ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

Rodrigo Olivato Ribeiro

TESTES DE VULNERABILIDADE COMO FERRAMENTA DE PROTEÇÃO CIBERNÉTICA DAS REDES SEM-FIO IEEE 802.11

Resende
2022

	APÊNDICE III (TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL) AO ANEXO B (NITCC) ÀS DIRETRIZES PARA A GOVERNANÇA DA PESQUISA ACADÊMICA E DA DOUTRINA NA AMAN	**AMAN 2022**

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

TÍTULO DO TRABALHO: TESTES DE VULNERABILIDADE COMO FERRAMENTA DE PROTEÇÃO CIBERNÉTICA DAS REDES SEM-FIO IEEE 802.11
AUTOR: RODRIGO OLIVATO RIBEIRO

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulgá-lo por publicação em revista técnica da Escola ou outro veículo de comunicação do Exército.

A Academia Militar das Agulhas Negras poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou da Direção de Ensino da Academia Militar das Agulhas Negras.

Resende, 18 de Abril de 2022.

Cad Rodrigo Olivato Ribeiro

Dados internacionais de catalogação na fonte

R484t RIBEIRO, Rodrigo Olivato
Testes de vulnerabilidade como ferramenta de proteção cibernética das redes sem-fio IEEE 802.11. / Rodrigo Olivato Ribeiro – Resende; 2022. 40 p. : il. color. ; 30 cm.

Orientador: Anderson Henrique De Moura
TCC (Graduação em Ciências Militares) - Academia Militar das Agulhas Negras, Resende, 2022.

1.Cibernética 2. Cibersergurança 3.Wi-Fi 4.Aircrack-ng I. Título.

CDD**:** 355

Ficha catalográfica elaborada por Jurandi de Souza CRB-5/001879

Rodrigo Olivato Ribeiro

TESTES DE VULNERABILIDADE COMO FERRAMENTA DE PROTEÇÃO CIBERNÉTICA DAS REDES SEM-FIO IEEE 802.11

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Orientador: Cap Anderson Henrique de Moura

Resende
2022

Rodrigo Olivato Ribeiro

TESTES DE VULNERABILIDADE COMO FERRAMENTA DE PROTEÇÃO CIBERNÉTICA DAS REDES SEM-FIO IEEE 802.11

Monografia apresentada ao Curso de Graduação em Ciências Militares, da AcademiaMilitar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Aprovado em 01 de Junho de 2022

Banca examinadora:

Anderson Henrique de Moura, Capitão
(Orientador)

Felipe Barcelllos Brasil, Capitão
(Avaliador)

Júlio César Lacerda do Nascimento, 1º Tenente
(Avaliador)

Resende
2022

Dedico este trabalho ao Agulhas Negras Security (Grêmio de Cibernética da AMAN), o qual me auxiliou nos estudos durante o período acadêmico, de forma que este TCC pudesse ser escrito, e que sirva para futuras pesquisas a quem for de interesse.

AGRADECIMENTOS

Agradeço, primeiramente, à minha mãe, Marília Aparecida Olivato Ribeiro, e meu pai, Renato de Lima Ribeiro, que estiveram sempre presentes nos momentos mais importantes e marcantes da minha formação.

À minha companheira, Celia Regina Spadacin da Silva, que sempre me apoiou nos momentos difíceis da minha formação e serviu de motivação para estar sempre buscando o aprimoramento técnico-profissional.

RESUMO

TESTES DE VULNERABILIDADE COMO FERRAMENTA DE PROTEÇÃO CIBERNÉTICA DAS REDES SEM-FIO IEEE 802.11

AUTOR: Rodrigo Olivato Ribeiro

ORIENTADOR: Anderson Henrique de Moura

O uso da tecnologia *Wi-Fi* para acessar às redes está cada vez mais presente nas Forças Armadas devido à sua maior flexibilidade que a conexão cabeada. Porém, sua tecnologia possui vulnerabilidades que podem ser exploradas por agentes mal-intencionados; e no contexto atual de Guerra da Informação, a insegurança na dimensão informacional pode trazer efeitos indesejados para a instituição. Portanto, o Oficial do Exército Brasileiro deve estar em condições de realizar a proteção cibernética das redes sem-fio sob a sua responsabilidade, seja em operações ou dentro da OM. A fim de enriquecer o trabalho, foi realizada uma pesquisa por meio de um formulário para questionar, por amostragem, os Cadetes da AMAN sobre o seu grau de conhecimento sobre o assunto; e uma pesquisa bibliográfica, que ajudou a compreender a ciência por trás da exploração de vulnerabilidades Wi-Fi, de forma a entender como protegê-las melhor.

Palavras-chave: Cibernética; Cibersegurança; Wi-Fi; Aircrack-ng.

ABSTRACT

PENTEST AS A CYBERSECURITY TOOL FOR IEEE 802.11 WIRELESS NETWORKS

AUTHOR: Rodrigo Olivato Ribeiro

ADVISOR: Anderson Henrique de Moura

The use of Wi-Fi technology to access networks is increasingly present in the Armed Forces due to its greater flexibility than the wired connection. However, its technology has vulnerabilities that could be exploited by malicious agents; and in the current context of Information Warfare, insecurity in the informational dimension can bring unwanted effects to the institution. Therefore, a Brazilian Army Officer must be able to carry out cybernetic protection of wireless networks under his responsibility, whether in operations or within the OM. In order to enrich this work, it was made a form survey with the AMAN Cadets about how far their knowledge about wireless vulnerabilities is, and a bibliographic research, which helped to understand the science behind the exploitation of Wi-Fi networks in order to understand how to protect them better.

Keywords: Cybernetics. Cybersecurity. Wi-Fi. Aircrack-ng.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

O uso das redes de dados como meio de fluxo de informações traz benefícios como velocidade e praticidade, porém aumenta consideravelmente a exposição a ataques cibernéticos. Um intruso pode invadir um sistema e obter informações sensíveis sem deixar vestígios. Portanto uma rede segura depende da conscientização dos usuários da rede, que devem ter atitudes favoráveis à proteção cibernética (IR 20-26, 2001).

Uma alternativa de acesso à rede é através da tecnologia Wi-Fi a qual está cada vez mais presente no dia a dia das Organizações Militares do Exército Brasileiro, por conferir maior flexibilidade ao usuário que a conexão cabeada. Ela é utilizada para tramitar processos simples e administrativos, mas, também, informações do mais alto nível de confidencialidade.

Dentro do contexto da Guerra Cibernética, um ataque às redes sem fio pode ser realizado por qualquer indivíduo, de forma muito simples, mas ao mesmo tempo muito danosa para a segurança das informações sigilosas, portanto conhecer sobre as vulnerabilidades dessa tecnologia pode auxiliar em políticas de proteção cibernética.

Os ataques à rede *Wireless* são pouco ruidosos, de forma que uma tropa não-adestrada dificilmente detectaria sua atuação, portanto deve-se criar políticas de segurança de forma a não comprometer sua segurança.

Buscando difundir o conhecimento sobre técnicas de proteção cibernética para redes Wi-Fi, o trabalho iniciará pela delimitação do problema, seguido de um referencial teórico divido em uma parte doutrinária, onde há o alinhamento da doutrina militar com os objetivos da pesquisa, e uma parte voltada para o conhecimento básico sobre os protocolos e vulnerabilidades das redes IEEE 802.11. Nos capítulos seguintes, o referencial metodológico elucida os métodos de pesquisa; os resultados e discussões analisam os resultados coletados através do instrumento de pesquisa; e, por fim a conclusão responde o objetivo do trabalho.

Esta pesquisa justifica-se pelo alinhamento com o Plano Estratégico do Exército 2020 – 2023, o qual enquadra a segurança de redes como prioridade 2 entre as linhas de pesquisa aplicáveis aos projetos de desenvolvimento de curto prazo recomendadas pelo Departamento de Cultura e Tecnologia (DCT), na área de pesquisa cibernética (ESTADO MAIOR DO EXÉRCITO, 2019).

1.1 PROBLEMA

Um ataque cibernético é imprevisível, de difícil detecção e de fácil emprego, pois pode ser realizado por qualquer civil, membro de força regular ou irregular sem dificuldade.

Baseado na facilidade em que pode ser realizado um ataque desse nível, permanecer no desconhecimento torna os sistemas do Exército vulneráveis à exploração cibernética alheia. Portanto, através do conhecimento das técnicas de invasão, é possível estruturar uma rede mais robusta, diminuindo o risco de ataques bem-sucedidos.

Quais os benefícios do conhecimento sobre o ataque a redes Wi-Fi para a proteção cibernética das redes utilizadas pela tropa convencional?

1.2 OBJETIVOS

Aspirando esclarecer o problema citado, seguem abaixo os objetivos do trabalho.

1.2.1 Objetivo geral

Compreender o protocolo IEEE 802.11 utilizado na tecnologia Wi-Fi, identificando ferramentas que exploram suas vulnerabilidades, de forma a contribuir para a segurança das informações que trafegam pelas redes sem fio utilizadas pelas Organizações Militares do Exército Brasileiro de todas as armas/ quadros e serviços.

1.2.2 Objetivos específicos

Identificar a necessidade do conhecimento sobre proteção cibernética para a tropa convencional através da doutrina militar.

Abordar o protocolo IEEE 802.11, inclusive suas emendas e criptografias.

Explicar a técnica de exploração de vulnerabilidades da tecnologia Wi-Fi através da ferramenta aircrack-ng.

Testar a relevância do trabalho através de uma pesquisa formulário com Cadetes da AMAN.

2 REFERENCIAL TEÓRICO

2.1 ASPECTOS DOUTRINÁRIOS DA GUERRA CIBERNÉTICA

A partir de 2008, a Estratégia Nacional de Defesa estabelece a responsabilidade pela segurança cibernética a cargo da Presidência da República, e a defesa cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas (EB70-MC-10.211, 2020).

A defesa cibernética pode ser definida como:

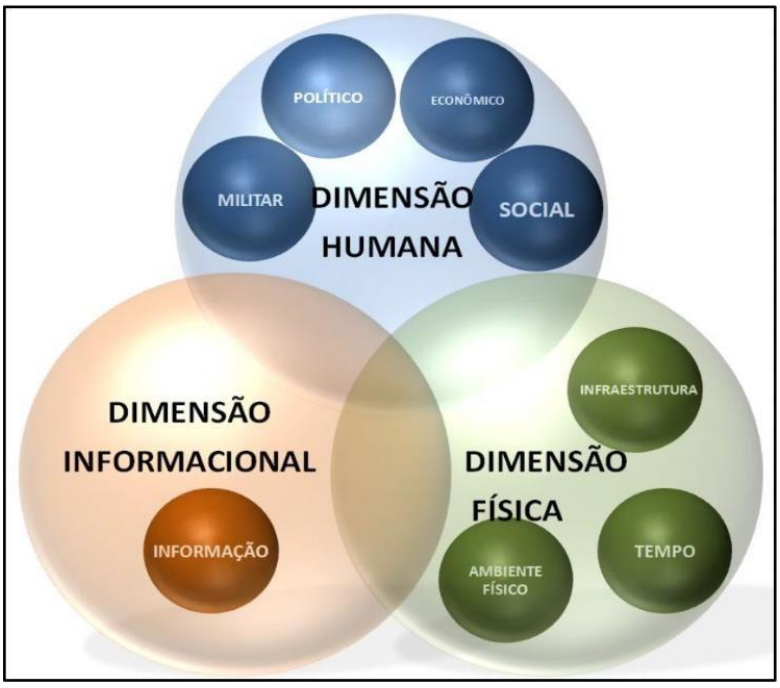
> −A defesa cibernética corresponde ao conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação (Sist Info) de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponentel (EB70-MC-10.211, 2020, p. 2-2).

2.1.1 Fatores operacionais

Os fatores operacionais são aspectos militares ou não, que afetam as operações em amplo aspecto. Para atingir a consciência situacional, é importante ter conhecimento sobre os fatores que englobam o ambiente operacional (EB70-MC-10.211, 2020).

A Guerra Cibernética atua dentro da dimensão informacional, influenciando o fator da informação, o qual se sustenta pela percepção dos sistemas de coleta, processamento, disseminação e emprego das informações das forças amiga, oponente e neutra. E um exemplo de fator operacional é a Guerra da Informação, portanto proteger as redes de dados do Exército pode evitar uma grande vantagem à força oponente (EB70-MC-10.211, 2020).

Figura 1 – Fatores operacionais



Fonte: EB70-MC-10.211, 2020.

2.1.2 O conceito operativo da Guerra Cibernética no Exército Brasileiro

O conceito operativo da Guerra Cibernética no Exército é explicado pelo manual EB70-MC-232 - Guerra Cibernética como:

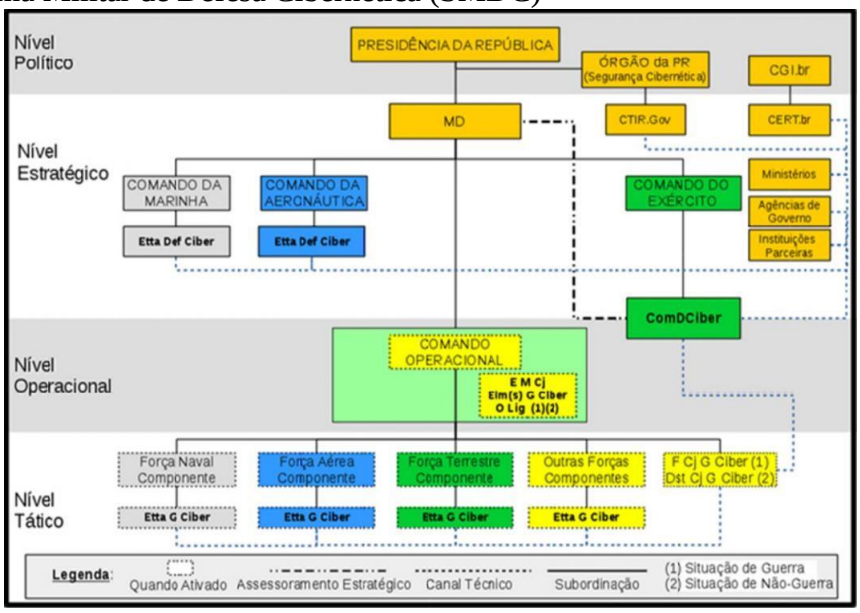
> –Baseando-se nas operações no amplo espectro, para se obter e manter resultados decisivos nas operações, simultânea ou sucessivamente, prevenindo ameaças, gerenciando crises e solucionando conflitos armados, em situações de guerra e de não guerra, há a necessidade de que os comandantes em todos os níveis possuam alto grau de iniciativa e liderança, potencializando a sinergia das forças sob sua responsabilidade. Atualmente, esse conceito operativo requer que, independente do seu nível, os comandantes saibam atuar no espaço cibernético, empregando a capacidade militar terrestre cibernética‖.

2.1.3 Sistema Militar de Defesa Cibernética (SMDC)

Para fins organizacionais, o Exército Brasileiro divide em 4 níveis seu planejamento estratégico, são eles político, estratégico, operacional e tático. No âmbito do nível tático, a Força Terrestre Componente, em situação de guerra ou não-guerra, aciona a Estrutura de Guerra Cibernética, a qual é composta pelas unidades mencionadas posteriormente pela figura 2 (EB70-MC-232, 2017).

Este trabalho foca na atuação da Guerra Cibernética dentro do nível tático, portanto, deve ser levado em consideração as estruturas respectivamente dentro da esfera de suas responsabilidades.

Figura 2 – Sistema Militar de Defesa Cibernética (SMDC)



Fonte: EB70-MC-10.232, 2017.

2.1.4 Capacidades operativas

As capacidades do Sistema de Guerra Cibernética do Exército estão divididas em 3 vertentes: Proteção cibernética, ataque cibernético e exploração cibernética. Este trabalho dedica-se à proteção cibernética, pois tem por objetivo estudar as vulnerabilidades da tecnologia Wi-Fi para diminuir a possibilidade de ataques bem-sucedidos (EB70-MC-10.232, 2017).

A figura 3 cita as capacidades operativas do Sistema de Guerra Cibernética do Exército e explica suas funções (EB70-MC-10.232, 2017).

Figura 3 - Capacidades do Sistema de Guerra Cibernética do Exército (SGCEx)

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: EB70-MC-10.232, 2017.

Cabe ressaltar que, no âmbito da proteção cibernética, podem ser empregadas técnicas de ataque cibernético e exploração cibernética através dos testes de vulnerabilidade, a fim de testar o grau de resiliência da rede (EB70-MC-10.232, 2017).

Portanto, as capacidades operativas se complementam em diversos aspectos, de forma que a proteção cibernética depende de conhecimentos de ataque e exploração cibernética para criar redes ainda mais resilientes.

As capacidades são atribuídas a estruturas diferentes de acordo com seu grau de preparo e especialização. Na figura 4, é possível observar a associação feita entre as estruturas, as capacidades operativas e suas responsabilidades.

Figura 4 – Estruturas operativas de Guerra Cibernética e suas responsabilidades

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (B Com)			X	Realiza a proteção cibernética dos sistemas de informação do grande comando apoiado. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da FTC.
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu comandante será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)			X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC			X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

Fonte: EB70-MC-10.232, 2017.

Como visto na figura, a proteção cibernética preventiva é responsabilidade de todas as OMs integrantes de uma Força Terrestre Componente (EB70-MC-10.232, 2017).

Existem tarefas e atividades relacionadas à proteção cibernética, como a proteção das comunicações, que se refere, dentre outras tarefas, ao exame das estruturas de rede (EB70-MC-10.232, 2017).

2.1.5 Princípios da Segurança da Informação e Comunicações (SIC)

A Segurança da Informação e Comunicações segue alguns princípios básicos que possuem o objetivo de balizar as necessidades dos sistemas de Tecnologia da Informação e Comunicações (TIC), os quais:

> a) Disponibilidade - Propriedade segundo a qual a informação deve ser acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade.
> b) Integridade – Propriedade segundo a qual a informação não deve ser modificada ou destruída de maneira não autorizada ou acidental.
> c) Confidencialidade – Propriedade segundo a qual a informação não deve estar disponível ou ser revelada a pessoa física, sistema, órgão ou entidade não autorizados ou não credenciados.
> d) Autenticidade – Propriedade segundo a qual a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade (EB70-MC-10.232, 2017, p. 2-3).

Um ataque Wi-Fi poderia ferir todos esses princípios em uma rede. Pode indisponibilizá-la, inutilizando e tonando inacessíveis os dados; corrompê-la, modificando ou destruindo os dados que trafegam por ela; expô-la, revelando informações sigilosas ao público; e modificar os dados, ao retirar a autenticidade das informações trafegadas (EB70-MC-10.232, 2017).

2.2 TECNOLOGIA WI-FI

2.2.1 Terminologias

As principais terminologias empregadas acerca da estrutura de uma rede são:

> a) LAN (*Local Area Network*) – Rede de área local. Nesse tipo de topologia há um pequeno número de ativos (computadores) interconectados e sua abrangência é pequena (redes domésticas, pequenas redes empresariais, redes de hotéis etc.).
> b) WLAN (*Wireless Local Area Network*) – Redes LAN que utilizam wireless como forma de comunicação e troca de dados (em vez de cabos).
> MAN (*Metropolitan Area Network*) – Rede de área metropolitana.
> c) Interligação das LANs/WLANs de uma mesma área geográfica.
> d) WAN (*Wide Area Network*) – Rede de longas distâncias. Redes WAN são a interligação das MANs. A internet é um exemplo de WAN.
> e) *Access Point* (AP) ou Ponto de Acesso – O ponto de acesso interconecta a rede local (LAN/WLAN) a outras topologias (WAN e MAN) (MORENO, 2016, p. 40).

O foco deste trabalho está nas redes WLAN e Ponto de Acesso, que se utilizam da tecnologia *wireless* como forma de conexão para criar um ponto de acesso à rede, a qual pode ser uma LAN, MAN ou WAN (MORENO, 2016).

2.2.2 Emendas

A tecnologia WiFi possui divisões que diferenciam as novas gerações. Dentre algumas das diferenças está a largura de banda e as frequências de operação. Portanto para um dispositivo se conectar a um ponto de acesso, eles devem ser de padrões compatíveis.

Segundo Mendes (2007, apud Sousa e Junior, 2007. p. 47):

> –Dentro do padrão IEEE 802.11, há diversos sub padrões desenvolvidos, entre eles podemos destacar alguns, como: o 802.11b: o padrão de rede Wi-Fi mais antigo usando uma frequência de 2,4 GHz e transmitindo dados a 11Mbp; o 802.11g: também utiliza a faixa de frequência de 2,4GHz e transmitindo dados em até 54 Mbps; o 802.11a: utilizada a faixa 5GHz para transmitir a 54Mbps. É um padrão pouco usado no Brasil; e o 802.11n: realiza transmissão da ordem de 300Mbps e usando duas faixas de frequência possíveis (2,4 GHz e 5 GHz) para que os equipamentos desse sub padrão possam se comunicar com todos os demais sub padrões.‖.

2.2.3 Protocolo IEEE 802.11

O IEEE (Instituto de Engenheiros Eletricistas e Eletrônico) possui diversos padrões de tecnologias de rede. O padrão 802.11 é o destinado para a tecnologia Wi-Fi, a qual não é licenciada, portanto não é necessário pagar taxas ou qualquer tipo de licença para a sua implementação e operação. (MORENO, 2016).

2.2.4 Criptografias

As criptografias de rede wireless é uma das estratégias de segurança das transmissões, elas cifram os dados que trafegam pelo ar, de forma que só quem tiver a chave pré-compartilhada possa decifrar o conteúdo que está trafegando na rede. Dessa forma, caso um atacante capture os pacotes, eles estarão criptografados, tornando a sua leitura ilegível. Porém, com o tempo, vulnerabilidades são descobertas e a capacidade de processamento dos computadores quebram com mais facilidade as criptografias, portanto as tecnologias de criptografia precisam ser frequentemente atualizadas (MORENO, 2016).

Inicialmente, foi criada a criptografia *Wired Equivalent Privacy* (WEP), depois o Wi-Fi *Protected Access* (WPA), WPA2 e, atualmente, está sendo desenvolvida a tecnologia WPA3 (MORENO, 2016).

A remessa ou transmissão de documentos sigilosos classificados como secretos, confidenciais ou reservado, quando por meio elétrico ou eletrônico, deverão ser obrigatoriamente criptografados, em sistema de cifra de alta confiabilidade. (IG 10-51, 2019)

Portanto, as criptografias utilizadas pelo Wi-Fi apenas asseguram a segurança das transmissões, devendo-se sempre acrescentar criptografias para assegurar a segurança das comunicações, através de softwares como o Kleópatra, o qual utiliza chaves assimétricas, por exemplo.

2.2.4.1 WEP

A criptografia WEP (*Wired Equivalent Privacy*) é um método simples de criptografia de dados que pode ser utilizado. O problema desse algoritmo é que a senha pode ser facilmente quebrada utilizando *softwares* de criptoanálise. Porém ainda é amplamente utilizado, pois poucos sabem da sua vulnerabilidade (MORENO, 2016).

2.2.4.2 WPA

Em 2002, a WFA (*Wi-Fi Alliance*) desenvolveu a criptografia WPA (Wi-Fi *Protected Access*), o qual utiliza o protocolo TKIP (*Temporal Key Integrity Protocol*), baseado na troca de chaves dinâmicas (cada pacote enviado contém uma chave diferente). Embora utilize a

mesma criptografia que o WEP, conseguiu implementar protocolos de segurança mais modernos (MORENO, 2016).

2.2.4.3 WPA2

O WPA2 utiliza o protocolo CCMP com algoritmo de criptografia AES, de maior complexidade, seu processo de autenticação ocorre por meio do mecanismo denominado *4-way handshake.* Porém, desde 2017, se tornou inseguro pois com uma placa de rede operando no modo monitor é possível decifrar os pacotes que a placa de rede envia ao *access point* para se autenticar, os quais contêm a cifra para autenticar o usuário à rede (MORENO, 2016).

2.2.4.4 WPA3

Disponibilizado desde 2018, tem por objetivo aprimorar os padrões de segurança do WPA2, adiciona criptografia 192 bits e da uma solução para a vulnerabilidade no 4-way-handshake. Porém ele não possui retro compatibilidade com dispositivos que usam o WPA2, portanto ainda há diversos dispositivos vulneráveis a ataques em uso pelo mundo, inclusive utilizados pelo Exército Brasileiro.

2.2.5 Modos de operação do adaptador de rede

Existem diferentes modos de operação que um adaptador de rede pode atuar. A fim de capturar pacotes de dados que não o foram endereçados diretamente, é necessário um dispositivo compatível com a interface do software Aircrack-ng, para que seja habilitada a função monitor. Um exemplo de interface compatível e amplamente utilizado é o adaptador de rede Alfa, modelo AWUS036NH (MORENO, 2016).

Figura 1.2 – Adaptador AWUS036NH

Fonte: <https://www.alfa.com.tw/products/awus036nh?variant=36481029374024> Acesso em 20 jul. 2021.

2.2.5.1 Modo *managed*

O modo *managed* é o modo convencional de operação de uma placa de rede, ela se conecta ao AP e a placa de rede *wireless* não tem a capacidade de monitorar e capturar os dados da rede além dos destinados à mesma (MORENO, 2016).

2.2.5.2 Modo promíscuo

Utilizado apenas na conexão cabeada, o modo promíscuo é um modo de operação da placa de rede em que já é possível capturar o tráfego de dados, mesmo que eles não sejam destinados diretamente à máquina, deve ser configurado manualmente, possibilitando a exploração cibernética (MORENO, 2016).

2.2.5.3 Modo monitor

O modo monitor é um modo em que a placa de rede consegue monitorar e captar todo o tráfego de dados da rede, não somente os dados destinados à mesma. O modo monitor também permite capturar pacotes sem a necessidade do atacante se associar ao ponto de

acesso. Portanto, para realizar um ataque cibernético à rede Wi-Fi é necessário configurar e operar a placa nessa configuração (MORENO, 2016).

2.3 FERRAMENTAS DE ATAQUE

O teste de vulnerabilidade de rede sem fio, padrão IEEE 802.11 (Wi-Fi), compreende diversas técnicas diferentes, a mais utilizada é a suíte Aircrack-ng, essa plataforma exige que os clientes da rede sejam desconectados, através de um ataque de desautenticação, para capturar o pacote *WPA-handshake*, que contém a senha de acesso ao ponto de acesso quando o usuário for reconectar ao Wi-Fi (MORENO, 2016).

2.3.1 Aircrack-ng

O Aircrack-ng é um *software* composto de ferramentas para análise de redes wireless, muito utilizado para explorar vulnerabilidades das redes Wi-Fi. As ferramentas mais utilizadas são: Airmon-ng, usado para criar ou finalizar interfaces em modo monitor; Airodump-ng, usada para captura de pacotes; Aireplay-ng, que contém múltiplos vetores de ataques como o de desautenticação, o qual desconecta um usuário da rede a ser atacada; e Aircrack-ng, ferramenta de quebra de criptografia nativa, podendo ser substituída por outra como a *Hashcat* (MORENO, 2016).

O ataque de desautenticação, por sua vez, pode gerar desconfiança entre os usuários, pois subitamente os usuários são desconectados, além de que se a rede for monitorada por um software de monitoramento como o *Wireshark*, é possível detectar o *spam* de pacotes de desautenticação.

2.3.2 HcxdumpTool

O HcxdumpTool é outra ferramenta utilizada para testes de vulnerabilidade em um AP, alternativa mais discreta ao Aircrack-ng. Essa ferramenta possui a vantagem de poder ser usada em combinação com o *software* Hashcat de forma a otimizar o ataque. Com o Hcxdumptool é possível induzir uma requisição simulada de conexão ao AP, sem a necessidade de desconectar ninguém da rede e levantar suspeitas.

2.3.3 Engenharia Social

A engenharia social é uma ferramenta que pode ser utilizada para um ataque, ou ao menos facilitá-lo, ela consiste no levantamento de informações que servirão para uma quebra de senha facilitada, por exemplo (WEIDMAN, 2014).

Os ataques de engenharia social podem envolver requisitos técnicos complexos ou nenhuma tecnologia. Um engenheiro social pode utilizar-se de um uniforme militar e se infiltrar em uma Organização Militar ou até mesmo no Centro de Operações sem ser percebido, de forma a levantar elementos essenciais de inteligência para a força adversa e implantar dispositivos danosos aos sistemas de TIC.

Um vetor comum em ataques de engenharia social é o correio eletrônico. Tentar enganar um usuário de modo que ele dê informações sensíveis ao se fazer passar por uma pessoa de confiança em um e-mail ou por outro meio eletrônico é conhecido como ataque de *phishing*. E-mails do tipo *phishing* podem ser usados para atrair alvos a visitarem sites maliciosos ou fazerem download de anexos maliciosos, entre outras atividades. Os ataques de engenharia social representam o elemento necessário que faltava para enganar os usuários (WEIDMAN, 2014).

2.4 QUEBRA DE CRIPTOGRAFIA

2.4.1 Wordlist

É possível realizar a quebra da criptografia utilizando uma lista de palavras conhecida como *wordlist* que contém palavras ‒em claro‖, geralmente oriundas de vazamentos de bancos de dados de senhas, e são utilizadas por softwares como *aircrak-ng* e *hashcat* para testar as palavras uma por uma até descobrir qual é a chave correta (MORENO, 2016).

O uso de *wordlists* não é totalmente eficaz, pois caso a senha do roteador Wi-Fi não esteja contida na *wordlist*, a criptografia não será quebrada. Portanto é necessário que o atacante conheça técnicas para criar *wordlists* de forma a aumentar as chances de sucesso (MORENO, 2016).

Da mesma forma, é importante que as senhas utilizadas não sejam as mesmas em todas as plataformas, além de que elas sejam complexas e mudadas regularmente, de forma que não estejam contidas nas wordlists e só sejam quebradas através de outras técnicas como força bruta. Entretanto, se a senha for razoavelmente complexa, até mesmo com força bruta, o

atacante demoraria tempo demais para conseguir descobrir a senha, tempo suficiente para o usuário trocar sua senha (MORENO, 2016).

2.4.2 John the Ripper

John the Ripper é uma ferramenta usada para quebra de *hash* de senhas, através de técnicas de força bruta, suportando vários métodos criptográficos (MORENO, 2016).

O John the Ripper pode operar de uma dessas formas:

> a) Single crack – O John the Ripper tentará quebrar as senhas usando o nome, derivações do nome, diretório home do usuário etc. Fornecido com a opção --single.
> b) Wordlist – Uma lista de palavras é fornecida ao John the Ripper para efetuar a quebra de senhas. Fornecido com a opção --wordlist=.
> c) Incremental mode – O John tentará todas as combinações possíveis de usuário e senha, método conhecido como força bruta. É a condição 100% certeira, porém dependendo da complexidade da senha a sua quebra levará muito tempo, sendo totalmente inviável. Fornecido com a opção --incremental.
> d) External mode – Poderá ser utilizado um componente externo para a quebra

2.4.3 Hashcat

O Hashcat é um *software* que possui as mesmas funcionalidades do John The Ripper, porém tem a capacidade de utilizares múltiplos núcleos da CPU para quebrar senhas e aceita acelerações de *hardware* da GPU, o que torna uma quebra de senha muito mais rápida. (MORENO, 2016)

3 REFERENCIAL METODOLÓGICO

Através das revisões literárias e do instrumento de pesquisa formulário, este trabalho buscou encontrar soluções para a vulnerabilidade de segurança nos pontos de acesso de rede *wireless*, a fim de criar o arcabouço de uma conclusão mais aprofundada a cerca do uso da tecnologia de redes sem fio como elemento multiplicador das capacidades de comando e controle.

3.1 TIPO DE PESQUISA QUANTO À ABORDAGEM

Pelo motivo do objeto de investigação ser uma situação estritamente particular em que são feitas análises subjetivas, a abordagem de pesquisa escolhida para atingir os objetivos estabelecidos pelo trabalho foi a qualiquantitativa, sendo a junção qualitativa com quantitativa.

A abordagem mista leva em consideração a qualitativa e quantitativa simultaneamente, sem uma ser excludente da outra. Enquanto a qualitativa busca descrever temas complexos através do ponto de vista do escritor, o qual se prova através da bibliografia, a quantitativa utiliza-se de números e gráficos para mensurar a realidade ao leitor (ROESLER et al., 2019).

Sobre abordagens mistas, Roesler et al. (2019, p. 57) estabelece que:

> Apesar de possuírem características distintas as pesquisas quantitativas e qualitativas não são mutuamente excludentes. Alguns trabalhos podem ter as duas abordagens simultâneas, ou seja, podem ocorrer pesquisas qualiquantitativas ou quantiqualitativas.

3.2 TIPO DE PESQUISA QUANTO À COLETA DE DADOS

Quanto à coleta de dados, foi utilizada a pesquisa bibliográfica para a abordagem qualitativa e o levantamento para a abordagem quantitativa.

A pesquisa bibliográfica é um tipo de pesquisa realizada com a intenção de explorar os assuntos através do conhecimento gerado previamente nos livros, manuais, artigos científicos, monografias, páginas da internet, entre outras fontes confiáveis (ROESLER et al., 2019).

O levantamento procura analisar as características de uma determinada população, podendo ser o seu todo ou apenas uma amostra. Seu uso será caracterizado pelo instrumento de pesquisa formulário (ROESLER et al., 2019).

3.3 MÉTODO DE PESQUISA

O método hipotético-dedutivo de Popper (1975, apud ROESLER et al., 2019, p. 45) é um procedimento que buscar resolver problemas através de tentativas e erros.

O método hipotético-dedutivo é defninido por Roesler et al. (2019, p. 46) como:

> –(...) consiste na construção de conjecturas (hipóteses) que devem ser submetidas a testes, os mais diversos possíveis — à crítica intersubjetiva, ao controle mútuo pela discussão crítica, à publicidade (sujeitando o assunto a novas críticas) e ao confronto com os fatos, para verificar quais são as hipóteses que persistem como válidas resistindo às tentativas de falseamento, sem o que seriam refutadas. É um método de tentativas e eliminação de erros, que não leva à certeza, pois o conhecimento absolutamente certo e demonstrável não é alcançado‖.

Para tanto, Popper (1975, apud ROESLER et al., 2019, p. 46) propõe que o método seja divido em três etapas: O problema, derivado da disparidade entre a realidade e a teoria; a solução, sendo o desenvolvimento de hipóteses; e os testes de falseamento, que são retificações ou ratificações das hipóteses, através de observações ou experimentações.

Seguindo a divisão proposta por Popper (1975), o problema do trabalho consiste na insegurança das redes Wi-Fi utilizadas pelo Exército Brasileiro devido à falta de conhecimento dos seus gerentes de rede.

A solução foi uma pesquisa bibliográfica sobre como é a ciência por trás do ataque à uma rede Wi-Fi. Além de uma pesquisa tipo formulário no âmbito do primeiro pelotão do Curso de Comunicações do ano de 2022, a fim de testar o nível de conhecimento dos militares que servirão nos corpos de tropa no ano de 2023.

O teste de falseamento se dará através dos formulários preenchidos pelos Cadetes que retificarão ou ratificarão as hipóteses levantadas por este trabalho, através do nível de conhecimento da população participante.

3.4 ETAPAS DA PESQUISA

Segundo Roesler et al. (2019, p. 53), a pesquisa deve seguir as seguintes etapas:

> Escolha do tema, determinando um assunto exequível de ser estudado e pesquisado; levantamento de dados que servirão de suporte à investigação que será realizada, escolhendo, nesse momento, o tipo de pesquisa apropriado a ser utilizado; formulação do problema, especificando-o de forma precisa e exata, com clareza, concisão e objetividade; definição dos termos a serem utilizados, tornando-os claros, compreensivos, objetivos e adequados; construção das hipóteses, a fim de orientar a busca de informações durante a pesquisa; indicação de variáveis, definindo-as com clareza, objetividade e de forma operacional; delimitação da pesquisa, estabelecendo limites para a investigação; determinação da amostragem, selecionando uma parcela do universo a ser investigado; seleção dos métodos e técnicas a serem utilizados na pesquisa científica; organização do material de pesquisa; e teste de instrumentos e procedimentos.

A delimitação do tema teve por objetivo alcançar objetivos exequíveis, pois possui amplo material bibliográfico para levantar os dados que embasam a teoria proposta e um pelotão de Cadetes de Comunicação voluntário para contribuir com a relevância do tema.

O presente estudo foca em atingir um objetivo concreto, que é resolver o problema de exploração de vulnerabilidade das redes Wi-Fi.

Embora os termos utilizados para descrever o ataque cibernético sejam complexos, todos foram esclarecidos através de explicações simples durante o texto e de um glossário ao final do trabalho.

A hipótese construída foi baseada na explanação de um ataque Wi-Fi, para instruir os militares na segurança de redes. Já as variáveis, estão na dificuldade das senhas utilizadas, de forma que quanto mais complexa a senha, mais difícil de quebrar.

A delimitação da pesquisa foi definida na conscientização dos futuros oficiais sobre sua atuação na Guerra Cibernética, e o limite da pesquisa foi estabelecido na proteção contra exploração de vulnerabilidades das redes Wi-Fi.

O Universo da pesquisa são os futuros oficiais de carreira da linha militar bélica que atuarão nos corpos de tropa em 2023. Apesar de que, conforme visto durante este trabalho, todas as OMs são responsáveis pela proteção cibernética, isso incluso unidades de todas as armas, quadros e serviços, as quais também utilizam redes Wi-Fi; com a finalidade de obter melhores resultados e ratificar a relevância da pesquisa, a amostragem escolhida foi um pelotão de comunicações, pois em seu plano de disciplina está prevista dentro da disciplina de cibernética, conceitos básicos de rede.

O método escolhido foi o formulário, pois é um instrumento de pesquisa que possibilita abstrair o máximo de informação de uma quantidade considerável de entrevistados, com facilidade.

A pesquisa bibliográfica como material de pesquisa, representa a parcela qualitativa do trabalho, já o formulário representa a parte quantitativa. A pesquisa bibliográfica foi o procedimento que formulou o arcabouço do problema e do desenvolvimento, enquanto o formulário foi o instrumento que aplicou a teoria, testando o nível de conhecimento prévio, de forma a demonstrar real necessidade da pesquisa.

3.5 INSTRUMENTO DE PESQUISA

O formulário é um dos métodos mais utilizados para a coleta de dados. Consiste em uma série de perguntas que devem ser respondidas pelo entrevistado, a fim de mensurar características de um universo, podendo ser utilizada uma amostragem para representar a população total (ROESLER et al., 2019).

Como universo da pesquisa, foi utilizado o 1° Pelotão de Comunicações, composto pelos Cadetes do 4° ano do Curso de Comunicações da AMAN. Sendo entrevistados um total de 32 militares que servirão nos corpos de tropa no ano de 2023 e que muito provavelmente terão redes de dados sob sua responsabilidade.

As perguntas do formulário foram formuladas com a finalidade de testar o nível de conhecimento dos militares sobre suas responsabilidades em relação à Guerra Cibernética e sobre vulnerabilidade de redes Wi-Fi.

Após a obtenção dos dados, foi possível ratificar a necessidade do constante preparo no setor cibernético dos futuros comandantes de pequena fração e suas atribuições.

4 RESULTADOS E DISCUSSÃO

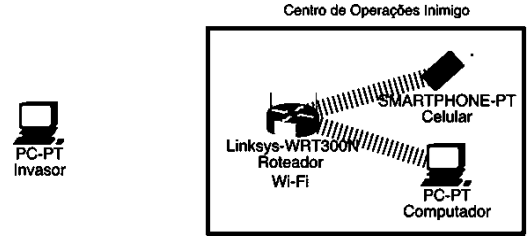
Através da pesquisa bibliográfica, foi possível abstrair o conceito geral da exploração de vulnerabilidades da tecnologia Wi-Fi. E por meio do formulário, ratificar a necessidade e relevância da pesquisa.

4.1 ATAQUE WI-FI

O *software* Packet Tracer, da Cisco, oferece uma plataforma de visualização e configuração de topologias de rede. Através dele, será exemplificado como é realizado o ataque em redes Wi-Fi. [12345]

Na figura 5, o invasor não possui acesso à rede, portanto ele faz um ataque de desautenticacão para desconectar os dispositivos do ponto de acesso.

Figura 5 – Topologia da rede com o invasor sem conexão

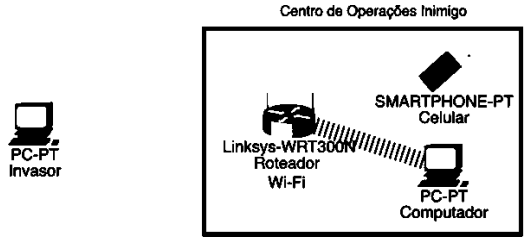


Fonte: AUTOR, 2021.

Na figura 6, um dos dispositivos recebeu o ataque de desautenticação, forçando-o a reconectar. Após o usuário reconectar, o invasor conseguirá capturar o pacote WPA-Handshake que contém a senha criptografada do roteador Wi-Fi. Após a captura do pacote, o

invasor irá começar o trabalho de quebra da criptografia para descobrir qual a senha, através das técnicas de *wordlist* ou força bruta.

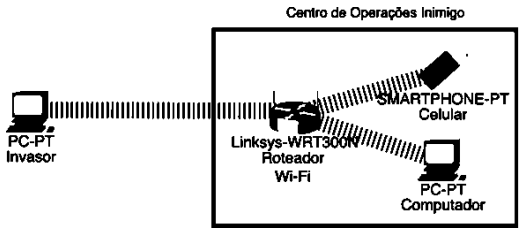
Figura 6 – Topologia da rede com um dispositivo interno desconectado da rede



Fonte: AUTOR, 2021.

Por último, na Figura 7, o invasor consegue quebrar a senha do pacote capturado e acessar a rede. Com a senha, ele terá agora acesso a todos os dados que trafegam por meio da rede Wi-Fi e todos os sistemas disponíveis.

Figura 7 – Topologia da rede com dispositivo interno e invasor conectados à rede



Fonte: AUTOR, 2021.

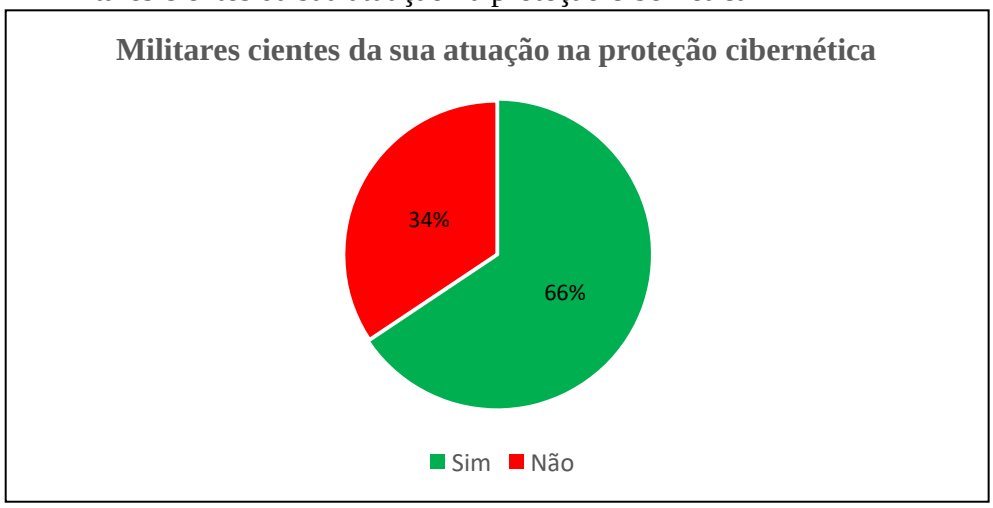
4.2 ANÁLISE DOS RESULTADOS

Foi realizada uma pesquisa no formato de formulário no âmbito do 1° Pel Com, 32 militares, da AMAN contendo 5 perguntas.

Questionados se estavam cientes de que todas as OMs atuam na Guerra Cibernética através da proteção cibernética, 66% dos militares responderam que sim, tinham ciência dessa responsabilidade, e 34% responderam que não (Gráfico 1).

Dessa forma, pouco mais da metade dos Cadetes entrevistados já sabiam da sua atuação na Guerra Cibernética através da proteção cibernética, ratificando a importância da presente pesquisa na função de orientá-los nesse quesito.

Gráfico 1 - Militares cientes da sua atuação na proteção cibernética

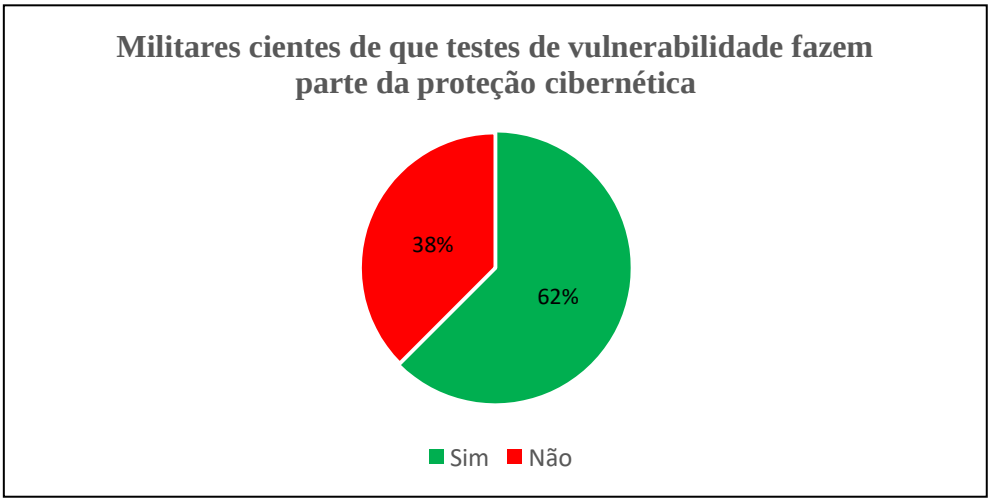


Fonte: AUTOR, 2022.

Foi perguntado se os militares sabiam que testes de vulnerabilidade fazem parte da proteção cibernética. Os resultados foram 62% respondendo que sabiam dessa inclusão e 38% dos 32 que não sabiam (Gráfico 2).

Portanto, uma quantidade ainda menor de entrevistados alegou não saber que no âmbito da proteção cibernética existe a possiblidade de realizar testes de vulnerabilidade para testar a resiliência de suas redes.

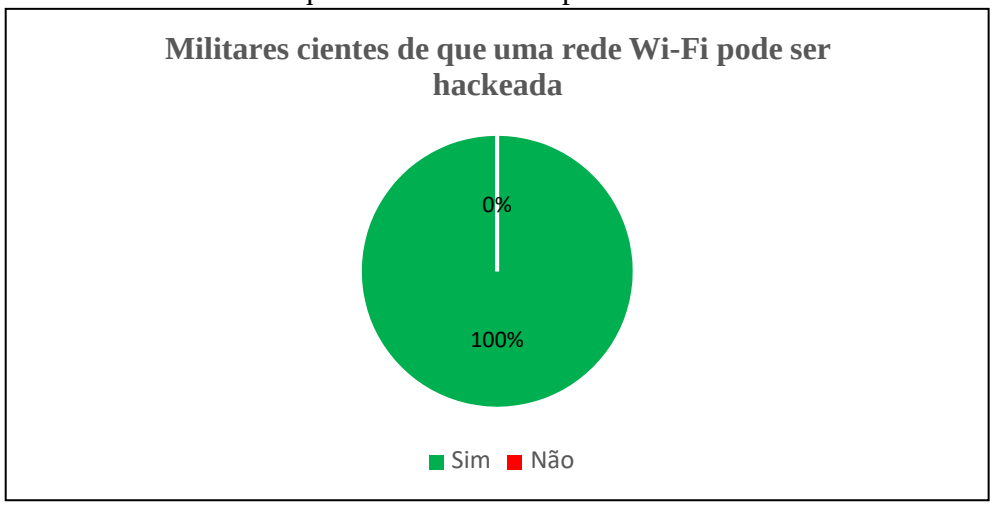
Gráfico 2 - Militares cientes de que testes de vulnerabilidade fazem parte da proteção cibernética



Fonte: AUTOR, 2022.

Foram questionados se tinham conhecimento que uma rede Wi-Fi poderia sofrer um ataque *hacker*, e todos responderam que já sabiam dessa vulnerabilidade (Gráfico 3).

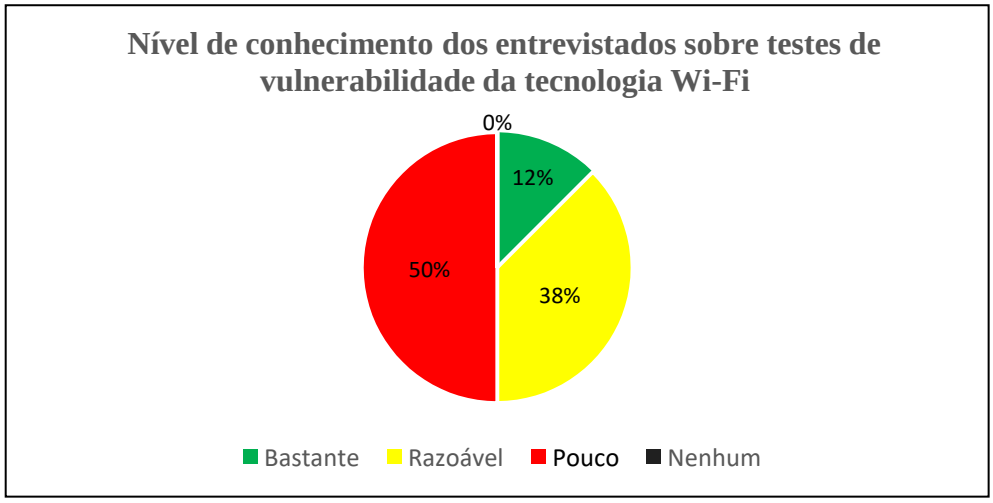
Gráfico 3 - Militares cientes de que uma rede Wi-Fi pode ser hackeada



Fonte: AUTOR, 2022.

Os entrevistados responderam sobre o nível de conhecimento que possuem sobre exploração de vulnerabilidade da tecnologia Wi-Fi. Dos 32 militares, metade afirmou que possui pouco conhecimento sobre o assunto, 38% responderam razoável, apenas 12% asseguraram saber bastante e ninguém alegou possuir nenhuma informação sobre o assunto (Gráfico 4).

Gráfico 4 - Nível de conhecimento dos entrevistados sobre testes de vulnerabilidade da tecnologia Wi-Fi



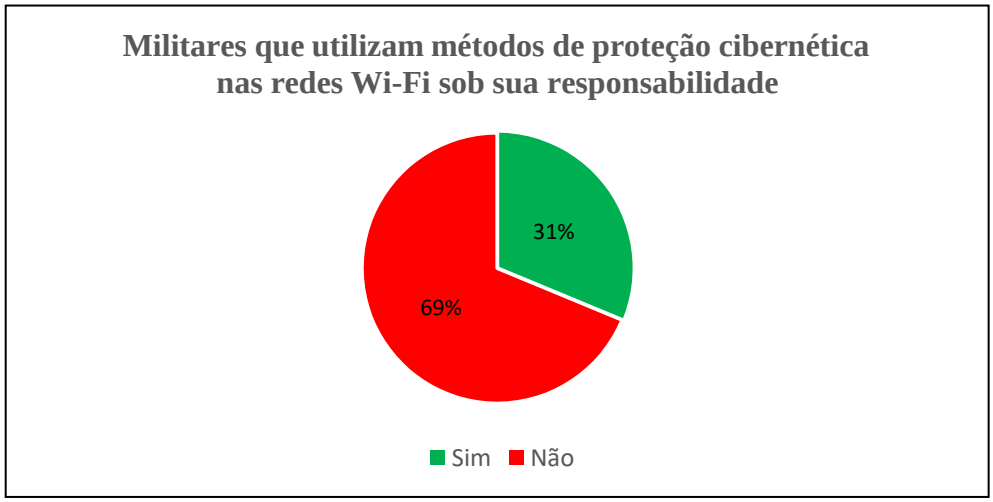
Fonte: AUTOR, 2022.

Por último, foi perguntado se já utilizam de métodos de proteção cibernética nas redes Wi-Fi sob sua responsabilidade, incluso exploração de vulnerabilidades. Porém apenas 31%

realmente levam em consideração a vulnerabilidade das redes Wi-Fi e as protegem apropriadamente (Gráfico 5).

Portanto, ainda que 50% dos entrevistados possuem conhecimento razoável ou bastante sobre o assunto, apenas 1/3 do pelotão efetivamente realiza testes de vulnerabilidade ou utiliza de outros métodos para a proteção de suas redes Wi-Fi.

Gráfico 5 - Militares que utilizam métodos de proteção cibernética nas redes Wi-Fi sob sua responsabilidade



Fonte: AUTOR, 2022.

Importante ressaltar que, em média, os resultados apresentados já eram esperados, pois a entrevista foi realizada com um pelotão de Cadetes do Curso de Comunicações, portanto os entrevistados já possuem um conhecimento consolidado em gerência de redes, aumentando o nível de exigência por parte dos militares.

5 CONCLUSÃO E SUGESTÕES

Através do presente estudo, foi possível concluir que é atribuição de todas as OMs atuar na Guerra Cibernética através da proteção cibernética, que engloba segurança de redes e testes de vulnerabilidade. Portanto é responsabilidade de todos os militares ter conhecimento sobre como realizar a proteção cibernética das redes Wi-Fi.

Foi constatado, também, a importância de se aprofundar no conhecimento de redes através dos testes de vulnerabilidade pelo *software* aircrack-ng, pois habilita o militar a testar o grau de resiliência da sua rede, identificando suas inseguranças; além de saber como melhor protegê-la nas diversas camadas da segurança das comunicações e transmissões.

Entretanto, através do formulário, foi detectado que há grande relevância os estudos sobre proteção cibernética de infraestruturas de rede, pois ainda que todos os entrevistados

tenham ciência da vulnerabilidade de uma rede Wi-Fi, nem todos sabem da sua responsabilidade na proteção da rede, ou como fazê-la.

Sugere-se ampliar o repertório de conhecimento dos militares nas escolas de formação em busca de um amplo domínio das tecnologias de rede Wi-Fi, para maior segurança no trânsito de informações nas OMs. Para isso, conhecer as vulnerabilidades da rede Wi-Fi e como testá-la é fundamental para estruturar redes mais seguras no Exército Brasileiro.

GLOSSÁRIO

Aircrack-ng: Software de análise de segurança de redes *Wireless*.

AP (*Access Point*): Termo em inglês que se refere ao ponto de acesso de uma rede Wi-Fi.

CPU (*Central Processing Unit*): Termo em inglês que se refere ao processador do computador.

ESSID: Abreviação de *Extended Service Set Identifier*, utilizado para se referir ao conjunto de serviços que envolvem uma rede reproduzidos por um nome, geralmente genérico, ao usuário.

GPU (*Graphic Power Unit*): Termo em inglês que se refere a unidade de processamento de vídeo.

Hacking: Termo em inglês referente a atividade de exploração ética de vulnerabilidades.

Hashcat: *Software* de quebra de criptografias.

Hcxdumptools: *Software* de análise de segurança de redes *Wireless*.

IEEE 802.11: Conjunto de padrões técnicos que especificam o uso da internet através da rede sem fio.

Pacote de Desautenticação: Pacote utilizado para controle do roteador que serve para desconectar um usuário.

Phishing: Termo em inglês que se refere a um tipo de ataque em que o usuário é atraído a compartilha informações privilegiadas, como suas credenciais.

PMK: Abreviatura em inglês de *pairwise mastar key*, base da geração de criptografia Wi-Fi.

PMKID: Abreviatura em inglês de *pairwise master key identifier*, responsável pela autenticação final de uma rede Wi-Fi.

***Spam*:** Termo em inglês que se refere a enviar exaustivamente mensagens indesejadas a um destinatário.

Wi-Fi: Abreviação de Wireless Fidelity, responsável por um ponto de conexão à internet sem fio.

***Wireless*:** Tecnologia que possibilita conexão de rede sem fio.

Wireshark: *Software* que analisa o tráfego de rede.

WPA-Handshake: Quadro utilizado pela tecnologia de criptografia WPA2 para autenticar um novo usuário possuidor de senha.

REFERÊNCIAS

BRASIL. Ministério da Defesa. **EB70-MC-10.246**: As Comunicações nas Operações. Brasília, 2020.

BRASIL, Ministério da Defesa. **EB70-MC-10.232:** Guerra Cibernética. Brasília, 2017.

BRASIL. Ministério do Exército. **IR 20-26**: Instruções Reguladoras para Utilização da rede Mundial de Computadores (Internet) por Organizações Militares e Militares do Exército. Brasília: EGGCF, 2001.

BRASIL, Ministério da Defesa. **IG 10-51:** Instruções gerais para a salvaguarda de assuntos sigilosos no Exército Brasileiro, Capítulo V – DA SEGURANÇA DAS COMUNICAÇÕES, Art. 105. Brasília, 2019.

ESTADO MAIOR DO EXÉRCITO. Portaria do Comandante do Exército nº 1.053, 11 de julho de 2018. **EB10-P-01.007**: Plano Estratégico do Exército (PEEx) 2020-2023, Brasília, 2019.

HASHCAT. (2018). **New attack on WPA/WPA2 using PMKID**. Disponível em: (https://hashcat.net/forum/thread-7717.html). Acesso em: 20 jul, 2021.

MENDES, Douglas Rocha. **Redes de Computadores:** teoria e prática. São Paulo. Novatec, 2007.

MORENO, Daniel. **Pentest em Redes Sem Fio**. São Paulo: Novatec, 2016.

NETO, Samuel Bombassaro. **A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas**. 2018. 55 p. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, [*S. l.*], 2018.

ROESLER, Rafael et al. **Iniciação à Pesquisa Científica** 2. ed. Resende: Academia Militar das Agulhas Negras, 2019.

RUFINO, Nelson Murilo de Oliveira. Segurança em redes sem fio: aprenda a proteger suas informações em ambientes Wi-Fi e bluetooth 4. Ed. São Paulo: Novatec, 2015.

SOUSA, Robson Everton; JUNIOR, Edilson Lima. Vulnerabilidades em Redes WI-FI. **Revista Científica de Redes de Computadores**, [*s. l.*], v. 1, n. 1, p. 38-47, 2018. Disponível em: https://revistas.laboro.edu.br/index.php/redes_de_computadores/article/view/10. Acesso em: 14 jul. 2021.

VISACRO, Alessandro. **A Guerra na Era da Informação**. Editora Contexto, 2018

WEIDMAN, Georgia. **Testes de Invasão:** Uma introdução prática ao hacking. São Paulo: Novatec, 2014.

ANEXO

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

DECEx – DESMil

ACADEMIA MILITAR DAS AGULHAS NEGRAS

O(a) Sr(a) está convidado(a) a participar da pesquisa "EXPLORAÇÃO DE VULNERABILIDADE DE REDES SEM-FIO IEEE 802.11 ADAPTADA AO CONTEXTO TÁTICO".
Este formulário é de interesse da AMAN com o objetivo de melhorar o processo de ensino e aprendizagem, e compõe o trabalho de conclusão de curso sobre exploração de vulnerabilidade de redes Wi-Fi.
Sua participação é voluntária e consiste em preencher um formulário que leva em média 1 minuto para ser respondido.
Você poderá recusar-se a participar, ou desistir de responder a qualquer momento.
As informações serão utilizadas para fins acadêmicos, sendo tratadas com sigilo e confidencialidade, preservando a identidade dos participantes.

Nome de guerra:_____

QUESTÕES

1) O Sr(a) sabia que toda OM é responsável atua na Guerra Cibernética através da proteção cibernética de seus sistemas de TIC?

( ) Sim

( ) Não

2)O Sr(a) sabia que faz parte da proteção cibernética testes de vulnerabilidade?(

) Sim

( ) Não

3)O Sr(a) sabia que seu WI-FI pode ser hackeado?(

) Sim

( ) Não

4)Qual o nível de conhecimento do(a) Sr(a) sobre o assunto?(

) Bastante

( ) Razoável

( ) Pouco

( ) Nenhum

5) O Sr(a) já utiliza métodos de proteção cibernética nas redes WI-FI sob sua responsabilidade?

( ) Sim

( ) Não