Faculdade de Administração e Negócios de Sergipe

Associação de Ensino e Pesquisa “Graccho Cardoso”

Autorizada a funcionar por intermédio da Portaria Ministerial nº 2.246 de 19/12/1997

Pós-graduação MBA em Gestão de redes e Segurança da Informação

Junior, José Alexandre Oliveira

Graduado em Gestão de tecnologia da Informação - FANESE/Aracaju

Rede e Segurança da informação

Wi-fi residêncial, a porta está aberta

Aracaju

Sergipe – Brasil

2016.1

José Alexandre Oliveira Junior

Rede e Segurança da informação
Wi-fi residencial, a porta está aberta

Projeto apresentado como requisito para obtenção de aprovação do curso de pós Graduação MBA em Gestão de Redes e Segurança da Informação, da Faculdade de Administração e Negócios de Sergipe.

Aracaju
Sergipe – Brasil
2016.1

Resumo

Este projeto tem proposito de apresentar de forma clara e objetiva as vulnerabilidades que uma rede Wi-Fi residencial e comprovar mediante laboratório a existência de diversas ferramentas podem ser utilizadas para ataques ou invasão de redes, principalmente no âmbito residencial, onde na maioria das vezes, seja por negligencia imperícia ou desconhecimento, requisitos básicos de segurança não são cumpridos, abrindo assim uma porta de entrada para os invasores. Nesta pesquisa será comprovada a capacidade de ferramentas simples de parar serviços ou clientes, capturar senhas criptografadas e descoberta de senhas de rede circunvizinhas. O projeto não tem o objetivo expor o assunto de forma leviana e sim levar conhecimento da existência de ameaças mais comum do que imaginamos

Palavras - Chave: rede, Wi-Fi, invasão, laboratório, criptografia, Segurança e vulnerabilidades.

Abstract

This project has purpose to present a clear and objective manner the vulnerabilities that a home wi-fi network and prove by laboratory the existence of different tools can be used to attack or network intrusion , especially at the household level , where most of the time , either by negligence or malpractice ignorance , basic safety requirements are not met , thus opening a gateway for invaders .In this research will be proven the ability simply to stop services or client tools , capture passwords and encrypted discovery surrounding network passwords .The project has the objective to expose the subject lightly , but bring knowledge of the existence of common threats we imagine the.

SUMÁRIO

1. INTRODUÇÃO

Nos dias atuais, muitas de nossas tarefas dependem ou demandarão, em algum momento de tecnologia, para comunicação não é diferente, seja por meio telefônico ou internet está comunicação deverá ser feito através de uma rede, seja com fios ou sem fios, como tudo hoje em dia trafega através de uma rede, a demanda de informações e serviços é muito grande, com isso aumenta também seus problemas de segurança. O projeto visou pesquisar informações sobre a segurança de redes sem fios, principalmente no âmbito residencial, não que no mundo corporativo não seja vulnerável também, mas é afirmado isso, pelo fato de que nas redes residenciais tenham muito menos recursos de segurança do que nas empresas. O projeto está dividido em duas etapas onde na primeira apresentamos a parte conceitual e de históricos sobre redes na segunda parte será demonstrado um ataque na forma de prática de laboratório com ferramentas que são facilmente encontradas na internet.

A pesquisa tem como finalidade expor a vulnerabilidade de forma prática e existência de ferramentas de ataques a rede sem fios e comprovar a invasão, o intuito aqui não é incentivar as práticas delituosas de ataque e sim comprovar a vulnerabilidade da rede, justifica-se tal pesquisa, pelo grande números de pequenas redes wireless residenciais que podem ser atacadas por invasores com grande facilidade. Acredita-se que com as informações destacadas neste documento aumente-se o conhecimento e a conscientização sobre a importância da segurança até mesmo no âmbito residencial. Para o desenvolvimento da pesquisa foram realizadas pesquisas bibliográficas para levantamento das informação, dados recolhidos de forma qualitativa, laboratório prático e pesquisas na internet sobre o assunto relacionado. Um projeto como este é de grande relevância uma vez que não fica destinado não só para quem gerência ou administra uma rede, mas também para o usuário residenciais em geral. Este contribui para uma diminuição de ataques e vítimas dos invasores de redes, abordando de forma simples o tema que possivelmente para muitos é totalmente desconhecido.

2. REDES DE COMPUTADORES

2.1 Histórico Redes computadores

A rede de computadores foi iniciada por volta da década de 60, sendo que a comunicação que predominava na época era via estrutura telefônica transmitida através de comutação de por comutação de circuitos a uma taxa constante entre a origem e o destino.Com o aparecimento de microcomputadores que tinham um bom desempenho e baixos requisitos de temperatura e umidade, permitiu-se a instalação de um número de equipamentos em várias localizações, onde antes era feito em determinadas áreas, faltava então um meio de interligação entre estes dispositivos , com o surgimento da multiprogramação, começou ocorrer à necessidade de interligar estes computadores de modo que se pudessem compartilhar informações entre diferentes usuários e diferentes regiões, esta necessidade surgiu naturalmente pela espera de acontecimentos futuros.

Na busca de transformar a comutação de circuitos em uma comutação de pacotes, três grupos de pesquisa separadamente iniciaram seus estudos. Sendo o primeiro em 1961, onde Leonard Kleinrock nos laboratórios MIT usou a teoria das filas, a comutação de pacotes baseada no tráfego em rajadas. Já por volta de 1964 Paul Baran do Rand Institute começou a estudar o uso da comutação de pacotes para a segurança da transmissão de voz para redes militares, e na Inglaterra Donald Davies e Roger Scantlebury desenvolviam ideias sobre a comutação de pacotes no National Physical Laboratory, junto com Lawrence Roberts também no MIT lideravam o projeto de ciência de computadores na ARPA (EUA - Agência de Projetos de Pesquisa Avançada).

Em 1967 Robert publica ARPANET (a precursora da grande rede mundial- a Internet), sendo a rede de computadores por comutação de pacotes. Os primeiros comutadores de pacotes ficaram conhecidos como IMPs (interface message processors), processadores de mensagens de interface, sendo fabricados pela empresa BBN.

Em 1969 o primeiro IMP foi instalado na Universidade da Califórnia com três IMPs adicionais derrubando o sistema então com 4 nós. Em meados 1972 a ARPANET já tinha instalados 15 nós e foi publicamente apresentada por Robert Kahn na Conferência Internacional de Computadores. O primeiro protocolo de controle de rede deste sistema foi o NCP (network-control protocol), sendo elaborado também o primeiro programa de e-mail por Ray Tomlinson na BBN. Devido a ARPANET ser única na época era uma rede fechada e para se comunicar com suas máquinas era preciso estar ligado a um de seus IMPs.

Foto 1- primeiro IMP-Leonard Kleinrock

Entre os anos de 1990 e 1996 a ARPANET deixou de existir onde, a Milnet e a Rede de Dados de Defesa passaram a controlar maior parte do tráfego do Departamento de Defesa dos EUA e a NSFNET passou a ser o backbone de conexão entre os Estados Unidos e todas as redes do exterior, mas perdeu seu valor comercial em 1995, pois essa tarefa passou a ser Encargo dos provedores de Internet.

As redes de computadores passaram por uma longa evolução antes de chegar aos padrões que utilizamos atualmente. As primeiras redes foram criadas como uma forma de transferir informações de um computador a outro. Eram utilizados cartões perfurados para o transporte externo de dados que continham poucas dezenas de caracteres (figura 2). Apesar de ser um modo lento para a transmissão de dados, este recurso era de grande utilidade na época.

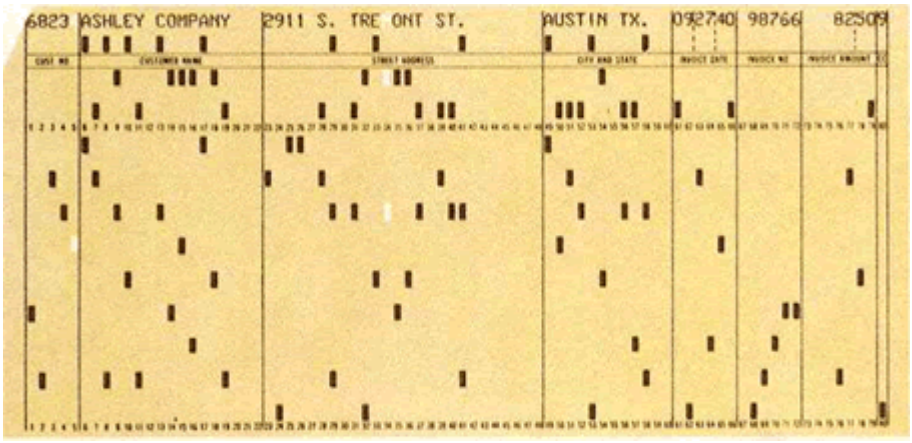

Figura 2 - Cartão utilizado na transmissão de dados década de 60

Fonte :Oliveira, 2008

2.2 Rede sem fio

As redes sem fio ou wireless (WLANS) surgiram da mesma maneira que muitas outras tecnologias de redes; no meio militar. Havia a necessidade de implantação de um método simples e seguro para troca de informações em ambiente de combate. Com o passar do tempo e evolução das tecnologias estas deixou o meio de ser restrito apenas ao meio militar e se tornou acessível a empresas e residências, Nos dias de hoje vemos as redes wireless como uma alternativa bastante interessante em relação as redes cabeadas, mesmo com seu custo um pouco elevado e relação àquela. De variadas aplicações e sua principal característica é a mobilidades e o fato de ter a mobilidade como principal característica, tem facilitado sua aderência, principalmente nas organizações.

Uma rede sem fios ou wireless lan (WLAN) é uma rede local sem fio padronizada pelo IEEE 802.11conhecida também pelo nome de WiFi, abreviatura de wireless fidelity (fidelidade sem fios) esta marca registrada pertencente à Wireless Ethernet Compatibility Alliance (WECA). (TELECO 2008).

O funcionamento desse tipo de rede é bem parecido com as redes cabeadas, utilizam o TCP/IP com protocolo de transmissão e também possuem um conjunto de parâmetros adicionais a diferença é que para comunicação não são utilizados cabos físicos.

2.3 Segurança em redes sem fio

Como qualquer outro meio de comunicação a rede sem fios necessita de também de mecanismos de segurança. Nas redes cabeadas, as informações transitam de forma através de algum componente da rede já na rede sem fio, basta que se tenha uma antena que transmita e receba os sinais para que a comunicação seja feita, nestes dois casos caso não tenha segurança. Em razão, inicialmente o protocolo utilizado para resolver esse problema foi desenvolvido o protocolo Wired Equivalent Privacy (WEP), ou Privacidade Equivalente com Fio. Esse protocolo está presente em todos os produtos que estão no padrão Wi-Fi.

Para colocar segurança nas redes sem fio Wi-Fi, inicialmente foi projetada a chave de criptografia WEP. Mas, com o passar dos anos está passou a perder a credibilidade por não ser mais segura onde muitos programas são capazes de encontrar a chave WEP das redes sem fio e, consequentemente, isso torna a rede vulnerável. Para suprir está vulnerabilidade, foi criada a chave de segurança WPA, uma evolução da WEP, Esta permite fazer a criptografia por TKIP e EAP. Apesar de não haver limitação na chave WPA, foi criada também a chave WPA2, que fornece maior segurança em redes sem fio.

Rufino (2005, p. 36), Define: WEP é um protocolo que utiliza algoritmos simétricos; portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifraras mensagens trafegadas". Os critérios que foram levados em consideração para o desenho do protocolo foi ser suficientemente forte, autos sincronismo requerer poucos recursos computacionais, exportável e de uso opcional.

Com o aparecimento de diversos problemas de segurança com o protocolo WEP foi desenvolvido o WPA Wi-Fi Protected Access, ou Acesso Protegido sem Fio

De acordo com a Linksys (2011), a WPA usa criptografia de chave de forma dinâmica, o que significa que essa chave muda constantemente tornando a invasão de uma rede sem fio mais difícil do que a WEP. A WPA é considerada um dos mais altos níveis de segurança sem fio para a rede e é recomendada se os seus dispositivos suportarem esse tipo de criptografia. Os roteadores mais novos podem oferecer segurança WPA2 onde está é compatível com a WPA, mas com um maior nível de segurança. Para a Linksys (2011), está cumpre os altos padrões de muitos órgãos governamentais. Se o roteador e o computador suportarem WPA2, esta é uma criptografia que deverá ser escolhida.

O protocolo WPA2 é como se fosse a segunda geração do protocolo WPA, sendo que esta não foi criado solucionar imitações do WPA prova isto que ele é compatível com versões

anteriores de produtos que suportam WPA. A principal diferença entre os dois é que a WPA2 exige AES (Advanced Encryption Standard) para criptografia de dados, enquanto a WPA original usa TKIP.

A implantação das redes sem fio trazem muitas vantagens, e em alguns casos é se torna-se inevitável. É fundamental importância que o administrador de rede ou usuários domésticos entendam as implicações de segurança de cada escolha na configuração das redes Wi-Fi. A IEEE é responsável por definir as faixas de endereço MAC que os fabricantes colocam nas interfaces de redes. Esse controle é feito para não haver interfaces de redes com o mesmo endereço MAC. Logo, o endereço MAC de sua interface de rede é único na internet essa característica fornece muita segurança em redes sem fio ao cadastrar o endereço MAC das estações de trabalho no roteador sem fio.

As normas (NBR ISO/IEC 27002:2005) Define segurança da informação como a proteção das informações quanto a vários tipos de ameaças, de modo a garantir a segurança do negócio, minimizando o risco para o negócio, maximizando o retorno sobre o investimento e as oportunidades de negócio. Para que seja utilizada, a informação necessita garantir quatro modelos fundamentais: a integridade, disponibilidade, confidencialidade e a autenticidade características estas que devem ser preservadas, pois são regidas como princípios da segurança da informação:

A **integridade** que é a garantia da exatidão e completeza da informação e dos métodos de processamento. Então a integridade está ligada a garantia de que a informação não seja modificada, alterada ou destruída sem autorização durante o seu manuseio ou armazenamento, e a certificação de que ela seja legítima e permaneça consistente. Está quebra ocorre quando a informação é corrompida, falsificada, roubada ou destruída. Garantir que isto não ocorra e manter a informação na sua condição original. Diversos fatores contribuem para a perda da integridade: inserções, substituições ou exclusões de parte do conteúdo da informação, que podem se ocasionadas por alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alterados para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

A **disponibilidade** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005). ocorre a não disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que for necessário utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito armazenamento da informação.

A **Confidencialidade** é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada (ISO/IEC 17799), é garantir que a informação só será disponível aqueles que tiver permissão de acesso, na informática está segurança é dada através de técnicas de criptografia.

A **Autenticidade** é a garantia que a informação provem de uma fonte legitima, e não sofreu mudanças ao longo do processo de recebimento do emissor.

3. LABORATÓRIO ATAQUE À REDE VULNERÁVEL

No início falamos das inúmeras vantagens de uma rede sem fio (Wireless), como foi dito acima no resumo mas toda tecnologia criada pelo homem tem falhas estas podem ser exploradas de diversas formas, tudo que se precisa é de tempo e algumas ferramentas. Como são desenvolvidos softwares para o bem outros podem ter o objetivo para o mal, esses podem ser poderosos e capazes de quebrar até as mais complexas senhas e criptografias causando problemas graves a suas vítimas tanto na sua casa e em grandes corporações mesmo com as criptografias, mas conhecidas e consideras as mais seguras pelos seus desenvolvedores. Os sistemas Windows de Código fechado não são muito usados para criação de ferramentas de ataques, ao contrário de sistemas Linux de código aberto, onde programadores desenvolvem algumas versões com finalidade de realizar testes de penetração em redes desprovidas de uma segurança razoável, mesmo assim sendo vulnerável a alguns tipos de ataques realizados via software.

3.1 O Pacote Backtrack Linux

Para desenvolvimento dos trabalhos utilizamos uma versão desenvolvida em Debian 7, chamada backtrack Linux na sua Versão 5, pacote com mais de 300 ferramentas 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 SecurityWireless Professional, certificações oferecidas pela Offensive Security que mantém o BackTrack, outra ferramenta que agiliza o processo à virtualização de softwares , onde permite que o sistema operacional opere dentro de uma outro que já instalado, dispensado uma nova instalação , o hardware pode ser

compartilhado para os dois operacionais simultaneamente , neste laboratório foi utilizada as ferramenta Vmware Player, mas existem outras ferramentas de virtualização que atendem bem.

Figura 3 - logo do Backtrack Linux Ver 5.

Reaver é uma ferramenta de ataque robusta e prática contra WPS, e foi testado com uma ampla variedade de access points e implantações de WPS. O Reaver implementa um ataque de força bruta contra PINS de redes sem fios com Wifi Protected Setup (WPS) a fim de conseguir as senhas WEP/WPA/WPA2. Na média reaver irá conseguir a senha de acesso dos APS em texto puro em cerca de 4 a 10 horas, dependendo do Access Point, Na prática, irá levar metade desse tempo para adivinhar o PIN WPS correto e conseguir a senha acesso. WPS (Wi-Fi Protected Setup), quando habilitado facilita a configuração de uma nova rede sem fio por meio de um assistente que acessa o roteador e define senha e nome da rede, por exemplo, de acordo com as solicitações do usuário. O recurso está disponível em muitos roteadores vendidos e vem em 90% dos casos habilitado, de posse do código do WPS, um hacker pode obter acesso ao software de configuração do roteador. Isso permite desabilitar a proteção da rede e até mesmo trocar a senha, para que o acesso seja feito livremente essas mudanças podem causar uma série de problemas.

O Aircrack-ng é uma poderosa ferramenta para quebra teste de senhas de redes Wireless, com o tipo de autenticação WEP/WPA/WPA2, na verdade está é um detector de redes.

Sniffer é uma ferramenta de análise para redes locais sem fios 802.11. Funciona com qualquer placa Wireless cujo driver suporta modo de monitoramento bruto e pode capturar e analisar (sniff) tráfego 802.11a, 802.11b e 802.11g está roda no GNU/Linux.

Aireplay-ng A função principal é gerar tráfego para uso posterior no aircrack-ng para quebrar chaves WEP e WPA-PSK, WPA2-PSK. Existem ataques diferentes que podem causar des autenticações com o propósito de capturar dados de wpa handshake WEP/WPA/WPA2 autenticações falsas, repetição de pacote interativo, injeção de ARP request forjados e reinjeção de ARP Request.

Airodump-ng é usado para captura de pacotes de frames brutos 802.11 e é particularmente apropriado para coletar IVs (Vetores de Inicialização) WEP/WPA/WPA2 com intuito de usá-los com o aircrack-ng. Se você tem um receptor GPS conectado ao computador, airodump-ng é capaz de registrar as coordenadas dos Access Points encontrados. Suplementarmente, airodump-ng cria um arquivo de texto (também chamado de (dump) contendo os detalhes de todos os Access Points e clientes vistos. Como foi dito acima precisamos instalar uma máquina virtual.

Para este laboratório utilizaremos software de virtualização Vmware Player que pode ser baixado de graça em **http://www.vmware.com/br/products/player**, depois de instalado devemos baixar a imagem Backtrack Linux versão 5 em **http://www.backtrack-linux.org/backtrack**, como ele é um live cd tanto você pode realizar a instalação total ou apenas, gravar em um dvd e rodar o sistema dele sem precisar perder tempo com a instalação completa, em 99% dos casos a placa de rede onboard no caso de notebooks não é reconhecida pela máquina virtual onde teremos que realizar os testes placa de rede Wi-Fi externa usb nos testes usamos D-Link zwa125, após tudo instalado abrimos o VMware Player, e subimos imagem da máquina virtual já pronta, procurando o local onde foi feito o download.

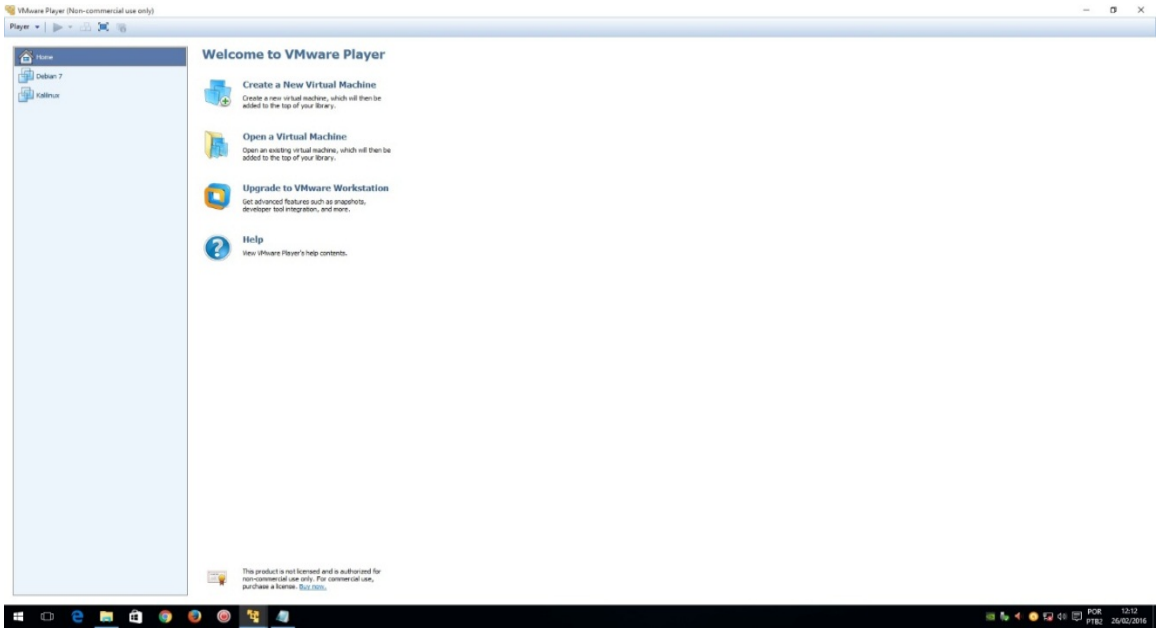

Imagem 4- Software de virtualização.

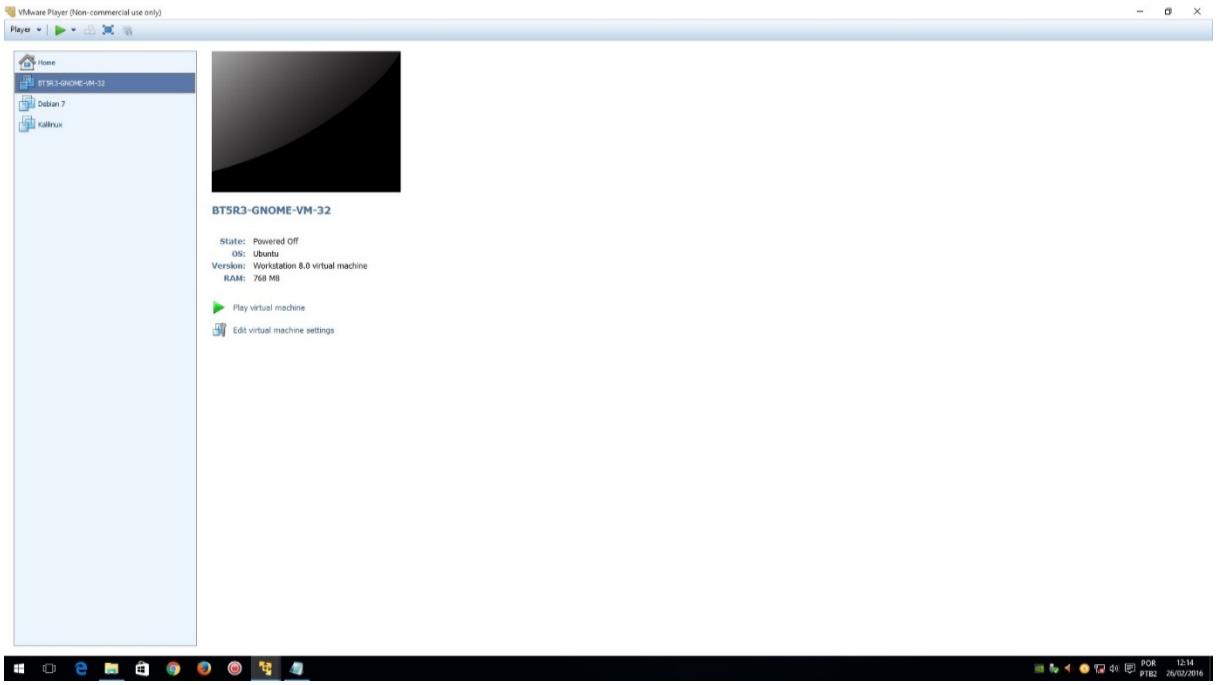

Imagem 5 - Software de virtualização.

Depois de acionarmos o play na virtual correspondente o sistema operacional da virtual será carregado entrando em estado de pronto. **login-root e senha-toor.**

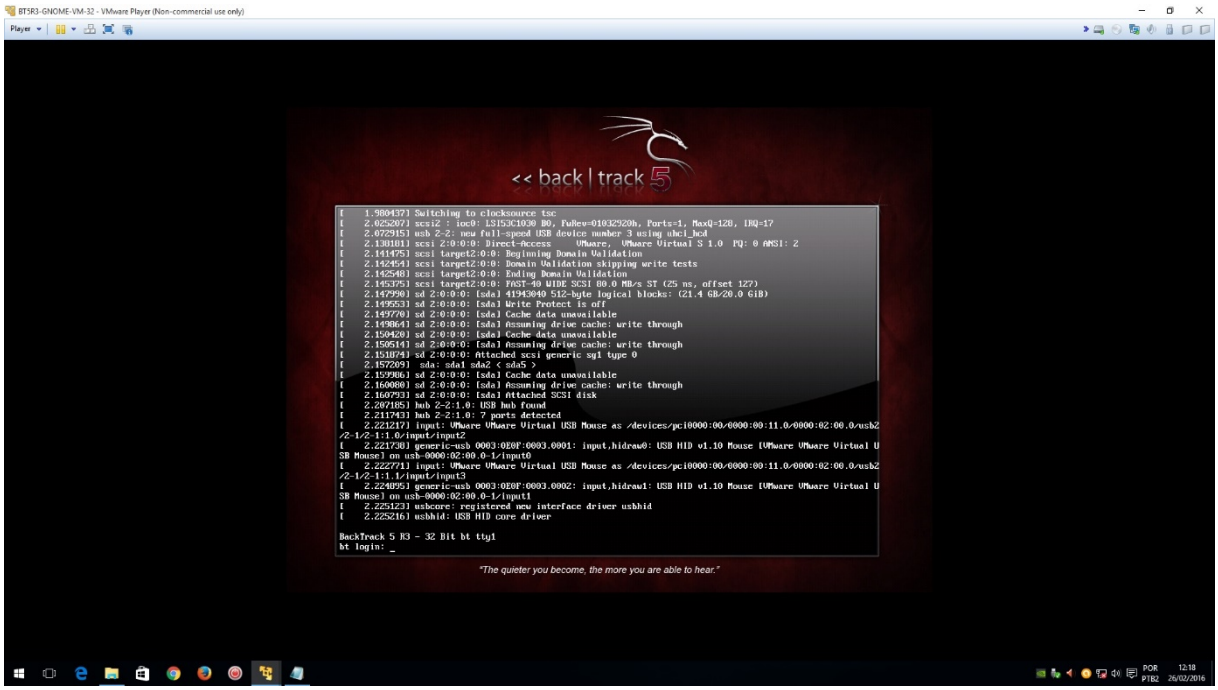

Imagem 6 - Subindo a imagem do backtrack Linux versão 5.

Imagem 7 - Tela inicial backtrack Linux versão 5.

Ao abrirmos o terminal digitamos o comando **ifconfig** para identificarmos as conexões de rede , abaixo está **wlan0** placa que será usada para a realização dos testes, em seguida o comando **airmon-ng start wlan0**,depois outro comando **airodump-ng mon0,** fará

que a placa entre em modo monitor identificando todas as redes sem fios que estiverem disponíveis em seu alcance, digitando ctrl+c para parar o serviço a qualquer momento, abrimos outro Terminal, escolhemos uma rede denominada *"**Pegue Vírus**"* que apareceu no espectro e que não sabemos de quem provavelmente de algum local próximo do local onde estamos realizando os testes , copiado o BSSID da rede, digitado o comando **reaver -i mon0 -b BSSID da rede -vv** o aplicativo reaver vai mandar um ataque de força bruta ao roteador até descobrir o pin do wps e com ele a senha da rede, este processo é demorado podendo levar horas, lembrando que ele só funciona se a opção estiver ativada no roteador, infelizmente 90% dos roteadores vendidos no mercado vem com o wps ativo, e o usuário comum não sabe desabilitar.

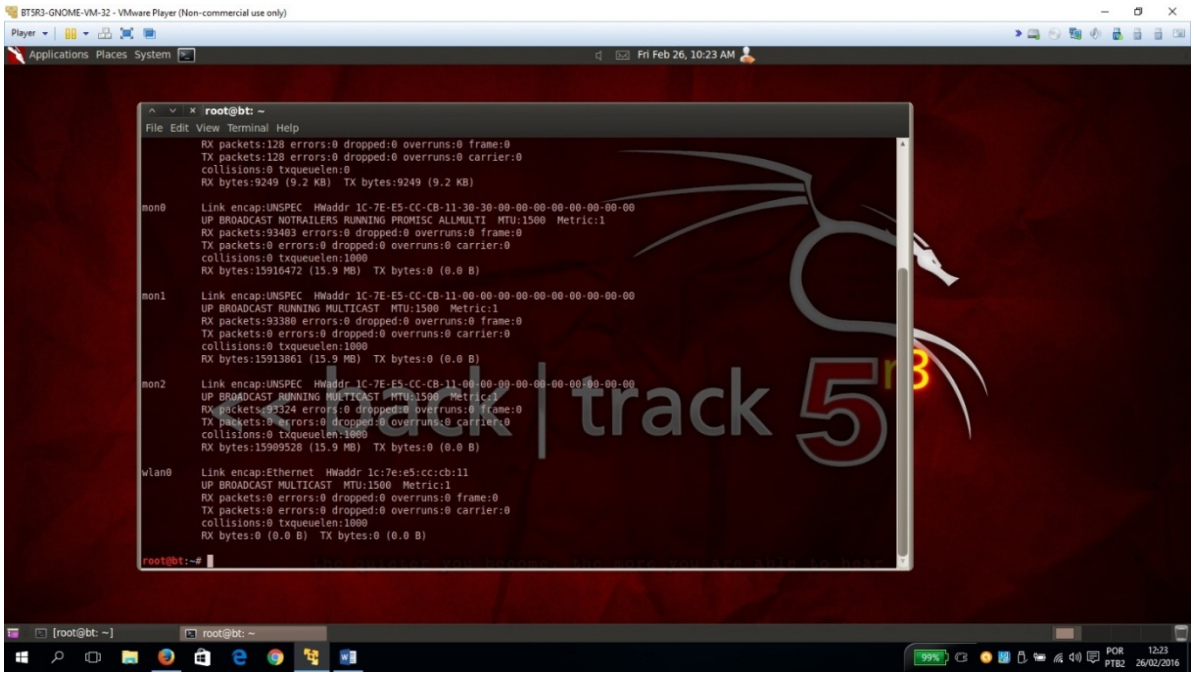

Imagem 8 - Tela resultado do comando ifconfig.

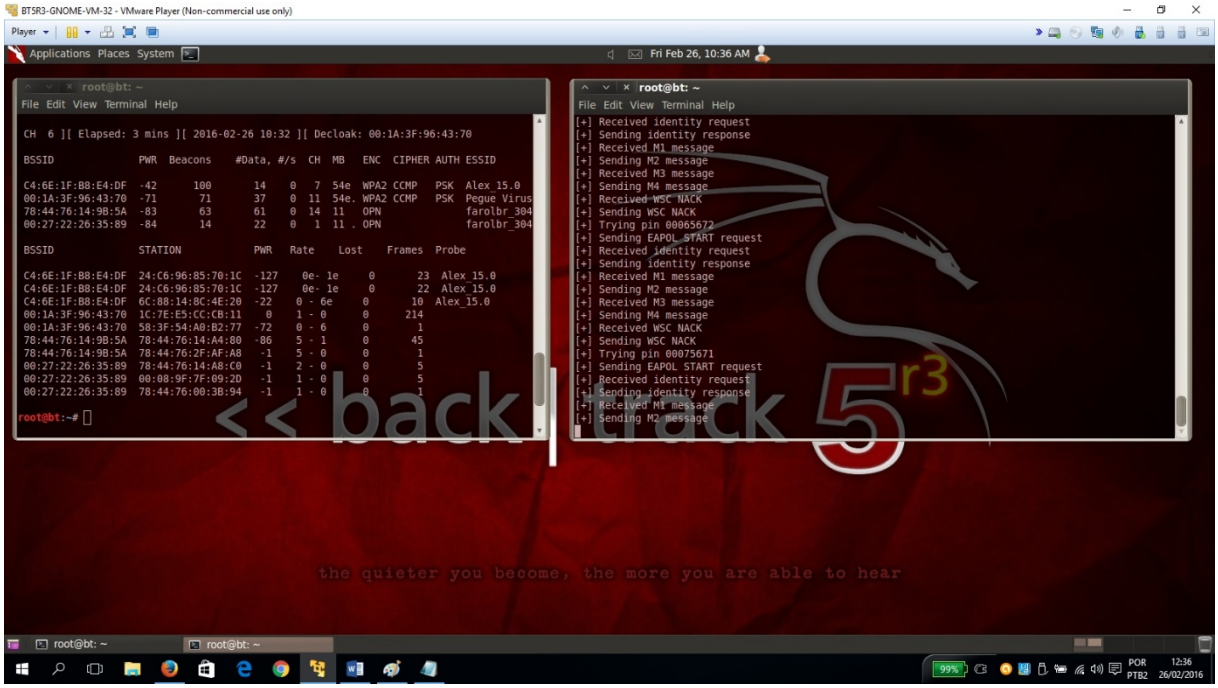

Imagem 9 - Backtrack Linux versão 5 monitorando as redes disponíveis e realizando o ataque.

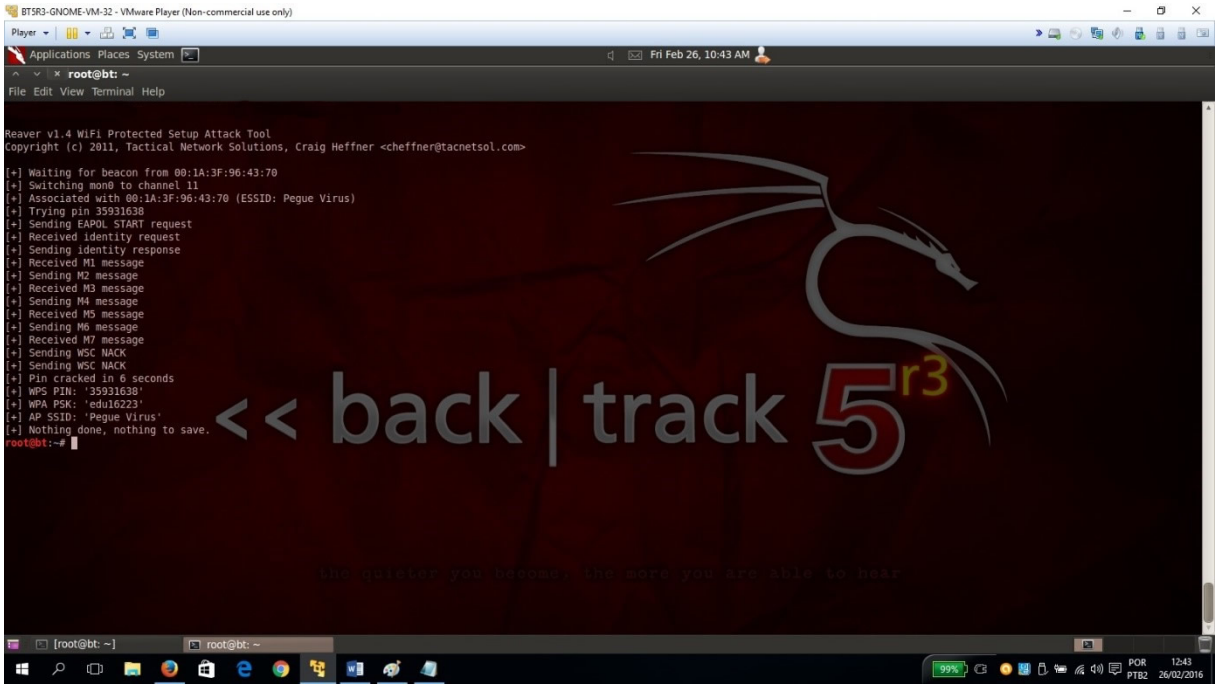

Imagem 10 - Backtrack Linux versão 5 demonstrando a senha.

Depois de finalizado o processo na última linha está apareceu lá o WPS pin **35931638**, WPA PSK **edu16223**, AP SSID Pegue Vírus. Como podemos ver, a segurança e WPA PSK2 que hoje é a mais segura, o aplicativo levou certa de 03 horas, trazendo os resultado com sucesso, existem processos que podem demorar até mais de 24 horas. No exemplo seguinte

vamos utilizar o aplicativo **aireplay-ng,** com este comando podemos derrubar um roteador sem estar na conectado a sua rede sem fio ou apenas desconectar algum dispositivo que estiver conectado a este roteador.

3.2 Derrubando o serviço

Na imagem abaixo está o roteador do nosso laboratório ainda sem rodar o comando, vejamos a marcação em verde, o status de normalidade de comunicação do aparelho, onde após o comando **aireplay-ng -0 100 -a BSSID da minha rede mon0** caiu o sinal para 0 e abaixo nas conexões de rede mostra a mensagem sem acesso à internet.Com este comando , invasor mal intencionado consegue deixar até um provedor e todos os seus clientes fora da rede infelizmente o Backtrack Linux versão 5 é desconhecido por muitos administradores de redes.

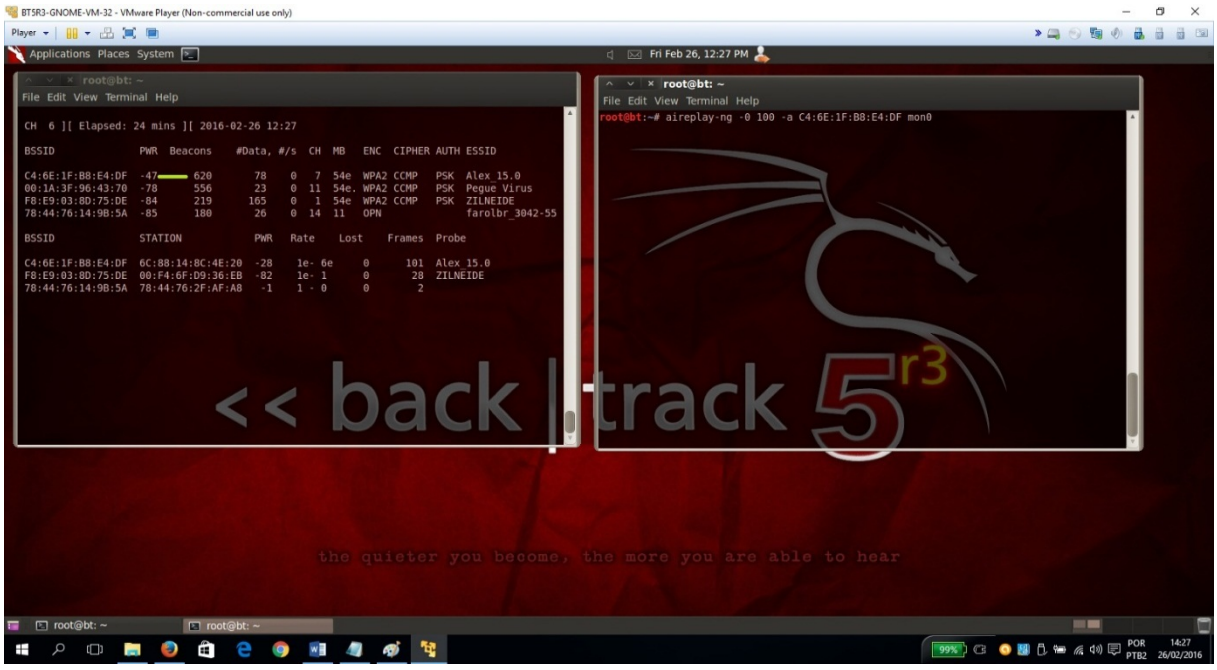

Imagem 11 - Backtrack Linux versão 5 rede Alex_15.0 normal em -47 PWR.

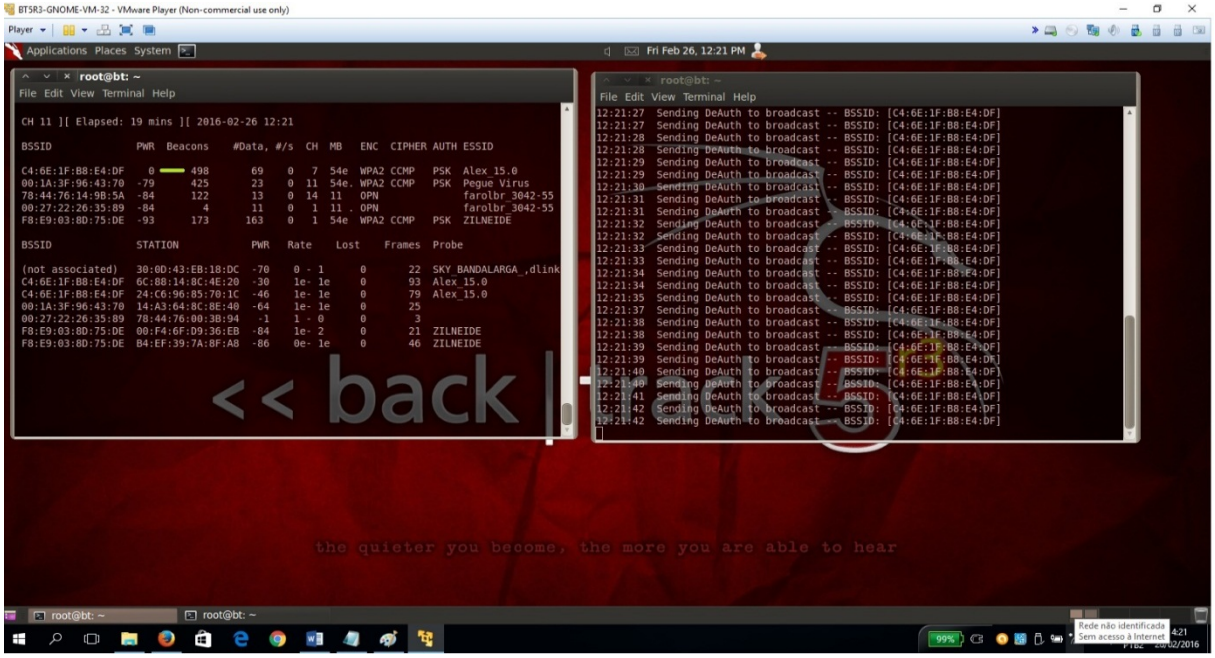

Imagem 12 - Backtrack Linux versão 5 rede Alex_15.0 em 0 PWR.

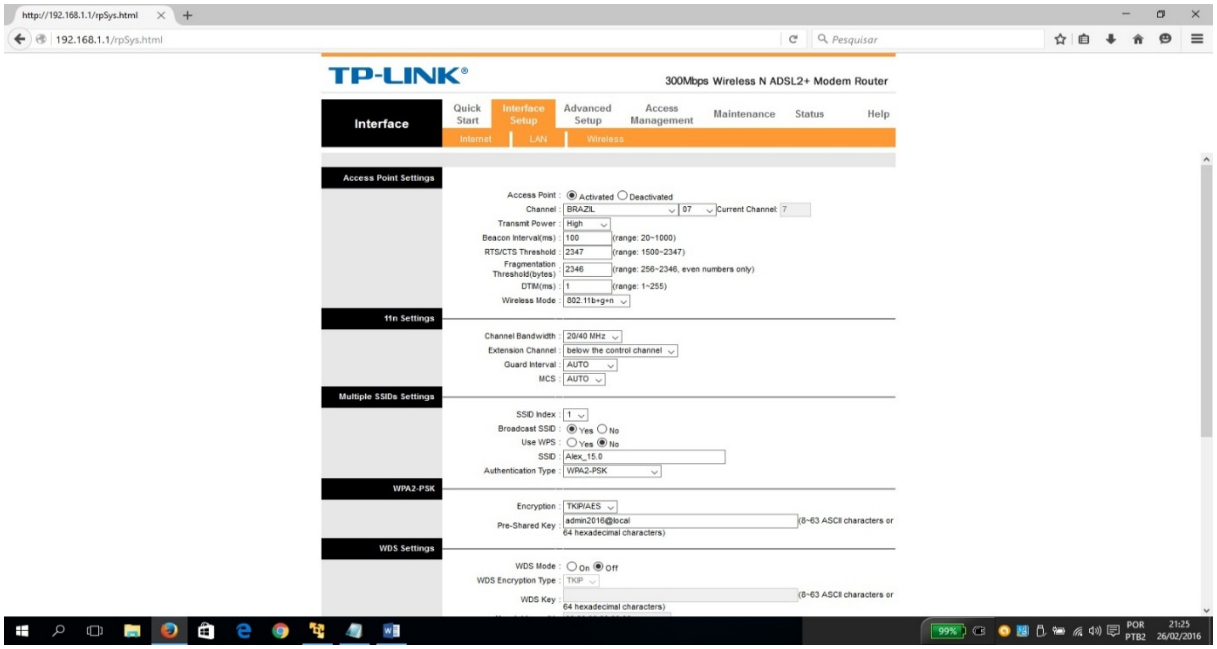

Imagem 13 – Roteador a ser atingido.

3.3 Capturando senhas criptografadas

Agora vamos utilizar o airodump-ng em conjunto com o aircrack-ng, com objetivo de o primeiro forçar a captura de pacotes para conseguir o arquivo chamado wpa handshake onde ficam as senhas criptografadas em seguida entra o aircrack-ng , este utiliza uma lista de senhas chamadas wordlists criadas pelo programa **crunch** que existe no Backtrack Linux versão 5, que usando o processamento do computador quebra a criptografia das senhas, este procedimento pode levar horas ou dias, facilmente são encontradas na internet listas enormes de 20,30 até 100gb de tamanho, vamos demonstrar abaixo o programa em execução, criamos uma wordlist.txt, e propositalmente colocamos a senha da minha rede do laboratório Wi-Fi, pois este processo levaria dias ou semanas e queremos só comprovar os dois aplicativos operando em conjunto. Utilizaremos o comando **airodump-ng mon0** no terminal para monitorar as redes sem fio ao alcance da nossa placa de rede, copiamos o BSSID no caso vai ser da rede do laboratório “rede Alex_15.0”, usamos o comando **airodump-ng mon0 –bssid da rede –channel canal --write teste**, ele vai desautenticar os clientes conectados ao roteador no caso de celulares e laptops, e captura o arquivo wpa handshake, salvar com o nome teste.cap na pasta do root, e quebrar com o aircrack-ng depois.

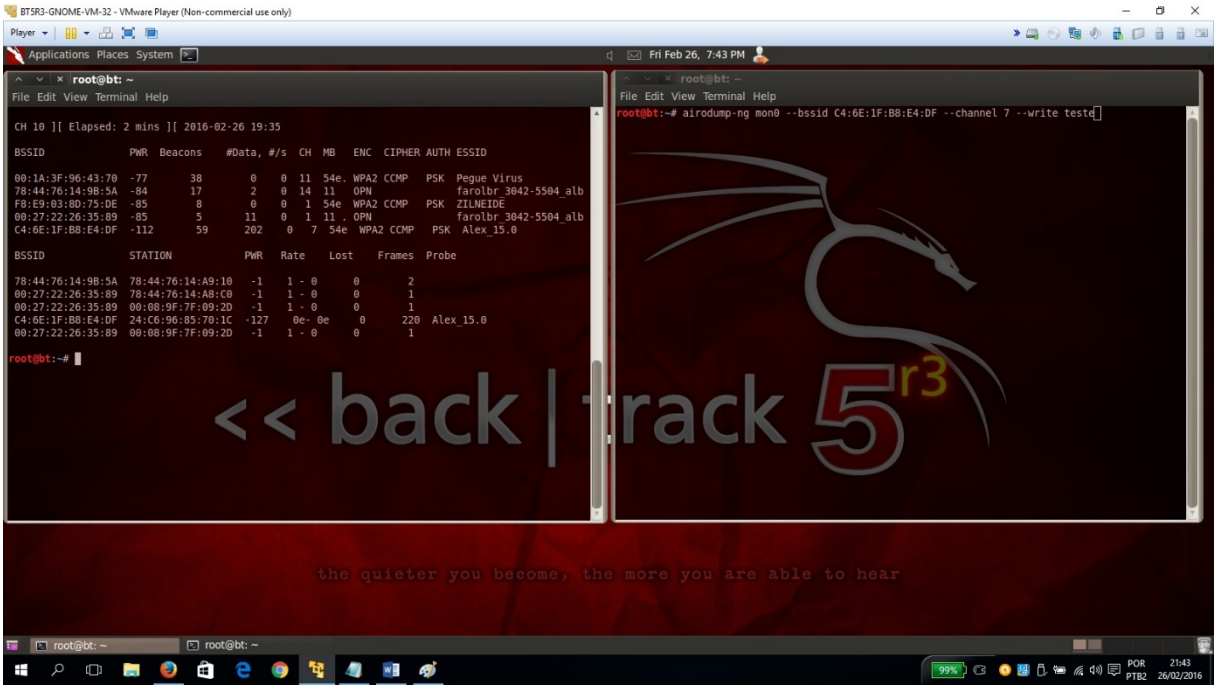

Imagem 14 - Backtrack Linux versão 5 capturando o arquivo wpa handshake.

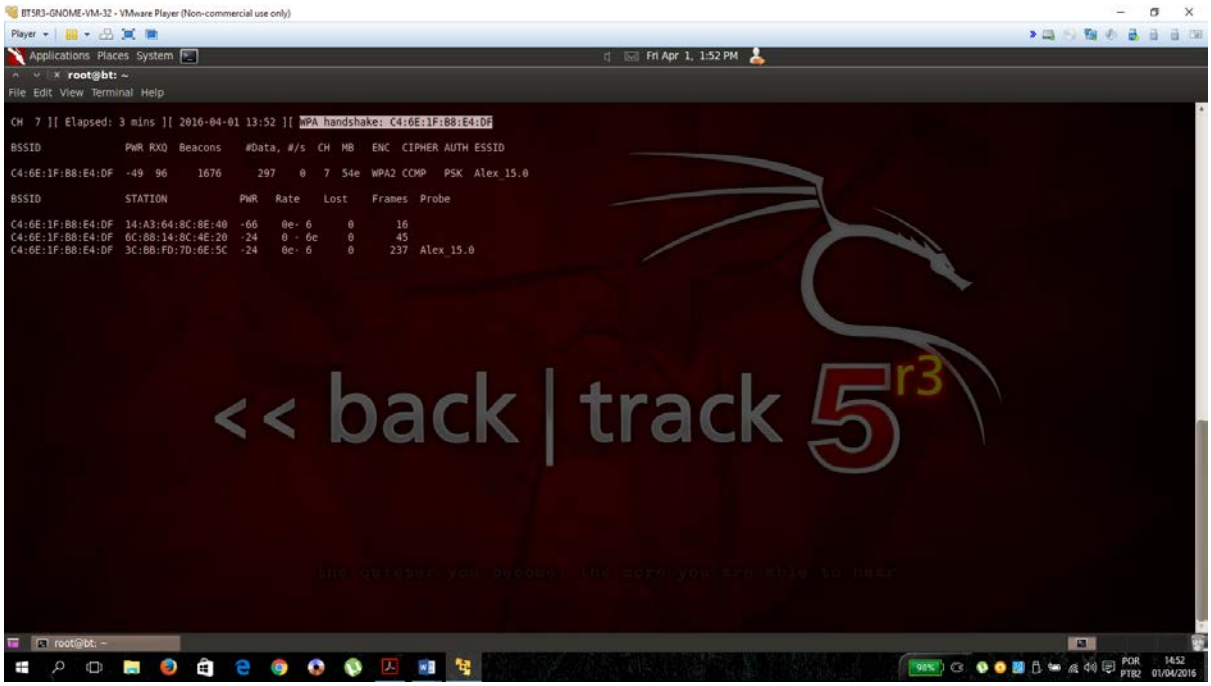

Imagem 15 - Backtrack Linux versão 5 com o arquivo wpa handshake capturado.

Na tela, o arquivo wpa handshake capturado no procedimento, depois vou rodar os comandos juntos o comprovar a quebra da senha, com o comando **aircrack-ng -wordlist.txt -teste.cap**, no terminal, localizando os arquivos na pasta, do root.

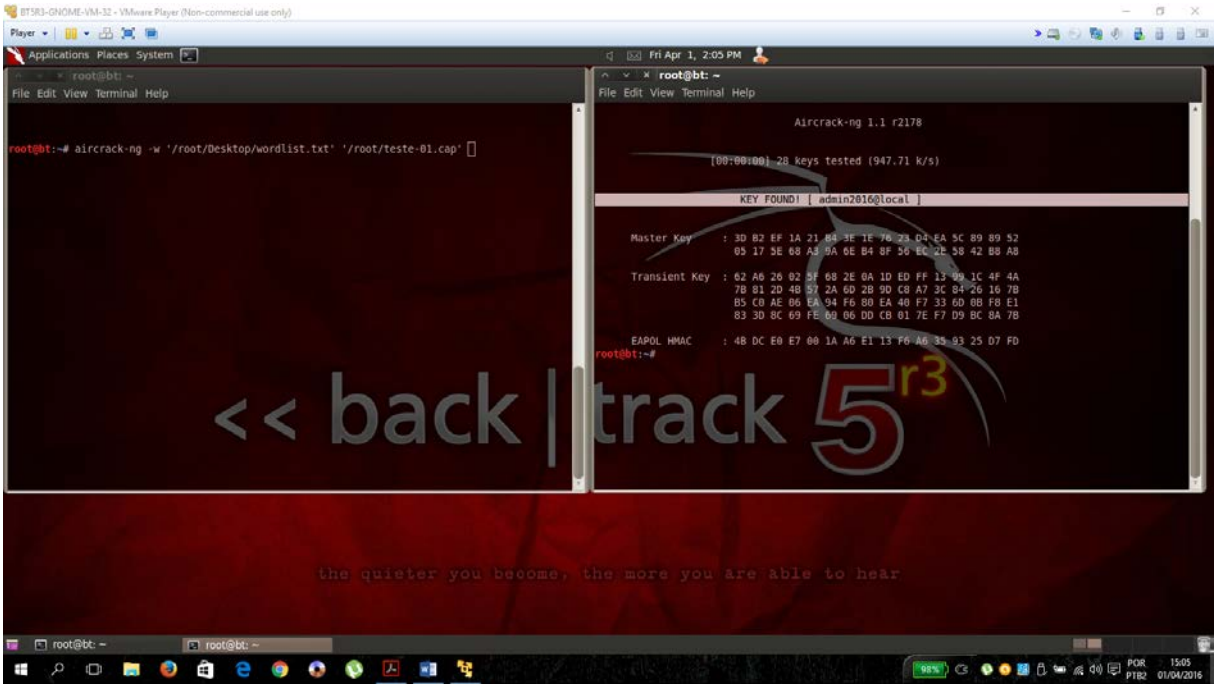

Imagem 16 - Backtrack Linux versão 5 revelando a senha do wpa handshake.

4. CONSIDERAÇÕES FINAIS

O documento abordou o assunto demonstrando e comprovando a vulnerabilidade da rede sem fio, como qualquer outra rede, vulnerabilidades não deixaram de existir, porém este documento vem para conscientizar e expor a existência de ameaças que podem prejudicar em muito o funcionamento das redes. O projeto alcançou as expectativas comprovando nos testes feitos em laboratório e em uma rede desconhecida que possibilitou que a ferramenta quebrasse a criptografia WPA2 PSK de proteção a redes , considerada mais segura do mercado, segundo seus desenvolvedores, então devemos atualizar nossos roteadores, as atualizações mas atuais disponibilizadas pelos fabricantes, investir pesado em tecnologias de segurança no caso de grandes corporações, colocar senhas mas complexas e conectar menos dispositivos moveis aos nossos roteadores, pois eles são o ponto mas franco no caso a porta de entrada as nossas redes, podendo causar pequenos problemas em redes caseiras e até mesmo graves danos em redes corporativas.

REFERÊNCIAS

Braga, Pedro Henrique da Costa- **Técnicas de Engenharia Social** A GRIS - Grupo de Resposta a Incidentes de Segurança -Cidade Universitária - Rio de Janeiro/RJ. Acessado 01/11/2015.

CARDOSO JÚNIOR, Walter Felix. **Inteligência empresarial estratégica**. Tubarão:Ed. Unisul, 2005. Acessado 01/01/2016.

Dantas, Marcus Leal- **Segurança da informação**: uma abordagem focada em gestão de riscos. / Marcus Leal Dantas. – Olinda: Livro Rápido, 2011. Acessado 01/10/2015.

D. Zisiadis, S. Kopsidas, A. Varalis and L. Tassiulas. "**Enhancing WPS** security", 2012. Acessado 04/04/2016.

GIAVAROTO, Sílvio César Roxo. SANTOS, Gerson Raimundo dos Santos - **Backtrack Linux-Auditoria e teste de invasão em redes de computadores**, Rio de Janeiro :Editora /Ciência Moderna LTDA ,2013. Acessado 15/03/2016.

https://www.oficinadanet.com.br/post/10123-**historia-das-redes-de-computadores.**Acessado em 29/01/16.

http://www.juliobattisti.com.br/tutoriais/paulocfarias/**redeswireless001**.asp Acessado em 29/02/2016.

http://www.psafe.com/blog/**inseguranca-grande-paradoxo-internet-das-coisas/** Acessado em 14/08/2015.

https://pt.wikipedia.org/wiki/Perfil_**(comunidade**)acessado em 22/02/16.

http://convergecom.com.br/tiinside/seguranca/mercado-seguranca/03/07/2015/**brasil-continua-como-maior-vitima-de-ataques-de-phishing/** Acessado 10/03/2016.

http://www.cin.ufpe.br/~pasg/gpublications/efs10-conic.pdf - **Segurança em redes sem fio IEEE 802.11 integridade de dados, autenticação e confidencia.** Acessado 04/04/2016.

J. F. Kurose and K. W. Ross. "**Redes de Computadores e a Internet**. Uma abordagem Top-Down 5th ed.", 2010. Acessado 04/04/2016.

Livro Wireless Hacking - **Ataque e Segurança de Redes Sem Fio Wi-Fi** 2013 Autor Marcos Flávio Araújo Assunção, Editora Visual Books. Acessado 01/03/2016.

PEIXOTO, Mario C. P- **Engenharia social e segurança da informação na gestão corporativa**. Rio de janeiro: Brasport, 2006. Acessado 01/01/2016.