarreta na identificação das ameaças ao sistema, as quais, por sua vez, induzem a adaptações e ajustes na estrutura do sis-

tema. Ao final desse processo teremos um sistema capaz de resistir às ameaças antecipadas. Entretanto, segundo Coles (2021), é crucial esclarecer desde o princípio: a modelagem de ameaças é uma atividade cíclica que se inicia com um objetivo claramente definido, prossegue com análise e ações, e então se repete. Não constitui uma solução completa e não aborda todas as preocupações de segurança. Coles (2021) destaca que a modelagem de ameaças é um processo lógico e intelectual que será mais eficaz se envolver a maioria, senão todos, da sua equipe. Ela gera discussões e proporciona clareza no design e na execução do projeto.

2.4.1 Vantagens da Modelagem

Coles (2021) ressalva que ao criar modelos, é possível explorar diferentes cenários e estratégias para garantir que o sistema atenda aos requisitos e objetivos estabelecidos. Além disso, a modelagem permite uma análise detalhada das interações entre os componentes individuais do sistema, ajudando a identificar potenciais pontos fracos ou vulnerabilidades que precisam ser abordados.

Uma das principais vantagens da modelagem é a capacidade de realizar alterações e ajustes no estágio de projeto, antes que qualquer construção real tenha começado, afirma Coles (2021). Isso porque é muito mais simples e econômico fazer modificações em um modelo esquemático do que em uma implementação física completa. Essa abordagem permite que os engenheiros e projetistas refinem e otimizem o sistema de forma iterativa, garantindo sua eficácia e eficiência antes da implementação final.

Portanto, Coles (2021) destaca que a modelagem de sistemas não apenas facilita a visualização e compreensão de um sistema complexo, mas também oferece uma plataforma flexível e adaptável para o planejamento e o projeto, permitindo que os projetistas tomem decisões informadas e eficazes em todas as fases do processo de desenvolvimento.

2.4.2 Tipos de estruturas na Modelagem de Ameaças

Coles (2021) destaca que podemos seguir com duas abordagens quando nos referimos a modelagem de ameaças: a modelagem com o ativo no centro e a modelagem focando no atacante.

Ao adotarmos a abordagem centrada no ativo, consideramos que o ativo será algo de valor, afirma Coles (2021). Durante a modelagem de ameaças, quando mencionamos ativos, estamos comumente nos referindo a algo que um invasor deseja acessar, controlar ou destruir. É crucial que todos os participantes do processo concordem sobre o que constitui um ativo, caso contrário, o processo pode se tornar confuso, e os participantes podem encontrar dificuldades em se comunicar efetivamente.

Conforme apontado por Coles (2021), o termo ativo pode ser empregado de três maneiras distintas durante o processo de modelagem de ameaças. Primeiramente, é utilizado para se referir aos elementos que são alvo do atacante, podendo incluir desde senhas de usuário até

números de cartões de crédito. Em segundo lugar, é empregado para designar os elementos que buscamos proteger contra possíveis ataques. Por fim, é utilizado para abranger as etapas que um atacante pode executar para alcançar quaisquer das duas opções mencionadas anteriormente.

A abordagem centrada no atacante, conforme destacado por Coles (2021), busca compreender as atividades potenciais que um invasor pode realizar, levando em conta o perfil típico desses atacantes. Especialistas em segurança frequentemente utilizam diversas categorias de tipos de atacantes para identificar ameaças contra um sistema. Além disso, o autor ressalta que as abordagens centradas no atacante podem revelar possibilidades relacionadas ao fator humano.

2.4.3 Árvore de ataques

Coles (2021) destaca que as árvores de ataque têm sido utilizadas no campo da ciência da computação por mais de 20 anos. Elas são úteis para compreender como um sistema é vulnerável, modelando como um atacante pode influenciar um sistema. As árvores de ataque são o principal tipo de modelo na análise de ameaças ao se adotar uma abordagem centrada no atacante.

R. Ingoldsby (2021) cita que as árvores de ataques são modelos da realidade, ou seja, são uma representação simplificada de objetos e forças complexas do mundo real. A precisão com que os os ramos subjacentes são conhecidos depende de muitos fatores, incluindo o tempo e o esforço dedicados a estudá-los. Importante destaque é que uma das diferenças mais significativas entre a análise de árvore de ataque e alguns outros métodos de análise de risco hostil é que as árvores de ataque são construídas, em grande parte, do ponto de vista do atacante em vez do defensor. Isso trás uma perspectiva importante para a realidade de segurança da infraestrutura ou sistema em questão.

Outro benefício significativo das árvores de ataque conforme destacado por R. Ingoldsby (2021) é a sua capacidade de incorporar informações específicas sobre a defesa contra um adversário único, analisando a perspectiva de um ataque contra uma defesa em particular. R. Ingoldsby (2021) destaca ainda que essa precisão é uma virtude crucial, pois oferece previsões mais exatas para situações específicas em comparação com estatísticas generalizadas. No entanto, a especificidade torna desafiador comparar previsões particulares de um defensor com estatísticas que abrangem uma ampla gama de defensores e atacantes. Essas disparidades dificultam a capacidade das estatísticas gerais de fornecer estimativas significativas de probabilidade e risco para casos individuais. Felizmente, os modelos de ameaças baseados em árvores de ataque podem oferecer estimativas de risco mais precisas para situações específicas.

Como Scheier (2004) escreveu em sua introdução ao assunto, *"As árvores de ataque fornecem uma maneira formal e metódica de descrever a segurança dos sistemas, com base em vários ataques. Basicamente, você representa os ataques contra um sistema em uma estrutura de árvore, com o objetivo como o nó raiz e as diferentes formas de atingir esse objetivo como nós intermediários"*.

2.4.4 Lógica booleana nas árvores de ataque

Segundo Scheier (2004) , o evento localizado no topo ou raiz da árvore representa o objetivo geral do atacante. O autor afirma que após a definição desse objetivo, o sistema ou infraestrutura passa por uma análise contextual em relação ao seu ambiente e operação, identificando todos os eventos relevantes que conduzirão diretamente à realização do objetivo geral. Scheier (2004) destaca também a importância de estabelecer uma relação lógica entre esses eventos, conectando cada um a uma porta OR ou uma porta AND. A porta OR indica que a saída ocorrerá se e somente se um ou mais eventos de suas entradas acontecerem. Por outro lado, as portas AND têm a saída condicionada à ocorrência de todos os eventos de suas entradas.

Ao identificar eventos que não podem ser mais divididos, encontramos um nó folha, que representa o objetivo específico do atacante, afirma Scheier (2004). Caso contrário, esses eventos se tornarão nós intermediários, servindo como sub-objetivos que serão divididos continuamente até que todos os eventos alcancem o estado de folhas. Vale destacar que a decisão de dividir um evento em sub-eventos ou folha depende exclusivamente do conhecimento do indivíduo sobre a infraestrutura ou sistema em questão. Consulte a Figura 2.14 para visualizar uma representação do processo descrito.

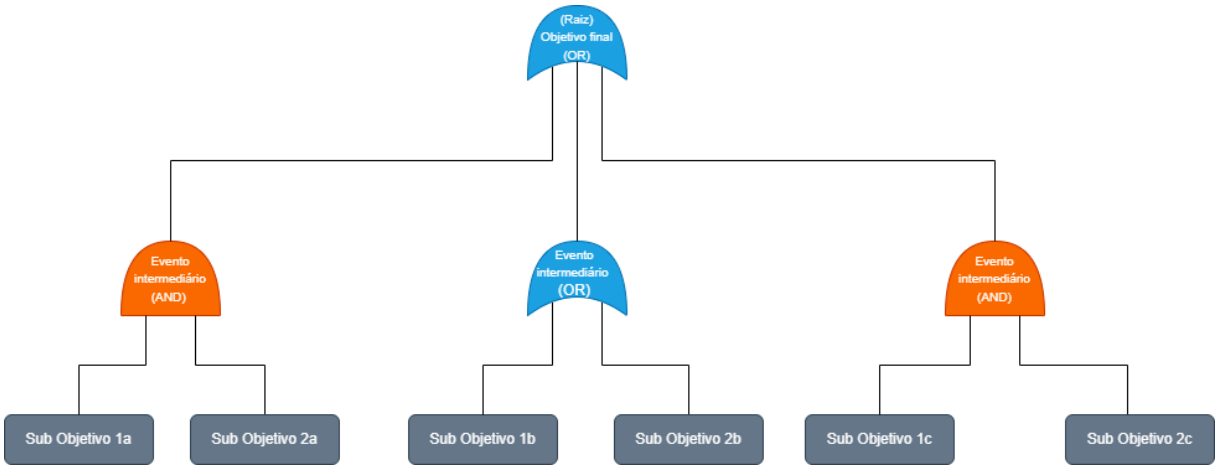

Figura 2.14: Modelo Árvore de ataque
Fonte: Elaborada pelo Autor

3

Trabalhos Relacionados

Nesta Seção iremos apresentar uma revisão dos estudos e pesquisas relevantes na área, destacando suas contribuições e pontos de convergência. Os trabalhos relacionados foram classificados em duas categorias distintas: (I) trabalhos relacionados à segurança em redes sem fio e (II) trabalhos relacionados à modelagem e análise de risco. Essa segmentação foi realizada com o intuito de proporcionar uma compreensão mais clara das diferentes abordagens presentes no estado da arte.

3.1 Trabalhos relacionados à segurança em redes sem fio

Nesta categoria, serão destacados dois trabalhos que se concentram na segurança das redes sem fio. Esses trabalhos oferecem uma análise aprofundada das principais vulnerabilidades e desafios enfrentados atualmente nesse domínio.

No estudo realizado por Thant (2019), é proposta a configuração de um ambiente de teste real para uma Rede Local sem Fio (WLAN), com o objetivo de analisar as vulnerabilidades dos ataques conhecidos relacionados à rede IEEE 802.11 e monitorar a análise dos pacotes. Com base nessas categorias de vulnerabilidades e ameaças, são conduzidos ataques de confidencialidade, como o *Evil Twin*; ataques de disponibilidade, como deautenticação, disassociação e *Café Latte*; e ataques de autenticação, como o ataque de dicionário, por meio de demonstrações em um ambiente real utilizando algumas configurações propostas.

A pesquisa conduzida demonstrou uma execução precisa de cada ataque, complementada por uma análise minuciosa das características individuais de cada um. No entanto, uma lacuna observada reside na ausência de ênfase sobre o impacto e o risco associados a esses ataques no ambiente do usuário.

Já o estudo conduzido por Dezengrini (2022), tem como propósito analisar as vulnerabilidades de segurança em redes sem fio. Realizado por meio de uma pesquisa bibliográfica

qualitativa, o trabalho consistiu em levantar as principais contribuições de autores que discutem a importância da segurança da informação nesse contexto. A análise resultante revelou as deficiências de segurança presentes nas redes sem fio, ressaltando, assim, a significância da tecnologia da informação na proteção dessas redes. O estudo destaca os principais tipos de ataques identificados e os métodos de proteção adequados para cada um, fornecendo orientações para a implementação de medidas de segurança nos ambientes dos usuários.

No entanto, uma lacuna identificada nessa pesquisa está relacionada à falta de consideração dos riscos e impactos reais para os usuários no caso de uma exploração bem-sucedida de alguma vulnerabilidade de segurança analisada. Essa omissão restringe a compreensão completa dos possíveis danos e desafios enfrentados pelos usuários diante das ameaças à segurança em redes sem fio.

3.2 Trabalhos relacionados à modelagem e análise de risco

Nesta categoria, destacaremos três trabalhos que se dedicaram à análise de risco em diversos ambientes, utilizando uma abordagem de modelagem para sua construção e análise. Esses estudos se concentram em identificar, compreender e gerenciar os riscos presentes em diferentes contextos, empregando técnicas de modelagem para representar e avaliar cenários de risco de forma sistemática e estruturada.

No estudo conduzido por Zhu (2011), foi introduzido um método de avaliação de risco para avaliar o risco de segurança da privacidade das Redes Veiculares *Ad Hoc* (VANETs) com base na modelagem de uma árvore de ataque. O esquema proposto fornece um framework de análise geral para estimar o grau que uma determinada ameaça pode trazer para as VANETs. A árvore de ataque construída foi utilizada para identificar possíveis cenários de ataque que um invasor pode executar em sistema de preservação de privacidade nas VANETs, o que é esperado para melhorar ainda mais a segurança do sistema. Adicionalmente, foi calculada a probabilidade total de alcançar o objetivo do ataque com base na árvore de ataque.

Em contrapartida, principal lacuna identificada neste estudo é a ausência de uma análise de risco que leve em consideração a viabilidade do ataque, ou seja, a capacidade de um invasor executar com sucesso um determinado tipo de ataque, explorando as vulnerabilidades no sistema. Essa análise adicional seria crucial para uma compreensão mais completa dos potenciais danos e desafios enfrentados pelas VANETs em relação à segurança da privacidade.

No estudo conduzido por Maciel (2018), avalia-se o impacto de um ataque distribuído de negação de serviço (DDoS) em sistemas computacionais. Foi proposto modelos hierárquicos que representam o comportamento dos principais componentes do sistema e avaliam os efeitos de um ataque DDoS na disponibilidade do sistema. Para realizar essa avaliação, foi adotado a modelagem de árvores de ataques, utilizando a ferramenta denominada *SeculTree* para construir a estrutura da árvore de ataques. Essa modelagem visava obter resultados com diversas métricas

de interesse como: viabilidade do ataque, habilidade técnica, perda operacional, benefício do atacante e custo do ataque. A partir disso foi possível identificar os benefícios da solução proposta.

Os resultados obtidos no fim do estudo mostraram que as técnicas de ataque distribuído de negação de serviço impactaram significativamente a vítima.

O estudo conduzido por Baldwin (2007) teve como objetivo principal abordar a segurança das contas bancárias online. Destacou-se a necessidade das instituições financeiras em identificar os métodos empregados por atacantes para comprometer tais contas, e desenvolver estratégias eficazes para protegê-las. A metodologia adotada envolveu a modelagem através de árvores de ataque e árvores de proteção. As árvores de ataque foram empregadas para evidenciar as vulnerabilidades nos sistemas, enquanto as árvores de proteção forneceram uma abordagem metodológica para mitigar essas vulnerabilidades. No âmbito desta pesquisa, foi realizado uma análise em um sistema bancário online fictício, com propostas de soluções de proteção adaptadas a diferentes níveis orçamentários. Métricas como custo do ataque, probabilidade de ocorrência e impacto associado a cada tipo de ataque foram utilizadas para cálculos e avaliação de risco. Ao final, foi possível identificar os ataques mais significativos em termos de riscos, bem como as medidas a serem adotadas para mitigar e proteger o sistema de maneira eficaz.

Todos os trabalhos aqui mencionados foram de grande relevância para a seleção da metodologia adotada nesta pesquisa. A proposta deste trabalho é integrar as principais técnicas utilizadas por esses autores e preencher a lacuna identificada, considerando o risco e o impacto para o usuário como um elemento crucial de segurança. Desta forma, será possível obter uma visão abrangente dos potenciais desafios e danos que os usuários podem enfrentar nas redes sem fio.

4

Metodologia

Neste capítulo será apresentado a metodologia adotada nesta pesquisa para a análise dos riscos em um ambiente controlado, ou seja, *Test Bed*[1]. Dessa forma, esse capítulo irá apresentar as especificações do ambiente avaliado, pilares de ataques escolhidos, árvore de ataque desenvolvida e quais métricas e fórmulas foram usadas para a realização da avaliação dos riscos.

4.1 Especificações do Ambiente

Para coleta de dados e avaliação do modelo a ser implementado, foi criado um ambiente de *Test Bed* para viabilizar as condições apropriadas para os testes. A Tabela 4.1 detalha os equipamentos usados.

Equipamentos
Notebook com Windows 11
Notebook com Kali GNU/Linux Rolling 2023.3
Adaptador wireless USB Realtek 8811CU Wireless LAN 802.11n USB NIC
Ponto de acesso Tp-link EAP115 V:4.20

Tabela 4.1: Equipamentos do ambiente
Fonte: Elaborada pelo Autor

Sobre a topologia da rede, como explicado na Seção 2.2, foi usados 2 notebooks conectados a um adaptador Wireless USB que fazia conexão com o ponto de acesso, formando nossa rede Lan-Wireless 802.11n. Podemos visualizar melhor na Figura 4.1.

4.1.1 Ferramentas usadas nos ataques implementados

No *Test Bed* foram usadas as seguintes ferramentas para a implementação desses ataques:

[1] Infraestruturas que tem como objetivo viabilizar as condições necessárias para o teste e experimentação de novos produtos ou serviços

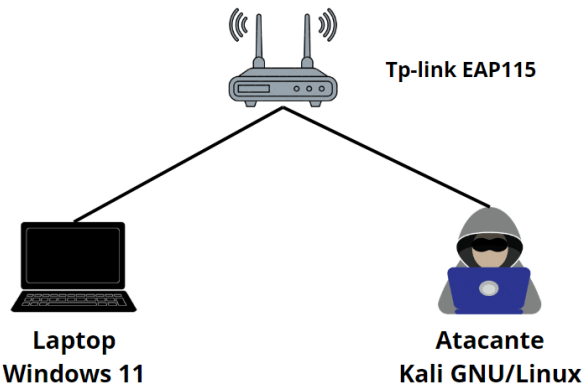

Figura 4.1: Topologia da rede do ambiente teste
Fonte: Elaborada pelo Autor

Aircrack-ng

O *Aircrack-ng* é uma coleção completa de ferramentas para avaliar a segurança de redes *wi-fi*, afirma Aspyct.org (2020). Ele se concentra em diferentes áreas da segurança *wi-fi*:

- Monitoramento: Captura de pacotes e exportação de dados para arquivos de texto para posterior processamento por ferramentas de terceiros.
- Ataque: Ataques de repetição, desautenticação, pontos de acesso falsos e outros por meio de injeção de pacotes.
- Teste: Verificação das capacidades de cartões *wi-fi* e *drivers* (captura e injeção).
- Quebra: WEP e WPA PSK (WPA 1 e 2).

Ainda segundo Aspyct.org (2020), é uma ferramenta de linha de comando, o que permite uso de *scripts* avançados. Muitas interfaces gráficas aproveitaram essa funcionalidade. Ele funciona principalmente no Linux, mas também no *Windows*, *macOS*, *FreeBSD*, *OpenBSD*, *NetBSD*, assim como no *Solaris* e até mesmo no *eComStation 2*.

Hashcat

Segundo Limited (2021), o *Hashcat* oferece suporte a cinco modos únicos de ataque para mais de 300 algoritmos de *hash* altamente otimizados. Atualmente, o *hashcat* suporta Unidades de Processamento Central (CPUs), Unidades de Processamento Gráfico (GPUs) e outros aceleradores de hardware no Linux, e possui recursos para facilitar a quebra distribuída de senhas.

De acordo com Limited (2021),a ferramenta oferece vários modos de ataque para obter uma cobertura eficaz e complexa do espaço de chaves de um *hash*. Alguns desses modos são:

- Ataque de Força Bruta
- Ataque de Combinação
- Ataque de Dicionário
- Ataque de Impressão Digital
- Ataque Híbrido
- Ataque de Máscara
- Ataque de Permutação
- Ataque de Tabela de Consulta

Hping3

Segundo Limited (2015), o *hping3* é uma ferramenta de rede capaz de enviar pacotes ICMP/UDP/TCP personalizados e exibir respostas do alvo, semelhante ao ping que faz com respostas ICMP. Ele lida com fragmentação e corpo/arbitrário do pacote e tamanho, e pode ser usado para transferir arquivos sob protocolos suportados. Usando o *hping3*, é possível testar regras de *firewall*, realizar varreduras de portas (falsificadas), testar o desempenho da rede usando diferentes protocolos, fazer descoberta de *MTU* de caminho, realizar ações semelhantes a *traceroute* sob diferentes protocolos, identificar sistemas operacionais remotos, auditar pilhas TCP/IP destaca Limited (2015).

DoS-Tester 802.11

Özgün Kültekin (2021) afirma que trata-se de uma ferramenta escrita com a linguagem *Python*, que testa alguns ataques de negação de serviço (DoS) em redes IEEE 802.11, inundando pacotes desejados.

Oferece uma interface de linha de comando simples, que permite aos usuários injetar facilmente pacotes e testar suas redes. Özgün Kültekin (2021) ressalta ainda que o *DoS Tester* realiza com sucesso os seguintes ataques:

- Inundação de Solicitação de Autenticação
- Inundação de Solicitação de Associação

Nmap

Segundo Lyon (2021), o *Nmap*, abreviação de *Network Mapper*, é uma poderosa ferramenta de código aberto amplamente utilizada para exploração de redes e auditoria de segurança. Projetado para escanear redes, descobrir hosts e serviços, além de identificar vulnerabilidades e configurações de segurança, afirma Lyon (2021). O autor afirma também que ele fará isso utilizando uma variedade de técnicas de varredura, como *TCP SYN scan*, *TCP connect scan*, *UDP scan* e outros métodos avançados, o *Nmap* fornece aos administradores de sistemas e profissionais de segurança uma visão detalhada da infraestrutura de rede e dos dispositivos conectados. Ainda segundo Lyon (2021) sua flexibilidade e extensibilidade permitem que os usuários

personalizem e automatizem tarefas de varredura e análise de segurança de acordo com suas necessidades específicas.

PRTG Network Monitor

O *PRTG Network Monitor* é uma ferramenta de monitoramento que oferece uma ampla gama de recursos para ajudar os administradores de rede a garantir o desempenho e a disponibilidade de suas infraestruturas de TI, destaca PaesslerAG (2022). O *PRTG* permite monitorar dispositivos de rede, servidores, aplicativos, serviços e tráfego de rede em tempo real, fornecendo uma visão abrangente do ambiente de rede.

Segundo PaesslerAG (2022) com o PRTG, os administradores podem monitorar vários aspectos da rede, incluindo o status dos dispositivos, o uso da largura de banda, a disponibilidade de serviços críticos, a performance de aplicativos, entre outros. A ferramenta utiliza uma abordagem baseada em sensores, onde cada sensor é responsável por monitorar um aspecto específico da rede. Os usuários podem configurar e personalizar esses sensores de acordo com suas necessidades de monitoramento.

Omada Controller

O Omada Software, desenvolvido pela *TP-Link*, representa uma solução abrangente de gerenciamento de rede, destaca Tp-link (2022). Focado especialmente em redes *Wi-Fi*, segundo, Tp-link (2022) o Omada Software tem como objetivo fornecer um controle centralizado e eficaz sobre a infraestrutura de rede. Por meio dessa plataforma, é possível realizar a configuração e monitoramento de uma variedade de dispositivos de rede, incluindo pontos de acesso sem fio, *switches* e roteadores, de maneira intuitiva e eficiente. Ainda de acordo com Tp-link (2022), entre os recursos oferecidos pelo Omada Software estão o provisionamento automático de dispositivos, a implementação de políticas de segurança, a supervisão do tráfego de rede e a análise do desempenho. Essa solução se destaca como uma ferramenta valiosa para empresas que necessitam gerenciar e manter infraestruturas de rede complexas, compostas por diversos pontos de acesso e dispositivos interconectados.

4.2 Pilares dos ataques

Como ressaltado na Seção 2.2.7, os ataques às redes sem fio têm se tornado mais frequentes na atualidade, principalmente devido à grande propagação dessas redes e a facilidade na coleta de suas informações. Para esta pesquisa, estabelecemos dois pilares fundamentais para a definição dos ataques: o consumo de recursos e a interceptação de dados.

No âmbito do primeiro pilar, o consumo de recursos refere-se à utilização de qualquer recurso do sistema, incluindo processamento, memória, armazenamento e largura de banda, por

parte de um processo específico. Este conceito está intrinsecamente ligado à quantidade de recursos que uma tarefa ou processo consome durante sua execução. Em consequência, qualquer ataque direcionado a este pilar comprometerá a disponibilidade do sistema. Nessa perspectiva, os ataques mais significativos escolhidos, que impactam diretamente este pilar, são o DOS *(Denial of Service)* e o DDOS *(Distributed Denial of Service)*, sendo que a distinção principal entre eles é que o primeiro é executado de uma única fonte, enquanto o segundo envolve múltiplas fontes. Para os ataques DOS, especificamos os ataques: *Syn Flood, Auth Flood, Assr Flood* explicados na sessão 2.2.7 e para os ataques DDOS foram usados os mesmos ataques com a diferença que se faz necessário a criação de uma *botnet* para que a distribuição da negação de serviço fosse realizada. Importante destacar que em nosso *Test Bed* implementamos apenas os ataques DOS e para os ataques DDOS usamos como referencia a base teórica e os resultados desses ataques.

No que diz respeito ao segundo pilar, a interceptação de dados abrange qualquer ação que resulte na obtenção, monitoramento ou captura de informações transmitidas entre dispositivos por meio de uma rede. Este processo está intrinsecamente ligado à segurança e privacidade das informações em trânsito, tornando-se suscetível a comprometimentos caso seja alvo de ataques. Nesse contexto, qualquer investida direcionada a este pilar tem o potencial de comprometer a confidencialidade e integridade do sistema. Dentre os ataques mais proeminentes que afetam diretamente este pilar, escolhemos o *Eavesdrop* e o *Evil Twin* para ser retratado nessa pesquisa. Destaca-se que conforme explicado na 2.2.7, o *Eavesdrop* tem por sua característica algumas variações como o *Man-in-the-middle* e o Ataque de escuta. Importante destacar também que no nosso *Test bed* foi implementado apenas o *Eavesdrop*. Com relação ao *Evil Twin* foi usado referencias teóricas e resultados dos outros ataques.

4.3 Modelagem: Árvore de ataque e métricas de avaliação

No escopo dessa pesquisa definimos que o objetivo final do atacante será prejudicar o alvo final, através os pilares escolhidos: interceptação de dados e o consumo de recursos. A partir disso, construímos a árvore de ataque destacando cada ataque escolhido em cada um dos pilares. Nos nós folhas foi definido as ações necessárias pelo atacante para concluir o ataque de maneira que cada ação está ordenada da esquerda para direita respectivamente. Cada nó folha foi definido com base nos ataques feitos no ambiente de teste. A Figura 4.2 é o resultado dessas definições.

Conforme destacado na Seção 2.3, é essencial estabelecer métricas de avaliação para conduzir uma análise de risco. Neste estudo, priorizamos duas métricas principais: o risco e a viabilidade do ataque. Para comparar os riscos associados aos diferentes tipos de ataques selecionados, adotamos a Equação 4.1, a qual considera a probabilidade, o custo e o impacto do ataque, (Baldwin, 2007). Ao integrar o custo à fórmula de risco, buscamos aprimorar a precisão na tomada de decisões com maior assertividade. Não apenas consideraremos a probabilidade e

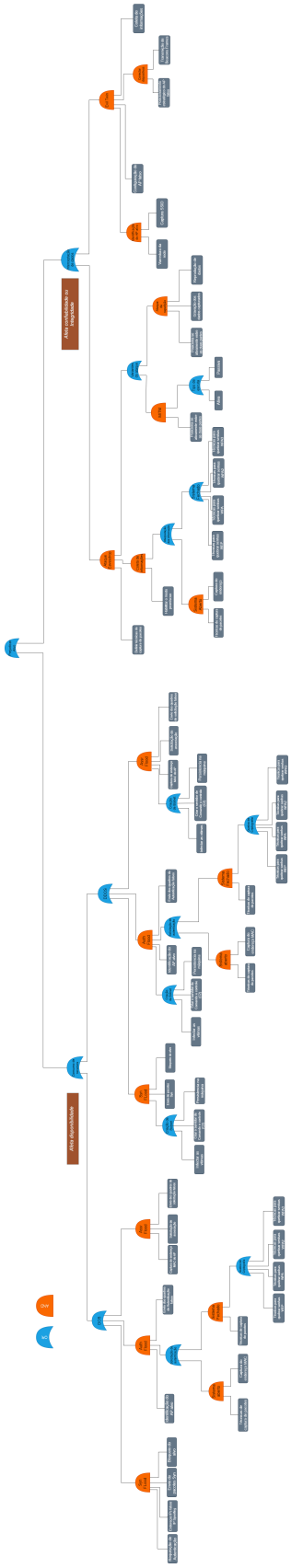

Figura 4.2: Árvore de ataque
Fonte: Elaborada pelo Autor

o impacto de um evento de segurança, mas também o custo associado, o que nos possibilitará priorizar recursos e esforços de mitigação com base na relação de custo-benefício. Essa abordagem abrangente nos permite não só identificar os riscos mais críticos, mas também otimizar a alocação de recursos para maximizar a eficácia das medidas de segurança.

$$Risco = (\frac{Probabilidade}{Custo}) \times Impacto \tag{4.1}$$

Para calcularmos o custo, probabilidade e impacto de cada ataque, atribuímos valores a cada folha da árvore de ataque construída levando em consideração nosso *expertise* na área. Em seguida, para determinar os valores intermediários e da raiz, aplicamos as regras de propagação das equações conforme expostas na Tabela 4.2, que considera as regras lógicas de conjunção (AND) e disjunção (OR) aplicadas na árvore de ataque.

Métrica	Equações	
	AND	OR
Custo	$\sum_{i=1}^{n} \text{custo}_i$	$\frac{\sum_{i=1}^{n} \text{prob}_i \times \text{custo}_i}{\sum_{i=1}^{n} \text{prob}_i}$
Probabilidade	$\prod_{i=1}^{n} \text{prob}_i$	$1 - \prod_{i=1}^{n} (1 \text{ - } \text{prob}_i)$
Impacto	$\frac{10^n - \prod_{i=1}^{n} (10 - \text{Impacto}_i)}{10^{(n-1)}}$	$\text{MAX}_{i=1}^{n} \text{Impacto}_i$

Tabela 4.2: Regras de propagação de métricas
Fonte: Baldwin (2007)

Para determinar os valores atribuídos às folhas da nossa árvore de ataque, adotamos uma abordagem baseada na definição de intervalos pré-definidos para cada métrica considerada. Em cada intervalo numérico, associamos um valor qualitativo correspondente, facilitando assim a interpretação dos dados resultantes. Tabelas 4.3, 4.4 e 4.5 mostra com mais detalhes.

Essa estratégia permitiu uma avaliação mais detalhada e precisa dos diferentes aspectos analisados. Por exemplo, ao considerar o custo de um ataque, estabelecemos faixas específicas, como "maior que 10k", "entre 4k e 10k", "entre 2k e 4k"e "menor que 2k". A cada uma dessas faixas, atribuímos um valor qualitativo que reflete a dificuldade associada à realização do ataque, indo desde "bem difícil"até "simples", foi usado como referência valores adotados por Maciel (2018). Essa abordagem padronizada nos permitiu comparar e contrastar diferentes ataques com base em critérios objetivos e consistentes. Além disso, possibilitou uma análise mais aprofundada das implicações e dos riscos envolvidos em cada cenário, fornecendo informações valiosas para a tomada de decisões estratégicas.

Para definir a viabilidade dos ataques foi usado métricas como custo monetário do ataque (C), notabilidade do ataque (Not), e a habilidade técnica (Ht) necessária para o atacante realizar o ataque. Para avaliar a viabilidade entre os distintos ataques, utilizamos a Equação 4.2. Para detalhes adicionais, consulte R. Ingoldsby (2021). Da mesma maneira que as métricas do risco, também definimos um intervalo pré-definido para a notabilidade do ataque e a habilidade técnica. Tabelas 4.6 e 4.7 mostram com mais detalhes, o custo usado foi o mesmo definido na

Custo	
Valor	Qualitativo
> 10k	Bem Difícil
4k - 10k	Difícil
2k - 4k	Mediano
< 2k	Simples

Tabela 4.3: Custo monetário
Fonte: Elaborada pelo Autor

Probabilidade	
Valor	Qualitativo
$0 \leq 0.3$	Muito baixa
$0.3 \leq 0.5$	Baixa
$0.5 \leq 0.8$	Média
$0.8 \leq 1$	Alta

Tabela 4.4: Probabilidade
Fonte: Elaborada pelo Autor

Impacto	
Valor	Qualitativo
$1 \leq x < 4$	Muito baixa
$4 \leq x < 7$	Baixa
$7 \leq x < 9$	Média
$9 \leq x \leq 10$	Alta

Tabela 4.5: Impacto
Fonte: Elaborada pelo Autor

Tabela 4.3.

Notabilidade	
Valor	Qualitativo
$1 \leq x < 4$	Muito baixa
$4 \leq x < 7$	Baixa
$7 \leq x < 9$	Média
$9 \leq x \leq 10$	Alta

Tabela 4.6: Notabilidade
Fonte: Elaborada pelo Autor

Habilidade Técnica	
Valor	Qualitativo
$1 \leq 3$	Usuário comum (não precisa de habilidade técnica)
$4 \leq 6$	Usuário Curioso (*script kiddie*)
$7 \leq 8$	Usuário avançado (profissionais na área)
$9 \leq 10$	Usuário expert (especialistas)

Tabela 4.7: Habilidade Técnica
Fonte: Elaborada pelo Autor

$$Viabilidade = \sqrt[n]{\prod_{i=1}^{n} \mathrm{C}_i * \mathrm{Not}_i * \mathrm{Ht}_i} \tag{4.2}$$

Foi definido os valores de cada métrica nas folhas e para os nós intermediários foi adotado duas abordagens: para portas lógicas do tipo AND os valores da notabilidade e habilidade técnica foram gerados por meio da Equação 4.3 e 4.4 já para portas OR foi gerados por meio da Equação 4.5 e 4.6.

$$Ht = \mathrm{MAX}_{i=1}^{n} \mathrm{Ht}_i \tag{4.3}$$

$$Not = \mathrm{MAX}_{i=1}^{n} \mathrm{Not}_i \tag{4.4}$$

$$Ht = \frac{\sum_i^n \mathrm{Ht}_i}{n} \tag{4.5}$$

$$Not = \frac{\sum_i^n \mathrm{Not}_i}{n} \tag{4.6}$$

Importante destacar que a viabilidade foi definida apenas para os 8 ataques estudados, já o risco estará presente em todo escopo da árvore.

Como abordado na Seção 2.3.5, para quantificar o risco de maneira eficaz, é crucial desenvolver uma métrica qualitativa. Isso irá nos ajudar a avaliar e comparar os diferentes níveis de risco associados a várias situações ou eventos. Ao criar essa escala para viabilidade e risco, teremos uma visão mais clara e estruturada dos ataques, auxiliando na tomada de decisões e auxiliando na implementação de mitigações. As Tabelas 4.8 e 4.9 abordam as classificações qualitativas aplicadas em cada uma. Para comparar os valores de risco e viabilidade, foi necessário normalizar os resultados usando a técnica de *Min-Max Scaling*, conforme demonstrado na

Equação 4.7. Nesta equação, o *valor norm* representa a saída final normalizada, enquanto *X* é o valor de entrada, *X min* é o menor valor encontrado no ramo da árvore e *X max* é o maior valor encontrado no ramo da árvore.

Risco	
Valor	Qualitativo
$0.0 \leq r < 0.2$	Irrelevante
$0.2 \leq r < 0.4$	Baixo
$0.4 \leq r < 0.6$	Médio
$0.6 \leq r < 0.8$	Alto
$0.8 \leq r \leq 1.0$	Crítico

Tabela 4.8: Risco
Fonte: Elaborada pelo Autor

Viabilidade	
Valor	Qualitativo
$0.0 \leq v < 0.2$	Irrelevante
$0.2 \leq v < 0.4$	Baixo
$0.4 \leq v < 0.6$	Médio
$0.6 \leq v < 0.8$	Alto
$0.8 \leq v \leq 1.0$	Crítico

Tabela 4.9: Viabilidade
Fonte: Elaborada pelo Autor

$$\text{valor}_{\text{norm}} = \frac{X - \text{X}_{\text{min}}}{\text{X}_{\text{max}} - \text{X}_{\text{min}}} \tag{4.7}$$

5

Resultados e Discussões

Com base no que foi discutido no capítulo anterior, neste capítulo serão apresentados os resultados obtidos da implementação e cálculo das métricas adotadas, apresentando um acompanhamento visual dos resultados, assim como uma visão comparativa de cada ataque realizado.

5.1 Valores Quantitativos

Como ressaltado na Seção 2.3.5, para realizarmos uma análise de impacto ela pode ter uma abordagem qualitativa ou quantitativa. A quantitativa utiliza uma metodologia baseada em números, métricas e cálculos matemáticos, dados esses coletados das equações e métricas explicadas no capitulo anterior.

Para facilitar a compreensão, a árvore de ataque foi subdividida em quatro subárvores principais: DOS, DDOS, *Eavesdrop* e *Eviltwin*. Embora os cálculos tenham sido realizados considerando a árvore completa (ver a Figura 4.2), a divisão tem o objetivo de aprofundar a análise visualmente e auxiliar na abordagem por partes. Isso significa que examinaremos cada subárvore separadamente para uma compreensão mais detalhada dos riscos e viabilidades envolvidos em diferentes tipos de ataques. Cada subárvore foi elaborada de forma sequencial, nos nós folhas da esquerda para a direita, detalhando as ações que o atacante precisa executar para efetivar o ataque.

Na subárvore que aborda os ataques de negação de serviço (DoS), estabelecemos um nó intermediário para classificar cada ação relacionada aos ataques *Syn-Flood*, *Auth-Flood* e *Assr-Flood*. Em seguida, atribuímos a cada nó folha valores para métricas como custo, impacto, probabilidade, habilidade técnica e notabilidade. Para os nós intermediários, aplicamos as regras de distribuição mencionadas no capítulo anterior, a fim de garantir uma análise abrangente e precisa dos potenciais riscos e impactos associados a esses ataques. Com base nos cálculos realizados, observamos que o ataque *Auth-Flood* apresenta um risco e viabilidade associados

mais elevados em comparação aos demais avaliados no ramo, o que ressalta sua relevância em termos de potenciais danos e ameaças. Para uma análise mais específica, consulte a Figura 5.1.

Na subárvore que aborda os ataques de negação de serviço distribuídos (DDoS), incorporamos os mesmos ataques utilizados no DOS, acrescentando, entretanto, a criação da *botnet* em cada ramificação. Tal aspecto é de extrema importância para o atacante, pois a execução eficaz desse tipo de ataque demanda a conexão com diversas máquinas simultaneamente para causar a negação do serviço. Atribuímos valores às métricas, como custo, impacto, probabilidade, habilidade técnica e notabilidade, em cada nó folha. Para os nós intermediários, empregamos a mesma abordagem utilizada na subárvore DOS. Com base nos resultados dos cálculos efetuados, constatamos que o *Auth-Flood* apresenta uma viabilidade mais acentuada em comparação aos demais ataques, sugerindo ser o mais propício para um potencial atacante, considerando métricas como habilidade técnica, custo e notabilidade. Por outro lado, quando falamos sobre o risco associado, o Syn-Flood apresenta um valor superior aos demais, destacando-se também como relevante para eventuais danos potenciais. Veja a Figura 5.2.

Na subárvore relacionada ao ataque *Eavesdrop*, delineamos as ações necessárias para a conclusão do ataque nos nós intermediários, enquanto nas folhas destacamos as ações iniciais que o atacante deve realizar. Assim como nas demais subárvores, atribuímos valores às métricas nos nós folhas, tais como custo, impacto, probabilidade, habilidade técnica e notabilidade, e procedemos aos cálculos para distribuição desses valores nos nós intermediários, utilizando o mesmo método adotado nas outras subárvores. Ao finalizar os cálculos, constatamos que o risco associado é relativamente baixo em comparação com outros ataques até então considerados, entretanto, a viabilidade do ataque é mais elevada. Veja a figura 5.3.

Já na subárvore referente ao ataque *Evil Twin*, estruturamos os nós intermediários e folhas, delineando cada ação que o atacante deve executar da esquerda para a direita até alcançar o resultado almejado. Seguindo o mesmo padrão das outras subárvores, procedemos à atribuição e cálculo das métricas, concluindo que o risco associado a esse ataque é extremamente baixo em comparação com os demais ataques abordados. No entanto, ele se destaca pela sua alta viabilidade, sugerindo que seria uma escolha viável para o atacante. Essa análise sugere que, embora o ataque em si represente um baixo risco para o usuário, a sua alta viabilidade o torna uma ameaça significativa. Veja a Figura 5.4.

Por fim, após calcular as métricas de distribuição em cada nó da árvore que representa os ataques, os resultados agregados na raiz da árvore são apresentados na Figura 5.5. Essas métricas agregadas fornecem uma visão geral dos riscos e viabilidades associados à árvore de ataque como um todo, consolidando os dados de todas as subárvores em uma única visualização. Legenda das métricas usadas nas subárvores[1]

[1] [C] = Custo [I] = Impacto [P] = Probabilidade [R] = Risco [Not] = Notabilidade [Ht] = Habilidade técnica

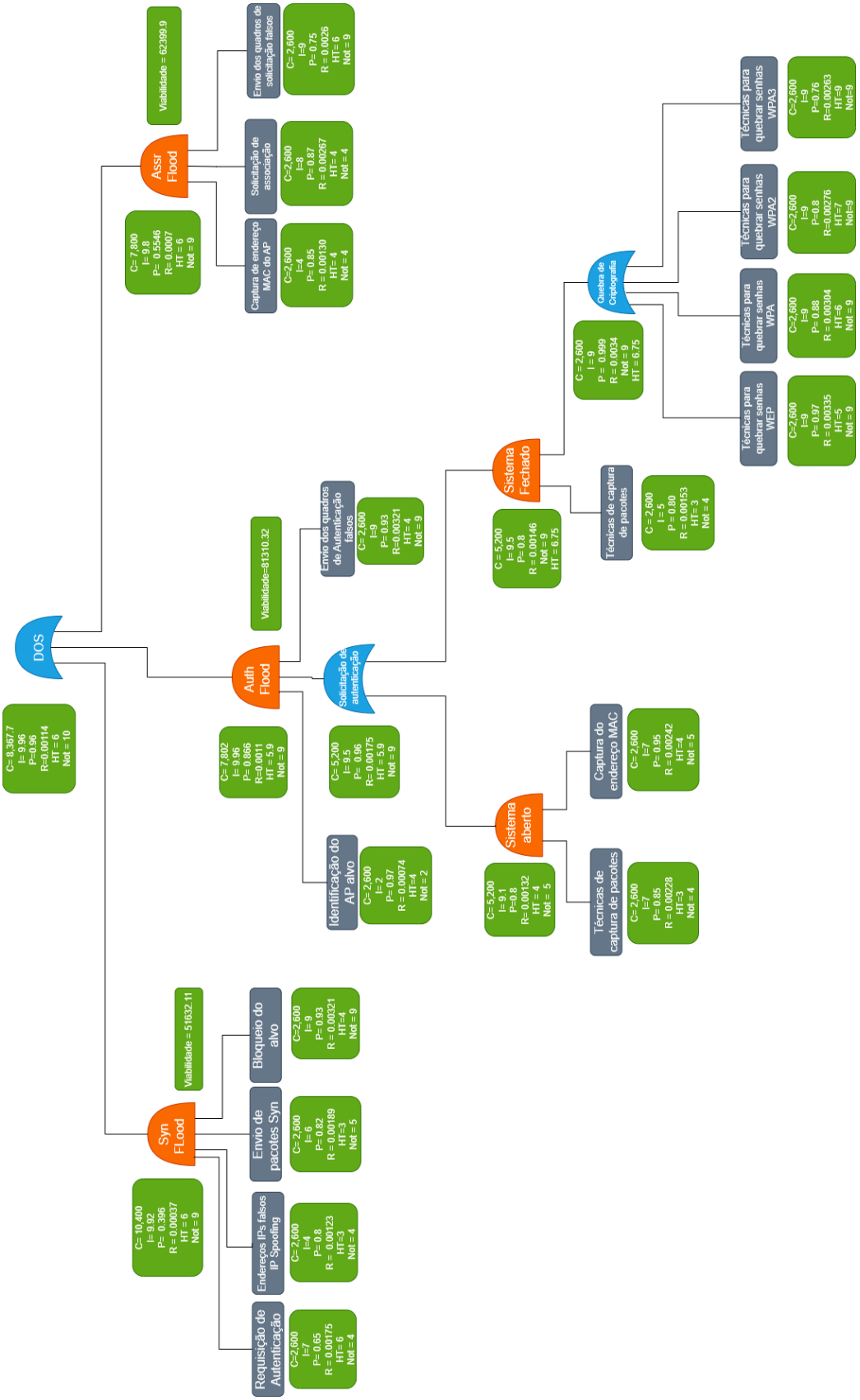

Figura 5.1: Subárvore DOS

Fonte: Elaborada pelo Autor

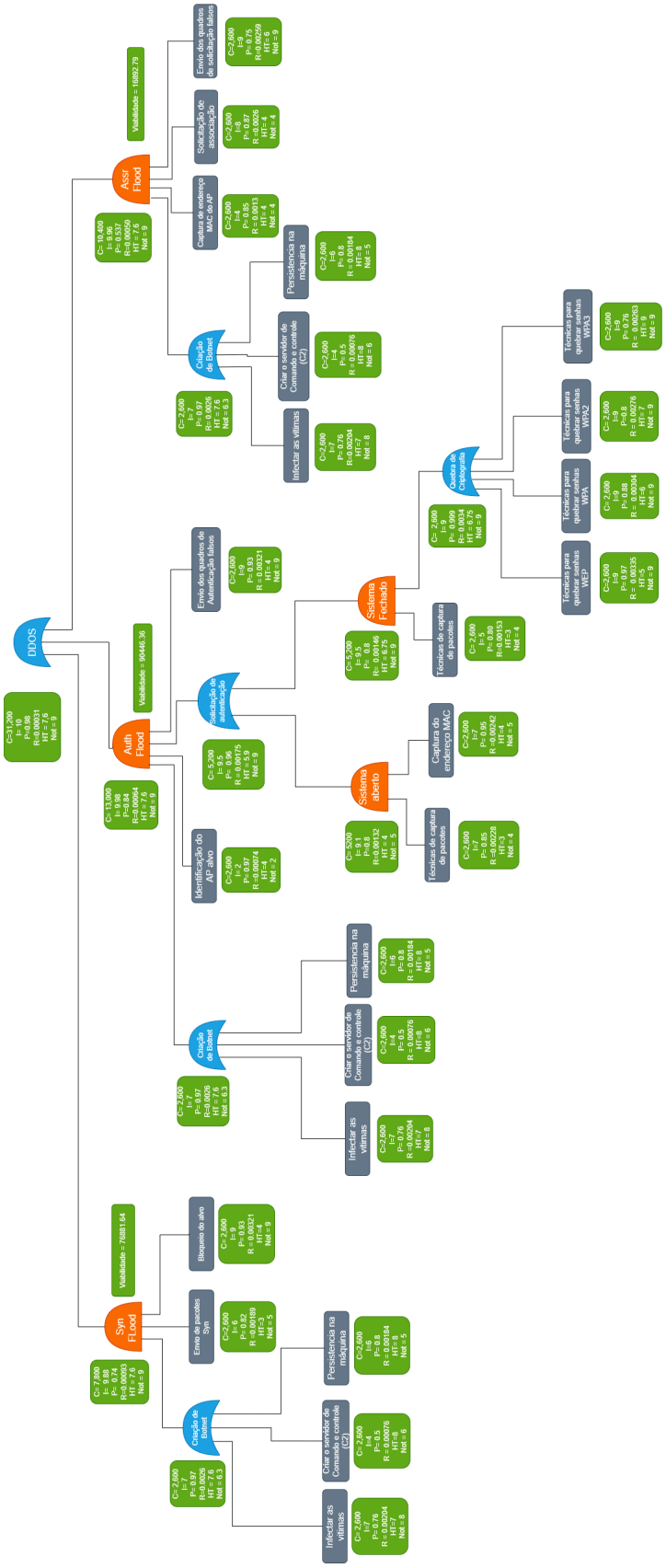

Figura 5.2: Subárvore DDOS

Fonte: Elaborada pelo Autor

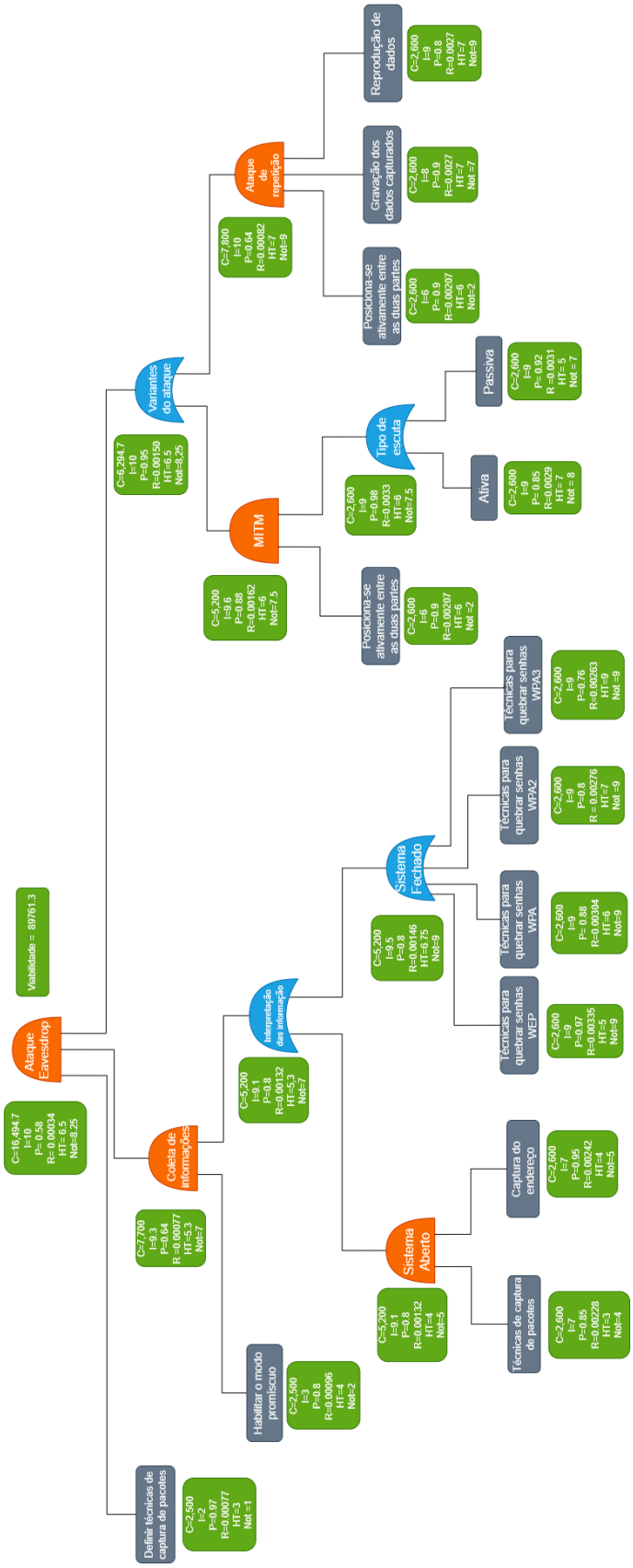

Figura 5.3: Subárvore Eavesdrop

Fonte: Elaborada pelo Autor

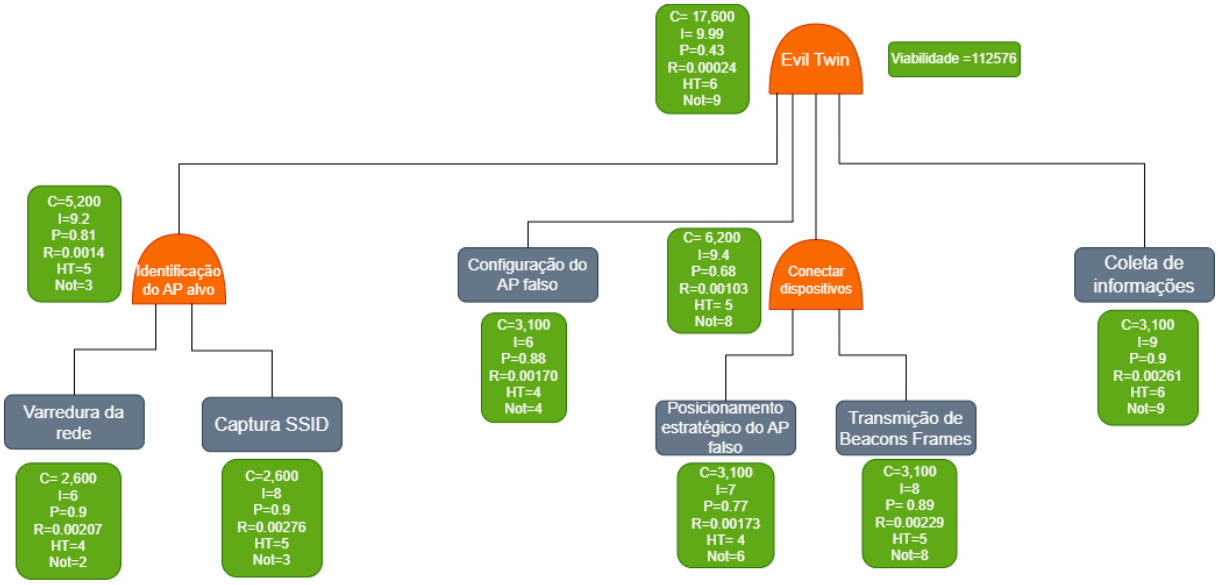

Figura 5.4: Subárvore EvilTwin

Fonte: Elaborada pelo Autor

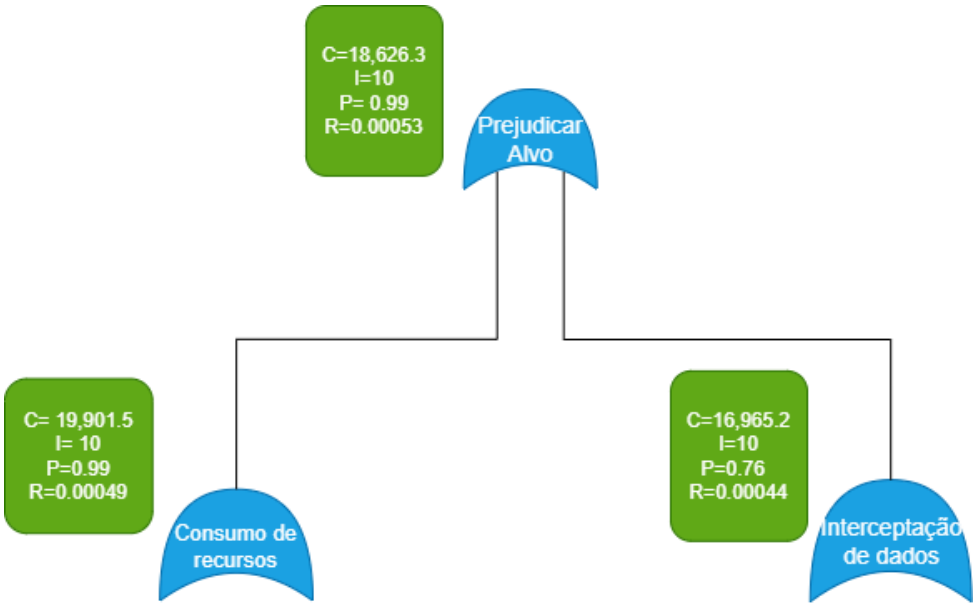

Figura 5.5: Subárvore Raiz

Fonte: Elaborada pelo Autor

5.2 Valores Qualitativos

Após atribuímos valores quantitativos às métricas associadas aos nós folhas, iremos classificar os valores definidos de forma qualitativa, utilizando como referência as Tabelas 4.3, 4.4, 4.5, 4.6 e 4.7. Esta classificação qualitativa nos permitirá avaliar os resultados de maneira mais abrangente, identificando padrões e tendências nos dados. Ao analisarmos as figuras resultantes, poderemos visualizar cada métrica em relação aos diferentes ataques relacionados anteri-

ormente, o que facilitará a comparação entre eles em termos de custo, probabilidade, impacto, habilidade técnica, notabilidade e viabilidade. Essa análise gráfica oferecerá uma perspectiva valiosa sobre a distribuição e o impacto de cada métrica nos diferentes tipos de ataques. Veja as Figuras 5.6,5.7, 5.8, 5.9 e 5.10.

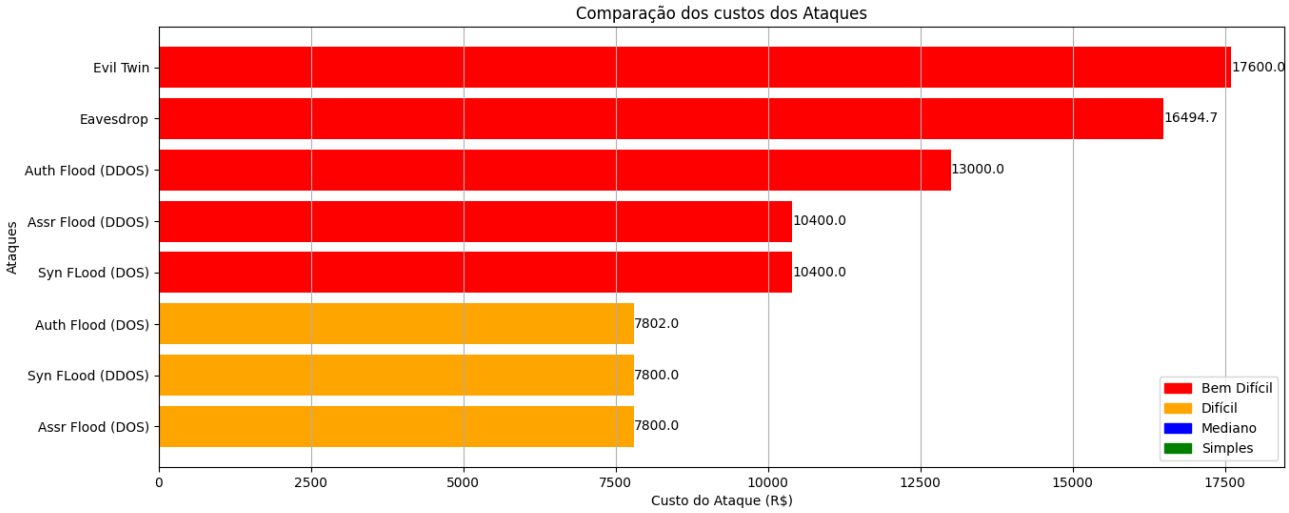

Figura 5.6: Comparação dos custos entre os ataques
Fonte: Elaborada pelo Autor

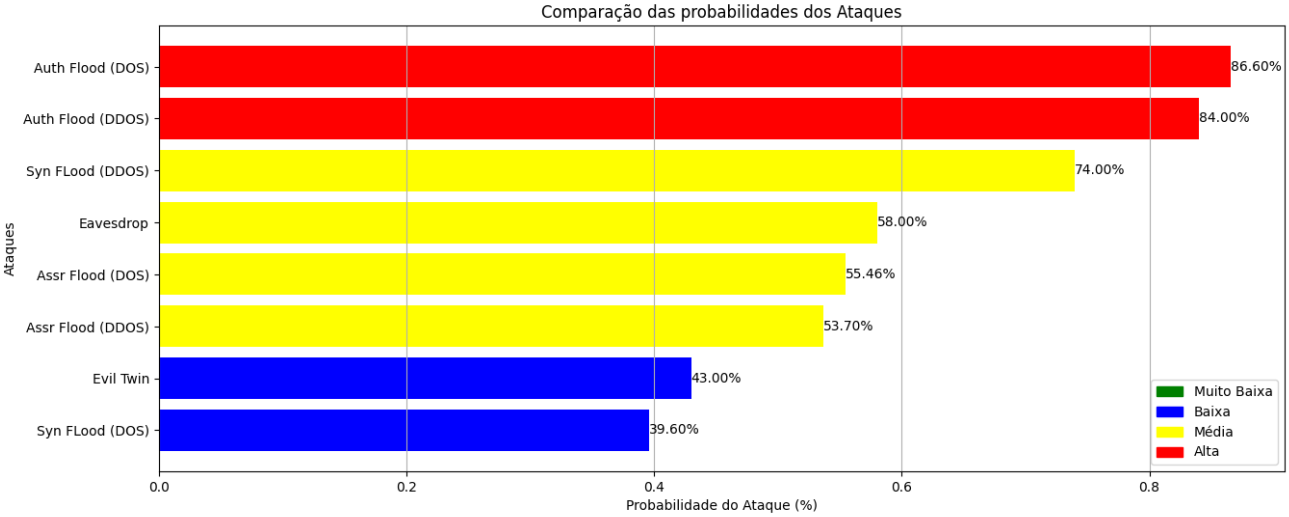

Figura 5.7: Comparação das probabilidades entre os ataques
Fonte: Elaborada pelo Autor

A partir dessas métricas foram calculados os valores dos riscos e a viabilidade do ataque. Ao calcular e avaliar esses valores, somos capacitados a tomar decisões estratégicas e operacionais mais informadas, alinhadas com as necessidades e desafios específicos do ambiente que criamos. Esses cálculos nos permitem identificar não apenas a probabilidade e o potencial

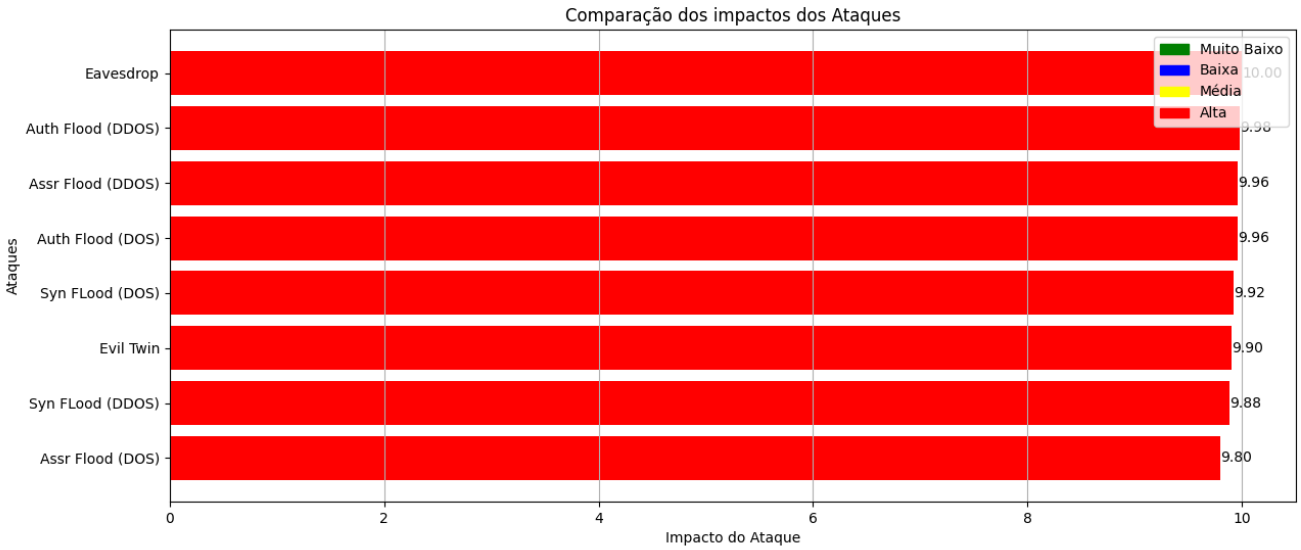

Figura 5.8: Comparação dos Impactos entre os ataques
Fonte: Elaborada pelo Autor

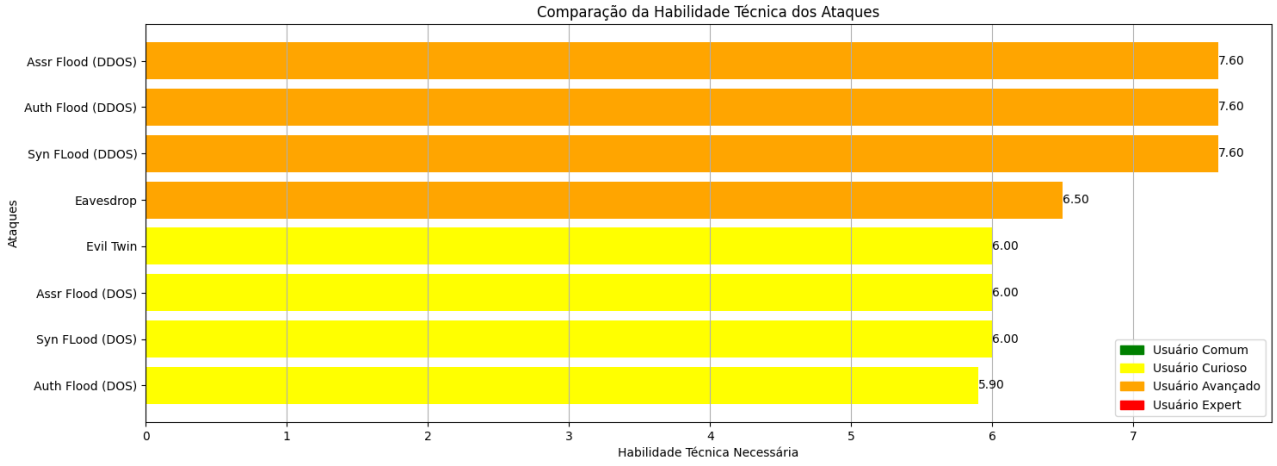

Figura 5.9: Comparação das Habilidades técnicas entre os ataques
Fonte: Elaborada pelo Autor

impacto de diferentes tipos de ataques, mas também a capacidade realista de um adversário em explorar vulnerabilidades específicas. Essa compreensão aprofundada nos permite priorizar adequadamente os recursos e esforços de mitigação, concentrando-os nas ameaças mais críticas e realistas que enfrentamos. Estas análises de risco e viabilidade nos capacita a desenvolver estratégias de segurança mais eficazes e adaptáveis, aumentando nossa capacidade de antecipar, detectar e responder a ameaças cibernéticas com agilidade e precisão. As Figuras 5.11 e 5.12 classificam os valores de risco e viabilidade entre cada ataque. A Figura 5.16 trás ainda uma visão comparativa entre essas duas métricas.

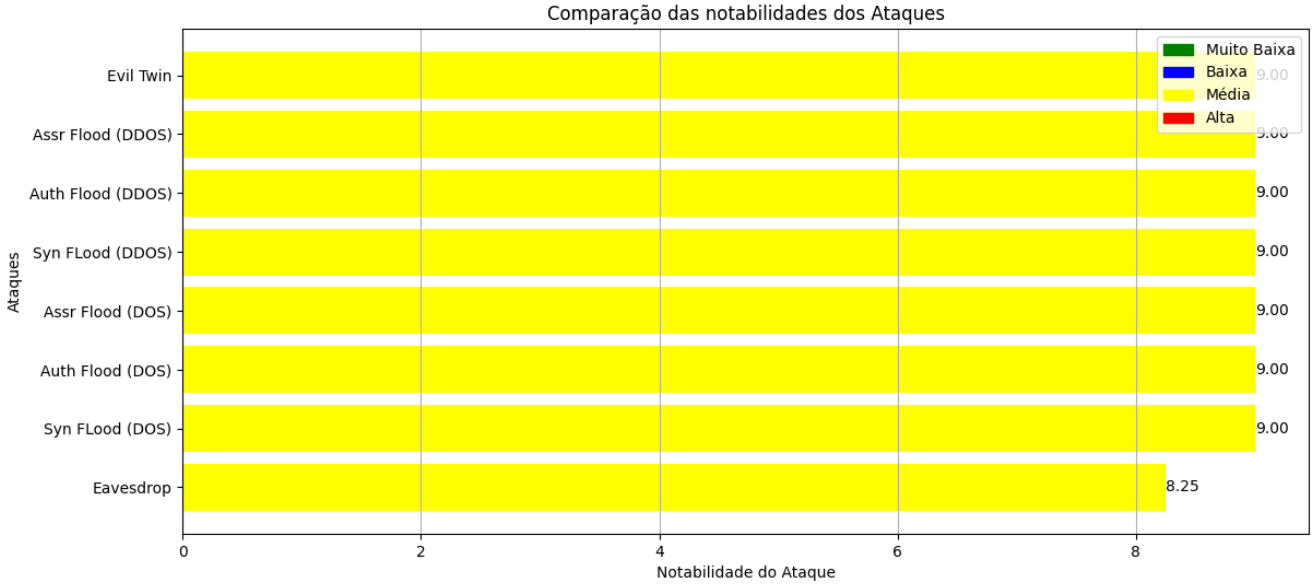

Figura 5.10: Comparação das Notabilidades técnicas entre os ataques
Fonte: Elaborada pelo Autor

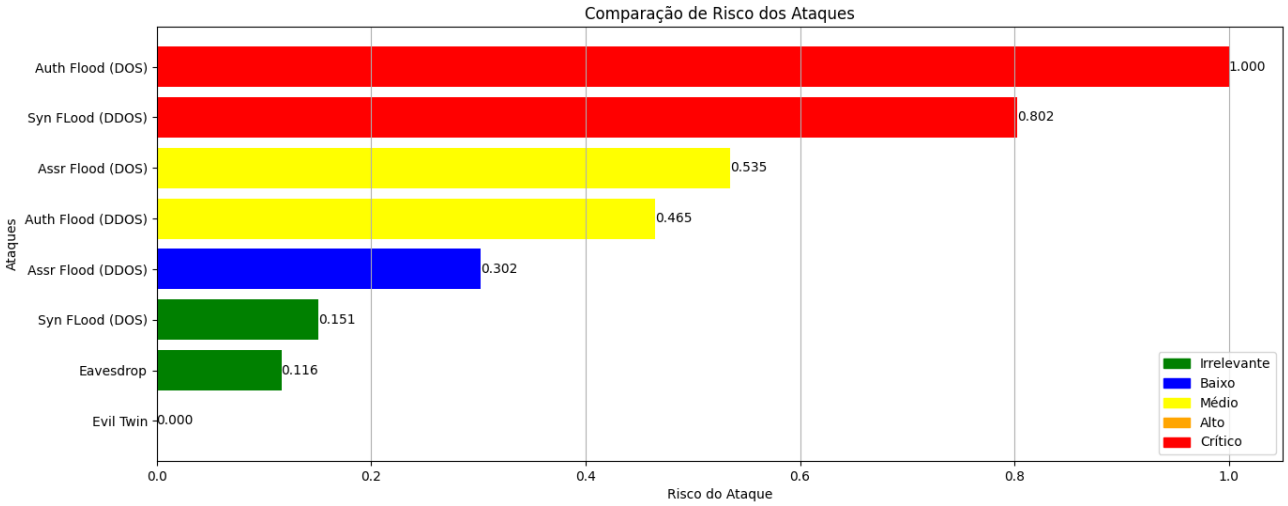

Figura 5.11: Risco entre os ataques
Fonte: Elaborada pelo Autor

Análise dos valores finais

Entre os 8 ataques abordados nesta pesquisa, destaca-se o *Evil Twin* como aquele com o maior custo associado à sua execução, seguido de perto pelo *Eavesdrop* e pelo *Auth Flood* do tipo DDOS. Esta classificação pode ser visualizada na Figura 5.6. No que diz respeito à probabilidade de ocorrência, observa-se que o *Auth Flood* do tipo DOS ocupa o primeiro lugar, com uma probabilidade de ocorrência de 86,6%. Em seguida, vêm o *Auth Flood* do tipo DDOS e o *Syn Flood* do tipo DDOS. Esses dados são ilustrados na Figura 5.7. Quando se trata do impacto

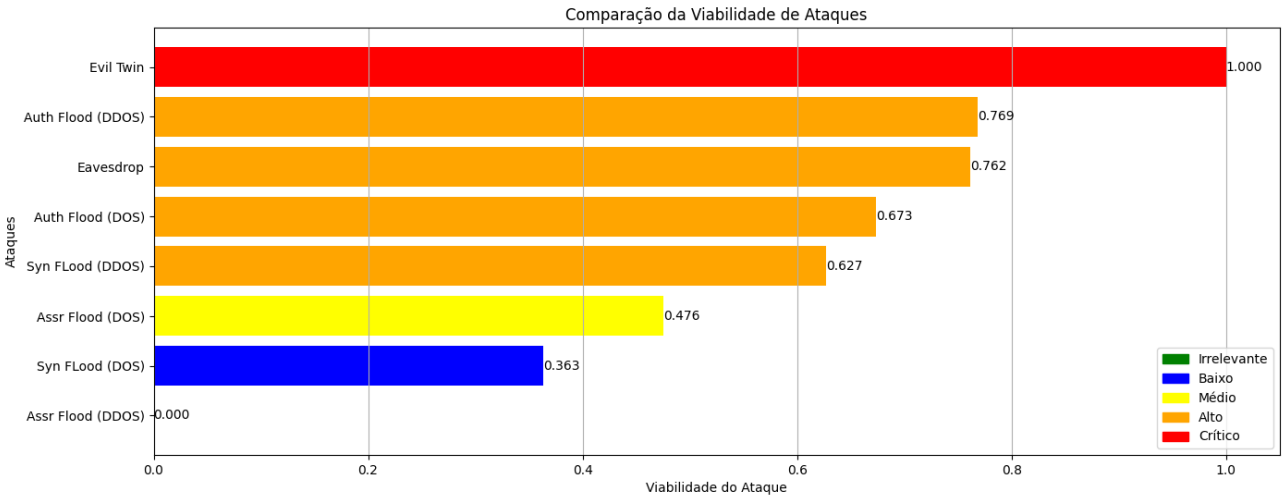

Figura 5.12: Viabilidade dos ataques
Fonte: Elaborada pelo Autor

potencial desses ataques nos sistemas dos usuários, todos eles apresentam um nível elevado, quase atingindo o máximo de 10. Mais informações sobre os impactos podem ser encontradas na Figura 5.8. Quanto à habilidade técnica necessária para realizar esses ataques, percebe-se que os ataques do tipo DDOS exigem um nível mais avançado de habilidade do usuário para sua execução eficaz. Esta análise é detalhada na Figura 5.9. Em relação à notabilidade de cada ataque, isto é, à sua capacidade de ser detectado pelo usuário ou pelo administrador da rede, todos eles têm uma classificação média. Consulte a Figura 5.10 para mais detalhes. Quanto aos riscos associados a cada ataque, destaca-se que o *Auth Flood* do tipo DDOS possui o maior risco, seguido pelo *Syn Flood* do tipo DDOS e pelo *Assr Flood* do tipo DOS. Estes dados são visualizados na Figura 5.11. Por fim, ao comparar a viabilidade de cada ataque, observa-se que o *Evil Twin* está em primeiro lugar, seguido pelo *Auth Flood* do tipo DDOS e pelo *Eavesdrop*. Mais informações sobre a viabilidade de cada ataque podem ser encontradas na Figura 5.12.

Ao compararmos os pilares de ataques selecionados para esta pesquisa, que são o consumo de recursos e a interceptação de dados, observamos que os ataques relacionados ao primeiro pilar tendem a ter valores mais altos de custo, risco e probabilidade em comparação com o segundo pilar. As Figuras 5.13, 5.14 e 5.15 representam esses valores.

Conforme destacado na Seção 2.3.7, ter uma visão sobre a viabilidade dos ataques e o risco atrelados a cada um deles é de grande importância para realizarmos a priorização na construção de controles de segurança para esses ataques. Ao examinar a Figura 5.16 podemos perceber que o *Evil Twin* possui uma viabilidade extremamente alta, contudo um risco muito baixo, ou seja a capacidade de um atacante explorar com sucesso as vulnerabilidades atreladas a esse ataque, levando em consideração as métricas adotadas como, custo, habilidade técnica e notabilidade é praticamente certa, contudo a magnitude das consequências negativas que isso vai causar ao usuário, levando em consideração métricas como, custo, probabilidade e impacto é quase nula.

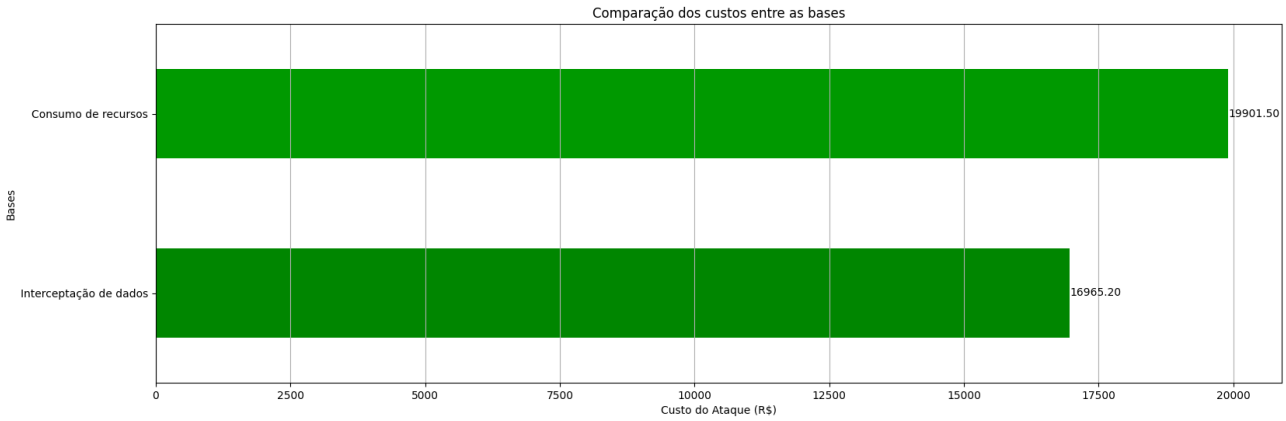

Figura 5.13: Comparação de custos entre os pilares dos ataques
Fonte: Elaborada pelo Autor

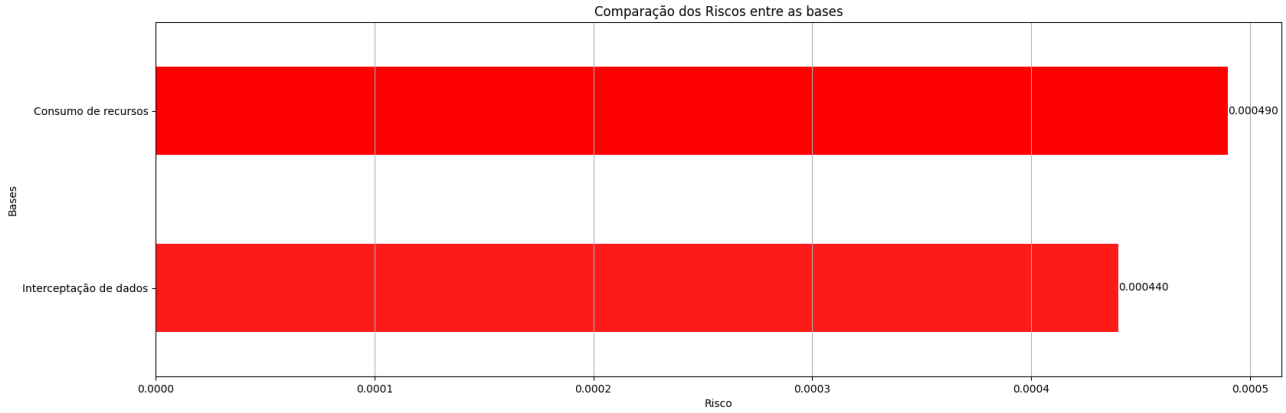

Figura 5.14: Comparação de riscos entre os pilares dos ataques
Fonte: Elaborada pelo Autor

Logo, o *Evil Twin* é um ataque que se for realizado uma tentativa de execução pelo atacante, ele provavelmente irá conseguir realizar sem muita dificuldade, porém não terá tantas repercussões no ambiente quando comparado aos diferentes ataques escolhidos.

Ao realizar uma análise comparativa entre todos os ataques investigados, torna-se evidente que o *Auth Flood* (DOS) e o *Syn Flood*(DDOS) emergem como os mais preocupantes em termos de potencial impacto no ambiente de segurança. Além disso, sua viabilidade para execução é consideravelmente alta, sugerindo que os atacantes têm uma probabilidade significativa de sucesso ao tentar realizá-los. Portanto, ao planejar e implementar medidas de segurança, é imperativo priorizar a mitigação desses ataques, dada sua potencial gravidade e probabilidade de ocorrência.

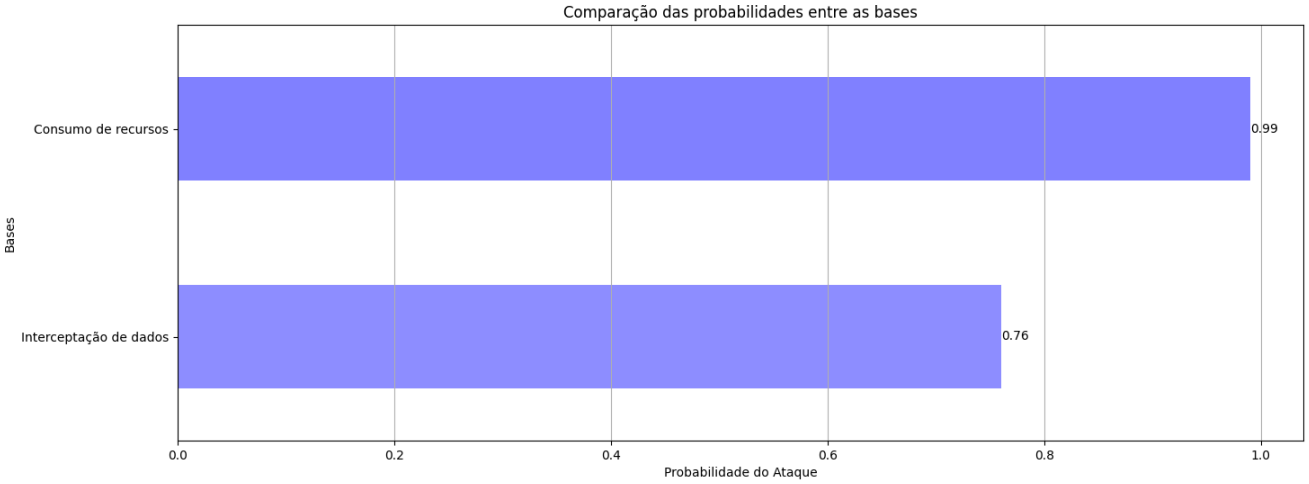

Figura 5.15: Comparação de probabilidade entre os pilares dos ataques
Fonte: Elaborada pelo Autor

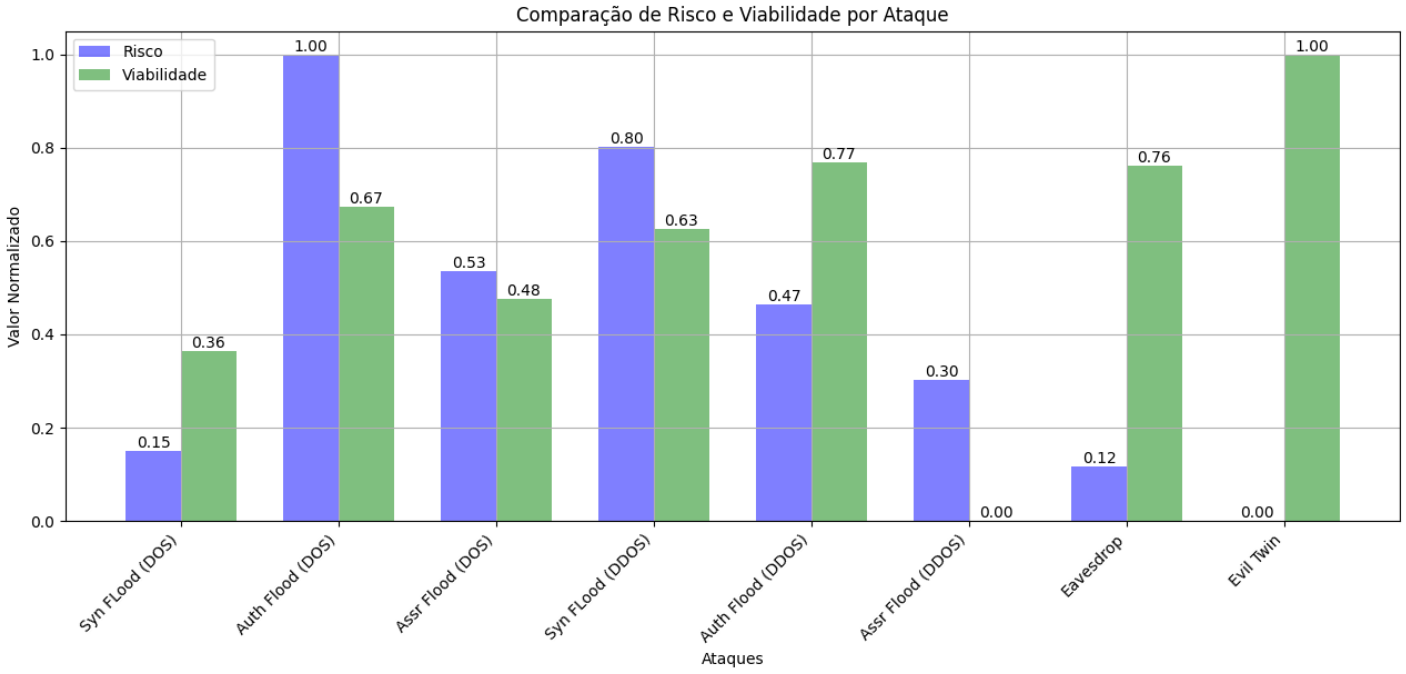

Figura 5.16: Comparação de Risco e Viabilidade por Ataque
Fonte: Elaborada pelo Autor

6

Conclusão

O presente estudo se dedicou a uma análise abrangente das ameaças em redes Wi-Fi 802.11n, adotando uma abordagem fundamentada no conceito de risco e utilizando uma estrutura de árvore de ataques. Essa metodologia considerou métricas comportamentais específicas para estimar não apenas a probabilidade de um ataque ocorrer em um ambiente determinado, mas também avaliar o potencial impacto que tais incidentes poderiam causar aos usuários. Como resultado dessa investigação detalhada, conforme evidenciado no capítulo anterior, é possível afirmar que os objetivos delineados foram alcançados com sucesso. Ao realizar uma análise comparativa entre todos os ataques investigados, destacam-se o *Auth Flood* (DOS) e o *Syn Flood* (DDOS) como os mais preocupantes em termos de potencial impacto no ambiente de segurança. Portanto, recomenda-se priorizar esses ataques ao desenvolver métodos de correção e prevenção.

Este estudo oferece ainda contribuições significativas ao campo da segurança da informação, destacando-se pela abordagem inovadora na classificação e priorização de ameaças em ambientes de rede. A metodologia proposta proporciona percepções valiosas para a identificação e correção de vulnerabilidades, representando uma ferramenta essencial tanto para administradores de rede quanto para profissionais de segurança cibernética. Além disso, o modelo desenvolvido irá oferecer uma visão clara e prioritária das ameaças mais relevantes em seu ambiente. Essa perspectiva direcionada permite a implementação de controles de segurança específicos e eficazes, voltados para mitigar os riscos identificados. Assim, espera-se que esse método contribua de maneira significativa para diminuir a incidência de ataques bem-sucedidos em redes sem fio, promovendo, consequentemente, um ambiente mais seguro e protegido.

Limitações

As principais limitações identificadas estão vinculadas à estimativa dos valores iniciais das métricas nas folhas de cada tipo de ataque. Cada valor deve ser atribuído considerando a expertise

e a pertinência do indivíduo que está desenvolvendo o modelo. Portanto, é aconselhável buscar contribuições de profissionais do ramo, ou a realização de uma pesquisa a fim de obter uma visão abrangente e especializada sobre cada ataque e vulnerabilidade selecionada. Essas informações desempenham um papel crucial no resultado final da análise. Caso não sejam estimadas com precisão desde o início, podem resultar em valores que não refletem adequadamente a realidade do ambiente em questão.

Além disso, tivemos outro ponto de limitação que foi o ambiente trabalhado para coleta dos resultados. Como as atividades foram realizadas em um ambiente de *Test bed*, com um número de usuários limitado, os resultados acabam sendo restritos para esse ambiente. Resultados diferentes seriam encontrados caso o ambiente fosse um corporativo com um número maior de usuários.

Trabalhos Futuros

A relevância do tema explorado nesta monografia implica em diversas possibilidades para estender e aprimorar a pesquisa no futuro. Entre os trabalhos futuros planejados, destaca-se uma investigação mais aprofundada das equações empregadas para calcular as métricas, explorando técnicas de *machine learning* e abordagens probabilísticas com o intuito de aprimorar a precisão dos resultados obtidos. Além disso, contempla-se a expansão do conjunto de métricas analisadas, visando identificar e classificar as vulnerabilidades associadas a cada tipo de ataque de forma mais abrangente. Adicionalmente, propõe-se a elaboração de uma análise defensiva por meio da construção de uma árvore de defesa do cenário em estudo, permitindo o desenvolvimento de estratégias mais eficazes para mitigar os diferentes tipos de ataques identificados. Essas perspectivas representam contribuições significativas para o avanço do conhecimento e a aplicação prática dos resultados obtidos neste trabalho.

Referências bibliográficas

Agrawal, M. T. S. N. C. (2018). A survey of different dos attacks on wireless network. *International Institute for Science, Technology and Education (IISTE)*.

Aspyct.org (2020). Aircrack-ng. Disponível em: https://www.aircrack-ng.org/. Acesso em: 14 de Março 2024.

Baldwin, T. E. R. B. R. R. C. R. M. G. R. (2007). The use of attack and protection trees to analyze security for an online banking system. *Hawaii International Conference on System Sciences*.

Boris Bellalta, Luciano Bononi, R. B. A. K. (2015). Next generation ieee 802.11 wireless local area networks: Current status, future directions and open challenges. *Elsevier*.

CloudFlare (2021). Ataque de inundação syn. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/syn-flood-ddos-attack/. Acesso em: 05 de Janeiro 2024.

Coles, I. T. M. J. (2021). *Threat Modeling A Pratical Guide for Development Teams*, volume 1. O'Reilly.

D. Gallagher, P. (2012). Guide for conducting risk assessments. *NIST*.

Datta, S. (2023). What are replay attacks? Disponível em: https://www.baeldung.com/cs/replay-attacks#:~:text=A%20replay%20attack%20is%20a,because%20it%27s%20challenging%20to%20detect. Acesso em: 06 de Janeiro 2024.

de Oliveira Rufino, N. M. (2019). *Segurança de redes sem fio: Aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth*, volume 2. Novatec.

Dezengrini, G. V. E. J. (2022). Os riscos de segurança da informação na utilização de redes sem fio. *TECHFAG MAGAZINE*.

Eclipse (2022). Risk likelihood: Meaning, usage, calculation, and more. Disponível em: https://www.eclipsesuite.com/risk-likelihood/#:~:text=Low%20Likelihood%

3A%20Will%20seldom%20occur,certain%20to%20occur%20(100%25). Acesso em: 04 de Janeiro 2024.

Fortinet (2022). What is eavesdropping? Disponível em: https://www.fortinet.com/br/resources/cyberglossary/eavesdropping. Acesso em: 10 de Janeiro 2024.

Giavaroto, S. C. R. (2013). *BackTrack Linux Auditoria e teste de invasão em redes de computadores*. Ciência Moderna.

Guard, H. (2023). The differences between risk management, risk assessment, and risk analysis. Disponível em: https://www.healthguardsecurity.com/difference-between-risk-management-and-risk-assessment/. Acesso em: 02 de Fevereiro 2024.

Hintezbergen, J. (2018). *Fundamentos de Segurança da informação com base na ISO 27001 e na ISO 27002*. Brasport.

HSC Brasil (2020). Evil twin wifi: o que é e como funciona este ataque. Disponível em: https://www.hscbrasil.com.br/evil-twin-wifi/. Acesso em: 05 de Janeiro 2024.

ISO27002 (2022). *Information security, cybersecurity and privacy protection — Information security controls*, volume 3. International Organization for Standardization.

James, K. (2023). Replay attack vs. man-in-the-middle attack. Disponível em: https://cybersecurityforme.com/replay-attack-vs-man-in-the-middle-attack/. Acesso em: 06 de Janeiro 2024.

Jorge Marin, TecMundo (2023). Brasil é líder do ranking de ataques ddos na américa latina pela 10ª vez; entenda. Disponível em: https://www.tecmundo.com.br/seguranca/272995-brasil-lider-ranking-ataques-ddos-america-latina-10-vez-entenda.htm. Acesso em: 04 de Dezembro 2023.

Kurose, K. W. R. J. E. (2022). *Computer Networking A Top Down approach*, volume 8. Pearson Education Limited.

Limited, O. S. (2015). hping3 usage example. Disponível em: https://www.kali.org/tools/hping3/. Acesso em: 14 de Março 2024.

Limited, O. S. (2021). hashcat usage examples. Disponível em: https://www.kali.org/tools/hashcat/. Acesso em: 14 de Março 2024.

Lyon, G. (2021). Nmap. Disponível em: https://nmap.org/. Acesso em: 14 de Março 2024.

Maciel, P. M. E. G. C. M. J. D. J. A. R. (2018). Impact of a ddos attack on computer systems: An approach based on an attack tree model. *IEEE Computer Society*.

Mendes, D. R. (2016). *Redes de Computadores, Teoria e Prática*, volume 2. Novatec.

Networks, S. (2022). Wi-fi eavesdropping. Disponível em: https://semfionetworks.com/blog/wi-fi-eavesdropping/. Acesso em: 06 de Janeiro 2024.

Oliveira, R. C. Q. (2018). *Tópicos de Segurança da Informação*. Senac.

PaesslerAG (2022). Powerful easy-to-use software to monitor your entire network. Disponível em: https://www.paessler.com/prtg/prtg-network-monitor. Acesso em: 14 de Março 2024.

R. Ingoldsby, T. (2021). Attack tree-based threat risk analysis. *Amenaza Technologies Limited*, 4.

Scheier, B. (2004). *Secrets Lies*. Robert Ipsen.

Tenenbaum, N. F. A. S. (2021). *Redes de Computadores*, volume 6. Bookman.

Thant, M. A. C. A. K. P. (2019). Ieee 802.11 attacks and defenses. *ResearchGate*.

Tp-link (2022). Omada software controller v5. Disponível em: https://www.tp-link.com/br/support/download/omada-software-controller/. Acesso em: 14 de Março 2024.

Tucker, J. F. B. E. (2012). *Risk Analysis and the security survey*, volume 4. Elsevier.

Wrightson, T. (2014). *Segurança de redes sem fio: Guia do iniciante*, volume 2. Bookman.

Zhu, D. R. S. D. H. (2011). A novel attack tree based risk assessment approach for location privacy preservation in the vanets. *IEEE Comunications Society*.

Özgün Kültekin (2021). Dos-tester-802.11. Disponível em: https://github.com/oz9un/dos-tester-802.11/blob/main/README.md. Acesso em: 14 de Março 2024.