INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO – CAMPUS PARACATU

CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

ELIZAR SEVERINO BOTELHO

ANÁLISE DE VULNERABILIDADES EM REDES WLAN DOMÉSTICA COM SOFTWARES LIVRES

PARACATU - MG

2016

ELIZAR SEVERINO BOTELHO

ANÁLISE DE VULNERABILIDADES EM REDES WLAN DOMÉSTICA COM SOFTWARES LIVRES

Artigo apresentado à disciplina de Segurança de Redes do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal do Triângulo Mineiro – Campus Paracatu, Prof. Roitier Campus Gonçalves.

PARACATU - MG

2016

ANÁLISE DE VULNERABILIDADES EM REDES WLAN DOMÉSTICA COM SOFTWARES LIVRES

Elizar Severino Botelho

Resumo: Esse artigo tem como objetivo o aprendizado sobre redes WLAN domésticas, bem como conhecer suas principais fragilidades e formas de se prevenir à elas. Neste trabalho é demonstrado algumas estatísticas de fragilidade sobre WLANs domésticas, algumas vulnerabilidades nas WLANs por causa das fragilidades dos roteadores, algumas ferramentas em software livre usadas nos ataques, demonstradas duas técnicas de ataque a roteadores, algumas dicas de como se prevenir à esses ataques, os resultados dos testes de ataque e considerações finais em relação a introdução e os resultados dos testes.

Palavras-chave: vulnerabilidades, redes WLAN, softwares livres, testes.

Abstract: This article aims at learning about home WLAN networks, as well as knowing their main weaknesses and ways to prevent the them. This paper shows some statistics of weakness on domestic WLANs, some vulnerabilities in WLANs because of the weaknesses of the routers, some free software tools used in the attacks, demonstrated two attack techniques the routers, some tips on how to prevent to these attacks, results of attack tests and final considerations regarding the introduction and test results.

Keywords: vulnerability, WLAN networks, free software, tests.

SUMÁRIO

1 INTRODUÇÃO

Estamos vivendo a era do conhecimento, e para se gerar conhecimento é necessária a absorção de informações por parte das pessoas e organizações, assim sendo, o grande tesouro do momento que todos buscam incansavelmente precisa estar acessível, essa acessibilidade gera lucro e desenvolvimento, não só nos referimos a lucro financeiro, mas principalmente lucro intelectual. O compartilhamento globalizado das informações se deve ao grande avanço das redes de telecomunicações. Em específico as redes de computadores é o maior canal de distribuição das informações existente hoje, e as redes locais são cada vez mais necessárias para o desenvolvimento das empresas, órgãos públicos e da sociedade em geral com as redes domésticas.

> Com o avanço da internet e as novas tecnologias da informação a interligação entre computadores se tornou cada vez mais necessária. A evolução das redes de computadores fez com que aumentasse a necessidade de comunicação entre os mais distintos dispositivos, não somente entre os dispositivos fixos, mas também entre os dispositivos móveis (OLIVEIRA, 2010, p. 12).

Na construção de uma rede local, a escolha por uma rede sem fio (WLAN) demonstra uma superior vantagem ao se comparar com uma rede cabeada, com relação a custo, a facilidade de instalação, a mobilidade dos equipamentos, a facilidade de expansão entre vários outros fatores. Porém, a facilidade traz consigo fatores críticos de segurança em relação à vulnerabilidade dessas redes. Para que as informações trafegadas numa rede estejam seguras, devem ser respeitados cinco requisitos básicos: Confidencialidade; Integridade; Disponibilidade; Não repúdio; Autenticidade.

> Por definição, essa norma define a segurança da informação como: Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (DANTAS, 2011, p. 11).

Buscando o melhor aproveitamento das redes locais sem fio, para que a informação continue a ser trocada de uma forma segura, e ainda, que empresas ou pessoas físicas não venham a ter prejuízos financeiros ou morais por causa de uma falsa sensação de segurança ao usar suas WLANs, os testes frequentes nessas redes e o emprego de técnicas de segurança para prevenção de ataques e fraudes se fazem necessários.

Uma pesquisa desenvolvida no ano de 2014 pela empresa Avast Software revela números alarmantes com relação à segurança de redes WLAN domésticas, como mostra a tabela 1, foram avaliados 18.000 domicílios que possuíam redes WLAN (Avast Software, 2014).

Tabela 1. Riscos em redes WLAN domésticas.

Percentual	Risco/Problema
80%	Estão sob risco de ataque nos roteadores wireless
+ 50%	Roteadores usam configuração padrão e senhas fracas
30%	Usam dados pessoais como senhas
- 25%	Acreditam que suas redes domésticas estão seguras
25%	Informaram que foram vítimas de ataques de hackers
28%	Preocupam-se com o roubo de informações confidenciais
28%	Estão preocupados com a perda de dados pessoais
23%	Estão preocupados em ter suas fotos hackeadas
19%	Estão preocupados com o roubo do histórico do navegador
+ 75%	Possuem 4 ou mais dispositivos conectados à rede WiFi
70%	Se incomodaram com a possibilidade de um vizinho acessar secretamente suas redes WiFi privadas
17%	Usam o WiFi de seus vizinhos sem o seu conhecimento
22%	Desconhecem se suas redes WiFi estão protegidas
20%	Têm certeza de que não utilizam uma proteção
32%	Usam a mesma senha para roteadores e páginas Web
26%	Utilizam senhas padrão em seus roteadores
14%	Nem sequer sabem se utilizam a senha padrão
34%	Usam mais do que um firewall para proteger os roteadores

Fonte: Avast Software, 2014.

Neste trabalho serão testadas algumas vulnerabilidades de um roteador **D-Link DIR-610** em uma rede WLAN doméstica**.** A rede foi preparada para os testes. Um roteador pode ser um dispositivo, uma máquina dedicada ou mesmo um software. O foco desse trabalho é um dispositivo de roteamento. Segundo Reis (2012, p. 56), um aparelho trabalha na forma de roteador quando é conectado a um modem na porta WLAN. Segundo Carmona (2014), “vulnerabilidades do roteador e

senhas fracas permitem que cibercriminosos acessem facilmente a sua rede doméstica. O seu roteador é o ponto fraco na segurança da sua rede doméstica".

2 METODOLOGIA

Foi realizada uma pesquisa exploratória de dados em anais de congresso, acervos bibliográficos, livros, revistas e internet a respeito de redes e redes sem fio, sobre a tecnologia Wi-Fi, sobre WLANs e seu funcionamento, sobre roteadores, sobre vulnerabilidades em WLANs e sobre ferramentas de testes de vulnerabilidade em software livre.

2.1 SOFTWARE LIVRE

De acordo com Costa e Paulino (2011, p. 2), "software é a parte interna do computador, aquela que traz os programas e não envolve o equipamento técnico, como monitor e teclado". Softwares podem ser definidos como programas, ou uma sequência de instruções escritas para serem interpretadas com o objetivo de executar tarefas específicas, ou a parte lógica do computador. De acordo com Palmieri e Aceti (2014), "a definição de software livre foi criada pela FSF (Free Software Foundation), que diz que todo software livre pode ser usado, copiado, estudado, modificado e redistribuído sem restrição, de acordo com a necessidade de cada usuário". Todas as ferramentas utilizadas nesse trabalho são software livre, começando pelo sistema operacional Debian GNU/Linux, e todos os pacotes e ferramentas que serão descritos a seguir. Um software de código fechado não oferece algumas ferramentas nem a possibilidade de se utilizar algumas técnicas necessárias nesse tipo de prática.

2.2 CAPTURA DE SENHA DO ROTEADOR PELA FALHA NA FUNÇÃO WPS

Esse teste não é possível ser realizado em *máquinas virtuais*, porque é necessária uma placa de rede wireless e a máquina virtual reconhece a interface de rede da máquina física como rede cabeada.

A função WPS permite que dispositivos acessem a rede wi-fi sem a necessidade de digitar a chave de rede, para isso basta habilitar essa função, e é

com ela habilitada que se abrem as brechas para ataques. O Wi-Fi Protected Setup (WPS) PIN é suscetível a um ataque de força bruta. A vulnerabilidade deve-se a uma falha que permite determinar quando os primeiros dígitos do PIN de oito dígitos estão corretos. (DINIZ; LIJÓ; SOUSA, 2013).

2.2.1 Aircrack-NG

"A suíte Aircrack-NG é um software open-source composto de várias ferramentas diferentes usadas em linha de comando para auditoria redes 802.11. Aircrack-ng é um "fork" do projeto original Aircrack (LÜDTKE, 2015, p. 25)".

Para este teste o primeiro passo será instalar o pacote *Aircrack-NG* no Debian GNU/Linux 7. Para isso é necessário se logar como root digitando no terminal o comando *su*, e após teclar *enter* digita-se a senha cadastrada para o root. O comando para instalação é **apt-get install aircrack-ng**, como mostra a figura 1.

Figura 1: Tela de instalação do Aircrack-NG

```
root@Elizar:/home/elizar# apt-get install aircrack-ng
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
aircrack-ng já é a versão mais nova.
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 52 não
atualizados.
root@Elizar:/home/elizar#
```

O *Aircrack-NG* já estava instalado nesta máquina, o processo só foi executado para demonstração.

O próximo passo é verificar as placas de rede existentes, com o comando **iwconfig**, como mostra a figura 2.

Figura 2: Usando o comando iwconfig

```
root@Elizar:/home/elizar# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:"Elizar"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 78:54:2E:F9:4F:C6
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr=2347 B   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=64/70  Signal level=-46 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:1   Missed beacon:0

eth0      no wireless extensions.

root@Elizar:/home/elizar#
```

Nesse caso há duas placas, a *eth0* representa a rede cabeada e a *wlan0* representa a rede wi-fi. Para fazer o teste via wi-fi, não se deve estar conectado a nenhuma rede.

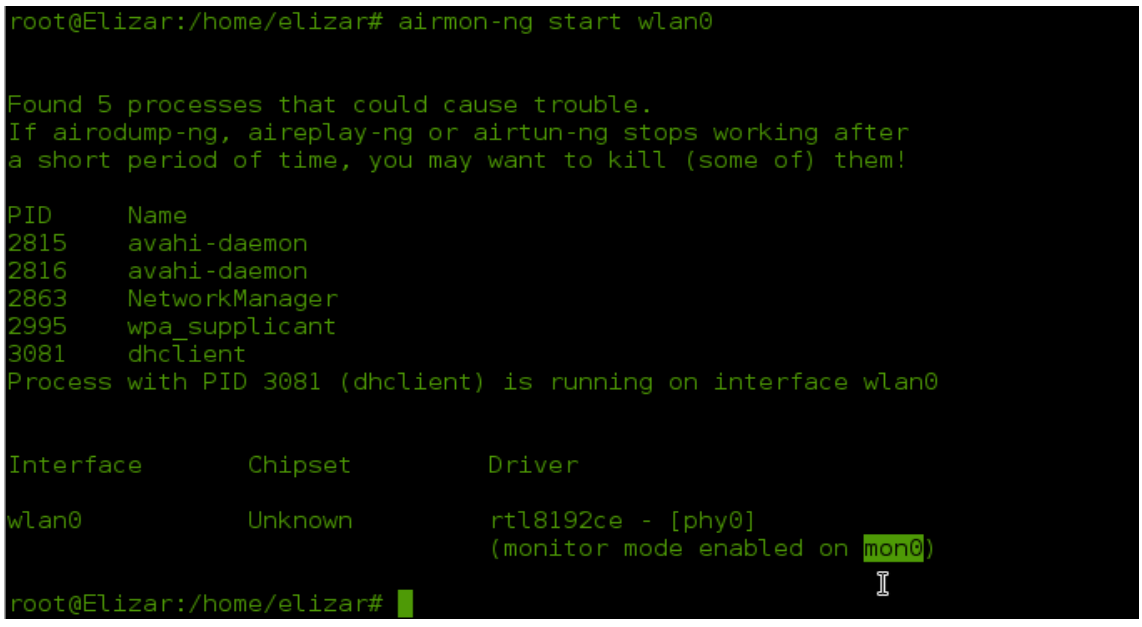
2.2.2 Airmon-NG

"Airmon-NG É um script que pode ser usado para ativar ou desativar o modo de monitor em interfaces sem fio (LÜDTKE, 2015, p. 26)". Airmon-NG faz parte do pacote Aircrack-NG.

O passo seguinte é colocar a placa de rede do roteador em modo monitor com o comando **airmon-ng start wlan0**, como mostra a figura 3.

Esse comando coloca a placa de rede wireless em modo promíscuo, escutando todas as redes que estão ao seu alcance, esta é uma configuração de recepção na qual todos os pacotes que trafegam pelo segmento de rede em que o receptor está conectado serão recebidos pelo mesmo, deixando de receber apenas os pacotes endereçados a ele. A placa foi renomeada para *mon0*.

Figura 3: Usando o comando airmon-ng

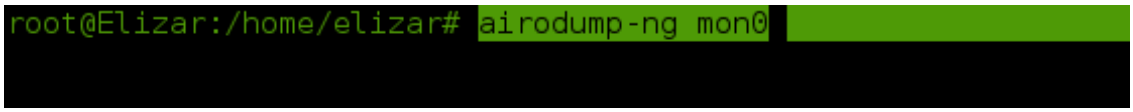


2.2.3 Airodump-NG

"O Airodump-NG é usado para captura de quadros 802.11 e também para a captura de IVs WEP (LÜDTKE, 2015, p. 26, 27)". Airodump-NG faz parte do pacote Aircrack-NG.

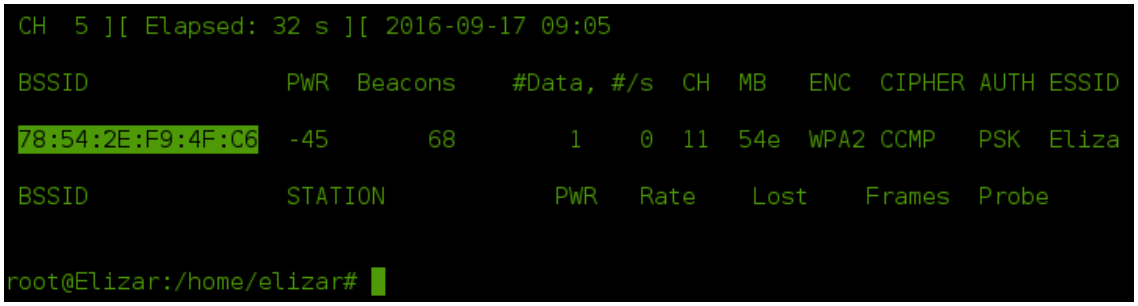
O passo seguinte é identificar e listar todos os pontos de acesso cujo sinal esteja ao alcance do roteador com o comando **airodump-ng mon0**, como mostra a figura 4.

Figura 4: Usando o comando airodump-ng



Após digitar o comando *airodump-ng* e teclar *enter*, o próximo passo é copiar o endereço MAC do roteador da rede escolhida e salvá-lo em algum lugar seguro, após fazer isto o comando *airodump-ng* não é mais necessário, podemos interrompê-lo com a combinação de teclas ‘Ctrl’ + ‘c’. Veja o exemplo do endereço MAC escolhido na figura 5.

Figura 5: Endereço MAC da rede escolhida

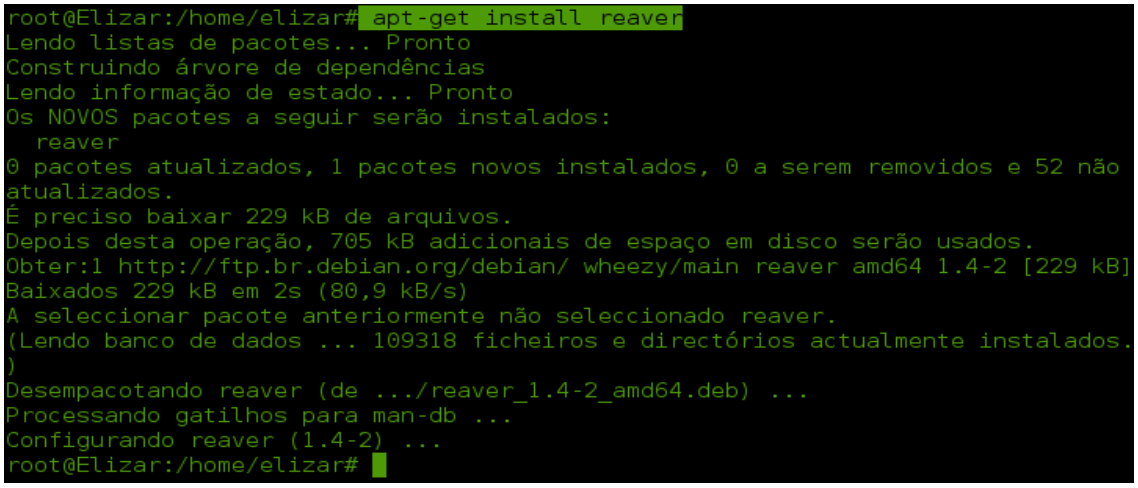


2.2.4 Reaver

“Reaver é uma ferramenta que pode ser utilizada para explorar uma vulnerabilidade do protocolo WPS, utilizado pelas chaves do tipo WPA e WPA2, a fim de resgatar a senha configurada no aparelho roteador (VISOTTO, 2014)”.

Agora, o próximo passo após capturar o endereço MAC da rede escolhida para o ataque, é instalar a ferramenta *Reaver*, utilizada para explorar vulnerabilidades do protocolo WPS. O comando usado para instalação é **apt-get install reaver**, como mostra a figura 6.

Figura 6: Instalação da ferramenta Reaver

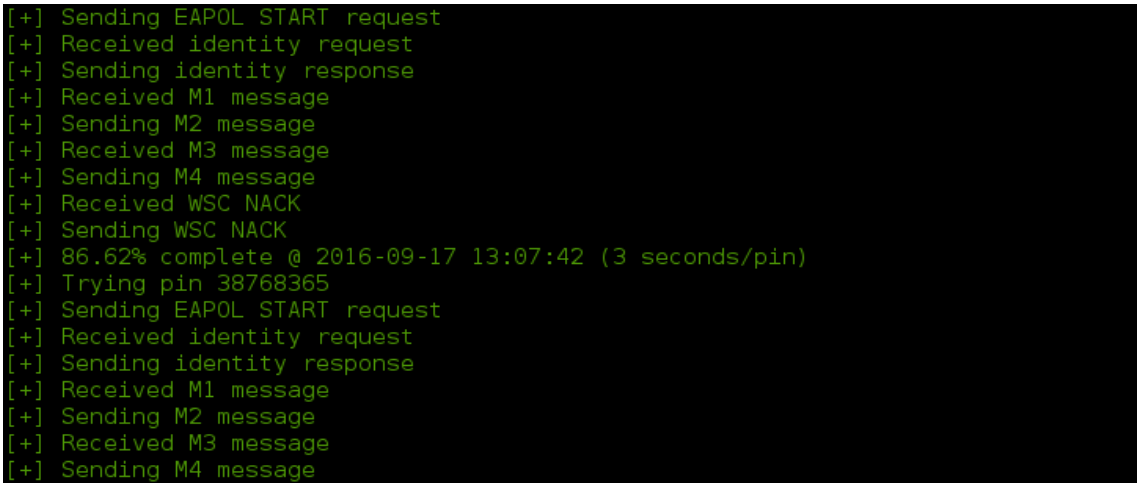


Após concluir a instalação do Reaver, o próximo passo é iniciar o ataque com o comando **reaver –i mon0 –b 78:54:2E:F9:4F:C6 -vv**, como é mostrado na figura 7. Através desse comando serão buscados os resultados através do MAC, do PIN - da Senha e do SSID. Detalhando o comando para melhor entendimento, *reaver* é a ferramenta de ataque, *-i* quer dizer interface, *-b* quer dizer BSSID que é o MAC do roteador, *78:54:2E:F9:4F:C6* é o endereço MAC que foi capturado e guardado anteriormente, e *-vv* quer dizer verbose que é um comando para mostrar os detalhes do que está acontecendo. Com esse comando o Reaver tentará descobrir o PIN do roteador através do MAC, e se descobrir terá acesso a senha e ssid do roteador.

Figura 7: Tela inicial do ataque

A figura 8 mostra o processo sendo finalizado às 13:07:42 horas, tendo sido iniciado às 09:05 horas, o processo teve duração total de 04:02:42 horas.

Figura 8: Processo de ataque em fase final



A figura 9 mostra o processo concluído com tempo de 14563 segundos (04:02:42 horas), e o processo obteve sucesso tendo sido capturado o nº do PIN do roteador, a senha WPA2 do roteador e o SSID que é o nome que aparece na rede.

Figura 9: Processo de ataque concluído

2.3 QUEBRA DE SENHA COM ATAQUE DE DICIONÁRIO

Nesse teste, ocorre a mesma situação que no ataque pela falha da função WPS, não é possível ser realizado em *máquinas virtuais*, porque é necessária uma placa de rede wireless e a máquina virtual reconhece a interface de rede da máquina física como rede cabeada.

Esse ataque consiste em utilizar um arquivo contendo uma lista com inúmeras variações e combinações possíveis de senhas, que geralmente é um arquivo com extensão .txt, essa lista é comparada com a senha da rede até que se

encontre a senha que seja igual, porém a senha só será descoberta se esta estiver contida na lista, por isso quanto maior a lista maiores são as chances de sucesso.

Foi utilizado uma WordList (dicionário, lista) de 1,00 GB com 1.454.700 combinações de senhas para este teste.

Para esse teste foi colocado no roteador uma senha possível de ser quebrada com ataque de dicionário, levando em conta que a senha usada no teste anterior é quase impossível ser descoberta com esse tipo de ataque.

No primeiro passo é necessário que se instale o pacote *Aircrack-NG*, que nesse caso não será necessário por já ter sido instalado para o teste anterior.

Para o próximo passo é necessário se logar como root digitando no terminal o comando *su*, após teclar enter digita-se a senha cadastrada para o root. O próximo passo é verificar as placas de rede existentes, com o comando **iwconfig**, como mostra a figura 2 da página 7.

Nesse caso há duas placas, a *eth0* representa a rede cabeada e a *wlan0* representa a rede wi-fi. Para fazer o teste via wi-fi, não se deve estar conectado a nenhuma rede.

O passo seguinte é colocar a placa de rede do roteador em modo monitor com o comando **airmon-ng start wlan0**, como mostra a figura 3 na página 8.

Para este teste, a senha do roteador foi trocada, sendo colocada uma senha parcialmente fraca e previsível para que o ataque pudesse ser testado. Foi colocada a senha **elizarsb**, que é o nome do proprietário da rede e as iniciais de seu sobrenome, senha com oito caracteres todos em minúsculo, somente texto puro sem nenhum tipo de mistura. Esta senha reflete em um modelo usado em uma grande parcela de proprietários de redes domésticas.

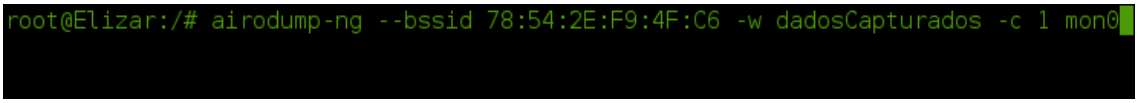
O passo seguinte é aplicar o comando **airodump-ng mon0** para identificar e listar todos os pontos de acesso cujo sinal esteja ao alcance do roteador, como mostra a figura 4 na página 9.

Após digitar o comando *airodump-ng* e teclar *enter*, o próximo passo é copiar o endereço MAC do roteador da rede escolhida e salvá-lo em algum lugar seguro, após fazer isto o comando *airodump-ng* não é mais necessário, podemos interrompê-lo com a combinação de teclas ‘Ctrl’ + ‘c’. Veja o exemplo do endereço MAC escolhido na figura 5 da página 9.

No passo seguinte inicia-se o processo de captura de pacotes na rede escolhida utilizando o comando **airodump-ng --bssid 78:54:2E:F9:4F:C6 -w**

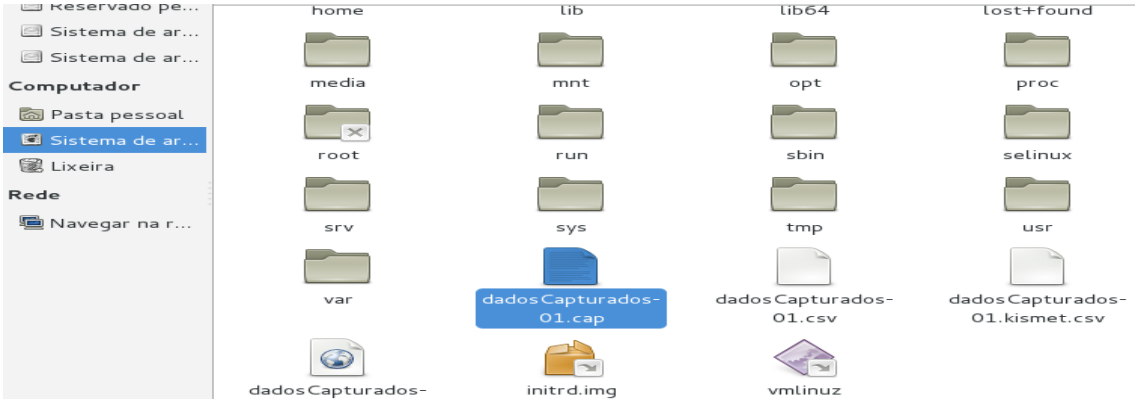
dadosCapturados -c 1 mon0, como mostra a figura 10. Explicando o comando detalhadamente, *airodump-ng* é uma ferramenta que faz parte do pacote Aircrack-NG e é usado para a captura de pacotes, *--bssid* é o endereço MAC do gateway da rede, *78:54:2E:F9:4F:C6* é o endereço MAC que foi capturado e guardado anteriormente, *-w* é o comando para criação do arquivo para armazenar os pacotes capturados, *dadosCapturados* é o nome do arquivo, *-c 1* é o canal que está sendo utilizado que no caso é 1 e *mon0* é a placa wlan0 em modo monitor.

Figura 10: Comando para Captura de Pacotes



Após executar o comando, automaticamente foi gerado dentro do diretório Sistema de arquivos um arquivo chamado dadosCapturados-01 com extensão .cap, onde serão guardados os pacotes pegos na captura, como mostra a figura 11.

Figura 11: Criação automática do diretório para guardar Pacotes



São necessários que sejam capturados no mínimo 500 pacotes para que essa técnica de ataque funcione.

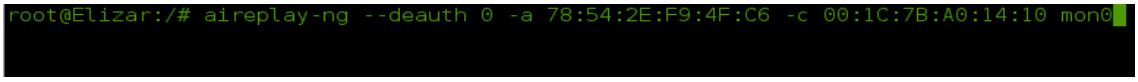
2.3.1 Aireplay-NG

"Aireplay-NG é uma ferramenta que pode ser utilizada para gerar ou acelerar o tráfego no AP. Existem diferentes ataques que podem: desautenticar o cliente com a finalidade de capturar dados de handshake WPA [...] (LÜDTKE, 2015, p. 26, 27)". Aireplay-NG faz parte do pacote Aircrack-NG.

O próximo passo será fazermos um ataque para derrubar a conexão de uma máquina da rede, assim que o ataque é interrompido a máquina volta a se conectar

com a rede, e é com essa reconexão (handshake), que concretizamos a captura, o comando utilizado é **aireplay-ng --deauth 0 -a 78:54:2E:F9:4F:C6 -c 00:1C:7B:A0:14:10 mon0**, como é mostrado na figura 12. Detalhando o comando, *aireplay-ng* é uma ferramenta que faz parte do pacote Aircrack-NG e é usada para derrubar conexões de rede, *--deauth 0* é o comando para desautenticação, *-a* é o comando que indica endereço MAC do gateway, *78:54:2E:F9:4F:C6* é o endereço MAC do roteador da rede capturado anteriormente, *-c* é o comando que indica o MAC da máquina a ter sua conexão derrubada, *00:1C:7B:A0:14:10* é o MAC da máquina. É através da reconexão da máquina que teve sua conexão derrubada é que serão capturados os pacotes.

Figura 12: Comando para derrubar conexão e capturar handshake

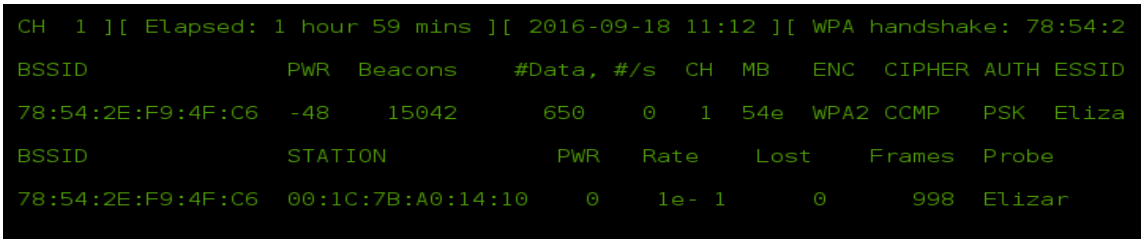


Houve um erro da placa de rede com o comando *aireplay-ng*, por isso foi usado o comando **aireplay-ng --deauth 0 -a 78:54:2E:F9:4F:C6 -c 00:1C:7B:A0:14:10 mon0 –ignore-negative-one**, como pode ser visto na figura 13. Esse comando ignora os erros da placa de rede em relação ao *aireplay-ng*.

Figura 13: Novo comando para derrubar conexão e capturar handshake

É possível identificar que houve nova conexão após a interrupção do ataque, podemos observar do lado direito superior da figura 14 que houve um handshake WPA com o MAC do gateway da rede atacada. Em #Data pode-se observar que já são 650 pacotes capturados.

Figura 14: Reconexão da máquina derrubada da rede



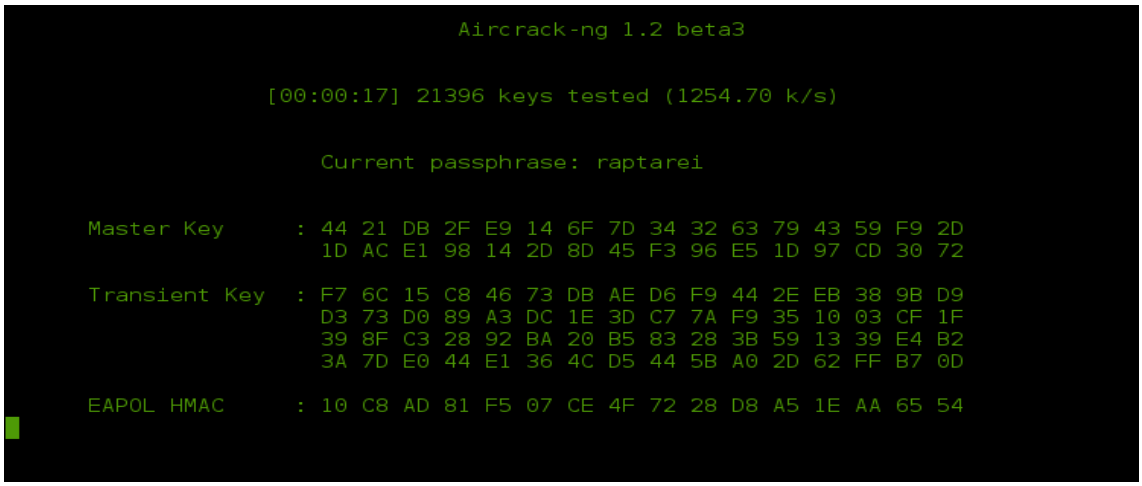
O próximo passo é dar início ao ataque de quebra de senha por dicionário. Será usado o comando **aircrack-ng -w '/home/elizar/dicionario.txt'**

'/dadosCapturados-01.cap', como pode ser visto na figura 15, em que será comparado a wordlist (dicionário, lista) com o arquivo dos pacotes capturados até que a senha seja encontrada. É preciso colocar o endereço completo do dicionário e do arquivo de dados capturados.

Figura 15: Comando para iniciar o ataque de dicionário

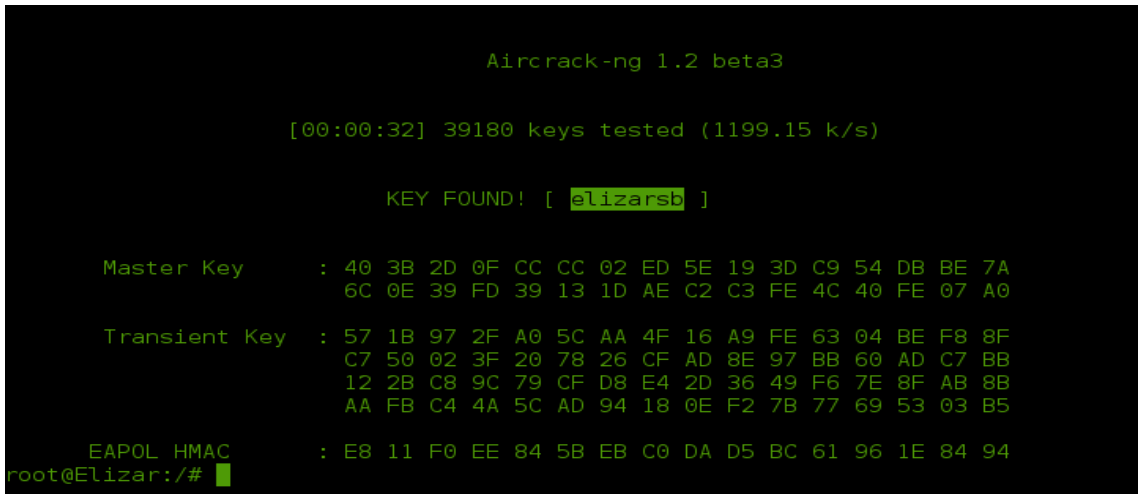
Após esse comando, o *aircrack-ng* inicia o processo de comparação da WordList com os pacotes capturados à procura da senha da rede, como mostra a figura 16.

Figura 16: Inicio da comparação das senhas



A senha do roteador **elizarsb** foi encontrada com 32 segundos e com 39.180 chaves testadas, como mostra a figura 17.

Figura 17: Comparação das senhas finalizada



2.4 RESULTADOS E DISCUSSÃO

Os resultados dos testes estão organizados na tabela 2 para que possam ser mais bem visualizados e analisados.

Tabela 2. Resultados dos testes.

Teste	Resultado	Senha Recuperada	Tempo Gasto
Função WPS	Positivo	E*s,b-981604392	04:02:42 Hs
Dicionário	Positivo	elizarsb	00:00:32 Hs

O ataque pela falha na função WPS foi iniciado às *09:05 horas* e finalizado às *13:07:42 horas* tendo uma duração total de *04:02:42 horas*. Foi encontrado o nº do PIN = **38768365**; e através do PIN encontrada a senha WPA2 PSK = **E*s,b-981604392** e o SSID = **Elizar**.

É interessante notar que, independente da complexidade da senha esta será descoberta do mesmo jeito, porque o ataque é para descobrir o número do PIN.

O ataque de Dicionário teve sucesso ao obter a senha do roteador **elizarsb** com apenas *32 segundos* e com *39.180 chaves testadas*.

A senha foi descoberta porque constava na wordlist, e com tanta rapidez por pura coincidência, dependendo da complexidade da senha e do tamanho da wordlist esse processo pode durar horas, dias e até semanas, e se a senha procurada não constar na wordlist o ataque terá insucesso. Usar senhas maiores e com grandes variações, como letras maiúsculas e minúsculas, números e símbolos e com no mínimo dez dígitos ‘como a senha usada no teste pela falha na função WPS’, torna a quebra uma tarefa quase impossível por força bruta e dicionário.

Duas medidas de segurança que se fazem necessárias como demonstrado nos testes é, utilizar senhas fortes e complexas e desabilitar a função WPS para que sua senha tenha utilidade em caso de ataques.

3 CONSIDERAÇÕES FINAIS

Os resultados obtidos nos testes confirmam a fragilidade das redes WLAN quando mal configuradas, demonstrando os motivos dos autos índices de risco gerados na pesquisa da Avast Software em 2014. “Nenhuma rede é 100% segura e nenhuma ferramenta ou tecnologia utilizada isoladamente garante proteção

completa contra ataques e invasões (COZER, 2006, p. 17)”. Mas, podemos concluir que tomando algumas medidas primordiais de segurança disponíveis e necessárias à particularidade de cada WLAN podemos dificultar muito a vida dos atacantes, eliminando as brechas mais previsíveis. Vários métodos de segurança utilizados em conjunto promovem maior proteção, tendo em vista que um pode suprir as fragilidades do outro.

REFERÊNCIAS

Avast Software. **Pesquisa desenvolvida pela Avast descobre que 81% das redes WiFi pessoais no Brasil estão sob risco de ataques cibernéticos**. 2014. PRESS-AVAST - Revista online da empresa Avast,
São Paulo, 2014. Disponível em: <https://press.avast.com/pt-br/pesquisa-desenvolvida-pela-avast-descobre-que-81-das-redes-wifi-pessoais-no-brasil-esto-sob-risco-de-ataques-ciberneticos> acessado em 12/10/2016

CARMONA, Lisandro. **A sua rede doméstica é alvo de ataques cibernéticos**. 2014. Disponível em: <https://blog.avast.com/pt-br/2014/12/03/a-sua-rede-domestica-e-alvo-de-ataques-ciberneticos/> acessado em 12/10/2016

COSTA, Fabiane Patrícia da; PAULINO, Lívia Emanuela Andrade. **SOFTWARE LIVRE**: *liberdade no compartilhamento de conhecimento e informação*. In: XIV Encontro Regional de Estudantes de Biblioteconomia, Documentação, Ciência da Informação e Gestão da informação, 16 a 22 de janeiro, 2011, São Luiz. Anais. EREBD2011.
São Luiz: 2011. 13 p.

COZER, Fabio Luiz. **Segurança Redes Sem Fio**. 2006. Monografia (Bacharel em Ciência da Computação) - Curso de Ciência da Computação, Faculdade de Jaguariúna,
Jaguariúna, 2006. 50 p.

DANTAS, Marcus Leal. **Segurança da informação**: *uma abordagem focada em gestão de riscos*. ed. 1. Olinda: Livro Rápido, 2011. 152 p.

DINIZ, Vanderson ; LIJÓ, Maria Camila; SOUSA, Marcelo Portela. **Reaver - Testes de segurança em redes sem fio**. 2013. Artigo - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba 'IFPB',
Campina Grande, 2013.

LÜDTKE, Rudolfo Kunde. **Teste de Invasão em Redes Sem Fio 802.11**. 2015. Monografia (Tecnólogo em Redes de Computadores) - Curso de Graduação em Tecnologia em Redes de Computadores, Universidade Federal de Santa Maria 'UFSM',
Santa Maria, 2015. 54 p.

OLIVEIRA, Alan Teixeira de. **Análise das Vulnerabilidades das Redes Sem Fio na Cidade de Vitória da Conquista - BA**. 2010. Monografia (Bacharel em Ciência da Computação) - Curso de Ciência da Computação, Universidade Estadual do Sudoeste da Bahia 'UESB',
Vitória da Conquista, 2010. 72 p.

PALMIERI, Laudessandro; ACETI, Patricia Aparecida Zibordi. **Software Livre**. 2014. Artigo - Curso de Ciência da Computação, Faculdade Municipal Professor Franco Montoro 'FMPFM',
Mogi Guaçu, 2014.

REIS, Gustavo Henrique da Rocha. **Redes Sem Fio**. 2012. Apostila - Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais-Campus Rio Pomba,
Rio Pomba, 2012. 63 p.

VISOTTO, Clayton. **Reaver – Descobrindo senhas Wi-Fi**. 2014. Tutorial. Disponível em: <https://www.vivaolinux.com.br/artigo/Reaver-Descobrindo-senhas-Wi-Fi > acessado em 16/09/2016