UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

LUCAS DA SILVA CARLESSI

ESTUDOS DE CASO DE SEGURANÇA EM REDES SEM FIO UTILIZANDO FERRAMENTAS PARA MONITORAMENTO E DETECÇÃO DE ATAQUES

CRICIÚMA, JULHO DE 2011

LUCAS DA SILVA CARLESSI

ESTUDOS DE CASO DE SEGURANÇA EM REDES SEM FIO UTILIZANDO FERRAMENTAS PARA MONITORAMENTO E DETECÇÃO DE ATAQUES

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, JULHO DE 2011

LUCAS DA SILVA CARLESSI

Estudos de Caso de Segurança em Redes Sem Fio Utilizando Ferramentas para Monitoramento e Detecção de Ataques

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. MSc. Rogério Antônio Casagrande (UNESC)

Prof. MEng. Evânio Ramos Nicoleit (UNESC)

Aos meus pais Ivanor e Paula e meus irmãos Ivan e Diana, que me deram todo o apoio necessário durante a realização deste trabalho.

AGRADECIMENTOS

A todos os professores e departamento do curso de Ciência da Computação da UNESC que fizeram parte de minha vida acadêmica, permitindo meu crescimento científico e pessoal.

Ao meu orientador Paulo, pelas experiências compartilhadas e horas dedicadas para que pudéssemos realizar o melhor trabalho possível.

Aos meus pais e irmãos, que sempre estiveram presentes e me incentivaram nos momentos difíceis.

A minha namorada Diana, pela paciência, compreensão e apoio.

Aos meus amigos e colegas de curso, pelos ótimos momentos juntos.

"The quieter you become, the more you can hear".

(Ram Dass)

RESUMO

As redes sem fio estão por toda a parte. Além de residências, várias empresas utilizam esta tecnologia pela sua facilidade de instalação e mobilidade que proporciona. Devido a essa popularidade, muitas redes *wireless* sofrem ataques constantes e podem ser comprometidas facilmente se não forem implementados métodos eficientes para segurança. Além disso, a cada dia são descobertas novas vulnerabilidades. Para prover ações pró-ativas dos administradores dessas redes, algumas ferramentas que monitoram e detectam ataques foram desenvolvidas. Estas ferramentas podem ser eficientes se utilizadas adequadamente, proporcionando um gerenciamento competente dos recursos de segurança e alertas de possíveis ataques. Este trabalho apresenta e discute os conceitos de redes sem fio, os métodos de segurança, as vulnerabilidades e alguns ataques existentes. A partir destes conceitos, é testada a eficiência no monitoramento e detecção de ataques utilizando as ferramentas de código aberto para Linux, Kismet e Beholder. Os testes realizados com estas ferramentas indicam a importância com a preocupação acerca da segurança e do monitoramento dos pontos da rede.

Palavras-chave: Segurança da Informação; Redes Sem Fio; Monitoramento e Detecção de ataques; Kismet; Beholder.

ABSTRACT

Wireless networks are everywhere. Besides homes, many companies use this technology for its ease of installation and mobility. Because of this popularity, many wireless networks suffer constant attacks and they can easily be compromised if not implemented effective methods for security. In addition, each day new vulnerabilities are discovered. To provide pro-active actions of the administrators of these networks, some tools that monitor and detect attacks have been developed. These tools can be effective if they are used properly, providing competent management of safety features and warnings of possible attacks. This paper aims to present and discuss the concepts of wireless networks, methods of security, vulnerabilities and some possible attacks. Based on these concepts, methods are tested for efficiency in monitoring and attack detection using open source tools for Linux, Kismet and Beholder. The tests with these tools indicate the importance to the concern about the safety and monitoring of network points.

Keywords: Information Security. Wireless Networks. Monitoring and Attack Detection. Kismet. Beholder.

LISTA DE ILUSTRAÇÕES

Figura 1. O espectro eletromagnético e a maneira como ele é usado na comunicação 27

Figura 2. Topologia de rede no modo Ad Hoc 32

Figura 3. Uma pequena rede em modo infraestrutura 33

Figura 4. A especificação 802 e a sua relação com o modelo OSI 34

Figura 5. O posicionamento de um ponto de acesso é importante na segurança da rede 40

Figura 6. Alguns símbolos utilizados no warchalking 43

Figura 7. Configuração do ambiente de testes 58

Figura 8. Tela inicial do Kismet 60

Figura 9. Informações da rede selecionada no Kismet 61

Figura 10. Lista de clientes respondendo aos anúncios da rede no Kismet 61

Figura 11. Informações detalhadas do cliente selecionado no Kismet 62

Figura 12. Tela de alertas do Kismet 62

Figura 13. Detecção de AP spoofing no Kismet 64

Figura 14. Detecção de D.o.S no Kismet 65

Figura 15. Detecção da assinatura BSSTIMESTAMP no Kismet 66

Figura 16. Mudando canal no Ovislink WL-1120AP 66

Figura 17. Detecção de mudanças de canais com o Kismet 67

Figura 18. Desativando criptografia nas configurações do Ovislink WL-1120AP 67

Figura 19. Detecção da assinatura CRYPTODROP no Kismet 68

Figura 20. Detecção de Karma com o Kismet 68

Figura 21. Iniciando o Beholder 69

Figura 22. Detecção de AP spoofing no Beholder 70

Figura 23. Detecção de BSSTIMESTAMP no Beholder 70

Figura 24. Detecção de mudanças de canal no Beholder 71

Figura 25. Detecção de mudanças na criptografia da rede no Beholder 71

Figura 26. Detecção de Karma no Beholder..... 72

LISTA DE TABELAS

Tabela 1. Características dos principais padrões da família 802.11 34

Tabela 2. Associação entre canal e respectiva frequência do padrão 802.11b 35

Tabela 3. Ferramentas para monitoramento e detecção de ataques que não funcionaram 56

Tabela 4. Ferramentas comerciais para monitoramento e detecção de ataques 57

Tabela 5. Ataques testados no Kismet e Beholder 72

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryption Standard*
AP	*Access Point*
ARP	*Address Resolution Protocol*
CRC	*Cyclic Redundancy Check*
CSMA/CA	*Carrier Sense Multiple Access / Collision Avoidance*
DES	*Data Encryption Standard*
DoS	*Denial of Service*
DSSS	*Direct Sequence Spread Spectrum*
EAP	*Extensible Authorization Protocol*
GHz	*Gigahertz*
GPS	*Global Positioning System*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IV	*Initialization Vector*
LAN	*Local Area Network*
MAC	*Medium Access Control*
MIMO	*Multiple Input, Multiple Out*
OFDM	*Orthogonal Frequency Division Multiplexing/Modulation*
PDA	*Personal Digital Assistants*
RADIUS	*Remote Authentication Dial-in User Service*
SSID	*Service Set Identifier*
TI	Tecnologia da Informação
TKIP	*Temporal Key Integrity Protocol*

VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	*Wi-Fi Protected Access*

SUMÁRIO

1 INTRODUÇÃO 17

1.1 OBJETIVO GERAL 18

1.2 OBJETIVOS ESPECÍFICOS 18

1.3 JUSTIFICATIVA 19

1.4 ESTRUTURA DO TRABALHO 20

2. SEGURANÇA DA INFORMAÇÃO 22

2.1 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO 22

2.2 POLÍTICAS DE SEGURANÇA 23

3. REDES SEM FIO 25

3.1 FUNDAMENTOS DE REDES SEM FIO 26

3.1.1 Frequências e Canais 26

3.1.2 Spread Spectrum 27

3.1.3 Direct Sequence Spread Spectrum (DSSS) 27

3.1.4 Orthogonal Frequency Division Multiplexing (OFDM) 28

3.1.5 Bandas de rádio frequência públicas no Brasil 28

3.1.6 Frequências licenciadas 29

3.2 CARACTERÍSTICAS 29

3.2.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) 29

3.2.2 Service Set Identifier (SSID) 30

3.2.3 Beacon Management Frame 31

3.2.4 Modos de Operação 31

3.2.4.1 Ad Hoc 32

3.2.4.2 Infraestrutura 32

3.1 PADRÕES DE REDES SEM FIO 33
3.1.1 Padrão IEEE 802.11b 34
3.1.2 Padrão IEEE 802.11a 35
3.1.3 Padrão IEEE 802.11g 36
3.1.4 Padrão IEEE 802.11i 36
3.1.5 Padrão IEEE 802.11n 37
4. SEGURANÇA EM REDES SEM FIO 38
4.1 VULNERABILIDADES 38
4.1.1 Vulnerabilidades Físicas 39
4.1.2 Vulnerabilidades no Envio e Recepção do Sinal 39
4.2 MÉTODOS DE ATAQUE 40
4.2.1 *Access Point Spoofing* 40
4.2.2 *ARP Poisoning* 41
4.2.3 *MAC Spoofing* 41
4.2.4 Ataques de Negativa de Serviço 41
4.2.5 *WLAN Scanner* (Ataques de Vigilância) 42
4.2.6 *Wardriving* 42
4.2.7 *Warchalking* 43
4.3 MÉTODOS DE DEFESA 43
4.3.1 Autenticação em *Access Points* 44
4.3.2 Criptografia 44
4.3.2.1 WEP 45
4.3.2.2 WPA 46
4.3.2.3 WPA2 46
4.3.3 RADIUS 47

4.3.4 *Virtual Private Network* (VPN) **47**

4.3.5 Firewalls **48**

5 MONITORAMENTO E DETECÇÃO DE ATAQUES EM REDES SEM FIO **49**

5.1 MÉTODOS DE MONITORAMENTO 50

5.2 EXEMPLOS DE FERRAMENTAS PARA MONITORAMENTO EM REDES SEM FIO 50

5.2.1 Kismet **50**

5.2.2 WIDZ **51**

5.2.3 AirTraf **51**

5.2.4 NetStumbler **51**

5.2.5 Beholder **52**

6 TRABALHOS CORRELATOS **53**

6.1 ANÁLISE DE VULNERABILIDADES DE REDES SEM FIO E MÉTODO DE DEFESA POR MEIO DE SENHAS SEGURAS 53

6.2 FERRAMENTAS DE SEGURANÇA EM REDES SEM FIO 53

6.3 REDES SEM FIO – TECNOLOGIA, SEGURANÇA E USABILIDADE 54

6.4 UM ESTUDO DE PROTOCOLOS EMPREGADOS NA SEGURANÇA DE DADOS EM REDES SEM FIO – PADRÃO 802.11 54

7 MONITORANDO E DETECTANDO ATAQUES EM REDES SEM FIO **55**

7.1 METODOLOGIA 55

7.1.1 Ferramentas para Monitoramento e Detecção de Ataques Testadas **56**

7.1.2 Ambiente e Ferramentas Utilizadas **57**

7.2 ESTUDO DE CASO 1: MONITORANDO REDES SEM FIO E DETECTANDO ATAQUES COM O KISMET 59

7.3 ESTUDO DE CASO 2: UTILIZANDO O BEHOLDER PARA DETECTAR ATAQUES EM REDES SEM FIO 68
7.4 RESULTADOS OBTIDOS 72
CONCLUSÃO 74
REFERÊNCIAS 76
APÊNDICE A – INSTALAÇÃO E CONFIGURAÇÃO DO KISMET NO UBUNTU 79
APÊNDICE B – ARTIGO 80
ANEXO A – ARQUIVO DE CONFIGURAÇÃO DO KISMET 91

1 INTRODUÇÃO

Redes sem fio são redes de computadores que permitem interligar, ao menos, dois equipamentos utilizando-se de ondas eletromagnéticas, sem a necessidade de uma estrutura física de cabeamento. Elas estão, cada vez mais, presentes no mundo devido à necessidade constante de conexão a rede dos vários equipamentos móveis (como notebooks e *Personal Digital Assistants* - PDA's) existentes no mercado (SGUAREZI, 2007).

As redes sem fio estão em amplo crescimento e atendem tanto o cenário doméstico quanto empresarial devido ao baixo custo e facilidade de instalação sem precisar modificar as instalações já existentes. Além de poder interligar redes privadas, é crescente o número de estabelecimentos como aeroportos e universidades que também disponibilizam o acesso sem fio para seus usuários (TANENBAUM, 2003).

A partir do princípio de que toda informação que trafega em redes sem fio é transmitida livremente pelo ar, a interceptação dessas informações é facilitada, bastando apenas que alguém opere na mesma frequência da rede para poder captar as ondas provenientes dela (AMORAS; BRABO; JUNIOR, 2004).

Isso torna mais fácil a sua utilização por pessoas não autorizadas, aumentando a importância da utilização de métodos de segurança para prevenir que essas pessoas mal intencionadas se apoderem de qualquer tipo de dado que trafegue nessas redes (CERT.br, 2009).

Considerando a facilidade de instalação, muitas redes sem fio estão sendo criadas sem o devido cuidado com a segurança, pois normalmente não é preciso realizar configurações adicionais nos equipamentos para que a rede funcione. Por outro lado, existem pessoas que até se preocupam com a segurança e aplicam determinados métodos de defesa, porém as técnicas utilizadas podem ser ineficientes ou insuficientes (ALVES, 2009).

Isso proporciona o aumento de redes inseguras e, portanto de pessoas que se utilizem desta falta de segurança para obter informações e os dados que ali trafegam. Segundo Alves (2009) é importante ressaltar que a falha de segurança não está necessariamente nas redes sem fio em si, mas sim no descaso com a segurança ou desinformação e falta/erros de configuração nas estações pertencentes à rede.

Portanto, além da utilização de métodos de defesa, os administradores de redes precisam monitorar, assim como em redes convencionais, as redes sem fio por eles gerenciadas. Com a utilização de ferramentas específicas pode-se detectar vários tipos de ataque às redes, como DoS ou *jamming*, acessos não autorizados, ataques às estações clientes entre outros, para que se possa tomar medidas que resolvam qualquer problema eventualmente encontrado (CERT.br, 2009).

Este trabalho propõe a criação de cenários que visam criar uma estrutura equivalente a de uma pequena rede para estudar casos com diferentes ferramentas para monitoramento e detecção de ataques, utilizando-se de diversos métodos de ataque para a realização dos testes.

1.1 OBJETIVO GERAL

Descrever e utilizar ferramentas para monitoramento e detecção de ataques em redes sem fio.

1.2 OBJETIVOS ESPECÍFICOS

A pesquisa tem os seguintes objetivos específicos:

a) descrever e aplicar os padrões de redes sem fio;

b) delimitar e utilizar algumas falhas de segurança em redes sem fio;
c) utilizar e descrever as principais ferramentas para monitoramento e detecção de ataques;
d) criar cenários para realização dos testes.

1.3 JUSTIFICATIVA

Com sua popularização, as redes sem fio se tornaram uma importante alternativa às redes cabeadas, devido à possibilidade e facilidade de suprir a falta de infraestrutura nas empresas e residências. Assim, a questão de segurança deve ser tratada com muito mais importância dado o valor que as informações têm para os proprietários da rede (SILVA; SOUZA, 2003).

O Padrão IEEE 802.11 é o responsável, além da criação de padrões, por agregar mecanismos de segurança das redes do conjunto 802. Porém estes mecanismos, unidos aos mecanismos de segurança também criados pelos fabricantes, não são suficientes para se criar redes seguras. Pois, à medida que os sistemas evoluem, as vulnerabilidades também aumentam, fazendo com que métodos atuais se tornem ineficazes contra novas ameaças (SILVA; SOUZA, 2003).

Segundo Albuquerque (2008) mesmo aplicando várias medidas de segurança, as redes sem fio continuam sendo alvo constante de pessoas mal intencionadas por considerar que mesmo utilizando vários mecanismos para evitar falhas na segurança, é possível que o atacante obtenha sucesso em suas tentativas de invasão.

O empenho da administração da rede pela melhoria de todos os aspectos envolvidos na rede deve ser constante, visto que os padrões e ferramentas evoluem

rapidamente, a atualização possibilita a adoção das melhores soluções para que a rede esteja de acordo com os padrões mais atuais.

Para poder controlar o uso da rede e avaliar se os aspectos de segurança tratados atualmente são eficientes, é imprescindível que o administrador da rede monitore-a constantemente, com o auxílio de ferramentas específicas que ajudam na detecção de ataques, permitindo que sejam tomadas medidas pró-ativas para minimizar as falhas de segurança atuais.

A vantagem principal do monitoramento é a possibilidade de detecção de falhas, não somente na segurança, mas em todos os aspectos que envolvam a rede, pois permite que seus administradores tenham um controle mais apurado em todos os pontos monitorados.

1.4 ESTRUTURA DO TRABALHO

O trabalho está dividido em seis capítulos. O primeiro tem a função de introduzir, listar os objetivos e justificar este trabalho.

No segundo capítulo é discorrido o tema da segurança das informações, sua importância e políticas para implementá-la.

O terceiro capítulo trata do conceito de redes sem fio, estudando seus principais padrões.

A questão da segurança em redes sem fio, suas vulnerabilidades e métodos de defesa são encontrados no quarto capítulo.

No capítulo seguinte, estuda-se como funciona o monitoramento em redes sem fio e as principais ferramentas que desempenham esta função.

O sexto capítulo traz informações acerca de trabalhos correlatos, desenvolvidos por outros acadêmicos.

Os estudos de caso com as ferramentas aqui testadas, bem como os resultados obtidos por esta pesquisa estão apresentados no sétimo capítulo.

2. SEGURANÇA DA INFORMAÇÃO

A segurança em Tecnologia da Informação (TI) é definida como processo de proteção contra ameaças das informações relevantes a pessoas ou instituições, a fim de garantir a integridade, disponibilidade e confidencialidade daquelas (BEAL, 2005).

A confidencialidade garante que os dados devem ser protegidos de acessos indevidos, ou seja, que somente os usuários permitidos tenham acesso a ele.

A integridade garante que as informações mantenham suas características originais em todo seu ciclo de vida, prevenindo-a de criação, alteração ou destruição não autorizada. Também permite identificar a autenticidade de seu autor.

A disponibilidade garante que a informação deve estar disponível aos usuários que tiverem seu direito de acesso.

Segundo Beal (2005) quando os dados forem transmitidos de um ponto a outro envolvendo algum processo de comunicação, é preciso que se observem outros aspectos em relação à segurança, portanto são tratados como objetivos da segurança da comunicação: integridade do conteúdo, irretratabilidade da comunicação, autenticidade do emissor e do receptor, confidencialidade do conteúdo e capacidade de recuperação do conteúdo pelo receptor.

2.1 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Devido ao crescente avanço das tecnologias da informação, as empresas se tornaram muito dependentes de tecnologias que permitem o armazenamento e manipulação de seus dados. Dado o valor que a informação tem para a empresa, esta pode ser prejudicada em todos os seus níveis, caso ocorra perda ou vazamento daquela (CARUSO; STEFFEN, 1999).

É preciso que se entenda a importância das informações para que as organizações possam manter sua infraestrutura tecnológica em segurança desde os estágios iniciais da implantação de seus sistemas, onde normalmente a segurança não é o foco principal (BEAL, 2005).

Para facilitar o trabalho do administrador nos aspectos relacionados segurança da informação, é importante definir uma metodologia para que sua implantação tenha sucesso.

2.2 POLÍTICAS DE SEGURANÇA

Para um administrador, garantir a segurança em TI de uma organização pode ser algo muito complexo, isso porque os dados nos sistemas da empresa são muito valiosos e "beneficiariam" muitas pessoas que tivessem sua posse e quisessem prejudicar a organização. Para deixar claro o que deve ser definido como meta na segurança da informação da empresa, uma política de segurança deve ser implantada.

As políticas de segurança têm o papel de metodizar o planejamento, implementação e gerenciamento da segurança dentro da organização. Elas auxiliam os administradores a terem um melhor controle de como a segurança das informações funcionará dentro da empresa. (NAKAMURA, 2000).

Descrevendo metas por meio de políticas bem estruturadas, é possível determinar o nível da segurança, quais funcionalidades ela oferecerá e suas facilidades de uso.

Deve-se objetivar uma política a partir das seguintes determinantes:

a) Serviços oferecidos versus Segurança fornecida: deve-se analisar se o risco de segurança de um determinado serviço é menor que o seu benefício. Caso positivo o serviço deve ser eliminado;

b) Facilidade de uso versus Segurança: O sistema deve ser o mais simples possível, porém não dispensando ou minimizando sistemas para deixá-lo mais seguro;

c) Custo da segurança versus o Risco da perda: deve-se analisar se o custo das informações vale o custo da implementação da segurança.

A política de segurança é idealizada a partir de um conjunto de regras seguras, que depois de pronta deve ser comunicada e imposta a todos os colaboradores da empresa. Segundo o IETF (1997) as características de uma boa política são:

> 1. Ela deve ser implementável através de procedimentos de administração, publicação das regras de uso aceitáveis, ou outros métodos apropriados.
> 2. Ela deve ser exigida com ferramentas de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível.
> 3. Ela deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

Vale ressaltar que o escopo de uma política de segurança não se resume somente a tecnologia, todo o pessoal envolvido na organização deve seguir regras de segurança para garanti-la em todo o meio de armazenamento de informações existente na empresa, como em documentos impressos.

Portanto, é importante que se conheça o conceito de redes sem fio e seus padrões para melhor entender como se pode protegê-las seguindo os conceitos básicos de segurança da informação e suas políticas.

3. REDES SEM FIO

As redes sem fio estão sendo amplamente utilizadas em residências e empresas, seja para comodidade ou por facilidade que ela proporciona ao permitir que seus usuários tenham mobilidade enquanto acessam sua rede local ou Internet.

Segundo Tanenbaum (2003) pode-se dizer que existem três principais categorias em redes sem fio:

a) Interconexão de sistemas;

b) LANs sem fio;

c) WANs sem fio.

A interconexão de sistemas diz respeito à interconexão de periféricos de um computador utilizando ondas de rádio com alcance limitado. Um exemplo disso são os mouses e teclados sem fio que utilizam a tecnologia Bluetooth para a conexão destes dispositivos com o computador, reduzindo o uso de cabos (TANENBAUM, 2003).

As LANs sem fio são redes locais em que os equipamentos ligados a rede devem ter um modem e uma antena de rádio para que possam se comunicar entre si diretamente ou através de concentradores de acesso (*access points* – AP's). Essas redes estão cada vez mais comuns em pequenas empresas e residências, onde a instalação com cabos seria trabalhosa demais (TANENBAUM, 2003).

A terceira categoria – WANs sem fio – permite que sejam criadas redes geograficamente distribuídas. Alguns exemplos são: interligação de empresas, redes para telefonia celular e distribuição de Internet banda larga sem utilização de linha telefônica. As WANs sem fio se assemelham às LANs sem fio, se diferenciando no fato de que as distâncias envolvidas são muito maiores (TANENBAUM, 2003).

3.1 FUNDAMENTOS DE REDES SEM FIO

Redes sem fio utilizam um meio totalmente diferente de redes convencionais, o ar. Devido a isso, é preciso utilizar-se de tecnologias específicas para garantir uma conexão eficiente entre os equipamentos da rede. Essas tecnologias devem compensar a impossibilidade de proteção física do meio utilizado nas redes *wireless*, fazendo com que estas obtenham um bom desempenho e estabilidade mesmo em ambientes poluídos (RUFINO, 2005).

3.1.1 Frequências e Canais

Frequência descreve o comportamento das ondas de rádio, ela determina sua velocidade de propagação, mais especificamente, quantas ondas são geradas no período de um segundo. Ela influencia diretamente na distância máxima que um sinal pode alcançar, sendo definido que quanto menor ela for, mais distante pode chegar (COLEMAN; WESTCOTT, 2006, tradução nossa).

As frequências são divididas em faixas, onde cada faixa é reservada para algum tipo de serviço. Em redes sem fio, as mais utilizadas são 2.4 e 5.8 GHz, que estão subdivididas em frequências menores. Essas subdivisões são chamadas de canais, que permitem a transmissão em paralelo de sinais diferentes em cada faixa de frequência (RUFINO, 2005).

Na Figura 1 pode-se ver como o espectro de frequências eletromagnéticas é dividido e utilizado nas comunicações.

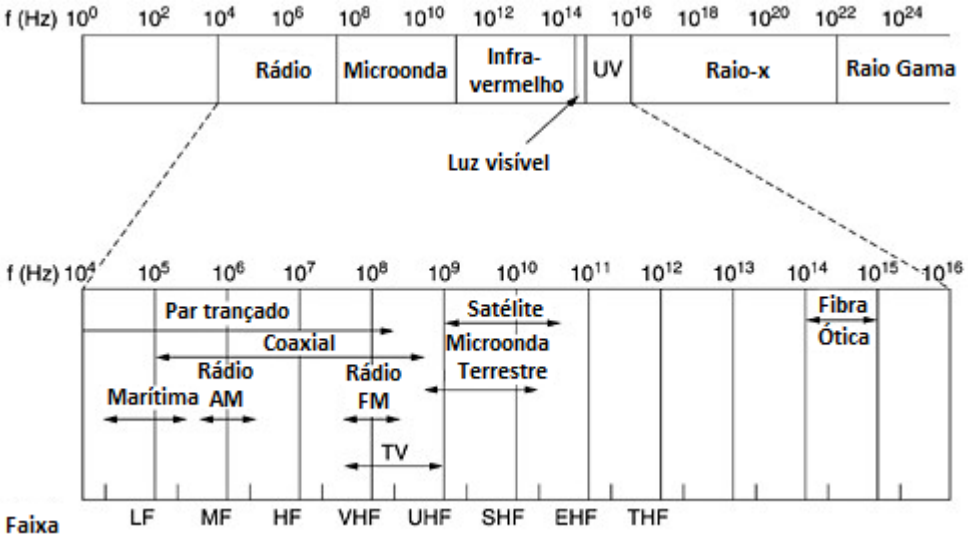

Figura 1. O espectro eletromagnético e a maneira como ele é usado na comunicação
Fonte: Adaptado de TANENBAUM, A. S. (2003, p. 90, tradução nossa)

3.1.2 Spread Spectrum

É uma tecnologia de transmissão de radiofrequência, desenvolvida inicialmente para uso militar, que se utiliza de todos os canais disponíveis na faixa de frequência para realizar a transmissão dos dados. Esta técnica consome mais banda do que seria necessário para o transporte dos dados, porém é mais imune a interferências externas já que utiliza várias frequências na conexão. Normalmente necessita de baixa potência nos transmissores - em média 100 *miliwatts* - para um bom funcionamento (COLEMAN; WESTCOTT, 2006, tradução nossa).

3.1.3 Direct Sequence Spread Spectrum (DSSS)

Foi criado no padrão 802.11, inicialmente para prover conexões de 1 e 2 Mbps, usando a faixa de frequência de 2.4 GHz. Mais adiante, foi adaptado ao padrão 802.11b, podendo estabelecer conexões de 5 e 11 Mbps (COLEMAN; WESTCOTT, 2006, tradução nossa).

Esta especificação divide a banda de 2.4 GHz em três canais distintos e separa cada bit de dados da transmissão em 11 subbits, que são enviados de forma redundante por um mesmo canal em diferentes frequências (RUFINO, 2005).

3.1.4 Orthogonal Frequency Division Multiplexing (OFDM)

Uma das tecnologias de comunicação mais populares atualmente, presente não somente em redes sem fio, mas também em redes cabeadas, como ADSL. Permite velocidades de transmissão de até 54 Mbps e é utilizada nos padrões 802.11a e 802.11g (COLEMAN; WESTCOTT, 2006, tradução nossa).

Esta tecnologia utiliza 52 frequências próximas e distintas para realizar a transmissão dos dados, chamadas de subportadoras. Quatro destas subportadoras são chamadas de portadoras piloto, que disponibilizam informações para as outras 48, auxiliando na prevenção da perda de sinal causada por interferências (ROSS, 2008, tradução nossa).

3.1.5 Bandas de rádio frequência públicas no Brasil

Segundo a Agência Nacional de Telecomunicações (2008) é possível utilizar certas faixas de radiofrequências para uso próprio sem autorização. As faixas públicas mais utilizadas são:

a) 902 – 907,5 MHz;
b) 915 – 920 MHz;
c) 2400 – 2483,5 MHz;
d) 5725 – 5875 MHz.

A faixa de 2.4 GHz é a mais utilizada em redes sem fio. Além dos padrões 802.11b, 802.11g e Bluetooth, vários equipamentos como telefones sem fio, fornos de microondas e babás eletrônicas se utilizam dessa frequência. Por esse motivo, é considerada como poluída e está mais sujeita a interferências (RUFINO, 2005).

3.1.6 Frequências licenciadas

Em oposição às frequências públicas, as licenciadas só podem ser utilizadas com autorização prévia da Anatel, além de requerer pagamento de taxas de atualização. Por serem regulamentadas estão menos sujeitas à interferência, podendo prover transmissões com uma qualidade de serviço superior às frequências públicas (RUFINO, 2005).

3.2 CARACTERÍSTICAS

Existem conceitos específicos para redes sem fio e outros que foram derivados das redes cabeadas. Essas características estão normalmente ligadas às camadas mais próximas do hardware e influenciam diretamente no modo como as transmissões são realizadas em uma rede *wireless* (RUFINO, 2005).

3.2.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Quando se trata de redes de comunicação, várias regras são necessárias para que o acesso ao meio seja compartilhado de forma eficiente entre todos os nós da rede. Hoje, o método mais utilizado em redes *wireless* é o CSMA/CA (COLEMAN; WESTCOTT, 2006, tradução nossa).

Esta série de regras especifica que, para que uma estação da rede possa transmitir, é necessário que esta verifique se algum outro dispositivo já esteja utilizando o meio. Caso esteja livre, será determinado um tempo de retardo aleatório antes de se iniciar a transmissão. Durante este tempo, a estação continua monitorando o meio para assegurar que outro equipamento não esteja transmitindo e só então começa sua transmissão. Caso não esteja disponível, o CSMA/CA manda instruções para que a estação entre numa fila de prioridade para depois poder transmitir (ROSS, 2008, tradução nossa).

Este processo garante que apenas um nó estará transmitindo de cada vez. E ocorre desta forma porque as redes sem fio operam utilizando o mesmo canal tanto para transmissão quanto para recepção, por isso não tem a capacidade de transmitir e detectar colisões simultaneamente (RUFINO, 2005).

3.2.2 Service Set Identifier (SSID)

É o nome da rede sem fio que deve ser conhecido por todos que estão na rede. Pode conter até 32 caracteres e é definido nos padrões 802.11, tornando possível a identificação das redes que estão ao alcance a partir de varreduras (ROSS, 2008, tradução nossa).

Em alguns concentradores é possível escolher por esconder o SSID das estações, para que só as que o configurem manualmente possam se conectar. Mesmo sendo uma medida muito fraca de prevenção contra intrusos, é utilizada por alguns administradores (COLEMAN; WESTCOTT, 2006, tradução nossa).

3.2.3 Beacon Management Frame

Beacons são utilizados por concentradores ou estações em modo Ad Hoc para enviar aos participantes da rede várias informações importantes para orientar os clientes conectados (RUFINO, 2005).

Segundo Coleman e Westcott (2006) os *beacons* podem carregar os seguintes dados:

a) informações de sincronização de tempo;
b) canal usado pelo AP;
c) taxas de dados básicas e suportadas;
d) nome da rede;
e) mapa de indicação de tráfego (que é utilizado durante o processo de economia de energia do AP);
f) informações extras da rede.

Normalmente são transmitidos 10 vezes por segundo, sendo possível alterar esse valor nas configurações do concentrador. A emissão de *beacons* não pode ser desabilitada (COLEMAN; WESTCOTT, 2006, tradução nossa).

3.2.4 Modos de Operação

Segundo Tanenbaum (2003) o comitê IEEE estabeleceu que os padrões da família 802.11 devessem funcionar em dois modos básicos de operação:

a) na ausência de um concentrador;
b) na presença de um concentrador.

3.2.4.1 Ad Hoc

O Ad Hoc e permite que os equipamentos se conectem diretamente uns aos outros sem precisar de um ponto central de conexão. Este modo de operação é mais utilizado para criação de pequenas redes de baixo custo ou para criar conexões de forma rápida para acesso momentâneo (RUFINO, 2005).

Na Figura 2 é demonstrado um exemplo de uma rede em Ad Hoc.

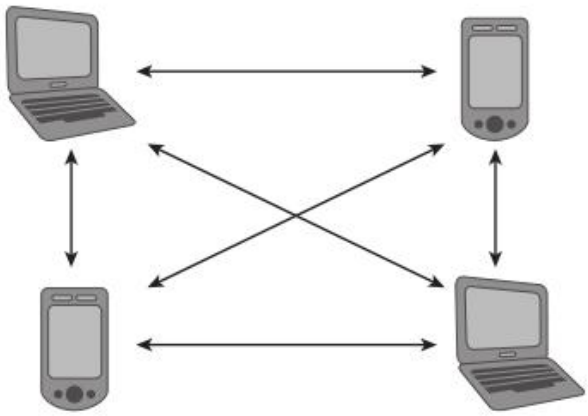

Figura 2. Topologia de rede no modo Ad Hoc
Fonte: COLEMAN, D; WESTCOTT, D. (2006, p. 207)

3.2.4.2 Infraestrutura

Neste modo de operação é necessário que todos os equipamentos participantes da rede se conectem num ponto central para poder realizar transmissões. Esta topologia permite um melhor controle da rede, pois as configurações de segurança são definidas no concentrador da rede e todas as transmissões obrigatoriamente passam pelo AP (RUFINO, 2005).

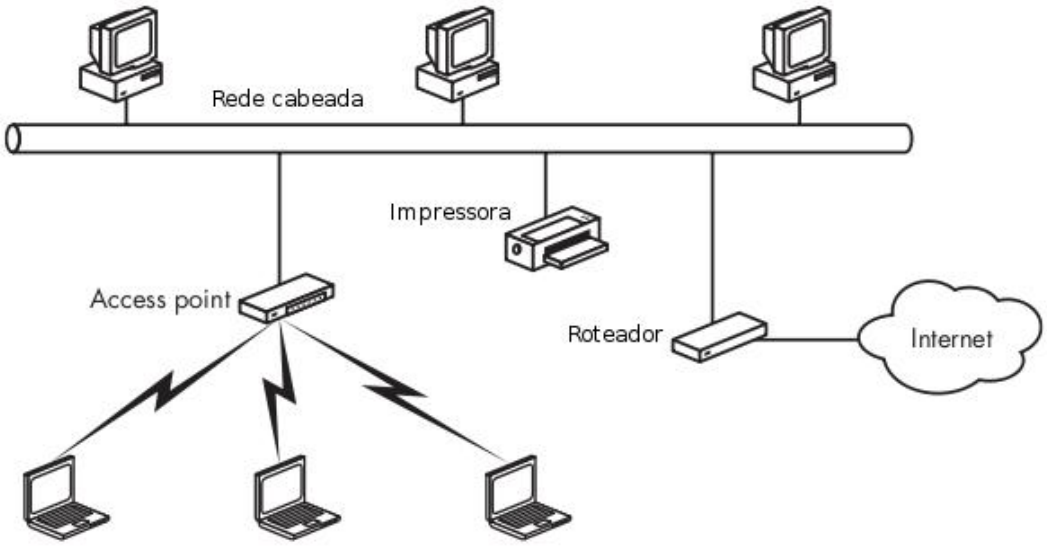

Figura 3. Uma pequena rede em modo infraestrutura
Fonte: Adaptado de ROSS, J. (2008, p. 39, tradução nossa)

3.1 PADRÕES DE REDES SEM FIO

Para que os equipamentos das mais variadas marcas tenham interoperabilidade entre si, o *Institute of Electrical and Electronics Engineers* (IEEE) desenvolveu padrões técnicos para redes sem fio conhecidos pela terminologia IEEE 802 (ALVES, 2009).

A especificação IEEE 802 foca nas duas camadas mais baixas do modelo de referência OSI porque incorpora tanto componentes físicos como de enlace de dados. Portanto, todas as redes do padrão 802 têm um componente MAC e um físico. O componente MAC é composto por uma série de regras que determina como acessar o meio e enviar dados, já o componente físico é encarregado de cuidar dos detalhes de transmissão e recepção (GAST, 2005, tradução nossa).

Esta relação da família 802 com o modelo OSI pode ser vista na Figura 4.

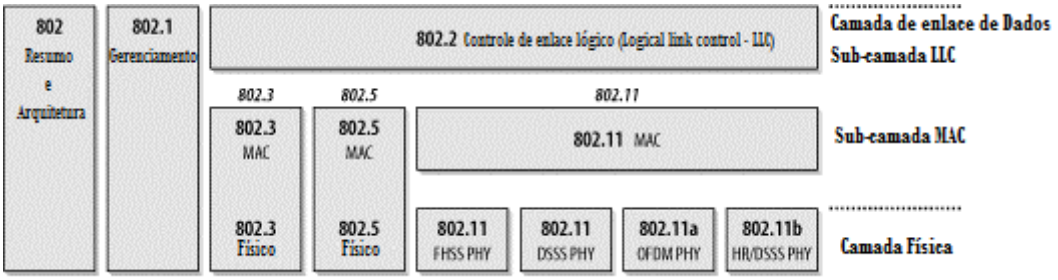

Figura 4. A especificação 802 e a sua relação com o modelo OSI
Fonte: Adaptado de GAST, M. (2005, p. 21, tradução nossa)

Do 802 surgiu a ramificação 802.11 onde são especificados os principais padrões para redes sem fio. É possível visualizar suas características na Tabela 1.

Tabela 1. Características dos principais padrões da família 802.11

PADRÃO	FREQUÊNCIA	ÁREA DE COBERTURA (em média)	VELOCIDADE MÁXIMA	VELOCIDADE TÍPICA
802.11b	2.4 GHz	30 metros (indoor) 100 metros (outdoor)	11 Mbps	4 Mbps
802.11a	5 GHz	35 metros (indoor) 110 metros (outdoor)	54 Mbps	23 Mbps
802.11g	2.4 GHz	35 metros (indoor) 110 metros (outdoor)	54 Mbps	20 Mbps
802.11n	2.4 GHz ou 5.8 GHz	70 metros (indoor) 160 metros (outdoor)	300 Mbps	120 Mbps

Fonte: Adaptado de ROSS, J. (2008, p. 27, tradução nossa)

3.1.1 Padrão IEEE 802.11b

Inicialmente proposto em 1999 e aprovado em 2003, o padrão IEEE 802.11b é a primeira ramificação do padrão IEEE 802.11, que foi criado com o intuito de alcançar velocidades maiores que o IEEE 802.11 (CARVALHO FILHO, 2005).

Este padrão opera na frequência de 2.4 GHz e suporta até 32 clientes conectados simultaneamente por AP (RUFINO, 2005). Utiliza modulação *Direct Sequence Spread Spectrum* (DSSS), o que faz com que sua taxa de transmissão máxima chegue a 11 Mbps, podendo ainda obter velocidades de 5.5 Mbps, 2 Mbps e 1 Mbps (FIGUEIREDO; DINIZ; COROA, 2005).

Apesar de ter poucos canais utilizáveis, ainda é o padrão mais utilizado no mundo.

Na Tabela 2 é possível visualizar a associação entre canais e frequências do 802.11b.

Tabela 2. Associação entre canal e respectiva frequência do padrão 802.11b

CANAL	FREQUÊNCIA
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Fonte: Adaptado de RUFINO, N. (2005, p. 27)

3.1.2 Padrão IEEE 802.11a

Este padrão veio após o 802.11b, com a proposta de tentar resolver os problemas existentes neste, como no aumento de velocidade e diminuição de interferência na transmissão (CARVALHO FILHO, 2005).

A velocidade máxima deste padrão atinge 54 Mbps, ou 108 Mbps em modo turbo, sendo que opera também em velocidades mais baixas e suporta até 64 clientes conectados simultaneamente. Sua faixa de frequência opera em 5 GHz, fazendo com que se torne incompatível com o antigo padrão 802.11b, porém melhorando a questão da interferência, já que existem agora 12 canais não sobrepostos disponíveis. Outra diferença é que este padrão utiliza o tipo de modulação *Orthogonal Frequency Division Multiplexing* (OFDM), que oferece mais largura de banda (RUFINO, 2005).

3.1.3 Padrão IEEE 802.11g

Mais recente que os anteriores, este padrão agrega benefícios do 802.11a e garante a compatibilidade com o padrão 802.11b, portanto ele trabalha na faixa de 2.4 GHz e oferece taxas de velocidade de até 54 Mbps. Utiliza a modulação OFDM e trabalha na mesma faixa de canais do padrão 802.11b, o que permite que sejam feitas redes mistas com equipamentos que suportem ambos os padrões, atentando para o fato de que a taxa de velocidade efetiva é sempre a do equipamento mais baixo envolvido na transmissão (RUFINO, 2005).

3.1.4 Padrão IEEE 802.11i

Este padrão possibilita o uso de mecanismos para prover segurança através de criptografia avançada (*Advanced Encryption Standard* – AES), autenticação e privacidade para proteger redes sem fio com a utilização de protocolos de chaves criptográficas (CARVALHO FILHO, 2005; RUFINO, 2005).

3.1.5 Padrão IEEE 802.11n

Segundo Rufino (2005) este padrão foi criado com o objetivo de alcançar altas taxas de velocidade (de 100 Mbps a 500 Mbps) e aumentar a área de cobertura atendida, mantendo a compatibilidade com os padrões em vigência.

A grande diferença é que nesse padrão foi modificado o OFDM para *Multiple Input, Multiple Out*-OFDM (MIMO-OFDM), em que se utiliza de diversas antenas transmissoras e receptoras para transmitir o sinal, proporcionando um aumento significativo na velocidade (FERREIRA; NOBRE, 2009).

Será visto no próximo capítulo como funciona a questão da segurança em redes sem fio, estudando suas principais vulnerabilidades e métodos de defesa existentes.

4. SEGURANÇA EM REDES SEM FIO

Redes sem fio são mais suscetíveis a ataques do que redes cabeadas pelo fato de que os dados trafegam pelo ar, isso proporciona certa facilidade aos atacantes se a rede não tiver os mecanismos necessários para proteger as informações que ali trafegam. Os ataques que atingem essas redes normalmente são os mesmos utilizados em redes guiadas, alguns apenas tiveram modificações para alcançar melhores resultados nas redes sem fio (SGUAREZI, 2007).

Segundo Rufino (2005) o uso de redes sem fio inseguras pode oferecer um risco às outras redes que se interligam a ela, por exemplo, em redes guiadas que contam com mecanismos eficazes contra invasões podem ter sua segurança comprometida ao se interligar a uma rede sem fio mal configurada.

A maioria das *Wireless LAN's* (WLAN's) provavelmente sofrerão ataques, que não são limitados somente a empresas, mas também a muitos usuários domésticos que usufruem dessa tecnologia em suas residências (SGUAREZI, 2007).

4.1 VULNERABILIDADES

A família de protocolos 802.11x apresenta muitas vulnerabilidades e apresentará muitas outras ainda não descobertas. Baseando-se nisso cada vez mais atacantes direcionam seus ataques às redes sem fio que podem estar comprometidas sem o conhecimento de seus donos. O fato de que essas redes podem ser atacadas até mesmo de locais distantes, dificulta muito o reconhecimento dos responsáveis e motiva os atacantes (FRANCISCATTI, 2005).

A seguir serão estudadas algumas dessas vulnerabilidades existentes em redes sem fios.

4.1.1 Vulnerabilidades Físicas

A segurança física em redes WLAN deve ser analisada diferentemente das redes convencionais, pois é possível se conectar a ela de lugares distantes, aumentando o risco de que alguém com um computador portátil aos arredores da empresa ou residência ataque a rede sem que se perceba (SGUAREZI, 2007).

Portanto é importante analisar a potência e o padrão utilizado nos equipamentos para que o sinal tenha alcance somente aos domínios da empresa, é importante também escolher o padrão correto e os mecanismos de segurança necessários para impossibilitar o acesso de pessoas não autorizadas à rede (RUFINO, 2005).

4.1.2 Vulnerabilidades no Envio e Recepção do Sinal

De acordo com Rufino (2005) é muito importante definir o local correto dos componentes de uma rede sem fio, pois com exceção de antenas direcionais ou setoriais, um concentrador envia sinal para todos os lados, portanto se for colocado em uma parede, o sinal será enviado tanto para dentro quanto para fora do ambiente o qual se encontra.

Para evitar ataques externos é recomendado que o administrador da rede posicione o concentrador mais ao centro possível do ambiente, pois melhor será a intensidade e qualidade do sinal recebido nas estações (SGUAREZI, 2007).

Na Figura 5 é demonstrado como o posicionamento do concentrador pode influenciar na segurança da rede WLAN, sendo que mesmo com um sinal baixo é possível que um atacante se conecte e comprometa a rede.

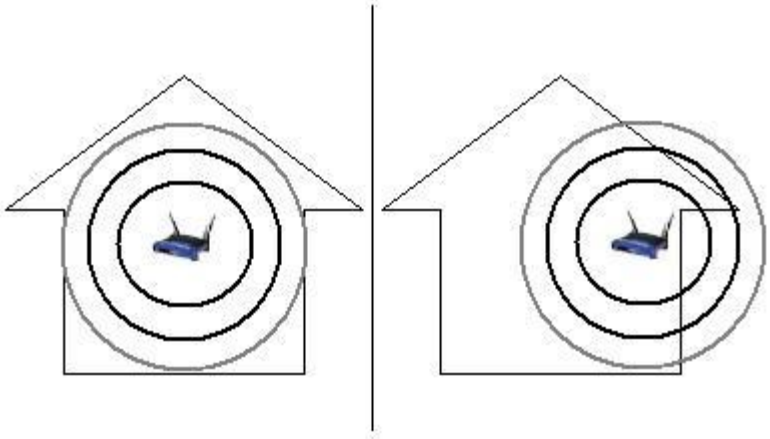

Figura 5. O posicionamento de um ponto de acesso é importante na segurança da rede
Fonte: RUFINO, N. (2005, p. 49)

4.2 MÉTODOS DE ATAQUE

A seguir serão estudados os principais mecanismos de ataques em redes sem fio, alguns são específicos para redes *wireless*, já outros são adaptados das redes cabeadas.

4.2.1 *Access Point Spoofing*

Também conhecido como associação maliciosa, é o ataque em que o invasor simula um AP real, fazendo com que os usuários que se conectam a ele fiquem vulneráveis a outros tipos de ataques, já que os dados que trafegarem pelo falso *Access Point* poderão ser capturados pelo atacante. Muitas vezes os usuários não percebem que foram vítimas desse ataque, por acreditarem que estão conectados a um AP real quando, na verdade, estão conectados diretamente ao atacante (SGUAREZI, 2007).

4.2.2 *ARP Poisoning*

O envenenamento do protocolo de resolução de endereços *Address Resolution Protocol* (ARP) é um tipo de ataque que é realizado na camada de enlace de dados e atua somente quando atacante e vítima estão na mesma rede local, portanto só é aplicável em redes conectadas por *switches*, *hubs* ou *bridges* (ANDRADE, 2004).

Este ataque surgiu nas redes guiadas e atua redirecionando o tráfego das vítimas para o atacante por meio da falsificação de endereços *Medium Access Control* (MAC), também conhecido como endereço físico (FRANCISCATTI, 2005).

4.2.3 *MAC Spoofing*

Segundo Rufino (2005) os concentradores de redes sem fio utilizam o registro de endereçamento MAC como medida de segurança para poder identificar os equipamentos que terão acesso a rede. Em contrapartida, os equipamentos clientes permitem a modificação de seu próprio endereço físico.

Portanto, este é o ataque em que o invasor descobre um endereço físico válido na rede e o utiliza para se conectar a ela (FRANCISCATTI, 2005).

4.2.4 Ataques de Negativa de Serviço

Também conhecido como *Denial of Service* (D.o.S), este ataque também surgiu em redes guiadas, e normalmente precisa de grande quantidade de banda para poder ter sucesso. Porém, em redes sem fio, este ataque pode ser bem sucedido mesmo com poucos recursos de rede. É possível utilizar métodos como associação, autenticação ou dissociação

em massa para promover o ataque mesmo com quantidade de banda limitada. Existem algumas ferramentas específicas para este tipo de ataque, que faz com que a rede fique tão ocupada respondendo aos ataques, que negue o serviço aos usuários legítimos (SGUAREZI, 2007).

4.2.5 *WLAN Scanner* (Ataques de Vigilância)

Segundo Franciscatti (2005) ataque de vigilância, mesmo não sendo considerado como ataque por muitos estudiosos, se torna uma ferramenta de ataque muito eficiente dependendo de sua finalidade.

Este ataque consiste em observar o local que se deseja invadir, procurando por WLAN's. Não é requerido nenhum equipamento especial, somente um dispositivo que capta sinais de redes sem fio. O objetivo principal desse ataque é conhecer a estrutura física onde estão os equipamentos que serão atacados posteriormente. Com isso, o atacante pode fazer com que os equipamentos voltem a sua configuração padrão ou até mesmo roubá-los (SGUAREZI, 2007).

4.2.6 *Wardriving*

Wardriving se assemelha muito ao ataque de vigilância estudado anteriormente, se diferenciando apenas na maneira como as WLAN's são encontradas. O foco não se limita a uma empresa ou residência, mas sim a todas as redes que forem possíveis de ser encontradas dentro da área de abrangência desejada. É praticada com o auxílio de um *Global Positioning System* (GPS) para mapear os AP's encontrados (DUARTE, 2003).

4.2.7 *Warchalking*

Este ataque se baseia na marcação de redes anteriormente encontradas pelas técnicas de wardriving. As marcações são feitas com pichação de símbolos em muros e calçadas onde se encontram essas redes para que os atacantes possam saber suas características (FRANCISCATTI, 2005).

Na Figura 6 pode-se observar alguns símbolos utilizados por atacantes.

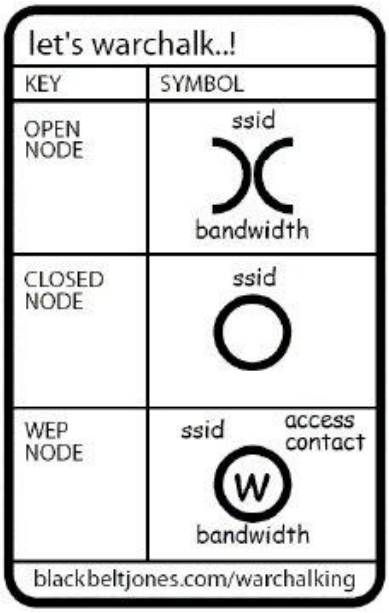

Figura 6. Alguns símbolos utilizados no warchalking
Fonte: PEIXOTO, R. (2004, p. 2)

4.3 MÉTODOS DE DEFESA

Segundo Alves (2009) é preciso implementar medidas como criptografia, meios apropriados de autenticação e monitoramento constante, para garantir a segurança em redes sem fio.

Com base nesse conceito, serão estudados nos próximos tópicos, os principais meios para proteger a rede, utilizando-se de medidas que provêem mecanismos para dificultar ao máximo a ação de invasores.

4.3.1 Autenticação em *Access Points*

De acordo com Duarte (2003) existem três modos de autenticação em concentradores de redes sem fio. São eles:

a) Autenticação aberta (*Open Authentication*): neste tipo de autenticação qualquer estação que conhecer o Identificador de Conjunto de Serviços (*Service Set Identifier* – SSID) pode se conectar a rede;
b) Autenticação compartilhada (*Shared Authentication*): neste modo, as estações clientes só terão acesso a rede caso compartilhem a mesma chave criptográfica do AP;
c) Rede-EAP (*Network-EAP*): aqui são utilizados algoritmos *Extensible Authorization Protocol* (EAP), que dão suporte a vários tipos de autenticação, por meio de servidores *Radius*.

4.3.2 Criptografia

Do grego *kryptós* (escondido) e *gráphein* (escrever), é definido como o ato de codificar dados em informações que pareçam sem sentido, sendo que somente alguém que conheça os métodos para decodificá-las terá acesso a elas. Existem várias utilidades da criptografia como: proteger documentos, transmitir informações confidenciais pela Internet, entre outros (SGUAREZI, 2007).

Serão discutidos nos próximos tópicos, os principais protocolos de criptografia de dados para uso em redes *wireless*.

4.3.2.1 WEP

O *Wired Equivalent Privacy* (WEP) é um protocolo que utiliza algoritmos simétricos, portanto para cifrar e decifrar as mensagens que trafegam, é exigida a existência de uma chave secreta que deve ser compartilhada entre o AP e clientes de uma rede *wireless* para que estes possam se comunicar (RUFINO, 2005).

A base de criptografia da chave secreta é feita pelo algoritmo RC4, o qual é conhecido pelo baixo custo de recursos e facilidade de implementação, funciona criptografando os dados ao mesmo tempo em que são transmitidos. Junto a ele existe um vetor de inicialização (IV) de 24 bits junto a uma chave secreta de 40 ou 104 bits (formando uma chave de 64 a 128 bits) que gera a informação criptografada (CARVALHO FILHO, 2005).

Também é utilizado *Cyclic Redundancy Check* (CRC-32) para calcular o *checksum* (soma de controle), que permite a verificação da integridade dos dados. Permitindo que os dados sejam averiguados pelo receptor para garantir que não foram alterados (CARVALHO FILHO, 2005).

Porém, muitas vulnerabilidades foram encontradas no algoritmo deste protocolo tornando-o inseguro. A mais significativa está relacionada a determinados valores do IV que permitem a quebra da chave secreta. Mesmo assim este protocolo ainda é utilizado, oferecendo apenas um nível básico de proteção (GRÜNEWALD, 2005).

4.3.2.2 WPA

O *Wi-Fi Protected Access* (WPA) foi criado pela *Wi-Fi Alliance*, em conjunto com o IEEE, para suprir as falhas de segurança encontradas no WEP. O WPA também utiliza o algoritmo criptográfico RC4 e mantêm a compatibilidade com os equipamentos que funcionam somente com o antigo protocolo, bastando uma atualização de *firmware* para estarem aptos a utilizar o novo. Seu principal propósito é implementar um mecanismo de mudança constante de chave para dificultar sua invasão ou descoberta (SGUAREZI, 2007).

A principal vantagem sobre o WEP é a utilização de um protocolo de chave temporária (*Temporal Key Integrity Protocol* – TKIP) que possibilita a criação de chaves por quadro, um mecanismo de distribuição de chaves e um vetor de inicialização de 48 bits, que é o dobro do antigo protocolo. Outra vantagem é a utilização do padrão 802.1x e do EAP que realiza a autenticação dos usuários antes de entrarem na rede (CARVALHO FILHO, 2005).

4.3.2.3 WPA2

O *Wi-Fi Protected Access* 2 (WPA2) é baseado no padrão IEEE 802.11i e utiliza como mecanismo de criptografia chamado protocolo *Advanced Encryption Standard* (AES). Este mecanismo foi escolhido, pois passou em todos os testes criptográficos conhecidos até então, sendo considerado como o substituto do *Data Encryption Standard* (DES) (SGUAREZI, 2007).

A principal vantagem do WPA2 é a compatibilidade com o WPA, que permite a utilização, além do AES, do TKIP e EAP (SOUZA, 2005).

Portanto, existem dois modos de funcionamento neste protocolo: WPA2-Enterprise, que possui todo o conjunto de requisitos WPA2 com suporte a autenticação

baseada em EAP, e WPA2-Personal, que foi desenvolvido voltado à utilização doméstica ou em pequenas empresas que não necessitam de tanta segurança (CARVALHO FILHO, 2005).

4.3.3 RADIUS

Abreviação de *Remote Authentication Dial-in User Service*, é um padrão de criptografia proprietário que utiliza uma camada extra de chaves de 128 bits reais para realizar a autenticação de usuários. Ele é mais seguro que o WEP, porém os equipamentos que o implementam são um pouco mais caros devido a necessidade dessa camada extra de criptografia (GRÜNEWALD, 2005).

Segundo Sguarezi (2007) esse método funciona basicamente através de requisições feitas pelo cliente e respostas enviadas pelo servidor. O processo de autenticação se inicia pela requisição enviada do cliente ao servidor com os dados do usuário. Após receber os dados, o servidor RADIUS encaminha uma resposta ao cliente, permitindo seu acesso ou negando, caso ocorra algum problema na autenticação. Ao permitir o acesso ao cliente, o servidor envia junto à resposta, os direitos e permissões referentes ao tipo/nível de acesso que usuário terá.

4.3.4 *Virtual Private Network* (VPN)

Uma VPN é uma rede privada construída sobre a infraestrutura de uma rede pública, funcionando como se os dados trafegassem em um túnel. Seu objetivo principal é a garantia de segurança dos dados transmitidos por meios inseguros, como a Internet. Portanto, nestas redes somente pessoas ou grupos com permissões específicas tem acesso a elas. Normalmente são utilizadas para: acessos remotos, conectividade entre redes locais ou para acesso a redes externas (FRANCISCATTI, 2005).

Utilizando-se desta tecnologia em redes *wireless*, é possível fazer com que todas as informações transmitidas entre as estações e o AP sejam criptografadas (SGUAREZI, 2007). Porém, Rufino (2005) explica que para obter todos os seus benefícios é preciso estender o domínio da VPN, não somente até o acesso a rede externa, mas também até a rede remota.

4.3.5 Firewalls

Firewalls são implementados para proteger uma rede de computadores contra intrusos. Normalmente funcionam como um filtro que protege redes privadas de ataques provenientes de redes públicas (SGUAREZI, 2007).

São eles que asseguram que todo o tráfego de origem ou destino à rede, deve obedecer a regras de uma política de segurança, que é configurável de acordo com as necessidades do administrador da rede.

5 MONITORAMENTO E DETECÇÃO DE ATAQUES EM REDES SEM FIO

Segundo Rufino (2005) o monitoramento é um dos mais importantes recursos de segurança que uma rede deve ter, independente do meio de transmissão. Utilizando-se deste método, é possível detectar possíveis falhas de segurança que, se não detectadas e corrigidas, podem deixar o ambiente vulnerável a diversos ataques.

Franciscatti (2005) descreve que o monitoramento pode coletar diversos dados importantes para o administrador de redes sem fio:

a) clientes conectados em determinado instante (em horários improváveis ou apenas para acompanhamento);
b) instalação de *Access Point's* não autorizados;
c) equipamentos que não estejam utilizando protocolos de segurança;
d) ataques contra clientes da rede;
e) acessos não autorizados;
f) mudanças de endereços MAC;
g) mudanças de canal;
h) qualidade do sinal transmitido;
i) algum serviço em D.o.S.

Com isso, fica clara a importância do monitoramento das redes sem fio para a preservação da segurança da informação, seja em ambientes corporativos ou residenciais.

A seguir serão descritos alguns métodos de monitoramento e defesa e suas principais ferramentas.

5.1 MÉTODOS DE MONITORAMENTO

O monitoramento desempenha a função de manter informações estatísticas sobre a rede, considerando o status da rede e dos equipamentos conectados a ela (SGUAREZI, 2007).

Existem dois métodos de coletar informações acerca de redes sem fio, que segundo Sguarezi (2007) são: passivo e ativo.

O método passivo é o tipo que coleta informações dos equipamentos da rede sem precisar interagir com eles.

O modo ativo é o que transmite perguntas (*queries*) aos ativos da rede para que seja possível a obtenção dos dados desejados.

5.2 EXEMPLOS DE FERRAMENTAS PARA MONITORAMENTO EM REDES SEM FIO

Nesta seção serão vistas algumas ferramentas para monitoramento e detecção de ataques em redes sem fio, com o intuito de conhecê-las melhor, para um posterior estudo de sua utilização.

5.2.1 Kismet

Esta ferramenta funciona como detector de redes, coletor de tráfego e um sistema de detecção de intrusão para uso em redes *wireless*.

O Kismet funciona com a maioria das placas de redes sem fio e monitora redes no padrão 802.11b, 802.11a, 802.11g e 802.11n. Com ele, é possível identificar redes a partir da coleta passiva de pacotes, além de detectar redes com o SSID escondido (KISMET WIRELESS, 2010).

5.2.2 WIDZ

O WIDZ é um sistema de detecção de intrusão para redes sem fio, que subdivide a função de monitorar problemas com tráfego em dois tipos de problemas: os de tráfego de forma geral e os de ataques específicos aos *Access Points*. O módulo widz_probemon, que é o encarregado de monitorar o tráfego geral, pode detectar varreduras e outras anomalias de tráfego (SGUAREZI, 2007).

5.2.3 AirTraf

Esta ferramenta é especializada em monitoramento e gerenciamento de redes sem fio. Suas principais características são:

a) Captura e analisa tráfego em redes com padrão 802.11b;
b) Faz cálculos de utilização de banda;
c) Determina a força de sinal de clientes wireless;
d) Encontra dinamicamente AP's em sua área de alcance;
e) Rastreia ações relacionadas ao acesso às redes sem fio, como varreduras, autenticação e associações, apontando sua possível natureza para determinar se o tráfego é suspeito.

5.2.4 NetStumbler

O NetStumbler é uma das ferramentas de varredura de redes sem fio mais conhecidas para o sistema operacional Windows. Pode informar vários dados importantes para o administrador da rede, como potência do sinal e SSID da rede, além do suporte a GPS.

Pode ser utilizado tanto para ataques quanto para auxiliar o administrador a monitorar todos os seus dispositivos *wireless* (FRANCISCATTI, 2005).

5.2.5 Beholder

É um monitor e detector de ataques em redes sem fio desenvolvido por brasileiros em código aberto. É escrito em linguagem de programação C e é desenvolvido para Linux. Pode detectar:

a) mudanças no AP (SSID, MAC e modo de operação);

b) mudanças de canal e criptografia;

c) AP *spoofing*;

d) AP's maliciosos.

6 TRABALHOS CORRELATOS

Vários trabalhos são desenvolvidos acerca da segurança de informações em redes sem fio, devido a sua grande importância nos dias atuais.

Neste capítulo, serão apresentados alguns trabalhos que se dedicaram a estudar as questões fundamentais de segurança e ferramentas de segurança em redes WLAN's.

6.1 ANÁLISE DE VULNERABILIDADES DE REDES SEM FIO E MÉTODO DE DEFESA POR MEIO DE SENHAS SEGURAS

Trabalho de conclusão de curso na área de Ciência da Computação feito na Universidade do Extremo Sul Catarinense – UNESC, por Ana Paula Biz no ano de 2010.

Este TCC explora a segurança em redes sem fio, com ênfase nas medidas de segurança que podem ser aplicadas. A autora explica algumas vulnerabilidades existentes e propõe métodos para aumentar a segurança nessas redes.

6.2 FERRAMENTAS DE SEGURANÇA EM REDES SEM FIO

Este trabalho é uma monografia de conclusão de curso na área de Ciência da Computação na Universidade Federal de Mato Grosso, escrita por João Vitório dos Reis Sguarezi no ano de 2007.

Nesta monografia o autor descreve as principais ferramentas utilizadas na segurança de redes sem fio, também estuda as principais vulnerabilidades existentes nessas redes.

6.3 REDES SEM FIO – TECNOLOGIA, SEGURANÇA E USABILIDADE

Monografia de pós-graduação Lato Sensu na área de Gestão de Tecnologia da Informação da Faculdade de Informática e Administração Paulista, desenvolvida por Marcus Albert Grünewald em 2005.

O autor estuda os principais padrões criados pelo IEEE, com o propósito de analisar a tecnologia de redes sem fio de forma simples, bem como suas vulnerabilidades.

6.4 UM ESTUDO DE PROTOCOLOS EMPREGADOS NA SEGURANÇA DE DADOS EM REDES SEM FIO – PADRÃO 802.11

Esta é uma monografia de conclusão de curso na área de Ciência da Computação no Centro Universitário de João Pessoa, escrita por João Rogério Lima de Carvalho Filho em 2005.

No trabalho, o autor realiza um estudo em redes do padrão 802.11 com ênfase em segurança. Ele apresenta os principais métodos de ataque e defesa a partir de cenários práticos, além de definir as principais precauções que um administrador dessas redes deve ter.

7 MONITORANDO E DETECTANDO ATAQUES EM REDES SEM FIO

Para testar a eficiência e demonstrar a correta utilização das ferramentas descritas nesta pesquisa, devem-se levar em consideração todos os aspectos que foram estudados relativos à segurança em redes *wireless*. Com isso, é possível definir quais ataques serão empregados e como detectá-los nos cenários criados.

Os ataques serão realizados por meio da suíte de ferramentas para ataques em redes sem fio Aircrack-ng, que oferece recursos de quebras de chave WEP e WPA, AP *spoofing*, D.o.S, entre outros.

O monitoramento dos ataques específicos para redes *wireless* será feito pela ferramenta Kismet – que é a mais completa e atualizada das ferramentas estudadas – e pela ferramenta Beholder – um simples detector de intrusão para redes *wireless*.

7.1 METODOLOGIA

Para a realização deste trabalho, foi feito levantamento bibliográfico desde seu início para obtenção de material científico. A maioria dos trabalhos é encontrada nos *sites* de universidades e outros em livros na biblioteca da UNESC.

Inicialmente, foram estudados os principais padrões de redes sem fio concretizados pelo IEEE e descritas suas principais vulnerabilidades e meios para garantir sua segurança. Alguns dos problemas na segurança podem ser resolvidos apenas com configurações feitas no AP ou até mesmo em seu reposicionamento físico. Porém, existem vulnerabilidades que podem ser exploradas mesmo quando os métodos corretos de segurança são aplicados.

Para monitorar e detectar possíveis ataques em redes sem fio, algumas ferramentas de monitoramento e detecção de ataques nessas redes foram testadas. A partir dos testes realizados, constatou-se que a maioria delas está desatualizada ou funciona em apenas alguns modelos de placas *wireless*. Isso influenciou e restringiu a escolha final das ferramentas, pois a maioria não funcionou como o esperado ou não suporta as placas comercialmente mais atuais.

Para completar o ambiente, também foi necessário o estudo de ferramentas para ataques em WLAN's. Com isso, será possível simular uma pequena rede, onde é possível identificar o concentrador da rede, monitor, atacante e clientes.

7.1.1 Ferramentas para Monitoramento e Detecção de Ataques Testadas

Durante a pesquisa, várias ferramentas foram estudadas para alcançar o objetivo de realizar testes com pelo menos duas ferramentas. Como citado anteriormente, a maioria delas estão descontinuadas e suas versões são antigas, outras suportam somente placas e *drivers* que eram utilizados na época em que foram criadas.

Para fins de documentação, estão listadas na Tabela 3 todas as ferramentas para monitoramento e detecção de ataques que foram pesquisadas e não funcionaram no ambiente de testes.

Tabela 3. Ferramentas para monitoramento e detecção de ataques que não funcionaram

Ferramenta	Problema encontrado	Data	Última versão
AirIDS	Suporta somente placas antigas (prism e aironet) / Sem link para download	-	-
AirTraf	Suporta somente placas antigas (prism2, orinoco e aironet)	2003	1.1
Garuda	Erro ao compilar ferramenta	2004	0.2.1
wIDS	Site retirado da Internet / Sem link para download	-	-
widz	Erro de *driver* não suportado ao executar	2003	1.5
snort-wireless	Site retirado da Internet / Sem link para download	-	2.0.1

Também foram encontradas ferramentas comerciais que não disponibilizam versões gratuitas para *download*. É possível ver quais são na Tabela 4.

Tabela 4. Ferramentas comerciais para monitoramento e detecção de ataques

Ferramenta	Fabricante
AirDefense	Motorola
AirMagnet	Fluke Networks
AirStorm	RandomStorm
AirWave	Aruba Networks
WiSentry	WiMetrics

7.1.2 Ambiente e Ferramentas Utilizadas

Procurou-se usar nessa pesquisa ferramentas atualizadas, gratuitas e disponibilizadas na Internet, a fim de permitir o máximo de compatibilidade nos mais variados ambientes.

Portanto, as ferramentas que serão estudadas nos testes de monitoramento e detecção de ataques são o Kismet 2011-03-R2 e Beholder 0.8.9 Beta.

Optou-se também por utilizar sistemas operacionais livres e gratuitos. E são:

a) distribuição Linux Ubuntu 10.10 para realizar o monitoramento e detecção de ataques;

b) distribuição Linux BackTrack 5 para efetuar os ataques.

Os seguintes aplicativos do pacote de ferramentas Aircrack-ng foram escolhidos para os ataques:

a) Airmon-ng: ativa ou desativa o modo monitor da interface *wireless*;

b) Aireplay-ng: permite realizar vários tipos de ataques em redes sem fio, como: injeção de pacotes para quebra de chaves WEP e WPA-PSK, desautenticação dos clientes, falsa autenticação, entre outros;

c) Airbase-ng: é capaz de criar um AP virtual, com a finalidade de realizar ataques de AP *spoofing*;

d) Airodump-ng: utilizado para pesquisar redes 802.11 e coletar dados.

Os equipamentos utilizados para a execução dos testes foram:

a) concentrador sem fio: Ovislink WL-1120AP;

b) placa de rede *wireless*: Atheros AR5B93;

c) placa de rede *wireless*: Tp-Link TL-WN422G - Atheros AR9271;

d) notebook Acer 4740: para monitoramento e detecção;

e) microcomputador Intel Core 2 Duo: para realização dos ataques;

f) celular Nokia 5800XM: cliente.

Na Figura 7 pode-se observar como ficou o ambiente de testes.

Figura 7. Configuração do ambiente de testes

7.2 ESTUDO DE CASO 1: MONITORANDO REDES SEM FIO E DETECTANDO ATAQUES COM O KISMET

O Kismet é capaz de monitorar e detectar ataques em redes 802.11 e funciona com qualquer placa *wireless* que suporte modo de monitoramento. Trabalha com redes nos padrões 802.11b, 802.11a, 802.11g e 802.11n (KISMET WIRELESS, 2010).

Esta ferramenta é robusta e tem atualizações constantes. É desenvolvida para Linux e OSX, mas pode ser instalado no Windows com suporte limitado de placas e recursos. Até a presente data da escrita desta seção, somente uma versão mais antiga (2009-06-R1) está disponível para Windows.

Como o foco é trabalhar com sistemas operacionais livres, esta pesquisa abordará somente a instalação e utilização em ambiente Linux.

O pacote de instalação para o Ubuntu e o código fonte podem ser baixados em seu site oficial. A instalação é facilitada em ambientes que utilizem o padrão de empacotamento do Debian por meio da ferramenta dpkg.

Depois de instalado, para iniciá-lo basta digitar no terminal: “kismet” (detalhes da instalação e configuração estão descritos no apêndice A).

Na Figura 8 pode-se ver a tela inicial da ferramenta.

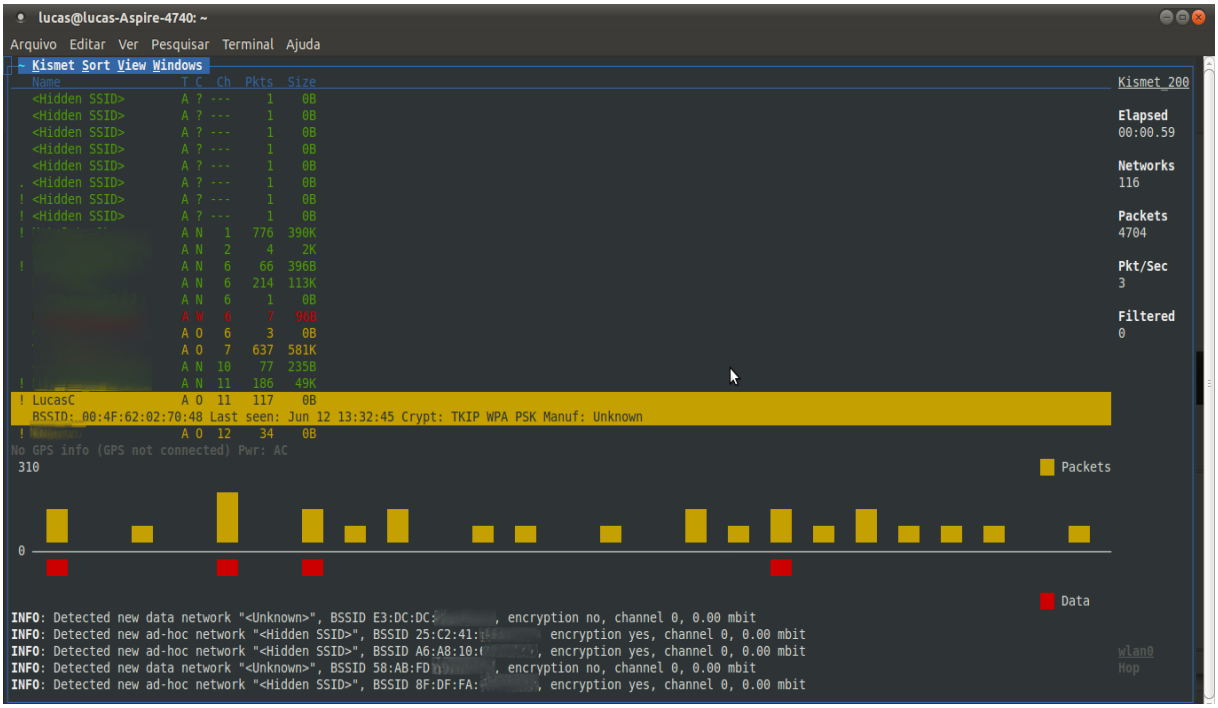

Figura 8. Tela inicial do Kismet

Nesta tela é possível identificar todas as redes que estão ao alcance do seu equipamento. Mais abaixo, pode-se ver a atividade de pacotes e dados que trafegam no momento. No canto inferior da tela estão os avisos de descoberta de novas redes e também alertas de possíveis ataques. Ofuscaram-se os nomes e endereços físicos para preservar redes que não são de propriedade do autor.

Além de detector de ataques, o Kismet também é uma ferramenta completa para monitoramento. Ele cataloga todas as redes encontradas com informações detalhadas de cada uma delas e as atualiza sempre que ocorrem mudanças.

Ao selecionar a rede, podem-se ver informações detalhadas da rede em questão. Na Figura 9 é mostrada a tela de informações da rede “LucasC”, a qual será monitorada e sofrerá os ataques para os estudos.

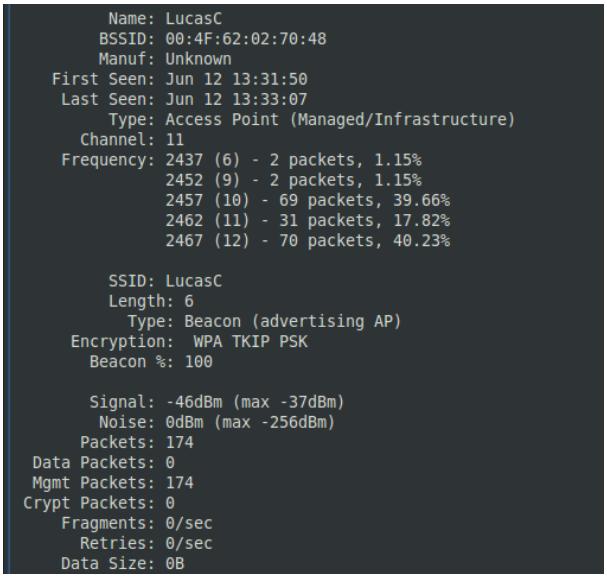

Figura 9. Informações da rede selecionada no Kismet

Pode-se perceber que a rede “LucasC” tem o endereço físico “00:4F:62:02:70:48”, está atuando como *Access Point* em modo infraestrutura no canal 11. Utiliza criptografia WPA e está com um nível de sinal de -46 dBm.

Selecionando a opção *Clients* no menu *View* é possível ver os clientes que estão respondendo aos anúncios da rede. Como mostra a Figura 10.

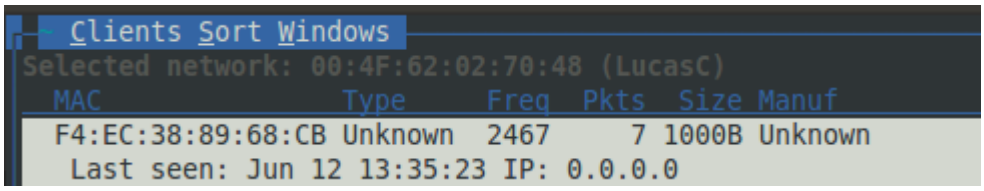

Figura 10. Lista de clientes respondendo aos anúncios da rede no Kismet

Neste caso, identifica-se apenas um cliente com o MAC “F4:EC:38:89:68:CB” respondendo aos anúncios desta rede. A Figura 11 mostra que também é possível obter informações detalhadas ao selecionar o cliente.

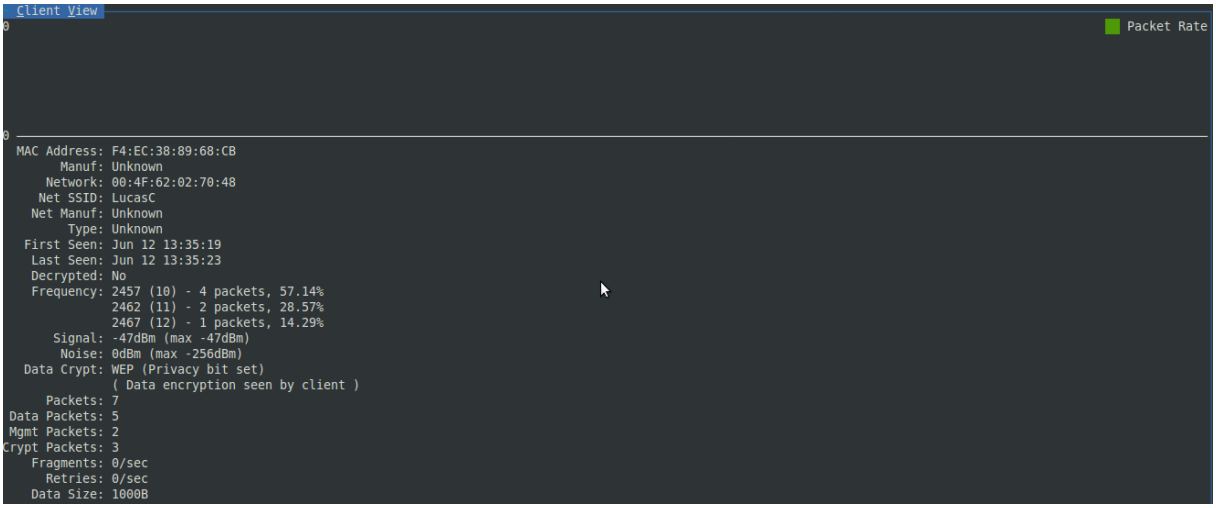

Figura 11. Informações detalhadas do cliente selecionado no Kismet

Com estes dados coletados, já se pode identificar se a rede que será monitorada sofrerá ataques. Portanto, os dados necessários para isso são:

a) SSID: LucasC;

b) MAC: 00:4F:62:02:70:48;

c) canal: 11;

d) criptografia: WPA.

Para ter uma visão específica dos alertas, entra-se na opção *Alerts* no menu *Windows* da tela principal.

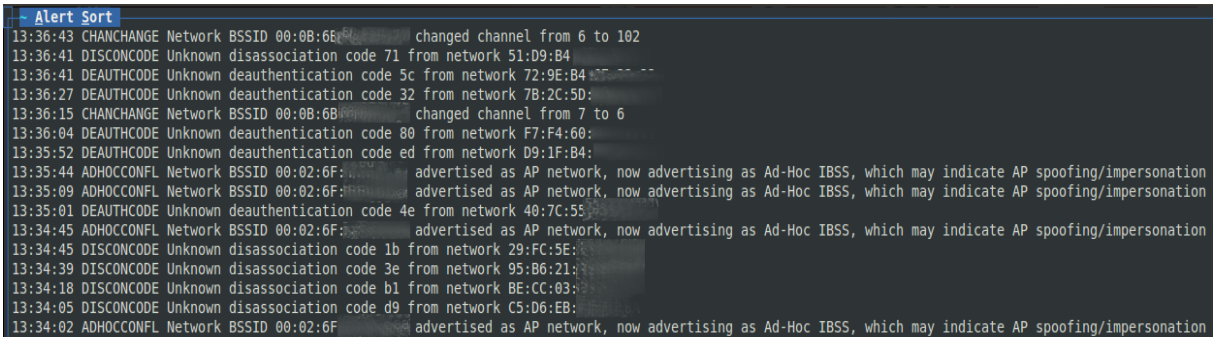

Figura 12. Tela de alertas do Kismet

Nesta tela são mostrados os alertas de todas as redes que estão ao alcance do computador e cada alerta tem uma assinatura específica.

Serão exploradas seis vulnerabilidades reportadas pelo grupo Wireless Vulnerabilites & Exploits (2005 a 2008). Que serão tratadas de acordo com suas assinaturas:

a) APSPOOF: detecta AP's que estão usando o mesmo SSID que o de sua rede, podendo fazer com que clientes se conectem pensando que é uma rede legítima. Este ataque pode permitir ao atacante capturar dados de quem esteja conectado a ele. Para isso, o Kismet permite que seja configurada uma lista com todos os seus concentradores e respectivos MAC's. Todo AP que não estiver nesta lista e estiver utilizando algum SSID que esteja nela gerará este alerta (no apêndice A pode-se ver como realizar esta configuração);
b) BCASTDISCON: este alerta ocorre quando o atacante forja pacotes de desassociação ou desautenticação e envia para toda a rede, fazendo com o que os clientes se desconectem. Isto caracteriza um ataque de negativa de serviço, já que os clientes legítimos ficam privados de acessar a rede.
c) BSSTIMESTAMP: AP's enviam regularmente seus *beacons* para orientar os clientes da rede. Nos *beacons* existe uma informação de sincronização de tempo. Quando estas informações são inválidas ou são recebidas fora de ordem, indica um possível ataque contra o AP legítimo que pode dificultar a comunicação com os clientes;
d) CHANCHANGE: indica que o AP está mudando de canal, isso pode ocorrer por ataques de AP *spoofing* ou por invasão no concentrador;
e) CRYPTODROP: indica que o AP parou de utilizar criptografia. Pode ser causado por ataques de *spoofing* contra o concentrador ou por invasão no mesmo;
f) KARMA: assinatura que caracteriza falsos concentradores que respondem por qualquer rede. Por exemplo, se um cliente procura por uma rede chamada

‘Teste123’, o falso AP responde como se fosse ‘Teste123’ (mesmo que ele já tenha respondido com outros SSID’s para outros clientes).

A primeira vulnerabilidade explorada será a APSPOOF. Para que seja gerado um alerta para este tipo de ataque, deve-se incluir o SSID e MAC da rede que se deseja monitorar no arquivo de configuração do Kismet (detalhado no apêndice A), ficando assim:

‘apspoof=Lucas:ssid="LucasC",validmacs=00:4F:62:02:70:48’

Para realizar o ataque primeiramente é necessário ativar o modo monitor da interface:

‘airmon-ng start wlan0’

Com isso, será criada uma interface virtual de monitoramento para sua placa *wireless*, normalmente referenciada como mon0. Logo após será utilizado o airbase-ng para criar um AP via software com o mesmo SSID (-e LucasC), criptografia (-z 2) e canal da rede (-c 11), porém com o endereço físico diferente (-a 00:4F:62:02:70:49):

‘airbase-ng -a 00:4F:62:02:70:49 -e LucasC -z 2 -c 11 -v mon0’

Com isso, o atacante pode interceptar os dados de clientes que se conectarem ao concentrador, caracterizando um AP *spoofing*.

Pelo fato deste MAC não estar configurado no Kismet como sendo uma rede legítima, imediatamente após a execução do ataque, foi gerado o alerta apontando a assinatura correta, como se pode visualizar na Figura 13.

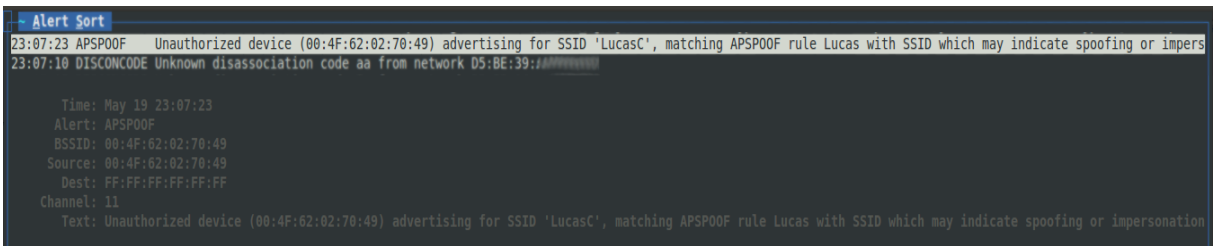

Figura 13. Detecção de AP spoofing no Kismet

O ataque foi repetido pelo menos cinco vezes, e em todas elas o alerta foi gerado corretamente, o que comprova a eficiência da ferramenta para este tipo de ataque.

O segundo teste será para a assinatura BCASTDISCON. Neste caso utilizou-se o programa aireplay-ng para mandar avisos de desassociação/desautenticação como se fossem do AP legítimo (-a 00:4F:62:02:70:48) a todos os clientes alcançáveis na rede:

‘aireplay-ng -0 0 -a 00:4F:62:02:70:48 mon0’

Este ataque também foi capturado imediatamente pelo Kismet. Como mostra a Figura 14.

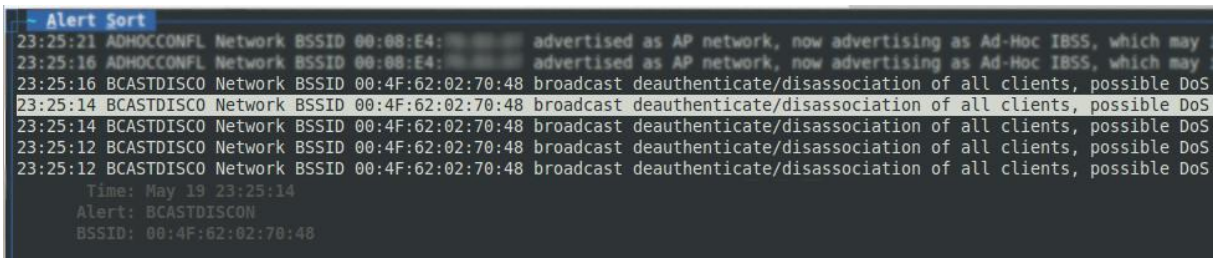

Figura 14. Detecção de D.o.S no Kismet

Apesar da imediata detecção desta assinatura, os clientes que estavam conectados a rede sofreram negação de serviço. Isto demonstra que o ataque foi bem sucedido.

Quando é direcionado para apenas um cliente, este ataque se mostrou mais efetivo e o Kismet não o detectou.

A próxima assinatura a ser testada é a BSSTIMESTAMP. Neste caso, criou-se um AP via *software* com as mesmas características do concentrador legítimo: SSID, MAC, canal e criptografia:

‘airbase-ng -a 00:4F:62:02:70:48 -e LucasC -z 2 -c 11 -I 4 mon0’

Sua detecção não foi imediata, somente quando um cliente trocou dados com o AP, é que foi mostrado o alerta:

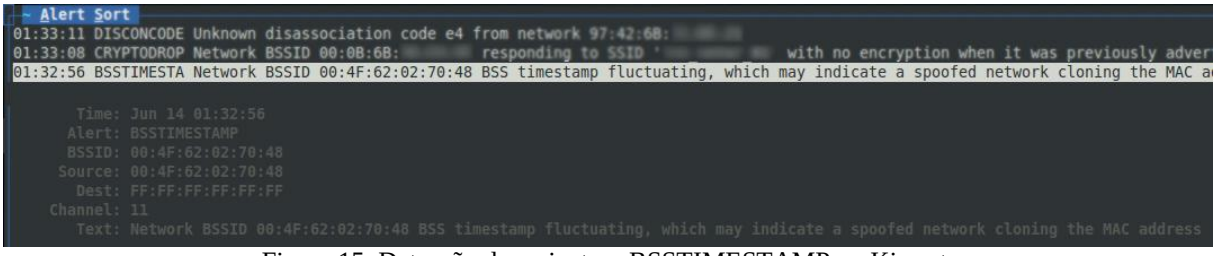

Figura 15. Detecção da assinatura BSSTIMESTAMP no Kismet

Outra vulnerabilidade testada foi a CHANCHANGE. Aqui o teste foi feito de duas maneiras. A primeira foi entrar nas configurações do concentrador e mudar o canal manualmente, simulando uma invasão no AP:

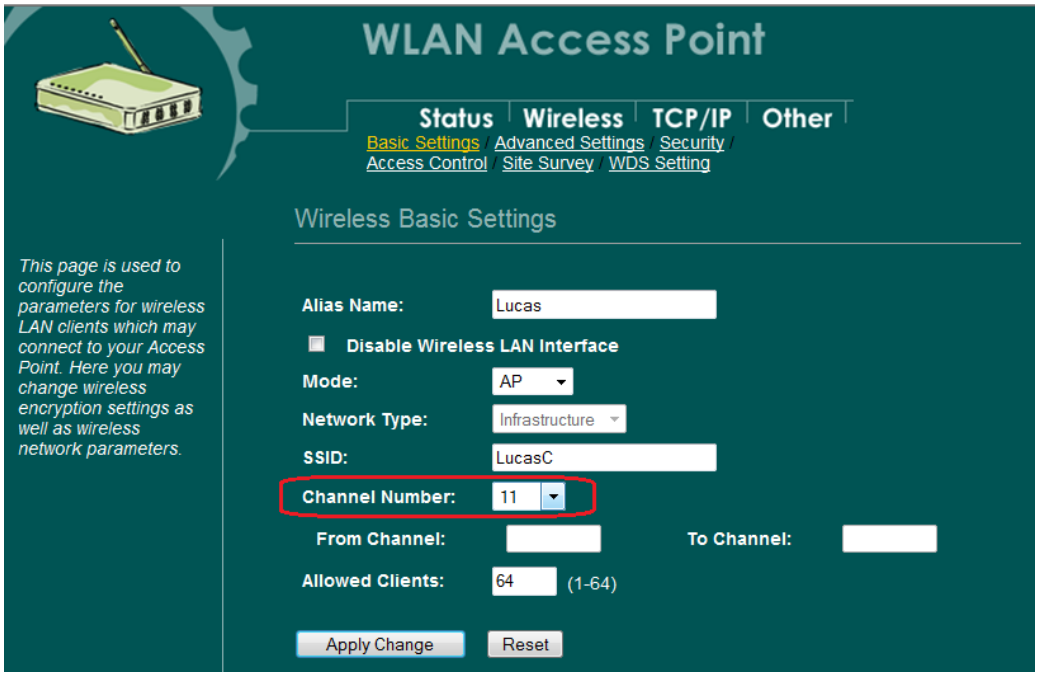

Figura 16. Mudando canal no Ovislink WL-1120AP

A segunda maneira foi criando um AP via *software* com as mesmas configurações do concentrador, apenas com um canal diferente:

‘airbase-ng -a 00:4F:62:02:70:48 -e LucasC -c 10 -z 2 mon0’

Das duas formas, o Kismet detectou imediatamente as mudanças de canal do AP. Como pode ser visto na Figura 17.

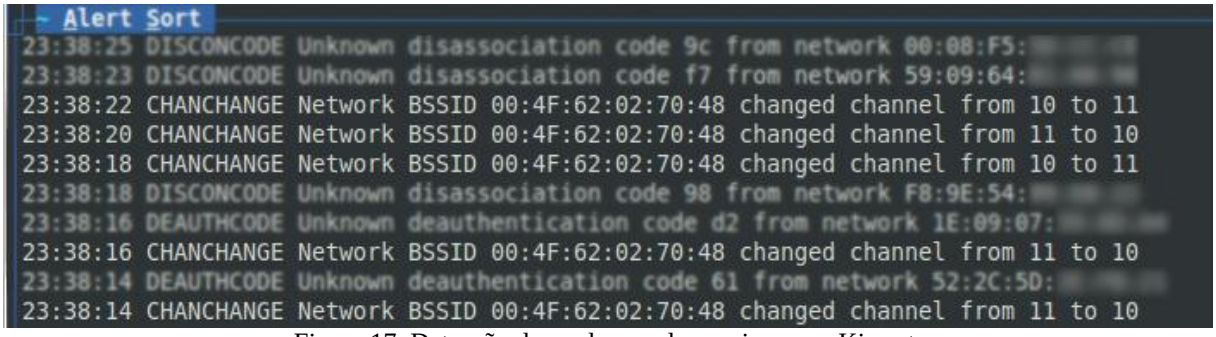

Figura 17. Detecção de mudanças de canais com o Kismet

A assinatura de CRYPTODROP também foi testada de duas formas. A primeira simulando uma invasão ao AP e desativando a criptografia em sua configuração:

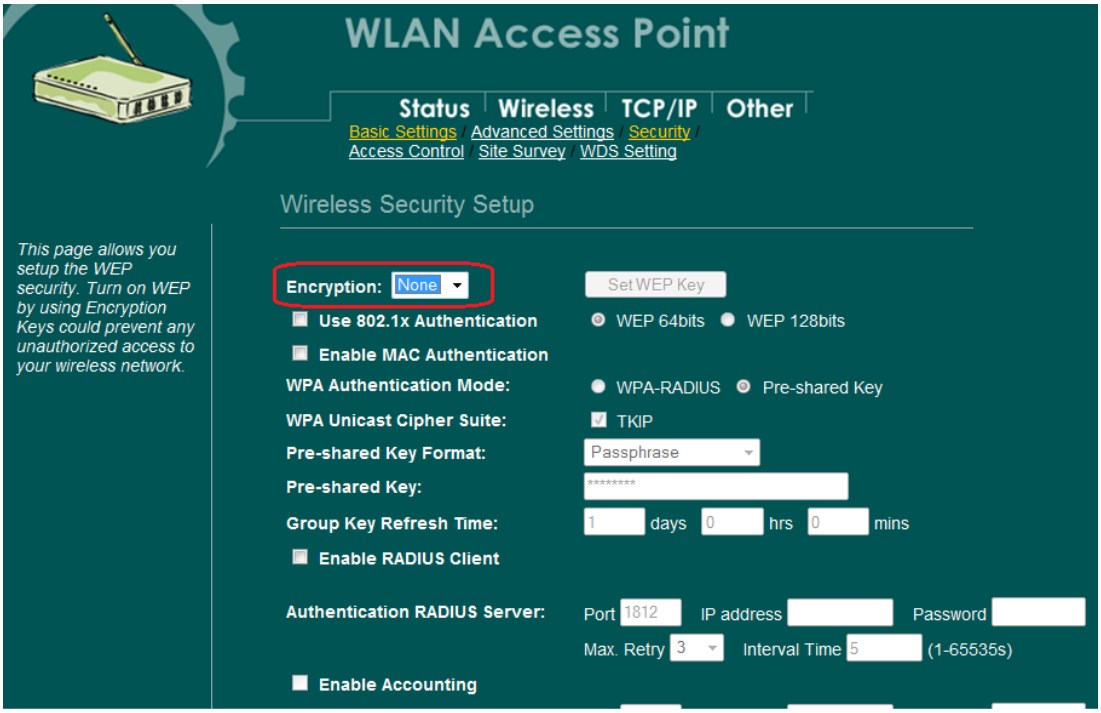

Figura 18. Desativando criptografia nas configurações do Ovislink WL-1120AP

A segunda, criando um softAP sem criptografia utilizando as mesmas configurações do AP para MAC, SSID e canal:

‘airbase-ng -a 00:4F:62:02:70:48 -e LucasC -c 11 mon0’

Em ambos os testes, o Kismet detectou as mudanças de criptografia imediatamente, gerando o alerta:

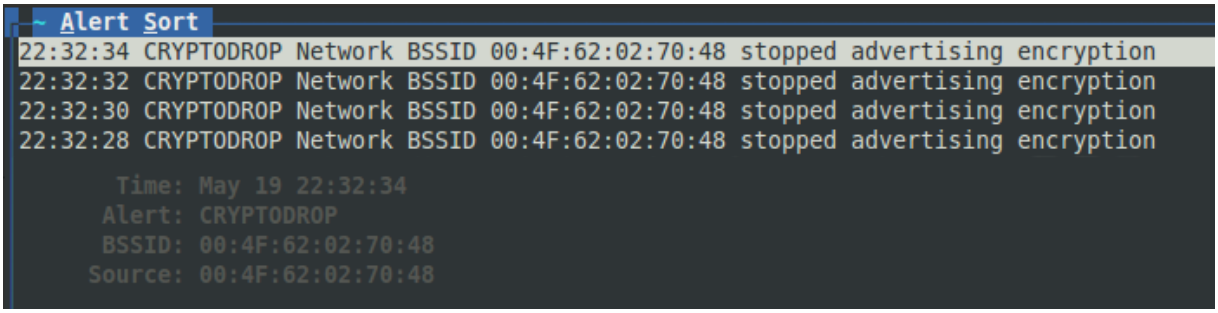

Figura 19. Detecção da assinatura CRYPTODROP no Kismet

O ataque de Karma também será realizado pela ferramenta airbase-ng, bastando informar apenas o MAC e canal desejados, com isso o AP passa a responder requisições em qualquer SSID que for pesquisado por clientes:

‘airbase-ng -a 00:01:02:03:04:05 -c 11 mon0’

A assinatura referente a este ataque foi detectada como APSPOOF pelo Kismet, porém agora informando que o Karma AP não é autorizado a responder pela rede:

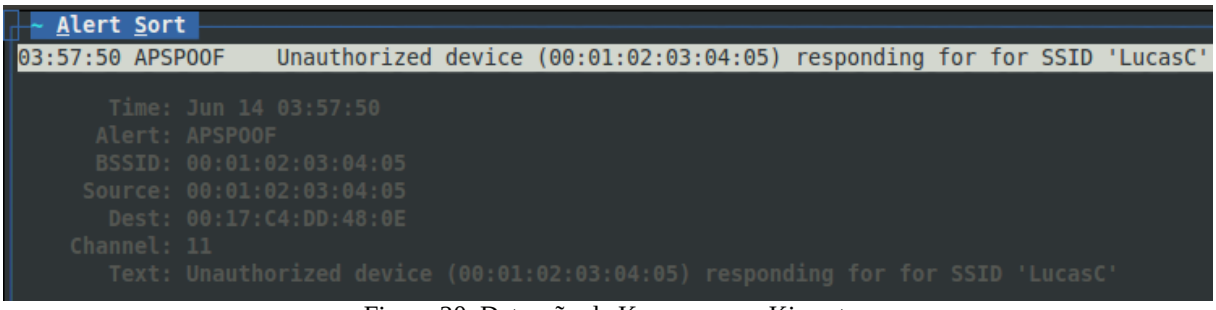

Figura 20. Detecção de Karma com o Kismet

7.3 ESTUDO DE CASO 2: UTILIZANDO O BEHOLDER PARA DETECTAR ATAQUES EM REDES SEM FIO

O Beholder é mais simples que o Kismet, porém garante uma boa funcionalidade na detecção de ataques a redes sem fio e também monitoramento. Ele não tem de uma

interface para gerenciamento, dispondo apenas de mensagens no terminal do Linux que mostram os avisos relacionados às redes.

Inicialmente, ele lista todas as redes encontradas, com seus respectivos MAC's, SSID's, canais e forças de sinal. Como se pode ver na Figura 21.

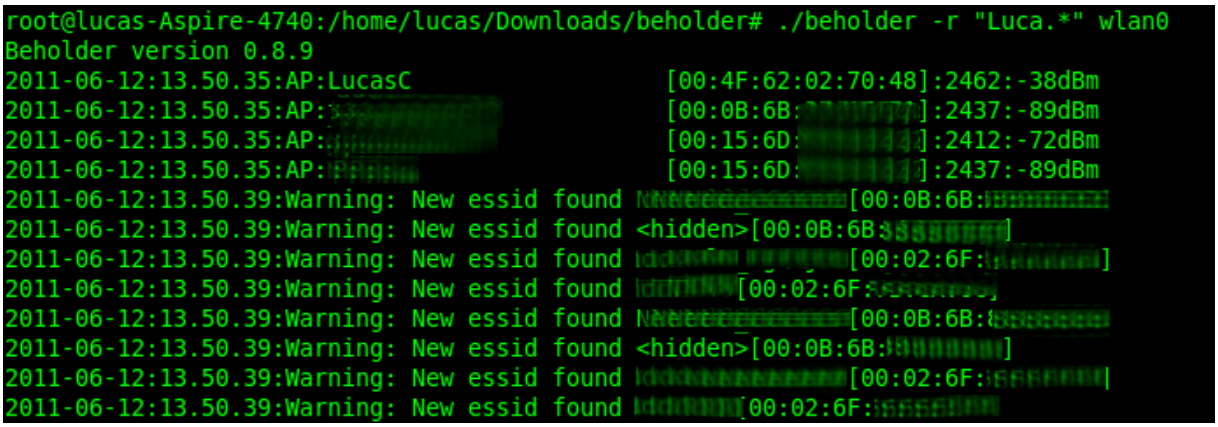

Figura 21. Iniciando o Beholder

Na hora de sua execução é possível definir o SSID da sua rede a partir da opção ' -c "NOMEDAREDE" '. Também é possível utilizar expressões regulares para determinar uma lista de SSID's que serão monitoradas. Isto é feito trocando a opção '-c' pela '-r', como mostrado na Figura 21. Neste caso, a ferramenta gerará um alerta toda vez que houver atividade suspeita em redes que comecem com 'Luca'.

Outra opção possível é a utilização da opção ' -m "NOMEDAREDE" ', que informa quando uma rede desaparece (também suporta expressões regulares). Em ambientes que monitoram muitas redes, aconselha-se a utilizar a opção '-a' para enviar os alertas para o log de sistema do Linux, para posterior análise.

Com os dados mostrados na tela da rede 'LucasC', já temos as informações necessárias para realizar os ataques, o monitoramento e a detecção destes ataques.

Aqui serão utilizados os mesmos ataques do tópico anterior, para ao final dos testes fazer uma breve comparação das duas ferramentas.

Iniciando com o teste da vulnerabilidade APSPOOF, a ferramenta imediatamente identificou atividades suspeitas:

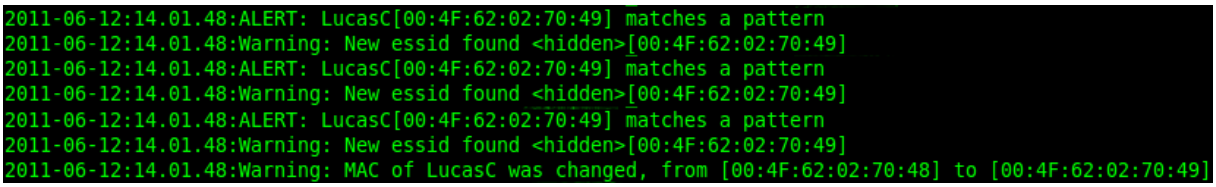

Figura 22. Detecção de AP spoofing no Beholder

A Figura 22 mostra que o Beholder detectou uma troca de endereço físico no AP, diferentemente do Kismet que utiliza a assinatura APSPOOF nesses casos. As duas abordagens estão corretas, pois se trata exatamente de um concentrador falso com as mesmas configurações do AP legítimo, porém com o MAC diferente.

Pode-se perceber também que, devido à opção passada o programa ‘-r “Luca.*” ’, sempre que for encontrada alguma rede que contenha ‘Luca’ no nome, será gerado um alerta.

O próximo teste realizado foi o de D.o.S, enviando pacotes que forçam os clientes a se desconectarem. Este ataque não foi detectado pela ferramenta. Em sua documentação não foram encontrados indícios de que exista alguma implementação para este tipo de ataque. Repetiu-se o teste cinco vezes, e em nenhuma delas houve detecção.

Continuando com os testes, a próxima vulnerabilidade testada foi a BSSTIMESTAMP. Este ataque não gerou nenhum alerta específico, porém avisos foram mostrados no terminal:

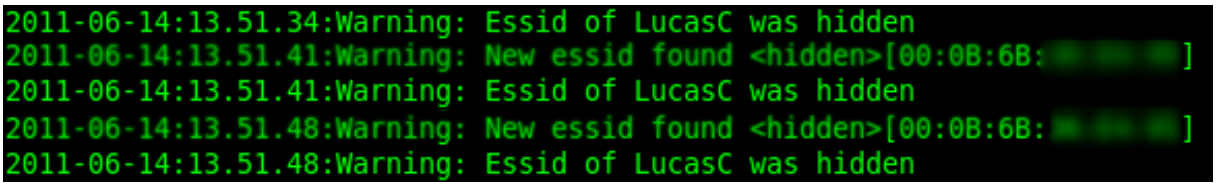

Figura 23. Detecção de BSSTIMESTAMP no Beholder

Como mostra a Figura 23, o ataque não foi identificado, porém, por meio dos avisos da ferramenta, é possível perceber que são encontradas anomalias na rede. Em determinado momento ela aparece com o SSID correto e logo após deixa de divulgar o SSID. Isso ocorre porque o Beholder hora detecta uma rede, hora a outra. Isso certamente faz com que estes avisos sejam gerados frequentemente quando a rede está sofrendo este tipo de ataque.

A assinatura CHANCHANGE foi detectada imediatamente após o ataque, mostrando a rede, em que canal o AP estava e para qual ele foi modificado:

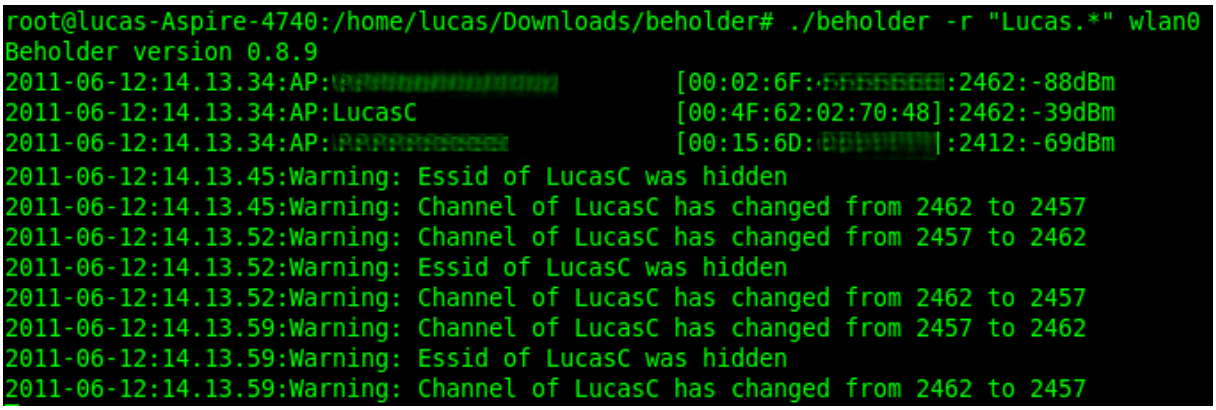

Figura 24. Detecção de mudanças de canal no Beholder

A mudança de criptografia na rede também foi detectada:

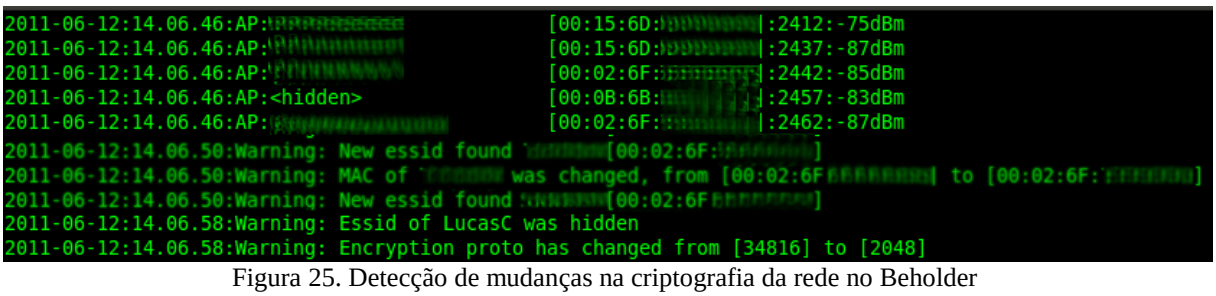

Figura 25. Detecção de mudanças na criptografia da rede no Beholder

Vale ressaltar neste caso, que apesar de ser detectada a mudança de criptografia, a mensagem deste aviso está incompleta, pois não define em qual rede isso ocorreu, nem qual criptografia o AP estava utilizando antes do ataque.

O último ataque testado foi o de Karma, que gerou um alerta (Karma is in the house) para a assinatura específica:

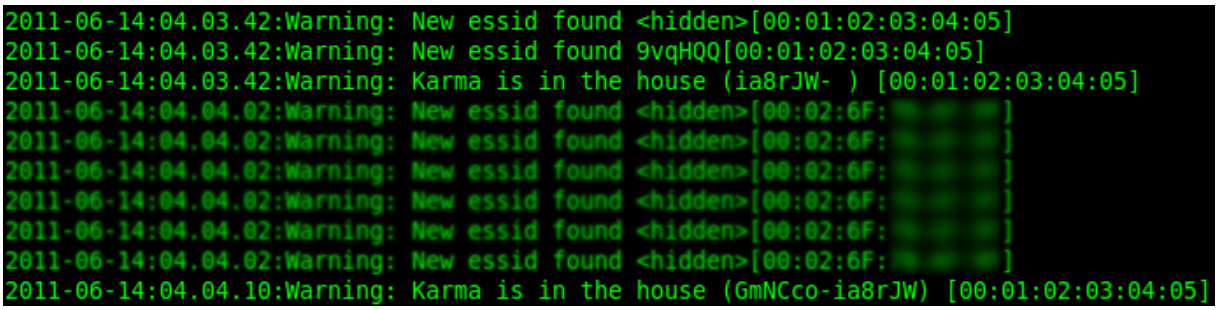

Figura 26. Detecção de Karma no Beholder

7.4 RESULTADOS OBTIDOS

Todos os testes foram realizados pelo menos cinco vezes cada para garantir que em todas as tentativas seria detectada a assinatura correta.

Ambas as ferramentas apresentaram resultados satisfatórios nos testes aplicados nesta pesquisa. A Tabela 5 demonstra os ataques e o resultado da detecção de cada um.

Tabela 5. Ataques testados no Kismet e Beholder

Ataque	Kismet	Beholder
APSPOOF	Detectado	Detectado
BCASTDISCON	Detectado	Não Detectado
BSSTIMESTAMP	Detectado	Detectado com outra assinatura
CHANCHANGE	Detectado	Detectado
CRYPTODROP	Detectado	Detectado
KARMA	Detectado	Detectado

O Kismet, por se tratar de uma ferramenta que vem sendo desenvolvida há longo tempo e sempre com atualizações constantes, tem muito mais opções e disponibiliza uma melhor interface de gerenciamento ao administrador. Ele também permite a integração com um aparelho de *Global Positioning System* (GPS) para delimitar o local das redes monitoradas.

Apesar de focar mais na parte de monitoramento e detecção de ataques, permite também realizar ataques, por meio de *plugins* que podem ser baixados em seu site.

Já o Beholder se trata de um projeto de dois desenvolvedores brasileiros que está em estágio *beta* e por isso não agrega muitas funções além dos alertas e avisos das redes. Mesmo não apresentando mensagens de aviso e alertas amigáveis, foi eficiente em detectar a maioria dos ataques aqui aplicados.

As duas ferramentas pecaram no tratamento das informações coletadas, pois permitem somente que sejam gravados arquivos de *log* sem nenhum tipo de filtro por assinatura ou por rede. Enquanto essa funcionalidade não é agregada nas ferramentas, existem programas analisadores de *log* que auxiliam o administrador da rede nesta deficiência, como o Swatch e Logwatch para Linux.

Em uma visão geral, tanto o Kismet quanto o Beholder, podem auxiliar o administrador no gerenciamento de suas redes, pois dão várias informações que ferramentas de monitoramento comuns não dão. Auxiliam também na segurança da rede como um todo, pois permitem detectar vários tipos de ataques em redes *wireless*.

CONCLUSÃO

Esta pesquisa tratou vários aspectos da segurança de redes sem fio, destacando sua importância para garantir as melhores formas de protegê-las contra ataques e vulnerabilidades. Esta tarefa é ainda mais complicada em redes *wireless* pelo fato de que os dados ficam mais expostos devido ao meio utilizado nas transmissões.

Existem vários métodos que diminuem os riscos a ataques nessas redes, porém também existem vulnerabilidades que podem ser exploradas mesmo com a utilização das medidas de segurança corretas. É aí que se vê a necessidade de um constante monitoramento que permita identificar dados importantes das redes e que possam detectar tentativas de ataques.

As ferramentas Kismet e Beholder foram utilizadas neste trabalho, e mostraram que é de extrema importância o monitoramento e a detecção de ataques constantes em redes sem fio. A partir destas ferramentas foi possível verificar possíveis vulnerabilidades e detectar com eficiência todos os ataques testados.

A maior dificuldade encontrada foi a falta de ferramentas com licença de uso livre e atualizadas para esta finalidade. Pelo menos seis ferramentas testadas não funcionaram adequadamente. A maioria delas teve a última atualização há longo tempo e só funcionavam em placas de modelos muito antigos e restritos que tipicamente não são mais comercializadas.

Outro fator que pode dificultar o funcionamento dessas ferramentas é a necessidade de suportar nas placas e *drivers*, o modo monitor. Por isso, procuraram-se utilizar placas atualizadas com seus *drivers* mais recentes.

Com esta pesquisa, foi possível aprimorar um conhecimento científico na área de segurança em redes, especialmente nos detalhes técnicos que são exclusivos a redes sem fio. Também foi possível analisar o funcionamento dos ataques e quais os riscos que uma rede

wireless sob ataque pode oferecer para todos os outros pontos da rede. Outro resultado foi a documentação de vários ataques e como as ferramentas para monitoramento e detecção de ataques se comportam em vários tipos de ataques.

Para trabalhos futuros, podem-se realizar testes utilizando ferramentas comerciais e posteriormente fazer um comparativo com as ferramentas livres. Também pode ser tratada a questão do gerenciamento dos *logs* das ferramentas aqui testadas, talvez implementando na própria ferramenta (já que é de código aberto) ou utilizando outras ferramentas para realizar esta tarefa.

REFERÊNCIAS

Agência Nacional de Telecomunicações – Anatel. **Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita**. Disponível em: <http://www.anatel.gov.br/Portal/documentos/biblioteca/Resolucao/2004/Anexo_res_365_2004.pdf>. Acesso em 13 maio 2011.

ANDRADE, Lidiane Parente. **Análise das Vulnerabilidades de Segurança Existentes nas Redes Locais Sem Fio: Um Estudo de Caso do Projeto Wlaca.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Federal do Pará, Belém, Pará, 2004.

ALVES, Walter F. Andrade. **Segurança em Redes Sem Fio: O caso da Assembléia Nacional de Cabo Verde.** Trabalho de Conclusão de Curso – Curso de Engenharia de Sistemas e Informática, Universidade Jean Piaget de Cabo Verde, 2009.

AMORAS, Romulo A. S.; BRABO, Gustavo S; JUNIOR, Carlos A. C. V. P. **Segurança em Redes Wireless padrão IEEE 802.11b: Protocolos WEP, WPA e Análise de Desempenho**. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade da Amazônia, Belém, Pará, 2004.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 175 p.

BIZ, Ana Paula. **Análise de vulnerabilidades de Redes Sem Fio e Método de Defesa por meio de Senhas Seguras**. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, Santa Catarina, 2010.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações.** 2.ed. São Paulo: SENAC/SP, 1999. 367 p.

CARVALHO FILHO, João R. Lima. **Um Estudo de Protocolos Empregados na Segurança de Dados em Redes sem Fio – Padrão IEEE 802.11**. Monografia do UNIPE – PE, 2005.

CBPF – NT 003/02. **Segurança em Redes Wireless 802.11**. Autores: Bruno Marques Amaral, Marita Maestrelli, Março de 2003.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA – CERT.br. **Práticas de Segurança para Administradores de Redes Internet**. Disponível em: < http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf >. Acesso em: 07 de Mai. de 2010.

COLEMAN, David D.; WESTCOTT, David A. **CWNA – Certified Wireless Network Administrator: Study Guide.** Indianapolis: Wiley Publishing, 2006. 594 p.

DUARTE, Luiz Otávio. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, São Paulo, 2003.

FERREIRA, Clécio Anderson de L.; NOBRE, Wendell. **802.11n**. Disponível em: <http://www.cefetrn.br/~valentim/disciplinas/interconexoes_redes/802_11n_.pdf>. Acesso em 13 de out. de 2010.

FIGUEIREDO, Marcio Edmar Girard; DINIZ, Palmenas Costa; COROA, Sérgio Vinícius. **Segurança em Redes sem Fio Utilizando VPN Baseado em SSL.** Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade da Amazônia, Belém, Pará, 2005.

FRANCISCATTI, Vagner. **Segurança em Redes Sem Fio**. Trabalho de Conclusão de Curso – Curso de Especialização em Redes de Computadores e Comunicação de Dados, Universidade Estadual de Londrina, Londrina, Paraná, 2005.

GAST, Matthew. **802.11 Wireless Networks: The Definitive Guide**. 2.ed. Sebastopol, CA: O'Reilly, 2005. 464 p.

GRÜNEWALD, Marcus Albert. **Redes sem fio – Tecnologia, Segurança e Usabilidade**. Monografia da Faculdade de Informática e Administração Paulista. São Paulo, 2005. Disponível em: <http://www.apostilando.com/download.php?cod=2215& categoria=Redes>. Acesso em 10 set. 2010.

IEEE STANDARS ASSOCIATION. IEEE 802.11: **LAN/MAN Wireless LANS**. Disponível em: <http://standards.ieee.org/getieee802/802.11.html>. Acesso em 07 maio 2009.

KISMET WIRELESS. **Kismet**. Disponível em: <http://www.kismetwireless.net>. Acesso em 07 nov. de 2010.

NAKAMURA, Emilio Tissato. **Um Modelo de Segurança de Redes para Ambientes Cooperativos.** Dissertação de Mestrado – Instituto de Computação, Universidade Estadual de Campinas, Campinas, São Paulo, 2000.

PEIXOTO, R. (2004). **Tecnologias wireless demandam cuidados extras: a prática do wardriving e warchalking**. Disponível em: <http://www.correiadasilva.com.br/midia/midia_23.pdf>. Acesso em 14 out. 2010.

ROSS, John. **The Book of Wireless: a Painless Guide to Wi-Fi and Broadband Wireless**. 2. ed. San Francisco: No Press, 2008.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes Sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. São Paulo: Novatec, 2005.

SGUAREZI, João V. Dos Reis. **Ferramentas de Segurança em Redes sem Fio**. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Federal de Mato Grosso, Cuiabá, Mato Grosso, 2007.

SILVA, G. M.; SOUZA, J. N. **Uma análise dos mecanismos de segurança de redes locais sem fio e uma proposta de melhoria**. III Workshop de Segurança de Sistemas Computacionais, Workshop de segurança – WSEG. In: Anais do SBRC 2003, Natal, 2003

SOUZA, Ricardo de Moura. **Análise das Vulnerabilidades e Ataques Existentes em Redes sem Fio.** Trabalho de Conclusão de Curso - Curso de Sistemas de Informação, Faculdades de Ciências Aplicadas de Minas, Uberlândia, Minas Gerais, 2005.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 2003.

THE INTERNET ENGINEERING TASK FORCE: **RFC 2196, Site Security Handbook.** Disponível em: <http://tools.ietf.org/html/rfc2196>. Acesso em: 23 out 2010.

WIRELESS VULNERABILITIES & EXPLOITS – WVE.**Wireless Vulnerabilities**. Disponível em: < http://www.wve.org/entries/vulnerabilities>. Acesso em 03 jun de 2011.

APÊNDICE A – INSTALAÇÃO E CONFIGURAÇÃO DO KISMET NO UBUNTU

Este apêndice aborda como foi feita a instalação e configuração do Kismet no ambiente utilizado neste trabalho.

Depois de baixar o pacote para Ubuntu no site do Kismet, entre na pasta em que ele foi baixado (cd PASTA) e instale-o com o seguinte comando (o nome do arquivo pode variar de acordo com a versão baixada):

sudo dpkg –i kismet-2011.03.2.i386.deb

Após isso, edite o arquivo de configuração do Kismet (normalmente fica em /usr/etc/kismet.conf). No ambiente utilizado nesta pesquisa, foram alterados os seguintes parâmetros:

a) ‘allowplugins=false’: para desativar a execução de plugins adicionais (foi desabilitado, pois na versão utilizada gerou instabilidades;
b) ‘ncsource=wlan0’: nome da interface *wireless* que será utilizada no Kismet;
c) ‘gps=false’: para desativar os avisos de falta de gps;
d) ‘apspoof=Lucas:ssid=”LucasC”,validmacs=00:4F:62:02:70:48’: para criar uma regra de APSPOOF na rede ‘LucasC’;

APÊNDICE B – ARTIGO

Estudos de Caso de Segurança em Redes Sem Fio Utilizando Ferramentas para Monitoramento e Detecção de Ataques

Lucas da Silva Carlessi[1], Paulo João Martins[2]

[1]Acadêmico do Curso de Ciência da Computação – Departamento de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC - Brazil

[2] Professor do Curso de Ciência da Computação – Departamento de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC - Brazil

lucascarlessi@gmail.com, pjm@unesc.net

Abstract*. Wireless networks are everywhere and, constantly, are targets of attacks. To provide proactive actions to the managers of these networks, some tools that monitor and detect attacks have been developed. These tools can be effective if they are used properly, offering competent management of safety features and warnings of possible attacks. This paper aims to present and discuss the concepts of wireless networks, methods of security, vulnerabilities and some attacks. Based on these concepts, methods are tested for efficiency in monitoring and attack detection using open source tools for Linux, Kismet and Beholder.*

Resumo. *As redes sem fio estão por toda a parte e, constantemente, são alvos de ataques. Para prover ações pró-ativas dos administradores dessas redes, algumas ferramentas que monitoram e detectam ataques foram desenvolvidas. Estas ferramentas podem ser eficientes se utilizadas adequadamente, proporcionando um gerenciamento competente dos recursos de segurança e alertas de possíveis ataques. Este artigo apresenta e discute os conceitos de redes sem fio, os métodos de segurança, as vulnerabilidades e alguns ataques existentes. A partir destes conceitos, é testada a eficiência no monitoramento e detecção de ataques utilizando as ferramentas de código aberto para Linux, Kismet e Beholder.*

1. Introdução

Redes sem fio são redes de computadores que permitem interligar, ao menos, dois equipamentos utilizando-se de ondas eletromagnéticas, sem a necessidade de uma estrutura física de cabeamento. Elas estão, cada vez mais, presentes no mundo devido à necessidade constante de conexão a rede dos vários equipamentos móveis (como notebooks e Personal Digital Assistants - PDA's) existentes no mercado [SGUAREZI 2007].

Atendem tanto o cenário doméstico quanto empresarial devido ao baixo custo e facilidade de instalação sem precisar modificar as instalações já existentes. Além de poder interligar redes privadas, é crescente o número de estabelecimentos como aeroportos e universidades que também disponibilizam o acesso sem fio para seus usuários [TANENBAUM 2003].

Com sua popularização, as redes sem fio se tornaram uma importante alternativa às redes cabeadas, devido à possibilidade e facilidade de suprir a falta de infraestrutura nas empresas e residências. Assim, a questão de segurança deve ser tratada com muito mais importância dado o valor que as informações têm para os proprietários da rede [SILVA; SOUZA 2003].

O Padrão IEEE 802.11 é o responsável, além da criação de padrões, por agregar mecanismos de segurança das redes do conjunto 802. Porém estes mecanismos, unidos aos

mecanismos de segurança também criados pelos fabricantes, não são suficientes para se criar redes seguras. Pois, à medida que os sistemas evoluem, as vulnerabilidades também aumentam, fazendo com que métodos atuais se tornem ineficazes contra novas ameaças [SILVA; SOUZA 2003].

Para poder controlar o uso da rede e avaliar se os aspectos de segurança tratados atualmente são eficientes, é imprescindível que o administrador da rede monitore-a constantemente, com o auxílio de ferramentas específicas que ajudam na detecção de ataques, permitindo que sejam tomadas medidas pró-ativas para minimizar as falhas de segurança atuais.

A vantagem principal do monitoramento é a possibilidade de detecção de falhas, não somente na segurança, mas em todos os aspectos que envolvam a rede, pois permite que seus administradores tenham um controle mais apurado em todos os pontos monitorados.

2. Redes Sem Fio

Utilizam um meio totalmente diferente de redes convencionais, o ar. Devido a isso, é preciso utilizar-se de tecnologias específicas para garantir uma conexão eficiente entre os equipamentos da rede. Essas tecnologias devem compensar a impossibilidade de proteção física do meio utilizado nas redes wireless, fazendo com que estas obtenham um bom desempenho e estabilidade mesmo em ambientes poluídos [RUFINO, 2005].

Na Tabela 1 estão descritos as principais técnicas de modulação utilizadas em redes sem fio.

Tabela 1. Técnicas de modulação utilizadas em redes sem fio

Técnica de Modulação	Velocidade
DSSS	até 11 Mbps
OFDM	até 54 Mbps

Além das técnicas de modulação, existem especificações para permitir que os equipamentos das mais variadas marcas tenham interoperabilidade entre si. Estes padrões técnicos para redes sem fio foram criados pelo *Institute of Electrical and Electronics Engineers* (IEEE) e são conhecidos pela terminologia IEEE 802 [ALVES 2009]. Estão representados na Tabela 2.

Tabela 2. Características dos principais padrões da família 802.11

Padrão	Frequência	Área de Cobertura (em média)	Velocidade Máxima	Velocidade Típica
802.11b	2.4 GHz	30 metros (indoor) 100 metros (outdoor)	11 Mbps	4 Mbps
802.11a	5 GHz	35 metros (indoor) 110 metros (outdoor)	54 Mbps	23 Mbps
802.11g	2.4 GHz	35 metros (indoor) 110 metros (outdoor)	54 Mbps	20 Mbps
802.11n	2.4 GHz ou 5 GHz	70 metros (indoor) 160 metros (outdoor)	300 Mbps	120 Mbps

3. Segurança em Redes Sem Fio

Redes sem fio são mais suscetíveis a ataques do que redes cabeadas pelo fato de que os dados trafegam pelo ar, isso proporciona certa facilidade aos atacantes se a rede não tiver os mecanismos necessários para proteger as informações que ali trafegam. Os ataques que atingem essas redes normalmente são os mesmos utilizados em redes guiadas, alguns apenas tiveram modificações para alcançar melhores resultados nas redes sem fio [SGUAREZI, 2007].

3.1. Vulnerabilidades

A família de protocolos 802.11x apresenta muitas vulnerabilidades e apresentará muitas outras ainda não descobertas. Baseando-se nisso cada vez mais atacantes direcionam seus ataques às redes sem fio que podem estar comprometidas sem o conhecimento de seus donos. O fato de que essas redes podem ser atacadas até mesmo de locais distantes, dificulta muito o reconhecimento dos responsáveis e motiva os atacantes [FRANCISCATTI, 2005].

Segundo Rufino (2005) as principais vulnerabilidades são:

a) física: nessas redes é possível estabelecer conexão mesmo de lugares remotos, portanto é importante analisar a potência e o padrão utilizado nos equipamentos para que o sinal tenha alcance somente aos domínios da empresa;

b) no envio e recepção do sinal: é importante definir o local correto dos componentes de uma rede sem fio, pois normalmente o concentrador envia sinal para todos os lados. Por isso, deve-se posicionar o AP mais ao centro possível do ambiente.

3.2 Métodos de Ataque

Existem vários ataques que podem ser aplicados em redes sem fio. Os principais estão descritos na Tabela 3.

Tabela 3. Principais métodos de ataque em redes sem fio

Ataque	Descrição
AP Spoofing	O invasor simula um AP real, fazendo com que os usuários que se conectam a ele fiquem vulneráveis a outros tipos de ataques, já que os dados que ali trafegarem poderão ser capturados.
ARP Poisoning	Redireciona o tráfego das vítimas para o atacante por meio da falsificação de endereços MAC.
MAC Spoofing	O atacante descobre um endereço físico válido na rede e o utiliza para se conectar a ela.
Denial of Service	O atacante faz com que o AP negue serviço aos usuários. Utiliza principalmente métodos de associação, autenticação, ou dissociação em massa para realizar o ataque.

3.3 Métodos de Defesa

Segundo Rufino (2005) é preciso implementar medidas para garantir a segurança em redes sem fio:

a) autenticação em AP's: utilizar métodos de autenticação seguros no concentrador da rede;

b) criptografia: utilizar protocolos de criptografia como o WPA ou WPA2 para garantir a codificação dos dados que trafegam pela rede para protegê-los de atacantes;

c) RADIUS: servidor que realiza autenticação de usuários por meio de chaves criptográficas;

d) VPN: criar um túnel protegido por criptografia, fazendo com que todas as informações transmitidas entre as estações e o AP estejam protegidas;

e) Firewalls: para criar uma política de segurança que obedeçam a regras pré-determinadas pelo administrador em prol da segurança da rede.

4. Monitoramento e Detecção de Ataques

Segundo Rufino (2005) o monitoramento é um dos mais importantes recursos de segurança que uma rede deve ter, independente do meio de transmissão. Utilizando-se deste método, é possível detectar possíveis falhas de segurança que, se não detectadas e corrigidas, podem deixar o ambiente vulnerável a diversos ataques.

Franciscatti (2005) descreve que o monitoramento pode coletar diversos dados importantes para o administrador de redes sem fio:

a) instalação de Access Point's não autorizados;

b) equipamentos que não estejam utilizando protocolos de segurança;

c) ataques contra clientes da rede;

d) acessos não autorizados;

e) mudanças de endereços MAC;

f) mudanças de canal;

g) algum serviço em D.o.S.

Segundo Sguarezi (2007), existem dois métodos para monitorar redes sem fio: passivo e ativo.

O método passivo é o tipo que coleta informações dos equipamentos da rede sem precisar interagir com eles. Já o modo ativo é o que transmite perguntas (queries) aos ativos da rede para que seja possível a obtenção dos dados desejados.

4.1 Exemplos de Ferramentas para Monitoramento em Redes Sem Fio

Algumas ferramentas para monitoramento e detecção de ataques em redes sem fio foram desenvolvidas. Aqui serão descritas algumas delas para permitir um posterior estudo de sua utilização:

a) Kismet: detector de redes, coletor de tráfego e um sistema de detecção de intrusão para uso em redes *wireless*. Funciona com a maioria das placas de rede sem fio;

b) AirTraf: ferramenta é especializada em monitoramento e gerenciamento de redes sem fio;

c) NetStumbler: uma das ferramentas de varredura de redes sem fio mais conhecida para o Windows;

d) Beholder: ferramenta desenvolvida por brasileiros que monitora e detecta ataques em redes sem fio.

5. Monitorando e Detectando Ataques em Redes Sem Fio

Para testar a eficiência e demonstrar a correta utilização das ferramentas descritas nesta pesquisa, devem-se levar em consideração todos os aspectos que foram estudados relativos à segurança em redes wireless. Com isso, é possível definir quais ataques serão empregados e como detectá-los nos cenários criados.

Os ataques serão realizados por meio da suíte de ferramentas para ataques em redes sem fio Aircrack-ng, que oferece recursos de quebras de chave WEP e WPA, AP spoofing, D.o.S, entre outros.

O monitoramento dos ataques específicos para redes wireless será feito pela ferramenta Kismet – que é a mais completa e atualizada das ferramentas estudadas – e pela ferramenta Beholder – um simples detector de intrusão para redes wireless.

5.1 Metodologia

Inicialmente, foram estudados os principais padrões de redes sem fio concretizados pelo IEEE e descritas suas principais vulnerabilidades e meios para garantir sua segurança. Alguns dos problemas na segurança podem ser resolvidos apenas com configurações feitas no AP ou até mesmo em seu reposicionamento físico. Porém, existem vulnerabilidades que podem ser exploradas mesmo quando os métodos corretos de segurança são aplicados.

Para monitorar e detectar possíveis ataques em redes sem fio, algumas ferramentas de monitoramento e detecção de ataques nessas redes foram testadas. A partir dos testes realizados, constatou-se que a maioria delas está desatualizada ou funciona em apenas alguns modelos de placas wireless. Isso influenciou e restringiu a escolha final das ferramentas, pois a maioria não funcionou como o esperado ou não suporta as placas comercialmente mais atuais.

Para completar o ambiente, também foi necessário o estudo de ferramentas para ataques em WLAN's. Com isso, será possível simular uma pequena rede, onde é possível identificar o concentrador da rede, monitor, atacante e clientes.

5.1.1. Ferramentas Testadas

Durante a pesquisa, várias ferramentas foram estudadas para alcançar o objetivo de realizar testes com pelo menos duas ferramentas. Como citado anteriormente, a maioria delas estão descontinuadas e suas versões são antigas, outras suportam somente placas e *drivers* que eram utilizados na época em que foram criadas. Estão listadas na Tabela 4

Tabela 4. Ferramentas que não funcionaram

Ferramenta	Problema encontrado	Data	Última versão
AirIDS	Só suporta placas antigas / Sem link para download	-	-
AirTraf	Só suporta placas antigas	2003	1.1
Garuda	Erro ao compilar ferramenta	2004	0.2.1
wIDS	Site retirado da Internet / Sem link para download	-	-
Widz	Erro de *driver* não suportado ao executar	2003	1.5
snort-wireless	Site retirado da Internet / Sem link para download	-	2.0.1

5.1.2. Ambiente de Testes

Procurou-se usar nessa pesquisa ferramentas atualizadas, gratuitas e disponibilizadas na Internet, a fim de permitir o máximo de compatibilidade nos mais variados ambientes.

As ferramentas para monitoramento e detecção de ataques que serão utilizadas: Kismet 2011-03-R2 e Beholder 0.8.9 Beta.

Para os ataques serão utilizadas ferramentas do pacote Aircrack-ng:

A distribuição Linux para o monitoramento será o Ubuntu 10.10, já para realizar os ataques será o Linux BackTrack 5.

Na Figura 1 pode-se ver como ficou o ambiente de testes.

Figura 1. Configuração do ambiente de testes

5.1.3. Ataques Testados

Serão exploradas seis vulnerabilidades reportadas pelo grupo Wireless Vulnerabilites & Exploits (2005 a 2008). Que serão tratadas de acordo com suas assinaturas:

a) APSPOOF: detecta AP's que estão usando o mesmo SSID que o de sua rede, podendo fazer com que clientes se conectem pensando que é uma rede legítima. Este ataque pode permitir ao atacante capturar dados de quem esteja conectado a ele;

b) BCASTDISCON: este alerta ocorre quando o atacante forja pacotes de desassociação ou desautenticação e envia para toda a rede, fazendo com o que os clientes se desconectem. Isto caracteriza um ataque de negativa de serviço, já que os clientes legítimos ficam privados de acessar a rede.

c) BSSTIMESTAMP: AP's enviam regularmente seus beacons para orientar os clientes da rede. Nos *beacons* existe uma informação de sincronização de tempo. Quando estas informações são inválidas ou são recebidas fora de ordem, indica um

possível ataque contra o AP legítimo que pode dificultar a comunicação com os clientes;

d) CHANCHANGE: indica que o AP está mudando de canal, isso pode ocorrer por ataques de AP *spoofing* ou por invasão no concentrador;

e) CRYPTODROP: indica que o AP parou de utilizar criptografia. Pode ser causado por ataques de *spoofing* contra o concentrador ou por invasão no mesmo;

f) KARMA: assinatura que caracteriza falsos concentradores que respondem por qualquer rede. Por exemplo, se um cliente procura por uma rede chamada 'Teste123', o falso AP responde como se fosse 'Teste123' (mesmo que ele já tenha respondido com outros SSID's para outros clientes).

5.2. Estudo de Caso 1: Monitorando e Detectando Ataques com o Kismet

Esta ferramenta é robusta e tem atualizações constantes. É desenvolvida para Linux e OSX, mas pode ser instalado no Windows com suporte limitado de placas e recursos. Até a presente data da escrita desta seção, somente uma versão mais antiga (2009-06-R1) está disponível para Windows.

Na Figura 2 pode-se ver sua tela inicial.

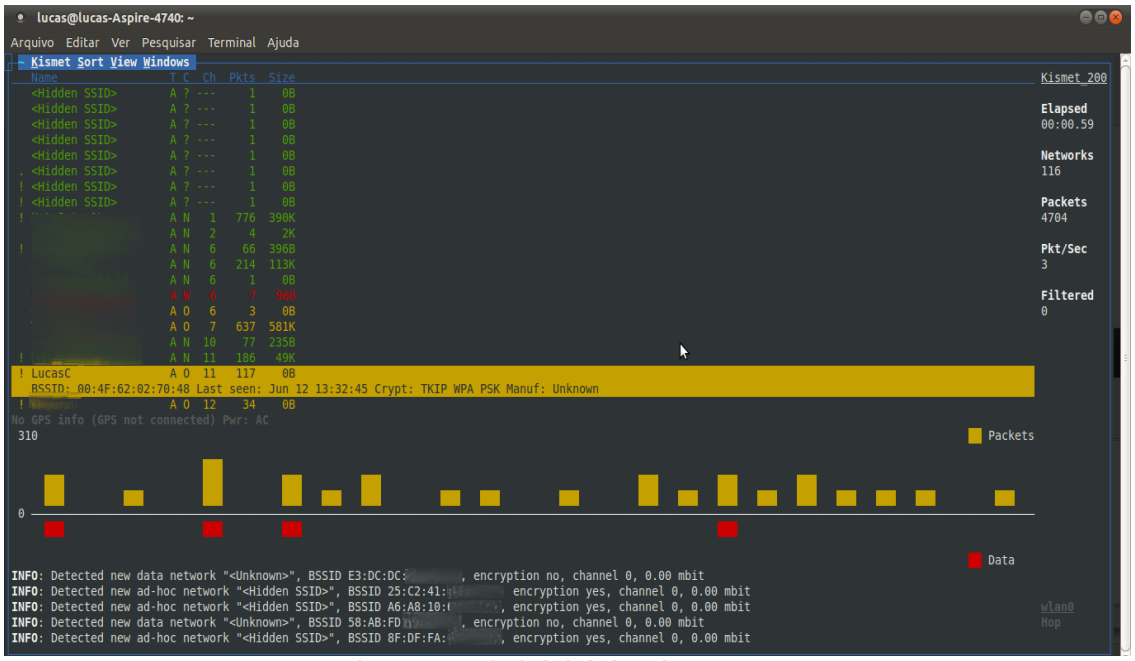

Figura 2. Tela inicial do Kismet

Todas as vulnerabilidades citadas na seção anterior foram testadas e a ferramenta foi capaz de detectar todos os ataques. Na Figura 3 é possível identificar a detecção de BCASTDISCON pelo Kismet.

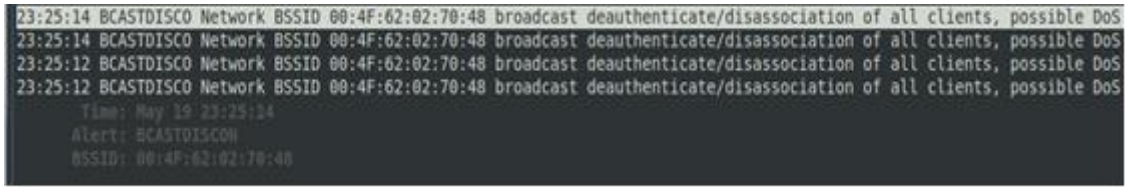

Figura 3. Detecção de BCASTDISCON no Kismet

Todos os outros ataques geraram os alertas com suas respectivas assinaturas.

5.3. Estudo de Caso 2: Monitorando e Detectando Ataques com o Beholder

O Beholder é mais simples que o Kismet, porém garante uma boa funcionalidade na detecção de ataques a redes sem fio e também monitoramento. Ele não tem de uma interface para gerenciamento, dispondo apenas de mensagens no terminal do Linux que mostram os avisos relacionados às redes.

Inicialmente, ele lista todas as redes encontradas, com seus respectivos MAC's, SSID's, canais e forças de sinal. Como se pode ver na Figura 4.

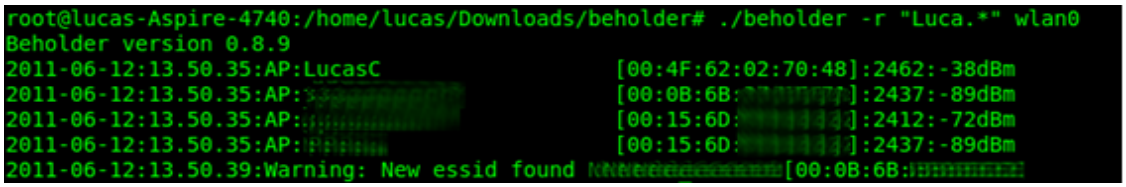

Figura 4. Tela inicial do Beholder

Todos os ataques citados anteriormente também foram testados nesta ferramenta. Pode-se ver na Figura 5 a detecção de Karma.

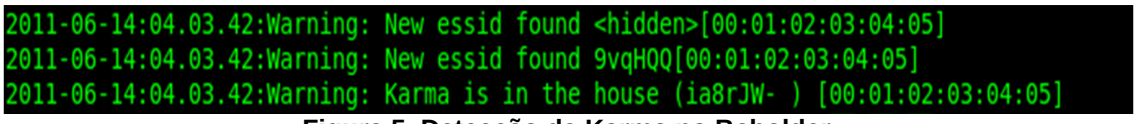

Figura 5. Detecção de Karma no Beholder

Dos ataques testados, um deles não foi detectado pela ferramenta (BCASTDISCON), e outro foi reconhecido sem identificar sua assinatura (BSTIMESTAMP).

5.4 Resultados Obtidos

Todos os testes foram realizados pelo menos cinco vezes cada para garantir que em todas as tentativas seria detectada a assinatura correta.

Ambas as ferramentas apresentaram resultados satisfatórios nos testes aplicados nesta pesquisa. A Tabela 5 demonstra os ataques e o resultado da detecção de cada um.

Tabela 4. Ataques testados no Kismet e Beholder

Ataque	Kismet	Beholder
APSPOOF	Detectado	Detectado
BCASTDISCON	Detectado	Não Detectado
BSSTIMESTAMP	Detectado	Detectado com outra assinatura
CHANCHANGE	Detectado	Detectado
CRYPTODROP	Detectado	Detectado
KARMA	Detectado	Detectado

As duas ferramentas pecaram no tratamento das informações coletadas, pois permitem somente que sejam gravados arquivos de log sem nenhum tipo de filtro por assinatura ou por rede. Enquanto essa funcionalidade não é agregada nas ferramentas, existem programas analisadores de log que auxiliam o administrador da rede nesta deficiência, como o Swatch e Logwatch para Linux.

Em uma visão geral, tanto o Kismet quanto o Beholder, podem auxiliar o administrador no gerenciamento de suas redes, pois dão várias informações que ferramentas

de monitoramento comuns não dão. Auxiliam também na segurança da rede como um todo, pois permitem detectar vários tipos de ataques em redes wireless.

6. Conclusão

Este trabalho tratou vários aspectos da segurança de redes sem fio, destacando sua importância para garantir as melhores formas de protegê-las contra ataques e vulnerabilidades. Esta tarefa é ainda mais complicada em redes wireless pelo fato de que os dados ficam mais expostos devido ao meio utilizado nas transmissões.

Existem vários métodos que diminuem os riscos a ataques nessas redes, porém também existem vulnerabilidades que podem ser exploradas mesmo com a utilização das medidas de segurança corretas. É aí que se vê a necessidade de um constante monitoramento que permita identificar dados importantes das redes e que possam detectar tentativas de ataques.

As ferramentas Kismet e Beholder foram utilizadas neste trabalho, e mostraram que é de extrema importância o monitoramento e a detecção de ataques constantes em redes sem fio. A partir destas ferramentas foi possível verificar possíveis vulnerabilidades e detectar com eficiência todos os ataques testados.

A maior dificuldade encontrada foi a falta de ferramentas com licença de uso livre e atualizadas para esta finalidade. Pelo menos seis ferramentas testadas não funcionaram adequadamente. A maioria delas teve a última atualização há longo tempo e só funcionavam em placas de modelos muito antigos e restritos que tipicamente não são mais comercializadas.

Com este trabalho, foi possível aprimorar um conhecimento científico na área de segurança em redes, especialmente nos detalhes técnicos que são exclusivos a redes sem fio. Também foi possível analisar o funcionamento dos ataques e quais os riscos que uma rede wireless sob ataque pode oferecer para todos os outros pontos da rede. Outro resultado foi a documentação de vários ataques e como as ferramentas para monitoramento e detecção de ataques se comportam em vários tipos de ataques.

Referências

ALVES, Walter F. Andrade. **Segurança em Redes Sem Fio: O caso da Assembléia Nacional de Cabo Verde.** Trabalho de Conclusão de Curso – Curso de Engenharia de Sistemas e Informática, Universidade Jean Piaget de Cabo Verde, 2009.

FRANCISCATTI, Vagner. **Segurança em Redes Sem Fio**. Trabalho de Conclusão de Curso – Curso de Especialização em Redes de Computadores e Comunicação de Dados, Universidade Estadual de Londrina, Londrina, Paraná, 2005.

IEEE. IEEE 802.11: **LAN/MAN Wireless LANS**. Disponível em: <http://standards.ieee.org/getieee802/802.11.html>. Acesso em 07 maio 2009.

KISMET WIRELESS. **Kismet**. Disponível em: <http://www.kismetwireless.net>. Acesso em 07 nov. de 2010.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes Sem Fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. São Paulo: Novatec, 2005.

SGUAREZI, João V. Dos Reis. **Ferramentas de Segurança em Redes sem Fio**. Trabalho de Conclusão de Curso – Curso de Ciência da Computação, Universidade Federal de Mato Grosso, Cuiabá, Mato Grosso, 2007.

SILVA, G. M.; SOUZA, J. N. **Uma análise dos mecanismos de segurança de redes locais sem fio e uma proposta de melhoria**. III Workshop de Segurança de Sistemas Computacionais, Workshop de segurança – WSEG. In: Anais do SBRC 2003, Natal, 2003

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 2003.

WVE.**Wireless Vulnerabilities**. Disponível em: < http://www.wve.org/entries/vulnerabilities>. Acesso em 03 jun de 2011.

ANEXO A – ARQUIVO DE CONFIGURAÇÃO DO KISMET

```
# Kismet config file
# Most of the "static" configs have been moved to here -- the command line
# config was getting way too crowded and cryptic.  We want functionality,
# not continually reading --help!

# Version of Kismet config
version=2009-newcore

# Name of server (Purely for organizational purposes)
servername=Kismet_2009

# Prefix of where we log (as used in the logtemplate later)
logprefix=/var/log/kismet/

# Do we process the contents of data frames?  If this is enabled, data
# frames will be truncated to the headers only immediately after frame type
# detection.  This will disable IP detection, etc, however it is likely
# safer (and definitely more polite) if monitoring networks you do not own.
# hidedata=true

# Do we allow plugins to be used?  This will load plugins from the system
# and user plugin directiories when set to true (See the README for the default
# plugin locations).
allowplugins=false

# See the README for full information on the new source format
# ncsource=interface:options
# for example:
# ncsource=wlan0
# ncsource=wifi0:type=madwifi
# ncsource=wlan0:name=intel,hop=false,channel=11
ncsource=wlan0
# Comma-separated list of sources to enable.  This is only needed if you defined
# multiple sources and only want to enable some of them.  By default, all defined
# sources are enabled.
# For example, if sources with name=prismsource and name=ciscosource are defined,
# and you only want to enable those two:
# enablesources=prismsource,ciscosource

# Control which channels we like to spend more time on.  By default, the list
# of channels is pulled from the driver automatically.  By setting preferred channels,
# if they are present in the channel list, they'll be set with a timing delay so that
# more time is spent on them.  Since 1, 6, 11 are the common default channels, it makes
# sense to spend more time monitoring them.
# For finer control, see further down in the config for the channellist= directives.
preferredchannels=1,6,11
```

```
# How many channels per second do we hop?  (1-10)
channelvelocity=3

# By setting the dwell time for channel hopping we override the channelvelocity
# setting above and dwell on each channel for the given number of seconds.
#channeldwell=10

# Channels are defined as:
# channellist=name:ch1,ch2,ch3
# or
# channellist=name:range-start-end-width-offset,ch,range,ch,...
#
# Channels may be a numeric channel or a frequency
#
# Channels may specify an additional wait period.  For common default channels,
# an additional wait period can be useful.  Wait periods delay for that number
# of times per second - so a configuration hopping 10 times per second with a
# channel of 6:3 would delay 3/10ths of a second on channel 6.
#
# Channel lists may have up to 256 channels and ranges (combined).  For power
# users scanning more than 256 channels with a single card, ranges must be used.
#
# Ranges are meant for "power users" who wish to define a very large number of
# channels.  A range may specify channels or frequencies, and will automatically
# sort themselves to cover channels in a non-overlapping fashion.  An example
# range for the normal 802.11b/g spectrum would be:
#
# range-1-11-3-1
#
# which indicates starting at 1, ending at 11, a channel width of 3 channels,
# incrementing by one.  A frequency based definition would be:
#
# range-2412-2462-22-5
#
# since 11g channels are 22 mhz wide and 5 mhz apart.
#
# Ranges have the flaw that they cannot be shared between sources in a non-overlapping
# way, so multiple sources using the same range may hop in lockstep with each other
# and duplicate the coverage.
#
# channellist=demo:1:3,6:3,11:3,range-5000-6000-20-10

# Default channel lists
# These channel lists MUST BE PRESENT for Kismet to work properly.  While it is
# possible to change these, it is not recommended.  These are used when the supported
# channel list can not be found for the source; to force using these instead of
# the detected supported channels, override with channellist= in the source defintion
#
# IN GENERAL, if you think you want to modify these, what you REALLY want to do is
# copy them and use channellist= in the packet source.
```

```
channellist=IEEE80211b:1:3,6:3,11:3,2,7,3,8,4,9,5,10
channellist=IEEE80211a:36,40,44,48,52,56,60,64,149,153,157,161,165
channellist=IEEE80211ab:1:3,6:3,11:3,2,7,3,8,4,9,5,10,36,40,44,48,52,56,60,64,149,153,157,
161,165

# Client/server listen config
listen=tcp://127.0.0.1:2501
# People allowed to connect, comma seperated IP addresses or network/mask
# blocks.  Netmasks can be expressed as dotted quad (/255.255.255.0) or as
# numbers (/24)
allowedhosts=127.0.0.1
# Maximum number of concurrent GUI's
maxclients=5
# Maximum backlog before we start throwing out or killing clients.  The
# bigger this number, the more memory and the more power it will use.
maxbacklog=5000

# Server + Drone config options.  To have a Kismet server export live packets
# as if it were a drone, uncomment these.
# dronelisten=tcp://127.0.0.1:3501
# droneallowedhosts=127.0.0.1
# dronemaxclients=5
# droneringlen=65535

# OUI file, expected format 00:11:22<tab>manufname
# IEEE OUI file used to look up manufacturer info.  We default to the
# wireshark one since most people have that.
ouifile=/etc/manuf
ouifile=/usr/share/wireshark/wireshark/manuf
ouifile=/usr/share/wireshark/manuf

# Do we have a GPS?
gps=false
# Do we use a locally serial attached GPS, or use a gpsd server?
# (Pick only one)
gpstype=gpsd
# gpstype=serial
# What serial device do we look for the GPS on?
gpsdevice=/dev/rfcomm0
# Host:port that GPSD is running on.  This can be localhost OR remote!
gpshost=localhost:2947
# Do we lock the mode?  This overrides coordinates of lock "0", which will
# generate some bad information until you get a GPS lock, but it will
# fix problems with GPS units with broken NMEA that report lock 0
gpsmodelock=false
# Do we try to reconnect if we lose our link to the GPS, or do we just
# let it die and be disabled?
gpsreconnect=true

# Do we export packets over tun/tap virtual interfaces?
```

```
tuntap_export=false
# What virtual interface do we use
tuntap_device=kistap0

# Packet filtering options:
# filter_tracker - Packets filtered from the tracker are not processed or
#                  recorded in any way.
# filter_export  - Controls what packets influence the exported CSV, network,
#                  xml, gps, etc files.
# All filtering options take arguments containing the type of address and
# addresses to be filtered.  Valid address types are 'ANY', 'BSSID',
# 'SOURCE', and 'DEST'.  Filtering can be inverted by the use of '!' before
# the address.  For example,
# filter_tracker=ANY(!"00:00:DE:AD:BE:EF")
# has the same effect as the previous mac_filter config file option.
# filter_tracker=...
# filter_dump=...
# filter_export=...
# filter_netclient=...

# Alerts to be reported and the throttling rates.
# alert=name,throttle/unit,burst
# The throttle/unit describes the number of alerts of this type that are
# sent per time unit.  Valid time units are second, minute, hour, and day.
# Burst describes the number of alerts sent before throttling takes place.
# For example:
# alert=FOO,10/min,5
# Would allow 5 alerts through before throttling is enabled, and will then
# limit the number of alerts to 10 per minute.
# A throttle rate of 0 disables throttling of the alert.
# See the README for a list of alert types.
alert=ADHOCCONFLICT,5/min,1/sec
alert=AIRJACKSSID,5/min,1/sec
alert=APSPOOF,10/min,1/sec
alert=BCASTDISCON,5/min,2/sec
alert=BSSTIMESTAMP,5/min,1/sec
alert=CHANCHANGE,5/min,1/sec
alert=CRYPTODROP,5/min,1/sec
alert=DISASSOCTRAFFIC,10/min,1/sec
alert=DEAUTHFLOOD,5/min,2/sec
alert=DEAUTHCODEINVALID,5/min,1/sec
alert=DISCONCODEINVALID,5/min,1/sec
alert=DHCPNAMECHANGE,5/min,1/sec
alert=DHCPOSCHANGE,5/min,1/sec
alert=DHCPCLIENTID,5/min,1/sec
alert=DHCPCONFLICT,10/min,1/sec
alert=NETSTUMBLER,5/min,1/sec
alert=LUCENTTEST,5/min,1/sec
alert=LONGSSID,5/min,1/sec
alert=MSFBCOMSSID,5/min,1/sec
```

```
alert=MSFDLINKRATE,5/min,1/sec
alert=MSFNETGEARBEACON,5/min,1/sec
alert=NULLPROBERESP,5/min,1/sec
#alert=PROBENOJOIN,5/min,1/sec

# Controls behavior of the APSPOOF alert.  SSID may be a literal match (ssid=) or
# a regex (ssidregex=) if PCRE was available when kismet was built.  The allowed
# MAC list must be comma-separated and enclosed in quotes if there are multiple
# MAC addresses allowed.  MAC address masks are allowed.
apspoof=Foo1:ssidregex="(?i:foobar)",validmacs=00:11:22:33:44:55
apspoof=Foo2:ssid="Foobar",validmacs="00:11:22:33:44:55,aa:bb:cc:dd:ee:ff"
apspoof=Lucas:ssid="LucasC",validmacs=00:4F:62:02:70:48

# Known WEP keys to decrypt, bssid,hexkey.  This is only for networks where
# the keys are already known, and it may impact throughput on slower hardware.
# Multiple wepkey lines may be used for multiple BSSIDs.
# wepkey=00:DE:AD:C0:DE:00,FEEDFACEDEADBEEF0102030405060708090

# Is transmission of the keys to the client allowed?  This may be a security
# risk for some.  If you disable this, you will not be able to query keys from
# a client.
allowkeytransmit=true

# How often (in seconds) do we write all our data files (0 to disable)
writeinterval=300

# Do we use sound?
# Not to be confused with GUI sound parameter, this controls wether or not the
# server itself will play sound.  Primarily for headless or automated systems.
enablesound=false
# Path to sound player
soundbin=play

sound=newnet,true
sound=newcryptnet,true
sound=packet,true
sound=gpslock,true
sound=gpslost,true
sound=alert,true

# Does the server have speech? (Again, not to be confused with the GUI's speech)
enablespeech=false
# Binary used for speech (if not in path, full path must be specified)
speechbin=flite
# Specify raw or festival; Flite (and anything else that doesn't need formatting
# around the string to speak) is 'raw', festival requires the string be wrapped in
# SayText("...")
speechtype=raw

# How do we speak?  Valid options:
```

```
# speech    Normal speech
# nato      NATO spellings (alpha, bravo, charlie)
# spell     Spell the letters out (aye, bee, sea)
speechencoding=nato

speech=new,"New network detected s.s.i.d. %1 channel %2"
speech=alert,"Alert %1"
speech=gpslost,"G.P.S. signal lost"
speech=gpslock,"G.P.S. signal O.K."

# How many alerts do we backlog for new clients?  Only change this if you have
# a -very- low memory system and need those extra bytes, or if you have a high
# memory system and a huge number of alert conditions.
alertbacklog=50

# File types to log, comma seperated.  Built-in log file types:
# alert                     Text file of alerts
# gpsxml                    XML per-packet GPS log
# nettxt                    Networks in text format
# netxml                    Networks in XML format
# pcapdump                  tcpdump/wireshark compatible pcap log file
# string                    All strings seen (increases CPU load)
logtypes=pcapdump,gpsxml,netxml,nettxt,alert

# Format of the pcap dump (PPI or 80211)
pcapdumpformat=ppi
# pcapdumpformat=80211

# Default log title
logdefault=Kismet

# logtemplate - Filename logging template.
# This is, at first glance, really nasty and ugly, but you'll hardly ever
# have to touch it so don't complain too much.
#
# %p is replaced by the logging prefix + '/'
# %n is replaced by the logging instance name
# %d is replaced by the starting date as Mon-DD-YYYY
# %D is replaced by the current date as YYYYMMDD
# %t is replaced by the starting time as HH-MM-SS
# %i is replaced by the increment log in the case of multiple logs
# %l is replaced by the log type (pcapdump, strings, etc)
# %h is replaced by the home directory

logtemplate=%p%n-%D-%t-%i.%l

# Where state info, etc, is stored.  You shouldnt ever need to change this.
# This is a directory.
configdir=%h/.kismet/
```