UNVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE.

JEFERSON LUIZ MIRANDA FERREIRA

SEGURANÇA EM REDES SEM FIO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA - PR

2013

JEFERSON LUIZ MIRANDA FERREIRA

SEGURANÇA EM REDES SEM FIO

Monografia de Especialização apresentada ao Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede. "

Orientador: Prof. Christian Carlos Souza Mendes.

CURITIBA - PR

2013

RESUMO

FERREIRA, Jeferson Luiz Miranda **Segurança em Redes sem Fio.** 2013. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Está monografia apresenta o estudo sobre os principais tipos de implementações nas redes sem fio dos usuários domésticos. Analisar os protocolos de rede sem fio utilizados por estes usuários, fazer a comparação dos protocolos WEP, WPA e WPA2, será utilizado também um software baseado em Linux para mostrar as principais vulnerabilidades destas redes sem fio.

Palavras-Chave: Segurança, Rede sem Fio, WEP, WPA, WPA2, Software.

ABSTRACT

FERREIRA, Jeferson Luiz Miranda Security in Wireless Networks in 2013. Monograph (Specialization in Configuring and Managing Servers and Networking Equipment). Federal Technological University of Paraná. Curitiba, 2013.

This monograph presents the study on the main types of implementations in wireless networks of home users. Analyze wireless network protocols used for these users, making comparison of WEP, WPA and WPA2, will also use a Linux-based software to show the main vulnerabilities of these wireless networks.

Keywords: Security, Wireless Network, WEP, WPA, WPA2, Software.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AP	Access Point
AES	Advanced Encryption Standard
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
EAP	Extensible Authentication Protocol
GTK	Group Temporal Key
ICV	Integrity Check Value
IEEE	Institute of Electrical and Eletronics Engineers
IP	Internet Protocol
ISO	International Standards Organization
LLC	Logical Link Control
MAC	Media Access Control
MIC	Message Integrity Check
OSI	Open Systems Interconnection
OUI	Organizationally Unique Identifier
PSK	Pre Shared Key
STA	Wireless LAN Stations
SSID	Service Set Identifier
PTK	Pairwise Transient Key
TKIP	Temporal Key Integrity Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol over Internet Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

WPAN	Wireless Personal Area Network
WI-FI	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access2
WIMAX	Worldwide Interoperability for Microwave Access
WWW	World Wide Web

SUMÁRIO

1. INTRODUÇÃO

As comunicações sem fio são utilizadas em larga escala e estão cada vez mais presentes no nosso dia a dia. Essas comunicações sem fio vêm para satisfazer diversas necessidades e desejos, tais como: conforto, comodidade, flexibilidade. Existem diversos aparelhos que usam a comunicação sem fio, Ex.: no controle remoto da televisão, do aparelho de som, do portão eletrônico, em celulares, notebooks, bem como para resolver diversos problemas que ao longo do tempo foram surgindo.

Hoje em dia a maioria das pessoas tem em casa uma rede sem fio, antigamente isto era só para pessoas com maior poder aquisitivo, mais estas pessoas não tem tanto conhecimento técnico sobre as redes sem fio e acabam não configurando corretamente os seus dispositivos.

O recomendado para estas pessoas é sempre buscar ajuda técnica, isto ajudará a prevenir ameaças futuras, como por exemplo, a invasão de sua rede sem fio.

1.1 OBJETIVOS

1.2 OBJETIVO GERAL

Realizar um estudo através de uma revisão bibliográfica e realizar uma pesquisa a campo para identificar as principais falhas nas redes sem fio dos usuários domésticos.

1.3 OBJETIVOS ESPECÍFICOS

Realizar uma pesquisa de campo, estudar a forma que os usuários domésticos estão configurando os Pontos de Acesso das Redes sem Fio.

Analisar a segurança que está sendo utilizada nas redes domésticas, permitindo verificar as falhas de segurança.

Realizar uma auditoria nas implementações com o intuito de coletar informações sobre o nível de segurança destas redes sem fio, utilizando um software baseado em Linux.

1.4 JUSTIFICATIVA

A evolução da tecnologia colaborou para o surgimento das redes de computadores, com novos sistemas que integram mais as áreas empresarias.

No passado as empresas e os usuários domésticos dependiam muito de um cabo de rede para poder se conectar e conseguir navegar, hoje em dia com o surgimento das redes sem fio, ficou muito mais fácil de conectar e navegar, o usuário só depende de uma placa de rede sem fio em seu computador e uma rede livre para se conectar, como existem em vários aeroportos e shopping, entre outros.

Portanto, as redes sem fio devem ser seguras e confiáveis, tendo que ser implementadas com um nível de segurança alto, assim deixando de ser um alvo fácil para pessoas mal intencionadas.

1.5 METODOLOGIA

Este projeto fundamenta-se em pesquisa bibliográfica, com pesquisas qualitativa, quantitativa e exploratória para coleta e análise de dados coletados nas redes sem fio dos usuários domésticos.

Articular e confrontar as informações adquiridas ao longo do projeto com os conhecimentos teóricos da literatura pesquisada em livros, artigos científicos, revistas especializadas, documentos oficiais, sites da internet entre outros, que possibilitam uma interação entre o estudo e a análise do caso.

2. REFERÊNCIAS TEÓRICAS

2.1 REDES SEM FIO

As Redes sem fio ou wireless (WLANs, **Wireless Local Area Network**) surgiram da mesma forma que muitas outras tecnologias, no meio militar. Havia a necessidade de implementação de um método simples e seguro para troca de informações em ambiente de combate. O tempo passou e a tecnologia evoluiu, deixando de ser restrito ao meio militar e se tornou acessível a empresas, faculdades e ao usuário doméstico. Nos dias de hoje podemos pensar em redes wireless como uma alternativa bastante interessante em relação as redes cabeadas. Suas aplicações são muitas e variadas e o fato de ter a mobilidade como principal característica, tem facilitado a sua aceitação, principalmente nas empresas. (FARIAS, 2005).

WPAN (Wireless Personal Area Network) ou rede pessoal sem fio, é normalmente utilizada para interligar dispositivos eletrônicos fisicamente próximos. Este tipo de rede é ideal para eliminar os cabos usualmente utilizados para interligar teclados, impressoras, telefones móveis, agendas eletrônicas, computadores de mão, câmeras fotográficas digitais, mouses e outros. Nos equipamentos mais recentes é utilizado o padrão Bluetooth para estabelecer esta comunicação, mas também é empregado raio infravermelho (semelhante ao utilizado nos controles remotos de televisores). (BUSCH, 2008).

O uso desta tecnologia vai desde transceptores de rádio até satélites no espaço. Seu uso mais comum é em redes de computadores, servindo como meio de acesso a Internet, através de locais remotos como um aeroporto, um restaurante ou até mesmo em casa. (BUSCH, 2008).

Em um ambiente típico, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso AP (Access Point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roaming semelhante a um sistema de telefonia celular. (SILVEIRA, 2013)

2.2 SEGURANÇA DA INFORMAÇÃO

De acordo com a NBR ISO/IEC 17799 (2005) define a SI (Segurança da Informação) como: é a política de proteção existente sobre as informações de uma determinada organização de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades do negócio. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

De acordo com a norma citada, é necessário estabelecer critérios para a definição do nível de segurança que se pretende, com análise periódica, possibilitando avanços ou retrocessos no cenário de SI (Segurança da Informação) na organização.

Melhorar um sistema de segurança da informação não está baseado apenas em aplicar em um conjunto de computadores antivírus ou barreiras de proteção (firewalls) interligada na rede de computadores de uma organização. Para se obter um sistema de segurança da informação é necessário entender os princípios de segurança para que possa se gerir políticas e soluções cabíveis para atender as necessidades de cada organização.

É relevante entender os princípios de segurança da informação para assim conseguir implementá-los. No processo de implantação é necessário conseguir verificar ferramentas que auxiliem o usuário antes que alguma falha ocorra. Esse processo de prevenção pode ser classificado em duas grandes categorias indispensáveis: a prevenção e a proteção dos sistemas de informação.

De acordo com Silva (2003), os principais pontos para implantação da segurança da informação devem seguir os cinco princípios básicos:

1. A relação custo e benefício: garantir investimentos para a implementação e a manutenção favoráveis, e o retorno que proporciona a prevenção e a proteção do sistema de informação. Tal situação só é lembrada pelos proprietários quando um grande desastre ou ataque ocorre e o custo de restauração das informações das

bases de dados muitas vezes, é maior do que se tivesse investido meses em um sistema de segurança da informação seguro e estável.

2. O princípio da concentração: proporciona à possibilidade de se administrar as medidas necessárias de segurança da informação para atender necessidades de melhoramento de proteção de diferentes bases de dados sensíveis a alterações.

3. O princípio da proteção em profundidade: proporciona medidas de proteção de segurança (físicas ou lógicas) como câmeras de vigilância, biometria e reconhecimento de voz. A utilização deste princípio evita um conjunto de medidas de proteção distintas e avulsas para não se tornar uma soma ineficiente e lenta de obstáculos para um ambiente mais seguro.

4. O princípio da consistência: determina que as medidas de proteção do SI possuam um nível de sensibilidade intercambiável para que reduzam as falhas dos programas de segurança das organizações. Sua utilização atinge a todos os níveis acessos do sistema de informação tanto como físico ou lógico, por exemplo, impedir que um filho de um sócio da organização instale jogos, acesse páginas indevidas com o servidor da empresa ou permitir pessoas não autorizadas ter acesso aos computadores da organização.

5. O princípio da redundância: determina a importância de se adotar mais do que uma forma de proteção da SI. Caso ocorra a falha do processo A de segurança será executado o processo B para que o sistema de informação continue em pleno funcionamento, Ex.: possuir servidores de contingência em locais diferentes replicando as informações entre as filiais efetuando *backups* automáticos diariamente com sistemas de espelhamentos de *hard disk*.

Estes princípios são responsáveis pela segurança da informação que deverá ser articulada de forma que venha definir princípios para um ambiente mais seguro. Para uma implementação satisfatória, deve ser bastante aprofundada para se obter o conhecimento, implicações e interação com a equipe responsável de segurança da informação e gestores, resultando melhores resultados dos esforços necessários para um ambiente mais seguro.

Tanto a segurança da informação e a gestão de risco devem trabalhar em conjunto para que, desta forma, seja possível elaborar um plano de contingência de segurança com o intuito de solucionar problemas e prever riscos para melhoria continua da segurança da informação.

2.3 Wi-FI

Foi uma marca licenciada originalmente pela (Wi-Fi Alliance) para descrever a tecnologia de redes sem fio embarcadas (WLAN) baseadas no padrão IEEE (Institute of Electrical and Eletronics Engineers) 802.11.

O padrão Wi-Fi opera em faixas de frequências que não necessitam de licença para instalação e/ou operação. Este fato as torna atrativas. No entanto, para uso comercial no Brasil é necessária licença da Agência Nacional de Telecomunicações (Anatel). Para se ter acesso à internet através de rede Wi-Fi deve-se estar no raio de ação de um ponto de acesso ou local público onde opere rede sem fios e usar dispositivo móvel, como laptop. (MENDES, 2008).

De acordo com o (MIRANDA, 2013). Os principais padrões das redes sem fio são:

802.11a

Chega a alcançar velocidades de 54 Mbps dentro dos padrões da IEEE e de 72 a 108 Mbps por fabricantes não padronizados. Esta rede opera na frequência de 5 GHz e inicialmente suporta 64 utilizadores por Ponto de Acesso (PA). As suas principais vantagens são a velocidade, a gratuidade da frequência que é usada e a ausência de interferências. A maior desvantagem é a incompatibilidade com os padrões no que diz respeito a Access Points 802.11 b e g, quanto a clientes, o padrão 802.11a é compatível tanto com 802.11b e 802.11g na maioria dos casos, já se tornando padrão na fabricação dos equipamentos.

802.11b

Alcança uma velocidade de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes não padronizados. Opera na frequência de 2.4 GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na

recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis, fornos micro-ondas e dispositivo Bluetooth. O aspecto positivo é o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo mundo. O 802.11b é amplamente utilizado por provedores de internet sem fio.

802.11g

Baseia-se na compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 54 Mbps. Funciona dentro da frequência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens também são as velocidades. Usa autenticação WEP (Wired Equivalent Privacy) estática. Torna-se por vezes difícil de configurar, como Home Gateway devido à sua frequência de rádio e outros sinais.

802.11n

Tem uma largura de banda até aos 300 Mbps e um alcance de 70 metros. Opera nas frequências 2,4GHz e 5GHz. É um padrão recente com uma nova tecnologia, MIMO (multiple input, multiple output) que utiliza várias antenas para transferência de dados de um local para outro. Os principais benefícios desta tecnologia são o aumento significativo da largura de banda e o alcance que permite.

2.4 ESTRUTURA DE CAMADAS NO PADRÃO 802.11

A figura a seguir ilustra as camadas do padrão IEEE 802.11, comparando com o modelo RM-OSI da ISO (Reference Model - Open System Interconnecttion of the International Satandardization Organization). (PUC-RIO)

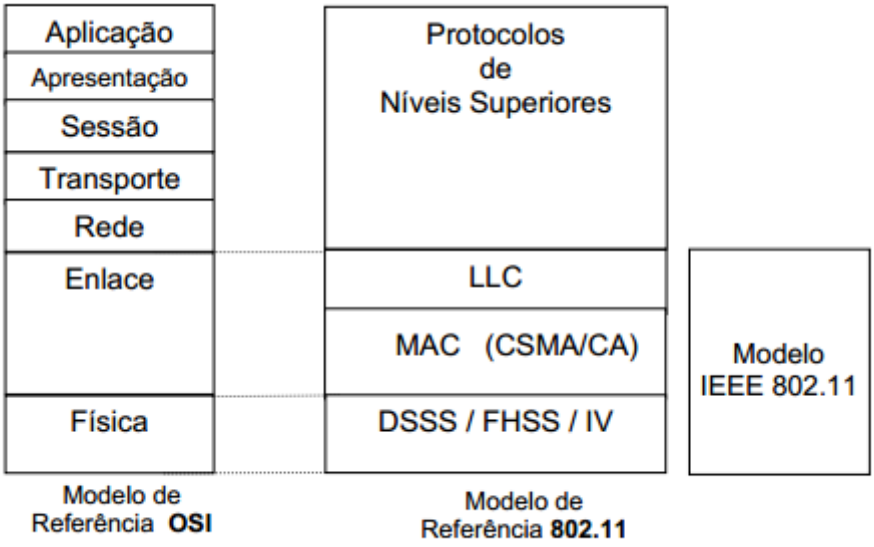

Figura 1
Estrutura de Camadas do padrão IEEE 802.11
Fonte: PUC-RIO

O modelo 802.11 abrange a camada física e de enlace (segundo o modelo de referência OSI).

A tabela seguinte resume as funções das diferentes camadas do modelo OSI:

Tabela 1

CAMADA	FUNÇÃO
APLICAÇÃO	Funções especializadas (transferência de arquivos, terminal virtual, e-mail)
APRESENTAÇÃO	Formatação de dados e conversão de caracteres e códigos
SESSÃO	Negociação e estabelecimento de conexão com outro nó
TRANSPORTE	Meios e métodos para a entrega de dados ponta-a-ponta
REDE	Roteamento de pacotes através de uma ou várias redes
ENLACE	Detecção e correção de erros introduzidos pelo meio de transmissão
FÍSICA	Transmissão dos bits através do meio de transmissão

Camadas do modelo OSI
FONTE: José Pinheiro

2.5 CAMADA FÍSICA

A camada física especificada no padrão IEEE 802.11 é responsável pela transmissão dos bits através do canal de comunicação, definindo as especificações elétricas e mecânicas. A principal função da camada física é a modulação,

preparando a informação para ser transmitida no meio, em forma de onda eletromagnética. Além da modulação, utiliza-se uma técnica de espelhamento do sinal denominada “Spread Spectrum” que tem a função de proteger o sinal contra interferência.(PUC-RIO)

2.6 OPERAÇÕES DA CAMADA FÍSICA

As operações da camada física são similares, independente da técnica de modulação utilizada. O Padrão definiu três estados possíveis, conforme descritos abaixo:

- Detecção de Portadora: estado que permite a camada MAC “escutar" o meio;
- Transmissão: modo de transmissão dos dados;
- Recepção: modo de recebimento dos dados

2.7 CAMADA ENLACE

Ela define o método de acesso ao meio. O Padrão IEEE 802.11 utiliza um método denominado CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), semelhante ao das redes locais ethernet, CSMA/CD (Carrier Sense Multiple Access with Collision Detection). (PUC-RIO)

A camada de enlace é divida em duas subcamadas:

- Controle Lógico do Link (LLC – Logical Link Control);
- Controle de Acesso ao Meio (MAC – Media Access Control).

  A subcamada LLC é idêntica à da especificação IEEE 802.2. Esta subcamada dá suporte à subcamada MAC para serviços de endereçamento, reconhecimento de quadros e detecção de erros.

2.8 MECANISMOS DE CRIPTOGRAFIA

2.8.1 WEP

Para que se possa ter uma comunicação em uma rede sem fio, basta apenas ter um meio para recepção do sinal, ou seja, uma recepção passiva, diferentemente de uma rede cabeada, que necessita obrigatoriamente de uma conexão física entre os dois componentes de rede. Por esta razão, o protocolo 802.11 oferece uma opção de cifragem de dados, onde o protocolo WEP é sugerido como solução para o problema, que está totalmente disseminado e presente nos produtos que estão dentro dos padrões definidos pela IEEE para redes Wi-Fi (RUFINO, 2005).

O protocolo WEP trabalha na camada de enlace de dados e é baseada na criptografia do tipo RC4 da RSA, utilizando um vetor de inicialização (IV) de 24 bits e sua chave secreta é compartilhada em 104 bits, que depois de concatenada completam os 128 bits utilizados para a cifragem dos dados. Para que seja checada a integridade dos dados, o protocolo WEP do transmissor utiliza o CRC-32 para calcular o*checksum* da mensagem transmitida e o receptor faz o mesmo para checar se a mensagem não foi alterada. Existe ainda a possibilidade de o protocolo trabalhar com o padrão mais simples, de 64 bits onde a chave pode ser de 40 ou 24 bits, portanto o padrão de cifragem dos dados é diferente do padrão de 128 bits, garantindo assim duas opções de escolha para tentar obter um nível mínimo de segurança na rede (CANSIAN et al., 2004, AMARAL e MAESTRELLI, 2004).

2.8.2 WPA (Wi-Fi Protected Access)

O protocolo WPA também conhecido como WEP2 ou TKIP (Temporal Key Integrity Protocol - protocolo de chave temporária) surgiu para corrigir os problemas de segurança encontrados no WEP, e implementou a autenticação e a cifragem do trabalho que estava sendo desenvolvido em outros padrões baseados no 802.11. O WPA atua em duas áreas distintas: sua primeira atuação é a substituição total do WEP, ou seja, sua cifragem objetivando a integridade e a privacidade das informações que trafegam na rede. A segunda área de atuação foca diretamente a autenticação do usuário utilizando uma troca de chaves dinâmica, que não era feita pelo WEP e, também, a substituição do vetor de inicialização de 24 bits do WEP para 48. Para isto o WPA utiliza as definições do padrão 802.1x e o EAP (Extensible Authentication Protocol - Protocolo de Autenticação Extensível). (RUFINO, 2005, CANSIAN et al., 2004).

SILVA (2003) afirma que “O WPA padronizou o uso do Michael, também conhecido como MIC (*Message Integrity Check*), em substituição ao CRC-32, melhorando a garantia da integridade dos dados em trânsito”. Michael é uma função *hash* com criptografia chaveada, que produz uma saída de 64 bits. A segurança do Michael baseia-se no fato de que o valor do MIC é cifrado e desconhecido pelo atacante. O método do algoritmo de cifração do WPA é o mesmo utilizado pelo WEP, o RC4.

2.8.3 WPA2

WPA2 foi ratificado em meados de 2004 corresponde a versão final do WPA, a diferença entre WPA e WPA2 e que o WPA utiliza o algoritmo RC4 o mesmo sistema de encriptação utilizado na WEB o TKIP (Temporal Key Integrity Protocol), enquanto o WPA2 se basea na criptografia AES (Advanced Encryption Standard) mais segura que a TKIP, mas exige mais processamento e algumas placas mais antigas não suportam o WPA2 nem mesmo atualizando a firmware (SILVA, 2012).

WPA-PSK (Pre Shared Key) de maneira simples WPA-PSK é uma criptografia forte em que as chaves de criptografia (TKIP) e frequentemente mudada o que garante mais segurança protegendo de ataques hackers, muito utilizado por usuários domésticos.

WPA2-PSK e ainda mais seguro que o WPA-PSK onde sua criptografia (AES) e extremamente forte e resistência a ataques, adotado como padrão de criptografia do governo americano.

2.9 MAC (Media Access Control)

Para que uma rede funcione de maneira eficiente e eficaz, seja ela uma Ethernet ou Wi-Fi, cada dispositivo da rede deve possui uma identificação, para que o equipamento que esteja controlando a rede possa ter a capacidade de concretizar uma organização da mesma. Essa identificação foi definida pelo IEEE, como sendo um número único para cada dispositivo fabricado mundialmente, para evitar qualquer tipo de conflito ou colisão entre os mesmos (RUFINO, 2005).

O IEEE padronizou os endereços MAC em um quadro com seis bytes, onde os três primeiros identificam o fabricante do dispositivo, e os três últimos são para controle do próprio fabricante, sendo necessário seu cadastramento o IEEE para poder receber sua OUI (Organizationally Unique Identifier). Um mesmo fabricante pode ter mais de um OUI, evitando assim o problema de repetição dos números em caso de fabricação de dispositivos em grande escala (TORRES, 2001).

Uma das formas de prevenir uma entrada indevida, ou uma invasão em uma rede sem fio, é cadastrando o endereço MAC de cada dispositivo da rede no controlador da rede, que pode ser um roteador, um ponto de acesso, entre outros. Esse controlador da rede, só permitirá a entrada dos cadastrados em sua base de dados, ignorando outros que porventura possa tentar entrar em sua área de atuação (RUFINO, 2005).

3. SEGURANÇA EM REDES SEM FIO

As redes de computadores baseadas em tecnologias wireless estão se tornando uma realidade para um grande conjunto de instituições e empresas. Entretanto, as redes sem fio apresentam uma série de vulnerabilidades que tem sua origem na concepção dos padrões adotados.

Ao contrário das redes cabeadas, as redes sem fios são de transmissão não guiada num meio comum e acessível a todos, dentro do raio de ação das antenas. Neste cenário, caso a rede não tenha configurado mecanismos mínimos de segurança, o acesso a essa rede fica imediatamente disponível a quem esteja dentro do raio de ação dos APs, com um terminal compatível com a tecnologia utilizada.

Os ataques mais comuns em redes sem fio referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviço. Estes ataques possuem graus de dificuldade dependentes das características de implantação da rede, o que significa dizer que, para que uma rede sem fio possua as mesmas características de segurança de uma rede com fios,

existe a necessidade de inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados.

3.1 SEGURANÇA FÍSICA

A segurança física de uma rede sem fio, muitas vezes não é lembrada e nem levada em consideração em muitos casos de implementação. Em uma rede cabeada, é um ponto importante que faz necessário a preocupação, e na rede sem fio não é diferente, pois a área de abrangência “física” aumenta substancialmente. Na rede cabeada, a segurança é feita configurando-se uma porta de entrada para a rede (um servidor de autenticação) e a necessidade de um ponto de acesso físico para conectar um equipamento (notebook, computador pessoal, e outros). Já agora a preocupação, além destes pontos citados, aumenta no que diz respeito à abrangência do sinal, o seu alcance e por quem será captado, pois este pode alcançar dezenas ou centenas de metros ao redor da empresa, ou onde esteja localizado (RUFINO, 2005).

O posicionamento dos pontos de acesso deve ser minuciosamente estudado, pois é possível que venha a colidir com necessidades essenciais: a velocidade e o desempenho da rede. Um ponto de acesso posicionado em um ponto alto terá um desempenho melhor, pois o sinal ficará mais limpo, possivelmente livre de interferências. Por consequência sua abrangência será maior, abrindo assim possibilidades de interceptações no sinal, facilitando o acesso não autorizado e sofrendo possíveis ataques.

Uma solução para este problema seria regular a potência de transmissão dos sinais emitidos pelos equipamentos de comunicação sem fio, pois este influencia diretamente na distância do sinal emitido. A escolha de um padrão de transmissão (802.11a, 802.11b ou 802.11g, por exemplo) deve ser levada em consideração também, pois os mesmos possuem características próprias de áreas de abrangência.

3.2 CONFIGURAÇÃO DE FÁBRICA

Sempre que uma empresa fabrica determinado produto, ela procura colocar seu produto o mais compatível possível com os dispositivos encontrados atualmente

no mercado e também tenta deixar o mais simplificado possível seu método de instalação. Para que isso tenha efeito positivo, o fabricante deixa muitos de seus recursos de segurança desativados, colocando assim em risco muitas redes montadas por administradores com pouca experiência, que por algumas vezes desconhecem ou não sabem como o fazer (RUFINO, 2005).

Um grande exemplo citado por RUFINO (2005) é o nome de usuário e a senha de acesso padrão em dispositivos controladores e também endereçamentos IP (*Internet Protocol* – Protocolo de Internet). Caso estas configurações não sejam trocadas, facilmente poderão sofrer um ataque e poderá fornecer todo o acesso à rede e a quem nela estiver conectada. As informações de fábrica são facilmente encontradas na Internet, pois os mesmos fabricantes disponibilizam os manuais em suas páginas na web, e assim qualquer pessoa pode ter acesso à mesma.

O SSID (*Service Set IDentifier* - Identificador do domínio de serviço) é uma cadeia de 32 caracteres que identifica cada rede sem fio, e também deve ser motivo de preocupação no momento da configuração de um Ponto de Acesso. (SILVA e DUARTE, 2005).

DUARTE (2003) aconselha alterar o SSID e o *broadcast* de SSID, pois um hacker em posse do mesmo, pode se passar por um ponto de acesso e assim invadir as estações clientes ou inundar a rede com pedidos de dissociação.

3.3 LOCAL DO ACCESS POINT

A qualidade e a segurança da rede estão diretamente ligadas ao posicionamento do ponto de acesso de uma rede sem fio dentro de uma pequena empresa, organização, ou até mesmo no meio doméstico. O sinal do ponto de acesso é enviado para diversas direções, e por este motivo que o concentrador e/ou ponto de acesso deve ficar em um local onde abrangerá toda a área necessitada, evitando que o sinal saia de seu perímetro de segurança (RUFINO, 2005).

Uma ressalva pode ser feita: o posicionamento do ponto de acesso pode ser considerado como uma tentativa de restringir o sinal, pois não é possível de forma alguma ter um controle sobre ondas eletromagnéticas.

3.4 MAPEAMENTO

Este com certeza é uma das primeiras ações que os invasores executam. O invasor tenta conseguir o maior número de informações detalhadas possíveis sobre a rede que está tentando invadir, permitindo que seu ataque seja mais preciso e que sua presença seja com maior dificuldade detectada. Vejamos os dois tipos possíveis de mapeamento:

Mapeamento Ativo

Com este tipo de mapeamento é possível identificar os equipamentos que estão atuando na rede, bem como seu endereço MAC, sendo suficiente para que, caso haja algum tipo de vulnerabilidade conhecida, ser usada pelo invasor para conseguir invadir a rede (RUFINO, 2005).

Um programa que pode ser usado para realizar o mapeamento ativo é o *TCH-rut*, que permite identificar os endereços MAC em uso pelos dispositivos, bem como o fabricante do mesmo. Porém para que isso seja possível, o atacante já deverá estar participando da rede. Após ter reconhecido e escolhido algum alvo na rede, o atacante parte agora para o ataque direto a ele, utilizando outras ferramentas combinadas, ou isoladamente, como por exemplo, o NMAP (*Network Mapper* – Mapeador de Rede), que verifica quais os serviços que estão ativos no momento, efetuando a varredura das portas abertas no alvo a ser atacado (RUFINO, 2005).

Mapeamento Passivo

Este é um método que é permitido ao atacante mapear os componentes e atividades da rede que se está tentando atacar, com a vantagem de não ser percebido. Uma ferramenta utilizada para fazer este mapeamento é o p0f, que necessita apenas que o intruso esteja dentro da área de sinal do ponto de acesso ou do componente que está transmitindo o sinal, sem a necessidade de comunicar-se com qualquer um. Esta ferramenta fornece informações para que o invasor possa

selecionar qual dos dispositivos conectados à rede possivelmente esteja mais vulnerável, sem ser visto, melhorando ainda as chances de conseguir êxito na invasão (RUFINO, 2005).

3.5 FALHAS NAS CRIPTOGRAFIAS WEP, WPA e WPA2

- **WEP**

A principal falha existente no protocolo WEP é a possibilidade de quebrar seu algoritmo, e muitos dos utilizadores (Administradores de redes, técnicos, etc.) deste protocolo o condenaram sem entender em que circunstâncias exatas isso pode ocorrer. O protocolo WEP necessita obrigatoriamente que em ambos os lados da comunicação os dispositivos conheçam a chave para cifrar e decifrar, e esse é o grande problema, pois muitas pessoas terão que saber esta chave, principalmente se for um ambiente muito amplo ou com grande mobilidade. Por mais segura que seja a distribuição desta chave, esta será menos secreta, visto que muitas pessoas saberão dela, e que equipamentos e dispositivos possam ser atacados, compartilhados e até roubados (RUFINO, 2005).

- **Vetor de inicialização**

Um dos grandes problemas do WEP se deve ao fato da reutilização do vetor de inicialização. O texto é encriptado usando uma cadeia pseudoaleatória, gerada pelo IV (possui 24 bits) e a chave (pode ser de 40 ou 104 bits). O IV com apenas 24 bits é muito pequeno (apenas 224 IVs diferentes) e, por exemplo, em uma conexão de 5Mbps demorará menos de 12 horas para ser repetido, e como essas chaves são geradas aleatoriamente, esse tempo de repetição tende a ser menor.

Com isso surge uma brecha para a quebra do WEP. Porque temos uma chave fixa que foi devidamente configurada nos clientes que estão se comunicando, sempre que tivermos uma repetição de IV teremos a mesma sequência pseudoaleatória gerada pelo IV e a chave.

Vamos supor que temos 2 textos que foram criptografados pelo mesmo par IV e chave, como propriedade do XOR, podemos encontrar um texto legível (sem estar

codificado) se tivermos posse do outro texto legível, usando esses dois textos codificados e o texto legível.

Alguns pacotes têm seu valor conhecido, como por exemplo, os que pedem a chave do usuário, contendo a palavra Payload. A partir de cada pacote novo descoberto fica ainda mais fácil de descobrir os outros, até q até que podemos saber todos os 224 das sequências pseudoaleatórias (ANDRADE, 2011).

- **Chaves**

Como não há nenhuma especificação no padrão IEEE 802.11 sobre o gerenciamento das chaves, esse gerenciamento se baseia no fato de existir um vetor de 4 chaves e cada mensagem possui um campo no qual indica qual chave do vetor deverá ser usada. Lembrando que na maioria das vezes a mesma chave é utilizada em todos os dispositivos.

Visto que todos os aparelhos que irão estar conectados a essa rede devem saber a chave, se essa informação chegar aos usuários se torna mais difícil de manter essa informação em sigilo.

Uma estratégia muito utilizada por aqueles que gerenciam as redes é que eles mesmos configuram as chaves nos computadores para que os usuários não tenham conhecimento sobre elas. Esta estratégia ameniza mas não resolve, visto que as chaves continuam armazenadas nos dispositivos remotos que acaba sendo uma fonte de informação para os invasores.

Outro problema ocasionado pelo compartilhamento de uma chave por vários usuários é que aumentam as chances de haver uma colisão. E ainda deve ser lembrado que para haver a troca de chaves o dispositivo deve ser reconfigurado que demanda um trabalho árduo e cuidadoso, portanto, na prática as chaves serão mantidas por um longo tempo, facilitando a analise de tráfego aos intrusos (ANDRADE, 2011).

- **CRC32**

Outra dificuldade a ser superada por aqueles que fazem uso do WEP é a linearidade do CRC32, que é o algoritmo usado para garantir a integridade (ICV - Integrity Check Value) dos dados recebidos. Como consequência da linearidade, o pacote pode sofrer alterações controladas que não serão percebidas pelos dispositivos receptores nem pelos emissores.

Basta saber a string pseudoaleatória utilizada na encriptação do texto que se torna possível alterar o texto original. Podemos interceptar a informação e fazer a alteração desejada, depois corrigimos o ICV de modo que a alteração não será detectada e a checagem da integridade da informação terá sido superada sem problemas, chegando assim uma informação alterada ao usuário (ANDRADE, 2011).

- **WPA**

De acordo com (LINHARES E GONÇALVES), O WPA solucionou praticamente todas as vulnerabilidades apresentadas pelo protocolo WEP. Porém, falhas em sua implementação o tornaram vulnerável:

- **Fraqueza no algoritmo de combinação de chave** - Tendo conhecimento de algumas chaves RC4 (menos de 10 chaves) geradas por IVs, cujos 32 bits mais significativos são os mesmos, um atacante pode achar a chave de criptografia de dados e a chave de integridade [10]. Esse ainda não é um ataque prático, pois possui complexidade de tempo o (2105), porém há uma redução significativa se comparado com um ataque de força bruta o (2128).

- **PSK é susceptível a ataques de dicionário** - Diferentemente do ataque de força bruta, que tenta todas as possibilidades possíveis exaustivamente, o ataque de dicionário tenta derivações de palavras pertencentes a um dicionário previamente construído. Este tipo de ataque, geralmente é bem sucedido porque as pessoas têm o costume de utilizarem palavras fáceis de lembrar e que normalmente pertencem a sua língua nativa. Além do dicionário, informações capturadas durante o 4-Way-Handshake são necessárias para a quebra da PSK. Um detalhe que não é muito sabido é que se a chave PSK for de mais de 20 caracteres este ataque não funciona em tempo factível.

- **Negação de Serviço** - O MIC possui um mecanismo de proteção para evitar ataques de força bruta, porém esse mecanismo acarreta um ataque de negação de serviço (DoS). Quando dois erros de MIC são detectados em menos de um minuto o AP cancela a conexão por 60 segundos e altera a chave de integridade. Portanto, com uma simples injeção de pacotes mal formados é possível fazer um ataque de negação de serviço. Além disso, o WPA continua sofrendo dos mesmos ataques de negação de serviço que o WEP já sofria, visto que esses ataques são baseados em quadros de gerenciamento.

- **WPA2**

De acordo com o (SOUZA, 2010), Especialistas em segurança da AirTight Networks descobriram uma falha de segurança no protocolo de rede Wi-Fi WPA2.

A falha foi chamada de "Hole 196", em referência à página 196 do manual de padrões da IEEE – entidade que regulamenta o setor.

Nessa página, o padrão IEEE explica as chaves usadas pelo WPA2: a PTK (Pairwise Transient Key), que é única para cada cliente Wi-Fi e usada para tráfego unidirecional e a GTK (Group Temporal Key), para broadcast.

Enquanto falsificações de dados e de endereços MAC podem ser detectadas pela PTK, a GTK não oferece essa funcionalidade.

Os especialistas da AirTight dizem que essa é a questão central, porque permite a um cliente gerar pacotes arbitrários de broadcast, para que outros clientes respondam com informação sobre suas PTKs secretas, que podem ser decodificadas pelos atacantes.

A AirTight disse que bastam 10 linhas extras de código disponível na web para o driver open source Madwifi para fazer um Computador com uma placa de rede comum simular o endereço MAC de um Acess Point (AP) e passar-se por gateway para o envio de tráfego.

Atacantes podem explorar isso para derrubar a rede, via ataque de negação de serviço (DoS). O único porém é que eles precisam estar dentro da rede Wi-Fi como usuários autorizados.

3.6 TÉCNICAS DE INVASÃO

Devido a facilidade de acesso que os dispositivos de redes sem fio proporcionam muitos usuários e algumas empresas da tecnologia wireless não se preocupam com a segurança de sua própria rede e acabam dando mais atenção ao seu desempenho. Muitos não adotam uma configuração necessária de segurança e criptografia para se obter uma confiabilidade maior de segurança de transmissão de dados em redes sem fio.

Através da falta de preocupação com a segurança nas redes sem fio, muitos indivíduos podem obter acesso não autorizado a ela, pelo fato de muitos usuários e empresas utilizarem equipamentos com configuração de fábrica (*Default*). Isso ocorre pela falta de informação que em algumas vezes não são passadas para o consumidor final (RUFINO, 2005).

Com tantas possibilidades de invasão facilitada através de *softwares* ou até mesmo sem nenhum conhecimento, muitos indivíduos obtêm acessos à rede sem fio sem autorização, comprometendo assim a confiabilidade e a integridade das informações que circulam pela rede sem fio. Indo mais a fundo o *hacker* pode ter quatro comportamentos estratégicos diferentes em relação ao processo de invasão de redes sem fio, de acordo com (RUFINO, 2005).

Interrupção: Nesse procedimento o invasor influi em interromper as passagens de dados de um ponto para outro.

Interseção: Nesse procedimento o invasor realiza coleta de informações para saber o que se passa dentro da rede e por fim ter acesso a ela futuramente.

Modificação: Nesse procedimento o invasor não apenas escuta o tráfego da rede, mas também modifica e compromete os dados para depois enviá-los para o

dispositivo a que está sendo atacado. O objetivo é que este se torne um dispositivo zumbi e o invasor tenha total controle os dispositivos.

Fabricação: Nesse caso, o invasor desenvolve os dados a serem enviados para um determinado destino com intuito de se obter acesso a rede sem fio.

Quando um invasor descobre uma rede sem fio completamente mal configurada, ele pode utilizar *softwares* maliciosos (*Scanners)* que capturam os pacotes de dados com o intuito de se obter o SSID e a chave de acesso.

Existe a possibilidade do atacante se passar por um membro da rede sem fio e assim os dispositivos dão a permissão para executar tarefas como se fosse um usuário normal (RUFINO, 2005).

3.7 ALGUMAS FERRAMENTAS PARA AS REDES SEM FIO

A seguir serão mostradas algumas das ferramentas disponíveis tanto para a segurança quanto para o ataque nestas redes. A idéia é simplificar as explicações de cada um dos ataques e relacionar cada um destes com as ferramentas que utilizam.

3.8 NETSTUMBLER

URL: http://www.netstumbler.com

Este é a ferramenta mais conhecida de scanner para redes sem fio. Inclui muitas características como potência do sinal, e SSID da rede em questão, além de suporte a GPS. Este programa modificou significantemente o mundo da rede sem fio. Pois, além de ser utilizado para ações maliciosas, pode ser utilizado pelo gerente da rede em questão para monitorar a qualidade do sinal e quantos dispositivos estão instalados na sua instituição. Este software possui uma versão para Pocket PC intitulada MiniStumbler, a qual pode ser utilizada sem que desperte muita atenção e tenha a mesma eficácia do NetStumbler tradicional. Apesar de todas as inovações trazidas por estes programas, a base de sua concepção também é a base de seu maior problema. Utilizando o método de sondagem ativa da rede, suas primeiras

versões enviavam informações que facilitavam a identificação destes softwares através da análise do tráfego da rede.

3.9 KISMET

URL: http://www.kismetwireless.net

Desenvolvido com a filosofia opensource este sniffer inclui um grande número de ferramentas e opções. Projetado como cliente e servidor, pode ter vários servidores rodando à distância de um único cliente. Além de monitorar uma gama muito grande de origens diferentes, pode armazenar os pacotes capturados em vários formatos diferentes. Além de funcionar como sniffer este programa ainda gera dados relacionados à localização aproximada do dispositivo monitorado. Isto é realizado através da união das características do Kismet com um GPS. Outro ponto favorável em relação às outras ferramentas é que automaticamente salva todas as redes encontradas. Trabalhando com a biblioteca Ncurses e tendo várias telas e opções, disponibiliza quase todas as informações necessárias para um atacante desenvolver seus ataques. Algumas das informações que o Kismet consegue obter sobre o estado geral da sua área de abrangência são: Número de WLANs detectadas, número total de pacotes capturados por WLAN, ausência ou não de criptografia WEP, número de pacotes com o I.V. fraco, número de pacotes irreconhecíveis, número de pacotes descartados e tempo decorrido desde a execução do programa.

3.10 WELLENREITER

URL: http://wellenreiter.sourceforge.net/

Esta é uma ferramenta para descobrimento e auditoria de redes sem fio. Os testes realizados com esta ferramenta mostraram que esta não difere das demais. Entretanto, é mais rudimentar e insere poucas funcionalidades adicionais. Uma destas funcionalidades é a capacidade de fazer um brute force dos SSIDs. Neste, a maioria dos SSIDs padrões são enviados em broadcast em pacotes de Probe Request forjados com endereços MAC (Media Access Control) de origem adulterados. Assim, o Wellenreiter mantém o atacante oculto enquanto observa as respostas aos Probes que havia feito. Hoje, o Wellenreiter esta disponível tanto em um script em perl e gtk como em C++. Tanto uma versão quanto outra foram testadas e nem uma das duas funcionou a contento, uma vez que a funcionalidade

de brute force não pode ser efetuada, pois é necessária a existência de duas placas sem um mesmo sistema.

3.11 WEPCRACK

URL: http://sourceforge.net/projects/wepcrack/

Este programa trabalha utilizando-se da vulnerabilidade encontrada no começo do ano 2001 no WEP. Na realidade este programa é um script perl e supostamente funcionaria em qualquer sistema com suporte a este tipo de script. No entanto, somente se torna inteiramente funcional em sistemas *nix.

Pessoas mal intencionadas utilizam o WEPCrack para obter informações vitais à rede como o BSSID para gerar ataques posteriores.

4. DESENVOLVIMENTO DO TEMA

4.1 BACKTRACK

O BackTrack é uma ferramenta voltada para testes de penetração muito utilizada por auditores, analistas de segurança de redes e sistemas, hackers éticos etc. Sua primeira versão é de 26 de maio de 2006, seguida pelas versões [2] de 6 de março de 2007, [3] de 19 de Junho de 2008, [4] de 22 de Novembro de 2010 e [5] de 2011. Atualmente, possui mais de 300 ferramentas voltadas para testes de penetração, existem ainda algumas certificações que utilizam o BackTrack como ferramenta principal, OSCP Offensive Security Certified Professional, OSCE Offensive Security Certified Expert e OSWP Offensive Security Wireless Professional, certificações oferecidas pela Offensive Security que mantém o BackTrack (GIAVAROTO e SANTOS, 2013)

4.2 UTILIZANDO O BACKTRACK

Para utilizarmos o Backtrack, teremos que fazer a instalação do mesmo, a instalação do é fácil, podemos fazer a instalação em uma máquina virtual, rodar direto de um CD ou pendrive.

Para o download do BackTrack consultar o **Anexo1**.

Neste trabalho realizei a instalação do BackTrack em uma máquina virtual utilizando o VIRTUAL BOX. Para download do Virtual Box, consultar **Anexo2.**

O desenvolvimento deste trabalho foi realizado em um condomínio residencial com cerca de 112 apartamentos divididos em 7 blocos conforme a imagem abaixo.

Figura 2
Condomínio
Fonte: Google Maps

Utilizei um adaptador Wireless da TP-LINK modelo 721N que trabalha em modo monitor para capturar os dados trafegados nas redes sem fio, consultar **Anexo3.**

Para localizar as redes sem fio utilizei o software que está disponível no Backtrack 5, esse software é denominado Gerix. Com este software é possível verificar o SSID da rede sem fio, o canal que a rede esta utilizando e o protocolo de segurança utilizado nesta rede sem fio, estas são informações importantíssimas da rede.

4.3 TESTES COM O BACKTRACK

Buscando as redes sem fio no conjunto residencial utilizando o Gerix, foi encontrado um grande número de redes sem fio, conforme as figura abaixo.

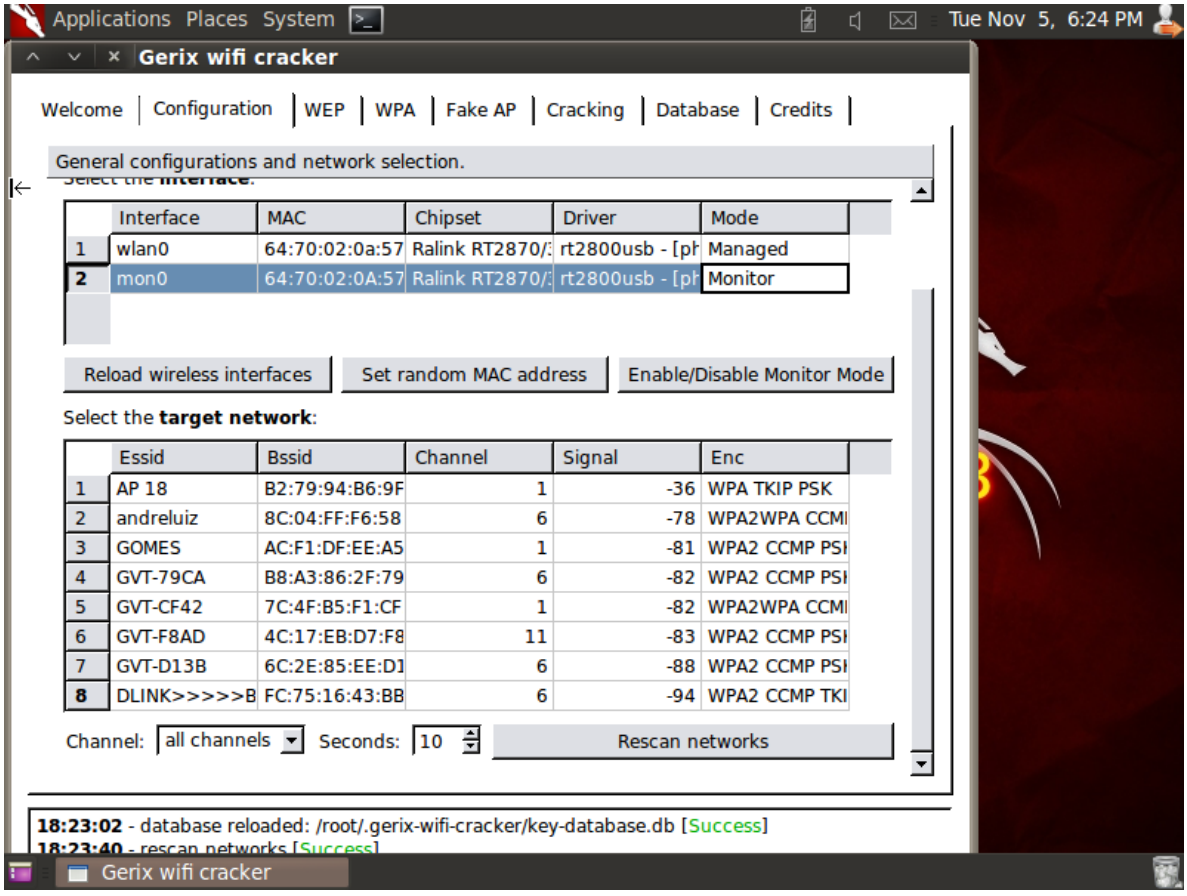

Figura 3

Interface do Gerix

Fonte: Autor

Acima podemos verificar como é fácil obter informações sigilosas de uma rede sem fio, Conseguimos identificar os ESSID da rede, qual é o MAC do ponto de acesso, o canal que está rede está utilizando, e a configuração do mecanismo de

segurança, estas informações são muito importantes para uma pessoa mau intencionada.

Neste caso iremos tentar descobrir a chave de segurança do ESSID da rede AP 18, que está configurada com mecanismo de segurança WPA, no caso são mais “fáceis” de serem invadidas.

Vamos iniciar o serviço dentro do Gerix chamado “Start Sniffing and Logging” que no caso nada mais é que começar a capturar os dados da rede, conforme a tela abaixo.

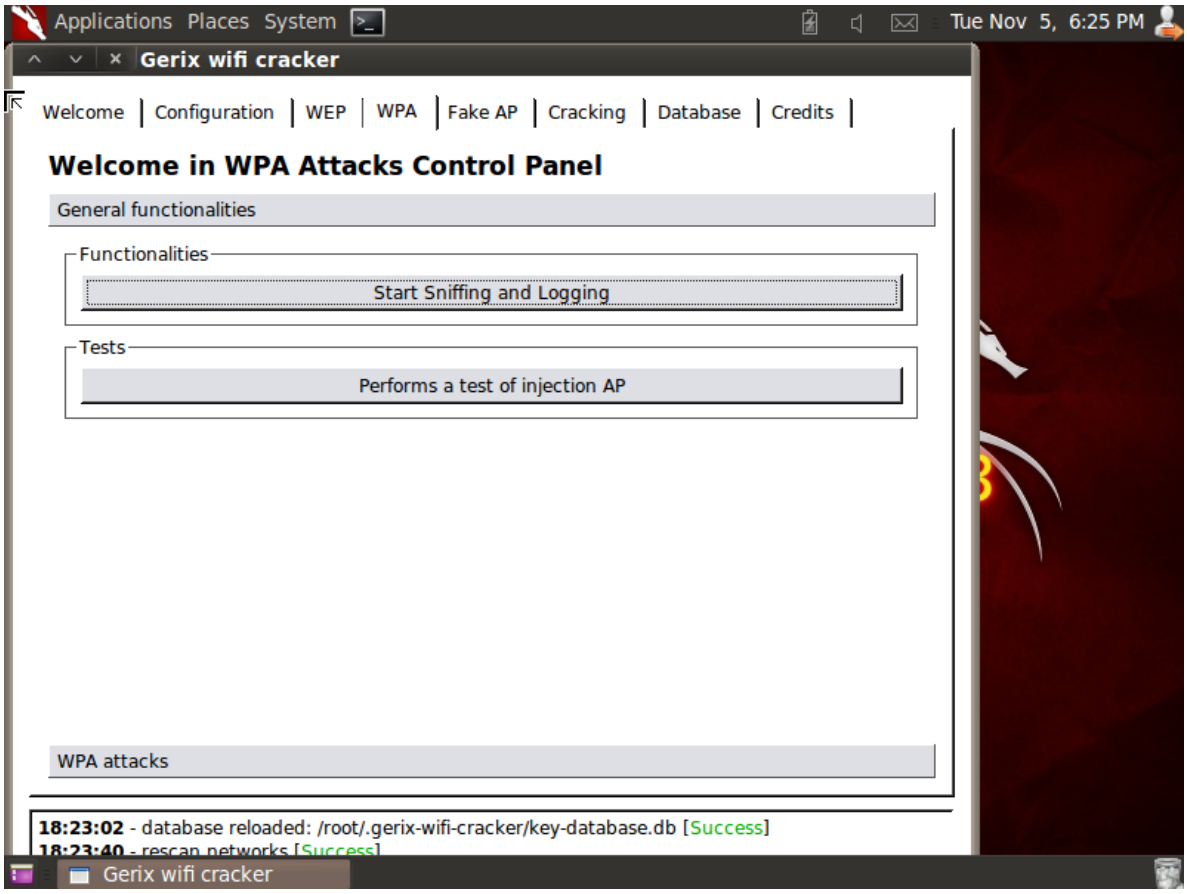

Figura 4
Iniciando a captura de pacotes
Fonte: Autor

Abaixo podemos verificar o serviço de captura de pacotes ativo, e no caso capturando os pacotes da rede sem fio AP 18 em BSSID podemos identificar o MAC do AP que no caso é B2:79:94:B6:9F:C4.

Para tentarmos descobrir a chave da rede sem fio que está sendo atacada, obrigatoriamente temos que ter alguém conectada nela, conforme podemos ver na tela abaixo em “STATION”, que quer dizer os endereços MAC que estão conectados nesta rede sem fio, que no caso é o 00:AA:70:B8:E4:39.

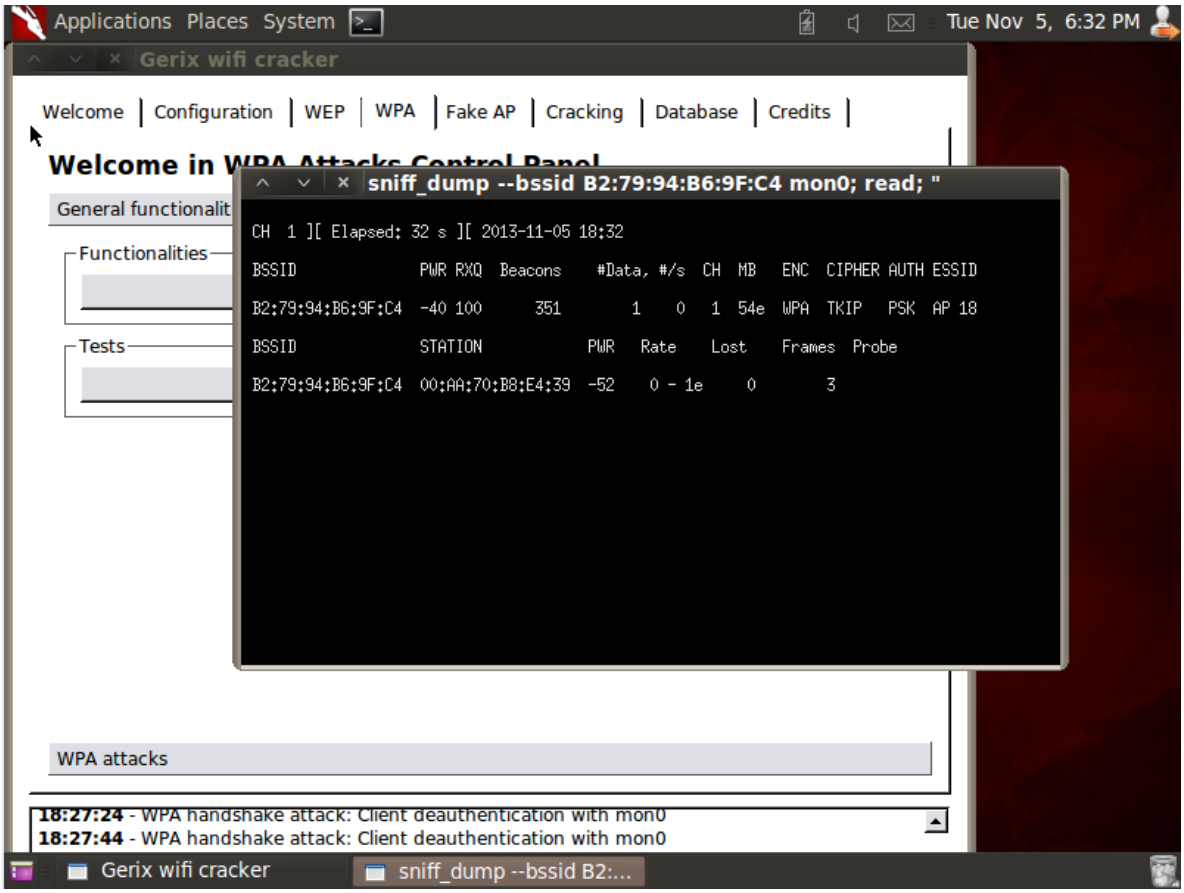

Figura 5
Capturando os pacotes
Fonte: Autor

No caso desta rede, com 1.118 pacotes capturados, já foi possível realizar um ataque pra tentar descobrir a chave de segurança conforme a tela abaixo.

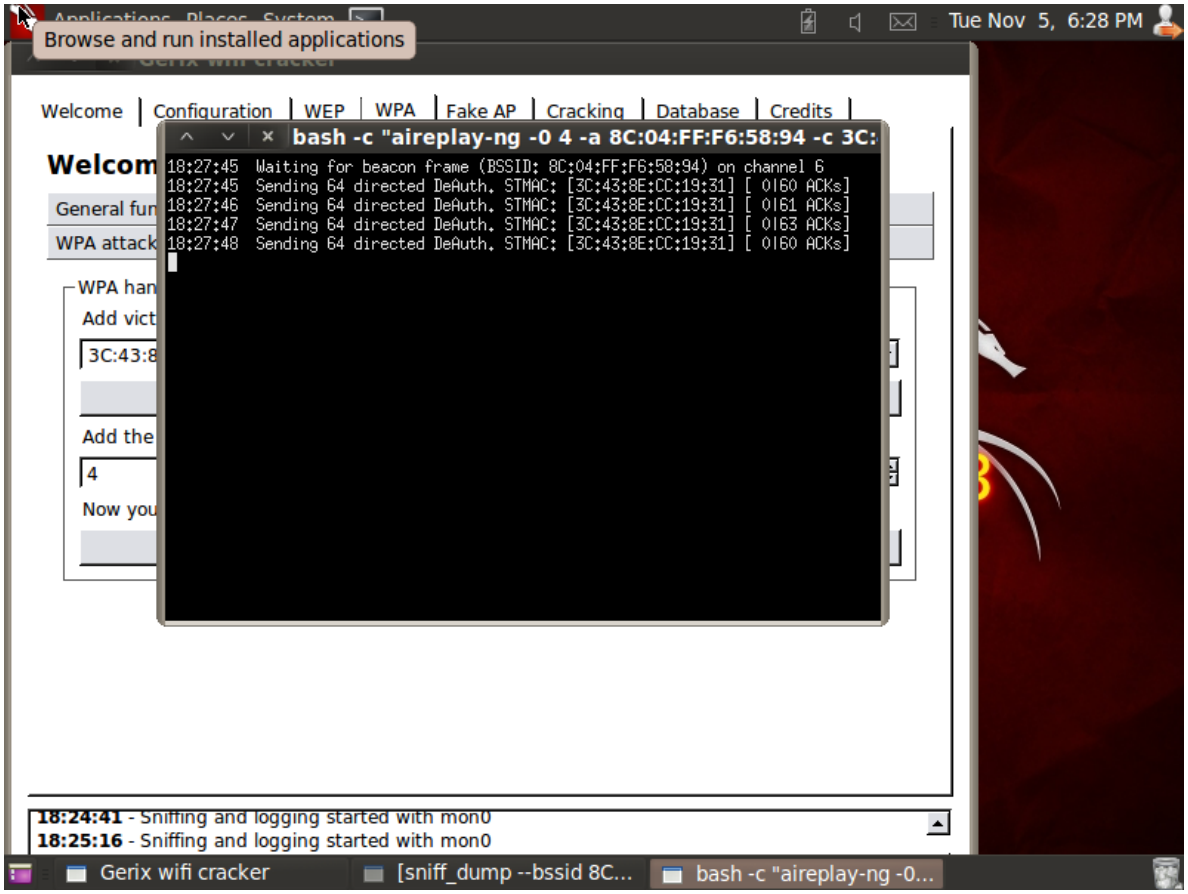

Figura 6
Atacando a rede sem fio

Fonte: Autor

Na tela abaixo podemos verificar que após o ataque conseguimos fazer com que o Gerix identificasse qual é a chave de segurança utilizada, no lado direito da tela podemos ver “WPA handshake: B2:79:94:B6:9F:C4”, isso significa que ele já encontrou a chave, mais para descobrirmos qual é está chave, temos que usar uma “WordList” que nada mais é que um “dicionário” muito utilizado por Hackers onde contém inúmeras palavras, números e caracteres.

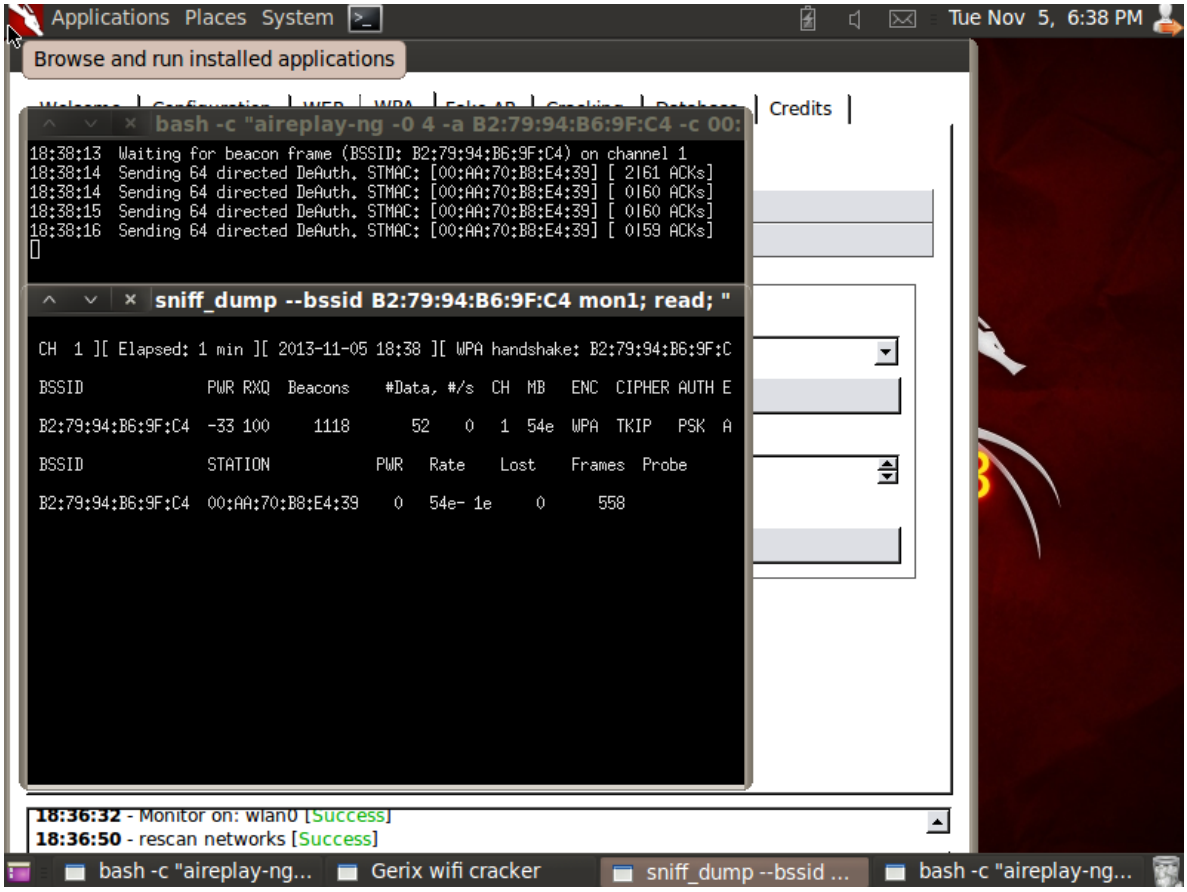

Figura 7
Chave Identificada
Fonte: Autor

Logo abaixo iremos buscar o dicionário para tentar identificar qual é a chave utilizada para está rede sem fio.

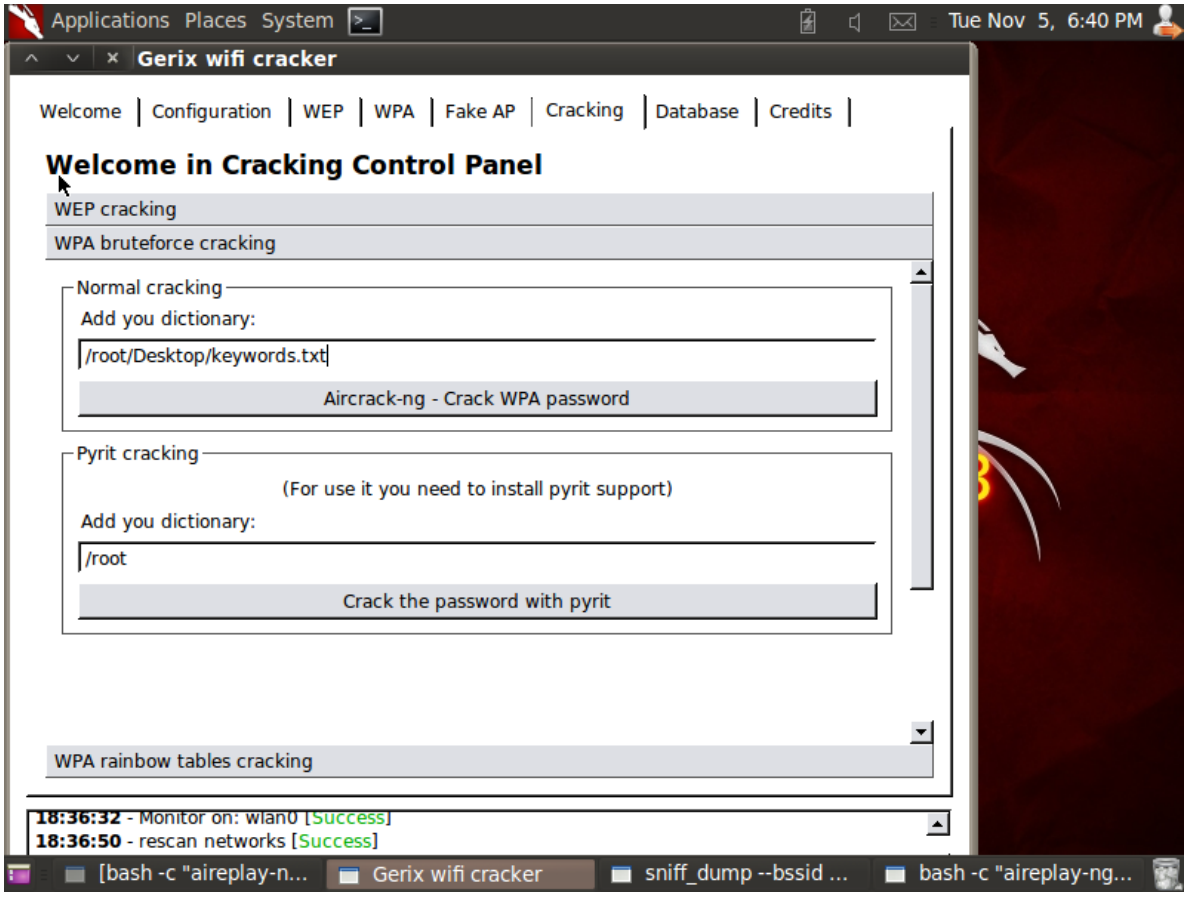

Figura 8
Utilizando o Dicionário

Fonte: Autor

Abaixo podemos ver o Gerix comparando os pacotes capturados e buscando no dicionário qual é a chave, neste caso ele encontrou e trouxe o resultado em “KEY FOUND”, a chave é “isabela2012”.

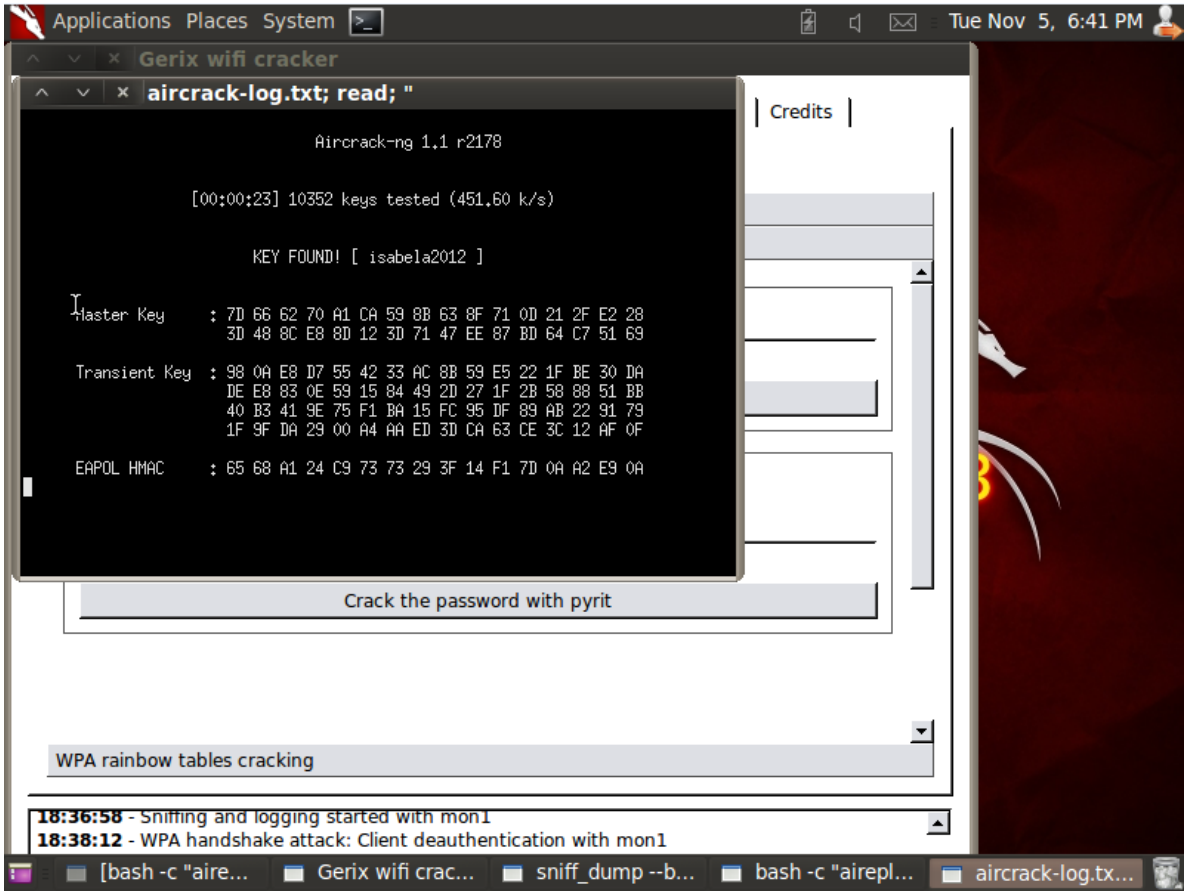

Figura 9
Chave descoberta
Fonte: Autor

Abaixo podemos identificar outra rede sem fio no mesmo condomínio com o mesmo mecanismo de segurança WPA, neste caso não foi possível realizar o ataque por causa do baixo sinal desta rede sem fio.

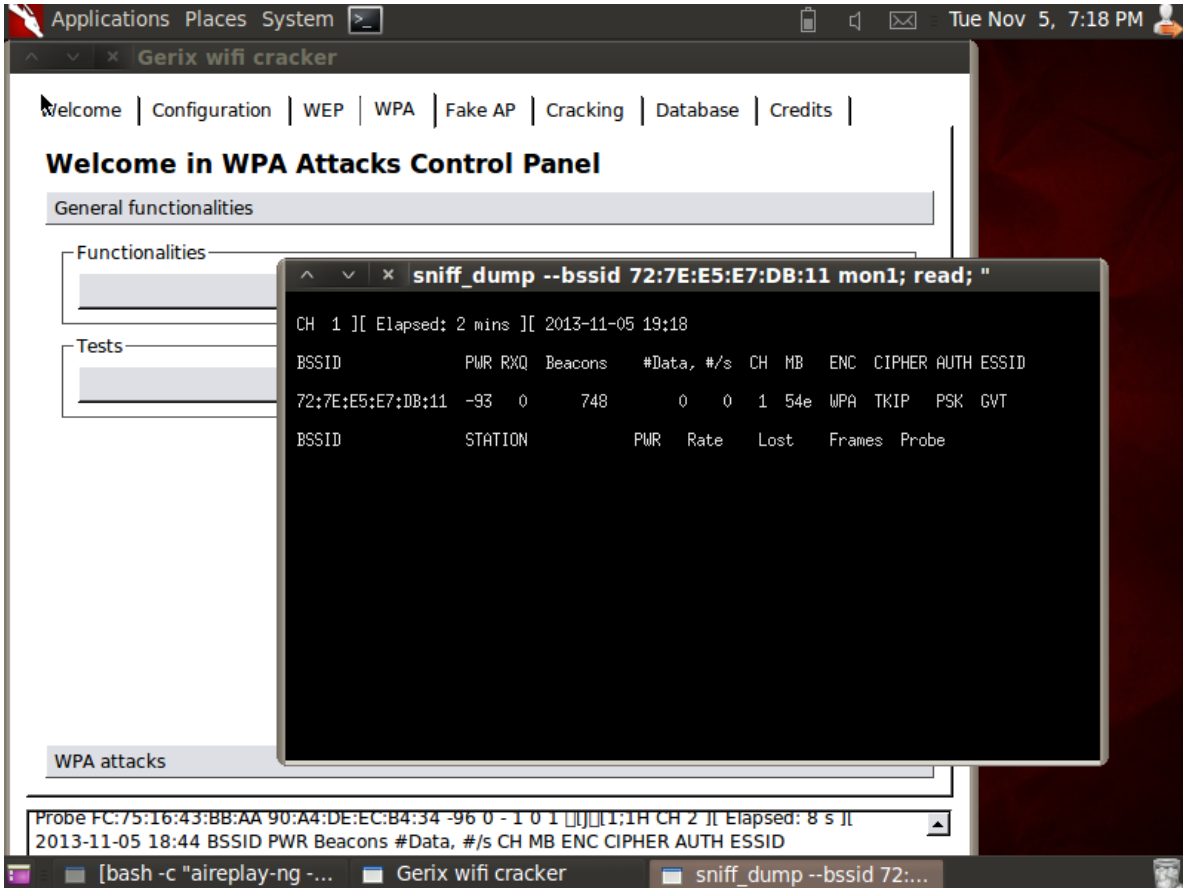

Figura 10
Outra rede sem fio
Fonte: Autor

4.4 BACKTRACK BRUTE FORCE

O método “Brute Force” ou força bruta é mais utilizado nos casos em que se tenta invadir uma rede sem fio configurada com o protocolo WPA2, se uma rede com este protocolo for bem configurada é quase impossível de invadir, o que acontece nas maioria dos casos é que as pessoas acabam colocando uma senha fácil de ser descoberta, mais para a pessoa que está atacando, isto acaba levando horas, dias, meses, com isso é possível a quebra, mais o sinal do AP pode cair ou a na própria máquina do atacante pode ocorrer algum problema, isto requer muita paciência.

Para iniciar o processo de Brute Force, precisamos abrir um prompt de comando dentro do BackTrack, e digitar os comandos abaixo para colocar a placa de rede em modo monitor.

- **airmon-ng** - verificar se interface tá sendo reconhecida.

- **airmon-ng** - start wlan0 coloca interface modo monitor.
- **airodump-ng** - mn0 busca as redes ao nosso alcance.
- **airodump-ng** --bssid (mac) -w (nome para salvar os pacotes .cab) -c (canal) mon0 – Aqui se escolhe o “MAC” da rede e escolher também o nome de um arquivo para salvar estes pacotes.
- **aireplay-ng** --deauth 0 -a (macdarede) -e (mac do usuário) mon0 – Neste passo atacamos a rede usando o MAC da rede e MAC do usuário que está conectado nela.
- **aircrack-ng** -w (dicionário) (arquivo.cap) – Após o ataque ser positivo, aqui buscamos no dicionário para tentar identificar a senha da rede, e fazemos comparações com os pacotes salvos no arquivo.cab.

Abaixo segue um exemplo das redes sem fio encontradas com o comando **airodump-ng.**

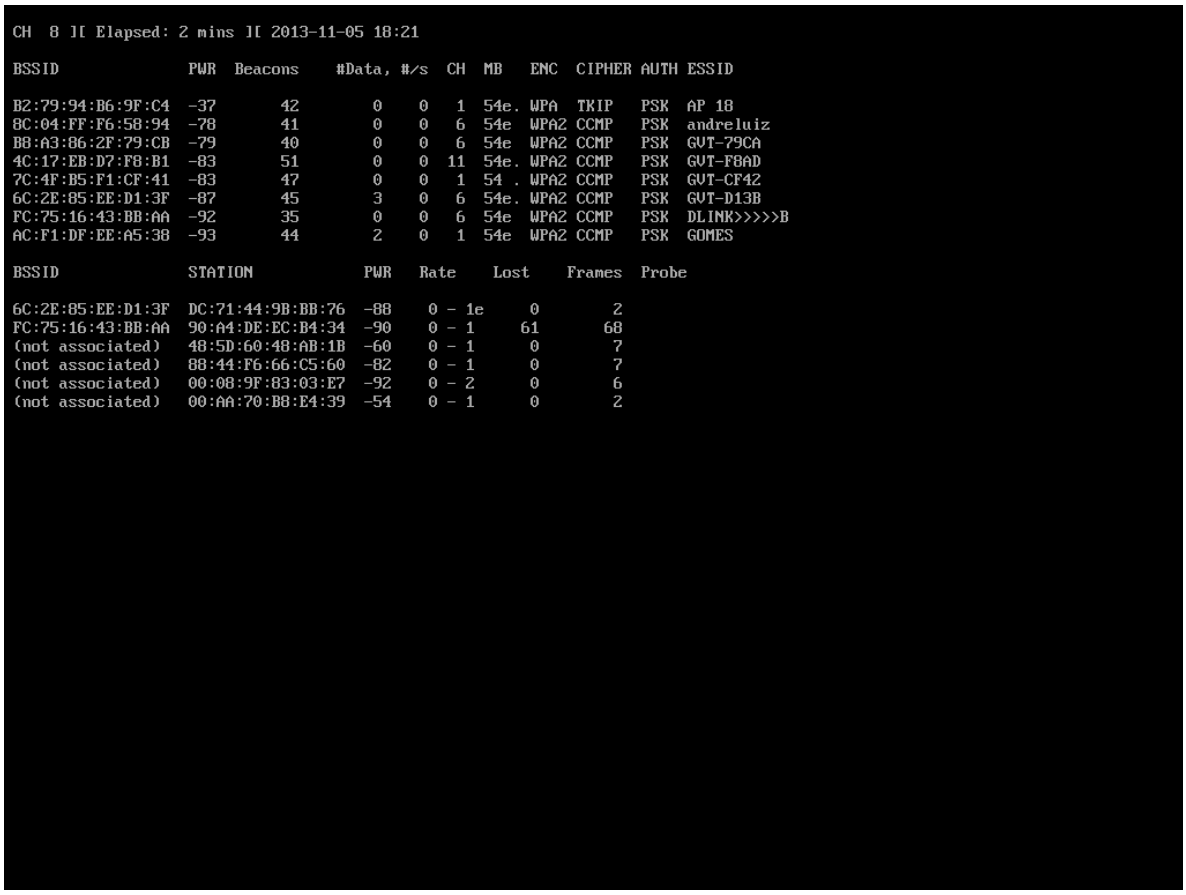

Figura 11
Redes sem fio - Brute Force

Fonte: Autor

5. RESULTADOS

Com o desenvolvimento da parte prática deste trabalho, consegui invadir uma rede sem fio onde estava configurado o protocolo de segurança WPA, a invasão nesta rede sem fio foi extremamente fácil, foram capturados pouco mais de mil pacotes e com isto já conseguimos descobrir a chave de segurança desta rede, as outras redes sem fio estavam configuradas com o protocolo WPA2 onde é muito difícil de ser invadida por causa de sua criptografia.

6. CONCLUSÃO

Com o desenvolvimento deste trabalho pela pesquisa teórica e de campo, conclui que os usuários domésticos ainda têm muitas dificuldades para configurar as suas redes sem fio, visto a quantidade de redes sem fio que conseguimos encontrar configuradas de modo inadequadas.

Hoje em dia é difícil encontrar pessoas que configurem os Pontos de Acesso com o protocolo WEP, mais muitas ainda continuam a usar o WPA que em si é seguro caso as pessoas configurem, por exemplo, com uma senha forte de mais de vinte caracteres, isto acaba tornando um possível ataque inviável por causa do tempo que demoraria.

O mecanismo de segurança WPA2 é o mais usado hoje em dia por causa de sua segurança, na análise que foi feita podemos verificar que uma grande quantidade de pessoas já utiliza este mecanismo.

Hoje em dia a maioria das empresas que oferecem a internet, já oferecem os equipamentos de distribuição de sinal wireless, ele já vem configurado de fábrica com o protocolo WPA2 e uma senha forte com bastantes caracteres, isto é muito importante, porque ajuda os usuários que não sabem configurar de maneira correta. Quando o usuário tem alguma dúvida com relação a configuração de equipamentos de terceiros, é sempre bom procurar um técnico especializado para configurar o seu ponto de acesso, tendo em vista que a maioria dos pontos de acesso vem de fábrica com uma senha padrão onde pode ser facilmente descoberta no manual.

Talvez em um futuro próximo tenhamos novos protocolos para as redes sem fio, onde tenha ainda mais segurança, e possa garantir a integridade dos dados trafegados nas redes sem fio.

Hoje em dia já temos uma nova tecnologia que está sendo implementada e que não é tão conhecida, ela se chama Wimax (Worldwide Interoperability for Microwave Access), em trabalhos futuros podemos pesquisar sobre a segurança desta nova tecnologia.

REFERÊNCIAS

ASSUNÇÃO, Marcos. F.A, **O Guia do Hacker Brasileiro**. SP: Visual Books, 2002.

MENDES, Douglas R. **Redes de Computadores: Teoria e prática**. SP: Novatec Editora, 2007.

JARDIM, Fernando de M, **Treinamento Avançado de Redes Wireless**. SP: Digerati, 2007.

CAMPOS, André. L. N. **Sistema de Segurança da Informação: Controlando os Riscos.** Florianópolis: Editora Visual books, 2006.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio.** 2. Ed. São Paulo: Novatec, 2005.

SILVA, Pedro Tavares et all. **Segurança em sistemas de informação**: gestão estratégica da segurança da empresa real. Portugal: Centro Atlântico, 2003.

GIAVAROTO, Silvio Cesar Roxo / SANTOS, Gerson Raimundo Dos, 2013 **BACKTRACK LINUX - AUDITORIA E TESTE DE INVASAO EM REDES DE COMPUTADORES.**

CANSIAN, Adriano Mauro, GRÉGIO, André Ricardo Abed e PALHARES, Carina Tebar. Artigo apresentado na Universidade Estadual Paulista – SP. Assunto: 69 **Falhas em Políticas de Configuração: Uma Análise do Risco para as Redes Sem Fio na Cidade de São Paulo**. Universidade Estadual Paulista – SP, 2004 Disponível em: http://www.acmesecurity.org/sites/default/files/publicacoes/artigos/acme-artigo-ssi-2004-wlan.pdf - Acessado em 25/09

AMARAL, Bruno Marques, MAESTRELLI, Marita. **Segurança em Redes Wireless. 802.11**. Centro Brasileiro de Pesquisas Físicas - 2004. Disponível em: http://homes.dcc.ufba.br/~italo/redes/seg-wireless/wirelesspt-br.pdf - Acessado em 28/09

SILVA, Luiz Antonio F. da, DUARTE, Otto Carlos M. B. **RADIUS em Redes sem Fio**. Universidade Federal do Rio de Janeiro. RJ – 2003.

Disponível em: http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RADIUS_em_Redes_sem_Fio.pdf - Acessado em 05/10

SILVEIRA, Claudio Heleno**. Tutorial de Redes sem Fio.** 2013**,** Disponível em: http://www.passeidireto.com/arquivo/1739478/tutorialderedesemfio-cursosonlinegratis - Acessado em 06/10

TORRES, Gabriel. **Redes de Computadores, Curso Completo.** Editora Axcel Books, 2001.

DUARTE. Luiz Otavio. **Analise de vulnerabilidades e ataques inerentes a redes sem fio 802.11x**. 2003. 53 f. Tese (Bacharel em Ciência da Computação) – Universidade do Estado de São Paulo, São José do Rio Preto.
Disponível em: http://pt.scribd.com/doc/84885857/Analise-de-Vulnerabilidades-e-Ataques-Inerentes-a-Redes-Sem-Fio-802 - Acessado em 07/10

HANETO, Pedro**. Modelo OSI e TCP/IP.** 2010**,** Disponível em: http://pedrohaneto.blogspot.com.br/2010/02/modelo-osi-e-tcpip.html - Acessado em 12/10

CRUZ**,** Christofer**. TCP/IP,** Disponível em: http://christofercruz.blogspot.com.br/2011/08/tcpip.html - Acessado em 13/10

PINHEIRO, José Mauricio Santos, **O modelo OSI**, 2004, Disponível em: http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php - Acessado em 16/10

NBR ISO/IEC 17799 (2005), Disponível em: http://pt.scribd.com/doc/2449992/Abnt-Nbr-Isoiec-17799-Tecnologia-da-Informacao-Tecnicas-de-Seguranca-Codigo-de-Pratica-para-a-Gestao-da-Seguranca-da-Informacao - Acessado em 17/10

FARIAS, Paulo César Bento, **Rede Wireless**, 2005, Disponível em: http://www.juliobattisti.com.br/tutoriais/paulocfarias/redeswireless001.asp - Acessado em 20/10

BUSCH, Jade, **Wired ou Wirelles**, 2008, Disponível em: http://jaderedes.blogspot.com.br/2008/11/wired-ou-wireless.html - Acessado em 23/10

MENDES, Osvane, **Wi-Fi**, 2009, Disponível em: http://osvanewireless.blogspot.com.br/2009_08_01_archive.html - Acessado em 23/10

MIRANDA, Antônio, **Redes Wi-Fi 802.11 o que é?**, 2013, Disponível em: http://antoniomjf.wordpress.com/2013/08/24/redes-wi-fi-802-11-o-que-e-e-seus-padroes/ - Acessado em 26/10

SILVA, Givonaldo, **Redes sem fio** 2012, Disponível em: http://givonaldogilvan.blogspot.com.br/2012/10/wep-wep2-wpa-wpa2-wpa-psk-wpa2-psk.html- Acessado em 27/10

SOUZA, Eric Cordeiro de, **Protocolo de Segurança Wi-Fi Wpa2**, 2010. Disponível em: http://wifinetnews.com/archives/002452.html - Acessado em 29/10

PINHEIRO, José Mauricio Santos, **O Modelo OSI**, 2004. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php - Acessado em 30/10

PUC-RIO, Certificação Digital, **Padrão IEEE 802.11**, Disponível em: http://www2.dbd.puc-rio.br/pergamum/tesesabertas/0210420_05_cap_02.pdf - Acessado em 03/11

Condomínio Residencial – Google Maps
https://maps.google.com.br/maps?q=mapa+de+curitiba&ie=UTF-8&hq=&hnear=0x94dce3f5fc090ff1:0x3c7a83b0092bb747,Curitiba+-+Paran%C3%A1&gl=br&ei=GsuAUtyXGMyMkAfm7oCQAQ&sqi=2&ved=0CDEQ8gEwAA - Acessado em 06/11

ANDRADE, Gil Eduardo de, **Segurança de Sistemas**, 2011. Disponível em: http://www.gileduardo.com.br/ifpr/ss/downloads/ss_aula06.pdf - Acessado em 16/11

LINHARES, André Guedes, GONÇALVES, Paulo André da S. **Análise de Mecanismos de Segurança**. Disponível em: http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf - Acessado em 17/11

Anexo1 – Download BackTrack
http://www.backtrack-linux.org/downloads/

Anexo2 – Download Virtual Box
https://www.virtualbox.org/wiki/Downloads

Anexo3 - Adaptador wireless usb Tp-Link 721N - Disponível em: http://www.tp-link.com.au/products/details/?model=TL-WN721N – Acessado em 06/11