CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

QUEBRA DE SENHAS: FERRAMENTAS AIRCRACK-NG E REAVEN

LEONARDO AUGUSTO POLA

Americana/SP
2015

CENTRO PAULA SOUZA

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

QUEBRA DE SENHAS: FERRAMENTAS AIRCRACK-NG E REAVEN

LEONARDO AUGUSTO POLA

leopola022@gmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação da Profa. Dra. Acácia Ventura.

Área: Segurança da Informação e Fator Humano

Americana/SP
2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Pola, Leonardo Augusto
P814q Quebra de senhas: ferramentas aircrack-ng e reaven. / Leonardo Augusto Pola. – Americana: 2015.
66f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. Acácia de Fátima Ventura

1. Segurança em sistemas de informação 2. Internet – rede de computadores I. Ventura, Acácia de Fátima II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5
681.519

Leonardo Augusto Pola

Quebra de senhas:

Ferramentas Aircrack-NG e Reaven

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da informação e Fator Humano.

Americana, 08 de Dezembro de 2015.

Banca Examinadora:

Acácia Ventura (Presidente)
Doutora
Fatec Americana

Maria Cristina Luz Aranha (Membro)
Mestre
Unisal Campinas

José Matias Lemes Filho (Membro)
Mestre
Fam

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, pois sem Ele em minha vida, nem cursando esse curso eu estaria. Muito Ele me ajudou, tanto em todo decorrer do curso, quanto na elaboração dessa monografia, abrindo minha mente, fazendo-me entender o que não conseguia.

Em segundo lugar, agradeço a meus pais, que desde quando falei que estaria prestando o vestibular, eles estiveram me apoiando e continuam até agora, dizendo que dará tudo certo. A eles, eu sou muito grato!

Agradeço a minha professora, Juliana Borsato Beckedorff Pinto, pela ajuda com alguns livros e material que me proporcionou, que sem eles também não conseguiria terminar minha monografia a tempo.

Por fim, porém não menos importante, pois sem essa pessoa eu não conseguiria sequer terminar minha monografia, quanto mais finaliza-la. Sou muito agradecido a minha orientadora, Dra. Acácia de Fátima Ventura, que com muito carinho me acolheu na sala dos professores para me ajudar na construção do meu trabalho, e mesmo com alguns momentos mais tensos, onde não conseguia realizar o que foi pedido, ela sempre esteve me dizendo para não desistir. Muito obrigado Acácia!

DEDICATÓRIA

Esse trabalho, que foi feito com um carinho tremendo é dedicado, primeiramente a Deus, como prova de minha sinceridade, uma vez que sem Ele em minha vida, não chegaria até o final. Também não posso me esquecer dos meus pais, que me apoiaram emocionalmente. Mesmo não tendo conhecimento técnico no assunto, mas sem eles eu jamais teria sido capaz de terminar. A eles, eu dedico esse trabalho!

RESUMO

O tema apresentado será “ferramentas de quebra de senhas”, dentro do assunto de “invasões a redes *wireless”*, que se encontra, como já dito na folha de rosto, na área de “Segurança da Informação”. O problema centrou-se na vulnerabilidade da quebra de senha dos roteadores *wireless*, que estão expostas os usuários de internet que utilizam a tecnologia *WiFi*, sem conhecimento. O objetivo é comparar a eficiência das ferramentas AirCrack-NG e Reaven com o propósito de saber como funcionam em sua base, ou seja, quais os pontos e que diferenciam ambas ferramentas. Foram utilizados os métodos: Dialético e Hipotético-Dedutivo. Após os estudos considerou-se importante destacar que as duas ferramentas têm seu foco de ataques diferentes e, dependendo da situação, uma ferramenta é mais eficaz do que a outra.

Palavras Chave: ferramentas AirCrack-NG e Reaven; usuários de internet; quebra de senha.

ABSTRACT

The topic presented will be “tools of password cracking”, inside of subject “invasion of wireless network”, that if find, as just said in title page, in area of “information security”. The problem focused in vulnerabilities of password cracking of wireless routers, which are exposed the internet’s users that use the technology wi-fi, no knowledge. The objective is compare the efficiency of tools AirCrack-NG and Reaver with purpose of know how works in your base, so, which the points differ both tools. Were used the methods: Dialectical and Hypothetical-Deductive. After the study considered important highlight that both tools has your attack focus different each other, and depending on situation, a tool is more effective than other. However, how the objective general this monograph is find, by means of bibliographical studies and tests carried out in controlled environments, what tool has more efficiency, so was possible make a conclusion, how can see in finals consideration.

Keywords: tools AirCrack-NG and Reaver; internet’s users; password cracking.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Com o surgimento de um grupo, criado por várias empresas, em 1999, o WECA (*Wireless Ethernet Compatibility Alliance*) foi fundado com o intuito de lidar com a questão de padronização das normas e das especificações de rede sem fio, uma vez que a ideia já existia, porém era estudada por vários grupos de pesquisas, com propostas diferentes.

A partir de então, essa tecnologia foi evoluindo e ampliando seu alcance, em relação a seu uso. Começou auxiliando as empresas, que tinha por necessidade mudar computadores de lugar, o que, com essa tecnologia disponível, era muito mais fácil, uma vez que não precisaria mexer na infraestrutura física do local.

Hoje, essa tecnologia está presente na maioria das organizações e, em praticamente todas as casas, restaurantes, lanchonetes, bares, livraria, escolas, dentre muitos outros. Foi quando surgiu a primeira e grande questão: todos querem estar sempre conectados.

Existem vários estabelecimentos que não divulgam a senha para acesso a rede sem fio (*Wi-Fi)*, e para que as pessoas conseguissem conectar, foram desenvolvidos alguns softwares, algumas ferramentas para quebrar essa senha de acesso, para que então, o indivíduo, não precise saber a senha, basta apenas estar no raio de alcance da rede, que esses softwares descobrem essa senha.

Nessa pesquisa, serão apresentadas duas ferramentas de “quebra de senha”.

Para tanto, o estudo justifica-se em função de que atualmente muitos lugares (lanchonete, bar, café, livraria, entre outros) não disponibilizarem a rede WiFi para seus clientes, o que causa, de uma certa forma, uma revolta. Para solucionar esse problema, alguns desenvolvedores criaram softwares para que essa senha seja quebrada. Essa é apenas uma pequena situação, já que também se pode observar um cenário mais impactante, quando um cliente vai até a empresa prestadora de

serviço, e consegue se conectar à uma rede wireless com mais privilégios, o que ocasionaria uma grande falha de Segurança da Informação.

Já o **problema** foi: Os usuários de internet que utilizam a tecnologia *WiFi*, sem conhecimento, estão vulneráveis à quebras de senhas. Indivíduos mal-intencionados se utilizam de ferramentas, tais como: Reaven e AirCrack-NG, para utilizarem da rede privada.

A **pergunta** foi: Quais das ferramentas, Reaven ou AirCrack-NG*,* é mais eficiente para a invasão de redes WiFi?

As **hipóteses** foram: a) A duas ferramentas utilizam os mesmos recursos, mudando apenas a forma de buscar as informações, sendo assim as duas se equivalem; b) A ferramenta AirCrack-NG tem maior eficiência que a Reaven e c) A ferramenta Reaven tem maior eficiência que a AirCrack-NG.

O **objetivo geral** consistiu em estudar as ferramentas *Reaven* e *AirCrack-NG*, objetivando compará-las, bem como analisar a eficiência de cada uma delas.

Os **objetivos específicos** foram: a) fazer um levantamento bibliográfico sobre Segurança da Informação, buscando identificar vulnerabilidades nas redes *wireless*. b) Realizar uma pesquisa bibliográfica sobre as ferramentas Reaven e AirCrack-NG, visando compará-las em termos de eficiência, bem como simular em um ambiente controlado, testes com as ferramentas. c) Discutir as teorias estudadas, buscando compreender as invasões que as ferramentas proporcionam.

Os **métodos** utilizados foram os: Dialético e Hipotético-Dedutivo. De acordo com Gil (1987b, p. 32, apud ANDRADE, 2009, p.122-123) o Método Dialético:

> [...] não envolve apenas questões ideológicas, geradoras de polêmicas. Trata-se de um método de investigação da realidade pelos estudos de suas ações recíprocas.
>
> Do exposto deduz-se que o método dialético é contrário a todo conhecimento rígido: tudo é visto em constante mudança, pois

> sempre há algo que nasce e se desenvolve e algo que se desagrega e se transforma.

Já o método Hipotético-Dedutivo é:

> [...] considerado lógico por excelência. Acha-se historicamente relacionado com a experimentação, motivo pelo qual é bastante usado no campo das pesquisas das ciências naturais.
>
> Não é fácil estabelecer a distinção entre o método hipotético-dedutivo e o indutivo, uma vez que ambos são fundamentados na observação. A diferença é que o método hipotético-dedutivo não se limita à generalização empírica das observações realizadas, podendo-se através dele, chegar à construção de teorias e leis. (ANDRADE, 2009, p.122).

A **pesquisa** foi classificada do ponto de vista da sua natureza como Básica e Aplicada.

Segundo Gerhardt (2009, p.34) a pesquisa básica objetiva: “[...] gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática prevista. Envolve verdades e interesses universais”.

Já a pesquisa aplicada objetiva: “[...] gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais.” (GERHARDT, 2009, p.35).

Para a abordagem do problema a Pesquisa Qualitativa foi utilizada. Definida como aquela que:

> [...] não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc. Os pesquisadores que adotam a abordagem qualitativa opõem-se ao pressuposto que defende um modelo único de pesquisa para todas as ciências, já que as ciências sociais têm sua especificidade, o que pressupõe uma metodologia própria. Assim, os pesquisadores qualitativos recusam o modelo positivista aplicado ao estudo da vida social, uma vez que o pesquisador não pode fazer julgamentos nem permitir que seus preconceitos e crenças contaminem a pesquisa. (GERHARDT, 2009, p.31, 32).

Para que os objetivos fossem atingidos utilizou-se a Pesquisa Descritiva, para que o resultado fosse o mais preciso exato, o que nas palavras de Barros e LEHFELD (2007, p.84):

> Nesse tipo de pesquisa, não há a interferência do pesquisador, isto é, ele descreve o objeto de pesquisa. Procura descobrir a frequência com que um fenômeno ocorre, na natureza, características, causas, relações e conexões com outros fenômenos.
>
> A pesquisa descritiva engloba dois tipos: a “pesquisa documental” e/ou “bibliográfica” e a “pesquisa de campo”.

Para os procedimentos técnicos a pesquisa utilizada foi a Bibliográfica que: “tanto pode ser um trabalho independente como constituir-se no passo inicial de outra pesquisa. Já se disse, aqui, que todo trabalho cientifico pressupõe uma pesquisa bibliográfica preliminar.” (ANDRADE, 2009, p.115).

O trabalho foi estruturado em três capítulos, sendo que o primeiro aborda a segurança da informação, seus pilares, bem como alguns tipos de configurações em redes privadas e as tecnologias sem fio (wireless). O segundo discute fatores relacionados às ferramentas de estudo, o AirCrack-NG e a Reaver, abordando uma breve definição do que é, de como trabalha e quais vulnerabilidades são exploradas por cada um, tendo por fim os resultados e explicações dos testes realizados em ambiente controlado. Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o capítulo três se reserva às Considerações Finais.

1 SEGURANÇA DA INFORMAÇÃO E SISTEMA *WIRELESS*

Nesse capitulo será abordado o conceito de segurança da informação, dizendo o que ela trabalha e como faz isso. Será mostrado quais são os três pilares da Segurança da Informação, explicando cada um deles. Também alguns tipos de configurações em redes privadas, para melhorar a segurança local. Será mostrado como que a tecnologia sem fio (*wireless*) surgiu e quais são os principais pontos em que podemos destacar. Será apresentado, por final, os mecanismos de segurança em redes *wireless*.

1.1 SEGURANÇA DA INFORMAÇÃO

Antes de falar o que é a segurança da informação, considera-se importante destacar o conceito de segurança, que para Ferreira (2000, p.627), segurança é: “Ato ou efeito de segurar (-se) ”. Vê-se que segundo essa definição, a palavra segurança se refere a algo ou alguém estar seguro, que segundo o dicionário Michaelis (acesso em: 19/09/2015, s/p), seguro é: “[...] Livre de perigo ou não exposto a ele[...]”. No dicionário Priberam (acesso em: 19/09/2015, s/p), perigo é definido como: “1. Situação em que está ameaçada a existência de uma pessoa ou de uma coisa; risco” e risco é: ”[...] probabilidade ou possibilidade de perigo: estar em risco” (DICIO, acesso em: 19/09/2015, s/p).

Olhando essas definições, é possível dizer que a segurança é o ato de estar seguro, ou seja, estar fora de perigo ou risco de perigo, que por sua vez trarão perdas para quem ou o que sofrer.

Seguindo a mesma linha de raciocínio, a palavra informação encontrada no dicionário Dicio (acesso em: 19/09/2015, s/p) significa: “[...] reunião dos dados que, colocados num computador, são processados, dando resultados para um determinado projeto [...]”. Por sua vez, a palavra “dado”, no dicionário Michaelis (acesso em 19/09/2015, s/p), significa: “[...]**3** Princípio ou base para se entrar no conhecimento de algum assunto[...]”.

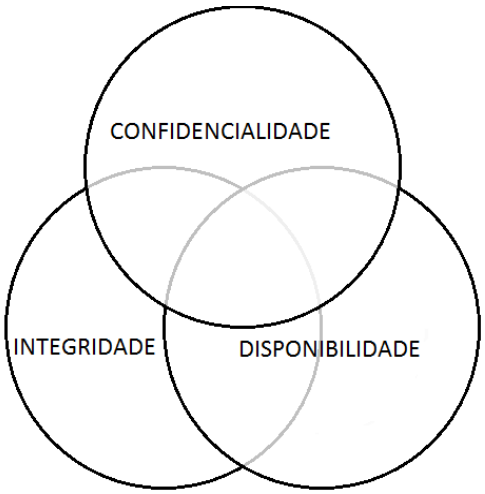
Sabendo dessas definições, é possível dizer que a informação é um conjunto de dados, que por sua vez, são os princípios para um conhecimento, que quando processados, gera um resultado para uma determinada razão.

A norma ISO 27002 define a segurança da informação como: “[...] proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio” (DANTAS, 2011, p.11, *apud* NBR ISO/IEC 27002:2005).

A segurança da informação é responsável por proteger as informações, tanto de uma pessoa em particular, de um grupo de pessoas e de corporações. As informações podem ser de, desde uma pessoa física, de uma pequena empresa, de uma Constituição Federal (um país), quanto de organizações multinacionais, como o MERCOSUL (Marcado Comum do Sul), OMC (Organização Mundial do Comércio), ONU (Organização das Nações Unidas), dentre outros.

Ela é composta por diversos requisitos e âmbitos de segurança, porém os três principais pilares da segurança da informação são: Confidencialidade; Integridade; Disponibilidade. Toda e qualquer prática de segurança, que visa proteger uma informação, tem enfoco esses três grandes pilares primeiramente, e depois podendo abranger também alguns atributos como a autenticidade e a confiabilidade, a irretroatividade, a legalidade, a privacidade, a auditoria e o não repúdio (OLIVEIRA, 2011).

Figura 1: Pilares da segurança da informação



Fonte: Adaptado de Oliveira (2011).

1.1.1 CONFIDENCIALIDADE

Para Oliveira (2011, p.14). “[...] é a garantia de que a informação será acessada apenas por pessoas autorizadas”.

Como o próprio nome diz, esse pilar é responsável por tornar a informação confidencial, para todas as pessoas que desejam acessa-la de alguma forma. Para as pessoas autorizadas a ter acesso a informação, sempre existirá um meio de revelar a informação. O pilar da confidencialidade trabalha para que a informação seja restrita e secreta.

Para Dantas (2011), a quebra de confidencialidade ocorre quando uma informação é disponibilizada para pessoas não autorizadas. Com a perda da confidencialidade também é perdido o segredo da mesma. Quando se garante a confidencialidade de uma informação é assegurado o valor da mesma.

Uma informação que mantém seu segredo tem muito mais valor do que alguma outra que não mantém, uma vez que essa informação pode ter um efeito positivo para quem a possuir.

Em uma situação de comércio. Se uma empresa X souber qual é o fornecedor de determinado produto para a empresa Y, a concorrente, ela consegue

saber qual é o custo para a empresa Y em determinado produto, podendo assim estabelecer um preço mais vantajoso para a empresa X para o mesmo produto. Em uma situação de guerra, se o exército T souber a onde o exército R está acampado, o exército T pode armar uma emboscada, ou mesmo um ataque direto.

Esses foram dois exemplos simples de como a informação divulgada afeta o dono da informação. Para o comerciante, se essa informação fosse camuflada por alguma ferramenta, a empresa Y não saberia qual seria o preço ideal para vender o seu produto. Se a localização do exército R não fosse revelada, eles não sofreriam algum tipo de ataque.

Para que certas informações permaneçam confidenciais, sem que pessoas ou grupos não autorizados possam ter acesso à essas informações, são utilizadas diversas ferramentas e técnicas, sendo a mais conhecida e comum, a criptografia.

Segundo Oded Goldreich, criptografia pode ser definida como “[...] esquemas que proveem comunicação segura sobre meios inseguros de comunicação”. (GOLDREICH, 2007, p.3).

Ela transforma uma mensagem, um texto, uma foto, um arquivo, de sua forma original para uma criptografada, ou seja, em um texto não legível. Existe dois meios para criptografar uma mensagem: encriptação simétrica e encriptação assimétrica.

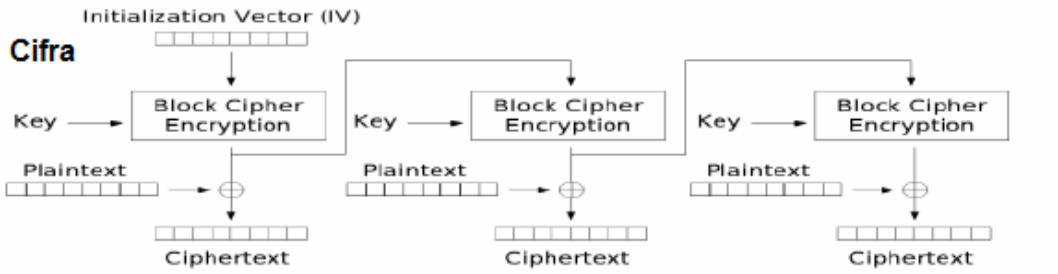
A encriptação simétrica utiliza cifras de criptografia para realizar a encriptação da mensagem e utiliza apenas uma chave, uma senha, que é usado para esconder e revelar a mensagem. As técnicas que são utilizadas podem ser a de substituição, a troca e operações matemáticas como *AND*, *OR* e *XOR* (AGUADO, 2014).

A encriptação assimétrica utiliza somente operações matemáticas, porém são muito mais complexas. Primeiro que são utilizadas duas chaves, ou um par de chaves, aonde uma chama “chave pública” e a outra chama “chave privada”. A

questão é: Tudo quanto for criptografado com a chave pública, só a chave privada revela, e tudo quanto for criptografado com a chame privada, só a chave pública revela (AGUADO, 2014).

Cifra, em criptografia, se diz para um conjunto de operações, como que um passo a passo, de: o que se deve fazer, em qual ordem, e com qual dado (no caso, bit ou conjunto de bits). Pode ser comparado com uma receita de bolo, sendo descrito assim: 1° Separar dois blocos de bits, com 8 bits em cada um; 2° fazer uma operação *XOR* entre o bloco 1 e o bloco 2; 3° substituir a posição dos bits da forma original para essa “2 4 1 7 6 3 8 5” (o bit que estava por segundo; vai para o primeiro lugar; o bit que estava em quarto, vai para o segundo lugar; assim por diante). Só que, essa cifra não é escrita, como foi descrita acima. Segue abaixo uma cifra de criptografia:

Figura 2: *Cipher Block Chaining*

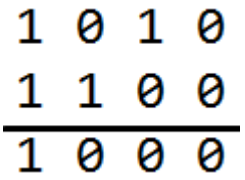


Fonte: Adaptado de Pinheiro (2010, s/p).

Para explicar a operação: *AND*, *OR* e *XOR* – são operações matemáticas usadas na criptografia, na forma de encriptação simétrica.

O Operador *AND* separa dois blocos de x bits (o número de bits depende de qual cifra está usando) e faz as devidas operações, ou seja, ele realiza uma operação com cada bit. Se os dois bits foram 1, então o resultado é 1, caso contrário, o resultado é 0. Na escrita, o operador lógico para *AND* é representado por “^” (AGUADO, 2014).

Figura 3: Operação lógica AND



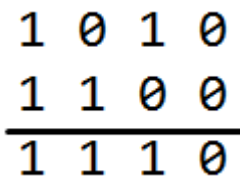
Fonte: elaborado pelo autor

Ou,

1010 ^ 1100 = 1000.

O operador *OR* separa, do mesmo jeito que o operador *AND*, dois blocos de x bits e faz as devidas operações com cada bit, porém, nesse caso, se um dos bits forem 1, então o resultado é 1, caso contrario, ou seja, os dois bits foram 0, então o resultado é 0. Na escrita, o operador lógico *OR* é representado por "v" (AGUADO, 2014).

Figura 4: Operação lógica OR



Fonte: elaborado pelo autor

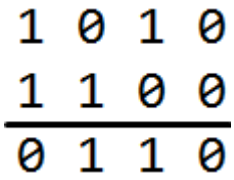
Ou,

1010 v 1100 = 1110.

O operador *XOR*, assim como os outros dois operadores, separa dois blocos, com o mesmo numero de bits cada um (podendo variar o número de bit, conforme a cifra usada) e faz as devidas operações com cada bit. O operador XOR calcula dois bits, se os dois forem iguais, "0 e 0" ou "1 e 1" então o resultado é 0,

caso contrário, é 1. Na escrita, o operador lógico *XOR* é representado por "⊕" (AGUADO, 2014).

Figura 5: Operação lógica XOR



Fonte: elaborado pelo autor

Ou,

1010 ⊕ 1100 = 0110.

1.1.2 INTEGRIDADE

Segundo Oliveira (2011, p.14), integridade é: "[...] a garantia de que a informação não sofreu nenhuma alteração após sua emissão".

Quando se diz que uma pessoa é integra, está se falando que ela é puta, imparcial, ou seja, ela não mudar o seu jeito de ser dependendo da situação. Do mesmo jeito, pode ser comparada, a informação. Quando chamamos uma informação de integra, está sendo atribuído a ela uma característica de pura e imparcial, ou seja, a informação é a mesma, desde de sua origem até quando ainda for utilizada.

A segurança da informação tem a integridade como um dos seus três maiores pilares, e com isso, foram desenvolvidos diversos métodos para garantir que tal informação seja integra. Um dos métodos mais conhecidos e também mais usados é, também, a criptografia.

Nesse âmbito, usamos a técnica de encriptação unidirecional ou resumo criptográfico, mais conhecido como *Hash*. Como o próprio nome diz, é uma encriptação unidirecional, ou seja, só trabalha em uma direção, logo, só é possível

criptografar a mensagem, e depois disso feito, é impossível voltar para a mensagem original, a partir do *hash* criado (AGUADO, 2014).

Segundo Pellegrini (2015, p.9): “Funções de *hashing* mapeiam sequências de bits de tamanho arbitrário (como arquivos e mensagens) em pequenas sequências, de tamanho fixo. Desta forma estes pequenos resumos podem ser usados para identificar arquivos”.

As funções e *hash* são feitas para serem um resumo do que for criptografado (do arquivo, da mensagem, da imagem, de um HD, dentre muitos outros), e por isso, muito dificilmente haverá duas mensagens com o mesmo *hash*. As cifras de encriptação unidirecional são feitas para minimizar esse “efeito colateral”, porém já foi descoberto que palavras com o mesmo *hash*, em determinadas cifras. Para solucionar esse problema, foram projetadas e implementadas outras cifras, mais robustas e com mais bits de resumo.

Então, como isso ajudará a garantir que minha informação é integra? Simples. Quando uma nova informação for gerada, ou mesmo se você tiver certeza que tal informação não foi modificada, então faça um *hash* (resumo criptográfico) da informação e guarde esse *hash* em um local protegido (se possível, sem conexão à internet) e quando você quiser checar se tal informação continua integra, então refaça o *hash* da informação, e compare com o que está guardado. Um jeito fácil de fazer é aplicando o *XOR*. Se o resultado for inteiro 0, então o *hash* é o mesmo, e a informação não foi alterada, porém, se no resultado aparecer, em qualquer bit o 1, então a informação foi alterada e não é mais íntegra (AGUADO, 2014).

1.1.3 DISPONIBILIDADE

Disponibilidade é definida como: “[...] a garantia de que uma pessoa autorizada tenha acesso a uma informação íntegra, no momento que desejar. ” (OLIVEIRA, 2011, p.14).

A segurança da informação trata como terceiro pilar, mas não menos importante, a disponibilidade da informação. Assim como foi descrito pelo autor

acima, ela garante que determinada informação esteja sempre disponível para as pessoas autorizadas a acessarem a mesma.

Para que se tenha uma disponibilidade maior de uma informação, é utilizado a técnica de redundância, ou seja, toda informação é replicada para um outro local, exatamente como ela é, para que, se porventura a informação que está alocada no primeiro local (o qual está sendo usado) ficar indisponível por algum motivo, então esse *backup*, que está alocado em um outro local como redundância, será usado no local do original. Desse jeito, nós conseguimos diminuir a probabilidade de a informação ficar indisponível.

Tratando-se de um ambiente coorporativo, para haver uma disponibilidade efetiva, é necessário que um outro atributo da segurança da informação seja atendido: a autenticidade.

Segundo Oliveira (2011, p.15), a autenticidade se divide em duas categorias: autenticidade do emissor e autenticidade do receptor.

> **›** Autenticidade do Emissor: é a garantia de que a pessoa que enviou a informação é realmente quem diz ser; e
>
> › Autenticidade do Receptor: é a garantia de que a informação foi recebida por uma pessoa autorizada.

Vemos então que existe uma necessidade de ter um controle de autenticação, para existir a disponibilidade da informação, uma vez que a informação deve estar sempre disponível, para quem tem permissão de acesso a ela. Logo, dentro de uma empresa, um servidor de autenticação será o suficiente para dizer quem pode realizar determinadas tarefas (como edição e/ou criação de informações) e quem pode ter acesso a essas informações.

1.1.4 SEGURANÇA EM REDES DOMÉSTICAS E CORPORATIVAS

Quando se fala da segurança em redes, muitas variáveis estão envolvidas. Em uma rede doméstica, muitas vezes ela é montada pelos próprios donos da residência (sendo ela apartamento ou casa), logo, pode existir casos onde

não é configurado nenhum tipo de segurança para a mesma, em contraposição, não são muitos os invasores que buscam invadir uma rede doméstica, logo o risco de invasão e perca de dado é pequeno. Já uma rede coorporativa é mais visada por invasores, por motivos como: roubo de informação; deixar a empresa com uma indisponibilidade de informação; dentre outros. Porém, para aqueles que desejam proteger suas informações, existem diversas técnicas de proteger sua rede interna.

Antes de qualquer configuração seja feita nas aplicações e equipamentos que rodam na rede da corporação, é necessário implementar um *firewall* de borda na rede, ou seja, um filtro de pacotes de rede, que, quando configurado corretamente, dificulta o acesso de possíveis invasores.

Uma outra técnica muito utilizada é a criação de uma DMZ (*demilitarized zone* ou zona desmilitarizada) é um local escondido dentro de sua rede interna, a onde todos os dispositivos, mesmo conectados em sua rede, não conseguem enxergar essa parte da rede, todavia, os dispositivos (geralmente servidores) que estão dentro da DMZ conseguem se comunicar com o resto da rede sem problema. Então, uma configuração muito importante é a criação de uma DMZ em sua rede interna e nela colocar todos os servidores que utiliza, assim como o(s) banco(os) de dados existentes na corporação (PINTO, 2015).

Também não podemos esquecer da tecnologia *wireless*, também conhecida como rede sem fio. A rede *wireless* proporciona inúmeras vantagens para a corporação, e também para as redes domésticas, todavia, traz consigo inúmeras vulnerabilidades de segurança.

Primeira vulnerabilidade que se mostra em uma rede *wireless*, é que não precisa estar conectados a nenhum cabo, obviamente, uma vez que basta estar no alcance da propagação de rede para se conectar via *Wi-Fi*.

Segunda grande vulnerabilidade existente é que ao entrar no alcance da propagação da rede, o invasor terá acesso aos pacotes que estão trafegando na rede. Esses pacotes contêm dados da rede *Wi-Fi*, e com esses dados, é possível aplicar técnicas de quebra da senha. Um detalhe muito importante é que.

Dependendo de como os pacotes estão cifrados, a quebra da senha é muito mais fácil. Inicialmente o protocolo usado foi o *WEP* (*Wired Equivalent Privacy*), porém já foram descobertas diversas falhas nesse protocolo, e com uma ferramenta de quebra de senha *wireless* é facilmente quebrada. Para solucionar esse problema, foram desenvolvidos esse protocolo e melhorado para os que usamos hoje e que oferecem mais segurança, os protocolos *WAP* (*Wi-Fi Protected Access*) e *WAP*2 (*Wi-Fi Protected Access2*) (RUFINO, 2015).

Outra grande falha, mais encontrada em redes domésticas, é ter uma rede *Wi-Fi* sem proteção de uma senha, o que facilita, e muito, o acesso de possíveis invasores.

1.2 REDE *WIRELESS*

Tecnologia de rede sem fio (wireless) está cada dia mais comum atualmente, estando em um ambiente de trabalho, em um ambiente doméstico, em uma cafeteria, em uma lanchonete, dentre muitos outros lugares. Segundo Nelson Murilo “como ocorre com toda a tecnologia mais recente, outro fator de adoção é a curiosidade, pois certamente muitos usuários estão mais interessados na novidade da tecnologia do que nas reais vantagens ” (RUFINO, 2015, p.15).

A preocupação com a segurança relacionada a esse assunto certamente surgira, tendo em vista que, pelo ponto de vista dos administradores de rede, houve dois tipos de reações: não adotar a tecnologia, pelo fato de não haver algum conhecimento referente a segurança; ou a situação oposta, a adoção imediata da tecnologia, sem ter nenhum conhecimento da tecnologia, riscos e vulnerabilidades. Mais uma vez, segundo Nelson Murilo “infelizmente, a segunda opção tem sido mais comum, quer seja realmente por descuido, quer seja por pressão da chefia pela adoção rápida da tecnologia” (RUFINO, 2015, p.15).

Antes de aprofundar no assunto, será abordado a história de como surgiu essa tecnologia. Em meio à Segunda Guerra Mundial, houve a necessidade de os militares transmitirem informações de forma que a mensagem não fosse

interceptada e nem interrompida. Para isso os militares transmitiam as informações via rádio (ZEINDIN, *et al*. Acesso em: 14/09/2015).

No século passado, “O inventor do rádio Marconi já demonstrava pelo uso das ondas de rádio a curvatura da terra [...]” (ZEINDIN, *et al*. Acesso em: 14/09/2015, p.2). A partir dessa tecnologia, e com o convívio direto com essas ondas de rádio, gerou uma grande evolução, até chegar no que existe hoje, a tecnologia Wireless.

Logo após o termino da Guerra Fria, por volta de 1992, essa tecnologia foi disponibilizada para o público, para uso civil. Com o uso dessa tecnologia pela população, a tecnologia foi barateando cada vez mais, e os estudos sobre ela foi evoluindo e melhorando.

“O Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) é a maior, em números de sócios, organização profissional do mundo” (COSTA, 2010, p.47). Formado em 1963, com a união de dois institutos, sendo o dos Engenheiros de Rádio (IRE) com o instituto Americano de Engenheiros Eletricistas (AIEE). Seu objetivo, o motivo desse instituto existir é: “[...] prover conhecimento no campo da engenharia elétrica, eletrônica e da computação. Um dos seus papeis mais importantes é o estabelecimento de padrões para formatos de computadores e dispositivos ” (COSTA, 2010, p.47).

O padrão wireless foi estabelecido por essa instituição, com a norma IEEE 802.11, que é conhecido como Wi-Fi. Foi licenciada pela empresa Wi-Fi Alliance, inicialmente, para descrever a tecnologia WLAN (redes sem fio).

1.2.1 PRINCIPAIS PADRÕES

Dentro do padrão já estabelecido pela IEEE, o 802.11b é o mais conhecido e o mais popular dentre os outros, segundo Zeindin (Acesso em: 14/09/2015). Esse protocolo atua na faixa de 2,4 GHz, sendo essa também a frequência que o micro-ondas e o telefone sem fio operam. Esse padrão consegue transferir dados em uma banda de até 11 Mbps. Com esse protocolo, a rede *wireless*

tem um alcance maior, conseguindo se propagar uma área mais ampla, todavia a capacidade de transmissão de dados é reduzida.

O segundo padrão que será abordado, é o 802.11a. O professor Costa (2010) afirma que diferente do padrão citado acima, ele trabalha na frequência de 5 GHz e tem a capacidade de transferir os dados em até 54 Mbps. Esse protocolo prioriza a transmissão de dados, onde a banda *wireless* é bem maior do que no protocolo 802.11b, contudo a propagação de sinal é reduzida, limitando-se a atender uma área menor.

O padrão 802.11g é mais recente do que os já visto. Segundo Rufino (2015), ele veio para solucionar a falha que o padrão 802.11a deixou, pois o 802.11g atua na mesma frequência que o padrão 802.11b (2.4 GHz), possibilitando assim que ambos os padrões possam operar junto, em uma mesma rede. O padrão 802.11g também traz a característica do padrão 802.11a de que é possível transmitir dados em até 54 Mbps.

Rufino (2015) também afirma que em junho de 2004 foi homologado o padrão 802.11i, que tem por maior prioridade a segurança dos dados que serão transmitidos. “[...] diz respeito a mecanismos de autenticação e privacidade e pode ser implementado em vários de seus os protocolos existentes” (Rufino, 2015, p.32). Nesse padrão está inserido o protocolo WAP (*Wi-Fi Protected Access*), para ter assim uma maior segurança.

Segundo Costa, o padrão 802.11n possui um grande diferencial dos demais:

> Tem uma largura de banda até aos 300 Mbps e um alcance de 70 Metros. Opera nas frequências 2.4GHz e 4GHz. 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 de largura de banda e o alcance que permite (COSTA, 2010, p.49).

Por fim, o ultimo padrão a ser abordado, porém não menos eficiente, o 802.11ac. Rufino (2015) diz que uma das principais características desse padrão é a

sua maior velocidade de tráfego, que pode chegar até 1,3 Gbps. Ele atua somente na frequência de 5 GHz, além de melhorar a qualidade do sinal, deixando a conexão mais estável.

1.2.2 MECANISMOS DE SEGURAÇA

Como já adiantado no subcapítulo 1.1.4, a rede wireless tem mecanismos de segurança, para que os pacotes de dados que trafegam na rede possam ser protegidos. Costa (2010) diz que o protocolo de segurança chamado WEP é encarregado de criptografar os dados que trafegam, dentro dos pacotes de dados, na rede, todavia é afirmado que esse protocolo é muito inseguro, sabendo-se como é feita sua arquitetura.

Sousa (acesso em: 15/09/2015) afirma que esse protocolo trata da segurança dos tráfegos de rede com criptografia e autenticação o cliente e o ponto de aceso. A forma em que os dados são criptografados não são especificados pelo protocolo, logo pode-se dizer que o cliente (o aparelho que está se conectando na rede) junto com o ponto de acesso concordam com uma chave. O algoritmo de criptografia utilizado para realizar a encriptação é o RC4. Esse é um algoritmo de criptografia simétrica e sua chave pode ter 64, 128 ou até 152 bits.

Esse é um protocolo já defasado, com diversas falhas de segurança. Sousa (acesso em: 15/09/2015) comenta alguns deles:

O primeiro passo de encriptação utiliza um vetor de 24 bits. É um vetor pequeno e fácil de ser quebrado;

A chave que o protocolo usa não é atualizada, o que ocasiona keystreams* semelhantes. Com isso, a senha pode ser quebrada muito mais rápido.

* São geradores pseudoaleatórios. A partir de uma chave, geram outras chaves (“pseudo-chaves”). (GOLDREICH, 2007)

Com essas fraquezas e fragilidades expostas, o protocolo tornou-se obsoleto. Para solucionar esse problema, foi inventado um novo protocolo, que será abordado a seguir. O novo protocolo se chama WPA.

O protocolo WPA tem dois focos de atuação, sendo o primeiro que é substituir completamente o protocolo usado até o momento, o WEP. Esse novo protocolo trata as falhas do anterior, em questão da criptografia, objetivando garantir a privacidade do que está sendo transmitido. O segundo foco de melhoria é a autenticação do usuário. Uma abordagem não tratada pelo WEP, esse novo protocolo utiliza o padrão EAP (Extensible Authentication Protocol) para que os clientes da rede wireless possam autenticar-se na rede (RUFINO, 2015).

A maior causa do problema em relação ao sigilo e confidencialidade dos protocolos WEP é decorrente do mecanismo de criptografia usado. O WPA trata diretamente esses pontos falhos, sendo eles a combinação de algoritmo e um fator que podemos destacar como chaves temporárias, uma vez que tratará a temporalidade das chaves.

O grande responsável por essa solução é o protocolo TKIP (Temporal Key Integrity Protocol). Criado para ser usado junto com WPA, o TKIP é responsável pela geração e gestão de chaves temporárias, que conserva a confidencialidade, com a constante troca de chaves. A segunda vulnerabilidade tratada pelo WPA, imposta pelo TKIP é o tamanho do vetor inicial de criptografia que aumento para 48 bits, o que aumenta o número de combinações possíveis. (RUFINO, 2015)

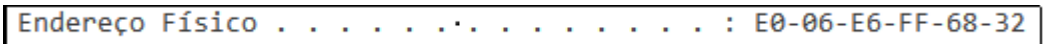
Com o tempo, o protocolo TKIP foi sendo usado cada vez mais, o que ocasionou a descoberta de vulnerabilidades nesse protocolo também, não tão graves quanto no WEP, mas que facilitaria o acesso indevido a informações.

“Com a homologação do padrão 802.11i, o protocolo CCMP juntou-se aos já conhecidos WEP e TKIP, só que, diferentemente destes, usa o algoritmo AES para cifrar os dados na forma de blocos (de 128 bits), e não mais byte a byte [...]” (RUFINO, 2015, p.43), essa é a descrição do protocolo WPA2.

Com base no protocolo WPA, o WPA2 foi feito para aumentar a segurança, uma vez que foi aplicado o algoritmo AES para criptografar os pacotes que trafegam na rede. Atualmente, esse é o padrão mais seguro para as conexões sem fio (VASCONCELLOS, 2013).

Um outro mecanismo de segurança que pode ser, e muitas vezes é, implementado é o endereçamento MAC (Media Access Control). O endereço MAC é uma sequência de doze (12) números hexadecimais de dois em dois. MAC também é chamado de endereço físico.

Figura 6: Endereço físico



Fonte: elaborado pelo autor

Esse endereço é único de cada equipamento dentro de uma mesma rede, logo cada computador, cada celular, cada ponto de acesso, dentre todos os demais dispositivos de rede possuem um MAC diferente do outro.

Quando é falado de endereçamento MAC, está querendo dizer que haverá uma restrição de equipamentos que terão permissão ou não para acessar da rede. É possível fazer uma lista de endereços MACs que só esses endereços podem acessar a rede, ou uma lista onde os equipamentos listados não poderão ter acesso a rede, liberando para todos os demais.

Esse mecanismo de segurança acarreta uma manutenção de tempo em tempo, dependendo do tamanho da rede e com o fluxo de usuários que possam acessar ou não a rede (RUFINO, 2015).

A partir do exposto se pode ter uma ideia do conceito e da importância da Segurança da Informação e o conceito de rede sem fio (*wireless*), bem como as ferramentas de segurança, como os protocolos *Wi*-F*i*. A seguir serão realizados testes de invasão e análise dos resultados.

2 FERRAMENTAS E TESTE

Neste capitulo, serão apresentados alguns conceitos de *hacking* e uma breve explicação de como surgiram os *hackers* éticos e antiéticos. Também serão apresentadas as duas ferramentas abordadas nessa monografia, reaver e aircrack-ng. Será mostrado qual é o foco de ataque, de cada ferramenta, como ele coleta as informações necessárias para efetuar o ataque. Por fim, terão os resultados dos testes feitos pelo aluno em ambiente controlado, mostrando qual foi o retorno de cada ferramenta, de acordo com o protocolo de segurança que será utilizado.

2.1 ÉTICA DE RAQUEAMENTO

Antes de explorar e divulgar as descobertas que essa monografia apresentará, é muito importante ressaltar que toda e qualquer tipo de invasão é ilegal.

Segundo Basta (2015), nos últimos 40 anos o conceito de “*hacker*” foi tomando uma definição mais pejorativa. Quando usamos essa palavra, estamos diretamente ligando à uma pessoa com habilidades técnicas para realizar ações ilegais e antiéticas, mas os “*hackers* legais”, que por vez, queriam manter esse novo, contradisseram essa tendência, respondendo que os indivíduos mal-intencionados são na verdade os *crackers*.

Falando sobre a ética nesta área abordada, a grande parte dos profissionais possuem um código de ética, que os redireciona a um conjunto de normas morais e valores compartilhados, afim de angariar o respeito dos que o observam (BASTA, 2015).

Quando se refere a um profissional de segurança de redes, a situação é a mesma. A grande, e maior preocupação desses profissionais é diferenciar os *hackers* éticos e os *crackers* antiéticos, a ondo o *hacker* que segue os conceitos e normais dentro do código de ética vai ajudá-lo a defender a rede, o *cracker*, que mesmo sem conhecer a infraestrutura da rede já à ataca, se tiver a oportunidade de

conhecer como ela é montada e organizada, ele vai explorar todas as vulnerabilidades da rede para tirar vantagem própria.

Falando um pouco sobre a evolução do raqueamento. No final da década de 50, estudantes do MIT (*Massachusetts Institute of Technology*) fizeram os primeiros acessos ao *mainframe* IBM do MIT afins de trabalhar em novas linguagens de programação. Nesse momento, não se tratava de um raqueamento antiético. As quebras de senha surgiram, primeiramente, no início da década de 60, como resposta ao CTSS (*Compatible Time-Sharinf System*), que por sua vez, foi carreado em primeiro lugar em um dos *mainframes* da IBM. Na década de 70, surge um novo tipo de *cracker*, o *cracker* de telefone. Esses *crackers* utilizavam diversos métodos para fazer ligações gratuitas sobre telefones pagos. Mais para frente, combinou-se essa ferramenta com uma linguagem de programação utilizada em computadores. Na década de 80, os *crackers* tomarem conhecimento que qualquer servidor, de qualquer que seja a entidade, que esteja conectado com um modem poderia ser invadido. Uma ferramenta chamada *War dialers* foi desenvolvida com o propósito de procurar *modems* abertos.

> Conforme o preço dos computadores caiu e os usuários se tornaram mais frequentes, as comunidades de *hackers* cresceram, e o termo “raqueamento (*hacking)*” começou a ganhar nova conotação. Os *hackers* já não eram apenas homens jovens sem habilidades sociais com curiosidade insaciável sobre computadores. Uniram-se a indivíduos maliciosos que tentaram invadir e danificar redes corporativas e governamentais suscetíveis, que eles acessavam com o uso de modems (BASTA, 2015, p.8).

Então chegou-se um momento que a pergunta certa a ser feita é, por que contratar um *hacker* ético? E a resposta que Basta (2015, p.12) fala é que as empresas “[...] preferem pagar um *hacker* ético para descobrir as vulnerabilidades de seus sistemas a esperar que um *hacker* antiético faça isso por elas. ”

Hoje, temos *hackers* trabalhando com muitos funcionários em diversas empresas. Uns estão sendo pagos, para achar alguma vulnerabilidade de segurança, sem que os outros funcionários saibam disso, outros se identificam aos funcionários e fazem os testes que precisarem, mas também têm aqueles que

aproveitam da situação e capturam informações privilegiadas da empresa, com o intuito de uso próprio e com interesses particulares.

Agora, vamos explanar algumas das ferramentas utilizadas por esses *hackers*, para quebrar as senhas *wireless*.

As ferramentas que serão apresentadas foram escolhidas por seus motivos. A ferramenta AirCrack-NG por ser uma das ferramentas mais conhecidas e fácil de usar. A ferramenta Reaven por não ser tão conhecida e por isso, mais difícil de usar.

2.2 FERRAMENTA AIRCRACK-NG

É uma ferramenta muito poderosa, capaz de quebrar senhas de roteadores que estão utilizando o protocolo WEP, WPA e WPA2.

Segundo Rufino (2015) é considerada uma das ferramentas mais conhecida e eficiente para quebra de senha, de chaves WEP. A ferramenta AirCrack-NG ataca a fragilidade do protocolo WEP já descrita no artigo “FMSattack” escrito por Fluhrer, Mantin e Shamir.

Falando um pouco mais a respeito da ferramenta, quando se faz a instalação dela em uma distribuição Linux, é instalado juntamente um pacote de ferramentas, uma com cada função, necessária para determinada atividade. Duas dessas ferramentas são o Airodump-ng e o Airdecap-ng. A primeira citada é responsável por coletas os pacotes que estão trafegando na rede. Com uma certa quantia de pacotes, já coletados, é possível fazer a tentativa de quebra, com a ferramenta AirCrack-NG. Quando é feita essa quebra, e a senha por fim revelada, é criado um arquivo por uma extensão “.cap”, onde estão todos os dados do tráfego de pacotes de forma cifrada. A ferramenta Airdecap-ng, combinada com a senha já descoberta, é capaz de transformar toda essa informação legível, ou seja, de forma decifrada. Mais para frente, há um exemplo de quebra WEP com a ferramenta AirCrack-NG com mais detalhes e informações de como fazer.

2.3 FERRAMENTA REAVEN

Segundo Visotto (2014), Reaven é uma ferramenta para quebra de senha utilizada para descobri e explorar vulnerabilidades do protocolo WPS que é utilizado pelos padrões de segurança WPA e WPA2.

Essa ferramenta tem como foco de ataque o código PIN (*Personal identification number*) do roteador ou Ponto de Acesso, sendo qual for o equipamento emissor do sinal wireless. É realizado um ataque de força bruta direcionado ao código PIN. Ao descobrir o verdadeiro código PIN, o equipamento emissor do sinal wireless informa ao atacante a senha do SSID (*Service Set Identifie*), independente da complexidade da senha (VISOTTO, 2014).

2.4 REALIZAÇÃO DOS TESTES E O RESULTADO

Nesse subcapítulo serão apresentados os testes que foram feitos pelo autor da monografia, de quebra das senhas *wireless*. O primeiro teste feito foi com a ferramenta AirCrack-NG, com o protocolo de segurança da WLAN sendo WEP. No segundo teste realizado, ainda foi usada a ferramenta AirCrack-NG, porém o protocolo de segurança usado foi o WPA2. Para o terceiro teste foi usada a outra ferramenta estudada, o Reaver, com o protocolo de segurança da WLAN sendo o WPA2.

Esse trabalho não tem o intuito de mostrar como se quebra uma senha, e nem mesmo como usar as ferramentas abordadas, logo em todos os testes realizados, que serão mostrados a seguir, não serão expostas as linhas de comando, todavia, a resposta que a ferramenta retornar para o usuário da ferramenta esta visível.

Para a realização de todos os testes, foi utilizada a distribuição Linux Kali 1.0.9. Para realizar a instalação das ferramentas, é necessário estar logado como root (administrador local da máquina) e executar os comandos “*apt-get update*”, “*apt-get upgrate*”, “*apt-get install aircrack-ng*” e “*apt-get install reaver*” (PINTO, 2015).

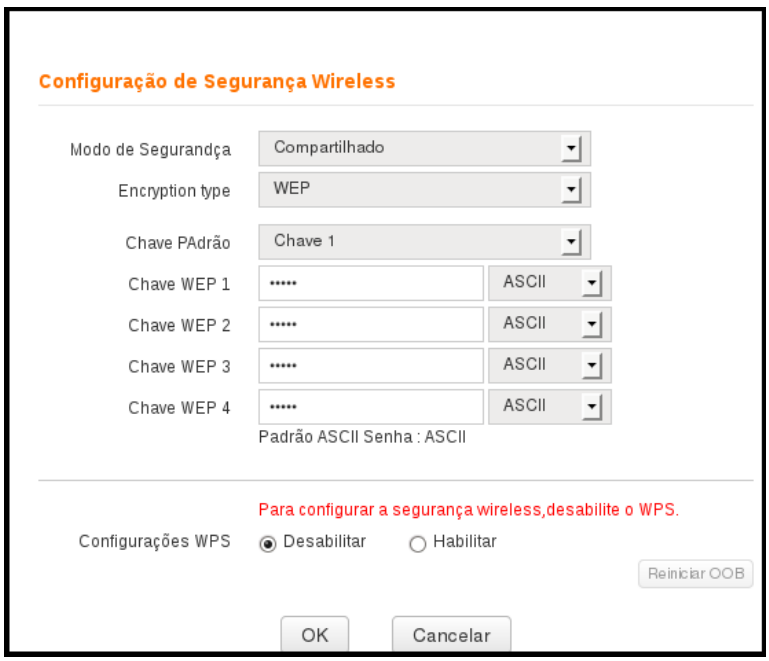
O primeiro comando citado é para atualizar a lista de programas já instalados na distribuição Linux, dessa forma o Sistema Operacional sabe qual programa está desatualizado e qual está com a sua última versão instalada. Logo após isso, o segundo comando faz com que os programas, que têm alguma atualização já disponível, sejam atualizados. Agora, por fim, podemos instalar as duas ferramentas. O terceiro e o quarto comando instalando as respectivas ferramentas (PINTO, 2015).

Após essa breve explicação de como os testes foram feitos, já é possível mostrar como as ferramentas trabalham e de que forma elas atacam.

2.4.1 Teste número 1

O primeiro teste realizado foi com a ferramenta AirCrack-NG, enquanto a rede está protegida com o protocolo WEP. Antes de começar os ataques, foi configurado no roteador esse protocolo e uma determinada senha.

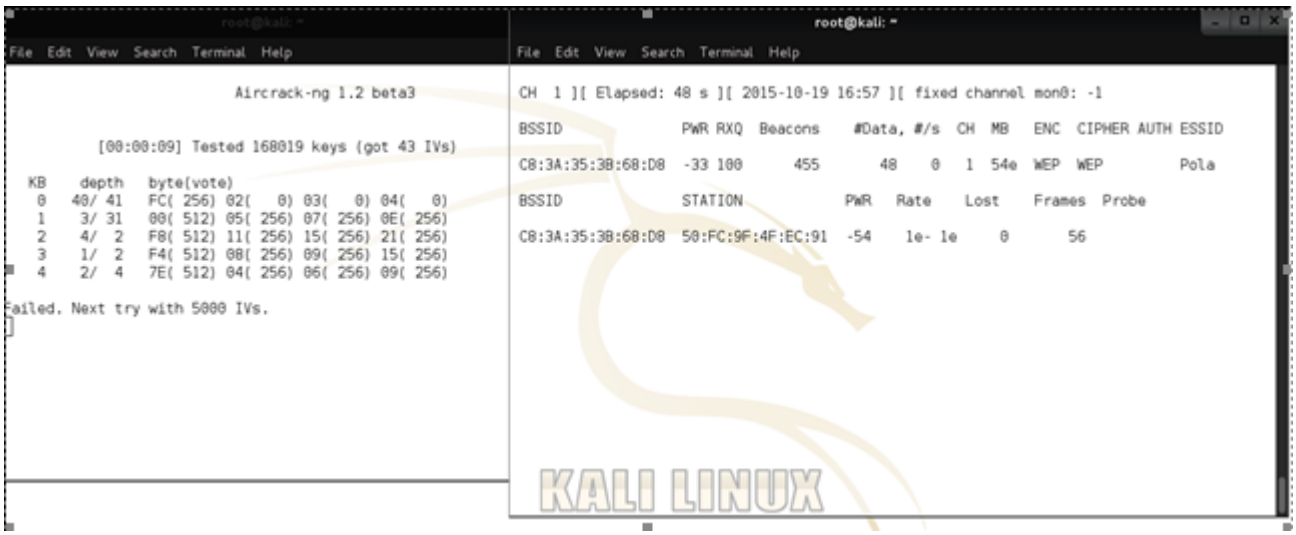
Figura 7: Configuração WEP no roteador



Fonte: elaborado pelo autor

Com essa configuração feita, torna-se possível começar o ataque. Para de fato fazer um ataque direcionado à senha de um roteador com essa ferramenta, é preciso inserir alguns parâmetros anteriormente. As últimas duas etapas mostram a resposta que se espera da ferramenta. Na imagem a seguir, pode ser visto os dois terminais abertos, pois é necessário que os dois últimos comandos sejam executados em terminais diferentes.

Figura 8: Primeira tentativa de quebra WEP



Fonte: elaborado pelo autor

No terminal da direita é possível ver os pacotes de rede que estão trafegando na rede e capturados pela ferramenta. Os pacotes que a ferramenta precisa para quebrar a senha é aqueles que estão na coluna “*#Data*”.

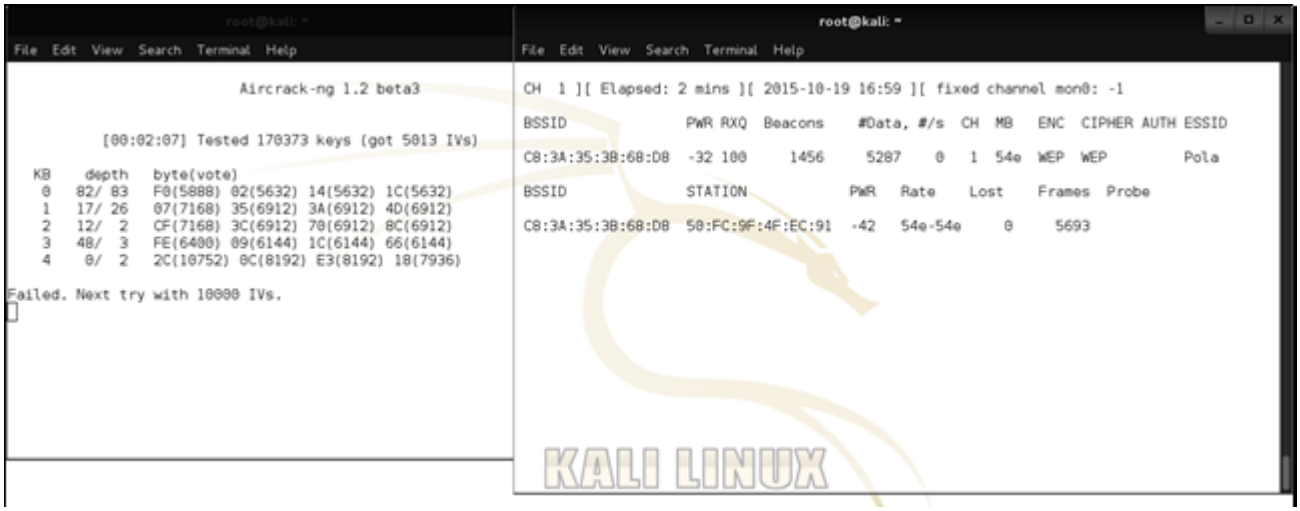
No terminal da esquerda, é a resposta do último comando, que de fato é o que quebra a senha. Na Figura 8, foi executado o comando logo no início da captura de dados (como se pode ver, no terminal da direita, “Elapsed: 48 s”, aos 48 segundos). Até esse momento, a ferramenta tinha capturado 48 pacotes *#Data* e 43 IVs (*Initialization Vectors*) ou Vetores de Inicialização, como visto no terminal da esquerda. Esses IVs estão contidos dentro dos pacotes *#Data*, porém não estão dentro de todos os pacotes. Esse número de IVs foi insuficiente para quebrar a senha e, a própria ferramenta pede para esperar completar 5000 IVs.

Ao completar a quantia de IVs necessária, automaticamente a ferramenta tenta quebrar a senha, como pode ser visto na figura a seguir.

Para que os pacotes #*Data* sejam trafegados na rede, é preciso que haja algum dispositivo (celular, *notebook*, *tablet*, dentre outros) conectado e utilizando a internet. Nesse teste, um *smartphone* ficou conectado na rede e utilizando a internet para que fossem gerados os pacotes #*Data*. Depois de um certo tempo, um segundo *smartphone* foi conectado. Ao se conectar, os pacotes #*Data* aumentaram de uma forma muito mais rápida.

Os dispositivos conectados à rede são visíveis no terminal da direita, sendo a última ou as últimas linhas, logo abaixo da tabela que mostra a quantidade de pacotes #*Data* coletado. Os dispositivos são identificados pelo MAC que se encontram na coluna “STATION”.

Figura 9: Segunda tentativa de quebra WEP

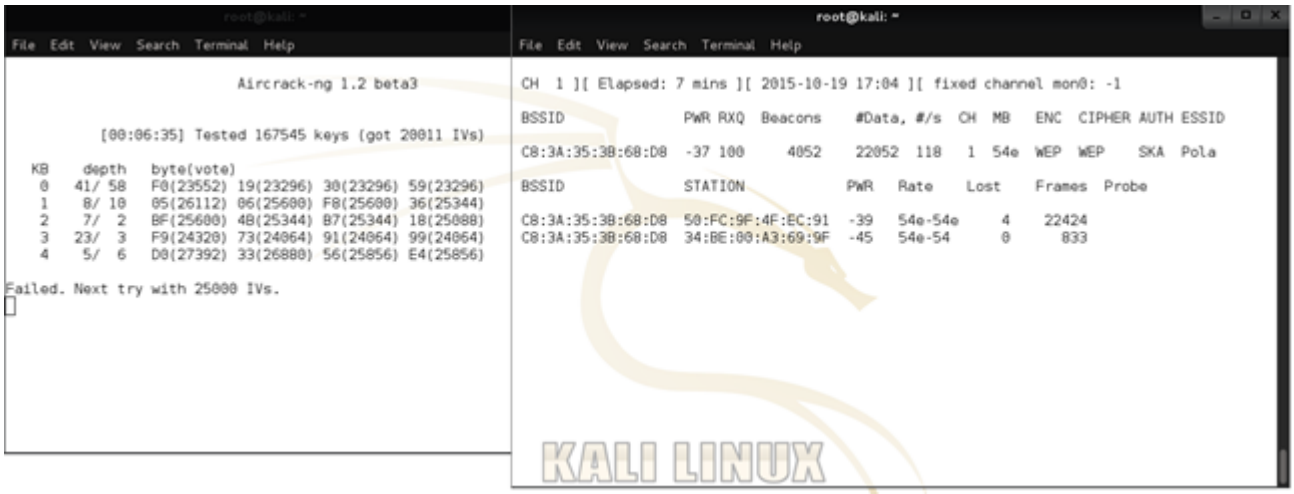


Fonte: elaborado pelo autor

Na figura acima, é possível ver que foi capturado 5287 pacotes #*Data* e 5013 IVs em 2 minutos. Outro detalhe da ferramenta é que quando não consegue quebrar a senha, ela pede mais 5000 IVs para tentar a quebra novamente, como visto na imagem acima. Agora ela pede 10000 IVs.

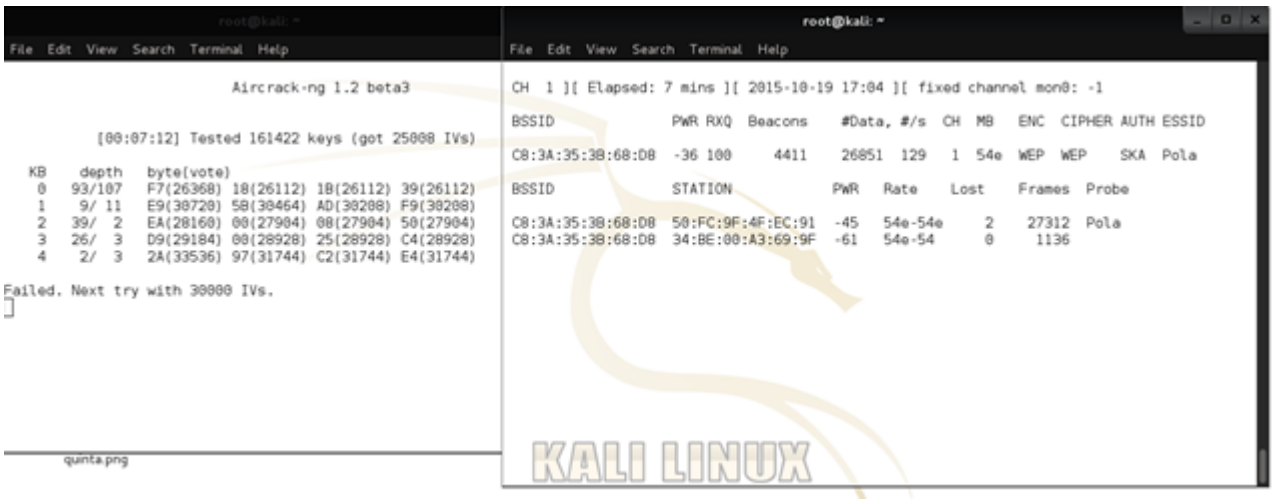
As próximas duas figuras mostrarão a diferença de velocidade na captura de pacotes *#Data* quando adicionado um segundo aparelho utilizando a internet.

Figura 10: Quinta tentativa de quebra WEP



Fonte: elaborado pelo autor

Figura 11: Sexta tentativa de quebra WEP

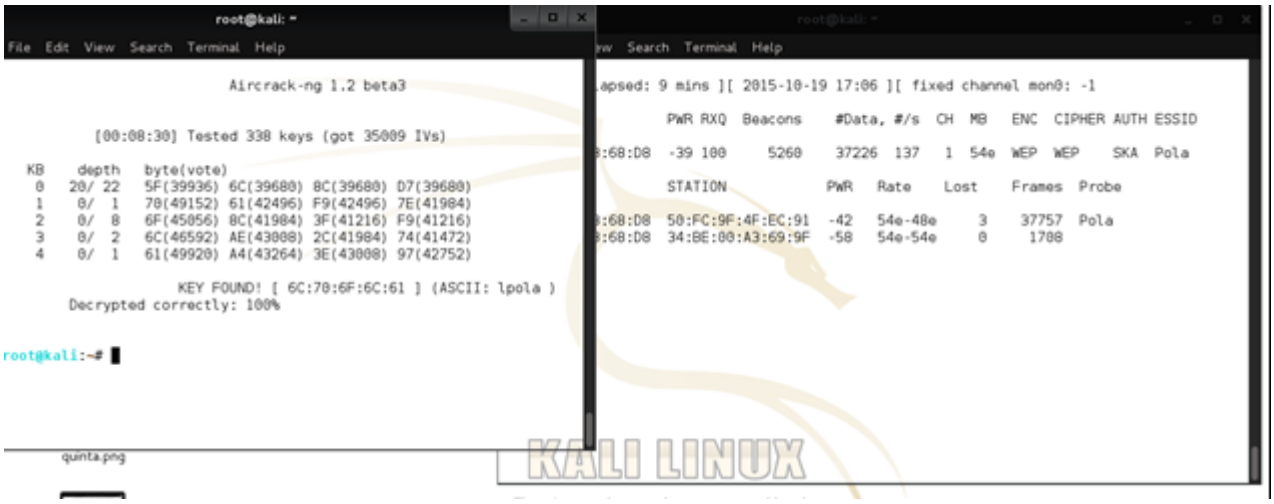


Fonte: elaborado pelo autor

Como pode ser visto, em menos de um minuto, com dois aparelhos conectados na rede, e com os dois utilizando a internet, a ferramenta consegue capturar 4997 IVs, o que demorou 2 minutos da primeira tentativa para a segunda (como mostrado na Figura 10 e Figura 11).

Depois de mais duas tentativas de quebra, a ferramenta consegue quebrar a senha.

Figura 12: A quebra de senha WEP



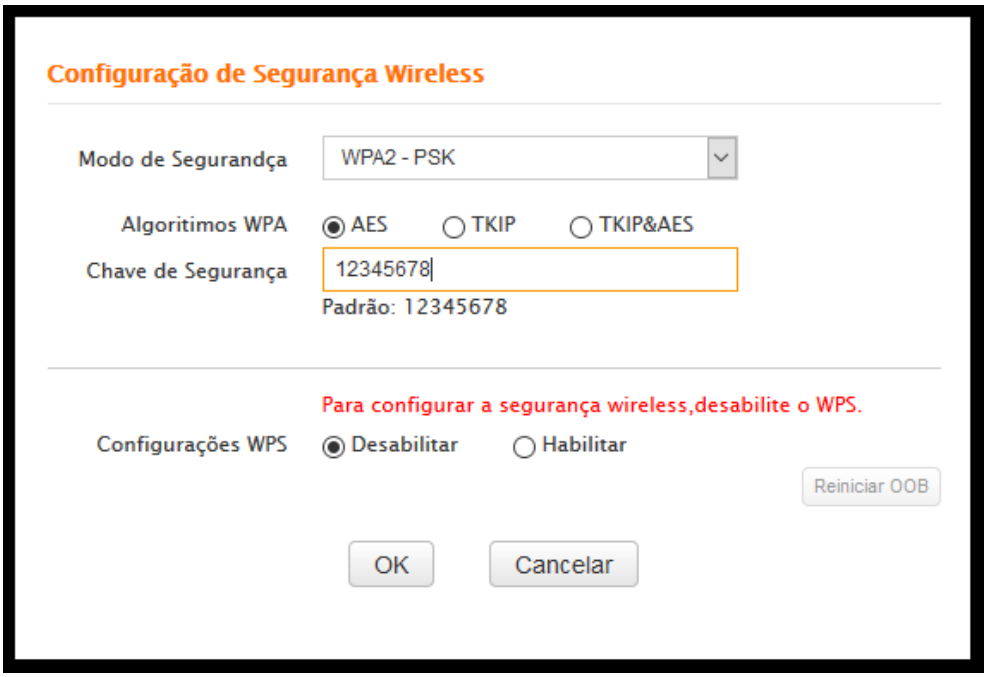
Fonte: elaborado pelo autor

A ferramenta retorna como resposta do último comando, no terminal da esquerda, de forma bem visível a senha da rede *Wi-Fi*. Esse teste levou 9 minutos para que conseguisse quebrar a senha *wireless*. Podemos observar que foram necessários 35009 IVs para quebrar a senha, e para coletar essa quantidade de IVs, foi preciso capturar 37226 pacotes *#Data*. Com essa última figura, é possível fazer mais uma comparação, vendo que do início do sétimo minuto (Figura 10) até o nono minuto (Figura 12), com dois aparelhos conectados, foram capturados 14998 IVs, enquanto nos 2 primeiros minutos (Figura 9), com um aparelho conectado, foram capturados 5013 IVs.

2.4.2 Teste número 2

O segundo teste realizado continua sendo com a ferramenta AirCrack-NG, porém agora o protocolo de segurança da WLAN é o WPA2. Mais uma vez, antes de iniciar os ataques, foram feitas as devidas configurações no roteador, como na figura abaixo.

Figura 13: Configuração WPA2 no roteador

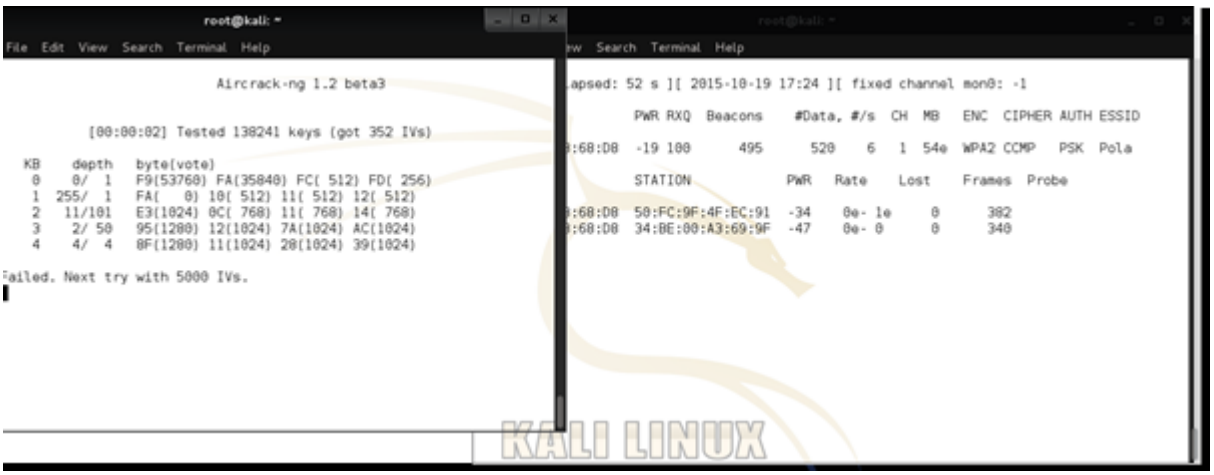


Fonte: elaborado pelo autor

Após a configuração feita, já é possível realizar os ataques contra o roteador. Mais uma vez, foi necessário inserir alguns parâmetros para que a ferramenta pudesse começar o ataque. Pelo fato de ser a mesma ferramenta, todos os dados explicados no teste anterior valem para esse também, sabendo que nesse segundo teste o protocolo segurança será o WPA2, logo estará mudando apenas o comportamento dos pacotes de rede.

Nesse teste que foi realizado, será notada grande diferença em relação ao tempo de captura de IVs e também na dificuldade de obter os Vetores de Inicialização, que é causada pela mudança do protocolo de segurança. Como Vasconcellos (2013) disse, que o protocolo WPA2 é uma melhoria do WPA, que por sua vez veio para solucionar os problemas deixamos pelo WEP, então é válido dizer que o fato de ter mudado o protocolo de segurança do WEP para o WPA vai dificultar a quebra da senha.

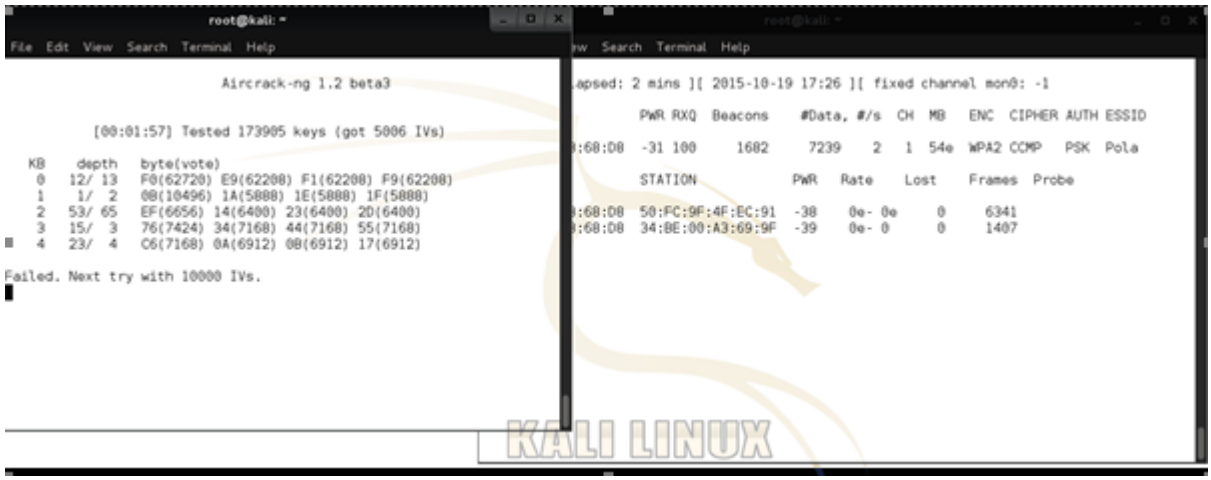
Figura 14: Primeira tentativa de quebra WPA2



Fonte: elaborado pelo autor

Logo no início, aos 52 segundos, foram capturados 520 pacotes *#Data*, mas somente 352 IVs. Aparentemente, comparando com a Figura 8, que mostra a primeira tentativa de quebra WEP, o aumento de pacotes capturados agora é muito maior, todavia a diferença entre os pacotes *#Data* e os IVs coletados também aumentou. Na primeira tentativa de quebra WEP, a diferença foi de 5 pacotes apenas, já na primeira tentativa de quebra WPA2 foi de 168 pacotes.

Figura 15: Segunda tentativa de quebra WPA2

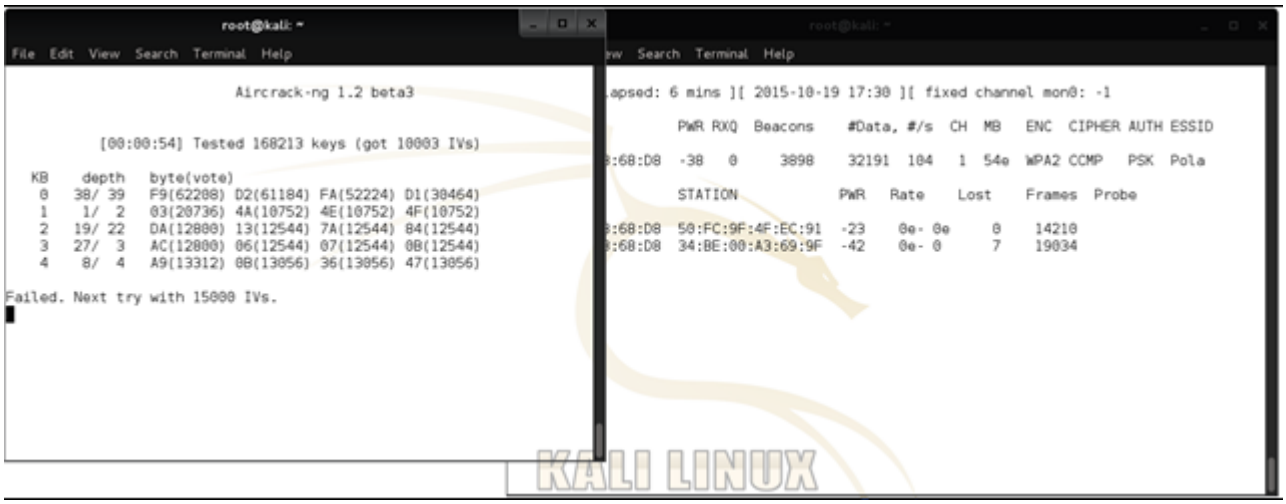


Fonte: elaborado pelo autor

Levou apenas 2 minutos para que o AirCrack-NG conseguisse reunir os 5000 IVs necessários para realizar a segunda tentativa de quebra e, mais uma vez, a diferença de pacotes *#Data* é foi muito maior do que os Vetores de Inicialização coletados. Lembrando que no teste número 1, aos 2 minutos de teste, apenas 1 equipamento estava conectado na rede e usando a internet, e agora no teste número 2, estavam conectados os dois aparelhos.

A partir da terceira tentativa de quebra, a diferença em relação ao tempo que a ferramenta levou para coletar os IVs será notável.

Figura 16: Terceira tentativa de quebra WPA2

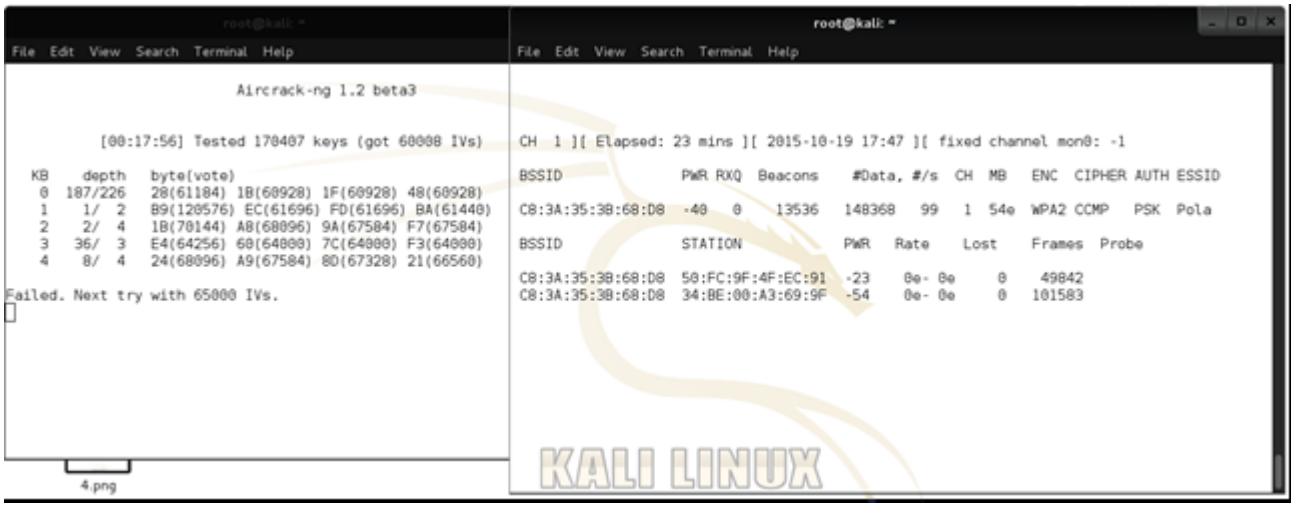


Fonte: elaborado pelo autor

É possível observar na figura acima, que levou 6 minutos para coletar 10000 IVs, e para coletar esses pacotes foi preciso coletar 32191 pacotes *#Data*. Aos 6 minutos, no teste de quebra WEP, já se tinha acumulado perto de 20000 IVs, uma vez que aos 7 minutos foi capturada essa quantidade Vetores de Inicialização, como exibido na Figura 10.

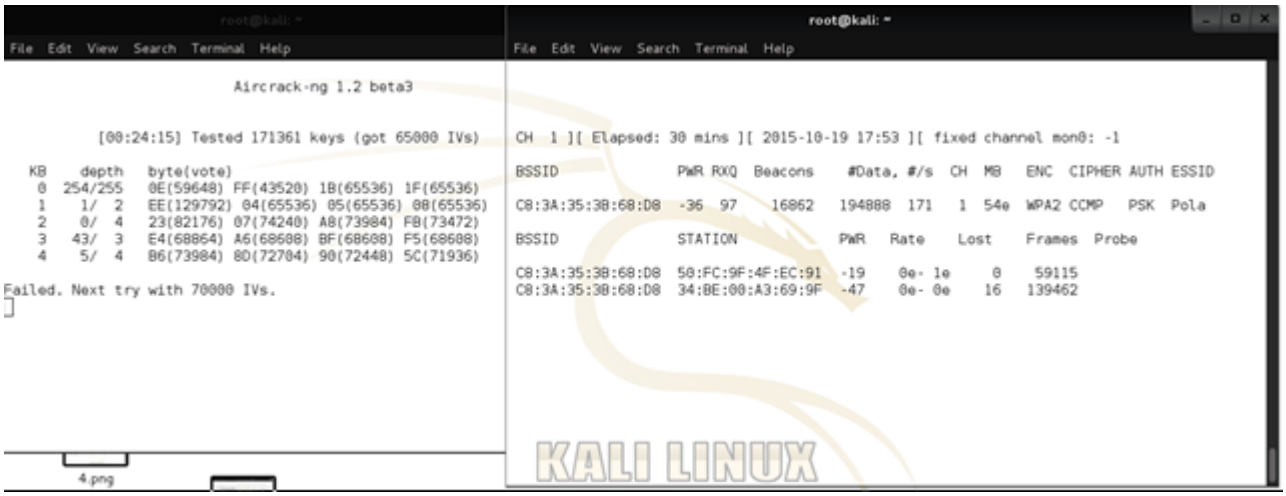
Após essa tentativa, a ferramenta levou em média 1 minuto e 40 segundos entre cada tentativa, até chegar à décima quarta tentativa, como está sendo mostrada nas suas figuras abaixo.

Figura 17: Décima terceira tentativa de quebra WPA2



Fonte: elaborado pelo autor

Figura 18: Décima quarta tentativa de quebra WPA2

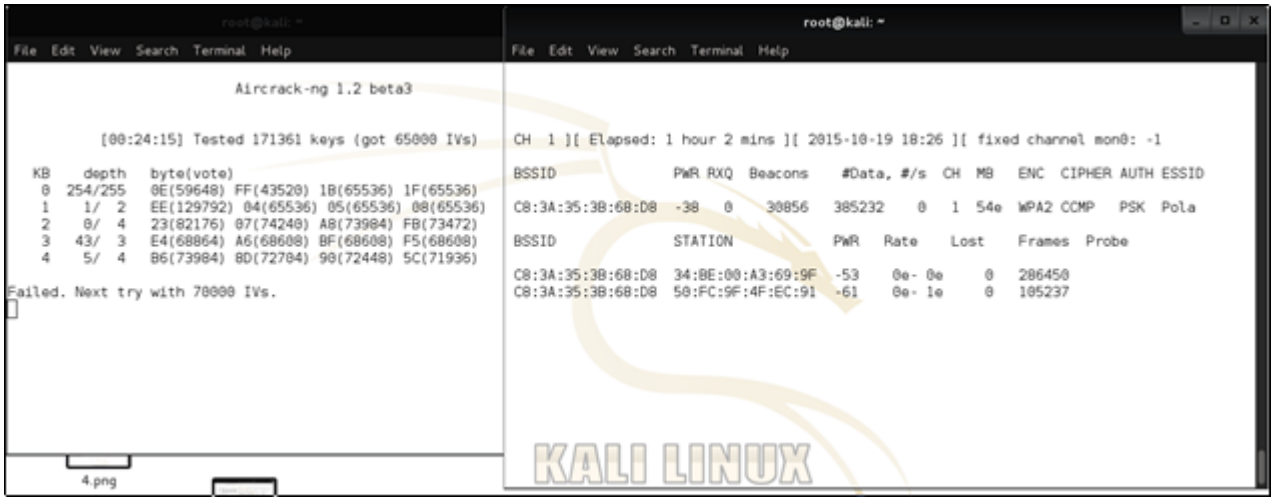


Fonte: elaborado pelo autor

Até a décima terceira tentativa de quebra, a média entre as tentativas era de 1 minuto e 40 segundos, e já na décima quarta tentativa, levou 7 minutos para capturar 5000 IVs e a diferença entre os pacotes *#Data* capturados foi de 46520 pacotes.

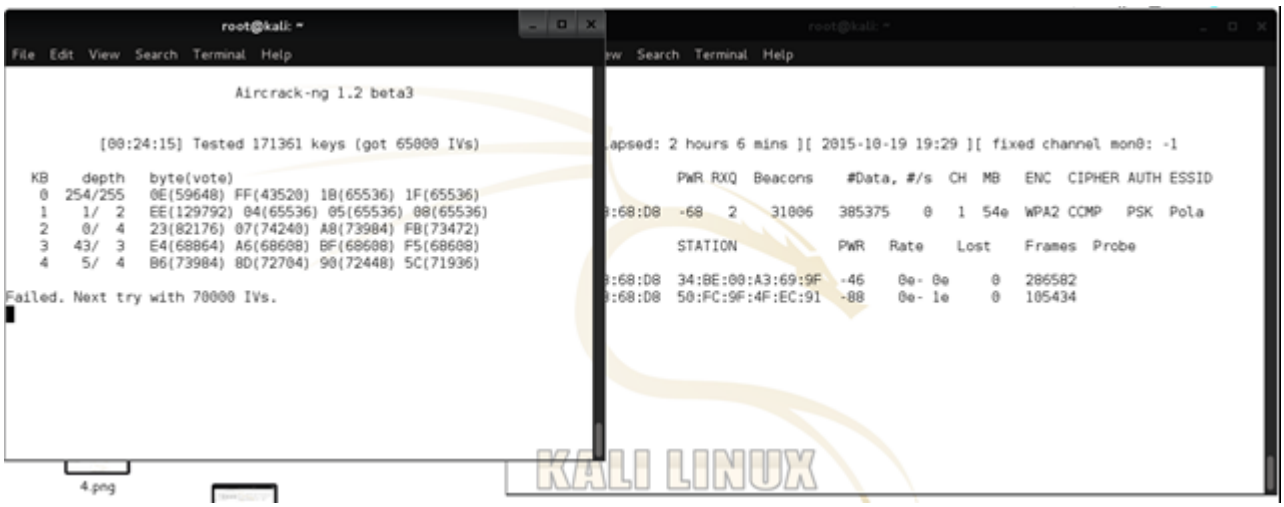
As duas últimas figuras mostram o resultado final desse teste.

Figura 19: Décima quinta tentativa de quebra WPA2



Fonte: elaborado pelo autor

Figura 20: Décima sexta tentativa de quebra WPA2



Fonte: elaborado pelo autor

A ferramenta levou mais 32 minutos para capturar 385232 pacotes *#Data* no total, porém o número de Vetores de Inicialização capturados não foi alterado. Foi deixado a ferramenta trabalhar por mais 1 hora e 4 minutos, porém o número de IVs continuou o mesmo, e o número de pacotes *#Data* subiram de 385232 para 38375.

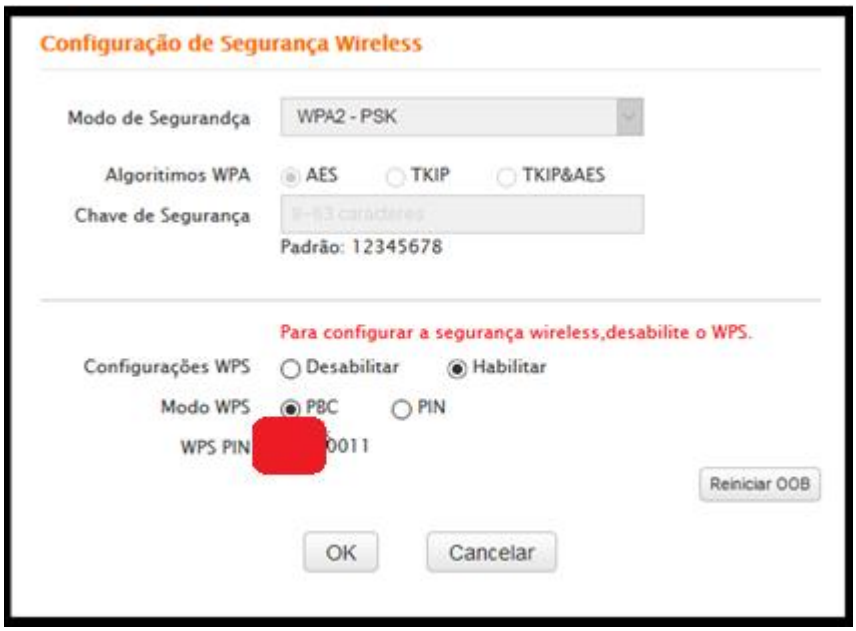
Levando em consideração esses dados coletados, e a informação de que a ferramenta AirCrack-NG levaria em torno de duas semanas para quebrar uma

senha com o protocolo de segurança WPA2, então o teste foi encerrado, sem mesmo ter conseguido descobrir a senha.

2.4.3 Teste número 3

O terceiro teste realizado foi com a ferramenta Reaver, enquanto o protocolo de segurança de rede utilizado foi o WPA2. Antes de começar o ataque, foram feitas algumas configurações no roteador.

Figura 21: Configuração WPA2/WPS no roteador



Fonte: elaborado pelo autor

Antes de realizar o ataque, foi necessário preparar a máquina com alguns comandos, todavia será mostrado apenas o ataque ao roteador e a resposta da ferramenta.

Após todos os preparativos para começar os ataques, a primeira resposta que é recebida da ferramenta foi uma tela dinâmica, mostrando as tentativas de quebra do PIN do roteador, com a técnica de força bruta. O PIN do roteador é formado por 8 números. Fazendo uma conta bem simples, é possível saber que existem 100000000 de possíveis PIN.

Nos roteadores, nos pontos de acesso, o PIN é formado por 8 números, porém é dividido em dois blocos, ondo o primeiro bloco é composto de 4 números e o terceiro de 3 números. O oitavo número é o resultado de um cálculo feito com os demais números. Então a primeira quebra a ser feita é do primeiro bloco, que totaliza 10000 possibilidades. Assim que a ferramenta descobrir o primeiro bloco, ele começa a procurar o segundo bloco que têm 1000 possibilidades, gerando um total de 11000 possíveis PINs, ao invés de 100000000.

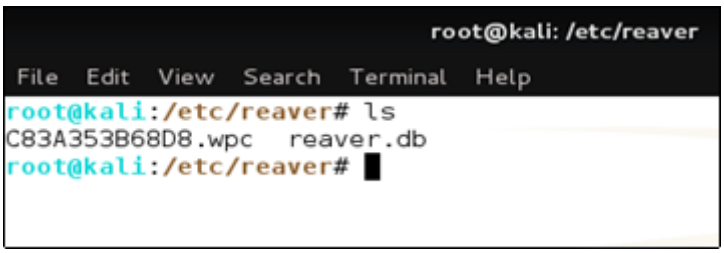
Como explicado em um fórum especializado na distribuição Linux BlackTrack (antiga versão do Kali):

> *Reaver attacks on WPS supported routers and WPS pin consist of 8 digits. This key is divided in 2 parts, 1 part consisting of 4 digits and other part of 3 digits, last digit is some random index number i think. Anyway, This makes upto 11,000 key combinations which reaver brute forces one by one*[1] (MUNNIBHAI, 2013, p.1).

Em um outro site, dessa vez especializado na distribuição Linux, mostra a conta feita por eles: "*Now the guesses would be 10^4 + 10^3 (not 10^4 *10 ^3). Now we need 11,000 guesses*" [2] (KALITUTORIALS, 2014).

Quando a ataque é iniciado, a ferramenta cria um arquivo de texto com o nome do MAC do roteador alvo, no meu caso foi C83A353B68D8.wpc, com todos os números de PINs, sequencialmente, como mostrado na figura abaixo.

Figura 22: Diretório e arquivo utilizado para o ataque

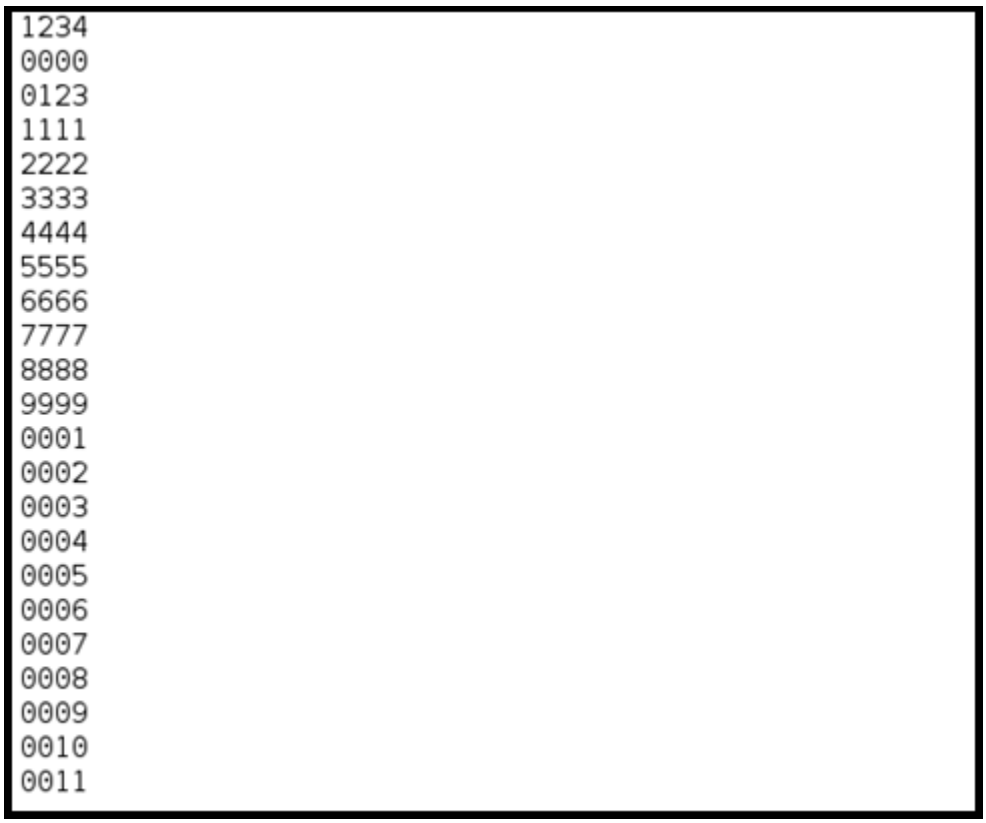


Fonte: elaborado pelo autor

[1] Reaver ataque roteadores com suporte WPS e WPS pin consiste de 8 dígitos. Essa chave é dividida em 2 partes. Parte 1 consiste de 4 dígitos e a outra parte de 3 dígitos, último dígito é um número aleatório eu acho. De qualquer maneira, isso faz com que até 11000 combinações de chaves que reaver força bruta uma a uma.
[2] Agora o palpite seria 10^4 + 10^3 (não 10^4 * 10^3). Agora nós precisamos de 11000 palpites.

Esse arquivo se encontra dentro do diretório /etc/reaver que foi criado quando foi instalada a ferramenta. O começo do arquivo é assim:

Figura 23: Arquivo com números PINs, primeira parte

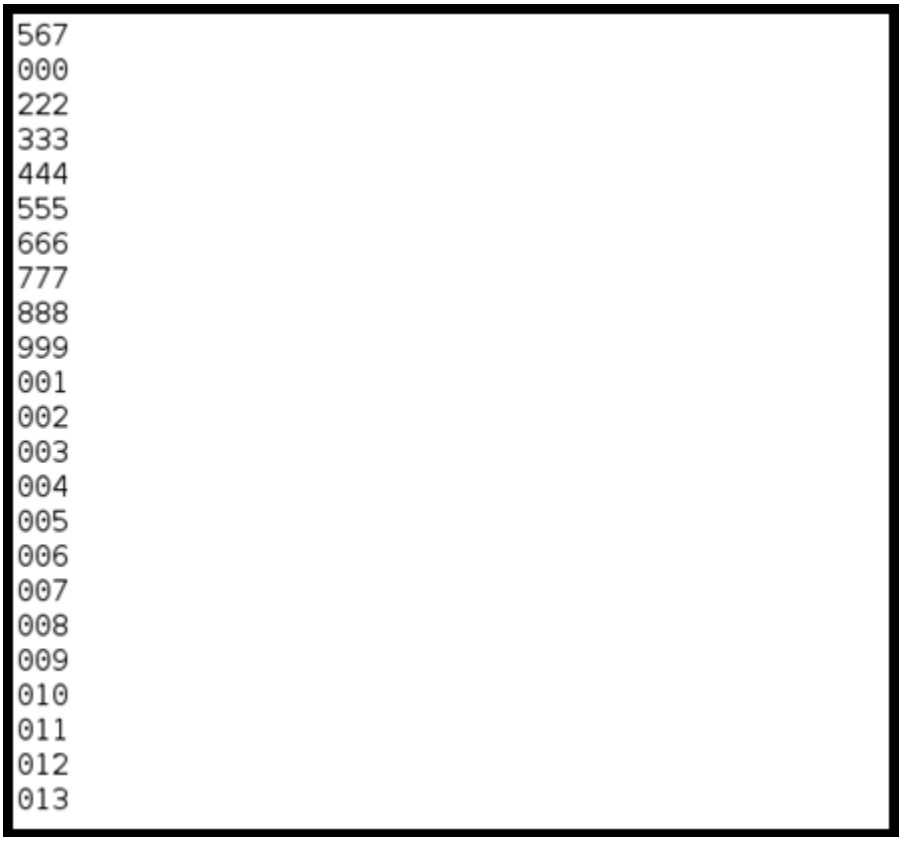


Fonte: elaborado pelo autor

A partir do “0011”, ele continua sequencialmente até o “9999”, exceto os números que já foram usados, no caso, “1111”, “2222”, “3333”, “4444”, “5555”, “6666”, “7777“, “8888”, “9999”.

Quando chegar no último número, que será o “9998”, então começa a contar os números do segundo bloco, que são formados por 3 dígitos. Lembrando que o primeiro PIN que a ferramenta tenta é o “12345670”, pois do primeiro bloco, a primeira parte dos PINs é “1234”, e como será visto na próxima figura, a segunda parte do PIN, os primeiros três dígitos são “567”, e como já foi explicado, o oitavo número é o *check sum*, ou seja, um número relacionado matematicamente com os demais 7 dígitos.

Figura 24: Arquivo com números PINs, segunda parte



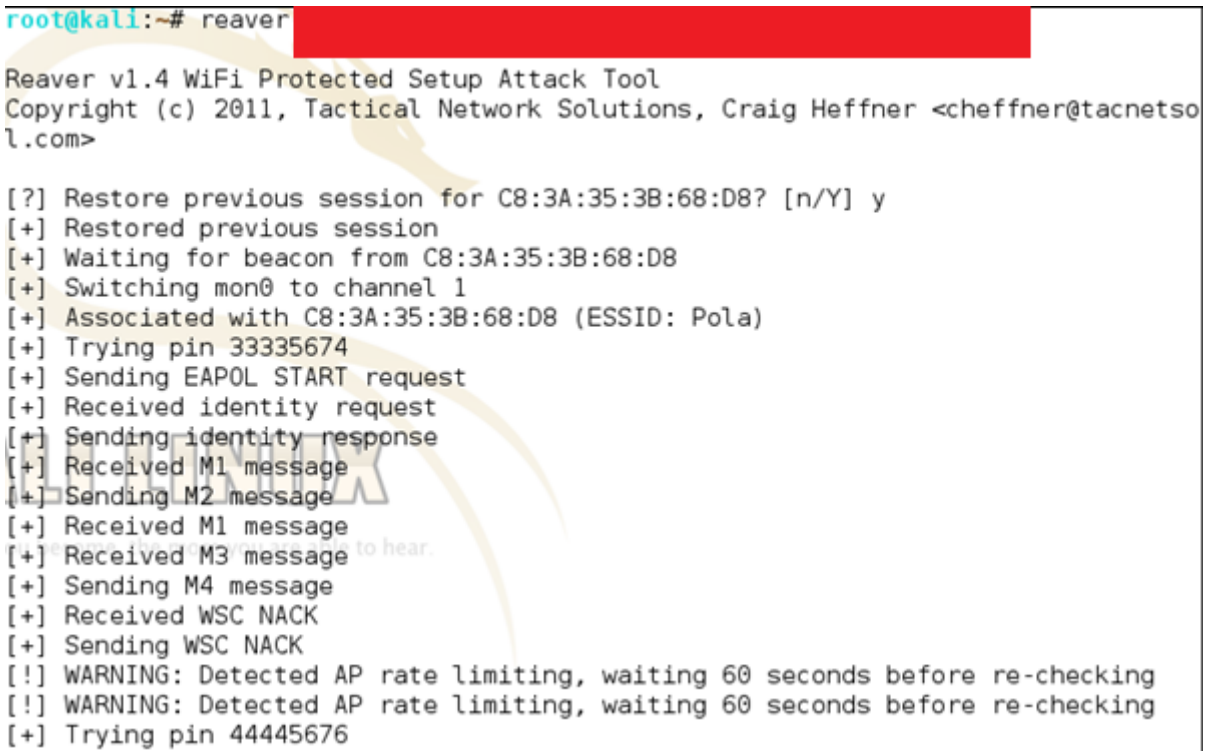
Fonte: elaborado pelo autor

Mais uma vez, após a sequência “013” ele continua até o “998”, pois não repete os números já digitados anteriormente, que são “111”, “222”, “333”, “444”, “555”, “666“, “777”, “888”, “999”.

Na próxima imagem a ser exibida, será mostrado o primeiro momento da ferramenta, em que ela tenta faze a primeira tentativa de quebra, e também o retorno.

Em teoria, é possível realizar o ataque de força bruta de forma muito rápida, ao ponto de testar cada 1 PIN por segundo (1 segundo / PIN), todavia para que a ferramenta consiga processar todos os dados, e mais o tempo que leva para os pacotes trafegarem a rede, demora em torno de 3 segundos por PIN. Estatisticamente, para que a ferramenta tente todos os 11000 PINs levaria 33000 segundos, ou seja, 9,1666 horas.

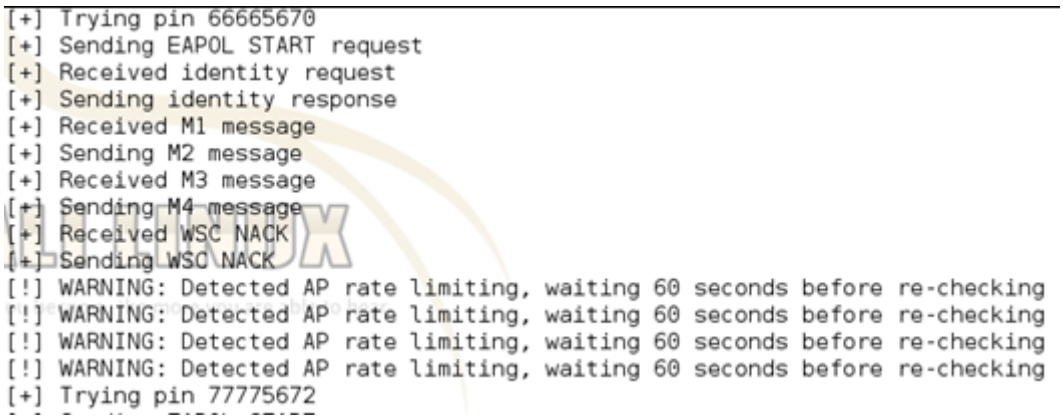
Figura 25: Primeiro momento da ferramenta reaver



Fonte: elaborado pelo autor

Quando o teste foi iniciado, em menos de 10 segundos apareceu uma mensagem de erro. Ao investigar o ocorrido (utilizando um dos comandos que utilizei para preparar o cenário) foi identificado que o roteador percebeu o ataque de força bruta, e bloqueou o tráfego dos pacotes.

Figura 26: Segundo momento da ferramenta reaver



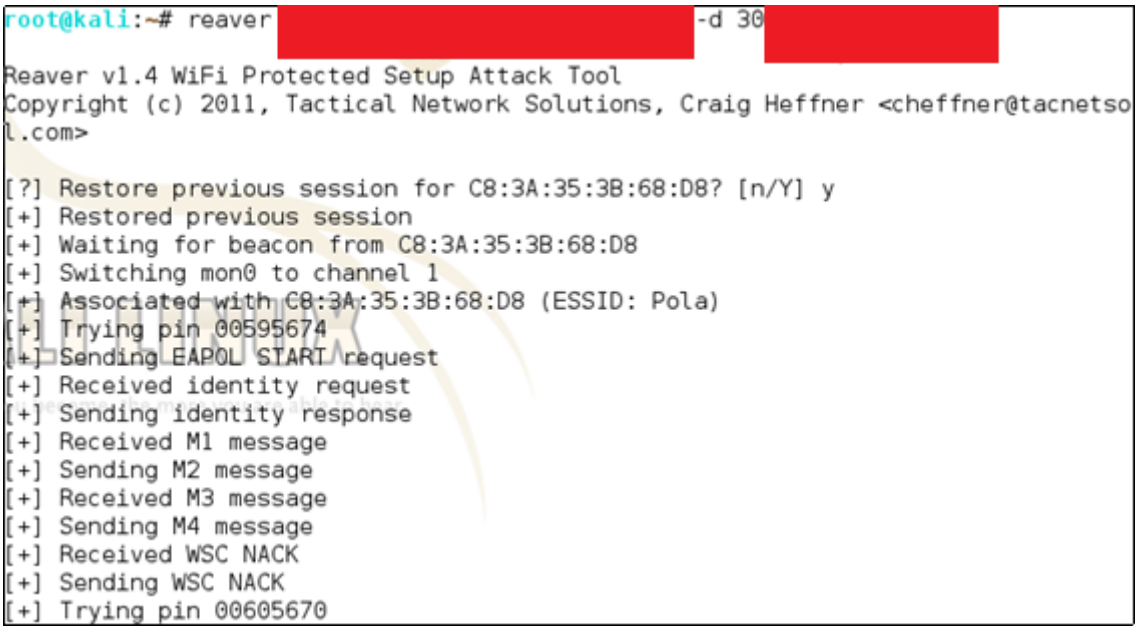
Fonte: elaborado pelo autor

Figura 27: Terceiro momento da ferramenta reaver

Fonte: elaborado pelo autor

Para resolver esse problema com o roteador, foi necessário fazer um reajuste no comando de execução. Foi adicionado um novo parâmetro.

Figura 28: Solução para o problema com o roteador



Fonte: elaborado pelo autor

O parâmetro “-d 30” fez com que as tentativas de inserção de PIN fossem atrasadas em 30 segundos, uma da outra, para que então o roteador não entendesse como um ataque.

Figura 29: Primeiro momento, após a mudança no código

```
[+] Trying pin 00615679
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00625678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00635677
```

Fonte: elaborado pelo autor

Figura 30: Segundo momento, após a mudança no código

```
[+] Trying pin 00645676
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 0.69% complete @ 2015-10-19 23:18:26 (32 seconds/pin)
[+] Max time remaining at this rate: 97:06:08 (10924 pins left to try)
[+] Trying pin 00655675
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00665674
```

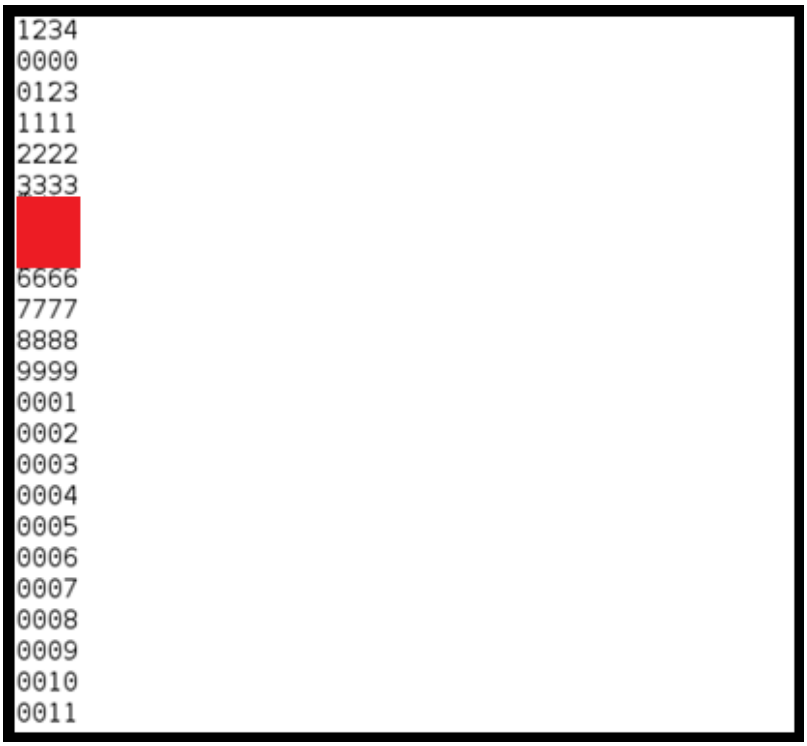
Fonte: elaborado pelo autor

Como pode ser visto, os pacotes não foram mais detectados como maliciosos pelo roteador e conseguiu efetuar os ataques normalmente. Na Figura 30, mostra exatamente qual o tempo que leva entre um ataque e outro, que nesse caso foi de 32 segundos.

Para a conclusão desse teste, foi feita uma modificação no arquivo “C83A353B68D8.wpc” que se encontra no diretório “/etc/reaver”. É importante ressaltar que independente dessa modificação ou não, o resultado seria o mesmo, mudando apenas o tempo em que a ferramenta levaria para quebrar a senha. Mesmo que o objetivo desses testes sejam provar a eficiente de cada ferramenta, nesse teste isso pode ser feito através de uma análise estatística.

Pelo fato do teste ter sido realizado em um ambiente controlado, o autor tem conhecimento de qual é o PIN do roteador que está sendo alvo dos ataques, logo a mudança que foi feita no arquivo já mencionado foi a inserção dos 4 primeiros dígitos do PIN no início da lista, como podemos ver na imagem abaixo.

Figura 31: Inserção dos primeiros dígitos do PIN



Fonte: elaborado pelo autor

Assim como na Figura 21, a Figura 31 tive os 4 primeiros dígitos censurados, pelo fato de ser um número único de cada roteador. Como é possível observar, os dígitos inseridos estão entre o “3333” e o “6666”. Foram adicionados 2 números, com 4 dígitos cada um, sendo o segundo número o PIN do roteador. Ao rodar a ferramenta novamente, desde o início, foram esses os resultados obtidos.

Figura 32: Primeiro momento, depois da modificação

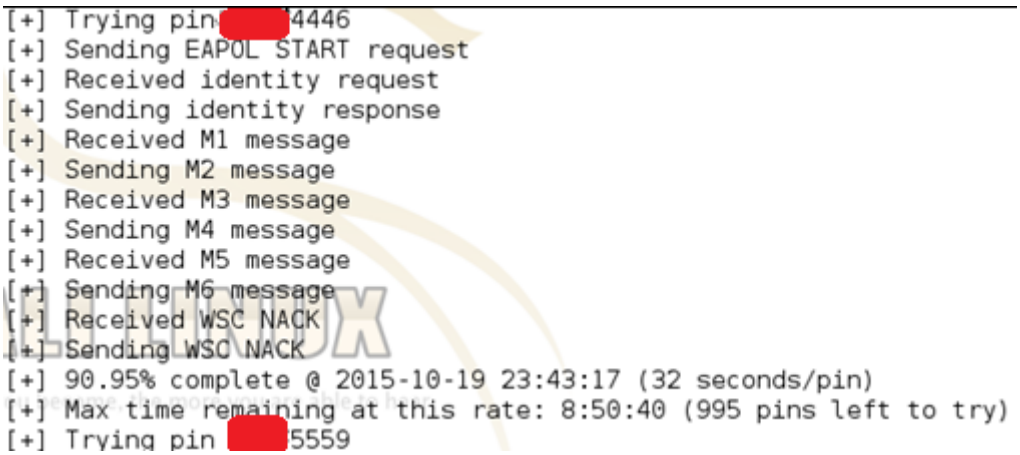
Fonte: elaborado pelo autor

Figura 33: Descoberta da primeira parte do PIN

Fonte: elaborado pelo autor

Na Figura 33, é possível ver os números inseridos no arquivo. Pode-se observar também que foi descoberto qual era os quatro primeiros dígitos do PIN pela mudança dos últimos três números do PIN. Até agora, a segunda parte do PIN (que é formada por três dígitos) sempre foi “567”, porém no final da figura, é possível ver que esse número mudou para “000”. Na figura 24, é possível ver que realmente é essa a sequência, começando do “567” e depois seguindo a ordem.

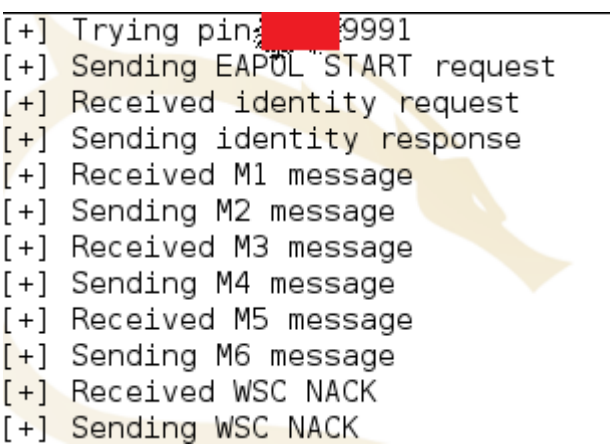
Figura 34: Segundo momento, após a descoberta da primeira parte do PIN



Fonte: elaborado pelo autor

Na imagem acima, está o segundo momento que a ferramenta retorna, mostrando também a média de duração entre cada pacote disparado na rede.

Figura 35: Último momento, antes da descoberta completa do PIN



Fonte: elaborado pelo autor

Figura 36: Descoberta completa do PIN

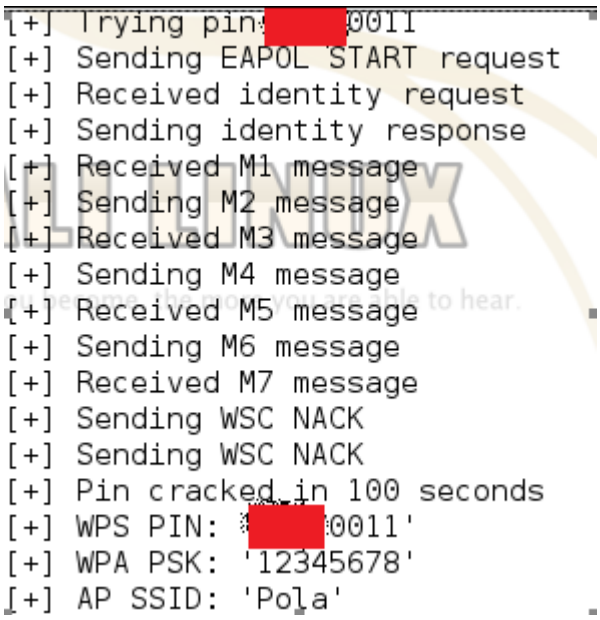
Fonte: elaborado pelo autor

O motivo de a segunda parte do PIN não ter sida ocultada, foi que é um número baixo, e facilmente a ferramenta chegaria nesse resultado. Como visto na Figura 36, o número do PIN foi descoberto, todavia a rede estava desprotegida de senha, provando que a ferramenta não ataca a senha *wireless* e sim o próprio roteador. Segue abaixo a configuração de senha, e a quebra da rede.

Figura 37: Configuração de senha na rede WPA2/PSK

Fonte: elaborado pelo autor

Figura 38: Descoberta completa do PIN, com senha



Fonte: elaborado pelo autor

Por fim, o teste prático foi finalizado. Com a conclusão levantada acima, em que a ferramenta ataca diretamente o roteador, e não a senha *wireless* do alvo, ficou claro que não seria necessário realizar o teste em uma rede com proteção WEP, pois o resultado seria exatamente o mesmo.

Nas figuras 36 e 38, é possível ver a frase *Pin cracked in 429 seconds* e *Pin cracked in 100 seconds* respectivamente. Essa informação nos mostra quanto tempo levou para descobrir o PIN do roteador, todavia como o arquivo com todos os possíveis PINs fora modificado, essa informação não é íntegra, mas podemos realizar uma operação matemática e levantar uma especulação estatística. Sabendo qual é o PIN do roteador, é possível fazer uma multiplicação com o tempo estimado entre uma tentativa e outra, no caso, de 32 segundos. Pelo motivo já citado anteriormente, não será exposto qual é o verdadeiro PIN do roteador, todavia ao fazer o cálculo, o resultado foi que levaria um pouco mais de 35 horas para chegar até o PIN do roteador. Tende essa mesma base, a ferramenta levaria mais de 97 horas e 30 minutos para realizar o ataque completo, com todos os possíveis PINs, um valor bem diferente do qual levaria em tese, tendo em base que levaria 3 segundos por PIN.

3 CONSIDERAÇÕES FINAIS

Ao finalizarmos todos os estudos e testes, foi possível absorver muita informação e conhecimento, tanto no tema abordado quanto na área escolhida, que foi a segurança da informação.

Também fomos muito cautelosos ao falar sobre raqueamento, pois essa palavra, muitas vezes, é associada a uma pessoa com má índole, que deseja roubar informações ou simplesmente destruí-las. O nosso objetivo foi mostrar que os *hackers* não são somente aqueles com má fé, com desejo de prejudicar o próximo, mas que também muitos deles utilizam de suas habilidades técnicas para o benefício de outros, claro que, não de graça.

Por fim, chegamos ao ponto em que comparamos a eficácia das duas ferramentas nos três testes realizados. No primeiro teste, obtemos um resultado muito favorável para o possível invasor, pois a senha foi quebrada em menos de 10 minutos. Todavia o cenário do primeiro teste foi o mais fraco, em relação a segurança. No segundo teste, nós chegamos a um “beco sem saída”, onde utilizamos a mesma ferramenta do primeiro teste, AirCrack-NG. Quando dizemos que chegamos a um “beco sem saída”, estamos nos referindo que não conseguimos descobrir qual era a senha do roteador, uma vez que a segurança da rede *wireless* foi diferente da que utilizamos no primeiro teste. O protocolo de segurança utilizado é considera o melhor dentre os demais. Por fim, no terceiro teste, foi constatado que não importa qual seja a complexidade da senha, muito menos qual é o protocolo de segurança que protege a rede *wireless*, porque a segunda ferramenta, Reaver, tem como foco de ataque o próprio roteador, ou seja, a senha não ocasionará diferença nenhuma na quebra da senha, como foi provado no terceiro teste, onde descobrimos o PIN do roteador, quando a rede não estava protegida por nenhuma senha, e também quando foi configurado uma senha de proteção. No terceiro teste, os dois cenários que utilizamos foram o pior possível (sem nenhuma senha de proteção) e o considerado melhor em relação a segurança *wireless* (WPA2).

Tendo essas informações em mãos, é possível dizermos que a última hipótese citada, a hipótese c) A ferramenta Reaven tem maior eficiência que a

AirCrack-NG é a verdadeira, pois essa ferramenta sempre mostrará a senha como resposta dos ataques, ainda que possa levar cerca de 98 horas, mas a ferramenta sempre trará como retorno a senha de proteção *wireless*.

Como sugestão para trabalhos futuros, seria interessante explorar os pontos fracos dessas duas ferramentas, com o intuito de aplicar as configurações necessárias na rede para defender os usuários desse tipo de ataque.

REFERÊNCIAS

AGUADO, Alexandre. **Criptografia**. Americana: Fatec Americana. 2014. (Informação Verbal).

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico**: elaboração de trabalhos na graduação. 9. ed. São Paulo: Atlas, 2009.

BARROS, Aidil Jesus da Silveira; LEHFELD, Neide Aparecida de Souza. 3. ed. São Paulo: Pearson Prentice Hall, 2007

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. 2. ed. São Paulo: Cengage Learning, 2014

COSTAS, Jefferson. **Apostila de Redes de computadores**. São Paulo, 2010. Disponível em: <http://www.jeffersoncosta.com.br/redes.pdf>. Acesso em: 14 set. 2015. 22h30.

DANTAS, Marcus Leal. **Segurança da informação**: Uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. Disponível em: http://www.marcusdantas. com.br/files/seguranca_informacao.pdf. Acesso em: 14 set. 2015. 22h40.

DICIO**. Significado de Informação**. (2015). Disponível em: http://www.dicio.com.br / informacao/**.** Acesso em: 14 out. 2015, às 22h06.

DICIONÁRIO PRIBERAM DA LÍNGUA PORTUGUESA. **Perigo**. (2008-2013). Disponível em: https://www.priberam.pt/dlpo/perigo. Acesso em: 19 set. 2015, às 22h06.

GERHARDT, Tatiana Engel; Silveira, Denise Tolfo. **Métodos de Pesquisa**. Porto Alegre: UFRGS, 2009. Disponível em: http://www.ufrgs.br/cursopgdr/ downloadsSerie/derad005.pdf. Acesso em: 4 set. 2015. 23h05.

GOLDREICH, Oded. **Fundamentos da Criptografia.** Ferramentas Básicas. Tradução Ruy J. Guerra B. de Queiroz. Cambridge: University Press, 2001. Disponível em: http://www.cin.ufpe.br/~ruy/crypto/fundamentos.pdf. Acesso em: 15 set. 2015. 23h35.

FERREIRA, Aurélio Buarque de Holanda. **Miniaurélio Século XXI Escolar**. 4. ed. rev. ampliada. Rio de Janeiro: Nova Fronteira, 2000.

KALITUTORIALS. **Hack WPA/WPA2 WPS** - Reaver - Kali Linux. 2014. Disponível em: http://www.kalitutorials.net/2014/04/hack-wpawpa2-wps-reaver-kali-linux.html. Acesso em: 25 out. 2015. 22h11.

MICHAELIS. **Dicionário de Português Online.** (2011). Disponível em: http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=seguro e http://michaelis.uol.com.br/moderno/portugues/definicao/dado_938420.html. Acesso em: 14 out. 2015. 22h06.

MUNNIBHAI. Forum: **[SOLVED] Resuming reaver from specific pin and onwards**. 2013. Disponível em: http://www.backtracklinux.org/forums/showthread.php?t=62523. Acesso em: 25 out. 2015. 22h02.

OLIVEIRA, Wender F. **Gestão da Segurança da Informação**. Brasília-DF, 2011. Disponível em: http://lms.ead1.com.br/webfolio/ Mod4467/gestao_da_seguranca _da_ informacao.pdf. Acesso em: 28 ago. 2015. 13h15.

PELLEGRINI, Jerônimo C. **Introdução à Criptografia e seus Fundamentos**. 2015. Disponível em: http://aleph0.info/cursos/ic/notas/cripto.pdf. Acesso em: 16 set. 2015. 00h32.

PINHEIRO, José Mauricio Santos. **Cifras em Bloco e Cifras de Fluxo**. 2010. Disponível em: http://www.projetoderedes.com.br/artigos/imagens/Image146.gif. Acesso em: 15 set. 2015. 23h48.

PINTO, Juliane. **Segurança em Sistema Operacional e Redes de Computadores I**. Americana: Fatec Americana. 2015. (Informação Verbal).

RUFINO, Nelson Murilo de O. **Segurança em Redes sem Fio**. 4ª ed. São Paulo: Novatec, 2015.

SOUSA, Airton Ribeiro de. **Redes de computadores**: Tecnologia de rede – Arquitetura Wireless. Disponível em: <http://www.lanwan.com.br/Aulas_Senac/Tecnico_Redes_Noturno/Aula%2029062010%20-%20Redes%20sem%20Fio%20-%20WEP.pdf>. Acesso em: 15 set. 2015, às 20h24.

VASCONCELLOS, Ronaldo. **Segurança em rede sem fio**. Rio de Janeiro: Escola superior de redes. 2013. Disponível em: <https://pt.scribd.com/doc/157215890/Seguranca-em-Redes-sem-Fio>. Acesso em: 25 set. 2015. 17h06.

VISOTTO, Clayton. Reaver. **Descobrindo senhas Wi-Fi**. 2014. Disponível em: gahttp://www.vivaolinux. com.br/artigo/Reaver-Descobrindo-senhas-Wi-Fi. Acesso em: 17 mai. 2015. 16h20.

ZEINDIN, Denise Carla A. *et al*. **A tecnologia do future Wi-Fi (*Wireless Fidelity*).** Blumenau: FURB (Universidade Regional de Blumenau). Disponível em: http://www.inf.furb.br/~zamba/artigos/Artigo_Wireless_Uniplac_2003_V1.pdf. Acesso em: 14 set. 2015. 22h00.