UNIVERSIDADE DO SAGRADO CORAÇÃO

DYLAN MARTINS JANINE DE ANDRADE

ANÁLISE DE RISCOS E VULNERABILIDADES EM REDES SEM FIO

BAURU
2016

DYLAN MARTINS JANINE DE ANDRADE

ANÁLISE DE RISCOS E VULNERABILIDADES EM REDES SEM FIO

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração, como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2016

Andrade, Dylan Martins Janine de

A5531a

Análise de Riscos e Vulnerabilidades em redes sem fio / Dylan Martins Janine de Andrade. -- 2016.

38f. : il.

Orientador: Prof. M.e Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Segurança. 2. Redes sem fio. 3. Teste de penetração. 4. Vulnerabilidade. 5. Força-Bruta. I. Martins, Henrique Pachioni. II. Título.

DYLAN MARTINS JANINE DE ANDRADE

ANÁLISE DE RISCOS E VULNERABILIDADES EM REDES SEM FIO

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração, como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

Banca examinadora:

_____
Prof. Me. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade do Sagrado Coração

Bauru, 7 de dezembro de 2016.

Dedico este trabalho de conclusão de curso à minha família e aos meus amigos.

AGRADECIMENTOS

Agradeço primeiramente aos meus familiares, principalmente minha mãe Eleine Aparecida Martins Janine pela paciência e por todo apoio e conselhos que me deu, e exatamente todos os meus amigos que conheci fora e durante a faculdade por também terem me apoiado, me ajudado durante minha vida toda e compartilhado tantos momentos de alegria e preocupação comigo.

Agradeço também a todos os meus professores que ao decorrer destes quatro anos nos passaram todo seu conhecimento e nos ajudaram a completar essa fase da nossa vida.

E por fim, agradeço especialmente a minha banca examinadora e ao meu orientador Prof. Me. Henrique Pachioni Martins que juntos me ajudaram e me incentivaram neste trabalho, muito obrigado mesmo.

“Conhecimento dá poder, mas só o caráter grangeia respeito.”. (Bruce Lee).

TABELA DE ILUSTRAÇÕES

TABELA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CCMP	Counter Cipher Mode
DSSS	Direct Sequency Spread Spectrum
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
ISM	Industrial Scientific and Medicinal
MAC	Media Access Control
UNII	Unlicensed National Information Infrastructure
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key
WWiSE	World Wide Spectrum Efficiency

SUMÁRIO

RESUMO

A evolução e massificação da tecnologia de redes sem fio têm servido de grande ajuda para empresas e pessoas, pois fornece uma maior mobilidade e flexibilidade. Entretanto, pela sua facilidade de acesso algumas preocupações são levantadas, uma delas é a segurança das informações que circulam em sua rede que talvez seja a mais importante, sendo assim as empresas necessitam de especialistas que possam proteger seus dados e redes de invasores mal-intencionados. Levando isso em consideração, essa pesquisa tem como objetivo realizar um estudo sobre técnicas de invasão a redes sem fio, a fim de demonstrar os riscos que os usuários estão expostos nos dias atuais, exemplificando também por meio de um ataque de força bruta utilizando listas numéricas, as chamadas Wordlists, geradas por uma ferramenta disponível em um sistema operacional voltado para testes de penetração, o sistema Kali Linux. Ao final da pesquisa é apresentado o desempenho dos ataques realizados, mostrando a ineficácia de um ataque de força bruta, isto é mostrado por meio de estatísticas de tempo necessárias para se quebrar uma senha com, por exemplo, oito caracteres, ressaltando a importância da utilização de senhas mais longas e complexas em um ambiente empresarial ou doméstico. Este trabalho visou contribuir com informações relevantes e orientações sobre a área de segurança da informação voltada para redes sem fio.

Palavras-chave: Segurança. Redes sem fio. Teste de penetração. Vulnerabilidade. Força-Bruta.

ABSTRACT

The evolution and massification of wireless networking technology have been helpful to companies and people. That is because this type of technology provides a greater mobility and flexibility. However, because of its access facility, some concerns are brought up. One of them is the security of the information that passes through your network and that may be the most important one. Therefore, companies need experts who can protect your data and networking from ill-intentioned hackers. Taking this into consideration, this research purpose is to accomplish a study about hacking techniques to wireless networking with the objective to present the risks that network users are exposed to nowadays. Using as an example, a brute-force attack that utilizes numbered lists, called Wordlists, created by a tool available in an operating system, Kali Linux, directed to penetration tests. By the end of this research is presented the performance of fulfilled attacks, demonstrating the inefficiency of a brute-force attack, this is shown through statistics of time needed to break a password with, for example, eight characters, highlighting the importance of using longer and complex passwords in business or domestic environment. This study aim was to contribute with valuable knowledge and orientations about the information security field directed to wireless networking..

Keywords: Security. Wireless networking. Penetration test. Vulnerability. Brute force.

1 INTRODUÇÃO

A tecnologia de redes de computadores permite ter uma forma-padrão para compartilhar recursos físicos e lógicos (MENDES, 2007). Um produto da evolução desta tecnologia é a rede sem fio, hoje em dia com o auxílio disto, da evolução da internet, e principalmente da internet móvel, é possível possuir celulares, periféricos, carros, roupas e talvez em um futuro próximo até casas conectadas em uma rede a todo o momento, sem a necessidade de se estar fixa em um só lugar.

A primeira rede sem fio ou em inglês Wireless, que empregou a técnica de envio de pacotes utilizando ondas de rádio ao invés de utilizar cabos ponto a ponto, foi criada na década de 70 no Hawaii, sendo utilizada por uma universidade para troca de informações (MENDES, 2007). Após isso começaram a serem desenvolvidas mais redes sem fio utilizando outras tecnologias, como o infravermelho (TANENBAUM, 2003). A tecnologia Wireless ganhou notoriedade nas pequenas e grandes empresas, pela facilidade em mobilidade e organização, não sendo mais preciso vários cabos pelo chão e furo em paredes, que muitas vezes comprometiam a estrutura de suas instalações, para se conseguir uma conexão entre vários computadores.

De acordo com a Symantec et al. (2003), os usos das redes sem fio vinham se multiplicando cada vez mais á medida que a qualidade das mesmas estava melhorando e os preços dos equipamentos iriam se tornando mais acessíveis. Hoje em dia claramente que estavam corretos, a tecnologia Wi-Fi ou Wireless, que é o nome dado a tecnologia das redes sem fio, está presente quase que constantemente em nosso dia a dia, desde recentemente nossas roupas e acessórios até nossos veículos estão sendo desenvolvidos conectados de alguma forma. Reforçando isto, Kurose e Ross et al. (2006) observam que, na época, havia mais europeus que possuíam um celular do que um computador de mesa ou um carro.

Apesar da facilidade e benefícios desta tecnologia ela possui muitas vulnerabilidades, por ser transmitida via sinais de ondas de rádio e em forma de ondas eletromagnéticas, a informação é enviada para todas as direções inclusive atravessando paredes. Desta forma, uma pessoa que possui más intenções com conhecimentos e equipamentos corretos, pode facilmente interceptar essas informações e utiliza-las, podendo causar prejuízos para o alvo. Os responsáveis

pela manutenção e segurança de redes deste tipo devem tratar suas vulnerabilidades e tomar medidas, para preservar os três principais pilares da segurança da informação, a confidencialidade, a integridade e a disponibilidade (LYRA, 2008), e evitar que qualquer pessoa não autorizada possa navegar por sua rede, amenizando os prejuízos que podem vir a ocorrer com roubo ou manipulação de informações. Sendo assim, justifica-se o desenvolvimento desse trabalho o compartilhamento destas informações, a fim de contribuir com informações relevantes e orientações sobre a área de segurança da informação voltada para redes sem fio.

2 OBJETIVOS

A seguir apresentam-se os objetivos desta pesquisa.

2.1 OBJETIVO GERAL

Realizar um estudo sobre técnicas de invasão a redes sem fio, a fim de demonstrar os riscos que os usuários estão expostos nos dias atuais, exemplificando também como atacantes conseguem efetuar estes tipos de invasões, e, ao final da pesquisa, apresentar o desempenho dos ataques realizados por meio de um relatório de invasão.

2.1 OBJETIVOS ESPECÍFICOS

a) Analisar o funcionamento de redes sem fio.
b) Pesquisar sobre redes públicas abertas.
c) Investigar os riscos de vulnerabilidades em redes sem fio.
d) Estudar técnicas de invasão de redes sem fio.
e) Realizar uma invasão controlada em uma rede sem fio.
f) Analisar resultados da invasão a rede sem fio.
g) Apresentar dados sobre a resistência do sistema a invasão.

3 REDES DE COMPUTADORES

Como explica Mendes et al. (2007), uma boa definição para redes de computadores é:

> As redes de computadores estabelecem uma forma-padrão de interligar computadores para o compartilhamento de recursos físicos ou lógicos. Esses recursos podem ser definidos como unidades de CD-ROM, diretórios do disco rígido, impressoras, scanners, placa de fax modem etc. (MENDES; DOUGLAS ROCHA, 2007, p. 17).

Com a ajuda de alguns fatores, como a popularização dos computadores no ambiente empresarial e o baixo custo e valor final dos componentes para se implementar uma rede, a tecnologia foi sendo massificada, decorrente disto houveram alguns avanços nessa área. A seguir serão dissertados sobre a tecnologia de rede cabeada e rede sem fio.

3.1 REDES SEM FIO

Como apresentado por Engst e Fleishman et al. (2005) redes sem fio, ou em inglês Wireless, são redes que não utilizam cabos para se conectar, ao invés disso é empregado uma tecnologia de transmissão por ondas de rádio.

A primeira rede sem fio era chamada de “Aloha” e foi desenvolvida em 1970 por uma universidade no Hawaii utilizando receptores de rádio FM, ela era necessária para a conexão de sub-redes. Apesar do alto custo para se mantiver linhas naquela época e da baixa qualidade e não oferecendo confiabilidade na transmissão de dados, a rede foi implementada transmitindo dados a 9600bps, porém, não foi muito utilizada por conta de problemas com limite de dados e vídeo. (MENDES, 2007).

A tecnologia se desenvolveu, ocorreu uma miniaturização dos componentes e massificação das redes sem fio, porém, também houve alguns problemas de compatibilidade e interoperabilidade entre equipamentos. (MENDES, 2007). Em 1997 a Institute of Electrical and Electronic Engineers (IEEE) decidiu elaborar um padrão para a utilização dos equipamentos, este padrão foi denominado 802.11 (TANENBAUM, 2003).

3.2 PADRÃO 802.11x

Criado na década de 1990 e conhecido como Wireless Fidelity (Wi-Fi) está presente em diversos lugares como locais de trabalho, residências, instituições educacionais, aeroportos e etc., e é um dos principais padrões utilizados em redes sem fio. Neste capitulo será tratado mais profundamente sobre este padrão em especifico.

De acordo com Kurose e Ross et al. (2006), existem alguns tipos de redes baseadas neste padrão, entre eles a 802.11b tendo a taxa de dados de até 11mbps e faixa de frequência de 2.4 a 2.485 GHz, era a predominante no ano de 2004, pois estas taxas de dados já são o suficiente, também as redes 802.11a e 802.11g que possuem a maior taxa de dados dentre as mencionadas, chegando até 54mbps, e faixa de frequência de 5.1 a 5.8GHz e 2.4 a 2.485 GHz respectivamente.

Os autores também citam que as três redes possuem características em comum, como utilizar o mesmo protocolo de acesso e a mesma estrutura de enlace, capacitando o hospedeiro a se conectar em outro hospedeiro sem fio ou a uma estação-base, também todos os três tipos citados podem reduzir a taxa de transmissão alcançando distancias maiores, e permite “modo infraestrutura”, o que quer dizer que os serviços tradicionais de rede são fornecidos pela rede que estiverem conectados por meio de uma estação-base, e o “modo ad hoc”, que será detalhado mais à frente.

3.2.1 Padrão 802.11b

Foi o primeiro padrão a ser desenvolvido pelo IEEE especificamente para redes Ethernet em fio e com a finalidade de suprir necessidades de empresas em geral, como cita Mendes et al. (2007).

Este padrão utiliza a técnica Direct Sequency Spread Spectrum (DSSS) e opera em uma frequência de 2.4GHz conhecida como Industrial Scientific and Medicinal (ISM), por ter uma frequência baixa está mais suscetível a interferências, também pode operar tanto na topologia ad-hoc quanto na cliente/servidor, que é quando todo o tráfego da rede passa pelo ponto de acesso sem fio (MENDES; 2007).

3.2.2 Padrão 802.11a

O segundo padrão a ser desenvolvido pelo IEEE, é em média cinco vezes mais rápido que o padrão anterior, opera a 5.8 GHz e possui uma taxa de transmissão de 54mbps, porem, por disponibilizar até oito canais por ponto de acesso ele pode ter uma taxa maior de transmissão para mais usuários simultâneos.

Por operar em uma banda conhecida como Unlicensed National Information Infrastructure (UNII), o padrão possui uma maior imunidade a interferências eletromagnéticas, entretanto apresenta maior dificuldade em ultrapassar paredes (MENDES, 2007)

3.2.3 Padrão 802.11g

Tendo como objetivo aplicar o melhor dos dois padrões anteriores, a IEEE criou o 802.11g, que transmite a 54 Mbps e em uma frequência de 2,4 GHz.

Este padrão é totalmente compatível com o 802.11b, ou seja, é possível transmitir dados de placas do padrão 802.11g para o 802.11b, sem necessidade de se pedir autorização de uso para a Anatel (MENDES, 2007).

3.2.4 Padrão 802.11n

Razoavelmente atual, este padrão foi homologado no último trimestre de 2009, ele também é conhecido como World Wide Spectrum Efficiency (WWiSE), tem foco em aumento de velocidade, cerca de 100 a 500 Mbps, e cobertura de área. (RUFINO, 2011).

Uma característica deste padrão é que possui compatibilidade com padrões anteriores, podendo trabalhar com canais de 40 MHz e 20 MHz, porém, a velocidade oscila para 135 Mbps (RUFINO, 2011).

3.3 MODO INFRAESTRUTURA

Neste modo cada ponto de acesso é responsável por coordenar a conexão de estações moveis da área aceitando ou não a inserção de novas estações na rede,

também colhe estatísticas de gerenciamento do canal ajudando a definir quando uma estação deve ser controlada por outro ponto de acesso (MENDES, 2007).

3.4 MODO AD-HOC

Este modo não utiliza um ponto de acesso, ou Access Point em inglês, ao servidor, isso é possível, por exemplo, em um ambiente com vários computadores onde um serve como roteador compartilhando o acesso à internet e os outros se conectando diretamente a este computador, gerando uma rede de troca de dados temporária entre si, redes simples que se comunicação por múltiplas estações são formadas por ela (MENDES, 2007).

3.5 PROTOCOLOS DE SEGURANÇA

Em redes sem fio existem alguns protocolos de segurança criados para proteger o acesso a sua rede, do mais antigo para o mais novo são eles, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) e Wi-Fi Protected Access II (WPA2).

Primeiramente como explica Demartini et al. (2013) em um artigo para o site TecMundo, o protocolo WEP foi criado em 1999, sendo compatível com praticamente todos os dispositivos WiFi disponíveis no mercado. Porém, por ser um sistema de segurança de 128 bits, ou seja, possui poucos caracteres possíveis de combinações sendo possível com o processamento de computadores mais atuais, descobrir a senha de uma rede sem fio que utiliza este protocolo com alguma facilidade por meio de um software de ataque, que será abordado mais a frente.

Sendo assim, o WEP foi tirado de circulação em 2004, dando espaço ao protocolo WPA que possuía um sistema de encriptação de 256 bits, possuindo uma maior combinação de caracteres para uma senha, e uma segurança muito maior para as redes. O problema deste protocolo-padrão é que muita coisa foi reaproveitada de seu antecessor, trazendo de volta muitos problemas antigos também, incluindo um método dos hackers quebrarem o algoritmo de senha deste protocolo não com força bruta, que seria muitas tentativas de senha até finalmente encontrar a correta, e sim por meio de sistemas suplementares, herdados do protocolo WEP, que serviam para facilitar a configuração e conexão entre dispositivos antigos e modernos (DEMARTINI, 2013).

E, finalmente, em 2006 foi implementado o WPA2, devido a o Advanced Encryption Standard (AES), que seria um padrão para a segurança das informações, e o Counter Cipher Mode (CCMP), um mecanismo de encriptação, alguns especialistas dizem que o risco de invasão utilizando o protocolo WPA2 é praticamente zero.

Porém, novamente devido a programações de compatibilidade para ligação de roteadores antigos, os hackers podem se conectar a sua rede possuindo acesso normal e conseguindo assumir o controle de outros dispositivos ligados à rede, ou obter dados contidos neles (DEMARTINI, 2013).

4 SEGURANÇA DA INFORMAÇÃO

Segurança da informação pode ser considerada uma das maiores preocupações de uma empresa nos dias de hoje. Sabe-se que muitas vezes o bem mais valioso de uma grande corporação pode não ser o serviço que ela proporciona e sim as informações que contem.

Neste capitulo serão abordadas algumas características da segurança da informação, assim como vulnerabilidades e técnicas desenvolvidas para se proteger ou obter uma informação.

4.1 SEGURANÇA EM REDES SEM FIO

A popularização das redes sem fio não foram nenhuma surpresa, além dos preços mais acessíveis e desenvolvimento tecnológico, como dito pela Symantec et al. (2003), houve uma pesquisa feita pela empresa de consultoria Gartner Inc., descobriu-se que funcionários que utilizavam notebook obtiveram um aumento em produtividade de meia hora a três horas, comparando a usuários de Desktop, e quando a conexão sem fio é adicionada ocorreram aumentos de até 11 horas de produtividade durante a semana.

Entretanto a Symantec et al. (2016) também cita que, de acordo com Laura Garcia-Manrique, gerente da Group Product - Wireless da Symantec, casos como perda de dispositivos moveis contendo informações importantes, interceptação da transmissão da rede sem fio à medida que viaja, entre outras coisas, demonstram como a segurança neste tipo de rede ainda é um dos maiores problemas enfrentados por gerentes de TI.

Para Laura et al. (2016), “a definição de políticas e padrões para os dispositivos sem fio é imprescindível”, ou seja, determinar procedimentos e limitações na utilização de alguns equipamentos, também o que deve ou não ser armazenado e qual tecnologia de segurança deve ser implementada visando garantir Confiabilidade, Integridade da informação, Disponibilidade da Rede, que são as três bases da segurança da informação e serão mais bem explicados mais a frente no trabalho, porém, como observado por Caruso e Steffen et al. (1991), é impossível obter-se segurança absoluta, pois a partir de um nível os custos para se manter a segurança se tornam maiores, superando os benefícios.

Finalizando a própria autora citada anteriormente reconhece que apesar de todo o cuidado na utilização dentro da empresa, pela rede sem fio transmitir a alguma distancia, alguém mal-intencionado pode facilmente se infiltrar nas informações sendo necessário somente uma antena potente e algum software de hacker que pode ser encontrado na internet (SYMANTEC, 2016).

De acordo com Lyra et al. (2008), existem alguns principais aspectos sobre a segurança da informação, e eles são Confiabilidade, Integridade e Disponibilidade.

4.1.1 Confiabilidade

Confiabilidade é a garantia que somente as pessoas autorizadas terão acesso à rede e as informações disponibilizadas na mesma.

4.1.2 Integridade da informação

A integridade da informação não é nada mais que garantir que os dados transmitidos na rede cheguem inteiros e sem nenhuma alteração de sua origem até seu destino.

4.1.3 Disponibilidade da Rede

A disponibilidade da rede garante que a informação tem de estar disponível sempre que solicitada para todas as pessoas autorizadas que necessitarem da mesma.

4.2 VULNERABILIDADES E RISCOS

Uma das preocupações em questão de segurança em redes sem fio é a utilização do Wi-Fi Público, hoje em dia encontrados com mais facilidade, muitas vezes os usuários não se perguntam quais são os riscos de se conectar nestas redes.

As redes que contem configurações mais avançadas de segurança garantem que apenas maquinas autorizadas se conectem na rede, muitas vezes essa autenticação é feita pelo Media Access Control (MAC) da máquina, que é um código único que identifica o dispositivo, e como explicado por Jordão et al. (2013) em seu artigo, muitas redes públicas não garantem estas medidas de segurança, sendo possível qualquer máquina se conectar na mesma rede.

Isso gera outra preocupação, pois Jordão também aponta que, ao contrário das redes domésticas onde o computador é protegido por um Firewall e uma senha da rede que impedem que o intruso tenha facilidade no acesso e manipulação de seus dados, nas redes públicas você é somente mais uma máquina e seu computador está vulnerável para que uma pessoa má intencionada explore alguma vulnerabilidade e acesse seus dados.

Entretanto mesmo com os riscos o usuário ainda pode acessar e utilizar redes públicas, utilizando as boas práticas como manter sempre programas de segurança instalados e atualizados, manter Firewall ativo e não acessar contas de bancos ou redes sociais que possam conter informações importantes, e sempre tomando cuidados com redes falsas, que simulam as redes de estabelecimentos próximos para roubo de informações, finalizando, tendo um cuidado redobrado em redes públicas é possível utiliza-las para fins básicos.

4.3 TÉCNICAS DE SEGURANÇA

Na área de segurança da informação a linha que divide quem defende a rede ou sistema e quem pretende ataca-lo é de certa tênue, ambas os objetivos muitas vezes utilizam as mesmas ferramentas e técnicas, e isso leva a o estudante de segurança da informação a ter de aprender utilizar softwares, técnicas e métodos muitas vezes hackers.

4.3.1 Ataques de Força-Bruta

De acordo com Scambray et al. (2001) um ataque que era muito utilizado para ganhar acesso a sistemas é o de força-bruta, que consiste em obter senhas de acesso testando vários valores possíveis, este método procura atacar principalmente serviços de File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), telnet entre outros.

Entretanto este é um método bem lento, dependendo da complexidade da senha, todo o processo pode levar inúmeras horas, por exemplo, como apontado por Brostoff et al. (2004), caso tente-se decifrar uma senha de oito caracteres com ao menos uma letra maiúscula, uma minúscula e um número, o processo levaria em torno de 6354 horas, tornando a utilização deste método inviável dependendo do caso.

4.3.2 Criptografia

A criptografia em si é talvez tão antiga quanto Júlio César, de acordo com Kurose e Ross et al. (2006), porém, as técnicas utilizadas hoje em dia são mais baseadas em progressos dos últimos anos.

Criptografia é a técnica ou método de se escrever utilizando códigos uma mensagem, onde somente pessoas autorizadas a receber tal informação saberão como acessa-la. Posto isto, sabe-se que estas técnicas surgiram da necessidade de se enviar informações sigilosas por meios de comunicação não confiáveis (ALMEIDA; MENDES, 2007).

É uma forma de proteção da informação, pois caso um atacante consiga obter dados que não devem ser acessados facilmente, a criptografia deixara a informações fora de uma ordem lógica e entendível, onde somente quem possui a chave da criptografia conseguirá decifrá-la (ENGST; FLEISHMAN, 2005).

4.3.2.1 Criptografia de chave simétrica

Conhecida como cifra de César, é uma cifra muito simples que consiste em substituir cada letra do alfabeto pela sua k-ézima, ou seja, se k = 3 a letra A se transforma na letra D no texto cifrado (KUROSE; ROSS, 2006).

Existe a cifra monoalfabética, que é basicamente uma versão aprimorada da cifra de Cezar, ela também substitui letras pelas outras, e ao contrário da cifra citada anteriormente esta cifra não se prende ao número do K, qualquer letra pode ser substituída por qualquer outra, desde que só exista uma única letra para cada substituição (KUROSE; ROSS, 2006).

4.3.2.1 Criptografia de chave pública

O conceito da utilização de uma criptografia de chave pública é bem simples, sem se aprofundar, cada usuário possui duas chaves, uma publica a disposição de todos e uma secreta que somente pessoas autorizadas possuem, e para ser feita a comunicação primeiramente quem quer enviar a mensagem precisa conseguir a chave pública do destinatário, após isso se deve aplicar a chave pública de destino juntamente com algum algoritmo de criptografia, então finalmente quem recebeu a mensagem utiliza sua chave secreta para descriptografar a mensagem recebida (KUROSE; ROSS, 2006).

Porém esta criptografia possui algumas preocupações, como alguém se passar pelo remetente ou, mesmo que o intruso que interceptar a mensagem não conseguir decifrá-la, ele irá possuir a chave pública do destino e o padrão de criptografia utilizado por quem enviou a mensagem, com isso o atacante pode tentar criptografar as mensagens mais provável de serem enviados, utilizando os mesmos métodos e talvez chegando perto da mensagem real (KUROSE; ROSS, 2006).

4.4 SISTEMAS DE SEGURANÇA

Como falado anteriormente estudantes e profissionais da área de segurança da informação tem de aprender e utilizar muitas vezes as mesmas técnicas e ferramentas utilizadas por hackers mal-intencionados, visando isso foram criados vários sistemas de operacionais com foco em penetração e testes de segurança.

Sendo em sua maioria baseados em GNU/Linux, contém inúmeras ferramentas de apoio e são facilmente encontrados na internet gratuitamente.

Nesta sessão serão apresentadas algumas destas distribuições.

4.4.1 Parrot Security OS

A Parrot Security OS é uma distribuição GNU/Linux baseada no Debian, é um sistema operacional voltado para penetração e teste de segurança, e possui compiladores e interpretadores para diversas linguagens de programação, como PHP, Ruby, Perl e Python, entre outros.

4.4.2 Cyborg Hawk

É uma distribuição baseado em Ubuntu 14.04 LTS, assim como o apresentado anteriormente, possui diversas ferramentas voltadas para a área de segurança da informação, porem o atrativo é o baixo consumo de memória do sistema.

4.4.3 Kali Linux

Também sendo uma distribuição GNU/Linux baseada no Debian, é considerada um sucessor do Backtrack, que é outro sistema operacional voltado para penetração em redes e testes de segurança, porém, já foi descontinuado.

Assim como seu antecessor, ele possui mais de 300 ferramentas diferentes que facilitam muito a invasão em redes com nível baixo de segurança.

Este e o sistema operacional escolhido para a realização deste trabalho, pois possui as ferramentas necessárias, e por ser mais popular possui mais material e suporte em fóruns. Além do Kali Linux, também será utilizado três ferramentas. Elas são Airodump-ng, Aireplay-ng e Aircrack-ng, elas na verdade fazem parte de um pacote de aplicativos para verificação de redes sem fio.

4.4.3.1 Ferramenta Airodump-ng

Uma das ferramentas que já vem por padrão no sistema operacional Kali Linux, ela é um sniffer de rede, ou seja, é responsável pela captura e monitoramento de pacotes criptografados de uma rede (TEWS; BECK, 2009). Após a captura de pacotes o Airodump-ng gera um arquivo com extensão CAP que mais tarde é lido pelo Aircrack-ng, que é outra ferramenta do mesmo pacote.

4.4.3.2 Ferramenta Aireplay-ng

Também sendo uma ferramenta padrão do Kali Linux, após a utilização da ferramenta citada anteriormente, geralmente utiliza-se a Aireplay-ng (TEWS; BECK, 2009), pois sua principal função é causar desautenticações a fim de capturar dados de handshake da rede, causar autenticações falsas, repetição de pacote interativo, injeção de ARP Request forjados e reinjeção de ARP Request.

4.4.3.3 Ferramenta Aircrack-ng

E, finalmente a ferramenta Aircrack-ng serve para uma análise de criptografia, e também é ele o responsável por realizar ataques a protocolos WEP/WEP2 e WPA (TEWS; BECK, 2009). O Aircrack-ng pode recuperar a chave WEP da rede sem fio utilizando os dados anteriormente capturados pelo Airodump-ng.

5 TRABALHOS CORRELATOS

A segurança da informação possui muitas pesquisas e informações, que são disponibilizadas e compartilhadas constantemente por membros e pesquisadores da área, ou seja, frequentemente diversas ferramentas, técnicas e programas são desenvolvidos visando facilitar os profissionais a protegerem suas informações. Entretanto, diversas ameaças surgem muitas vezes tão rápido quanto os pesquisadores desenvolvem medidas de proteção, o que pode acabar prejudicando muitas pessoas. Isso demonstra o quão importante e ativa esta área acaba se tornando, e o quanto seria bom termos mais profissionais interessados neste tipo de pesquisa.

A metodologia deste trabalho foi conduzida de acordo com outras pesquisas feitas anteriormente, utilizando programas e seguindo técnicas já elaboradas por outros profissionais.

De acordo com algumas pesquisas, a maioria dos ataques é feito de modo mal-intencionado, e uma parte das vulnerabilidades é devido à má gestão e configuração dos equipamentos de segurança, e principalmente o mau uso da rede por usuários não cientes das políticas de segurança.

Um dos trabalhos analisado foi o intitulado: “Análise das Vulnerabilidades de Segurança Existentes nas Redes Locais Sem Fio: Um Estudo de Caso do Projeto WLACA”, de autoria de Lidiane Parente Andrade, Daniel Nelo Soares, Mauro Margalho Coutinho e Antônio Gomes Abelém, que aborda a segurança em redes sem fio que utilizam o padrão 802.11x, que estava sendo muito adotado por empresas e instituições. Este trabalho foi feito com o intuito de se transmitir informações corretas e especificas para pesquisadores e profissionais.

Para reforçar, também foi analisado o trabalho intitulado: "Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x", de autoria de Luiz Otávio Duarte, que assim como o trabalho citado anteriormente, visa agregar um maior conhecimento a pesquisadores, analistas e técnicos interessados em colaborar com este tipo de pesquisa.

Sendo assim, a intenção deste trabalho foi contribuir com informações relevantes e conclusões, também a fim de orientar mais pesquisadores, técnicos, analistas e usuários sobre os riscos e vulnerabilidades que pode-se estar expostos

em redes sem fio e quais métodos são aconselháveis para proteção dos mesmos, e talvez mantendo ativo o interesse nesta linha de pesquisa tão interessante.

6 METODOLOGIA

O presente trabalho foi desenvolvido em duas etapas distintas e visou demonstrar os riscos que estão expostos os usuários de redes sem fio nos dias atuais.

Foi elaborado primeiramente um material de referencial teórico baseado em livros, artigos, matérias online e etc., que contextualizará a origem das redes e padrões utilizados em redes sem fio, conjuntamente alertará sobre os riscos de se conectar em redes públicas, foi apresentado uma breve descrição de técnicas de segurança, sistemas operacionais voltados para invasão de redes e os pilares que são baseados a segurança da informação.

Em seguida, na segunda etapa, foi realizado o desenvolvimento prático, onde foram utilizadas as ferramentas Airodump-ng, Aireplay-ng e Aircrack-ng, que de acordo com alguns sites especializados em Linux e segurança da informação, são ferramentas indicadas para se manipular redes com protocolos WEP e WPA. Elas inclusive já vêm disponíveis no sistema operacional Kali Linux voltado para penetração de redes e testes de segurança.

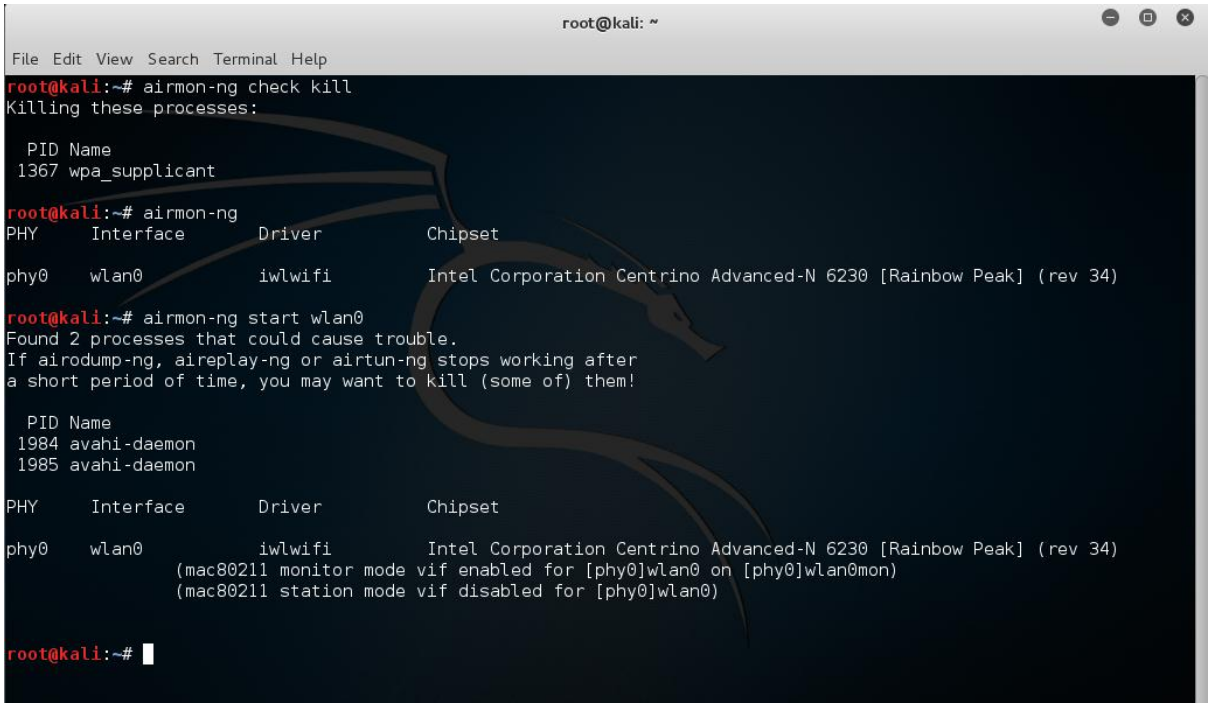
Foi definido o alvo da invasão, uma rede sem fio que utiliza um roteador Thomsom com encriptação WPA-PSK, e o método empregado foi o de força bruta utilizando um sistema operacional voltado para invasões e testes de segurança, chamado Kali Linux.

Para a pesquisa foi utilizado um Notebook Intel Core i3 com 4GB de RAM, pois é o recurso próprio do pesquisador. O sistema operacional Kali Linux foi escolhido por ser um dos mais mencionados nas pesquisas realizadas, e por possuir uma maior quantidade de material e suporte online e de fácil acesso. Quanto ao método de invasão foi utilizado a força bruta, onde o atacante tenta várias combinações de caracteres aleatórios em grande velocidade buscando a combinação exata.

Ao iniciar os testes, primeiramente foi utilizada a ferramenta Airmon-ng, onde foi colocada a placa de rede do computador em modo monitor, para que fosse possível capturar pacotes na rede wireless usando o comando “airmon-ng start <interface da rede>”, porém, antes foi necessário utilizar o comando “airmon-ng check kill”, para finalizar qualquer processo que pudesse causar algum problema no

procedimento. Como apresenta a Figura 1, os comandos mencionados estão sendo utilizados.

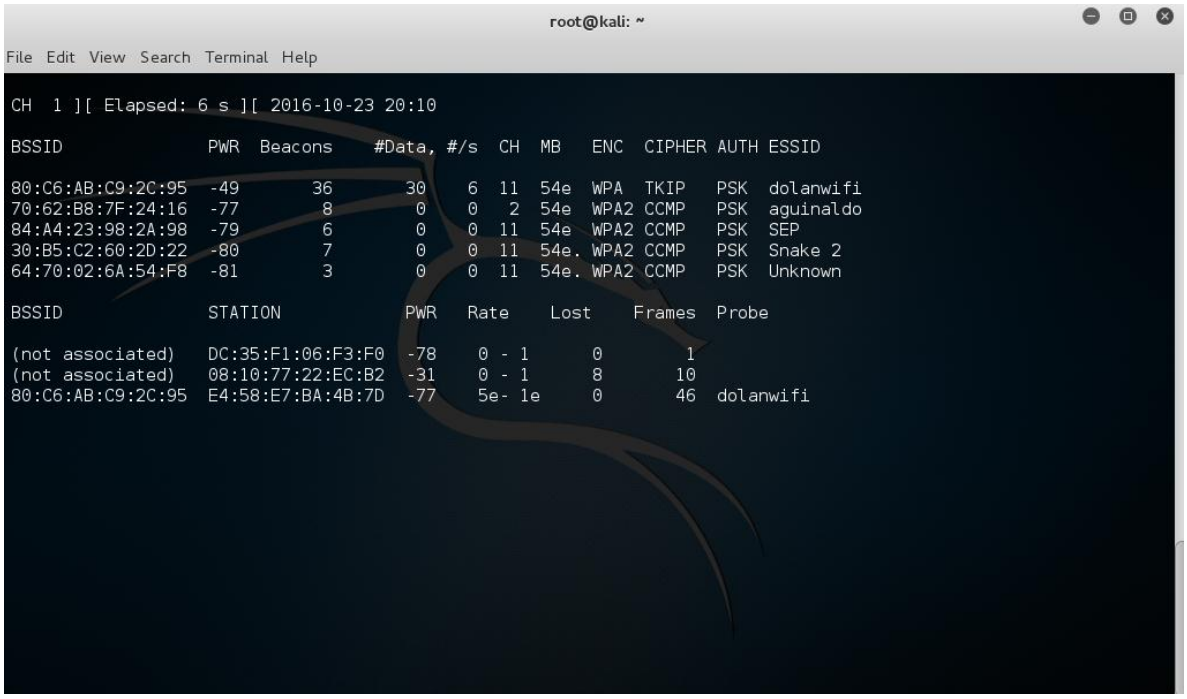
Figura 1 - Utilização do Airmon-ng para ativação do modo monitor na rede.



Fonte: Elaborada pelo autor.

Em seguida com auxílio da ferramenta Airodump-ng, foi possível monitorar e capturar pacotes WEP de redes sem fio próximas. Estes pacotes são utilizados mais tarde pela ferramenta Aircrack-ng. Como ilustrado na Figura 2, primeiramente foi utilizado o comando “airodump-ng wlan0mon” que retorna as redes wireless próximas com alguns dados.

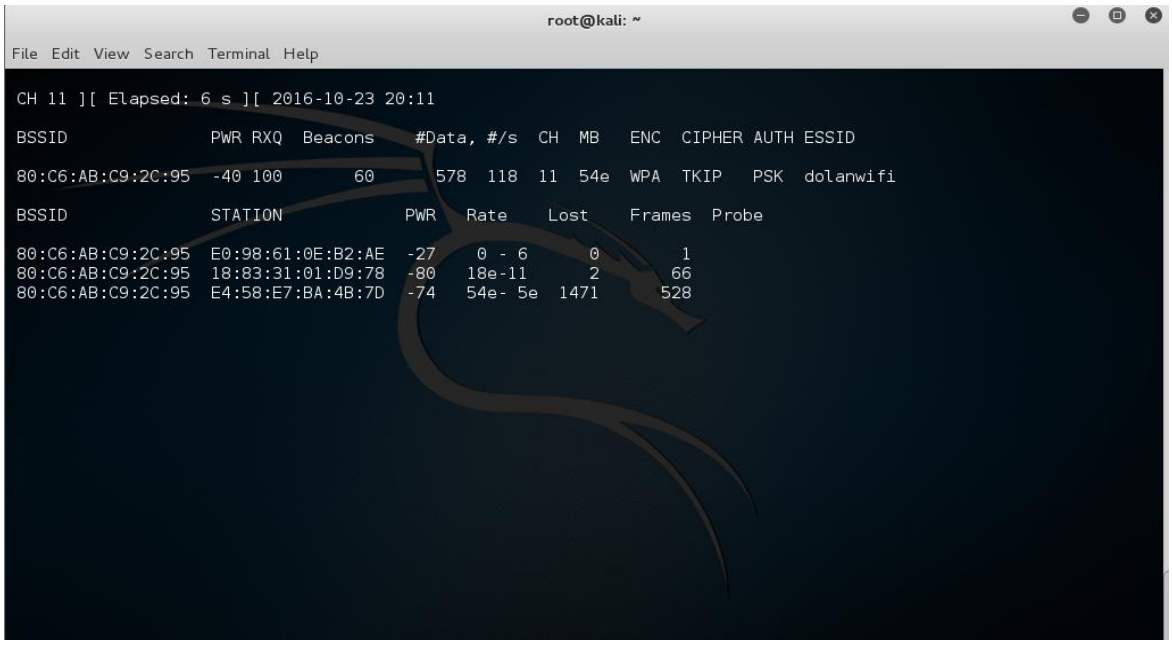
Figura 2 – Redes próximas sendo monitoradas.



Fonte: Elaborada pelo autor.

O próximo comando executado foi o comando “airodump-ng –c <canal da rede> -w <nome da rede> --bssid <BSSID da rede> wlan0mon” onde ele captura diretamente os pacotes da rede especificada, no caso a rede “dolanwifi”, como ilustrado na Figura 3.

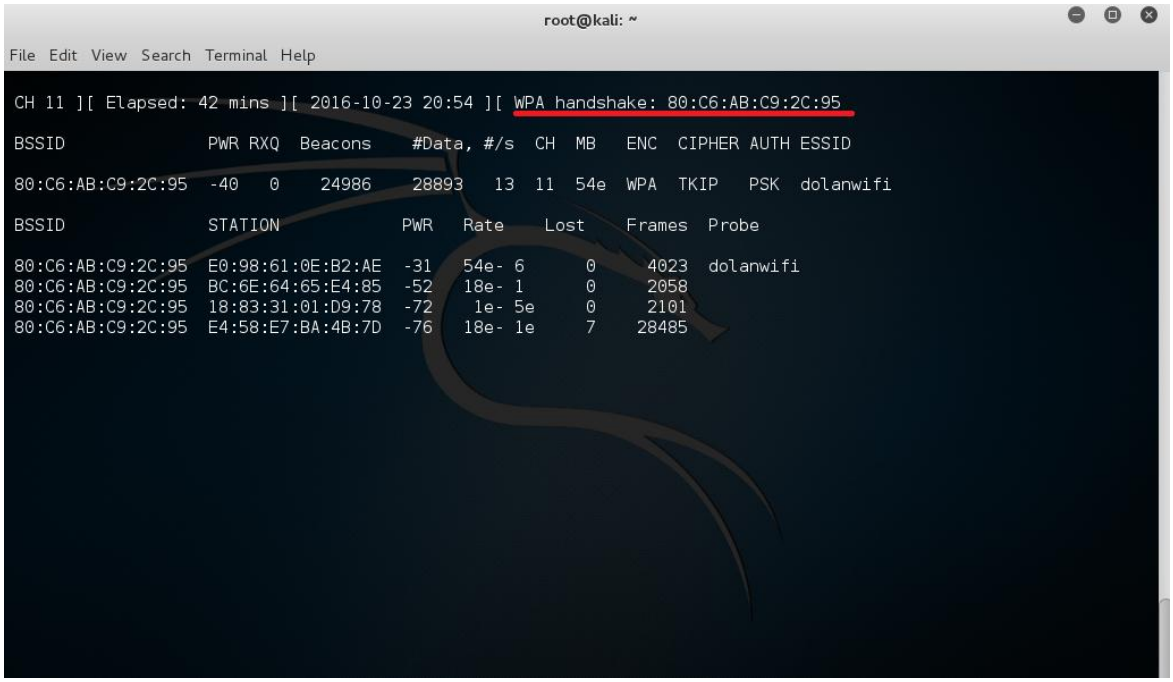
Figura 3 – Redes alvo sendo monitorada para o ataque.



Fonte: Elaborada pelo autor.

Então foi aplicada a ferramenta Aireplay-ng, esta é uma ferramenta de invasão e sua principal função é capturar dados e causar uma Desautenticação, ou seja, este tipo de ataque faz com que o usuário conectado no ponto de acesso “desautentique” e volte a se conectar com a rede, neste momento uma nova requisição Address Resolution Protocol (ARP) é feita e o atacante consegue obter o novo handshake do alvo, como ilustrado na Figura 4.

Figura 4 – Obtenção do novo handshake da rede.

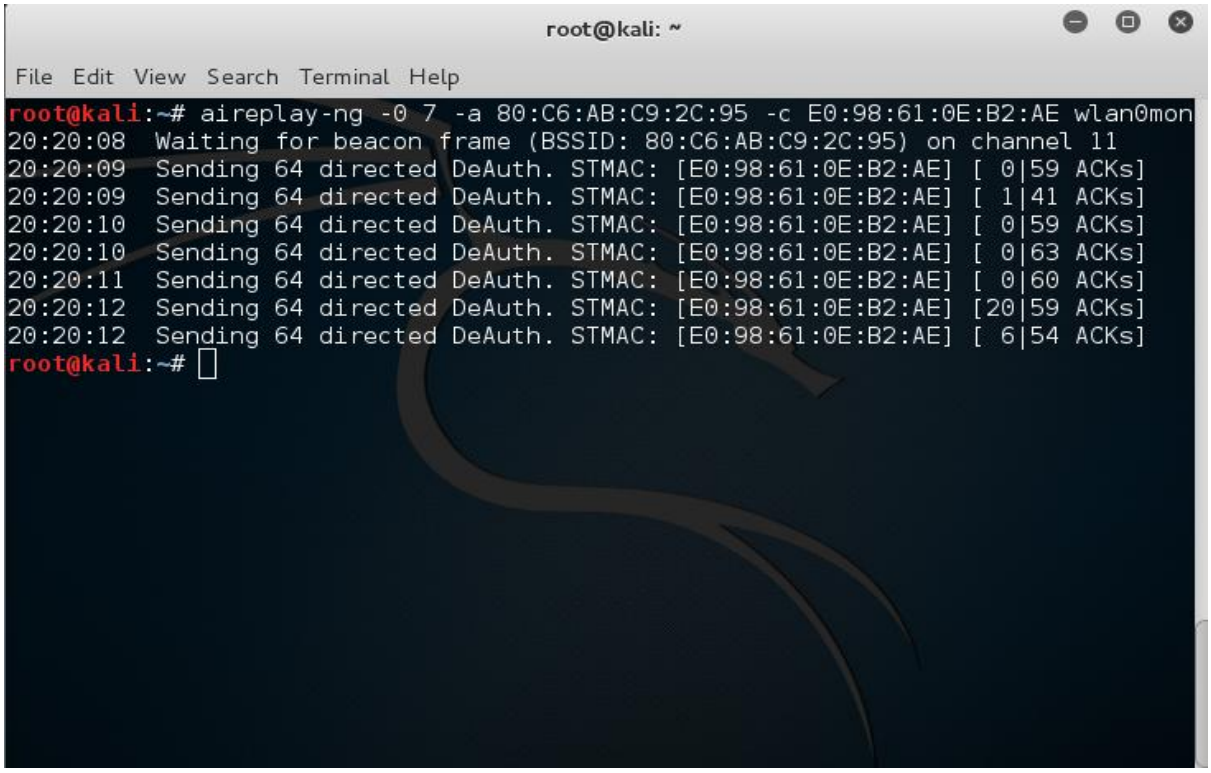


Fonte: Elaborada pelo autor.

Esta requisição ARP é um protocolo de rede que basicamente tenta descobrir o endereço MAC do outro equipamento para se comunicar.

Para o ataque usou-se o comando “aireplay-ng -0 7 -a <BSSID da rede> -c <estação da rede> wlan0mon”, as opções “-a” e “-c” configuram o endereço MAC do ponto de acesso e o destino do endereço MAC para o ataque, como ilustrado na Figura 5.

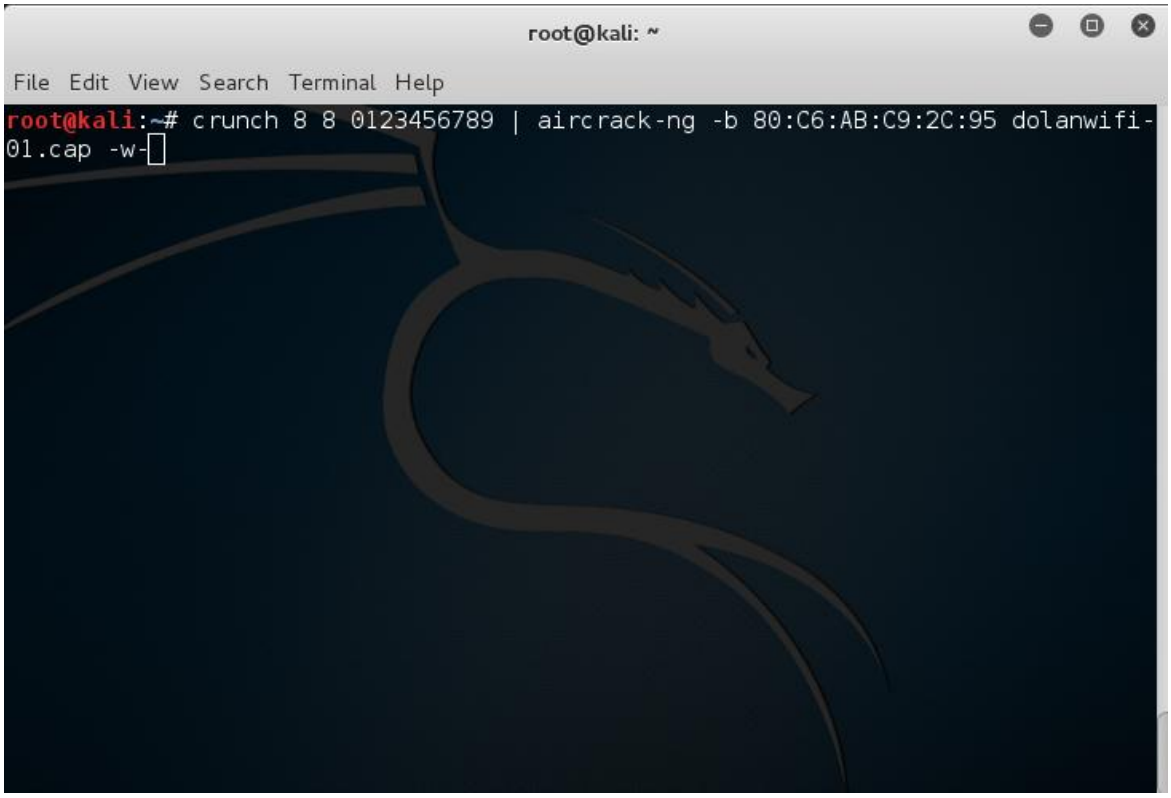
Figura 5 – Procedimento do ataque de desautenticação.



Fonte: Elaborada pelo autor.

Por fim, foram utilizadas duas ferramentas, a Aircrack-ng que é um programa utilizado para quebrar chaves WEP e WPA/WPA2-PSK utilizando pacotes criptografados capturados pelo Airodump-ng, e a Crunch que serve para criar wordlists e já vem nativa no sistema operacional Kali Linux. Utilizando o comando “crunch <mínimo de caracteres> <máximo de caracteres> <variação dos caracteres> | aircrack-ng –b <handshake da rede> <Arquivo *.cap> -w-“, já é iniciado o ataque de força bruta na rede, usando como base uma wordlists, ou seja, um dicionário de caracteres que a ferramenta Crunch criou no momento e o arquivo .cap criado pela ferramenta Airodump-ng, como ilustrado na Figura 6.

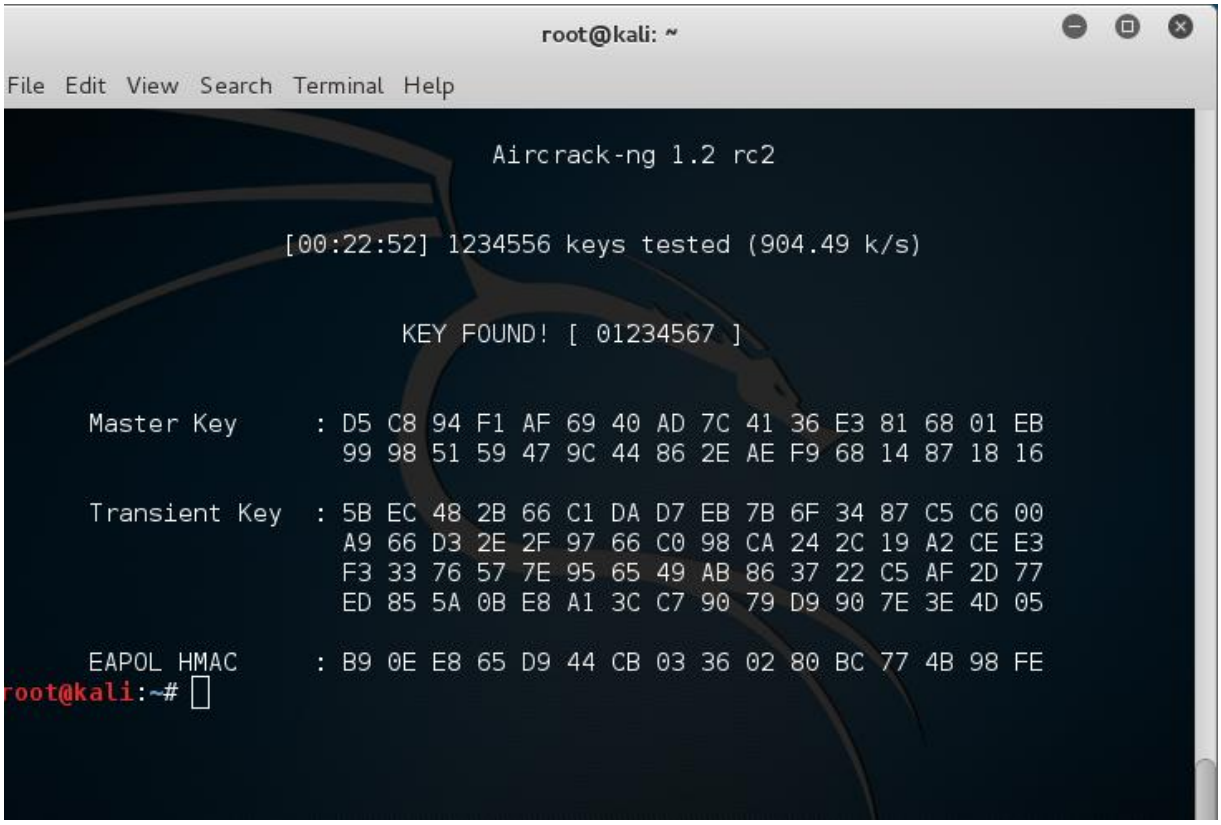
Figura 6 – Sintaxe do comando Aircrack-ng juntamente com a ferramenta crunch.



Fonte: Elaborada pelo autor.

Após o tempo de 22min52seg o programa conseguiu encontrar a combinação correta de caracteres da chave de segurança da rede alvo, no caso a senha encontrada foi o valor no campo KEY FOUND [012345567], como ilustrado na Figura 7.

Figura 7 – Chave encontrada em um ataque bem sucedido.



Fonte: Elaborada pelo autor.

Uma vez tendo acesso direto a rede do alvo é possível interceptar ou transferir dados trafegando pela rede, podendo desta forma manipular ou capturar dados de uma possível vitima.

7 RESULTADOS

Como apresentado no capítulo da metodologia, foram feitos alguns testes utilizando força bruta para quebra de senhas em redes sem fio, com o intuito de comparar a eficácia e a dificuldade de se utilizar um ataque deste tipo. Foram realizados três testes com senhas diferentes, e o resultado está sendo apresentado na Figura 8.

A Figura 8 apresenta uma tabela dividida pela quantidade de caracteres que há nas senhas e qual a combinação de caracteres utilizada na mesma, qual o tempo decorrido para a quebra da senha e a velocidade média que foram testadas as chaves com o método de força bruta.

Figura 8 – Testes de ataques realizados com combinações diferentes de senhas.

Quantidade de Caracteres	Senha utilizada	Tempo para quebra	Velocidade testada de chaves por segundo (k/s)
8 caracteres	01234567	00h22min52seg	904.49 k/s
	35528299	10h01min22seg	993.27 k/s
	22331100	06h31min37seg	961.89 k/s

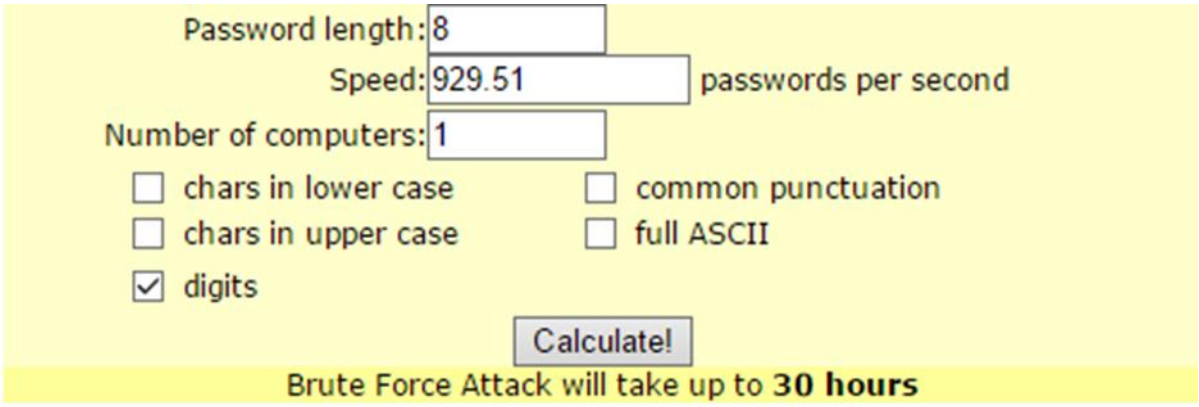
Fonte: Elaborada pelo autor.

A ferramenta Crunch wordlist não gera listas aleatórias e sim de forma uniforme da esquerda para direita, isto agrega no tempo de execução do ataque, pois os testes são feitos com todas as combinações dos caracteres começando pela esquerda e a senha só é descoberta quando o último caractere da direita estiver correto. As velocidades dos testes dependem do processador e de toda a estrutura do computador atacante, no caso a velocidade dos testes é executada por cada núcleo do processador da máquina, necessitando um hardware especifico e de grande poder de processamento para viabilizar um pouco mais este tipo de ataque.

Baseando-se nos dados apresentados na Figura 8, fica evidente a inviabilidade do uso do ataque de força bruta utilizando dicionários e desautenticação, mesmo sendo uma das formas mais simples de se implementar um ataque, sendo possível encontrar facilmente muitas informações na internet como ,por exemplo, em vídeos no Youtube ou Fóruns online, o tempo e processamento

não compensam, levando em conta ainda que a dificuldade e tempo se agravam conforme a quantidade de caracteres que a senha possui e a quantidades de caracteres que a mesma pode utilizar.

Figura 9 – Estimativa de tempo com dígitos.

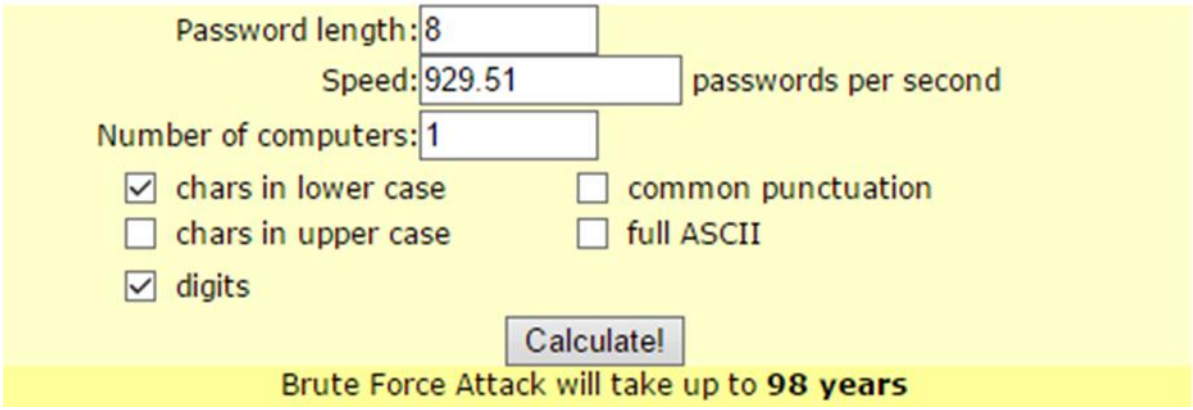


Fonte: Elaborada pelo autor.

Na Figura 9 foi utilizado o site da Last Bit (2015) que calcula a estimativa de tempo para se quebrar senhas com força bruta utilizando algumas características, como o tamanho da senha ou Password lenght, a velocidade dos testes por segundo ou Speed, o número de computadores processando o ataque, no campo Number of computers e as características da senha, ou seja, se só são utilizados dígitos numéricos, caracteres em minúsculos ou maiúsculos e etc. O calculo da estimativa é possível utilizando as variáveis de quantidade de caracteres que podem estar presentes na senha, dez dígitos do zero ao nove, por exemplo, elevado a quantidade de caracteres que a senha possui, e logo após dividindo pela velocidade de testes, com isso chegasse ao tempo para a quebra.

A Figura 9 ajuda ainda a exemplificar a dificuldade de se quebrar uma senha mostrando que um computador levaria aproximadamente 30 horas para quebrar uma senha com 8 caracteres utilizando somente números em uma velocidade constante de 929.51 chaves por segundo, enquanto que se pudéssemos utilizar números e letras em minúsculo levaríamos aproximadamente 98 anos utilizando as mesmas configurações, como mostrado na Figura 10.

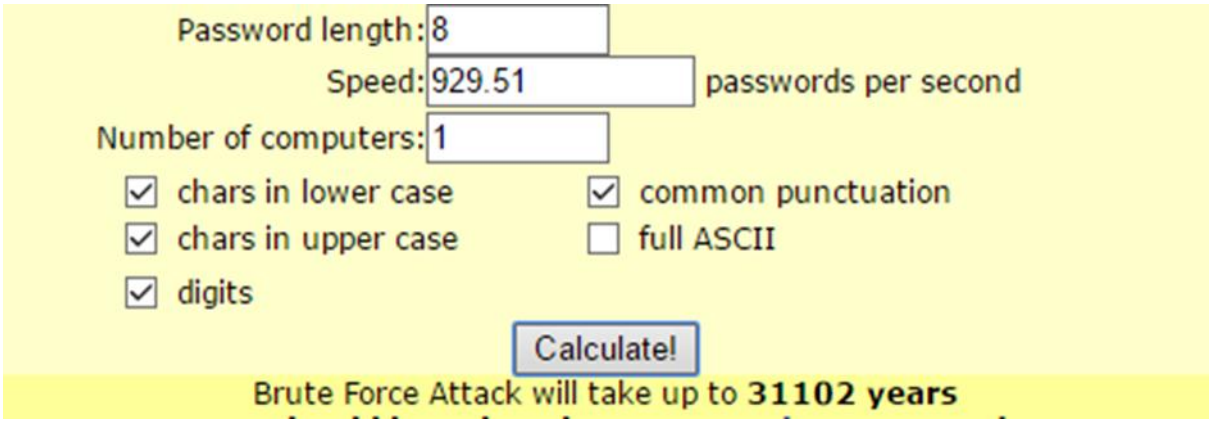
Figura 10 – Estimativa de utilizando dígitos e letras minúsculas.



Fonte: Elaborada pelo autor.

E ainda, utilizando caracteres maiúsculos, minúsculos, números e pontuações, a quantidade de anos sobe para surpreendentes 31102 anos, como mostrado na Figura 11.

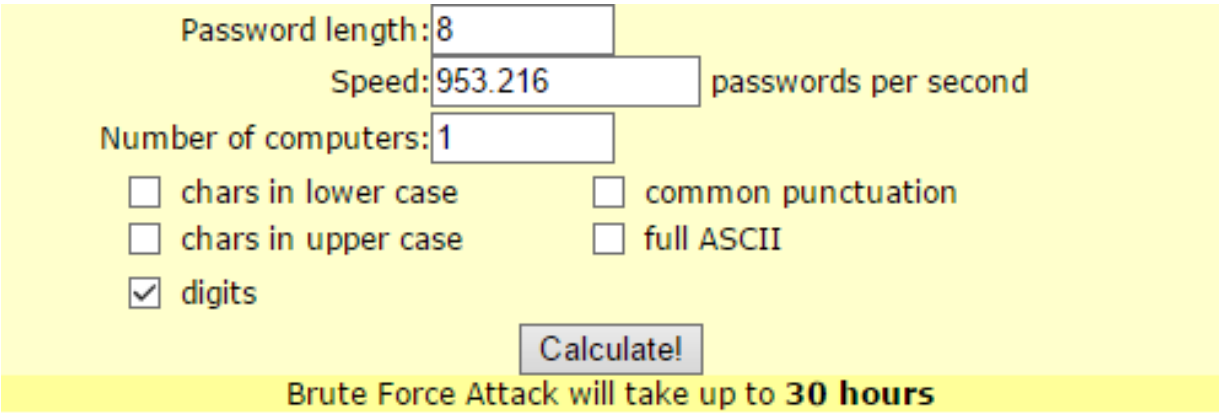
Figura 11 – Estimativa de tempo utilizando dígitos, letras minúsculas.



Fonte: Elaborada pelo autor.

Utilizando os dados disponibilizados na Figura 8 neste mesmo site, pode-se observar que uma senha com 8 caracteres usando somente dígitos numéricos poderia demorar aproximadamente 30 horas dependendo da combinação de caracteres, para se conseguir quebrar uma senha na velocidade de 953.216 chaves por segundo, que é a média em que foram feitos os testes, como apontado na Figura 12.

Figura 12 – Estimativa de tempo utilizando velocidade média dos testes feitos anteriormente.



Fonte: Elaborada pelo autor.

Utilizando estes exemplos fica evidente que invadir uma rede sem fio por este método de força bruta é inviável, e também fica clara a importância de uma rede devidamente protegida utilizando senhas bem pensadas e seguindo boas práticas de segurança em relação a este assunto, além de evitar se conectar em redes de acesso público, pois como apontado por Thiago Hyppolito que é engenheiro de produtos da McAfee no Brasil, na matéria de Guilherme et al (2015), pessoas mal intencionadas costumam se aproveitar de falhas de segurança afim de monitorar atividades de vítimas online, interceptando dados de transações em redes bancarias ou logins em redes sociais.

8 CONCLUSÃO

Ao decorrer de toda a pesquisa para se desenvolver este trabalho, foram expostas várias informações sobre as redes sem fio, desde sua origem até padrões utilizados anterior e atualmente, também foram apresentados conceitos de segurança da informação e perigos envolvendo vulnerabilidades em redes sem fio, principalmente ao utilizar redes públicas, e ao final foi visto o passo a passo de um simples teste de penetração controlado, com isto acredito que foi possível observar a importância que deve ser tratado este tema.

Tendo sido executado um tipo de ataque simples, foi possível demonstrar a eficiência de alguns meios de proteção que possuímos nos dias de hoje, também a necessidade de se utilizar senhas mais complexas seguindo algumas boas práticas e como dito no objetivo geral, foi exemplificado como atacantes conseguem efetuar tais ataques. Apesar de apontada nos resultados da invasão do trabalho a ineficácia de um ataque de força bruta em redes que utilizam uma melhor criptografia com senhas um pouco mais complexas possuindo uma maior resistência, são criados muitos outros tipos de ataques diariamente que podem facilmente serem implementados por pessoas mal intencionadas, além de é claro existirem muitas outras vulnerabilidades que podem ser exploradas, portanto faz-se necessário a contínua atenção e exploração do tema segurança da informação, tanto em um ambiente empresarial quanto doméstico, evitando-se graves problemas no futuro.

A área de segurança da informação é ainda pouco explorada pelas pessoas e muitas vezes pouco incentivada pelo trabalho e atenção necessária para sua aplicação, muitas pessoas não tem ideia do risco que suas informações correm diariamente utilizando redes públicas, senhas fracas ou simplesmente deixando a própria rede sem proteção para qualquer tipo de pessoa. Acredito que os objetivos propostos do trabalho, de informar futuros pesquisadores da área e servir como orientação sobre riscos que usuários estão expostos foram concluídos, portanto para trabalhos futuros pode-se mostrar a aplicação e eficiência de outros tipos de ataques em redes sem fio, assim como, demonstrar efetivamente ataque dentro da rede para obtenção de dados, como senhas, arquivos, conversas e etc., conseguindo demonstrar ainda mais a relevância da segurança em uma rede sem fio, doméstica ou empresarial.

REFERÊNCIAS

ALMEIDA, J. do R. C. de; MENDES, M. D. N. C. **Criptografia em sistemas distribuídos**. Pará: IESAM, 2007.

BROSTOFF, S. **Improving password system effectiveness**. University College London, 2004.

CARUSO, C. A. A.; STEFFEN, F. D**. Segurança em informática**. Rio de Janeiro: LTC - Livros Técnicos e Científicos, 1991.

DEMARTINI, F. WEP, WPA, WPA2: o que as siglas significam para o seu Wifi?. **Tecmundo**. 2016. Disponível em: <http://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm>. Acesso em: 9 Mai 2016.

ENGST, A.; FLEISHMAN, G**. Kit do Iniciante em Redes Sem Fio:** O guia prático sobre redes Wi-Fi para Windows e Macintosh. 2. Ed. rev. São Paulo: Pearson Makron Books, 2005.

JORDÃO, F. Quais os riscos de usar um Wifi público?. **Tecmundo**. 2016. Disponível em: <http://www.tecmundo.com.br/wi-fi/39348-quais-os-riscos-de-usar-um-wifi-publico-.htm>. Acesso em: 8 Maio 2016.

KUROSE, J. F.; ROSS, K. W**. Redes de computadores e a internet**: uma abordagem top-down. 3. Ed. rev. São Paulo: Pearson Addison, 2006.

LastBit Software. **LastBit Corp.**, 1997. Disponível em: <http://lastbit.com/pswcalc.asp>. Acesso em: 8 Nov 2016.

LYRA, M. R**. Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

MENDES, D. R**. Redes de computadores**: teoria e pratica. São Paulo: Novatec, 2007.

Parrot Security OS. **parrotsec.org**, c2011-2016. Disponível em: <https://www.parrotsec.org/features.fx>. Acesso em: 8 Maio 2016.

SCAMBRAY, J.; MCCLURE, S.; KURTZ, G. **Hackers Expostos**: Segredos e soluções para a segurança de redes. São Paulo: Makron Books, 2001.

SCHMIDT, T. Assegurando a Empresa Móvel em Tempo Real. **Symantec**. C1995-2016. Disponível em: <http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html>. Acesso em: 16 Abr 2016.

SIMIONI, D. Cyborg Hawk Linux, a distribuição de PenTest avançado que você procurava. **Diolinux.** c2012-2016. Disponível em: <http://www.diolinux.com.br/2015/07/cyborg-hawk-linux-pentest-distro.html>. Acesso em: 8 Mai 2016.

TAGIAROLI, G. Usar rede Wi-Fi aberta oferece riscos aos usuários; veja como se proteger. **Uol Noticias**. c1996-2016. Disponível em: <http://tecnologia.uol.com.br/noticias/redacao/2015/01/29/usar-wi-fi-aberto-oferece-riscos-aos-usuarios-veja-como-se-proteger.htm>. Acesso em: 2 Nov, 2016.

TANENBAUM, A. S. **Redes de computadores**. 4. Ed. rev. Rio de Janeiro: Campus, 2003.

TEWS, E.; BECK, M. **Practical attacks against WEP and WPA**. Alemanha, 2008.