Segurança em Rede Wireless: Um estudo de Caso

Juliana Barroso LOMILER[1], Fábio Éder CARDOSO[2]
julianalomiler@gmail.com, fabioeder.professor@gmail.com
Instituto Municipal de Ensino Superior de Assis (IMESA)
Fundação Educacional do Munícipio de Assis (FEMA) – Assis/SP (Brasil)

RESUMO: Atualmente as redes de computadores se tornaram mais presentes na sociedade, devido ao crescimento da quantidade e qualidade de informações disponíveis na Internet. Também o uso da tecnologia Wireless está sendo cada vez mais presente nos ambientes corporativos como nos domésticos, pelo baixo custo dos equipamentos e pela grande facilidade da implementação da Rede Sem Fio. Porém, a transmissão dos dados pela rede sem fio é muito vulnerável, pelo fato da transmissão ser realizada por meio da propagação, que é o ar, assim facilitando que qualquer invasor consiga furtar informações que estão sendo transmitidas no momento, mas isso só ocorre se o mesmo estiver dentro do campo de atuação, ou seja, conectado a rede.

PALAVRAS-CHAVE: Vulnerabilidade; Ataque; Rede sem fio; Integridade; Confidencialidade;

ABSTRACT: Nowadays the computer networks have become more present in the society, due the growing of the quantity and quality of information available on the Internet. Also the use of Wireless technology is increasingly more present in the corporate environments as in home appliances, for the equipment's low-cost and the very easy wireless network implementation. But, the data transmission through the wireless network is too vulnerable, by the fact that the transmission is made by propagating, that is the air, therefore, facilitating that any invader can steal information that are being transmitted on the moment, but it only happens if the invader is inside the playing field, i.e., connected to the network.

KEYWORDS Vulnerability; Attack; Wireless Network; Integrity; Confidentiality;

Antes do surgimento das redes de computadores, a mobilidade de dados consistia unicamente em utilizar um disquete para transferir informações de um local para outro, e apenas isso. A Internet, mesmo que de forma restrita, já existia, e dispositivos móveis tais quais os celulares também, porém eram tratados como algo além da imaginação

uma futilidade desnecessária para a vida em sociedade. Neste cenário, filmes como "Hackers", de 1995, apresentam jovens rebeldes utilizando telefones públicos e procurando senhas em papéis jogados na lata de lixo para invadir computadores por diversão (GALLO, 2003; KIZZA, 2009; SOARES, 1995).

Com a inserção das redes sem fio, mais comumente conhecidas como redes *Wireless Fidelity* (WIFI) houve uma grande expansão no uso dos dispositivos móveis. A mobilidade, como uma das características das redes *wireless* (sem fio), foi uma das mais importantes para a sua disseminação no mercado. (TANEMBAUM, 2003)

Com o passar do tempo e a evolução da informática, a Internet tornou-se não apenas útil, mas obrigatória à vida das pessoas. Foi popularizada tão rapidamente que exigiu um rápido aprendizado a respeito de seu uso básico, deixando para trás os cuidados com a segurança da informação. O problema tomou maiores proporções a partir da necessidade da mobilidade, essencial para pessoas físicas e empresas de pequeno, médio e grande porte. Segundo dados da companhia Ericsson (2015) em agosto de 2015 existiam, cerca de 7.2 bilhões de dispositivos, divididos entre *notebooks, modems com roteadores, tablets* e *smartphones,* estes últimos servindo ao propósito de estarem conectados o tempo todo. A figura 1 mostra essa evolução do uso da mobilidade no ano de 2015.

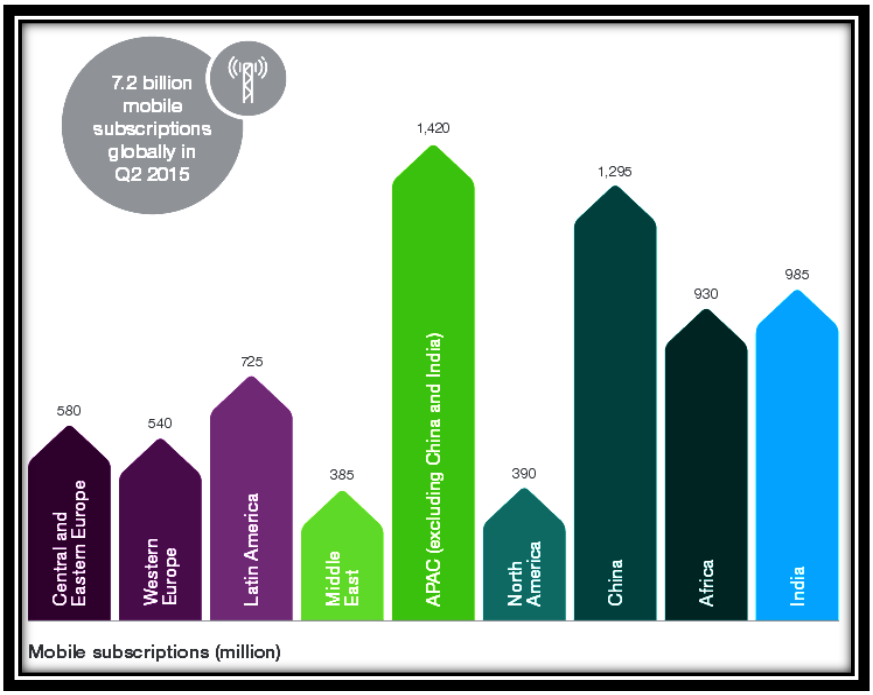

Figura 1: Demonstração do crescimento do uso de dispositivos móveis com acesso à Internet (Ericsson, 2015).

Com o uso massivo de redes sem fios e também, com a inserção de dispositivos móveis que conectam a redes; prover segurança nestas conexões é extremamente importante para que os usuários utilizem esta importante tecnologia de forma segura. Porém em pontos de acesso a falta segurança é o fator principal, tento a possibilidade de perda de informações ou mesmo ter informações roubadas.

Portanto é de extrema importância garantir as três características básicas da segurança da informação que são a confidencialidade, integridade e disponibilidade. A confidencialidade é a garantia do resguardo das informações em confiança para que pessoas não autorizadas tenham acesso às mesmas, a integridade é garantir que a informação chegará ao seu destino sem sofrer nenhum tipo de dano ou modificação e a disponibilidade é a garantia de acesso à informação onde quer que o usuário esteja, se a informação estiver disponível para o acesso (TANENBAUM, 2003).

As três características básicas são fundamentais para a segurança de uma rede sem fio ou para uma rede de computadores cabeada, possibilitando assim um acesso seguro ao usuário, entretanto existem diversas ferramentas de invasão a rede, essas invasões têm como objetivo adquirir dados importantes para uso indevido, ou para chantagear o proprietário dos dados furtados. Essas ferramentas também são muito utilizadas para encontrar a vulnerabilidade na rede para que não haja a possibilidade de invasão para roubo de informações.

Aplicar técnicas e métodos de segurança é um fator primordial para qualquer segmento que utilize esta tecnologia. Alguns procedimentos básicos, como inserção de senhas complexas, evitam que qualquer pessoa, má intencionada, tente obter vantagens, ilicitamente, no uso das redes sem fio.

Este trabalho apresenta o uso de técnicas de detecção e testes de vulnerabilidades em redes sem fio, explorando os padrões de segurança utilizados no mercado, comparando-os de modo a reportar ao leitor os modelos de configuração mais seguros.

Explorar, de forma prática, as vulnerabilidades apresentadas em redes sem fio que utilizam o padrão IEEE 802.11 é um conjunto de padrões criados pela IEEE para o uso de redes wireless. Este padrão levou à criação de uma certificação para produtos compatíveis com os padrões, que assegurava que eles sejam intercompatíveis, ou seja, apenas os produtos certificados podem utilizar o Wi-Fi. Alguns padrões utilizando o certificado foram criados com o decorrer dos anos, a tabela a seguir ilustra esses padrões, a frequência, as taxas (MORIMOTO,2010).

Padrão	Frequência	Taxa de transferência	Ano
IEEE 802.11	2.412 GHz | 2.462 GHz	1, 2 Mb/s	1997
IEEE 802.11 b	2.412 GHz | 2.462 GHz	2, 5.5,11 Mb/s	1999
IEEE 802.11 a	5.8 GHz	6 até 54 Mb/s	1999
IEEE 802.11 g	2.4 GHz	Até 54 Mb/s	2003
IEEE 802.11 n	2.4GHz | 5.8 GHz	300 Mb/s até 600 Mb/s	2006
IEEE 802.11 ac	5 GHz	433 Mb/s até 6 Gb/s	2012

E comparando os padrões de segurança mais utilizados neste tipo de rede, dentre eles: segundo MORIMOTO, o WEP (*Wired Equivalent Privacy*) é um mecanismo de autenticação, pode ser configurado de forma privada ou publica, ou seja, configurado com senha ou sem senha, esse método não é indicado devido as suas falhas de segurança; WPA (*Wired Protected Access*) é baseada no protocolo TKIP (*Temporal Key Integrity*), nesse sistema a chave é trocada periodicamente, por essa razão é recomendado à utilização do WAP; WPA2 (*Wired Protected Access*) é baseado no protocolo o AES esse mecanismo oferece um alto grau de segurança, entretanto, tem como deficiência a alta exigência de processamento, não é recomendável para usuários domésticos, e também não ser compatível com equipamentos antigos e o WPS (*Wi-fi Protected Setup*) é o padrão de segurança que permitem que o usuário mantenha facilmente sua rede doméstica segura, quando o usuário for acessar ele irá requerer um PIN (*Personal Identification Number)*. Esse método tornou-se vulnerável desde 2014, pois foi alvo de ataques brutos e pela facilidade de descobrir o PIN.

Para realizar os testes de vulnerabilidade foi utilizado o Sistema Kali Linux, que é uma distribuição GNU/Linux baseada no sistema operacional Debian, é um projeto *open source* que é mantido e financiado pela ofensiva de Segurança, um fornecedor de treinamento de segurança da informação de classe mundial e serviços de teste de penetração, ou seja, tem como finalidade voltada principalmente em auditoria e segurança de rede computadores (Kali Linux, 2013).

Ainda segundo o site oficial do Kali Linux, existem diversas ferramentas disponíveis para realização de ataques, defesa e analise de dados, tais como NMAP (utilizado para realizar escaneamento de portas abertas), Wireshark (utilizado para capturar pacotes que estão trafegando pela rede), Aircrack-ng (software para realização de testes de segurança em rede sem fio), entre outras.

A partir de todos os fundamentos e técnicas estudadas, foram efetuados os testes práticos, onde foram utilizadas as técnicas do Airmon-ng, esse script permite ativar o modo de monitoramento da interface wireless, após ter uma interface com o modo de monitoramento ativo é possível utilizar o Airodump-ng, que é um script que captura pacotes de fames brutos 802.11 e é particularmente apropriado para coletar Vetores de Inicialização (IVs) WEP, assim pode-se enxergar qualquer rede sem fio que esteja ativa ao alcance da interface de rede mesmo que ela esteja invisível a um dispositivo, a partir da utilização do Airodump-ng utilizando o script Aireplay-ng, que tem como função principal de gerar tráfego para o uso posterior do Aircrack-ng para quebrar senhas WEP e WAP, existem diferentes ataques que podem causar desautenticação coma finalidade de capturar dados *handshake* WPA. Após a captura de um dado *handshake* utiliza-se o *script* Aircrack-ng que tem como função comparar o dado *handshake* com uma *word list* com o objetivo de nessa comparação adquirir a senha. (AIRCRACK-NG)

Observação: Os testes foram realizados em diferentes lugares, as figuras ilustrando os testes são em diferentes ambientes, e os testes foram realizado no método de autenticação WPA.

Foram realizadas as seguintes etapas:

I. Foi utilizado o comando Airmon-ng para colocar a placa de rede sem fio em modo de monitoramento para que poça capturar os pacotes, para iniciar a placa em modo de monitoramento, utilizamos o comando **airmon-ng start wlan0**, este comando colocará a *interface* de rede sem fio (wlan0) em modo de monitoramento, automaticamente o comando dá um nome a placa em modo de monitoramento de wlan0mon. A figura a seguir ilustra o comando.

Figura 2: Ilustração do comando Airmon-ng

II. Após ativar o modo de monitoramento da placa, utiliza-se o comando **airodump-ng wlan0mon** para iniciar o modo de monitoramento, assim que o comando é utilizado irá ser gerado em tempo real uma lista de equipamentos que distribuem *Internet* e em baixo as estações conectadas.

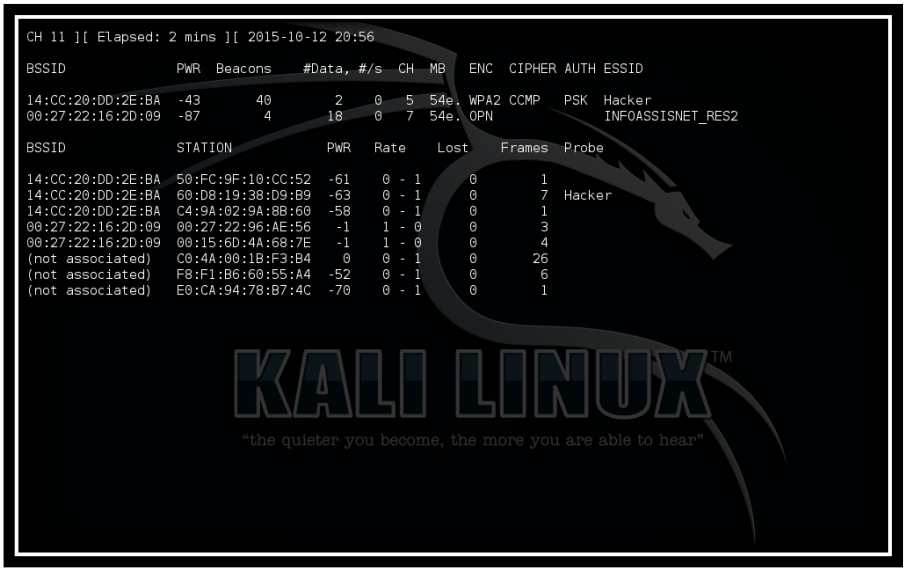

Figura 3 Ilustração do comando Airodump-ng wlan0mon

III. Após alguns minutos de esperar para listar todos os equipamentos que distribuem *Internet*, abra um novo terminado e utilize o comando **airodump-ng -c canal(CH) -w nomedoarquivo --bssid MAC wlan0mon,** para utilizar esse comando deverá escolher um equipamento que deverá realizar o ataque, digite o comando **airodump-ng**, o, é para destinar o canal qual o equipamento escolhido trafega, em seguida digite o nome de sua escolha para colocar em um arquivo à onde os dados coletados serão armazenados, o –w é para dizer que você vai escrever dentro do arquivo, o **–bssid** é o *Media Access Control* (MAC) e por fim você escreve o nome da sua placa de rede em modo de monitoramento **wlan0mon.**

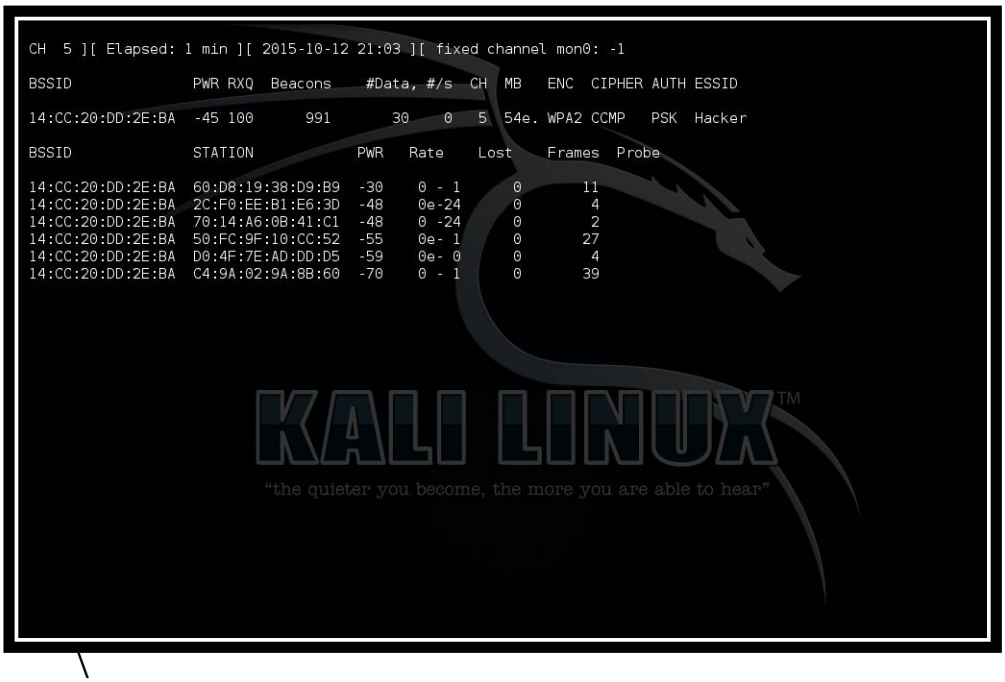

Figura 4 Ilustração do comando Airodump-ng

IV. Após utilizar o comando na etapa anterior, abra um novo terminal e mantenha o anterior aberto, agora utilize o comando **aireplay-ng -0 10 -a mac –c estacao wlan0mon,** este comando funciona da seguinte forma, o mesmo é utilizado para desautenticar ou autenticar uma estação que está conectado à rede sem fio, o -0 significa desautenticar e -1 autenticar, em seguida devesse colocar a quantidade de vezes que será feito a autenticação ou desautenticação da estação, o –a e em seguida deverá ser digitado o MAC do equipamento que será atacado e o –c será a estação que irá ser desautenticada ou autenticada e em seguida digitamos a *interface* de rede que estamos utilizando. Neste caso como queremos descobrir a senha iremos desautenticar a estação, este comando iremos fazer diversas vezes.

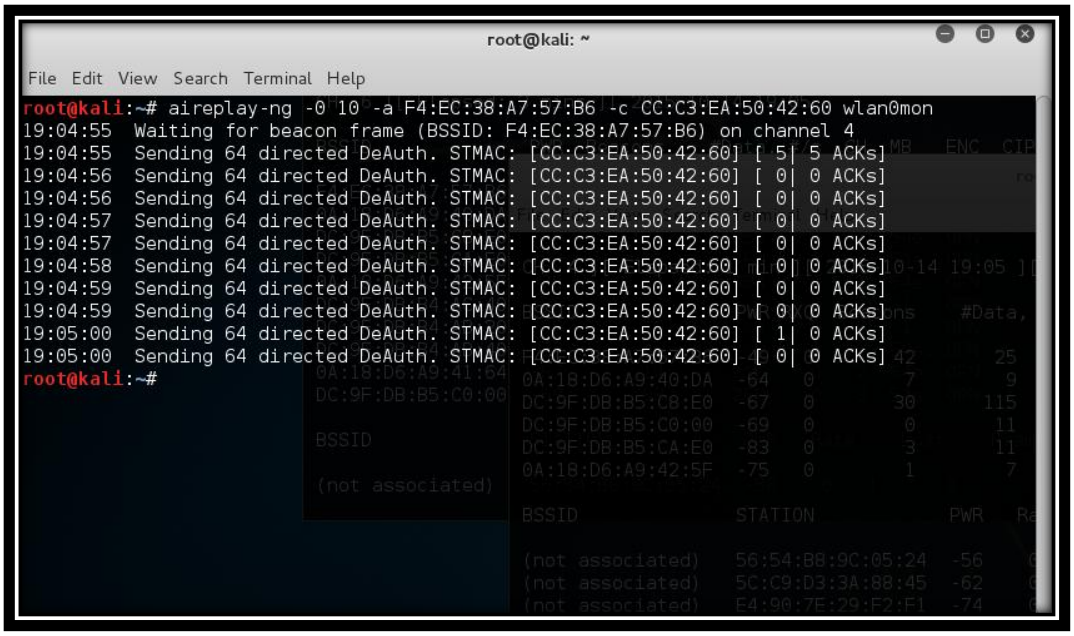

Figura 5 Ilustração do comando Aireplay-ng

V. Utilizando o comando **aireplay-ng -0 10 -a mac –c estacao wlan0mon** iremos monitorar a etapa III, enquanto na etapa III não aparecer no canto superior direito escrito: **WPA handshake: MAC da equipamento** que distribui a *Internet* não pode parar de utilizar o comando da etapa IV. E quando significa que conseguiu capturar a senha, porém ela está criptografada.

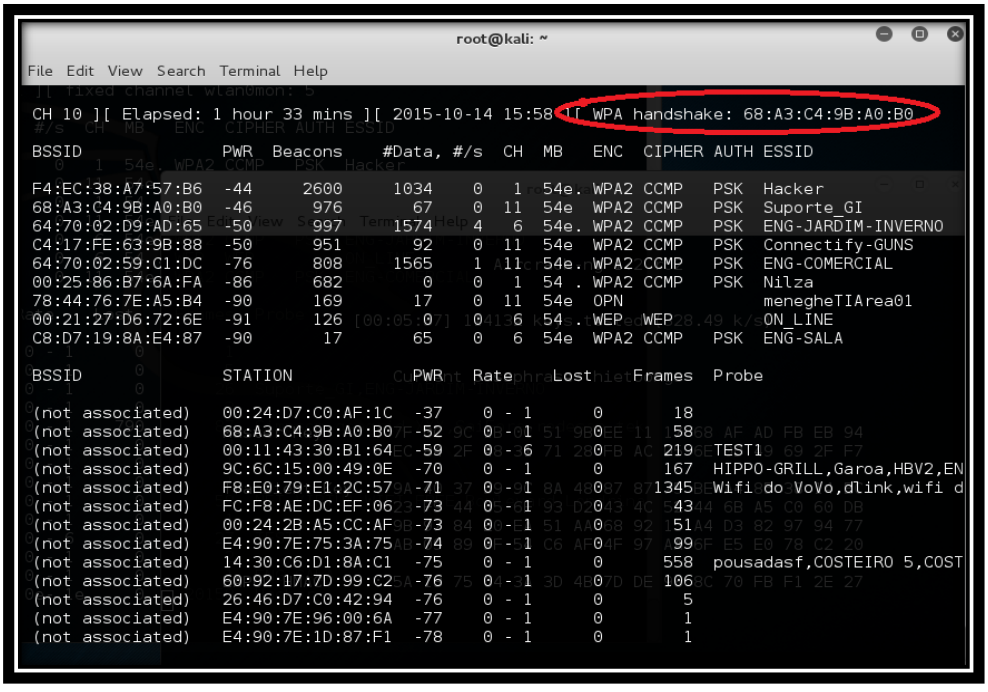

Figura 6 Ilustração do WPA handshake.

VI. Por fim, utilizaremos o comando aircrack-ng, que é um script de decriptografia, para utiliza-lo você deverá ter uma *wordlist*, ou seja, uma lista de combinações palavras, números e letras que são possíveis senhas colocadas por usuários. O comando completo é Aircrack –ng nome do arquivo –w *wordlist*, este "nome do arquivo" é o nome que você destinou para o arquivo da etapa III e –w para você escrever dentro do arquivo e na frente o nome da sua *wordlist.* O processo pode demorar alguns segundos como pode demorar várias horas, você utiliza o comando e aguarde a resposta. A senha só será encontra se ela existir dentro da *wordlist* caso contrário a decriptografia não ocorrerá.

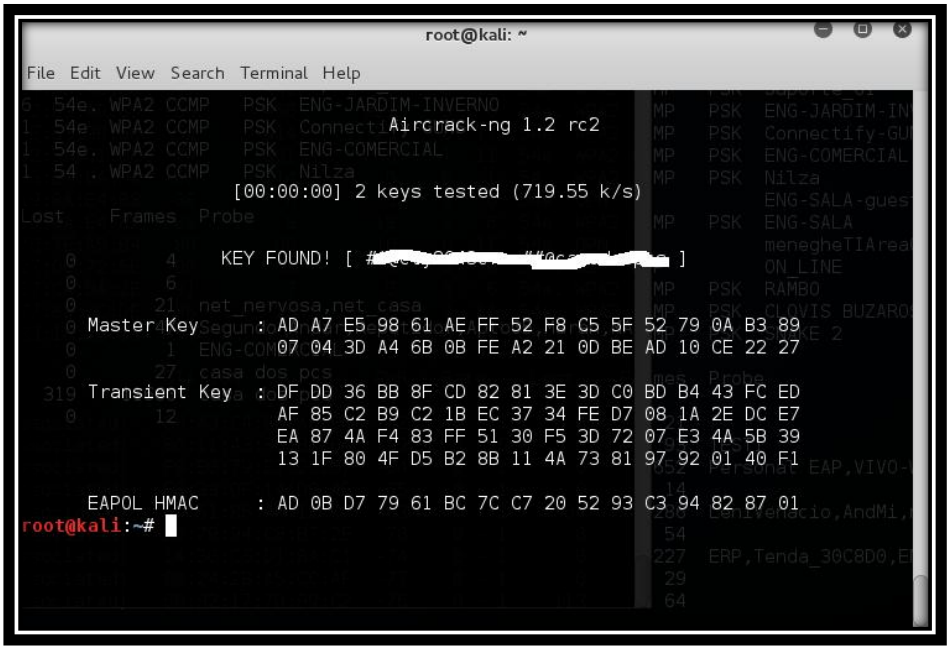

Figura 6 Ilustração do comando Aircrack-ng

Com base nos testes realizados pode-se concluir a Rede Wireless é muito vulnerável ainda, que esse tipo de tecnologia não é recomendado para transferência de dados confidenciais e também que o Kali linux é uma ótima distribuição GNU/Linux para se trabalhar com testes de vulnerabilidade, defesa, computação forense, entre outros.

Referência Bibliográfica

AIRCRACK-NG. **Aircrack-ng, Airodump-ng, Aireplay-ng, Airmon-ng.** Disponível em < http://www.aircrack-ng.org/doku.php?id=Main> . Acesso em 05/05/2015.

GALLO, Michael A.; HANCOCK, W. M. **Comunicação entre Computadores e Tecnologias de Rede.** São Paulo, 2003.

ERICSSON. **Mobility report on the pulse of the networked society**. Disponível em <http://www.ericsson.com/ericsson-mobility-report>. Acesso em 10/10/2015.

MORIMOTO, Carlos E. **Redes Guia Prática.** 1º edição. Porto Alegre: Sul Editores, 2010.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. 2ºedição. São Paulo: Futura, 2003.

LINUX, Kali. About the Kali Linux Distribution, 2013. Disponível em <HTTPS://www.kali.org/about-us/>. Acesso em 15/03/2015.

KIZZA, Joseph Migga. **A Guide to Computer Network Security**. University of Tenesse-Chattanooga, 2009. Disponível em <http://gen.lib.rus.ec/book/index.php?md5=B1B8800CCBF9798DD36542DADF60B0D6>. Acesso em 20/10/2015.

TANENBAUM, Andrew S. **Computer Networks**. 4º edição, New Jersey, 2003