UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ERASMO PEREIRA DOS SANTOS
RODOLFO JOSÉ DE PAULA WANDERLEY

ANÁLISE DE VULNERABILIDADES EM PROTOCOLOS DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS E COMERCIAIS DE PEQUENO PORTE.

Maceió - AL
2020

ERASMO PEREIRA DOS SANTOS
RODOLFO JOSÉ DE PAULA WANDERLEY

ANÁLISE DE VULNERABILIDADES EM PROTOCOLOS DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS E COMERCIAIS DE PEQUENO PORTE.

Trabalho de Conclusão de Curso submetido ao Curso de Sistemas de Informação do Instituto de Computação da Universidade Federal de Alagoas como requisito parcial para a obtenção do Grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. ALMIR PEREIRA GUIMARÃES

Maceió - AL
2020

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 - 1767

S237a Santos, Erasmo Pereira dos.

Análise de vulnerabilidades em protocolos de segurança em redes sem fio domésticas e comerciais de pequeno porte / Erasmo Pereira dos Santos, Rodolfo José de Paula Wanderley. – 2021.

89 f. : il.

Orientador: Almir Pereira Guimarães.

Monografia (Trabalho de conclusão de curso em Sistemas de Informação) - Universidade Federal de Alagoas, Instituto de Computação. Maceió, 2020.

Bibliografia: f. 71-78.

Anexos: f. 79-89.

1. Redes locais sem fio. 2. Segurança de redes. 3. IEEE 802.11 (Normas). 4. PMKID, Ataque de. 5. *Aircrack-ng* (Suíte). I. Wanderley, Rodolfo José de Paula. II. Título.

CDU: 004.056

ERASMO PEREIRA DOS SANTOS
RODOLFO JOSÉ DE PAULA WANDERLEY

ANÁLISE DE VULNERABILIDADES EM PROTOCOLOS DE SEGURANÇA EM REDES SEM FIO DOMÉSTICAS E COMERCIAIS DE PEQUENO PORTE

Este Trabalho de Conclusão de Curso (TCC) foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Instituto de Computação da Universidade Federal de Alagoas.

Maceió, _01_ de __dezembro_ de 2020.

Prof. PETRÚCIO ANTÔNIO MEDEIROS BARROS, Me.
Coordenador do Curso de Sistemas de Informação

Banca Examinadora:

Prof. ALMIR PEREIRA GUIMARÃES, Dr.
Orientador

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

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

AGRADECIMENTOS

Agradecemos aos nossos familiares e amigos que nos motivaram e presenciaram toda a nossa batalha durante todo o curso.

Ao Prof. Dr. Almir Pereira Guimarães por nos mostrar o rumo do trabalho e pelo apoio imprescindível para o desenvolvimento deste trabalho.

SUMÁRIO

LISTA DE SIGLAS E ABREVIATURAS

3DES - Padrão De Criptografia De Dados Triplo (Sigla proveniente do inglês *Triple Data Encryption Standard*)

ACK – Reconhecimento (Sigla proveniente do inglês *Acknowledgement*)

AES -Algoritmo de Encriptação Avançada (Sigla proveniente do inglês *Advanced Encryption Algorithm*).

AP - Ponto de Acesso (Sigla proveniente do inglês *Access Point*).

ARP - Protocolo de Resolução de Endereço (Sigla proveniente do inglês *Address Resolution Protocol*).

ASCII - Código Padrão Americano para Intercâmbio de Informações (Sigla proveniente do inglês *American Standard Code for Information Interchange*).

BIP-GMAC-256 - Código de autenticação de mensagem de Galois de 256 bits (Sigla proveniente do inglês *Galois Message Authentication Code*)

BSS - Conjunto de Serviço Básico **(**Sigla proveniente do inglês *Basic Service Set***)**

BSSID - Identificador do Conjunto de Serviços Básicos (Sigla proveniente do inglês *Basic Service Set Identifier*).

CBC- MAC - Código de autenticação de mensagem de encadeamento de bloco de criptografia (Sigla proveniente do inglês *Cipher Block Chaining Message Authentication Code*)

CCMP - Protocolo no Modo contador CBC-MAC de Cifra (Sigla proveniente do inglês *Counter Mode CBC-MAC Protocol*).

DDoS - Negação de Serviço distribuída (Sigla proveniente do inglês *Distributed Denial of Service*).

DHCP - Protocolo de Configuração Dinâmica de Host (Sigla proveniente do inglês *Dynamic Host configuration Protocol*).

DMZ - Zona desmilitarizada (Sigla proveniente do inglês *DeMilitarized Zone*)

DNS - Sistema de Nomes de Domínio (Sigla proveniente do inglês *Domain Name System*).

DoS - Negação de serviço (Sigla proveniente do inglês *Denial of Service*).

DS - Sistema de distribuição (Sigla proveniente do inglês *Distribution System*)

EAP - Protocolo de Autenticação Extensível (Sigla proveniente do inglês *Extensible Authentication Protocol*).

EAPOL - Protocolo de autenticação extensível por LAN (Sigla proveniente do inglês *Extensible Authentication Protocol Over LAN*)

ECDH - Curva elíptica Diffie-Hellman (Sigla proveniente do inglês *Elliptic Curve Diffie-Hellman*)

ECDSA - Assinatura Digital De Curva Elíptica (Sigla proveniente do inglês *Elliptical Curve Digital Signature*)

ESS - Conjunto de Serviço Estendido **(**Sigla proveniente do inglês *Extended Service Set*)

ESSID - Identificador do Conjunto de Serviço Estendido (Sigla proveniente do inglês *Extended Service Set Identifier*).

GCMP-256 - Protocolo de Modo Contador Galois de 256 bits (Sigla proveniente do inglês *Galois / Counter Mode Protocol*)

HIDS - Sistema de Detecção de Intrusão Baseado em Host (Sigla proveniente do inglês *Host-Based Intrusion Detection System*)

HMAC - Modo de autenticação de mensagens com hash (Sigla proveniente do inglês *Hashed Message Authentication Mode*)

HTTP - Protocolo de Transferência de Hipertexto (Sigla proveniente do inglês *Hypertext Transfer Protocol*)

HTTPS - Protocolo de Transferência de Hipertexto Seguro (Sigla proveniente do inglês *Hypertext Transfer Protocol Secure*)

IBSS - Conjunto de Serviço Básico Independente **(**Sigla proveniente do inglês *Independent Basic Service Set*)

ICMP - Protocolo De Mensagens De Controle Da Internet (Sigla proveniente do inglês *Internet Control Message Protocol*)

IDEA - Algoritmo Internacional de Criptografia de Dados (Sigla proveniente do inglês *International Data Encryption Algorithm*)

IDS - Sistema de Detecção de Intrusão (Sigla proveniente do inglês *Intrusion Detection System*).

IEEE - Instituto de Engenheiros Elétricos e Eletrônicos (Sigla proveniente do inglês *Institute of Electrical and Electronics Engineers*).

IP - Protocolo de Internet (Sigla proveniente do inglês *Internet Protocol*).

IPS - Sistema de Prevenção de Intrusões (Sigla proveniente do inglês *Intrusion Prevention System*).

ISM - Instrumentação Científica e Médica (Sigla proveniente do inglês *Instrumentation, Scientific & Medical*)

IVs - Vetores de Inicialização (Sigla proveniente do inglês *Initialization Vectors*).

LAN – Rede de Área Local (Sigla proveniente do inglês *Local Area Network*)

MAC - Controle de Acesso de Mídia (Sigla proveniente do inglês *Media Access Control*).

MAN – Rede de Área Metropolitana (Sigla proveniente do inglês *Metropolitan Area Network*)

MIMO - Entrada múltipla, Saída múltipla (Sigla proveniente do inglês *Multiple Input, Multiple Output*)

MIT – Instituto de Tecnologia de Massachusetts (Sigla proveniente do inglês *Massachusetts Institute of Technology*)

MITM - Homem no meio (Sigla proveniente do inglês *Man-in-the-Middle*).

NIDS - Sistema de detecção de intrusão de rede (Sigla proveniente do inglês *Network Intrusion Detection System*)

NIST - Instituto Nacional de Padrões e Tecnologia (Sigla proveniente do inglês *National Institute of Standards and Technology*)

OSPF - Abrir O Caminho Mais Curto Primeiro (Sigla proveniente do inglês *Open Shortest Path First*)

PIDS - Sistema de detecção de intrusão baseado em protocolo (Sigla proveniente do inglês *Protocol-Based Intrusion Detection System*)

PMF - Quadros de gerenciamento protegidos (Sigla proveniente do inglês *Protected Management Frames*)

PMK - Chave Mestra em Pares (Sigla proveniente do inglês *Pairwise Master Key*).

PMKID - Identificador de Chave Mestra em Pares (Sigla proveniente do inglês *Pairwise Master Key Identifier*).

RADIUS - Servidor de usuário discado com autenticação remota (Sigla proveniente do inglês *Remote Authentication Dial-In User Server)*

RC4 – Cifra *Rivest* 4 (Sigla proveniente do inglês *Rivest Cipher 4*)

RFC - Pedido de Comentários (Sigla proveniente do inglês *Request for Comments*)

RFMON - Monitoramento de radiofrequência (Sigla proveniente do inglês *Radio Frequency Monitoring*)

RPC - Chamada de procedimento remoto (Sigla proveniente do inglês *Remote Procedure Call*)

RSN IE - Elemento de Informações de Rede de Segurança Robusta (Sigla proveniente do inglês *Robust Safety Net Information Element*)

SRP - Protocolo Remoto Seguro (Sigla proveniente do inglês *Secure Remote Protocol*)

SSH - Capsula segura (Sigla proveniente do inglês *Secure Shell*)

SSID - Identificador do conjunto de serviços (Sigla proveniente do inglês *Service Set Identifier*)

SYN – Sincronizar (Sigla proveniente do inglês S*ynchronize*)

TCP - Protocolo De Controle De Transmissão (Sigla proveniente do inglês *Transmission Control Protocol*)

TKIP - Protocolo de integridade de chave temporal (Sigla proveniente do inglês *Temporal Key Integrity Protocol*)

TxBF - Transmissão de formação de feixe (Sigla proveniente do inglês *Beam forming transmission*)

UDP - Protocolo De Datagrama Do Usuário (Sigla proveniente do inglês *User Datagram Protocol*)

UML - Modo de Usuário Linux (Sigla proveniente do inglês *User Mode Linux*), diferente da *UML* (*Unified Modeling Language* - Linguagem de modelagem unificada) utilizada em Engenharia de Software.

USB - Barramento Serial Universal (Sigla proveniente do inglês *Universal Serial Bus*).

VM - Máquina Virtual (Sigla proveniente do inglês *Virtual Machine*).

VMWARE - Software de infraestrutura virtual (Sigla proveniente do inglês *Virtual Infrastructure Software*)

WAN – Rede de Área Ampla (Sigla proveniente do inglês *Wide Area Network*)

WEP - Privacidade Equivalente à Cabeada (Sigla proveniente do inglês *Wired Equivalent Privacy*).

wIDS - Sistema de detecção de intrusão sem fio (Sigla proveniente do inglês *wireless Intrusion Detection System*)

WI-FI - Fidelidade sem Fio (Sigla proveniente do inglês *Wireless Fidelity*).

WIMAX - Interoperabilidade Mundial para Acesso a Microondas (Sigla proveniente do inglês *Worldwide Interoperability for Microwave Access*).

wIPS - Sistema de prevenção de intrusões para redes sem fio (Sigla proveniente do inglês *wireless Intrusion Prevention System*)

WLAN - Rede Local sem Fio (Sigla proveniente do inglês *Wireless Local Area Network*).

WMAN - Rede sem Fio de Área Metropolitana (Sigla proveniente do inglês *Wireless Metropolitan Area Network*).

WPA - Acesso Protegido por Wi-Fi (Sigla proveniente do inglês *Wi-Fi Protected Access*).

WPA-PSK - WPA de Chave Pré-compartilhada (Sigla proveniente do inglês *WPA Pre-Shared Key*).

WPA-TKIP - WPA com Protocolo de Integridade de Chave Temporal (Sigla proveniente do inglês *WPA-Temporal Key Integrity Protocol*).

WPS - Configuração de Wi-Fi Protegido (Sigla proveniente do inglês *Wi-Fi Protected Setup*).

WWAN – Rede sem fio de Área Ampla (Sigla proveniente do inglês *Wireless Wide Area Network*)

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

O uso da tecnologia *wireless* com o passar dos anos tem sido cada vez maior e fica cada vez mais clara a sua evolução através de dispositivos portáteis e eletrônicos como notebook, *smartphones*, *tablets*, *Smartv*, sistemas residenciais inteligentes, dispositivos de assistência pessoal, e até eletrodomésticos que antes eram impensáveis em ter alguma conexão com a Internet. Hoje é possível ter conexões para eletrodomésticos tais como geladeira, fogão, entre outros. As redes sem fio, tem sido amplamente difundidas em ambientes domésticos e corporativos tanto com a finalidade de economia em infraestrutura de cabeamento, quanto ao fato de permitir maior portabilidade e flexibilidade para redes locais. Porém, em contrapartida exige algumas preocupações adicionais em segurança que são intrínsecas a um meio de comunicação sem fio. Devido à importância dos dados que circulam em redes sem fio, a segurança da informação é uma questão de grande relevância para essas redes, sejam elas domésticas ou corporativas.

Nosso trabalho busca analisar determinados protocolos e até mesmo configurações utilizadas neste tipo de rede com o propósito de exibir alguns tipos de ataques e fragilidades relativas à segurança de redes sem fio, dando ênfase ao padrão IEEE 802.11 (IEEE 802.11b, IEEE 802.11g, IEEE 802.11n). Nos testes realizados foram feitos ataques do tipo *sniffer*, desautenticação, *dicionário*, *captura de handshake*, *PMKID*, força bruta, dentre outros, que obtiveram êxito com a utilização de ferramentas como *AirCrack-ng*, *Wifite2*, *Bettercap*, *Hashcat* para explorar suas respectivas vulnerabilidades.

Palavras-chaves: Redes sem Fio; Segurança de Redes; IEEE 802.11, Ataque de *PMKID*, *AirCrack-ng*.

ABSTRACT

The use of wireless technology over the years has been increasingly greater and its evolution is increasingly clear through portable and electronic devices such as notebooks, smartphones, tablets, Smartv, smart home systems, personal assistance devices, and even appliances that were previously unthinkable to have an internet connection. Today it is possible to have connections for appliances such as refrigerator, stove, and others. Wireless networks have been widely used in domestic and corporate environments, both for the purpose of saving cabling infrastructure and allowing greater portability and flexibility for local networks. However, in return, it requires some additional security concerns that are intrinsic to a wireless medium. Due to the importance of data circulating on wireless networks, information security is an issue of great relevance for these networks, whether they are domestic or corporate.

Our work seeks to analyze certain protocols and even configurations used in this type of network with the purpose of showing some types of attacks and weaknesses related to the security of wireless networks, emphasizing the IEEE 802.11 standard (IEEE 802.11b, IEEE 802.11g, IEEE 802.11n). In the tests carried out, sniffer, deauthentication, dictionary, handshake capture, *PMKID*, brute force attacks were performed, among others, which were successful with the use of tools such as AirCrack-ng, Wifite2, Bettercap, Hashcat to exploit their respective vulnerabilities.

Keywords: Wireless Networks; Network Security; IEEE 802.11, *PMKID* attack, AirCrack-ng.

CAPÍTULO 1 – INTRODUÇÃO

1.1 - Visão Geral

A palavra *wireless* é um termo em inglês e significa “sem fio” (*wire* - fio, *less* - sem ou menos). Nos últimos anos tem se popularizado o uso de redes sem fio, porém a ideia de comunicação sem fio não é tão recente assim. Em 1901, um físico italiano chamado Guglielmo Marconi demonstrou o funcionamento de um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código Morse (TANENBAUM, 2002). Com o surgimento das redes sem fio, o uso desta tecnologia permitiu que diversas estações se comunicassem sem a necessidade de cabos, por meio de ondas eletromagnéticas. Figura 1.1 demonstra os elementos contidos em uma rede sem fio.

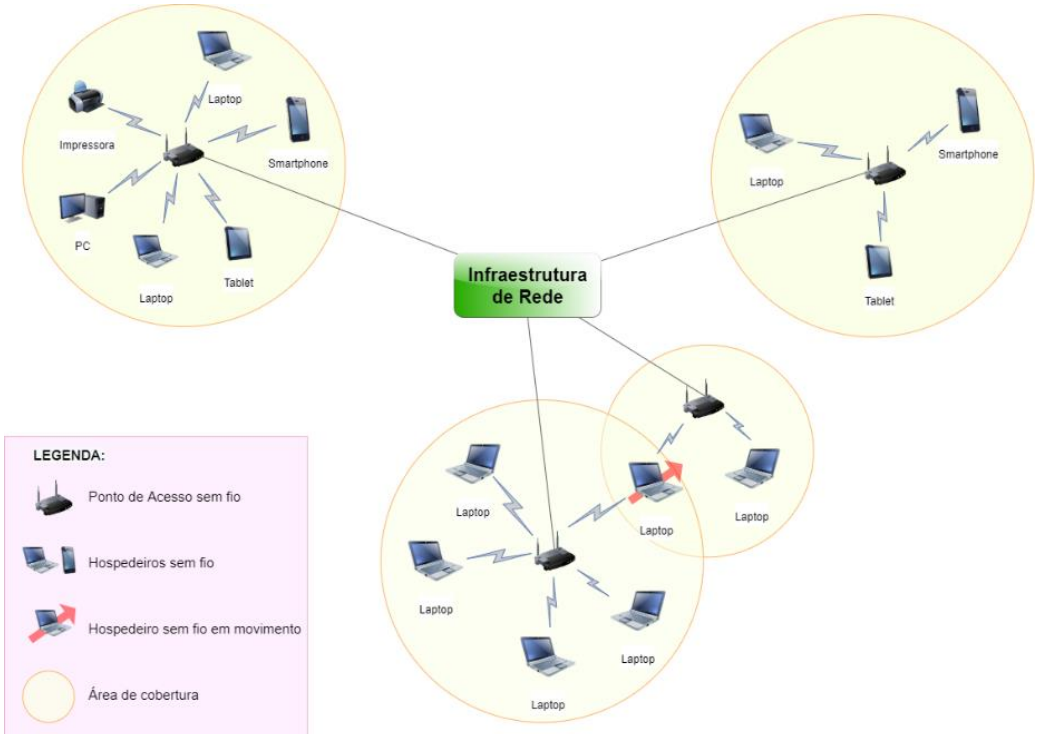


Figura 1.1 - Elementos de uma rede sem fio
Fonte: (KUROSE et al., 2014)

As redes sem fio surgiram inicialmente como complemento às redes que utilizam cabeamento convencional, possibilitando dessa maneira um maior alcance para as redes locais, através das chamadas *WLANs*. Atualmente o que vemos é a competição entre as redes sem fio e as redes cabeadas nas aplicações em *LANs*, nas redes *MANs* e mesmo nas redes *WANs*. A

princípio podemos dividir as redes sem fio em três categorias: *WLAN*, *WMAN* e *WWAN* (PINHEIRO, 2003).

Estas redes são implementadas como extensão ou alternativa para redes convencionais fornecendo as mesmas funcionalidades, mas de forma flexível, de fácil configuração e com boa conectividade em áreas prediais ou de campus (BARROS et al., 2010). Figura 1.2 demonstra de forma correta o arranjo de uma *WLAN*.

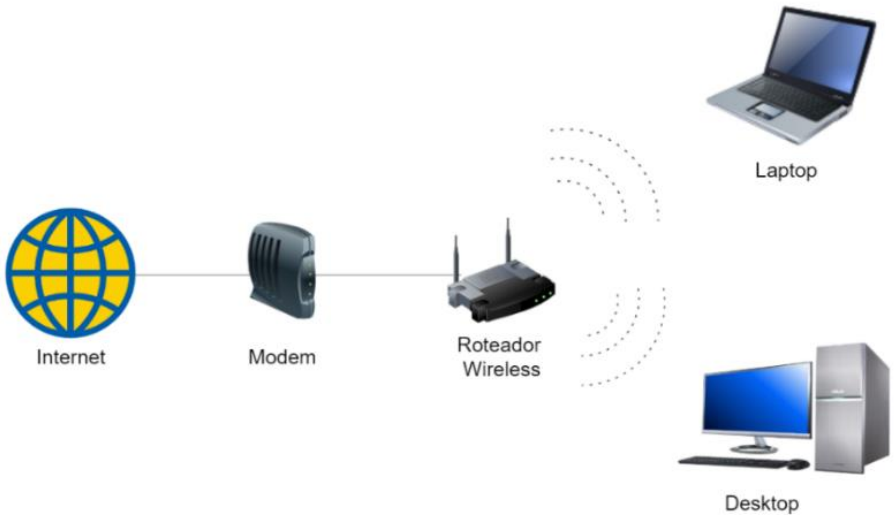


Figura1.2 – Arranjo de uma *WLAN*
Fonte: (SHARMA & DHIR, 2014)

De acordo com Franceschinelli (2003), as redes *WAN* sem fio, conhecidas também como *WWAN***,** têm suporte na tecnologia desenvolvida inicialmente para a comunicação de voz e depois foram adaptadas para suporte a dados. Elas se baseiam, fundamentalmente, na infraestrutura da tecnologia celular existente. Na Figura 1.3 podemos perceber o modelo de funcionamento de uma *WWAN*.

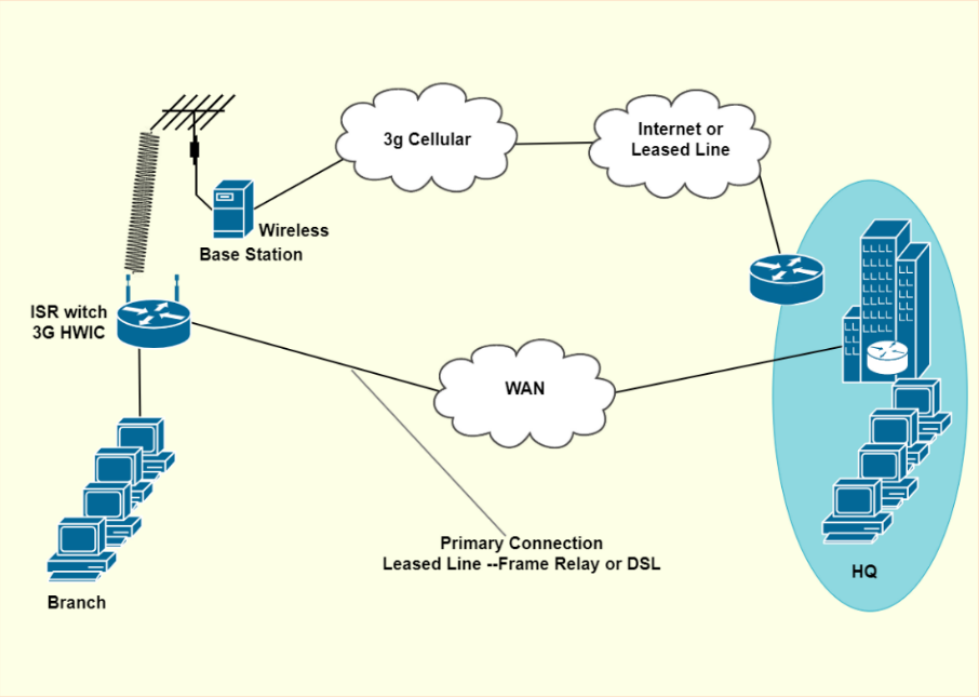


Figura1.3 – Funcionamento de uma *WWAN*
Fonte: (SHARMA & DHIR, 2014)

Ainda segundo Franceschinelli (2003), as redes ***MAN*** sem fio, conhecidas também como ***WMAN*** oferecem uma cobertura geográfica maior que as *WLANs* e altas taxas de transmissão. As *WMANs* são padronizadas pelo IEEE 802.16 (*Wireless Metropolitan Área Network Working Group)* (EKLUND et al., 2002), também popularmente conhecido como *WiMAX* (ENDLER et al., 2004). Figura 1.4 exemplifica a estrutura de uma *WMAN*. Conforme Reis (2018) O padrão *WiMAX* foi projetado para ser usado em redes de área metropolitana sem fio (*WMAN* / *Wireless MAN*), podendo cobrir uma distância em torno de 50 km com sinal.

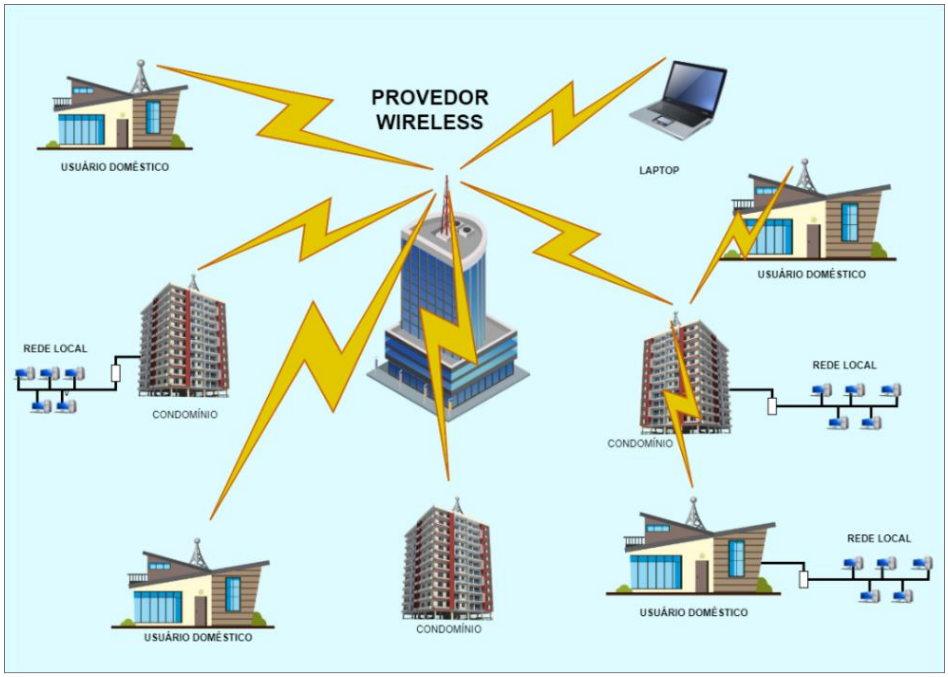


Figura1.4 – Estrutura de uma *WMAN*
Fonte: (SHARMA & DHIR, 2014)

As redes sem fio trouxeram para as empresas e pessoas diversos tipos de vantagens, tais como flexibilidade e baixo custo de instalação, porém, como em toda rede de computadores, nas redes sem fio sempre é importante priorizar a segurança das informações que são transmitidas. Como esse tipo de rede utiliza ondas eletromagnéticas para trafegar as suas informações, acaba se tornando uma rede frágil deixando suas informações vulneráveis a diferentes tipos ataques, que podem ocorrer através de técnicas e ferramentas especializadas. Por exemplo, o ataque de *Evil Twin* (OLIVEIRA, 2007) onde o *cracker* cria um ponto de acesso igual ao da vítima, fazendo com que o usuário pensa que está se conectando ao ponto de acesso legitimo, mas na realidade está se conectando a uma rede maliciosa. Um outro tipo de ataque é o de força bruta (BARBOSA et al., 2017), onde é criada uma lista de palavras com diversas combinações possíveis. No entanto é muito lento porque são verificadas todas as possibilidades existentes em uma determinada quantidade de dígitos. Também existe o ataque de *sniffer* (BARBOSA et al, 2017), que são programas responsáveis por capturar os pacotes da rede. Os *sniffers* exploram o tráfego dos pacotes que não utilizam qualquer tipo de cifragem nos dados. Com esse programa, qualquer informação que não esteja criptografada é obtida. Por outro lado, diferentes protocolos tais como *WEP* (KUROSE et al., 2014), *WPA* (CARRIÓN, 2005), *WPA2* (LÜDTKE,2015) e *WPA3* (RETTONDIN et al, 2018), foram propostos para solucionar os problemas originados intrinsecamente pelas redes sem fio.

Diante do que foi apresentado a cima, este trabalho visa analisar diferentes tipos de ataque, como o ataque *deauth* (MORENO, 2016), ataque de força bruta, ataque de captura de *handshake* (MACÊDO, 2016), ataque de captura de *PMKID* (FOUSEKIS, 2018), ataque de dicionário (SILVA et al., 2007), ataque de *sniffer*, dentre outros, realizando o passo a passo de como é configurado este tipo de ataque, mostrando para os usuários como estas redes podem ser facilmente invadidas, também serão apresentados alguns métodos que podem ser utilizados para tentar evitar uma possível invasão a rede.

1.2 Motivação

As redes sem fio são amplamente utilizadas em ambientes domésticos e empresariais, possuindo uma importância significativa na atualidade. Com a enorme quantidade de informações importantes que transitam nas redes sem fio, a preocupação com a segurança de suas informações está mais ascendente do que nunca devido aos diferentes tipos de ameaças que vêm surgindo nos últimos anos. As organizações, assim também como os usuários domésticos, possuem informações sigilosas, que passaram a ser alvo de criminosos que tentam acessá-las por meio de diversos ataques.

De acordo com Nakamura (2014), nas décadas de 70 e 80, a informática fazia parte da retaguarda dos negócios das organizações, onde, o elemento fundamental era o sigilo dos dados. Posteriormente, com o advento dos ambientes de redes, outro elemento passou a ter uma grande importância, a integridade dos dados. Hoje, a tecnologia da informação passou a ser primordial para as organizações, já que as informações circulam de forma muito rápida nesses meios e, por isso influenciam profundamente os negócios. Ainda conforme (NAKAMURA, 2014) uma falha, uma comunicação com informações falsas, roubo ou fraude de informações podem trazer graves prejuízos, como a perda de mercado, de negócios e perdas financeiras. Desse modo, a segurança de rede, em especial, a segurança de redes sem fio é primordial para garantir o sigilo da empresa e de todos os recursos envolvidos na infraestrutura das redes. Com isso, a segurança passa a fazer parte do processo de negócios das empresas. Em seu livro, Nakamura cita alguns acontecimentos que envolveram falhas de segurança como: O banco francês Société Générale sofreu uma fraude financeira de 4,9 bilhões de euro em 2008; - Foi roubada a base de dados dos clientes da loja virtual CD *Universe*, que tinha 300 mil números de cartões de crédito.

> Em anos recentes, contudo, a informação assumiu importância vital para a manutenção dos negócios, marcados pela dinamicidade da economia globalizada e permanentemente on-line, de tal forma que hoje não há organização humana não dependente da tecnologia da informação, em maior ou menor grau, de forma que o comprometimento do sistema de informações por problemas de segurança pode causar grandes prejuízos ou mesmo levar a organização à falência." (CARUSO, 1999).

De acordo com Nakamura (2014), as falhas de segurança podem causar grandes prejuízos, sejam eles, financeiros ou morais. Vale ressaltar que uma boa reputação pode demorar anos para ser construída, todavia, pode ser destruída em questão de instantes. Supondo que aconteça um incidente de segurança em um banco, por menor que seja, acarretará a migração de seus clientes para outras instituições financeiras devido à insatisfação na confiança dos serviços prestados na realização de suas transações financeiras. Assim, todas as instituições devem assegurar a seus clientes a integridade de seus dados.

Visto a importância da segurança da rede no ambiente doméstico e comercial de pequeno porte, nesta pesquisa serão abordadas diversas falhas de segurança em redes sem fio como: falhas nos protocolos de segurança WEP (KUROSE et al., 2014), WPA (CARRIÓN, 2005), WPA2 (LÜDTKE, 2015), senha fraca, capturas de handshakes, capturas do *PMKID* [1](FOUSEKIS, 2018) entre outros. Também serão detalhados alguns mecanismos de segurança, como: criptografia, *firewalls*, IDS, IPS, *Honeypot*, *Honeynet* entre outros.

1.3 Objetivos

1.3.1 Objetivo Geral

Analisar e expor vulnerabilidades de protocolos em redes sem fio IEEE 802.11 (IEEE 802.11b, IEEE 802.11g, IEEE 802.11n) por meio de ferramentas de código aberto, além de apresentar e sugerir mecanismos viáveis de proteção para estes tipos de ataques a estas redes.

[1] *PMKID* (*Pairwise Master Key Identifier*) é um ataque recente, onde de acordo com Kinzie (2020), esse tipo de ataque não depende da interceptação de comunicações bidirecionais entre dispositivos em uma rede sem fio para tentar quebrar a senha.

1.3.2 Objetivos Específicos

- Especificar conceitos fundamentais relacionados à segurança em redes sem fio;
- Apresentar algumas falhas de segurança em redes sem fio;
- Observar os protocolos de segurança que são amplamente utilizados na atualidade;
- Executar os testes de ataques em redes sem fio em nosso *testbed*;
- Sugerir algumas soluções para restringir a insegurança em relação às falhas apresentadas.

1.4 Estrutura do trabalho

Além do capítulo introdutório, este trabalho apresenta o Capítulo 2 que aborda uma breve síntese de alguns trabalhos relativos à temática deste estudo. O Capítulo 3 retrata os padrões para comunicação em rede sem fio assim como padrões de segurança nestas redes. São também abordados os principais tipos de ameaças e mecanismos de defesa utilizados nestas redes, além de ferramentas utilizadas neste trabalho. O Capítulo 4 apresenta a metodologia utilizada, o ambiente utilizado para os testes, as ferramentas utilizadas nos testes como o *bettercap*, *aircrack-ng*, *wifite2* e *hashcat*, e uma breve análise dos resultados. O Capítulo 5 traz o estudo de caso realizado para a pesquisa, com os resultados obtidos com as ferramentas usadas nos ataques. O Capítulo 6 apresenta a conclusão e as considerações finais.

CAPÍTULO 2 - TRABALHOS RELACIONADOS

Neste capítulo apresentaremos um breve resumo e metodologias dos trabalhos pesquisados na área de vulnerabilidades em redes sem fio, com o propósito de contribuir na elaboração deste trabalho.

No estudo apresentado em (JESUS et al., 2016) os autores exibiram uma análise sobre padrões de redes sem fio expondo seus pontos fortes e suas vulnerabilidades. Foi constituído um ambiente de testes com base nos padrões IEEE 802.11 (IEEE 802.11b, IEEE 802.11g, IEEE 802.11n) (MOREIRA, 2018) com as ferramentas disponíveis no *Kali Linux* (WEIDMAN, 2014) e por conseguinte na suíte *Aircrack-ng* (*Airmon-ng, Airodump-ng, Aireplay-ng, Airbase-ng*) (MORETTI et al., 2014) para a quebra de senhas *WEP* (KUROSE et al., 2014) e *WPA* (CARRIÓN, 2005) / *WPA2-PSK* (LÜDTKE,2015). Foram realizadas também simulações através de métodos de monitoramento e a captura de pacotes; ponto de acesso falso; quebra de chaves e clonagem de endereços *MAC*.

No estudo proposto em (SOLA et al., 2018) foi exposto o uso e a aplicação de ferramentas contidas em um ponto de acesso, com o propósito de analisar e demonstrar as vulnerabilidades e, dentro das possibilidades deixá-los menos expostos aos ataques que acontecem nesse tipo de rede com base nos padrões IEEE 802.11 (IEE 802.11b, IEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac) (MOREIRA, 2018). Este trabalho compôs um ambiente para a realização de *Pentests* e usou as ferramentas contidas no *Kali Linux* (WEIDMAN, 2014), e duas ferramentas em específico foram usadas em conjunto, o *crunch* (FILHO, 2018) para a criação de *wordlists* e a suíte de ferramentas *Aircrack-ng* (MORETTI et al., 2014).

No estudo exposto em (LÜDTKE et al., 2015) apresentou uma análise dos padrões e protocolos de redes sem fio IEEE 802.11 (IEEE 802.11b, IEEE 802.11g, IEEE 802.11n) (MOREIRA, 2018) objetivando identificar, conhecer e caracterizar as diferenças existentes, bem como os pontos fortes e suas vulnerabilidades. Neste trabalho foi montado um ambiente composto por um computador com uma máquina virtual (*VM - Virtual Machine*) com a distribuição *Kali Linux* (WEIDMAN, 2014) instalado, além de dispositivos móveis usados como estações para provocar fluxo de dados e um ponto de acesso, com a finalidade de usufruir

de todas as ferramentas essenciais para a realização dos testes de quebra de senha. As ferramentas principais utilizadas nos testes foram as da suíte *Aircrack-ng* (MORETTI et al., 2014), o *Crunch* (FILHO, 2018), o *REAVER* (CARRANZA et al., 2017), o *JOHN THE RIPPER* (DIORIO et al., 2019) e o *MDK3* (PRITCHETT et al., 2013).

O estudo exposto em (CARRIÓN, 2005) propôs uma avaliação na implementação dos protocolos de autenticação e trocas de chaves, como o *WEP* (KUROSE et al., 2014), IEEE 802.11x (DUARTE, 2003), *EAP-TLS* (SIMON et al., 2008), *EAP-MD5* (RIVEST, 1992), *WPA* (PIOTO, 2006). Apesar da abordagem de todos os protocolos IEEE 802.11 (IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac) (MOREIRA, 2018), em particular o estudo foi focado no protocolo IEEE 802.11b. Foram analisados diversos protocolos de autenticação e troca de chaves com relação a um conjunto de métricas que foram definidas ao longo da pesquisa. Além disso foram propostas inovações como na utilização de protocolos como *SRP* (*Secure Remote Protocol*) (RIBEIRO, 2005) e novas propostas de segurança para o protocolo *DHCP* (*Dynamic Host Configuration Protocol*) (MONTANARI, 2019).

O estudo mostrado em (BARBOSA et al, 2017) apresentou os padrões IEEE 802.11 (IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n) (MOREIRA, 2018) ressaltando suas vulnerabilidades, seus pontos fortes e alguns cuidados a serem tomados em relação a segurança. Realizaram ataques como quebra de senha, *Man-in-the-Middle* (BOTTI et al., 2015), *MAC Spoofing* (DUARTE, 2003), ataque de força bruta (BERTOLLI, 2018), ataque de negação de serviço (*DoS*) (TURCATO et al., 2015) em seus principais protocolos de segurança, o *WEP*, *WPA* e o *WPA2*. A maior parte das recomendações propostas como medidas de precaução a eventuais ataques lidam com o comportamento do usuário, como: alterar o nome do usuário, alterar a senha padrão do ponto de acesso, utilizar criptografia adequada, entre outras.

Por fim, o estudo apresentado em (DUARTE et al., 2003) analisou os padrões IEEE 802.11 (IEEE 802.11b, IEEE 802.11g) (MOREIRA, 2018) com o propósito de verificar suas falhas, como por exemplo falha existente na criptografia *WEP* com *RC4* (ENGELMANN et al., 2013) e as vulnerabilidades nas formas de autenticação. Os ataques apresentados foram: ataque de negação de serviço (*DoS*) (TURCATO et al., 2015), *Man-in-the-Middle* (BOTTI et al., 2015), *ARP Poisoning* (FLECK et al., 2002), *MAC Spoofing* (ANDRADE et al., 2008), *Wardriving* (ANDRADE et al., 2008) e o *Warchalking* (ANDRADE et al., 2008). As

ferramentas usadas foram o *NetStumbler* (BRYAN, 2018), o *Kismet* (MORIMOTO, 2006), o *Wellenreiter* (ROGER, 2008), o *WEPCrack* (RAGER, 2004), o *AirSnort* (TOMASINI, 2008) e o *Ethereal* (TOMASINI, 2008).

Nosso trabalho propõe um estudo de caso que, a partir de um *testbed*, executa análises dos padrões de comunicação em redes em fio IEEE 802.11b, IEEE 802.11g e IEEE 802.11n (SOLA, 2018), além dos protocolos que proporcionam segurança *WEP* (KUROSE et al., 2014), *WPA* (PIOTO, 2006) e *WPA2* (LÜDTKE, 2015). Os principais tipos de ataques realizados foram: ataque de dicionário (SILVA et al., 2007), ataque de força bruta (BERTOLLI, 2018), ataque de sniffer (LATTO, 2020), ataque *deauth* (MORENO, 2016) e o ataque ao *PMKID* (FOUSEKIS, 2018). Através das ferramentas: suíte *AirCrack-ng* (MORETTI et al., 2014), *bettercap* (LLERENA, 2020), *Hashcat* (ABELARDO et al., 2018) e *Wifite* (ABELARDO, 2018) constatamos vulnerabilidade nos protocolos *WEP, WPA* e *WPA2*.

CAPÍTULO 3 - FUNDAMENTAÇÃO TEÓRICA

3.1 Visão Geral

Este capítulo se destina a tratar de conceitos referentes a redes sem fio, tais como os principais protocolos de comunicação, protocolos de segurança, principais tipos de ameaças e mecanismos de segurança utilizados em redes sem fio, assim como as ferramentas utilizadas em nosso estudo de caso, a fim de explorar as vulnerabilidades destes tipos de redes.

Inicialmente, as redes sem fio fazem a comunicação entre dispositivos utilizando-se de ondas de rádio frequência. As frequências de rádio utilizadas para formar essas redes ocupam os valores de 900 MHz, 2.4 GHz e 5.0 GHz, como afirma (RUFINO, 2011). Estas frequências estão localizadas na chamada banda ISM, que são faixas de frequências reservadas internacionalmente para o desenvolvimento Industrial, científico e médico, sem a necessidade de licenciamento (SOARES, 1995). A frequência de 2.4 GHz, em especial, é amplamente utilizada em diversos dispositivos como Bluetooth e telefones sem fio e por esta razão estão mais suscetíveis a interferências (KHALED, 2006).

3.2 - Arquiteturas de Redes Sem Fio (802.11)

Segundo Reis (2018), a arquitetura de uma rede se refere ao modo como os dispositivos são interligados e aos tipos de equipamentos necessários para implementar tais redes. Ainda de acordo com Reis (2018), existem três tipos de arquiteturas disponíveis para redes locais sem fio *WLAN*, são elas:

- IBSS - (*Independent Basic Service Set*) Conjunto de serviço básico independente
- BSS - (*Basic Service Set*) Conjunto de Serviço Básico
- ESS - (*Extended Service Set*) - Conjunto de Serviço Estendido

Segundo Reis (2018), todos os dispositivos que se conectam a uma rede sem fio são denominados estações e se comunicam com a rede por meio de uma interface de rede sem fio.

3.2.1 - *IBSS* (*Independent Basic Service Set*) Conjunto de serviço básico independente

As Redes ***IBSS*** também são conhecidas como as redes ***Ad-Hoc***. As Redes *Ad-Hoc* são o tipo de rede sem fio mais simples, pois se tratam de dispositivos que se comunicam diretamente entre si – apenas clientes, incluindo computadores, notebooks, tablets, smartphones e outros dispositivos. Para isso, necessitam apenas de uma interface de rede wireless e antenas apropriadas, que geralmente são embutidas no dispositivo (REIS, 2018).

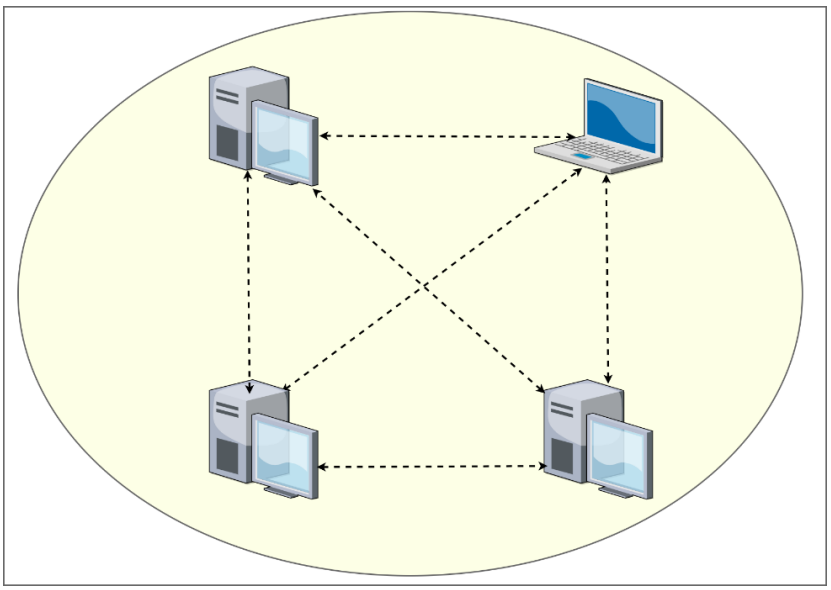


Figura 1.5 – Rede sem fio na topologia *ad-hoc*
Fonte: (WRIGHTSON, 2014)

Nas redes *Ad-Hoc* as comunicações são estabelecidas entre múltiplas estações, sempre com certa área de cobertura, como mostrado na Figura 1.5.

De acordo com Reis (2018), pode-se resumir as características de uma rede *IBSS* em:

- Não existem Pontos de Acesso (AP).
- Comunicação de cliente para cliente.
- O desempenho da rede diminui à medida que novos clientes são acrescentados.
- Suporta no máximo cerca de 5 clientes para um desempenho aceitável com tráfego leve.
- Não existe canalização do tráfego.

3.2.2 - *BSS* (*Basic Service Set*) Conjunto de Serviço Básico

Segundo Reis (2018), este tipo de arquitetura se trata do tipo mais comum de arquitetura de redes sem fio, onde os clientes se comunicam e são conectados através de um dispositivo central, que podemos chamar de ponto de acesso.

Toda rede *BSS* possui um nome que a identifica, conhecido pela sigla *SSID* (*Service Set Identifier*). Este nome pode ser escolhido pelo administrador da rede, e vem configurado com algum valor padrão de fábrica, diferente para cada modelo de ponto de acesso / roteador sem fios (REIS, 2018).

As redes *BSS* (ver Figura 1.6) e *ESS* dependem de um equipamento denominado ponto de acesso, que é uma espécie de "*switch* sem fio", responsável por oferecer serviços de autenticação e conexão para as estações de clientes da rede, além de prover a conexão à rede cabeada (normalmente ao *backbone* de sua rede) (REIS, 2018).

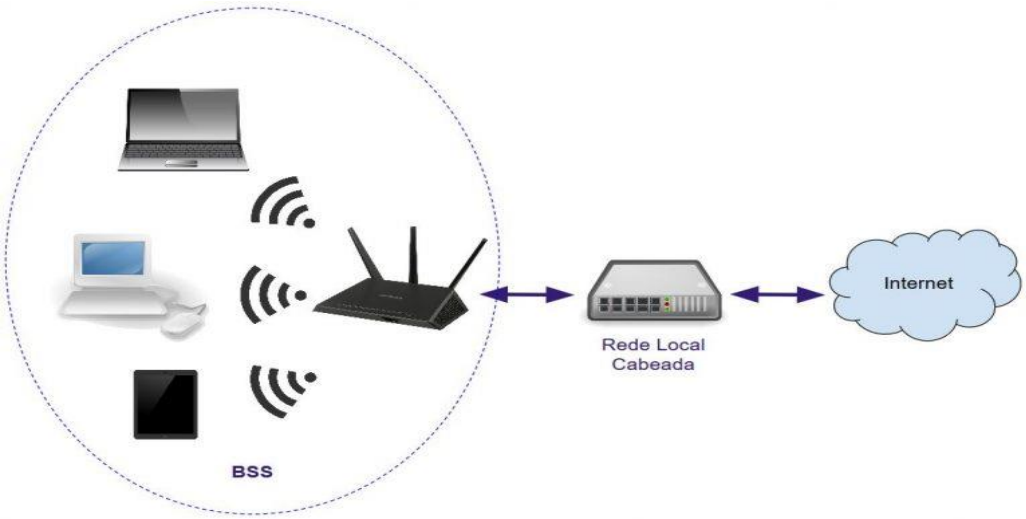


Figura 1.6 – Típica rede *BSS*
Fonte: (REIS, 2018)

3.2.3 - *ESS* (*Extended Service Set*) - Conjunto de Serviço Estendido

Para Reis (2018), esta arquitetura de rede é na verdade um conjunto de *BSSs* interconectadas com o intuito de aumentar o alcance e a capacidade da rede sem fio, podendo

consistir em até dezenas de pontos de acesso e conter centenas de estações de clientes conectados. Ainda segundo Reis (2018), os pontos de acesso em um *ESS* são conectados por meio de um Serviço de Distribuição (DS / *Distribution System*), o qual pode ser cabeado ou sem fio também.

A seguir (ver Figura 1.7) veremos um exemplo de arquitetura *ESS*, com duas *BSSs* interligadas:

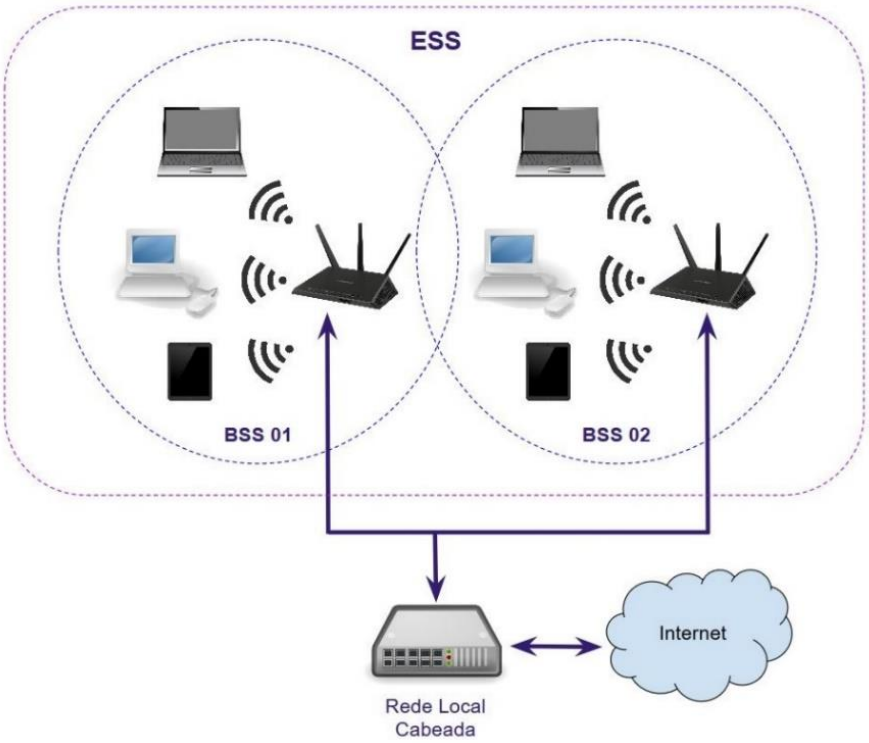


Figura 1.7 – Típica rede *ESS*
Fonte: (REIS, 2018)

3.3. - Padrões de Comunicação em Redes sem Fio

IEEE 802.11: O padrão IEEE 802.11 foi o primeiro padrão wireless, lançado em 1997, com uma taxa de transferência que opera entre 1Mbps a 2Mbps, uma taxa de transferência realmente baixa para as demandas atuais. Neste padrão as transmissões de wireless são realizadas por radiofrequência (SOLA, 2018).

IEEE 802.11b: O padrão IEEE 802.11b foi lançado em 1999, como uma atualização do padrão IEEE 802.11. A principal característica que diferencia estas duas versões é a

possibilidade de estabelecer conexões nas seguintes velocidades de transmissão: 1Mb/s, 2Mb/s, 5.5 Mb/s e 11 Mb/s. A frequência utilizada pelo padrão IEEE 802.11, é mantido no IEEE 802.11b que é de 2,4GHz (SOLA, 2018).

IEEE 802.11a: O padrão IEEE 802.11a foi disponibilizado no final do ano de 1999. Sua principal característica é a possibilidade de operar em taxas de transmissão de dados maiores que seu antecessor nos seguintes valores: 6Mb/s, 9Mb/s 12Mb/s, 18Mb/s, 24Mb/s, 36 Mb/s, 48 Mb/s e 54Mb/s. O alcance de sua transmissão é de cerca de 50 metros, porém a sua frequência de operação é diferente do padrão IEEE 802.11, ela opera em 5 GHz. O uso desta frequência é de grande conveniência por apresentar menos possibilidades de interferência, afinal, este valor é pouco usado, porém pode trazer alguns problemas, já que muitos países não possuem regulamento para esta frequência (SOLA, 2018).

IEEE 802.11g: O padrão IEEE 802.11g foi lançado em 2003, e é tido como o sucessor da versão IEEE 802.11b, pois ele é totalmente compatível com a sua versão antiga. O principal atributo do padrão IEEE 802.11g é o fato de que ele pode trabalhar com taxas de transmissão de até 54 MB/s, assim como acontece com o padrão IEEE 802.11a. Entretanto, o IEEE 802.11g opera com frequências na faixa de 2,4GHz e possui praticamente o mesmo poder de cobertura do seu antecessor, o padrão IEEE 802.11b (SOLA, 2018).

IEEE 802.11n: De acordo com Sola (2018), o início do desenvolvimento da especificação IEEE 802.11n iniciou-se em 2004 e foi finalizado em setembro de 2009. O padrão IEEE 802.11n é capaz de fazer transmissões de dados na faixa de 300 MB/s e, teoricamente, pode atingir taxas de até 600 MB/s. No modo de transmissão mais simples, com uma via de transmissão, o protocolo IEEE 802.11n pode chegar à casa dos 150 MB/s. Em relação à frequência deste padrão, ela pode trabalhar com faixas de 2,4 GHz e 5GHz, o que faz com que ele se torne compatível com os padrões anteriores, inclusive com o IEEE 802.11a. O padrão IEEE 802.11n tem como principal característica o uso de uma técnica chamada *MIMO* (*Mutiple-Input Multiple Output*), capaz de aumentar de maneira considerável as taxas de transferência de dados por meio da combinação de várias vias de transmissão. Conforme (PAULRAJ et al., 2011) a tecnologia *MIMO* foi incorporada aos padrões de redes sem fio rapidamente, seguido por alguns anos de desenvolvimento comercial para finalmente alcançar grande proporção no mercado, melhorando bastante a cobertura e o rendimento destas redes.

IEEE 802.11ac: O padrão IEEE 802.11ac (SOLA, 2018) é o sucessor do padrão IEEE 802.11n, cujas especificações foram desenvolvidas quase que totalmente entre os anos de 2011 e 2013. O principal foco do desenvolvimento do protocolo IEEE 802.11ac é a sua velocidade, que é estimado em até 433 MB/s no modo mais simples de operação (SOLA, 2018). Porém, teoricamente, é possível fazer a rede superar os 6GB/s em um modo mais avançado, que se utiliza de múltiplas vias de transmissões, no máximo até oito. O protocolo IEEE 802.11ac trabalha na frequência de 5GHz (SOLA, 2018). Este protocolo também possui técnicas mais avançadas de modulação, mais precisamente, trabalha com o esquema *MU-MIMO (Multi-User MIMO*) (FELISBERTO, 2018), de forma que este permite a transmissão e receptação de sinal de vários terminais, como se estes estivessem trabalhando de maneira colaborativa, todos na mesma frequência (SOLA, 2018). Tabela 3.1 abaixo, mostra uma comparação de padrões citados neste tópico, como data de publicação, taxas de transmissão, frequência, e largura de banda de cada um deles.

Padrões De Redes Wireless				
Padrão	**Data da publicação**	**Largura de banda (Mhz)**	**Taxa máx. de transmissão**	**Frequência (Ghz)**
IEEE 802.11	Jun 1997	22	2 Mbps	2.4
IEEE 802.11a	Set 1999	20	54 Mbps	5
IEEE 802.11b	Set 1999	22	11 Mbps	2.4
IEEE 802.11g	Jun 2003	20	54 Mbps	2.4
IEEE 802.11n	Out 2009	20 até 40	600 Mbps	2.4 ou 5
IEEE 802.11ac	Dez 2013	20 até 160	6 Gbps	2.4 e 5

Tabela 3.1: Padrões de rede *Wireless* IEEE 802.11
Fonte: Cisco.com

3.4 - Protocolos que Proporcionam Segurança em Redes sem fio

3.4.1 - *WEP* (*Wired Equivalent Privacy*) – Privacidade Equivalente Cabeada

Como o nome sugere, a *WEP* (PAIM, 2011) tem como propósito fornecer um nível de segurança semelhante ao que é encontrado em redes cabeadas. O *WEP* foi o primeiro padrão de

segurança para redes IEEE 802.11, criado em 1997 e ratificado em setembro de 1999. Foi introduzido na tentativa de dar segurança durante o processo de autenticação, proteção e confidencialidade na comunicação entre os dispositivos de redes sem fio. Oficialmente, o *WEP* é considerado obsoleto desde 2004, quando a *Wi-Fi Alliance* encerrou o suporte. *WEP* é baseado em uma chave secreta que é compartilhada entre computadores ligados a um ponto de acesso. Originalmente o tamanho da chave *WEP* é de 64 bits, mas existem dispositivos com suporte a chaves de 128 e 256 bits. As chaves podem ser apresentadas em caracteres hexadecimais ou *ASCII* (PAIM, 2011).

O *WEP* suporta o *RC4* (ENGELMANN et al., 2013), que é um algoritmo de fluxo que envia um conjunto de bits cifrados em fluxo contínuo, classificado como sendo um sistema criptográfico simétrico (KUROSE et al., 2014).

3.4.2 - *WPA*

De acordo com Pioto (2006), o *WPA* surgiu de um esforço conjunto de membros da *Wi-Fi Aliance* e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do protocolo *WEP*. Usa o protocolo de criptografia *TKIP* (STANGARLIN, 2012), uma tecnologia mais segura de encriptação de chave do que *RC4* do protocolo *WEP*. Segundo Carrión (2005), o objetivo do *WPA* é prover mecanismos de autenticação, confidencialidade e integridade utilizando algoritmos mais robustos e uma arquitetura mais adequada.

Inovações importantes foram disponibilizadas ao longo dos anos de 2005 e 2006 no *WPA*, no entanto, apesar de ter sido uma promessa quanto à segurança em redes sem fio, houve um consenso entre os especialistas de segurança com relação ao nível de segurança de um protocolo/tecnologia ser diretamente proporcional à maturidade de uma tecnologia, uma condição que se mostrou necessária, mas não suficiente (CARRIÓN et al., 2005).

3.4.3 - *WPA2*

O *WPA2* (LÜDTKE, 2015) foi lançado num consórcio *Wi-Fi* em 2004 baseado na especificação IEEE 802.11i, e utiliza o algoritmo *AES* (MAIA, 2017). Considerado o melhor

padrão de segurança que existe atualmente, com proteção dos dados, acessos e autenticação dos usuários, sendo que seu algoritmo base é o *AES*. Ainda conforme Lüdtke (2015), existem duas versões do *WPA2*: *WPA2-Personal* e *WPA2-Enterprise*: *O WPA2- Personal* protege o acesso à rede, utilizando uma senha, já o *WPA2-Enterprise* verifica os usuários da rede através de um servidor.

3.4.4 – *CCMP*

Segundo Lüdtke (2015) o *CCMP* é um protocolo de criptografia que faz parte do padrão IEEE 802.11i para *WLANs*. Além disso oferece maior segurança em comparação com tecnologias semelhantes, como o *TKIP* (STANGARLIN, 2012), empregando chaves de 128 bits e um vetor de inicialização de 48 bits que minimiza a vulnerabilidade a ataques. Responsável pela integridade e confidencialidade da informação é um protocolo baseado no algoritmo *AES* (MAIA, 2017).

3.4.5 - *WPA3*

Segundo Franklin (2018) o *WPA3* é a versão mais recente do *Wi-Fi Protected Access*, um conjunto de protocolos e tecnologias que fornece autenticação e criptografia para redes sem fio, sendo a próxima geração de segurança de redes sem fio. Também será lançado o padrão IEEE 802.11ax, o substituto do IEEE 802.11ac, onde o protocolo *WPA3* terá suporte ao padrão. Foram adicionados novos recursos para incrementar a segurança em redes sem fio permitindo autenticação mais robusta, maior força criptográfica para mercados de dados altamente confidenciais, mantendo a invulnerabilidade de redes de missão crítica que operem com o protocolo *WPA3*.

De acordo com Rettondin (2019), o protocolo *WPA3* possui melhoras (ou vantagens) como:

- Uso dos protocolos de segurança mais recentes do mercado.
- Desativação de protocolos desatualizados herdados de seu antecessor *WPA2*.
- Exige o uso do gerenciamento protegido, evitando que os dados possam ser interceptados durante a transmissão.

3.5 - Principais Tipos de Ameaças em Redes sem Fio.

Os principais tipos de ameaças encontradas em redes sem fio são descritos a seguir:

3.5.1 - *Evil Twin* (Gêmeo maligno)

Conforme Oliveira (2007) um ataque *Evil Twin* (tradução livre do inglês "gêmeo malvado") é uma situação em que um atacante utiliza um suposto ponto de acesso, nesse caso um *rogue* (impostor), se fazendo passar por um legítimo, para interceptar efetivamente as conexões de estações móveis. Este ataque ocorre geralmente em *hotspots* que oferecem conexão com a Internet e em redes sem fio domésticas, e fazem com que usuários pensem que estão se conectando a uma rede legítima, porém estão se conectando a uma rede maliciosa.

Na Figura 3.1 podemos observar que um impostor usa um ponto de acesso falso e se passa pelo ponto de acesso verdadeiro, e o usuário não percebe pois o sinal está forte, já que o impostor não apenas utilizou o mesmo nome e configurações da rede que o ponto de acesso verdadeiro. Se o usuário for tentado pelo sinal forte e se conectar manualmente ao ponto de acesso impostor, ou se o computador do usuário escolher automaticamente essa conexão, o ponto de acesso impostor se tornará o ponto de acesso à Internet do usuário, dando ao invasor a capacidade de interceptar dados confidenciais, como senhas por exemplo.

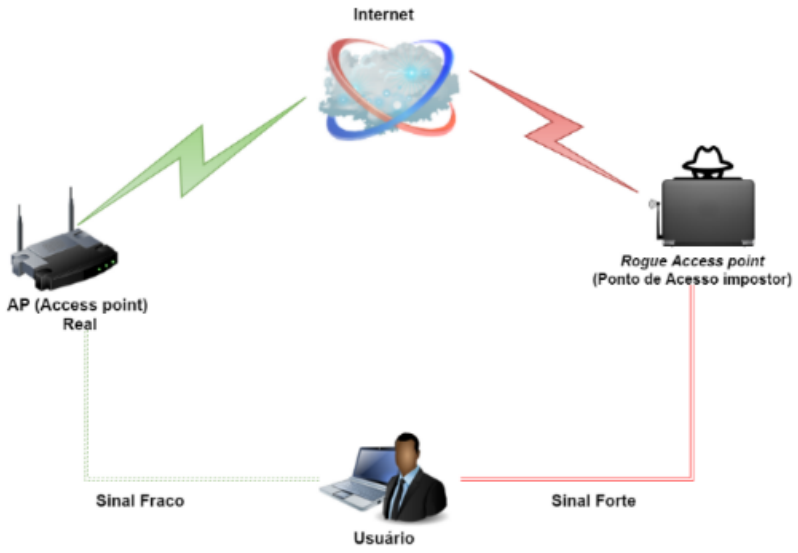


Figura 3.1: Ataque *Evil Twin*
Fonte: (OLIVEIRA et al., 2017)

> Pelo fato do padrão IEEE 802.11 não disponibilizar autenticação do ponto de acesso, a estação móvel se reassocia desapercebidamente com o *rogue access point*. Uma vez ocorrida a reassociação, todo o tráfego da conexão é interceptado pelo *hacker*. Pela natureza do ataque praticamente invisível para o usuário, a quantidade de informações que o atacante pode interceptar nesta situação é limitada apenas pelo tempo que ele pode executar sem ser pego (VLADIMIROV et al., 2004).

3.5.2 - *MAC Spoofing*

Segundo Duarte (2003), nas redes onde os pontos de acesso utilizam o endereço *MAC* como controle dos usuários autorizados, o sistema pode ser invadido por este tipo de ataque. Um atacante pode capturar um endereço *MAC* válido de um cliente e trocar o endereço dele próprio pelo do cliente, pois alguns dos dispositivos para redes sem fio possuem a particularidade de permitir a troca do endereço físico. De posse de tal endereço, o atacante poderá utilizar a rede e todos os seus recursos (ANDRADE et al, 2008).

A técnica de falsificação de endereços não é utilizada apenas para falsificação de endereços, mas serve também para evitar que o endereço real de um atacante seja reconhecido durante uma tentativa de invasão, ou seja, o usuário pode alterar o endereço *MAC* do próprio dispositivo com o intuito de esconder o endereço verdadeiro (BARBOSA et al., 2017).

3.5.3 - Ataques de dicionário

Este tipo de ataque é baseado nas combinações de frases, palavras, letras, números, símbolos ou qualquer outro tipo de combinações que são geralmente usadas na criação das senhas pelo o usuário. Conforme Bertolli (2018), este ataque é um tipo de ataque de força bruta dos mais simples existentes, onde o atacante faz uso de um dicionário, ou *wordlist* (lista de palavras), contendo prováveis senhas e realiza tentativas com todas essas senhas. Os ataques de dicionário iniciam com hipóteses sobre senhas comumente utilizadas na tentativa de decifrar a senha correta a partir da lista no dicionário. Se a senha estiver na *wordlist* o atacante terá sucesso, caso contrário o ataque não terá êxito.

3.5.4 - Força bruta

Enquanto as listas de palavras, ou dicionários, dão maior velocidade no processo de quebra de senha, esse método de quebra de senhas simplesmente faz a repetição de todas as combinações possíveis. Este é um método muito bom para descobrir as senhas, no entanto é muito lento porque são verificadas todas as possibilidades existentes em uma determinada quantidade de dígitos (BARBOSA et al., 2017).

3.5.5 - Ataques *Sniffers*

Os *sniffers*, chamados também de analisadores de pacotes, podem ser *softwares*, e por vezes *hardwares*, de monitoramento em redes. Diante disso, os criminosos têm preferência por *softwares* do tipo *sniffer*. Segundo Latto (2020), um programa do tipo "*sniffer*" é utilizado para monitorar o tráfego nas redes em tempo real, podendo ser lícitos ou ilícitos, com o propósito de capturar, decodificar e interpretar pacotes de dados enviados em uma rede. O uso de programas ilegais do tipo *sniffer* buscam essencialmente: a captura de informações privadas como nomes de usuários, senhas, números de cartões de crédito; gravação de mensagens, como e-mails e mensagens instantâneas; fraude de identidade e roubo financeiro.

> Normalmente, os computadores ignoram todo o tráfego direcionado para algum local qualquer da rede, mas esses aplicativos alteram essencialmente as configurações e permissões de um computador. Assim, ele passa a coletar e copiar todos os pacotes de dados disponíveis na rede. Isso permite que o criminoso examine e armazene todos os dados da rede quando quiser. Essa configuração é chamada de *modo promíscuo* e é tão sorrateira e irrestrita quanto seu nome sugere (LATTO, 2020).

3.5.6 - *Port Scanning*

Port Scanning (escaneador de porta) é o processo de verificação de quais serviços estão ativos em um determinado *host*, ou seja, é um processo que faz uma varredura nas portas TCP (POSTEL, 1981) e UDP (POSTEL, 1980) do sistema alvo para determinar quais serviços estão em execução. Segundo Lima (2000), "este processo é utilizado tanto por um administrador de redes para realizar uma auditoria eliminando assim quaisquer serviços que estejam rodando sem necessidades ou pode ser utilizado por um *hacker* para obter informações sobre as vulnerabilidades existentes no sistema". Detectar atividades de varredura de portas é essencial para saber quando um ataque pode ocorrer e como ocorrerá (BARBOSA et al., 2017).

3.5.7 - *Man-in-the-Middle* (Homem-no-Meio)

Segundo Botti (2015), o principal objetivo desse ataque é interceptar os dados que saem de uma máquina cliente até o servidor. Na maior parte das vezes o usuário não sabe que seus dados foram capturados, ou que ele tenha sofrido um ataque. O atacante é capaz de ler, inserir e modificar, mensagens entre duas entidades sem que estas tenham conhecimento que a ligação entre ambas está comprometida. Tipicamente o atacante insere-se no meio da comunicação entre dois hosts, fazendo parte do canal de comunicação. Ainda de acordo com Botti (2015), o autor do ataque pode se comportar de duas maneiras, passivo, onde os dados das vítimas são apenas monitorados e ativo, onde os dados são monitorados e podem sofrer alterações antes de chegar no servidor de destino.

Na Figura 3.2 podemos observar um ataque do tipo *Man-in-the-middle*, onde o elemento C está interceptando todos os pacotes transmitidos nesse "meio" entre os elementos A e B, e estes não sabem da existência do elemento C.

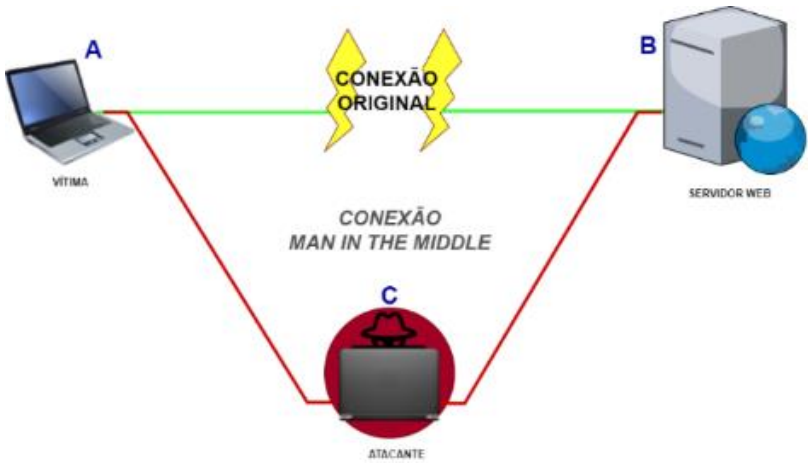


Figura 3.2: Ataque *Man in the Middle*
Fonte: (FRANZINI, 2013)

3.5.8 – Negação de Serviços (*DoS*)

De acordo com Turcato (2015), a negação de serviços é um tipo de ataque onde o atacante faz com que os recursos computacionais, sobrecarreguem de tal forma que as

requisições normais provenientes da rede não sejam atendidas. Podemos perceber esse tipo de ataque na Figura 3.3.

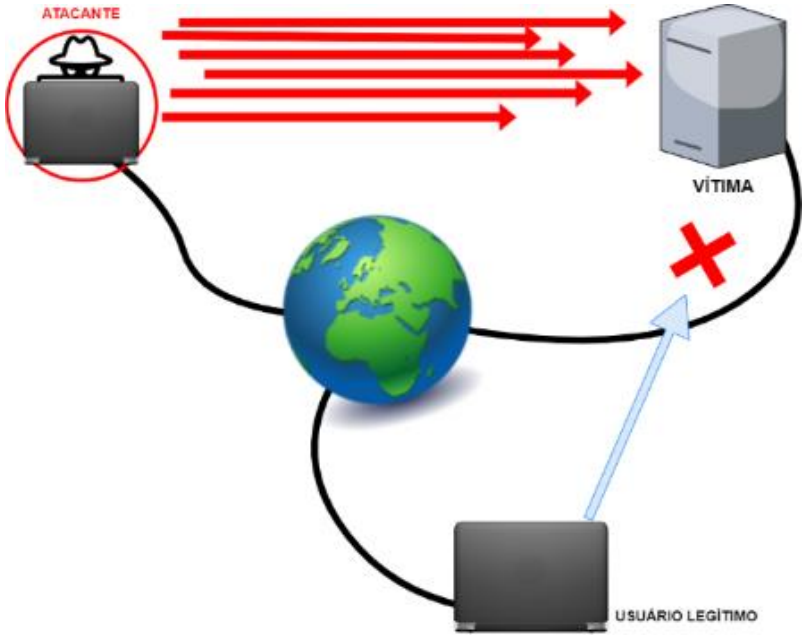


Figura 3.3: Ataque de Negação de Serviços
Fonte: (JORDÃO, 2011)

3.5.9 – Negação de Serviços Distribuído (*DDoS*)

Conforme Maciel (2018), a negação de serviços distribuído é um tipo de ataque de negação de serviços só que de maneira coordenada e distribuída, ou seja, quando é utilizado um conjunto de equipamentos objetivando o consumo de recursos computacionais e da largura de banda de modo que a vítima não consiga fornecer os serviços aos usuários legítimos. Figura 3.4 demonstra esse tipo de ataque.

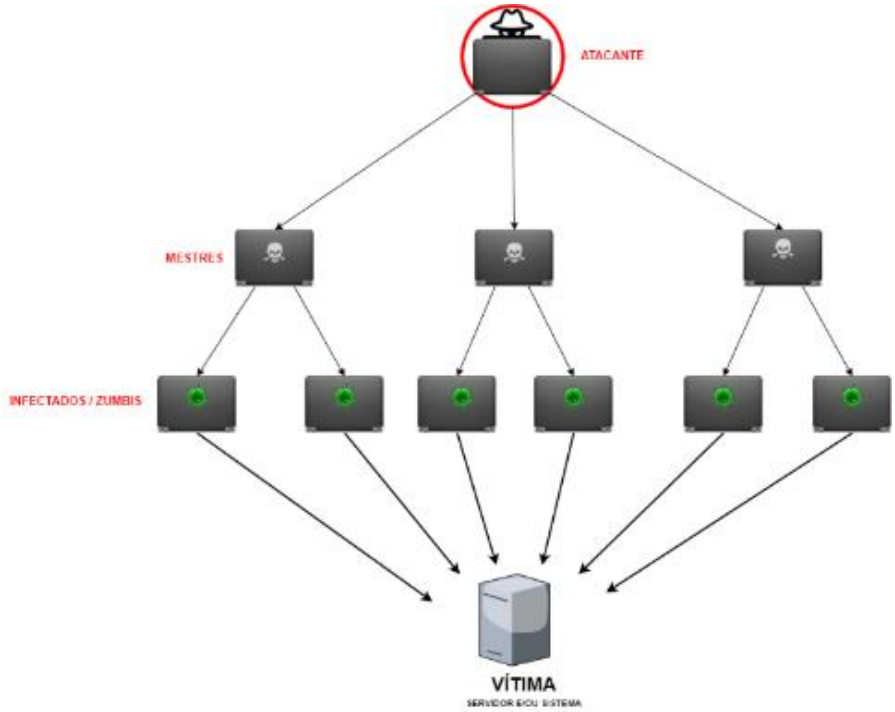


Figura 3.4: Ataque Negação de Serviços Distribuído
Fonte: (Canaltech.com)

3.5.10 – Ataque *PMKID*

O Ataque *PMKID* (*Pairwise Master Key Identifier*) é um ataque recente, onde de acordo com Kinzie (2020), esse tipo de ataque não depende da interceptação de comunicações bidirecionais entre dispositivos em uma rede sem fio para tentar quebrar a senha, como é o caso de captura de *handshakes*, onde é necessário que tenha clientes conectados ao ponto de acesso havendo comunicação. No caso do *PMKID* um invasor pode se comunicar diretamente com um ponto de acesso vulnerável usando esse tipo de ataque. Ele funciona fazendo um ataque contra o *RSN IE* (Elemento de Informações de Rede de Segurança Robusta) de um único quadro *EAPOL* [2]para capturar as informações necessárias para tentar um ataque de força bruta. O Ataque *PMKID* por si só, é um ataque onde busca por capturar informações a respeito do ponto de acesso, sendo usado em conjunto com outros ataques como o ataque de força bruta. Não é mais necessário que tenha clientes conectados para conseguir capturar um handshake, mesmo sem cliente conseguimos capturar um *PMKID* e posteriormente fazer a quebra de senha com força bruta (KINZIE, 2020).

[2] *Extensible Authentication Protocol* (EAP) do 802.1x igualmente conhecido como o EAP sobre LAN (EAPOL) fornece a estrutura para que um dispositivo autentique quando conecta à rede.

3.6 – Mecanismos de Segurança em Redes sem Fio

Esta seção irá detalhar os principais mecanismos de segurança aplicados a redes sem fio. Optou-se apenas em falar sobre soluções aplicáveis a ambientes heterogêneos, não fazem parte do escopo deste trabalho as soluções proprietárias, que porventura, possam vir a proporcionar maior segurança. Primeiramente, aborda-se sobre criptografia para melhor entendimento de como estes mecanismos funcionam.

3.6.1 – Criptografia

Segundo Almeida (2012), criptografia é a arte e ciência de enviar mensagens secretas, onde o emissor usa uma chave para cifrar a mensagem, sendo esta enviada até ao receptor que usa uma outra chave para a decifrar, que poderá ser igual ou não à chave do emissor. O problema consiste em inventar chaves que tornem impossível ou computacionalmente irrealizável que o inimigo (ou qualquer pessoa que não queiramos que leia a mensagem) decifre a mensagem interceptada.

Devemos lembrar que a criptografia não garante que as mensagens não serão acessadas por outra pessoa que não o receptor, e sim que as mensagens não sejam entendidas por quem as interceptar.

3.6.2 - Algoritmos de chave simétrica

Segundo Kurose (2014), todos algoritmos criptográficos envolvem a substituição de um dado por outro, como tomar um trecho de um texto aberto e então, calculando e substituindo esse texto por outro cifrado apropriado, criando uma mensagem cifrada. Os sistemas criptográficos simétricos utilizam um método de cifragem tradicional onde a chave de cifragem é a mesma da chave de decifragem. Figura 3.5 ilustra como acontece uma criptografia simétrica.

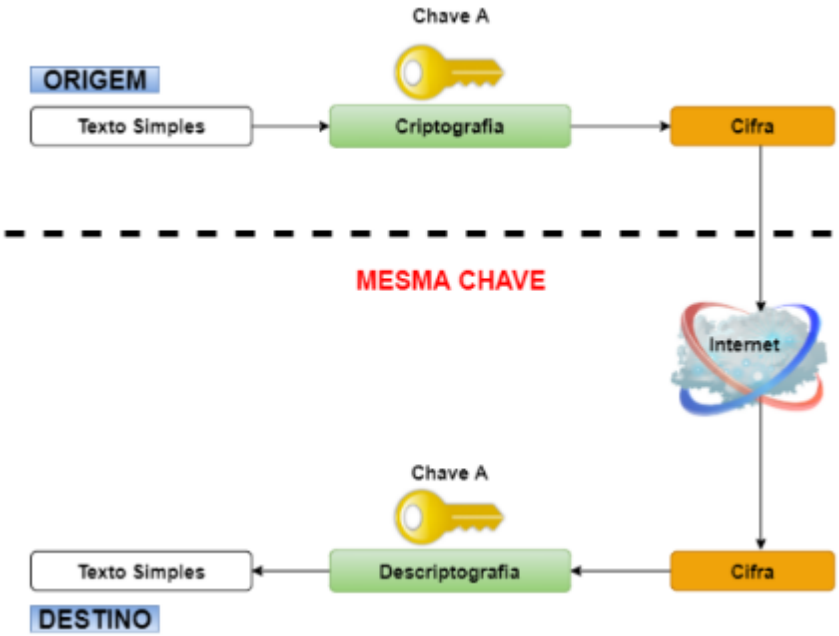


Figura 3.5: Criptografia de Chave simétrica
Fonte: (MACORATTI, 2010)

3.6.3 - Algoritmos de chave Assimétrica

De acordo com Oliveira (2012), nos algoritmos de chave assimétrica, as partes envolvidas na comunicação usam duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública. Na figura 3.6 observamos a diferença com a criptografia simétrica, pois há a utilização de chaves diferentes para o processo de criptografia.

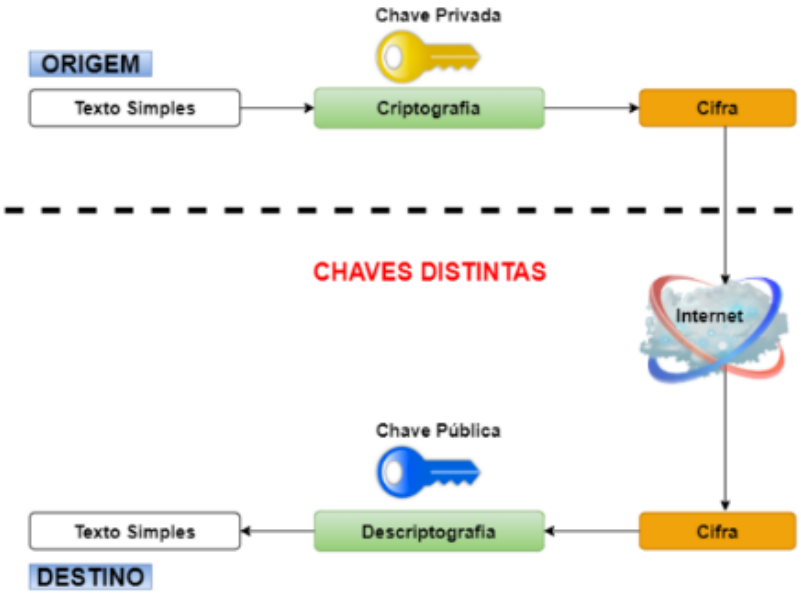


Figura 3.6: Criptografia de Chave assimétrica
Fonte: (MACORATTI, 2010)

3.6.4 – *Firewalls*

De acordo com Kurose (2014), um *firewall* é uma combinação de *hardware* e *software* que isola a rede interna de uma organização da Internet, permitindo que alguns pacotes passem e bloqueando outros. O *firewall* permite a um administrador de rede controlar o acesso entre o mundo externo e os recursos da rede que ele administra, gerenciando o fluxo de tráfego. Ainda segundo Kurose (2014), os *firewalls* podem ser classificados em três categorias:

3.6.4.1 - Filtros de Pacotes Tradicionais

Todo o tráfego que entra ou que sai da Internet, passa por um roteador de borda que conecta uma rede interna com seu provedor de Internet, como podemos ver na Figura 3.7. É nele que acontece a filtragem de pacotes, ou seja, um filtro de pacotes examina cada datagrama, determinando se deve passar ou ficar, baseado nas regras específicas definidas pelo administrador (KUROSE et al., 2014).

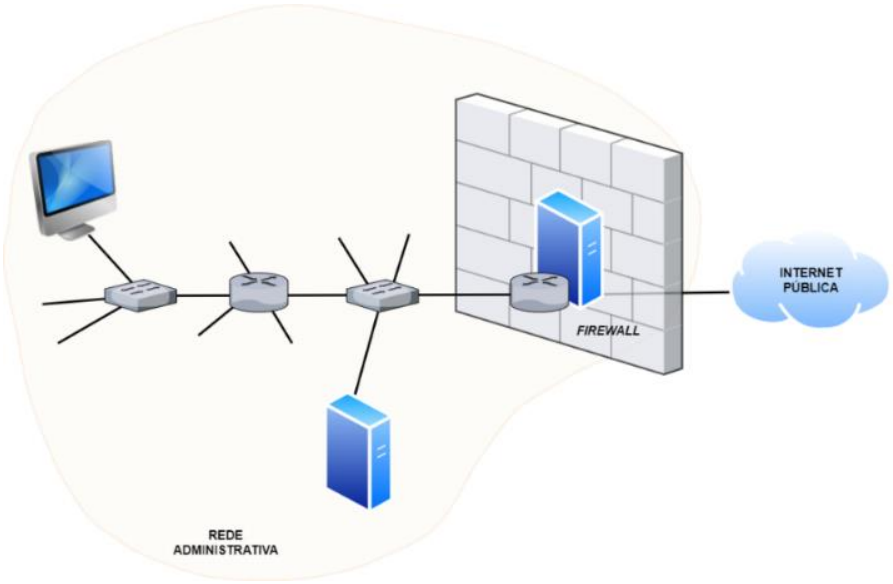


Figura 3.7: Filtro de Pacotes Tradicionais
Fonte: (KUROSE et al., 2014)

Ainda conforme Kurose (2014) estas regras são baseadas em:

a. Endereço IP de origem e de destino;
b. Tipo de protocolo no campo do datagrama (IP, TCP, UDP, ICMP, OSPF etc.);
c. Porta TCP ou UDP de origem e de destino;
d. Bits de flag do TCP: SYN, ACK etc.;
e. Tipo de mensagem ICMP;
f. Regras diferentes para datagramas que entram e saem da rede;
g. Regras diferentes para diferentes interfaces do roteador.

De acordo com Kurose (2014), um administrador de rede configura o *firewall* com base na política da organização. Tal política pode considerar a produtividade do usuário e o uso da largura de banda, bem como as preocupações com segurança da organização. Tabela 3.2 mostra exemplos de diversas políticas que uma organização pode ter, e como elas seriam endereçadas com um filtro de pacotes.

POLÍTICA	CONFIGURAÇÕES DE FIREWALL
Não há acesso exterior a Web	Descartar todos os pacotes de saída para qualquer endereço IP, porta 80
Não há conexões TCP de entrada, exceto aquelas apenas para o servidor Web público da organização.	Descartar todos os pacotes TCP SYN para qualquer IP exceto 130.207.244.203, porta 80
Impedir que rádios Web devorem a largura de banda disponível	Descartar todos os pacotes UDP de entrada - exceto pacotes DNS
Impedir que sua rede seja usada por um ataque DoS *smurf*	Descartar todos os pacotes *ping* que estão indo para o endereço de difusão (por exemplo, 130.207.255.255)
Impedir que a sua rota de rede seja rastreada	Descartar todo o tráfego de saída ICMP com TTL expirado.

Tabela 3.2 - Políticas e regras de filtragem correspondentes para uma rede da organização 130.27/16 com servidor Web 130.207.244.203 (KUROSE et al., 2014)

3.6.4.2 -Filtros de Pacotes com Estados

De acordo com Lima (2000), um filtro de pacotes com estados usa no seu processo de filtragem um conjunto de regras de filtragem, como no caso dos filtros tradicionais, e as informações de estados obtidas das conexões e sessões. A filtragem tradicional somente ocorre com o primeiro pacote da conexão ou sessão, ou seja, somente o primeiro pacote pertencendo a uma sessão ou conexão é verificado contra o conjunto de regras. Se este pacote é permitido, o *SPF* cria uma entrada para esta conexão ou sessão em sua tabela de estados. Deste momento em diante, os demais pacotes de uma conexão ou sessão somente serão permitidos se existir alguma entrada na tabela de estados para esta conexão ou sessão. Há tabelas de estados que acompanham o andamento de cada conexão ou sessão atravessando o filtro em um dado momento (LIMA, 2000).

3.6.4.3 - *Gateways* de Aplicação

Segundo Kurose (2014), um *gateway* de aplicação é um servidor, através do qual todos os dados da aplicação (que entram e que saem) devem passar. Vários *gateways* de aplicação podem executar no mesmo hospedeiro, mas cada *gateway* é um servidor separado, com seus próprios processos. Para exemplificar, suponha um tipo de *firewall* que permite apenas um conjunto restrito de usuários executar telnet (PINHO, 2000) para o exterior e impede que todos

os clientes externos executem telnet para o interior. Essa política pode ser aplicada pela execução da combinação de um filtro de pacotes (em um roteador) com um *gateway* de aplicação de telnet, como mostra a Figura 3.8.

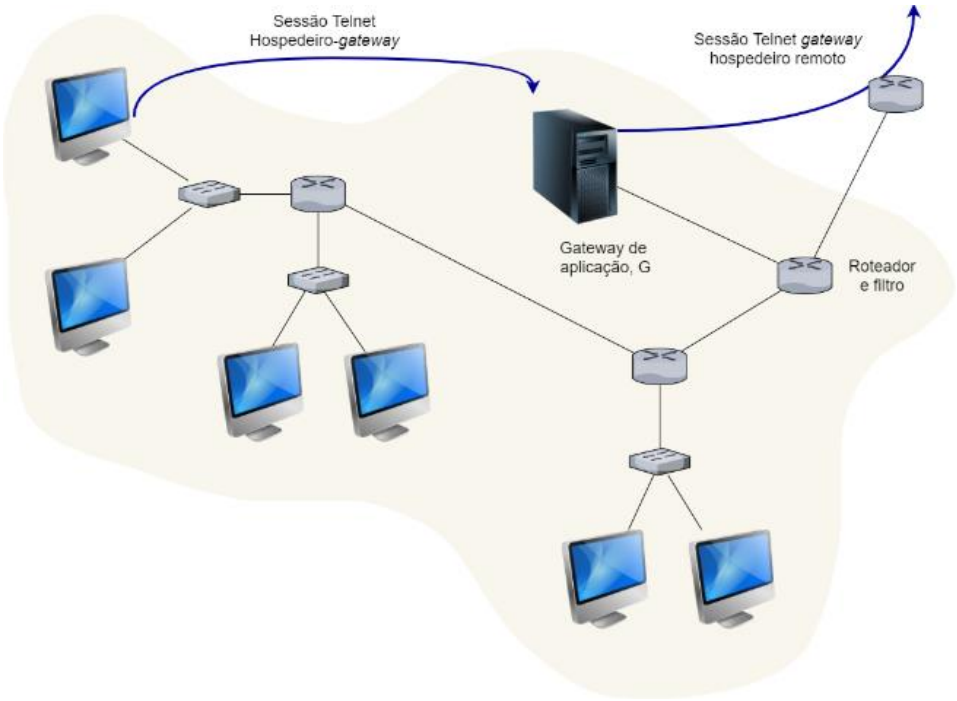


Figura 3.8: *Gateway* de Aplicação
Fonte: (KUROSE et al., 2014)

3.7 - Sistemas de Detecção de Intrusão (*IDS - Intrusion Detection System*)

Para Junior (2004), o sistema de detecção de intrusão pode ser visto como mais uma ferramenta para reforçar a política de segurança da informação de uma empresa. Um *IDS* é composto basicamente por dois dispositivos principais: o console de comando e o sensor (PROCTOR, 2001). “O sensor é o dispositivo responsável pela coleta de informação para análise de descoberta de uma invasão” (CROTHERS, 2003). O console de comando tem como função permitir o controle do sistema de detecção de intrusão, monitorar o estado do sensor e processar os alertas enviados pelo sensor (PROCTOR, 2001).

Segundo Moreno (2016), sistemas de detecção de intrusão é um nome genérico para quaisquer sistemas usados para detectar a presença de acessos não autorizados. Assim como o *firewall*, o balanceador de carga, estes sistemas podem ser implementados por *software* ou por *hardware*. Ainda de acordo com Moreno (2016), estes sistemas podem ser classificados em:

• **Sistemas de Detecção de Intrusão Baseado em Redes *(NIDS - Network Intrusion Detection System)*:** O sistema de detecção de intrusão baseado em rede monitora a atividade do tráfego em um determinado segmento de rede. A detecção é feita com a captura dos pacotes e análise comparativa com padrões ou assinaturas conhecidas pelo *NIDS* (GONÇALVES, 2015).

Segundo Shah (2001), uma característica relevante do *NIDS* é a sua possibilidade em detectar os ataques de rede em tempo real. Como o sensor atua em modo promíscuo no mesmo segmento de rede de um host atacado, por exemplo, ele pode capturar os pacotes referentes ao ataque, analisar e responder aproximadamente ao mesmo tempo em que o ataque é executado.

• **Sistemas de Detecção de Intrusão baseado em Host *(HIDS- Host-Based Intrusion Detection System)*:** O sistema de detecção de intrusão baseado em *host* faz o monitoramento do sistema, com base em informações de arquivos de *logs* ou de agentes de auditoria. O *HIDS* pode ser capaz de monitorar acessos e alterações em importantes arquivos do sistema, modificações nos privilégios dos usuários, processos do sistema, programas que estão sendo executados, uso da *CPU*, entre outros aspectos, como a detecção de *port scanning* (RANUM, 2001).

3.8 – Sistemas de Prevenção de Intrusão *(IPS – Intrusion Prevention System)*

Segundo Krause (2008) os IPS conciliam a propriedade de intensa verificação de pacotes com propriedades de filtragem inerentes aos *firewalls*. Conforme Coser (2011) o conceito de *IPS* tem semelhança com o conceito de *IDS*, pois tanto um quanto o outro detecta ameaças na rede. Porém um *IDS* detecta tentativas de intrusão, realiza o registro e/ou envia avisos ao administrador da rede, como mencionamos na seção 3.5. Já um *IPS* é projetado para agir no bloqueio automático de prováveis ataques, impedindo assim que o ataque seja bem sucedido, ou seja, o ataque não atingirá o seu alvo.

> Um *IDS* é como se fosse um alarme de um carro que soa somente quando alguém abre a porta, e um IPS dispara o alarme e trava as portas com o intuito de que o invasor não leve o carro (MAGGIORA, et al., 2008).

De acordo com Moreno (2016), o sistema *wIDS* é um sistema de defesa com finalidade de monitorar o tráfego e mostrar as tentativas de ataque em redes sem fio.

No estudo apresentado por (SILVA, 2010), em um *wIDS* o tráfego tido como suspeito é verificado e analisado em um intervalo de tempo que existe entre os *Beacons* (quadros de sinalização enviados periodicamente) de cada ponto de acesso, realizando assim as detecções das requisições, das frequências das requisições de reassociação, e de uma grande quantidade de requisições de autenticação. Por outro lado Moreno (2016), afirma que o *wIPS* tem como finalidade prevenir possíveis ataques antes de serem executados, ou seja, enquanto o *wIDS* monitora o *wIPS* protege.

3.9 – *Honeypot*

Segundo Hijazi (2004), a principal arma que podemos usar contra o inimigo é poder conhecer suas atitudes e conseguir prever o que ele pode fazer contra nós. No mundo da informática existe muito pouca informação de como são efetuados os ataques e como eles acontecem. Se não for possível conseguir prever o que o inimigo pode fazer contra o sistema, não tem como implementar meios para se proteger. Hoje existem algumas ferramentas para analisar o comportamento dos inimigos virtuais e analisar suas atitudes. Com essas ferramentas podemos conhecer o que ocorre após a invasão de um sistema e qual a atitude de um invasor depois que ele consegue comprometer o sistema.

Uma dessas ferramentas é o *Honeypot* (Pote de Mel). Esta ferramenta é instalada em um computador com o objetivo de ser atacado para analisar todos os dados que entram e saem do sistema e como ocorre uma invasão. Ainda segundo Hijazi (2004) os *honeypots* são sistemas criados para atraírem e serem comprometidos por um atacante, gerando um registro histórico de todas as ações feitas neste ataque. Após o comprometimento dos sistemas podemos extrair informações que auxiliem no mecanismo de defesa ou mesmo sejam utilizados como alertas de invasão. As máquinas com um *Honeypot* instalado executam serviços falsos, que respondem como seus originais, mas na verdade estão fazendo outras operações totalmente diferentes (HIJAZI et al., 2004).

De acordo com Assunção (2009), existem dois tipos de *honeypots* que falaremos a seguir: os de baixa interatividade e os de alta interatividade.

3.9.1 - *Honeypots* de baixa interatividade

Em um *honeypot* de baixa interatividade são instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir. Desta forma, o sistema operacional real deste tipo de *honeypot* deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. O *honeyd* é um exemplo de ferramenta utilizada para implementar honeypots de baixa interatividade (HOEPERS et al., 2007).

Em *honeypots* que tem serviços de baixa interação, todos os serviços, seja um *shell* do sistema ou um servidor de correio, são simulados (ASSUNÇÃO, 2009). O invasor nunca terá acesso ao sistema real, apenas a versões simuladas do mesmo. Entretanto, qualquer invasor com um nível mínimo de habilidade conseguirá detectar com grande rapidez um serviço de baixa interação (ASSUNÇÃO, 2009).

3.9.2 - *Honeypots* de alta interatividade

Nos *honeypots* de alta interatividade os atacantes interagem com sistemas operacionais, aplicações e serviços reais. Exemplos de *honeypots* de alta interatividade são as *honeynets* e as *honeynets* virtuais (HOEPERS et al., 2007).

Esses serviços de *honeypots* podem ser um programa que funcione como servidor de correio ou de transferência de arquivos. Pode também ser fornecido ao shell de comandos do seu sistema operacional, dando controle total. Então, em um sistema real com serviços que funcionem de verdade, esses serviços são de alta interação (ASSUNÇÃO, 2009).

3.10- Ferramentas utilizadas para a realização dos testes

3.10.1 - Suíte *AirCrack-ng*

Segundo Moretti (2014), o *Aircrack-ng* é uma ferramenta utilizada para recuperar chaves em redes com protocolos *WEP* e *WPA-PSK*. A recuperação da chave ocorre mediante a captura de pacotes e a quantidade varia de acordo com o tamanho da chave. Através de técnicas de otimização o *Aircrack-ng* consegue recuperar chaves de forma mais ágil quando comparado

a outras ferramentas com o mesmo propósito. Dentre as ferramentas no conjunto dessa suíte, podemos citar algumas na Tabela 3.3.

FERRAMENTA	FUNÇÃO
Airmon-ng	Converte nossa placa sem fio em uma placa sem fio de modo monitor, que significa que ela pode ver e receber todo o tráfego da rede.
Airodump-ng	Permite capturar pacotes de acordo com nossas especificações.
Aireplay-ng	É usado para gerar ou acelerar o tráfego no ponto de acesso. Isso pode ser especialmente útil em ataques como um ataque de negação de serviço, como um ataque de desautenticação (*Deauth*) que tira clientes do ponto de acesso, ataques de senha *WEP* e *WPA2*, bem como ataques de injeção e reprodução de *ARP*.
Aircrack-ng	Quebra da chave.
Besside-ng	Coleta de dados de *IVs*

Tabela 3.3- Ferramentas suíte *aircrack-ng*
Fonte: autoria própria

3.10.2 – *Bettercap*

BetterCap (LLERENA, 2020) é uma ferramenta poderosa, flexível e portátil que foi criada para executar vários tipos de ataques *MITM* (*man-in-the-middle*) contra uma rede. O *BetterCap*, em uma única ferramenta, proporciona ao pesquisador de segurança tudo o que é necessário para medir vulnerabilidades. Além disso, ele funciona nos sistemas *GNU* / *Linux*, *MacOS X* e *OpenBSD* (LLERENA, 2020).

Esta ferramenta possui muitos módulos para pesquisa de redes após a conexão a um segmento de rede. O uso mais direto da ferramenta é usar os módulos de varredura para identificar alvos próximos para direcionar ataques e, em seguida, tentar identificar redes com senhas fracas após capturar as informações necessárias (KINZIE, 2020).

3.10.3 – *Hashcat*

O *Hashcat* (ABELARDO et al., 2018) é uma ferramenta multiplataforma de código aberto e gratuita, otimizada para aproveitar ao máximo o poder de processamento das *GPUs* em placas gráficas e *CPUs* modernas.

Segundo Abelardo (2018), a vulnerabilidade do protocolo *WPA2* foi descoberta pela primeira vez em outubro de 2017 por Mathy Vahoef, e hoje os criadores do *Hashcat* (uma ferramenta de teste de segurança para *cracking* de senhas) descobriram uma nova vulnerabilidade, que ataca diretamente o roteador, e de maneira remota permite acesso ao *Peer Master Key Identifier* (*PMKID*). A descoberta deste novo ataque aconteceu acidentalmente, já que os desenvolvedores do *Hashcat* procuravam possíveis falhas no novo protocolo *WPA3*, que é considerado muito mais difícil de atacar. Para isso, são levadas em consideração três ferramentas: *Hcxdumptool*, *Hcxtools* e *Hashcat*. A Tabela 3.4 apresenta a função de cada uma delas.

FERRAMENTA	FUNÇÃO
Hcxdumptool	Uma ferramenta de captura de pacotes em dispositivos wlan, permitindo executar testes para estabelecer se os pontos de acesso ou clientes são inseguros.
Hcxtools	Permite converter os pacotes de captura para que possam ser usados com o último hashcat.
Hashcat	Ajuda a recuperação de senha mais rápida e avançada, que oferece suporte a cinco métodos de ataque exclusivos para mais de 200 algoritmos de hash altamente otimizados.

Tabela 3.4- Ferramentas *Hashcat*
Fonte: autoria própria

3.10.4. *Wifite* 2

O *Wifite* (ABELARDO, 2018) é uma ferramenta automatizada de teste de penetração sem fio que utiliza as ferramentas associadas ao *Aircrack-ng* e as ferramentas de linha de

comando *Reaver* (AVELINO, 2013) e *Pixie WPS* (MORENO, 2016). Isso permite ao *Wifite* a capacidade de capturar tráfego e credenciais de autenticação reversa para redes sem fio *WEP*, *WPA* e *WPS*.

Segundo Abelardo (2018), o *Wifite* foi projetado para usar os métodos conhecidos para recuperar a senha dos pontos de acesso sem fio. Que incluem:

- *WPS*: Ataque *offline* de Pixie-Dust.
- *WPS*: Ataque de *PIN* de força bruta *online*.
- *WPA*: Captura do *Handshake* + quebra *offline*.
- *WPA*: Captura do hash *PMKID* + quebra *offline*.
- *WEP*: Alguns ataques conhecidos contra o *WEP*, que incluem fragmentação, *Aireplay* etc.

A execução do *Wifite* seleciona os alvos e a ferramenta começa automaticamente a tentar capturar ou quebrar a senha. Ele foi projetado para funcionar com a versão mais recente do *Kali Linux* (WEIDMAN, 2014), também é compatível com o *ParrotSec* (OLIVEIRA, 2016), que é uma distribuição GNU / *Linux* baseada no Debian *Testing* e projetada com a segurança do desenvolvimento e a privacidade em mente. Outras distribuições *pentesting* (como *BackBox* ou Ubuntu) possuem versões desatualizadas das ferramentas que o *Wifite* usa (ABELARDO et al., 2018).

CAPÍTULO 4 – METODOLOGIA

Esta seção apresenta o processo adotado para avaliação de questões de segurança em redes sem fio. A metodologia proposta consiste em quatro etapas: A primeira consiste na elicitação das características do sistema e do escopo do estudo a ser realizado. A segunda etapa trata da definição dos protocolos e ferramentas que são utilizados para parametrizar o experimento que será construído. A terceira etapa consiste na construção do *testbed* a ser utilizado para representar uma rede sem fio. Por fim, consiste na definição dos cenários a serem avaliados e interpretação de resultados e diagnósticos.

A primeira etapa do processo trata sobre a caracterização do problema/sistema a ser avaliado, definição do escopo, identificação dos componentes relevantes (sob o ponto de vista de segurança) do sistema e interface entre estes componentes e demais componentes externos. Neste contexto, a finalidade principal da metodologia considerada é a análise de questões de segurança em uma rede sem fio assim como sugestão de medidas para a proteção de diferentes tipos de ataques. Para elucidar todas as características do sistema, temos que ter conhecimento de quais redes sem fio irão fazer parte do sistema, qual a tecnologia destas redes em termos de comunicação e de segurança e quais topologias estão sendo utilizadas entre os componentes das redes.

A segunda etapa refere-se à definição dos protocolos de comunicação e de segurança utilizados para a testagem, assim como na definição das ferramentas e dos componentes de *hardware* utilizados. Os protocolos de comunicação utilizados foram IEEE 802.11b/g/n, ao passo que os protocolos de segurança utilizados foram *WEP*, *WPA* e *WPA2*. Por fim, as ferramentas utilizadas foram *Aircrack-ng*, *Bettercap*, *Hashcat* e *Wifite 2*.

A terceira etapa detalha como foram utilizados os protocolos (comunicação e segurança) e as ferramentas para as medições, analises e configuração dos componentes do sistema que diretamente integram a rede sem fio. Foram feitas configurações nos pontos de acesso e nos computadores que se conectam a estes. Particularmente nos computadores foram instalados a ferramentas *Kali Linux* e *Virtual Box* a fim de proporcionar configuração para os ataques especificados. No ponto de acesso foram executadas as seguintes configurações: Protocolo *WEP* com senha pré-definida e em hexadecimal, protocolos *WPA* e *WPA2* com *WPS* ativo e

inativo, com os algoritmos de criptografia *TKIP* (STANGARLIN, 2012) e *AES* (MAIA, 2017) definido para testes com ataques aos protocolos *WPA* e *WPA2*, e senha pré-definida. Os componentes das redes testadas são heterogêneos em relação a diferentes características tais como: fabricantes, potência gerada pelas antenas em cada componente, versões de *softwares* (*firmwares*), ambientes de configurações, e suporte a protocolos de transmissão e de segurança.

Para conduzir o processo de ataques às redes sem fio, o sistema deve ser isolado, de maneira que a rede não sofra interferência com outros tipos de tráfegos, além dos especificados. Para realizar os ataques e assim propor as devidas melhorias, foram feitas as seguintes suposições.

Suposição 1: Roteador configurado com protocolo *WEP*, com o formato da chave em hexadecimal. Foi utilizada a ferramenta *Aircrack-ng*, onde fez o uso dos ataques: Ataque *Sniffer*, *ARP Poisoning* e força bruta. Foram utilizados os comandos *Airodump*, *Besside-ng* e *Aircrack-ng*.

Suposição 2: Roteador configurado com o protocolo *WPA2* e algoritmo de criptografia *PSK-TKIP* e *WPS* ativo. Foi utilizada a ferramenta *Bettercap*, onde foram utilizados os ataques: Ataque *Sniffer*, Captura de *Handshake*, e Ataque *Deauth*.

Suposição 3: Roteador configurado com o protocolo *WPA2* e algoritmo de criptografia *PSK-AES* e a senha definida. Também foi criado um arquivo.txt com várias senhas incluído a senha definida no roteador dentro, para simular um ataque de dicionário. Foi utilizada a ferramenta *Hashcat*, e com ela os ataques: Ataque *Sniffer*, Captura de *PKMID* e ataques de Dicionário.

Suposição 4: Roteador configurado com o protocolo *WPA* e algoritmo de criptografia *PSK-AES* com *WPS* ativo, e senha definida. Foi utilizada a ferramenta *Wifite2* e com ela os ataques: Ataque *Sniffer*, Captura de *Handshake*, Captura de *PMKID*, Ataque *Pixie-Dust WPS*, Ataque *PIN Attack* (ABELARDO, 2018).

Após a realização dos testes, a funcionalidade de tais ferramentas foi verificada, algumas se mostrando mais efetivas para alguns tipos de ataques que outras, e a vulnerabilidade de alguns protocolos junto com funções no ponto de acesso, levando a repensar na escolha do protocolo mais adequado a segurança da rede e em uma senha mais forte definida.

CAPÍTULO 5 - ESTUDO DE CASO

O objetivo desse estudo de caso é simular ataques contra uma rede sem fio em um ambiente doméstico e em redes de pequeno porte, realizando ataques com o uso de ferramentas específicas para cada tipo de ataque, afim de identificar a vulnerabilidade naquela rede, seja ela no protocolo utilizado, na tecnologia, no algoritmo de criptografia, ou até mesmo numa simples escolha de uma senha.

Todos os testes foram realizados em ambiente doméstico e foram necessários os equipamentos descritos a seguir.

- Um Computador *Desktop*
- *VirtualBox, VirtualBoxExtention Pack* e o *VirtualBoxguestaddiction*.
- Máquina Virtual com o Kali Linux 2.
- Adaptador *wireless* USB, o utilizado foi o Ralink *Technology* Corp. MT7601U *Wireless Adapter*.
- Ponto de acesso.

As configurações do ponto de acesso variam de acordo com a ferramenta utilizada, pois diferentes ferramentas utilizam diferentes métodos para obter sucesso na captura de informações e quebra da senha.

Na Figura 5.1, demonstramos a rede doméstica usada para os testes. Temos um AP utilizado apenas para os testes chamado de *AP* Teste, que estava conectado ao roteador principal, chamado *AP Link DSL*, onde chega o *link* de Internet. Além dele temos um *notebook* que foi usado para realizar os ataques, chamado de *Notebook* com *Kali* e adaptador *Wi-fi* além de outros 2 dispositivos conectados ao *AP* Teste. Os demais dispositivos são dispositivos que estão conectados ao roteador *AP Link DSL*, ficando assim, de fora dos testes.

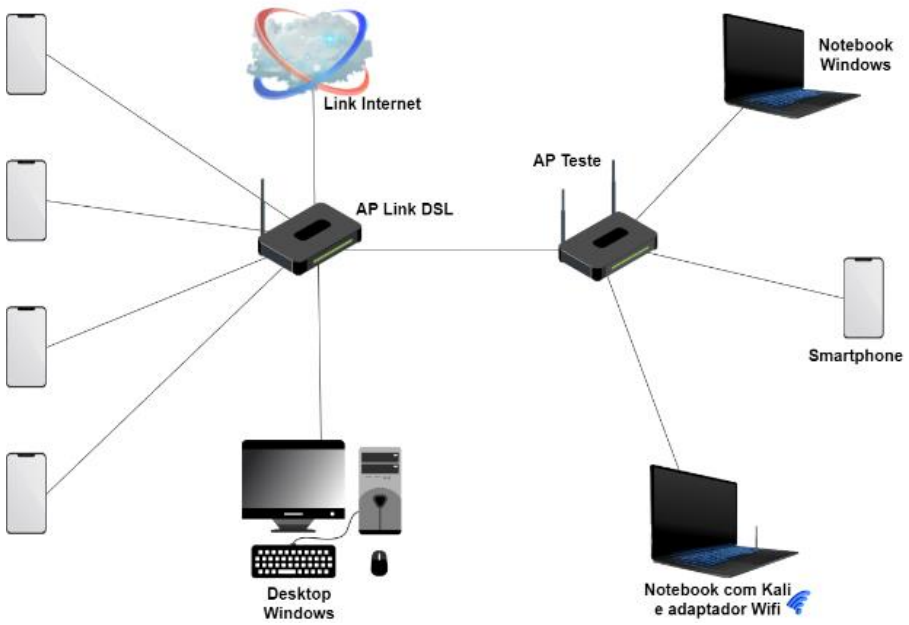


Figura 5.1 - Diagrama da rede doméstica
Fonte: Autoria própria

Na Tabela 5.1 mostramos a relação das ferramentas que foram utilizadas em nossos testes. Vale ressaltar que não foram usados especificamente todos os ataques que elas são capazes de executar, mas apenas os que julgamos mais eficazes para cada vulnerabilidade proposta.

Ferramentas	**Ataques**
Bettercap	Ataque *Sniffer*, Captura de *Handshake*, Ataque *Deauth* (*DOS*).
Hashcat	Ataque *Sniffer*, Captura de *PMKID*, Ataque de Dicionário.
Aircrack-ng	Ataque *Sniffer*, Força Bruta.
Wifite2	Ataque *Sniffer*, Ataque de Dicionário, Captura de *Handshake*, Captura de *PMKID*.

Tabela 5.1 – Ferramentas e Ataques
Fonte: Autoria própria

5.1. Ataques utilizados nesse estudo de caso

Nesse estudo de caso foram utilizados ataques a rede sem fio com várias finalidades, sejam elas como varredura de dispositivos na rede, captura de *handshakes*, injeção de pacotes, força bruta, e etc. Abaixo estão listados os ataques utilizados.

- **Ataques de Dicionário**

Um ataque de dicionário faz uso de *wordlists* que podem incluir amplos dicionários e por vezes intensamente especializado (SILVA et al., 2007). Este tipo de ataque faz tentativas de desvendar uma determinada senha analisando todas as palavras ou combinações de palavras contidas na *wordlist*, conforme visto na seção 3.3.3. Muitos usuários fazem uso de senhas com combinações bastante comuns, o que torna muito provável o sucesso do ataque pois existem muitas *wordlists* pela Internet repletas desse tipo de combinações.

- **Ataque de Força Bruta**

De acordo com Diorio (2019), um ataque do tipo força bruta objetiva decifrar, de forma exaustiva através de tentativa e erro, logins e senhas de acesso de usuários legítimos de determinado serviço de rede e/ou sistema, tornando-se uma das mais populares e principais ameaças, conforme apresentado na seção 3.3.4 deste trabalho.

- **Ataque de *Sniffer***

Um ataque do tipo *sniffer* é praticado com o auxílio de ferramentas de “escuta de tráfego” e pode ser usado para o bem ou para o mal (ALBUQUERQUE, 2008). Caso seja usado para o bem, serve como ferramenta de suporte ao administrador na análise do tráfego na rede. E se for usado para o mal, pode ser uma ferramenta de ataque para o roubo de informações dentro da rede. Este tipo de ataque pode ser visto com mais detalhes na seção 3.3.5 deste trabalho.

- **Ataque *PMKID* (Identificador de Chave Mestra em Pares)**

De acordo com Fousekis (2018), um ataque *PMKID* consiste no *PMK* (Chave Mestra em Pares), um recurso do *RSN* (Rede de Segurança Robusta) que inclui o nome do *PMK*, o endereço *MAC* do ponto de acesso e o endereço *MAC* da estação. Para mais detalhes ver a seção 3.3.10, que trata do mesmo ataque. Todos estes dados são processados pelo algoritmo *HMAC-SHA1-128* (KRAWCZYK et al., 1997), resultando em um valor de *hash*. (FOUSEKIS, 2018) afirma que um ataque contra o *RSN IE* (Elemento de Informações de Rede de Segurança Robusta) de um único quadro *EAPOL* para capturar as informações necessárias para tentar um ataque de força bruta.

- **Ataque *Deauth* (*Deauthentication*)**

De acordo com Moreno (2016), ataques de *Deauth* são ataques que enviam um pacote para o ponto de acesso desautenticando todos da rede sem fio. E o pior lado desse ataque é que o atacante não precisa ter a senha ou estar conectado na rede em que queira realizar o ataque. Ainda conforme Moreno (2016), neste tipo de ataque existe a possibilidade de desautenticar o cliente somente uma vez ou deixar essa desautenticação por um tempo indefinido, até que o atacante determine a hora de parar. Este ataque também pode ser considerado um ataque de negação de serviço (*DoS*), já que sua ação faz com que o serviço fique inoperante, em nosso caso o ponto de acesso, os clientes que foram desconectados ficam sem conseguir reconectar durante um tempo.

- **MAC *Spoofing***

De acordo com Castro (2008) nesse tipo de ataque o endereço físico da placa de rede é falsificado. É bastante simples falsificar este endereço, já existem diversas ferramentas que ajudam a forjar este endereço alterando o endereço *MAC*. Na seção 3.3.2 podemos ver o mesmo ataque com maiores detalhes.

5.2 – Ferramentas utilizadas neste estudo de caso

5.2.1 - Suíte *AirCrack-ng*

Neste teste com o *Aircrack-ng* serão utilizados os seguintes ataques: ataque de *sniffer*, e força bruta, e testaremos a vulnerabilidade do protocolo *WEP*. A suíte já vem pré-instalada no *Kali Linux* por padrão, caso fosse utilizado outra distribuição seria necessário instalar com o comando:

#apt-get install aircrack-ng

Após instalado, o primeiro passo é colocar a placa de rede em modo promíscuo, ou modo monitor como é popularmente conhecido. Ele é usado para obter informações acerca das redes onde a placa de rede alcança.

#airmon-ng start wlan0

Após a placa estar em modo monitor em nossa estação nomeada como Notebook com *Kali*, vamos executar o *airodump-ng* com a nossa interface em modo monitor e usamos o argumento **–encrypt WEP** como filtro para buscar apenas por redes *WEP* próximas.

#airodump-ng wlan0mon --encrypt WEP

O *airodump-ng* verificará a área em busca de pacotes usando a criptografia *WEP*, retornando o nome e as informações da rede, se houver, como podemos ver no Anexo B. Como saída desse comando, nós obtemos informações como:

- **BSSID:** Número *MAC* do dispositivo;
- **PWR:** Intensidade do sinal captado pelo dispositivo *wifi* (quanto menor melhor);
- **Beacons:** Número de pacotes *beacons* que o ponto de acesso enviou;
- **#Data:**Número de pacotes de dados capturados (se utilizar criptografia *WEP*, contagem de *IVs*), incluindo os pacotes de transmissão de dados;
- **#/s:** Número de pacotes de dados por segundo capturados nos últimos 10 segundos;
- **CH:** Número do canal que está sendo utilizado no momento;
- **MB:** Velocidade máxima suportada pelo ponto de acesso.

- **ENC:** Algoritmo de criptografia que está sendo usado.
- **CIPHER:** A cifra detectada
- **AUTH:** O protocolo de autenticação usado.
- **ESSID:** Mostra o nome da rede sem fio. O chamado "SSID", que pode estar vazia se SSID oculto é ativado.

Depois da varredura feita em nosso notebook *Kali* em busca de informações, vamos utilizar outra ferramenta que faz parte do pacote *aircrack-ng*, é o ***besside-ng***, com ele capturaremos os vetores de inicialização (*IVs*) necessários para decifrar o *WEP*. Vetores de Inicialização são uma entrada de tamanho fixo a uma primitiva de criptografia que é normalmente necessária para ser aleatório ou pseudoaleatório. Sendo assim, capturaremos os *IVs* gerados e inserimos no arquivo **wep.cap**.

Para iniciar o ataque, digitamos o seguinte comando:

 # besside-ng wlan0mon -c *3* -b <Endereço_MAC_AP>

Onde **wlan0mon** se refere a interface, o –c ao canal que o *AP* está, e **–b** o bssid da rede, popularmente chamado de *MAC*.

Enquanto o ataque prossegue, o Besside-ng registrará todos os dados coletados em um arquivo **.cap**. Podemos executar o *Aircrack-ng* no arquivo **.cap** à medida em que é adicionado mais dados gerados pelo **Besside-ng**, e todos os seus *IVs* coletados estarão lá. Isso significa que podemos executá-lo mais vezes e reunir mais *IVs* no arquivo **.cap** até que possamos quebrá-los para obter a senha executando o *Aircrack-ng*.

Para tentar quebrar a rede *WEP* das informações coletadas, precisamos executar o *Aircrack-ng* com o local do arquivo **.cap** como argumento. Geralmente fica salvo no diretório raiz. Executaremos o seguinte comando:

 # aircrack-ng ./wep.cap

Esse comando lerá o arquivo **.cap** e permitirá que você selecione a rede que deseja quebrar dentre as que o Besside-ng encontrou. Se salvou *IVs* suficientes, pode quebrar a senha imediatamente ou deixá-la em execução enquanto Besside-ng é executado, e o ataque será repetido automaticamente a cada 5.000 *IVs* até que seja bem-sucedido. Para conseguir

quebrar a senha, são necessários geralmente um valor em torno de 25.000 *IVs* para obter sucesso. A quebra é feita rápida em questão de segundos.

Conforme descrito no Anexo E podemos ver a chave *WEP* encontrada, em *ASCII*.

5.2.2 – *Bettercap*

Neste teste, utilizaremos o *Bettercap* em nossa estação Notebook Kali. Com o *Bettercap* serão utilizados os Ataque de *Sniffer* e o Ataque *Deauth*, ou ataque de desautenticação. O *Bettercap* já vem previamente instalado no Kali Linux, então é necessário apenas executar, ou caso esteja sendo testado em outra distribuição, instalar com o comando:

 # sudo apt-get install bettercap

Após instalado, deixamos a interface em modo monitor com o *aircrack-ng*.

 # airmon-ng start wlan0

Com a placa em modo monitor, podemos executar o *Bettercap* informando a interface usada com o argumento **-iface**

 # sudo bettercap --iface wlan0mon

Digitando o comando **-help** podemos ver uma lista de todos os módulos em execução e comandos. Nos módulos, podemos ver que o módulo Wi-Fi não é iniciado por padrão no Anexo G. Para nosso teste selecionaremos o módulo de reconhecimento Wi-Fi, para iniciá-lo digitamos o comando:

>> **wifi.recon**

Com o comando em execução, começaremos a receber uma grande quantidade de mensagens assim que as redes começarem a serem detectadas. Quando o volume de informações na tela é muita, podemos desabilitar com o comando:

>> **events.stream.off**

Ao final, para visualizarmos a lista das redes, executamos o comando:

>> **wifi.show**

Podemos ver no Anexo J muitas informações sobre o ambiente sem fio nas proximidades, como quais redes são mais fortes, os tipos de criptografia que usam, se utilizam WPS, canais, clientes conectados, etc. Podemos ver também duas redes com a criptografia em vermelho, são as mesmas que com o comando acima **wifi.recon** também ficaram em vermelho, detectando assim *handshakes* nessas redes, com isso podemos tentar forçá-las. Vamos usar o módulo **deauth** para tentar obter *handshakes*.

Para iniciar o módulo *deauth*, digitamos **wifi.deauth** e em seguida como argumento o endereço MAC do ponto de acesso que desejamos atacar.

>> **wifi.deauth <Endereço_MAC_AP>**

Pode ser utilizado o argumento **all** ou ***** caso o ataque seja direcionado a todas as redes, mas esse não é o nosso objetivo, e sim apenas testar com o nosso ponto de acesso que faz parte de nosso ambiente de testes, a rede **"TP-Link".**

Depois de permitir que a ferramenta seja executada por alguns minutos, podemos ver os resultados digitando:

>> **wifi.show**

Em nosso exemplo, podemos ver que conseguimos capturar *handshakes*. Foi um bom resultado, em nosso caso conseguimos capturar *handshakes* pois haviam 2 clientes conectados à rede, mas algumas das redes que foi feito varredura não tem clientes conectados, como pode ser visto no Anexo K, seria necessário utilizar outro método, de ataque ao *PMKID*, que veremos mais na frente com outra ferramenta em nosso estudo de caso. Para salvar os *handshakes* capturados, usamos o comando **set wifi.handshake** seguido pelo diretório em que deseja salvar o arquivo.

wlan0mon > set wifi.handshakes '/root/bettercaphandshake'

Com o *Bettercap* conseguiremos coletar as informações necessárias para as redes sem fio mais próximas. Se abrirmos o arquivo *Bettercap* gerado a partir dessas capturas, podemos ver as informações que ele salvou. A partir disso podemos utilizar outras ferramentas para o ataque de força bruta.

5.2.3 – *Hashcat*

Neste teste com o Hashcat serão utilizados os Ataque de *Sniffer*, Ataque *PMKID*, e ataque de Dicionário.

O Hcxdumptool e o hcxpcaptool são ferramentas escritas para auditoria e teste de penetração em redes sem fio, e permitem interagir com redes sem fio próximas para capturar *handshakes WPA* e *hashes PMKID.*

Vale lembrar que nem todas as redes são vulneráveis ao ataque ao *PMKID***.** Como este é um campo opcional adicionado por alguns fabricantes, não se deve esperar sucesso total com esta técnica. Em nosso caso utilizamos um ponto de acesso onde obtivemos sucesso. Capturar o ***PMKID*** depende se o fabricante do ponto de acesso incluiu esse campo e se for possível quebrar o ***PMKID*** capturado depende se a senha subjacente está contida na sua lista de senhas de força bruta. Se uma das condições não for atendida, esse ataque falhará.

Primeiramente vamos instalar as ferramentas necessárias com o comando:

#git clone https://github.com/ZerBea/hcxtools.git

Após baixar, mudar para o diretório **hcxtools/** e executamos os comandos **make** e **make install**. Os comandos **make** e **make install** são utilizados para instalação de aplicações onde não é por meio de algum executável, mas sim através da compilação a partir do código fonte.

#cd hcxtools/
 # make

#makeinstall

Depois de terminado a instalação do **hcxtools**. Abriremos uma nova janela do terminal e instalaremos da mesma forma o **hcxdumptools.** E em seguida, mudamos para o diretório e executamos o **make** e **makeinstall** como antes.

#git clone https://github.com/ZerBea/hcxdumptool.git
#cd hcxdumptool/
 # make
#makeinstall

Após este procedimento, só falta instalar o hashcat. Por padrão no *kali linux* ele já vem instalado, caso não esteja instalado em outra distribuição, basta apenas digitar o comando:

#sudo apt-get install hashcat

Após a instalação vamos dar o comando abaixo para que ative em nosso adaptador para redes sem fio em modo monitor, como já fizemos nos outros testes anteriores utilizando o **airmon-ng.**

#airmon-ng start wlan0

Com o ambiente pronto para capturar o *PMKID* dos dispositivos e com o adaptador de rede em modo monitor, basta executarmos o comando:

#hcxdumptool -i wlan0mon -o galleria.pcapng --enable_status=1

Os argumentos utilizados foram os seguintes:

- **-i =** Informa ao programa qual interface estamos usando, neste caso, wlan1mon.
- **-o =** Informa o nome do arquivo no qual salvaremos os resultados, ou seja, os *PMKIDs* capturados.

Embora você possa especificar outro valor de ***status***, vamos utilizar o valor **1,** para habilitar mensagem de status.

Quando reunir o suficiente de *hashes PMKID*, podemos parar o programa utilizando **Control+C** para finalizar o ataque. Isso deve produzir um arquivo **PCAPNG** contendo as informações necessárias para tentar um ataque de força bruta, mas precisaremos convertê-lo para um formato que o Hashcat possa entender.

Para converter o arquivo **PCAPNG**, usaremos hcxpcaptool com alguns argumentos especificados. Na mesma pasta em que seu arquivo. **PCAPNG** é salvo, executaremos o seguinte comando em uma janela de terminal.

 # hcxpcaptool -E essidlist -I identifylist -U usernamelist -z galleriaHC.16800 galeria.pcapng

Este comando quer dizer ao hxcpcaptool para usar as informações incluídas no arquivo para ajudar o *Hashcat* a entendê-lo com os argumentos **-E**, **-I** e **-U**. Onde **-E** indica a lista de saída de palavras para ser usada como lista de palavras na quebra da senha, o **-I** indica a lista de saída de identidade não classificada, o **-U** indica a saída da lista de nomes de usuário não classificada, o argumento **-Z** é indicado para a saída do arquivo *PMKID*, usado para definir o nome do arquivo recém-convertido para uso do Hashcat, e a última parte do comando é o arquivo **PCAPNG** que queremos converter.

Como resultado, podemos ver no Anexo N, foi capturado apenas 1 ***PMKID*** num pequeno período de tempo, quanto mais tivesse melhor, mas esse ***PMKID*** encontrado foi o suficiente. Com isso, podemos usar o arquivo "galleriaHC.16800" no *Hashcat* para tentar decifrar senhas de rede.

Para começar a atacar, precisamos escolher uma boa lista de senhas. Existem algumas boas na *web* como a **SecList**, já pronta. Em nosso caso usamos uma lista própria com várias senhas, entre elas incluindo a senha real, no arquivo **topwifipass.txt**. Depois de ter uma lista de senhas, colocamos na mesma pasta que o arquivo “galleriaHC.16800” que acabamos de converter e executamos o seguinte comando em uma janela do terminal.

#hashcat -n 16800 galleriaHC.16800 -a 0 --kernel-accel=1 -w 4 --force “topwifipass.txt”

Neste comando, estamos iniciando o *Hashcat* no modo 16800, que serve para atacar os protocolos de rede *WPA-PMKID-PBKDF2*. A seguir, especificaremos o nome do arquivo onde temos a captura, neste caso, "galleriaHC.16800". O argumento **-a** indica quais tipos de ataque usar, nesse caso, um ataque "direto" e, em seguida, os argumentos **-w** e **--kernel-accel = 1** especificam o perfil de carga de trabalho de mais alto desempenho. Se o computador apresentar problemas de desempenho, pode diminuir o número no argumento **-w**. Em seguida, a opção **--force** ignora todos os avisos para prosseguir com o ataque, e a última parte do comando especifica a lista de senhas que estamos usando para tentar forçar brutalmente os *PMKIDs* em nosso arquivo, neste caso, chamado "**topwifipass.txt**"

Dependendo da velocidade do *hardware* e do tamanho da lista de senhas, isso pode levar algum tempo para ser concluído. Quando a lista de senhas estiver chegando ao fim, o Hashcat ajustará automaticamente a carga de trabalho e fornecerá um relatório final quando estiver concluída. Finalizando o ataque, no Anexo O podemos ver que em **Candidates.#1** temos a senha revelada ao lado. **Candidates.#1 = "senha"** significa que dentre as senhas que foram testadas no dicionário, a senha real encontrada foi a que é mostrada ao lado.

5.2.4 – *Wifite 2*

Neste teste com o *Witife2*, serão utilizados os Ataque de *Sniffer*, Ataque *PMKID*, Ataque *WPS Pixie-Dust*, Ataque *PIN* e Ataque de Força Bruta.

O *Wifite2* é uma ferramenta poderosa que automatiza a invasão a uma rede sem fio, permitindo selecionar alvos dentro do alcance e deixar o próprio "*script*" da ferramenta escolher a melhor estratégia para cada rede, não tendo sucesso em uma, ele segue para a próxima estratégia ou técnica. O *Wifite2* segue um fluxo de trabalho simples, mas eficaz, para invadir redes próximas em pouco tempo.

Para instalarmos o *Wifite2* em nossa máquina vamos dar os seguintes comandos:

 # git clone https://github.com/derv82/wifite2.git

 # cd wifite2

 # pythonsetup.py install

Em seguida colocamos o adaptador sem fio em modo monitor com o comando:

#airmong-ng start wlan0

Para iniciarmos devemos saber em que canal estamos atacando, podemos selecioná-lo adicionando o comando **-c** seguido pelo número do canal. Executamos uma varredura no canal 11 e encontramos 5 destinos diferentes, como podemos ver no Anexo P. Desses destinos, dois têm clientes conectados, um tem *WPS* ativado e todos estão usando a segurança *WPA*. Em nossa pesquisa podemos ver que o número 2 pode se apresentar como o melhor alvo, pois está em bom alcance, e está com *WPS* ativo. Embora não haja clientes conectados, provavelmente podemos receber um *handshake* com o ataque ***PMKID***, mesmo que ninguém esteja conectado.

Se estivermos procurando senhas fracas, as três primeiras redes têm a força de sinal mais forte, enquanto os alvos 1 e 3 têm a melhor chance de obter um *handshake* para tentar ataque de força bruta mais tarde. Se quisermos escolher as redes mais prováveis, podemos selecionar os alvos 1, 2 e 3 para a probabilidade de um *handshake* rápido ser capturado e quebrado, se o *PIN WPS* não for quebrado primeiro. Como o nosso *AP* para testes é o alvo 2, iremos utilizar ele como opção de ataque.

Se quisermos focar em alvos fáceis, podemos dar comandos à ferramenta para exibir apenas alvos vulneráveis a um determinado tipo de ataque. Para mostrar apenas alvos com WPS, podemos executar o ***Wifite2*** com a *flag* **-wps**. Assim como também podemos usar **-wep** ou **–wpa**, para os protocolos de segurança *WEP* e *WPA* respectivamente.

Em nosso exemplo foi utilizado a rede "***TP-Link***", um ponto de acesso instalado para testes. Utilizando criptografia ***WPA*** com ***WPS*** ativado. Então colocamos a opção de número 2 equivalente a rede *TP-Link*. Depois de selecionar o número da rede que desejamos atacar, o Wifite2 continuará com os ataques mais convenientes contra a rede.

No Anexo Q podemos ver que, o ataque ***WPS-Pixie*** falhou, atingiu o tempo limite rapidamente, por isso perdemos um tempo mínimo explorando esse caminho de ataque. O *PIN attack* foi interrompido por nós mesmos por conta do tempo espera, continuando então com o ataque de captura de ***PMKID*** que também falhou, e próximo *WPA handshake* nós obtivemos um handshake, e com isso capturamos a senha, podemos ver a mensagem *Cracked WPA handshake PSK*, com a senha logo em seguida.

Quando a senha é quebrada, é gerado um arquivo chamado cracked.txt, podemos visualizar se dermos o comando:

cat cracked.txt

Podemos ver no Anexo R a senha no campo *Key*, assim como outras informações, como o arquivo do *handshake* capturado, o *MAC* do ponto de acesso, o tipo de criptografia, etc.

Também podemos quebrar a senha, caso não obtenha sucesso diretamente com o *handshake*, configurando a *flag--dict* para definir o arquivo que contém senhas para quebrar, o padrão sendo definido como /usr/share/wordlists/fern-wifi/common.txt. Essa lista de senhas contém muitas senhas comuns, podemos usar nossas próprias ou baixar uma lista já pronta com milhares de senhas. Ao adicionar um bom arquivo de senha, podemos melhorar nossas chances de quebrar uma senha de rede sem fio, mesmo que os ataques *WPS* mais rápidos falhem.

Abaixo seguem alguns procedimentos que podem ser utilizados nessas redes para diminuir o risco de vulnerabilidades e possíveis ataques contra as mesmas.

- Senha Forte, com mais de 8 dígitos sendo com letras caixa alta e caixa baixa, números e caracteres.
- Não ativar a função *WPS*, pois torna a rede vulnerável a alguns tipos de ataques.
- Utilizar protocolos de segurança mais novos, como o *WPA2* e *WPA3* se for o caso de roteadores recentes. Deixando de lado protocolos como o *WEP* que são mais vulneráveis.
- Utilizar Algoritmos de Criptografia mais atuais como é o caso do *AES*.
- Em caso de uma rede em uma empresa de pequeno porte pode ser utilizado como alternativa um servidor *RADIUS* (*Remote Authentication Dial-In User Server*) para autenticação de usuários na rede. Podendo utilizar certificados digitais para autenticar usuários.
- Manter o *Firmware* do roteador sempre atualizado, pois empresas podem lançar atualizações com correções de algumas vulnerabilidades detectadas.

CAPÍTULO 6 – CONCLUSÃO

Este trabalho apresenta uma análise a respeito das vulnerabilidades encontradas numa rede sem fio doméstica, que também se aplicam em empresas de pequeno porte. Tal análise visa propiciar um entendimento sobre ameaças existentes em uma rede sem fio, assim como conhecer suas vulnerabilidades e então poder aplicar algumas medidas de segurança afim de manter a rede mais segura acerca dessas possíveis ameaças.

Ao decorrer do trabalho, pudemos entender como ocorre o processo de ataque em cada tipo de ameaça mencionada. Inicialmente são encontrados os pontos fracos de uma rede sem fio, sejam eles uma senha fraca, o uso de um protocolo com tecnologia mais defasada, ou uso de algum mecanismo que facilita a quebra de senha, e com o uso de algumas ferramentas conseguimos explorar algumas de suas falhas. As vulnerabilidades encontradas nesse tipo de rede são várias e com a evolução das ferramentas de ataques novas falhas aparecerão, e em decorrência dessas falhas novos métodos de segurança também surgirão.

Destacamos também que para haver uma segurança mais efetiva nesse tipo de rede, se faz necessário que o administrador não faça uso somente das ferramentas de *Pentest* aqui mencionadas (no intuito de averiguar a segurança de sua rede), mas que tome algumas medidas e adote uma política de segurança na sua rede. Com uma senha mais forte e uma configuração correta, torna-se mais difícil a obtenção de sucesso no ataque realizado por parte do possível invasor.

No caso das empresas, o comportamento deve ser um pouco semelhante ao do usuário doméstico, porém com o compromisso de se elaborar regras de segurança e disseminá-las extensivamente por todos os seus níveis, dado que nós mesmos, num ato de imprudência ou descuido, podemos divulgar informações expressivas sobre a rede.

Com isso, reafirmamos e concluímos nossos objetivos em especificar conceitos fundamentais relacionados à segurança em redes sem fio, apresentar algumas falhas de segurança em redes sem fio, observar os protocolos de segurança que são amplamente utilizados na atualidade, executar os testes de ataques em redes sem fio de forma isolada da rede, e por fim sugerir algumas mudanças para restringir a insegurança em relação às falhas apresentadas,

como uma senha forte acima de 8 caracteres, com caixa alta e caixa baixa, letras, números e caracteres especiais; *WPS* desativado, usar os protocolos *WPA2* ou *WPA3* como protocolos de segurança; *AES* como algoritmo de cifra / criptografia; *Firmware* do *AP* sempre atualizado e por último usar *WPA2* em conjunto com um servidor de autenticação, como o servidor *RADIUS*.

Como trabalhos futuros, pode-se apontar:

- Implementação e realização de testes com o protocolo *WPA3* que com o passar do tempo irá se tornar mais comum e utilizado globalmente;
- Além da implementação citada anteriormente, a implementação de uma política de segurança para ser usado no âmbito empresarial de pequeno porte;

Outro trabalho futuro se diz respeito a implementação de *IDS* e/ou *IPS* para realização de testes de penetração nas redes sem fio, afim de detectar qualquer ação de invasão a rede e tomar as medidas de proteção cabíveis

REFERÊNCIAS

ABELARDO, S. R. J. **Análisis de la Vulnerabilidad en el WPA2 usando la Metodologia PMKID en puntos de Accesos del Cantón Naranjito**. Dissertação (Engenheiro em Sistemas Computacionais) - Universidad Estatal de Milagro - Facultad Ciencias de la Ongeniería. Milagro - ECU. 2018.

AIRCRACK-NG. **aircrack-ng.org**. Disponivel em: <https://www.aircrack-ng.org/>. Acesso em: 18 Abril 2019.

ALBUQUERQUE, A. F. D. **Estudo de Métodos de Proteção de Redes Wireless**. Monografia (Pós Graduação Lato Sensu em Redes de Computadores e gerenciamento de Ativos) - UTFPR – Universidade Tecnológica Federal do Paraná, Campus Medianeira. Medianeira - PR - Brasil. 2008.

ALMEIDA, P. J. **Criptografia e Segurança**. Departamento de Matemática da Universidade de Aveiro - Portugal. Aveiro - POR. 2012.

ANDRADE, L. P. et al. **Análise das Vulnerabilidades de Segurança Existentes nas Redes Locais sem fio: Um Estudo de Caso do Projeto WLACA**. TCC (Estudo de caso) Universidade Federal do Pará - UFPA. Belém - PA - Brasil. 2008.

ASSUNÇÃO, M. F. A. **Honeypots e Honeynets - Aprenda a Detectar e Enganar Invasores**. 1ª. ed. [S.l.]: Visual Books, 2009.

AVELINO, E. F. **Avaliação preventiva de vulnerabilidade nos sistemas computacionais da universidade federal do Ceará - Campus Quixadá**. TCC (Trabalho de Conclusão de Curso - Tecnólogo em Redes de Computadores) Universidade Federal do Ceará - Campus Quixadá. Quixadá - CE - Brasil, p. 65. 2013.

BARBOSA, G. A. et al. Estudo de Caso: Vulnerabilidades em Redes Wireless. **Revista em Foco**, n. 9, p. 575-574, 2017. Disponivel em: <https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/057_estudo10.pdf>. Acesso em: Agosto 2019.

BARROS, H. S. et al. Tecnologia Wireless (WLANS). **Engenharia de Computação em Revista**, v. 1, n. 1, 2010.

BARROS, L. G.; JUNIOR, D. C. F. Autenticação IEEE 802.1x em Redes de Computadores Utilizando TLS e EAP. **Congresso Internacional de Administração - Gestão e Estratégia na Era do Conhecimento**, Ponta Grossa - PR - Brasil, 08 Setembro 2008.

BERTOLLI, E. O que é um ataque de força bruta? **blog.varonis.com.br**, 2018. Disponivel em: <https://blog.varonis.com.br/o-que-e-um-ataque-de-forca-bruta/>. Acesso em: 08 Agosto 2020.

BOTTI, C. F.; MARTINS, D. M. S. **Análise comparativa entre ferramentas de ataque Man in the Middle**. Artigo - Centro de Ensino Superior de Juiz de fora (CES/JF). Juiz de Fora - MG - Brasil. 2015.

BRYAN, A. Com o NetStumbler, você pode detectar redes LAN sem fio. **windowsbulletin.com**, 2018. Disponivel em: <http://windowsbulletin.com/pt/with-netstumbler-you-can-detect-wireless-lan-networks/>. Acesso em: 22 Maio 2020.

CANALTECH. O que é DoS e DDoS? **canaltech.com**. Disponivel em: <https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/>. Acesso em: 15 Agosto 2020.

CARRANZA, A. et al. Automated Wireless Network Penetration Testing Using Wifite and Reaver. **15th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Global Partnerships for Development and Engineering Education"**, Boca Raton - Fl - USA, 19 Julho 2017.

CARRIÓN, D. D. S. D. **Avaliação de Protocolos de Autenticação**. Dissertação (Mestrado em Ciências em Engenharia de Sistemas e Computação) - UFRJ. Rio de Janeiro - RJ - Brasil. 2005.

CARUSO, D.; JOHNSON, R. **The Vision Thing.Intelligent Enterprise**. [S.l.]: [s.n.], 1999.

CASTRO, M. M. D. **Segurança em Redes Wireless: Uma Visão Geral**. Monografia (Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet) - Núcleo de Computação Eletrônica da Universidade do Rio de Janeiro - NCE/UFRJ. Rio de Janeiro - RJ - Brasil. 2008.

CASTRO, R. M. D. **Estudo de Algoritmos Adaptativos de Beamforming com Detecção de Ângulo de Chegada**. Dissertação (Dissertação em Engenharia Elétrica) - COPPE - UFRJ. Rio de Janeiro - RJ - Brasil. 2011.

COSER, E. **Automatização do Processo de Contenção de Ameaças baseada em Ferramenta de IDS/IPS (Sistema de detecção e prevençaõ de intrusão)**. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Controle de Automação) - UNIVATES. Lajeado - RS - Brasil. 2011.

CROTHERS, T. **Implementing Intrusion Detection Systems:** A Hands-on guide for Securing the Network. Indianápolis - USA: Wiley Publishing, 2003.

DIORIO, R. F. et al. Ataques de Força Bruta: Um Estudo Prático. **2019 Brazilian Technology Symposium**, Capivari - SP - Brasil, 30 Setembro 2019.

DUARTE, L. O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. TCC (Trabalho de Conclusão de Curso) - Universidade Estadual Paulista (UNESP) - Instituto de Biociências, Letras e Ciências Exatas (IBILCE). São José do Rio Preto - SP - Brasil. 2003.

EKLUND, C. et al. IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access. **IEEE Communications Magazine**, v. 40, p. 98-107, June 2002.

ENDLER, M.; LIMA, L. D. S.; SOARES, F. G. **WiMax: Padrão IEEE 802.16 para Banda larga Sem Fio**. Monografia (Monografia em Ciência da Computação) - Pontifícia Universidade Católica do Rio de Janeiro PUC-RIO. Rio de Janeiro - BR. 2004.

ENGELMANN, C. P. et al. Protótipo de um Aplicativo para o Sistema Operacional iOS para Criptografia via Algoritmo RC4. **XIII Seminário de Iniciação Científica - 4ª. Semana de Ciência & Tecnologia UNESC**, Criciúma-SC-Brasil, 21 Outubro 2013.

FELISBERTO, L. A. **Sistemas de Comunicação sem Fio (Wireless)**. Monografia (Bacharelado em Ciência e Tecnologia) - Universidade Federal Rural do semi-Árido (UFERSA). Angicos - RN - Brasil. 2018.

FILHO, P. M. D. **Estratégias Voltadas a Segurança da Informação em Micro e Pequenas Empresas, com o Auxílio da Tecnologia Mikrotik**. TCC (Trabalho de Conclusão de Curso em Ciência da Computação) - Instituto Municipal de Ensino Superior de Assis (IMESA) e a fundação Educacional do Município de Assis (FEMA). Assis - SP. 2018.

FLECK, B.; DIMOV, J. Wireless Access Points and ARP Poisoning. **cigital.com**, 2002. Disponivel em: <www.packetnexus.com/docs/arppoison.pdf>. Acesso em: 22 Outubro 2020.

FOUSEKIS, D. The PMKID Attack. **bitcrack.net**, 2018. Disponivel em: <https://www.bitcrack.net/the-pmkid-attack/>. Acesso em: 25 Abril 2020.

FRANCESCHINELLI, D. A. **Estudo Comparativo dos Aspectos de Segurança em Redes WWAN, WLAN e WPAN**. Mestrado (trabalho final de Mestrado Profissional) - UNICAMP. Campinas - SP - Brasil. 2003.

FRANKLIN, C. WPA3 Brings New Authentication and Encryption to Wi-Fi. **darkreading.com**, 2018. Disponivel em: <https://www.darkreading.com/operations/wpa3-brings-new-authentication-and-encryption-to-wi-fi/d/d-id/1332145>. Acesso em: 08 Agosto 2020.

FRANZINI, F. Ataque 10 – Man in the Middle – MITM. **Fernando Franzini Blog**, 2013. Disponivel em: <https://fernandofranzini.wordpress.com/2013/07/12/ataque-10-man-in-the-middle-mitm/>. Acesso em: 5 Junho 2020.

GONÇALVES, D. P. Utilização de Sistema de Detecção e Prevenção de Intrusos modo NIDS. **6ª EATI - Encontro Anual de Tecnologia da Informação e Semana Acadêmica de Tecnologia da Informação**, São Vicente do Sul - RS, 09 Novembro 2015.

GONÇALVES, W. J. **Termos Técnicos Fundamentais em Redes, teoria e prática**. Artigo - UFMS. Campo Grande - MS - Brasil. 2014.

HIJAZI, H. A.; RAVANELLO, A. L.; MAZZORANA, S. M. **Honeypots e Aspectos Legais**. Dissertação (Pós Graduação em Informática Aplicada) - Pontifícia Universidade Católica do Paraná. Curitiba. 2004.

HOEPERS, C.; STEDING-JESSEN, K.; CHAVES, M. H. P. C. Honeypots e Honeynets: Definições e Aplicações. **www.cert.br**, 2007. Disponivel em: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/>. Acesso em: 15 Janeiro 2019.

JESUS, A. A. J. D.; JÚNIOR, B. F. D. S. **Redes sem fio: Uma análise dos principais padrões**. TCC (trabalho de Conclusão de Curso) - UFAL. Maceió - AL - Brasil. 2016.

JORDÃO, F. DDoS: como funciona um ataque distribuído por negação de serviço. **Desmonta & CIA**, 2011. Disponivel em: <https://desmontacia.wordpress.com/2011/07/01/ddos-como-funciona-um-ataque-distribudo-por-negao-de-servio/>. Acesso em: 17 Novembro 2020.

JUNIOR, J. S.; BASTOS, E. L. análise das Ferramentas IDS SNORT e PRELUDE quanto a eficácia na detecção de ataque e na proteção quanto à evasões. **Revista Tecnologia e Tendências**, Novo Hamburgo - RS, n. V.3, n.1, Janeiro/Junho 2004.

KALI, Our Most Advanced Penetration Testing Distribution, Ever. **kali.org**. Disponivel em: <https://www.kali.org/>. Acesso em: 8 Junho 2019.

KHALED, J. B. F. J. **Falhas de Segurança em uma rede Wireless Fidelity (Wi-Fi)**. Monografia (Monografia em Engenharia da Computação) - IESAM. Belém - PA - Brasil. 2006.

KINZIE, K. Cracking WPA2 Passwords Using the New PMKID Hashcat Attack. **null-byte.wonderhowto.com**, 2018. Disponivel em: <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-passwords-using-new-pmkid-hashcat-attack-0189379/>. Acesso em: 2 Agosto 2020.

KINZIE, K. Hack Wi-Fi Networks with Bettercap. **null-byte.wonderhowto.com**, 2020. Disponivel em: <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-networks-with-bettercap-0194422/>. Acesso em: 02 Agosto 2020.

KRAUSE, M.; TIPTON, H. F. **Information Security, Management Handbook**. 6ª. ed. New York: Auerback Publications, v. 2, 2008.

KRAWCZYK, H.; BELLARE, M.; CANETTI, R. **HMAC:** Keyed-Hashing for Message Authentication - Technical report, IETF - RFC 2104 - section 2, "Definition of HMAC", page 3, February 1997.

KUROSE, J.; ROSS, K. **Redes de Computadores e a Internet uma abordagem top-down**. São Paulo - SP - Brasil: Pearson, 2014.

LATTO, N. O que é um sniffer e como não ser espionado? **www.avg.com**, 2020. Disponivel em: <https://www.avg.com/pt/signal/what-is-sniffer>. Acesso em: 20 Agosto 2020.

LIMA, M. B. Firewalls - Uma introduçõ à segurança. **Revista do Linux**, Curitiba, p. 16, 2000.

LIMA, M. B. **Provisão de Serviços Inseguros Usando Filtros de Pacotes com Estados**. Dissertação (Mestrado em Ciência da Computação) Universidade Estadual de Campinas - UNICAMP. Campinas - SP - Brasil. 2000.

LLERENNA, A. E. R. Herramientas fundamentales para el hacking ético. **Revista Cubana de Informática Médica**, Havana - CUB, 2020.

LÜDTKE, R. K. **TESTE DE INVASÃO EM REDES SEM FIO 802.11**. TCC (Trabalho de Conclusão de Curso) - Universidade Federal de Santa Maria - Colégio Técnico Industrial de Santa Maria - curso Superior de Tecnologia em Redes de Computadores. Santa Maria - RS - Brasil. 2015.

MACÊDO, D. Atacando redes wifi com Aircrack-ng protegidas com criptografia WPA e WPA2. **Diego Macêdo - Um pouco sobre T.I.**, 2016. Disponivel em: <https://www.diegomacedo.com.br/atacando-redes-wifi-com-aircrack-ng-protegidas-com-criptografia-wpa-e-wpa2/>. Acesso em: 17 Novembro 2020.

MACIEL, D. S. **Avaliação do impacto de ataques DDoS e Malware: Uma abordagem baseada em Árvore de Ataque**. Dissertação (Pós Graduação) - UFPE. Recife - PE - Brasil. 2018.

MACORATTI, J. C. MiniCurso : Criptografia na plataforma.NET. **www.macoratti.net**, 2010. Disponivel em: <http://www.macoratti.net/Cursos/Cripto/net_cripto4.htm>. Acesso em: 30 Maio 2020.

MAGGIORA, P. D.; ANDERSON, N.; DOHERTY, J. **Cisco Networking Simplified**. 2ª. ed. Indianapolis - USA: Cisco Press, 2008.

MAIA, W. P. **Projeto, Implementação e Desempenho dos Algoritmos Criptográficos AES, PRESENT e CLEFIA em FPGA**. Dissertação de Mestrado (Engenharia Elétrica) - PROEE - Universidade Federal de Sergipe. São Cristóvão - SE - Brasil. 2017.

MEDEIROS, E. M. **Redes sem fio Wlan - Termos técnicos**. Campo Grande - MS: Universidade Federal de Mato Grosso do Sul, 2014.

MILLS, M. Como Invadir uma rede Wi-Fi do zero com essas ferramentas gratuitas. **itigic.com**, 2020. Disponivel em: <https://itigic.com/pt/hack-wifi-network-from-scratch-with-free-tools/>. Acesso em: 21 Outubro 2020.

MONTANARI, L. Protocolo DHCP: O que é, como funciona e mais. **www.tiespecialistas.com.br**, 2019. Disponivel em: <https://www.tiespecialistas.com.br/protocolo-dhcp-o-que-e-como-funciona-e-mais/>. Acesso em: 25 Outubro 2020.

MOREIRA, E. **Método para avaliação do desempenho de implementações dos padrões IEEE 802.11a/b/g/n/ac**. Dissertação de mestrado (Sistema de Informação e Comunicação) - UNICAMP - Universidade Estadual de Campinas. São Paulo - SP - Brasil. 2018.

MORENO, D. **Pentest em Redes Sem Fio**. 1ª. ed. São Paulo - SP - Brasil: Novatec, 2016.

MORETTI, C.; BELLEZI, M. A. Segurança em Redes Sem Fio 802.11. **T. I. S. - Tecnologias, Infraestrutura e Software**, São Carlos, v. 3, Janeiro 2014.

MORIMOTO, C. E. Usando o Kismet. **www.dicas-l.com.br**, 2006. Disponivel em: <https://www.dicas-l.com.br/arquivo/usando_o_kismet.php>. Acesso em: 21 Outubro 2020.

NAKAMURA, E. T.; GEUS, P. L. D. **Segurança de Redes em Ambientes Cooperativos**. [S.l.]: Novatec, 2014.

OLIVEIRA, A. N. **Autenticação em Redes Wireless com Certificação Digital Evitando "Evil Twin"**. TCC (Trabalho de Conclusão de Curso) - UNICEUB. Brasília - DF - Brasil. 2007.

OLIVEIRA, M. Conheça Parrot Security OS uma distro Linux para Teste de Invasão. **terminalroot.com.br**, 2016. Acesso em: 21 Outubro 2020.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. **Segurança Digital**, n. 5, p. 11-15, Junho 2012.

PAIM, R. R. Gta / UFRJ. **Grupo de Teleinformática e Automação**, 2011. Disponivel em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/index.html>. Acesso em: Abril 2019.

PAULRAJ, A. et al. **MIMO WirelessCommunications**. 1ª. ed. Cambridge - UK: Cambridge University Press, 2007.

PINHEIRO, J. M. S. A Trilogia Wireless. **www.projetoderedes.com.br**, 2003. Disponivel em: <https://www.projetoderedes.com.br/artigos/artigo_trilogia_wireless.php>. Acesso em: 10 Novembro 2019.

PINHO, J. B. **Publicidade e Vendas na Internet**. 1ª. ed. São Paulo - SP - Brasil: Summus Editorial, 2000.

PIOTO, M. A. V. **Redes Wireless Padrão IEEE 802.11: Protocolos de Segurança WEP e WPA**. TCC (Trabalho de Conclusão de Curso Bacharelado em Ciência da Computação) - Centro Universitário - UNIVEM. Maríia - SP - Brasil. 2006.

POSTEL, J. User Data Protocol (UDP). Technical report, IETF - RFC 768, 1980.

POSTEL, J. Trasmission Control Protocol (TCP). Technical report, IETF - RFC 793, 1981.

PRITCHETT, W. L.; SMET, D. D. **Kali Linux Cookbook**. Birmingham - UK: Packt Publishing, 2013.

PROCTOR, P. E. **Practical intrusion detection handbook**. Upper Saddle River - New Jersey - USA: Prentice Hall, 2001.

RAGER, A. T. WepCrack. **Sourceforge.net**, 2004. Disponivel em: <http://wepcrack.sourceforge.net/>. Acesso em: 21 Outubro 2020.

RANUM, M. J. **Coverage in Intrusion Detection Systems**. NFR Security, Inc. [S.l.]. 2001.

REIS, F. D. Arquiteturas de Redes Locais Sem Fio (Wi-Fi). **Bóson Treinamentos em Ciência e Tecnologia**, 2018. Disponivel em: <http://www.bosontreinamentos.com.br/redes-wireless/arquiteturas-de-redes-locais-sem-fio-wi-fi/>. Acesso em: Julho 2020.

RETTONDIN, H. S.; FILHO, J. D. L. Segurança em Redes sem fio: o aumento da segurança com o novo protocolo a partir de 2019. **SIMTEC – Simpósio de Tecnologia - Faculdade de Tecnologia de Taquaritinga**, Taquaritinga - SP - Brasil, 8 Outubro 2018.

RIBEIRO, J. R. C. L. **Um Protocolo de Autenticação de Senhas em Ambiente Cifrado para Acesso a Base de Dados**. Pós-graduação (pós-graduação em ciência da Computação) - Universidade Federal de Uberlândia. Uberlândia - MG - Brasil. 2005.

RIVEST, R. The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science and RSA Data Security RFC 1321, 1992

ROGER, D. Teste de Invasão em Redes Wireless. **Under-Linux.org**, 2008. Disponivel em: <https://under-linux.org/entry.php?b=155>. Acesso em: 21 Outubro 2020.

RUFINO, N. M. D. O. **Segurança em Redes sem fio - Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. 3ª. ed. São Paulo - SP - Brasil: Novatec, 2011.

SHAH, B. **How to Choose Intrusion Detection Solution**. SANS Intitute Resources, v24. [S.l.]. 2001.

SHARMA, K.; DHIR, N. A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison. **(IJCSIT) International Journal of Computer Science and Information Technologies**, Punjab - Índia, v. 5, p. 7810 - 7813, 2014.

SIEWERT, V. C. **Ferramenta Web para Administração do Servidor proxy SQUID**. Trabalho de Conclusão de Curso (Ciências da Computação) - Universidade Regional de Blumenau. Blumenau - SC - Brasil. 2007.

SILVA, D. R. P. D.; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, Porto Alegre - RS - Brasil, v. 10, p. 46-53, Março 2007.

SILVA, L. C. Redes Wi-Fi: Estudo do Furto de Sinal. **Teleco - Inteligência em Comunicações**, 2010. Disponivel em: <https://www.teleco.com.br/tutoriais/tutorialwifiroubo/>. Acesso em: 5 Junho 2020.

SIMON, D. et al, The EAP-TLS Authentication Protocol, Network Working Group – Microsoft Corporation RFC 5216, 2008

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de computadores - Das LANs, MANs e WANs às Redes ATM**. Rio de Janeiro - RJ - Brasil: [s.n.], 1995.

SOLA, P. L. P. **Segurança em Redes Wireless**. TCC (Trabalho de Conclusão de Curso) - FEMA - Instituto Municipal de Ensino superior de Assis. Assis - SP - Brasil. 2018.

STANGARLIN, D. P. **Análise de Desempenho de Redes sem fio com Diferentes Protocolos de Criptografia**. TCC (Trabalho de Conclusão de Curso) - UFSM-RS. Santa Maria - RS - Brasil. 2012.

TANENBAUM, A. S. **Computer Networks**. 4ª. ed. Upper Saddle River: Prentice Hall, 2002.

TOMASINI, D. C. Burlando a Segurança em uma Rede Wireless. **dickrips.wordpress.com**, 2008. Disponivel em: <https://dickrips.wordpress.com/2008/11/20/burlando-a-seguranca-em-uma-rede-wireless/>. Acesso em: 21 Outubro 2020.

TURCATO, A. C. et al. Ataque Denials os Service em Redes PROFINET: Estudo de Caso. **XII Simpósio Brasileiro de Automação Inteligente (SBAI)**, Natal - RN - Brasil, 25 Outubro 2015.

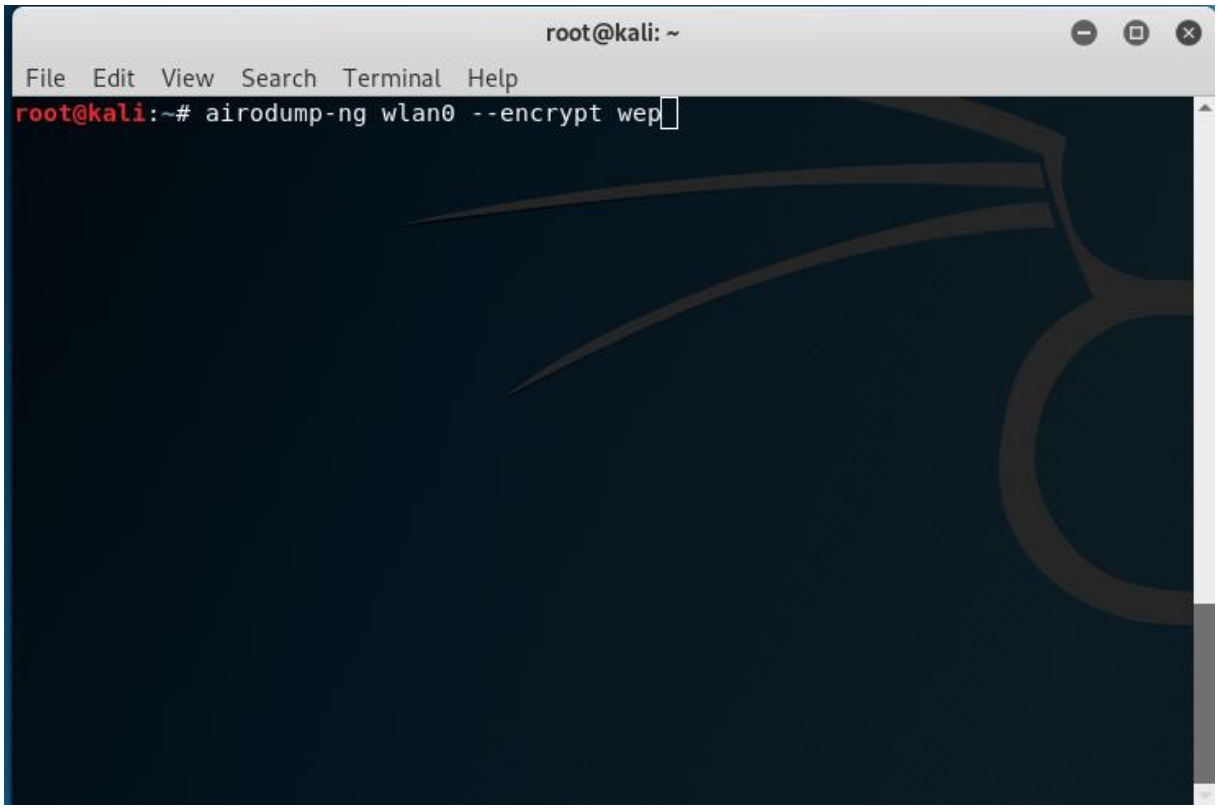
VLADIMIROV, A.; GAVRILENKO, K. V.; MIKHAILOVSKY, A. A. **"Wi-Foo:** The Secrets os Wireless Hacking". 1ª. ed. [S.l.]: Addison Wesley, 2004.

WEIDMAN, G. **Testes de Invasão - Uma introdução prática ao Hacking**. 1ª. ed. São Paulo - BR: Novatec, 2014.

WRIGHTSON, T. **Segurança de redes sem fio:** guia do iniciante. [S.l.]: Bookman, 2014.

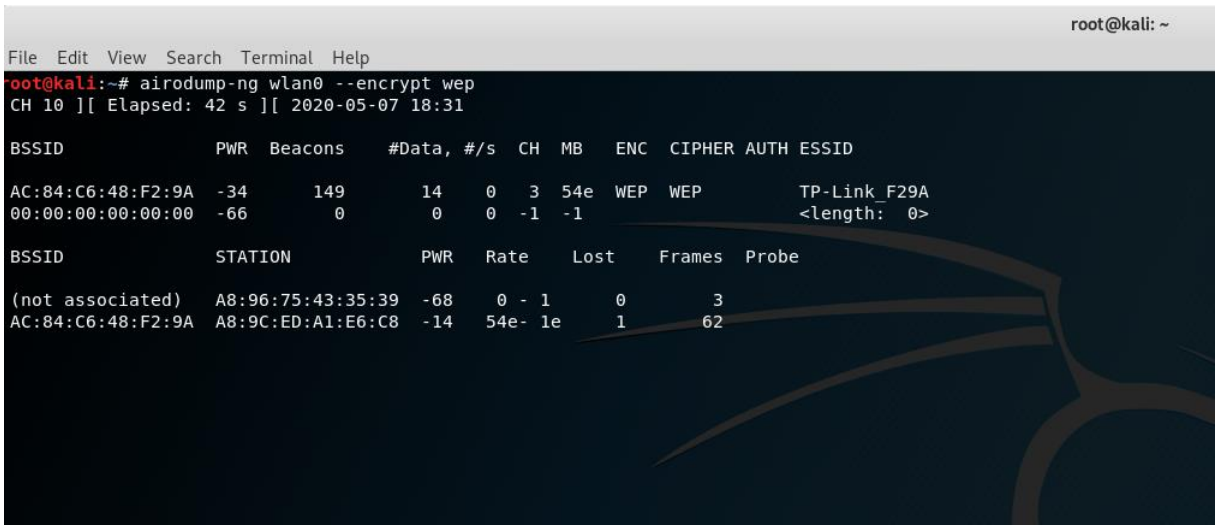
ANEXO

ANEXO A – Comando Airodump-ng



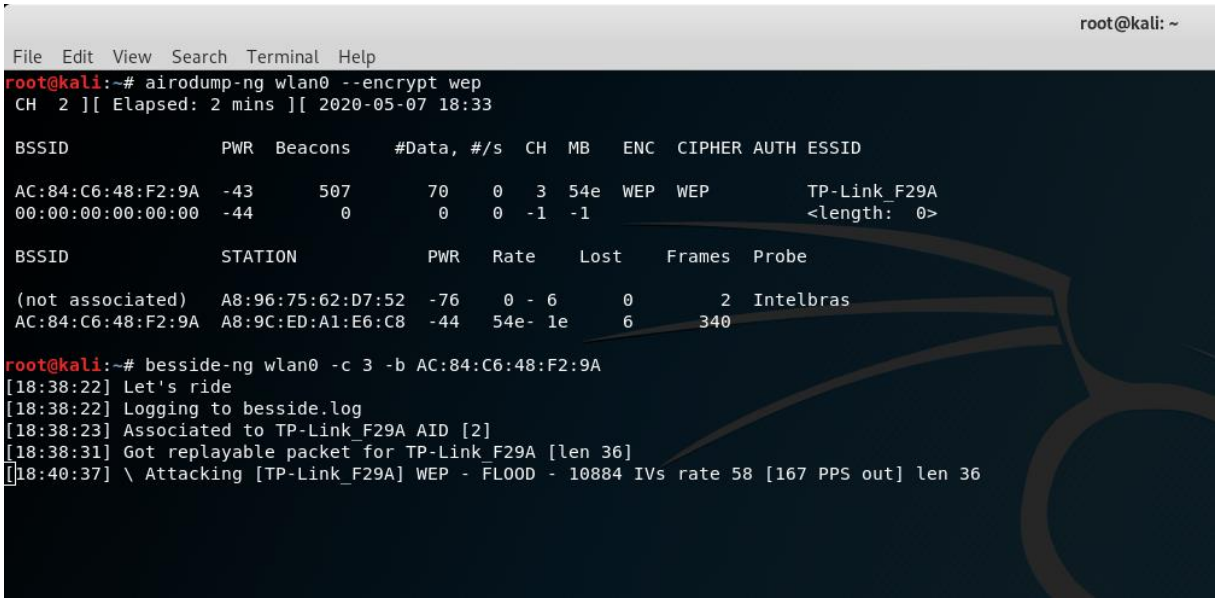
Fonte: Autoria Própria

ANEXO B – Resultado do Airodump-ng



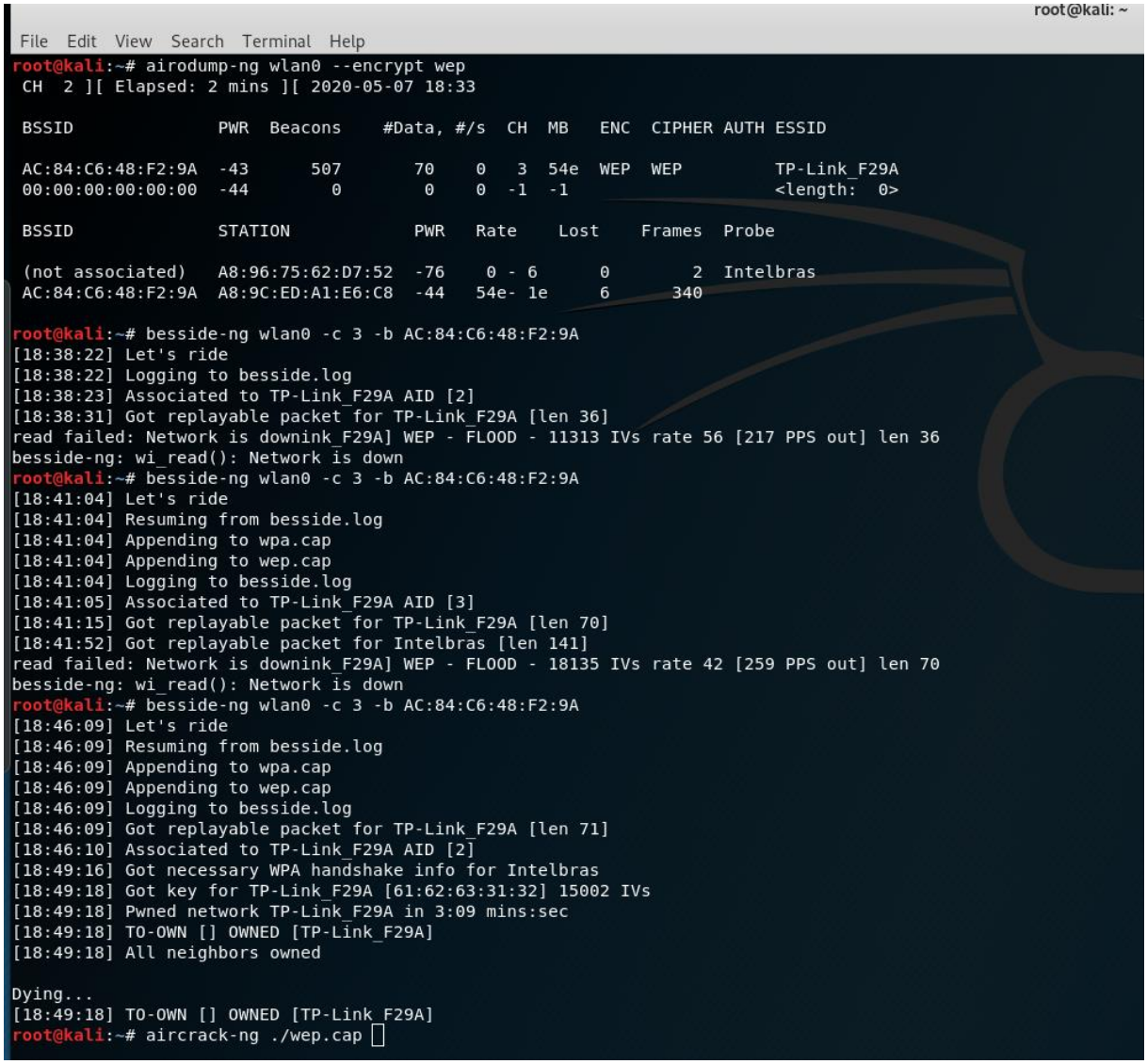
Fonte: Autoria Própria

ANEXO C – Comando Besside-ng



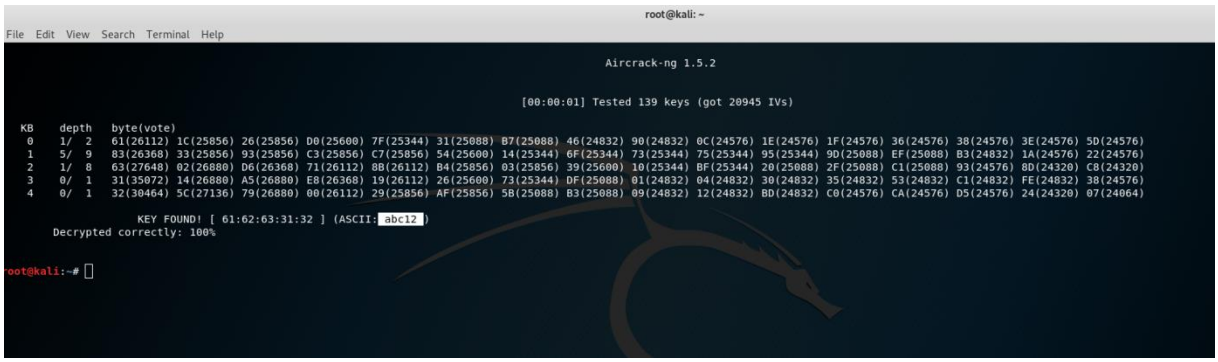
Fonte: Autoria Própria

ANEXO D – Captura de IVs Concluída



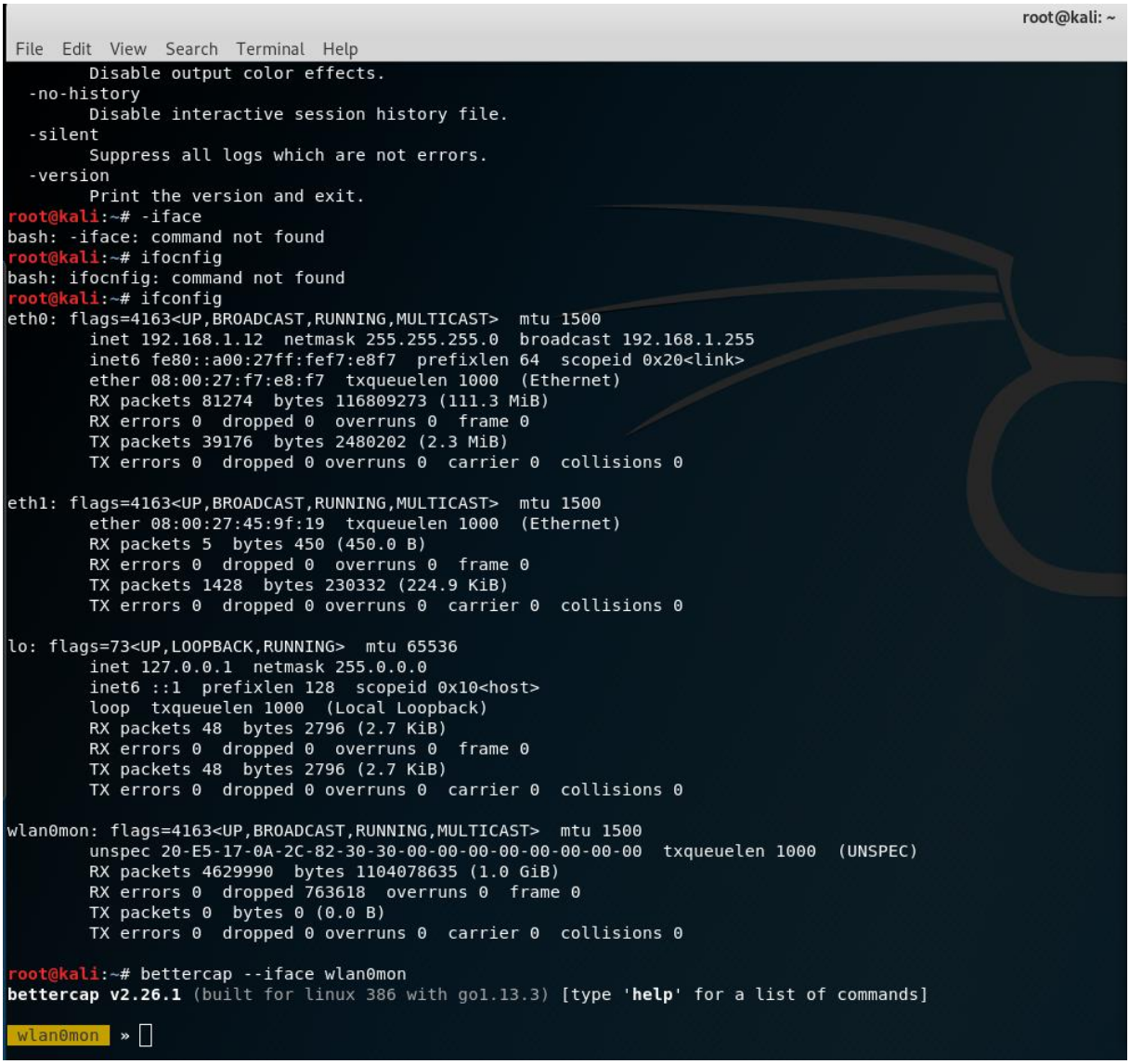
Fonte: Autoria Própria

ANEXO E – Quebra de Senha



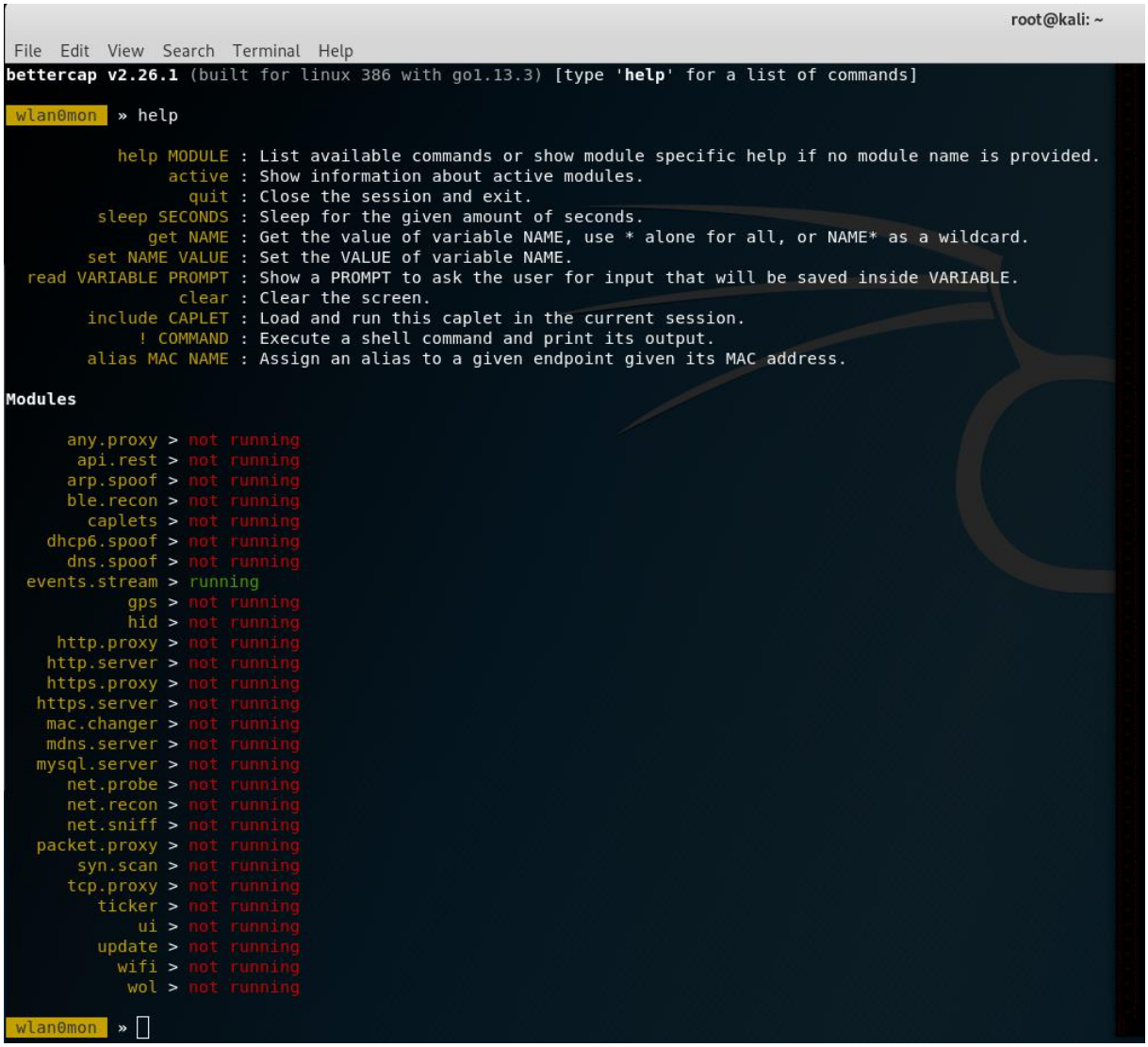
Fonte: Autoria Própria

ANEXO F – Executando em modo monitor



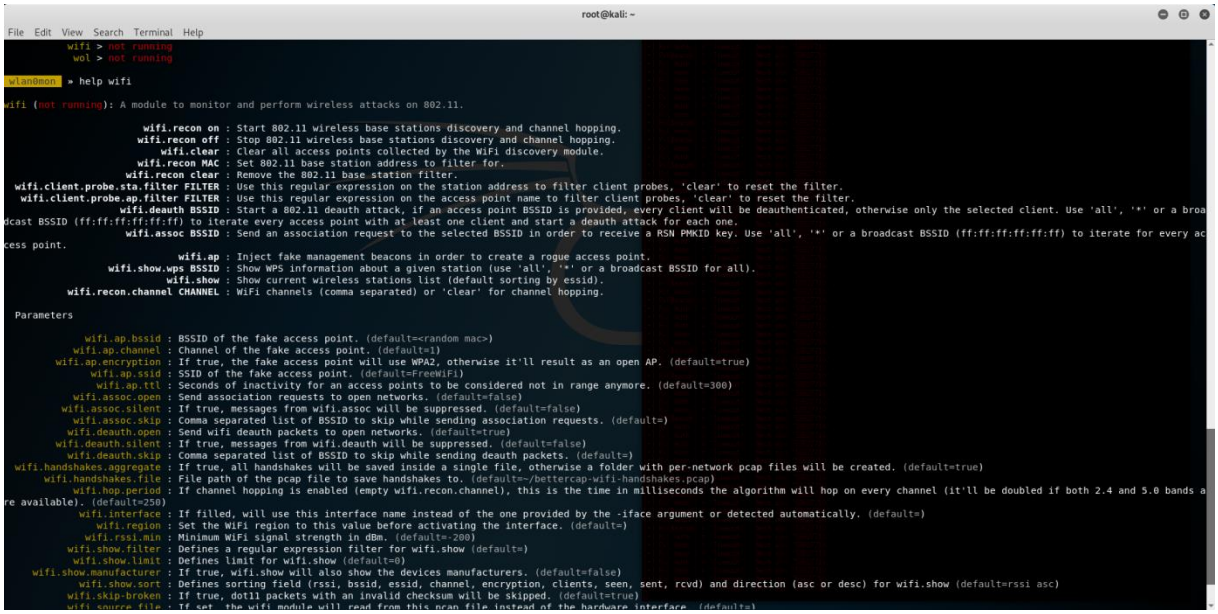
Fonte: Autoria Própria

ANEXO G – Comando Help



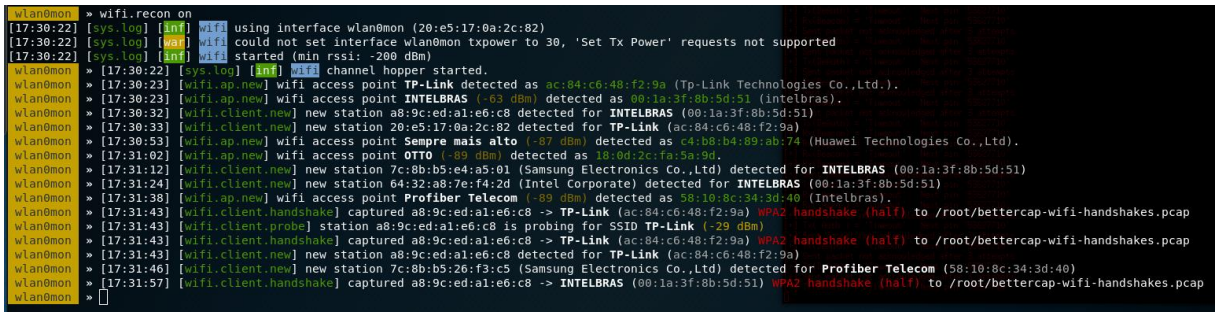
Fonte: Autoria Própria

ANEXO H – Comando Help Wifi



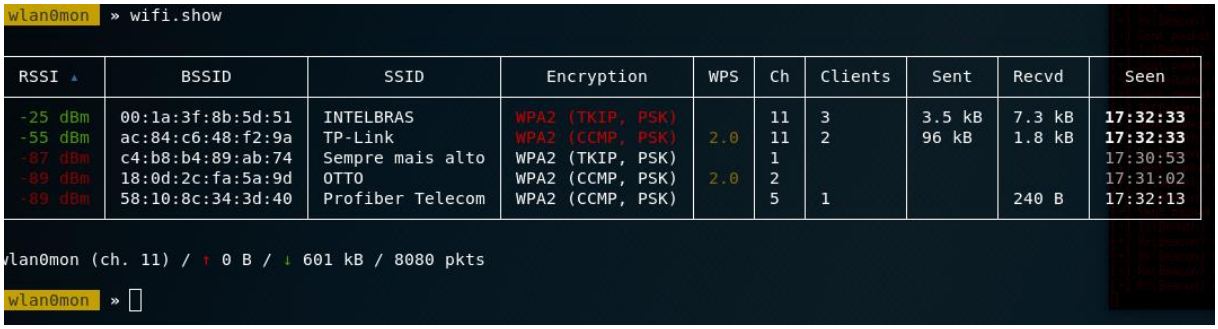
Fonte: Autoria Própria

ANEXO I – Comando Help Wifi.recon



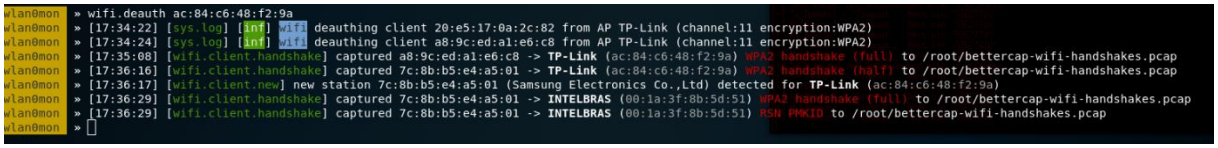
Fonte: Autoria Própria

ANEXO J – Comando Help Wifi.show



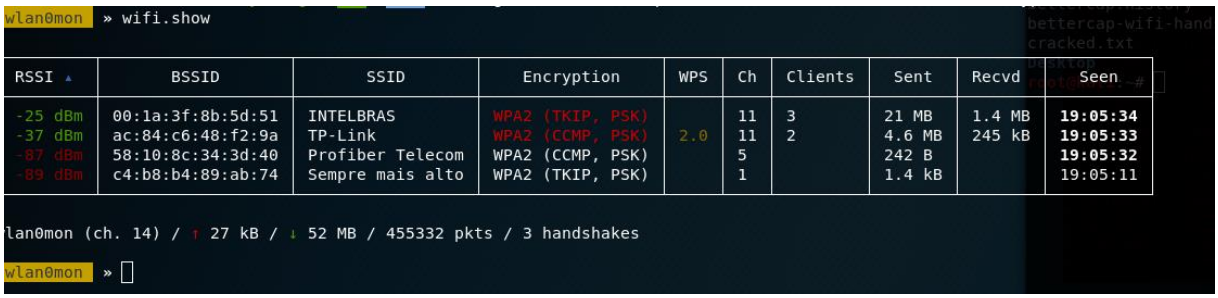
Fonte: Autoria Própria

ANEXO K – Comando Help Wifi.deauth



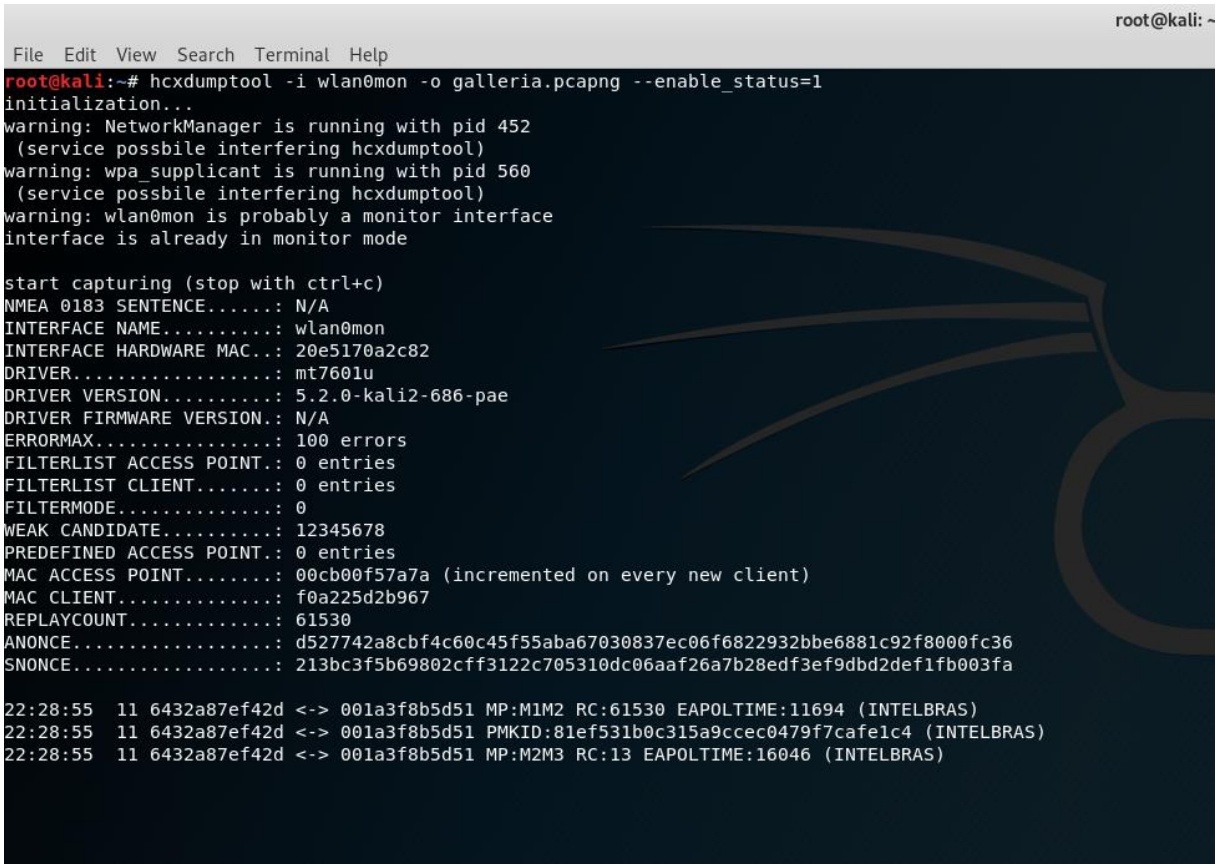
Fonte: Autoria Própria

ANEXO L – Comando Help Wifi.show



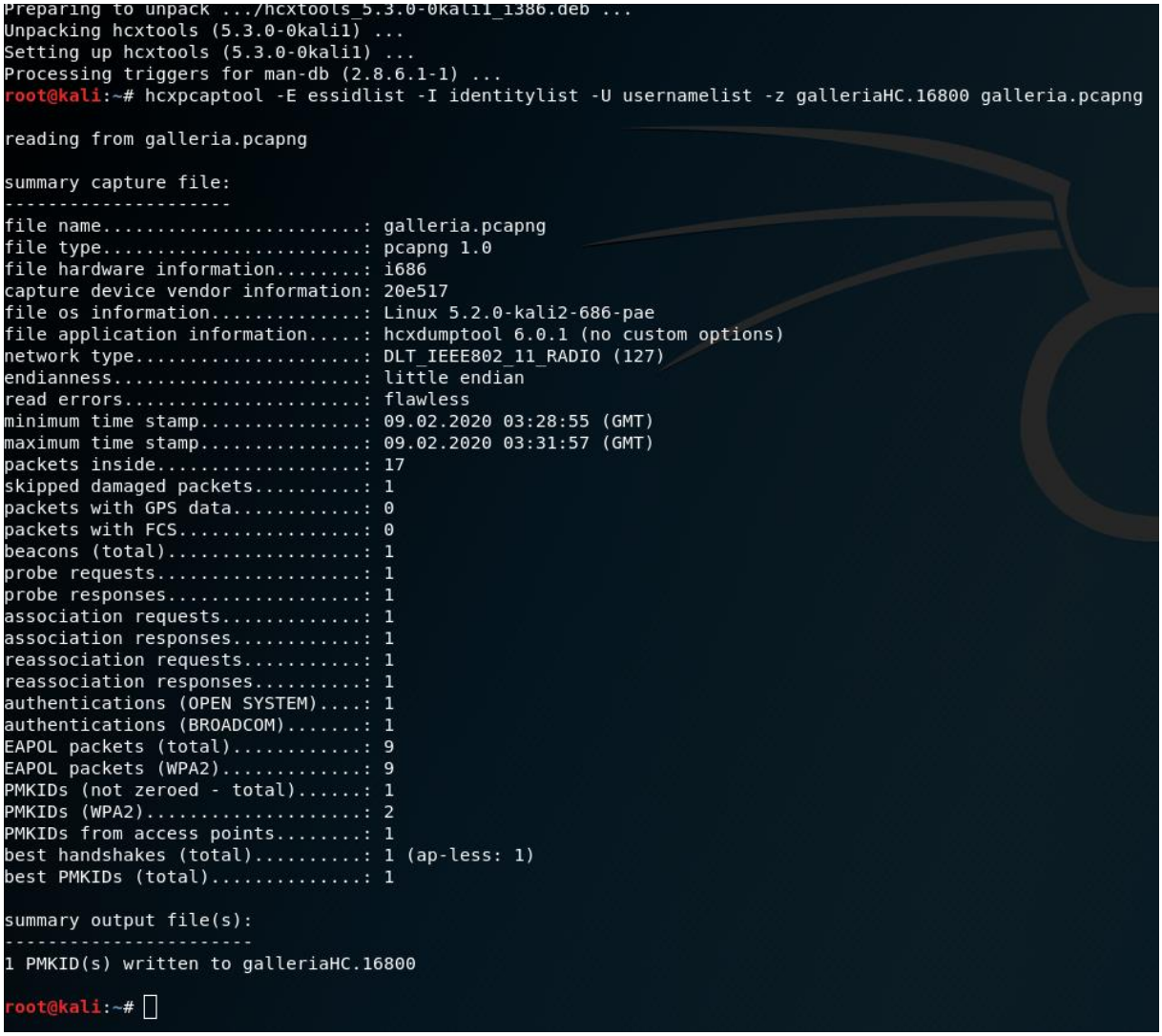
Fonte: Autoria Própria

ANEXO M – Comando hcxdumptool



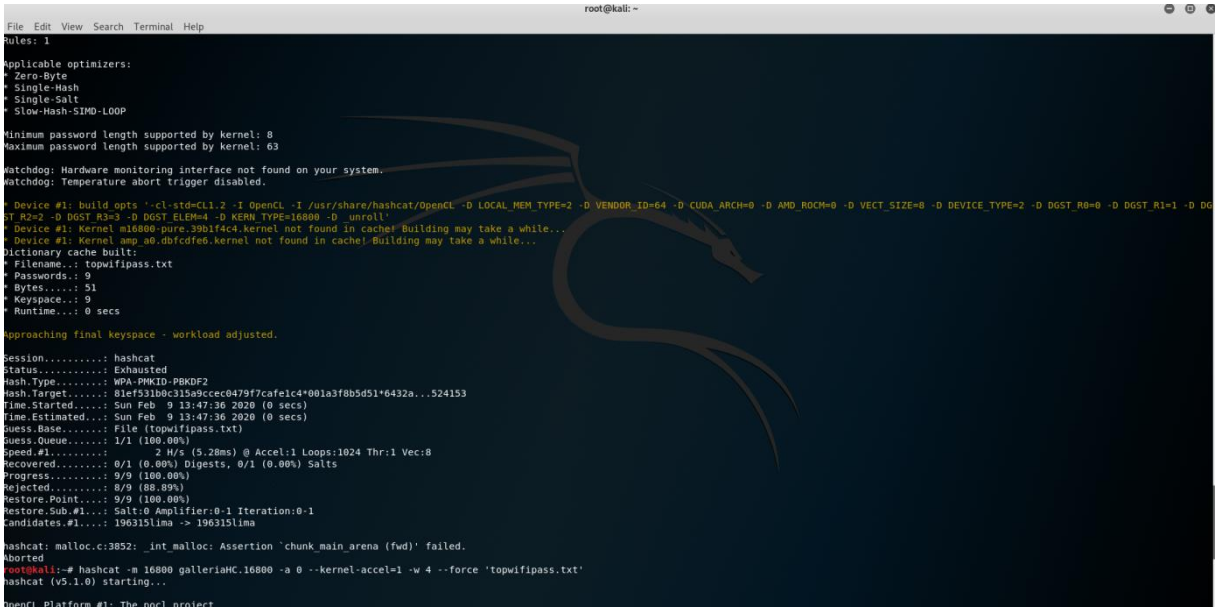
Fonte: Autoria Própria

ANEXO N – Comando hcxpcaptool



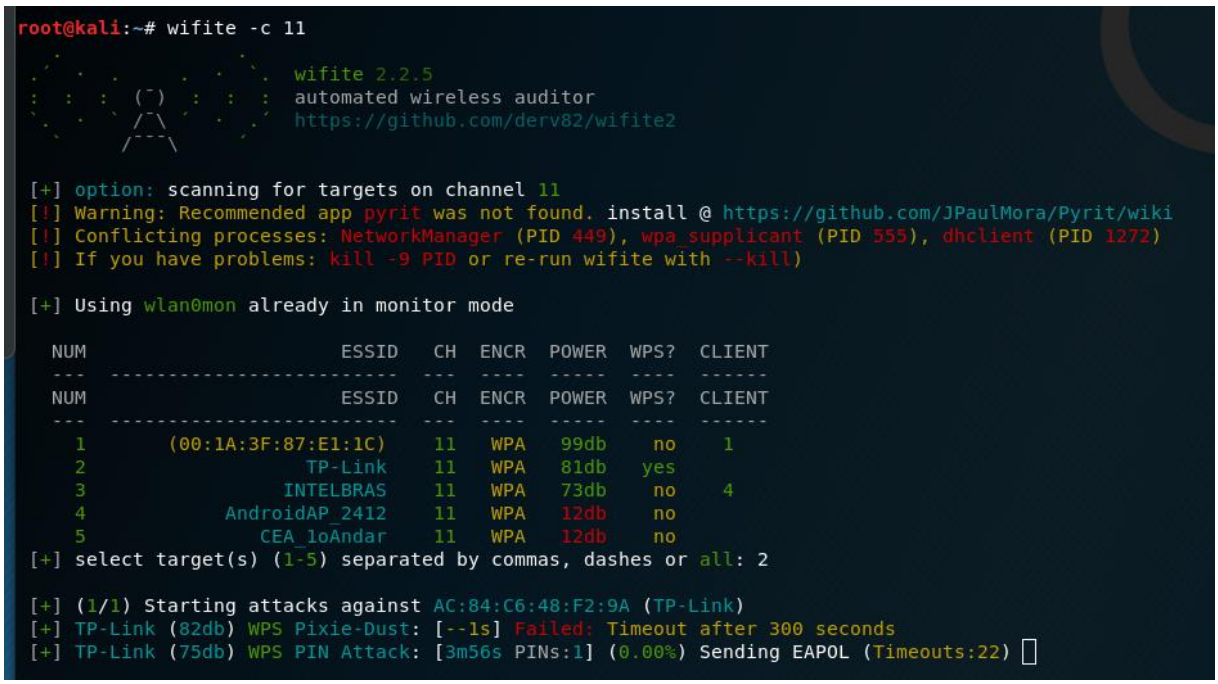
Fonte: Autoria Própria

ANEXO O – Comando hashcat



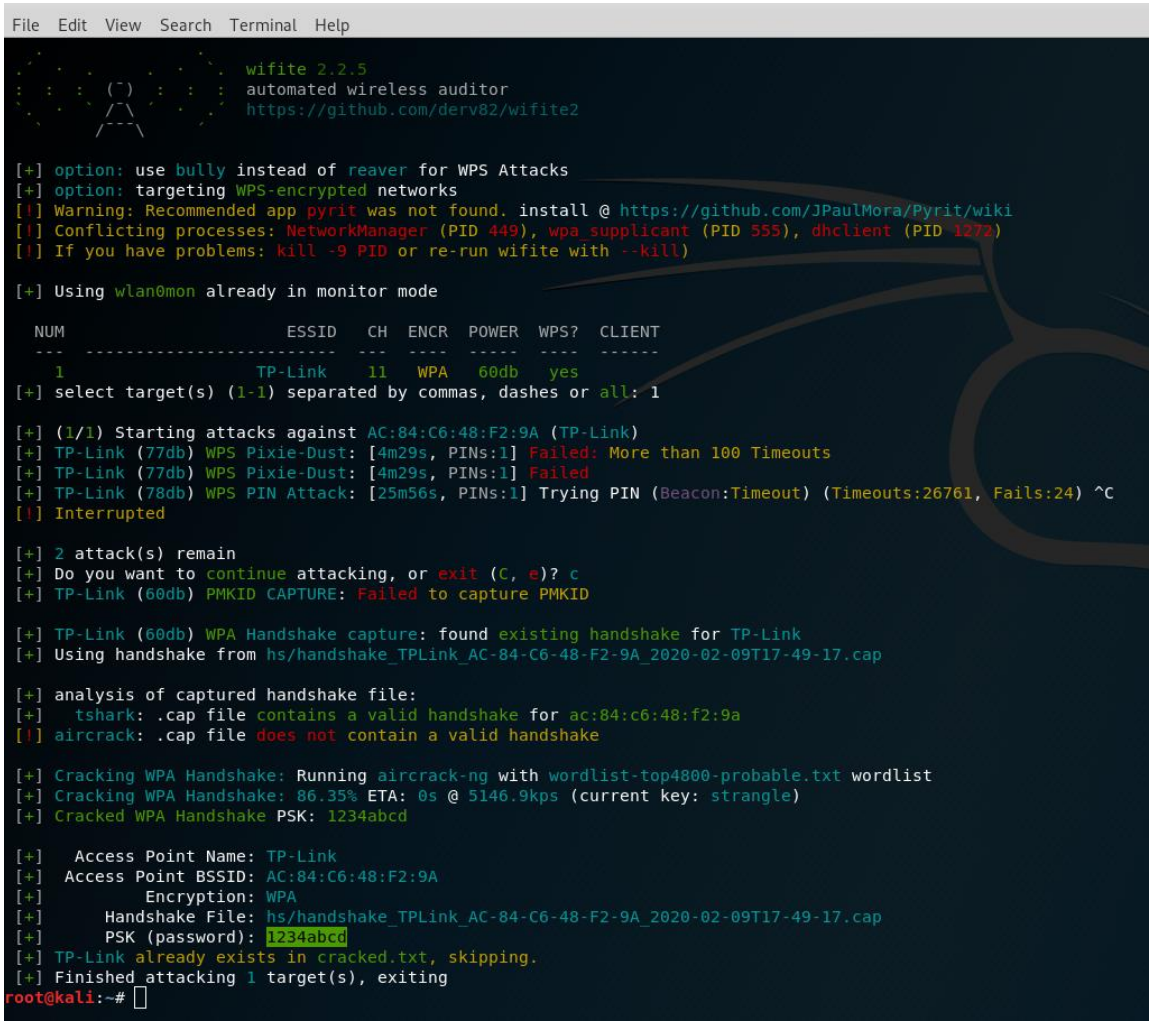
Fonte: Autoria Própria

ANEXO P – Execução do wifite 2



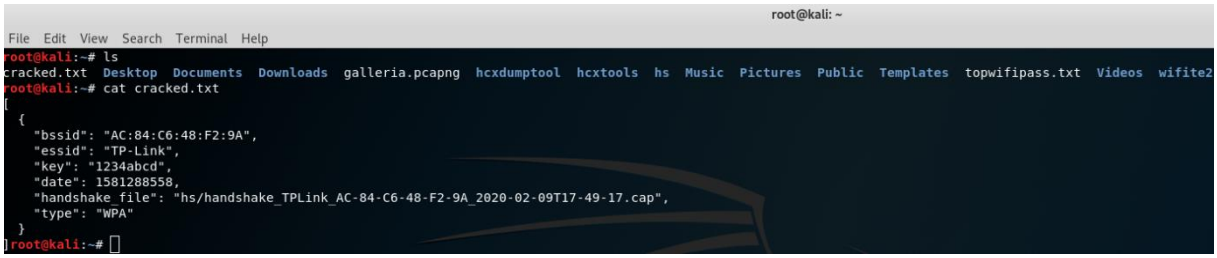
Fonte: Autoria Própria

ANEXO Q – Sucesso Captura



Fonte: Autoria Própria

ANEXO R – Arquivo cracked.txt



Fonte: Autoria Própria