ESTUDO DE CASO: VULNERABILIDADES EM REDE WIRELESS

GRACIEINY A. BARBOSA, HELDER A. MEDEIROS, IGOR XAVIER, LEANARDO D. C. SOUZA, ELIANE CRISTINA AMARAL, ELINEY SABINO, NARUMI ABE, SAMUEL DE OLIVEIRA

RESUMO

O objetivo deste artigo é mostrar possíveis falhas e vulnerabilidades de segurança wireless, analisando ataques e mecanismos de segurança utilizados para a proteção dos mesmos, buscar as falhas e formas de corrigi-las. Sabemos hoje em dia que o problema é não ter o conhecimento exato do que podemos fazer para realizar uma segurança limpa, a ausência de infraestrutura também dificulta a criação de mecanismos de defesas simples e eficientes. Verificar e entender como é possível implementar soluções de segurança em redes para reduzir drasticamente as vulnerabilidades das informações seria uma forma de minimizar esse problema. Pode se dizer que: A tecnologia avança em uma velocidade tão surpreendente, mas não acontece o mesmo com a segurança dela, criar uma tecnologia avançada é mais importante do que saber como mantê-la segura. Isso até que surjam as consequências. Não é por falta de tentativa, pois técnicos do mundo todo sempre estão tentando evoluir conforme as tecnologias e criam demasiados tipos de hipóteses que possam gerar proteções, mas nem sempre sai do papel. Em uma época onde a tecnologia está em todos os lugares 24h do nosso dia, temos que nos sentir como se vivêssemos em segurança, ao menos, era essa a sensação de que a tecnologia deveria nos trazer. Cada vez mais as empresas estão utilizando esta tecnologia por sua praticidade, wireless estão presentes em quase todos os lugares nos dias de hoje, em shoppings, aeroportos, lojas, escritórios, etc..... Por conta do tráfego de dados na rede, empresas podem ficar vulneráveis a ataques mal-intencionados de pessoas que querem informações privilegiadas, colocando em risco informações que são de estrema importância para o bom funcionamento dela. Portanto, diante da relevância do tema, as redes sem fio devem ser seguras e confiáveis aos usuários. Por este motivo este artigo foi elaborado com o intuito de contribuir para melhorias na segurança da rede sem fio, apresentando aos empresários e usuários, medidas de segurança que devem ser tomadas para os que possuem este tipo de rede e a forma mais segura de se usá-la.

Palavras chaves: Wireless, Wifi, Vulnerabilidade, Rede, Internet.

ABSTRACT

The main point of this article is to show possible flaws and vulnerabilities of wireless safety, analyzing attacks and secure methods used for its protection, searching flaws and ways of correcting them.Nowadays it is known that the issue is not having exact knowledge of what it can be done in order to perform a safe clean. The absence of infrastructure also raise difficulties in the development of simple and efficient defense mechanisms. Verifying and understanding how it is possible to implement safety solutions in networks to drastically reduce the vulnerability of information, would be a way to minimize this issue.It is not due the lack of attempts, since technicians all over the world are always trying to keep ut with the technologies' progress, creating several types of hypotesis that can generate protections, but they not always come out of the paper.In a time that technology is everywhere 24/7, we have to feel as if we lived in safety. At least this is the feeling that technology should grant us.Companies are increasingly using this technology for its practicality. Wireless networks are in almost every stablishment nowaydays, such as shopping malls, airports, stores, offices, etc... Technology moves forward extremely fast, but it's safety remains the same. Creating an advanced technology is more importante than knowing how to keep it safe. Until the consequences appear. Due to network's data traffic, companies can become vulnerable to malicious attacks of people who want favoured informations, putting in danger informations that are extremelly necessary for their functioning.

Therefore, in the face of this theme's relevance, wireless networks should be safe and reliable to their users. For this reason, this article has been developed in order to contribute with wireless network's safety improvement, being presented to entrepreneus and users, the safety measures that must be taken by those who have this type of network, in addition to the safest way of using it.

Key-words: safety, network, technology, protection, vulnerability

Introdução

A rede de computadores revolucionou o mundo, possibilitando a comunicação global em tempo real e a evolução na era digital.

Em meados dos anos 60 nos Estados Unidos EUA, surge à primeira rede de computadores batizada de ARPANET financiada pelo governo americano com o objetivo militar de estabelecer a transmissão de dados entres a base militar e os departamentos de pesquisa. No inicio dos anos 70 as universidades da

Califórnia em Los Angeles, SRI (em Stanford), a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah foram conectadas a rede ARPANET.

No final dos anos 70 a rede ARPANET se divide, e foi criada a rede MILNET para fins militares e a INTERNET que se tornou uma rede publica. .

Com o passar dos anos a internet cresceu e o numero de acesso também, até pouco tempo atrás a maioria dos acessos à internet eram feitos através de conexões discadas que raramente ultrapassavam 56kbps. O usuário precisava de um modem e de uma linha telefônica, se conectando através de um provedor de acesso que mantinha a conexão por determinado tempo. Com os avanços da tecnologia, novas alternativas apareceram, e atualmente grande parte dos computadores pessoais ficam conectados na internet pelo tempo que quiserem e a velocidade chega até 100mbps. A conexão com internet também não é mais um recurso disponível apenas para computadores, visto que por causa da grande quantidade de equipamentos que surgiram foi necessário a inserção dessa tecnologia neles também.

O Institute of Electrical and Electronic Engineers (IEEE)

O *Institute of Electrical and Electronic Engineers (*IEEE) é uma organização profissional fundada nos Estados Unidos e tem como objetivo desenvolver padrões técnicos de acordo com fabricante, definindo como dará a comunicação entre fabricante e cliente de rede. Ao longo do tempo, foram desenvolvidos diversos padrões, a qual destacou e melhor desenvolveu foi o 802.11, conhecido como Wi-Fi (Wireless Fidelity ou fidelidade sem fio) (RUFINO, 2005).

A seguir serão citados os principais padrões utilizados.

Padrões de rede sem fio.

Padrão IEEE 802.11

O padrão IEEE 802.11 foi criado em 1997 pelo *Institute of Electrical and Electronic Engineers, desenvolvido para suprir aplicações com altas taxas de transmissão de dados,* como as redes *Ethernet.*

Após sete anos de estudos que determinou o padrão operasse no intervalo de frequências entre 2,4 GHz e 2,4835 GHz. Sua taxa de transmissão de dados é de 1 Mb/s ou 2 Mb/s (megabits por segundo) e é possível usar as técnicas de transmissão *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS).

Na época o principal objetivo da primeira versão chamada de IEEE 802.11 era estabelecer um padrão com os fabricantes para criar uma compatibilidade entre os dispositivos existentes.

Padrão 802.11a:

Disponibilizado no final do ano de 1999, o padrão 802.11a possibilita operar com taxa de transmissão de dados de 6 mb/s, 48 Mb/s e 54 Mb/s, alcançando uma transmissão de 50 metros, assim regulamentando redes WLAN (Wireless local Area Network) uti:lizando a maior frequêcia de 5 GHz de transmissão, o seu alcance diminui conforme o poder de penetração nos obstáculos.

ENGST e FLEISHMAN (2005) destacam suas características: Aumento de velocidade para utilização em 54 Mbps ou aproximadamente 25 Mbps de Thoughput real.

Opera com faixa de 5 GHz, tendo poucos concorrentes, porém o alcance é reduzido, mas com melhores protocolos que o 802.11b, conectando 64 clientes, Contém 12 canais não sobrepostos, que permite que os pontos de acessos possam cobrir a área um do.

E sua desvantagem é a incompatibilidade com o padrão 802.11b, ao qual possui uma plataforma instalada no cenário tecnológico atual. Mesmo com a taxa de transmissão maior, o padrão 802.11a não chegou a ser popular, pelo seu alto custo destinando ao mercado corporativo.

Padrão 802.11b:

O padrão 802.11b surgiu entre 1999 a 2001, ENGST e FLEISHMAN (2005) chama-o de "O Rei Dominante", pelo fato de ser popular e com a maior base instalada e com muitos produtos e ferramentas de administração disponíveis no mercado atual.

O 802.11b utiliza a frequência de 2.4 GHz permitindo transmissões de até 11Mbit/s, suporta no Maximo 32 clientes conectados. (Rufino 2005)

Este padrão está sendo substituído aos poucos pelo padrão g com maior velocidade.

Padrão 802.11g:

O Padrão 802.11 g é o mais usado no Brasil, seu surgimento foi em meados de 2002 possuindo uma tecnologia ideal para a utilização, sendo rápida e compatível com o mercado de redes sem fio, trabalhando com a frequência 2.4GHz e permite transmissões de até 54 Mbit/s.

Tendo como suas características a velocidade que pode chegar a atingir 54 Mbps; Compatibilidade total dos equipamentos do protocolo 802.11b.

Padrão 802.11n:

Padrão 802.11n também conhecido como Word Wide Spectum Efficiency (WWiSE) seu objetivo é alcançar um determinado aumento na área de cobertura de sinal, esse padrão é muito utilizado no Japão e Estados Unidos EUA pois nestes países a conexão residencial passa de 50 Mbit/s e transmite em 300 Mbit/s com alcance máximo de 400 metros.

Podendo operar com canais de 40 Mhz, e mantém compatibilidade com os padrões existentes que trabalham em 20 Mhz, podendo ter sua velocidade oscilando em torno de 135 Mbps (Rufino, 2005).

Principais Protocolos de Segurança

Segurança do padrão IEEE 802.11

É o mais difundido para *Wireless Local Area Network* (WLAN) provê segurança para WLAN com autenticação e cifragem da comunicação. O protocolo especificado pelo IEEE para a segurança em redes sem fio é o WEP, que é alvo de críticas por possuir uma maior vulnerabilidade e ser alvo de diversos ataques. Um caso que demonstrou a fraqueza do WEP aconteceu nos Estados Unidos: Análises de segurança em redes sem fio foram conduzidas por empresas especializadas nos aeroportos internacionais de Denver e de San Jose.

A análise em Denver revelou que a American Airlines operava uma rede sem fio totalmente em claro no aeroporto e houveram ataques em tempo real no meio da análise. Em San Jose, a análise revelou resultados similares aos de Denver: Pouca ou nenhuma segurança contra esses ataques.

WEP (*Vire Equivalente Priva*)

Para que haja uma comunicação numa rede sem fio basta que tenha um receptor de sinal, uma recepção passiva, diferente de uma rede cabeada, que necessita de uma recepção física entre as duas partes. Diante disto o protocolo 802.11 oferece a opção de cifragem de dados, ao qual o WEP é sugerido para solucionar o problema.

O padrão WEP não tem suporte a uma autenticação, seu objetivo é proteger os dados para não serem capturados por qualquer um no meio de transmissão. O algoritmo WEP se baseia em uma senha

(chave) secreta que é compartilhada entre o AP e os usuários. O WEP utiliza esta senha para codificar toda a informação que circula pela rede. O WEP usa um algoritmo de criptografia chamado de RC4, que foi feito pela entidade RSA. A senha secreta compartilhada pode ser de 64, 128 ou 256 bits.

WPA - Persona (Acesso Protegido Wi-Fi Pessoal)

O WPA foi criado para solucionar a vulnerabilidade do WEP e normalmente utilizado na solução de segurança mais forte (TEIXEIRA; SILVA, 2012) é um dos métodos de segurança sem fio que fornece proteção forte dos dados e evita o acesso não autorizado às redes. Utiliza criptografia TKIP e impede o acesso não autorizado à rede com o uso de uma senha pé-compartilhada (PSK).

O WPA trabalha com duas áreas diferentes, a primeira substitui o WEP, para cifrar objetivando a integridade e a privacidade das informações na rede, a segunda atua diretamente na autenticação do usuário utilizando troca de chaves dinâmica que não era feito pelo WEP.

WPA2 - Persona e WPA2-Enterprise

Foi lançado num consórcio WI-FI em 2004 baseado na especificação 802.11i, utiliza-se do algoritmo criptográfico Counter Cipher Mode Protocol (CCMP).

Considerado o melhor padrão de segurança que existe atualmente, com proteção dos dados, acessos e autenticação dos usuários. A base do algoritmo é o AES, sem falhas, diferente do algoritmo RC4.

Protected Acess (WPA) e padrão IEEE 8002.11i

Tissato e Lício (2007) descreve que, o WEP possui falhas de projetos que envolvem o uso de chaves estáticas, a falta de autenticação mútua e o uso de criptografia fraca, entre outros. Novos padrões estão sendo desenvolvidos como o Wi-Fi Protected Acess (WPA), o IEE 802.11i, também conhecido como Task Group 1 (TGi), e o 802.1X.

O subgrupo IEEE 802.11i ou TGi tem como objetivo eliminar dois principais problemas do WEP, que são o uso de chave estática e a criptografia fraca.

Além do padrão 802.11i, a Wi-Fi Alliance está especificando, em conjunto com o IEEE, o Wi-Fi Protected Acess (WPA), também desenvolvido para sanar erros do WEP como a proteção de dados e o controle de acesso.

A melhoria da criptografia de dados que é fraca no WEP, é feita no WPA pelo Temporal Key Integrity Protocol (TKIP), ele usa um conjunto de técnicas para incrementar a segurança.

Já o mecanismo de autenticação dos usuários que não existe no WEP, é feito no WPA pelo 802.1X e pelo Extensible Authentication Protocol (EAP), que formam o framework de autenticação do WPA.

Tipos de ataques na rede WI-FI

Os tipos de ataques que podem ocorrer numa rede Wi-Fi são: Engenharia social, WLAN Scanners, *Man in the Middle*, Ataque de Inundação UDP, Ataque de Inundação UDP, IP *Spoofing*, Ponto de Acesso Falso, Ataque de Engenharia Elétrica, MAC *Spoofing*, Ataque de Senhas, Força bruta, Ataques *Sniffers*, Ataque usando o *Aireplay*, *Denial of Service* (DoS), *Port Scanning.*

Descreveremos a seguir cada ataque em rede WI-FI selecionados pelos autores de acordo com SILVA, Luiz Carlos da (2010) apontou em seu artigo.

Engenharia Social

Termo referente a uma forma de ataque, seu ataque é persuadir algum usuário para obter informações privilegiadas sem a devida autorização, pessoa má intencionada se infiltra na empresa ou se aproxima de funcionários para obter informações restritas do sistema da empresa para posteriormente efetuar o ataque.

Exemplo de ataque de engenharia social:

Você recebe uma mensagem de e-mail, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

O ataque só terá sucesso se o usuário decidir fornecer informações sensíveis ou executar programas.

WLAN *Scanners*

Quando algum dispositivo operando na mesma frequência do ponto de acesso dentro do alcance, pode captar os sinais transmitidos. Mesmo desabilitado o envio de broadcasts no AP não impede que scanners como o NetStumbler detectem uma rede sem fio, pois está enviando pacotes mesmo sem nenhum usuário conectado, os scanners enviam pacotes de solicitação de SSID para todos os canais e é aguardada a resposta do AP. Faz a captura das informações da rede, alguns scanners como o NetStumbler possui a capacidade de localização do Ponto de Acesso através do uso de um GPS.

Man in the Middle

O ataque Man in the Middle nada mais é do que roubar informações de usuários, o sequestro de uma conexão TCP é um dos possíveis ataques do tipo *man-in-the-middle*. Ou também conhecido como ataque de penetra, porque ficar entre o cliente e o servidor observando os dados sigilosos.

O ataque de penetra permite uma conexão normal do usuário com a rede usando a autenticação entre dois pontos para depois assumir o controle da conexão entre o usuário e o AP. Existem dois métodos usados pelo usuário: um é durante o *handshake* (passos iniciais da comunicação) de três etapas do TCP, e o outro é no meio de uma conexão que se aproveita de uma falha no estado "desincronizado" da comunicação TCP. Quando dois hosts (pontos na rede) não estão adequadamente sincronizados, descartam (ignoram) pacotes um do outro. Nesta hora o atacante pode injetar pacotes forjados na rede que tenham os números sequenciais corretos. Assim o atacante no caminho da comunicação entre o cliente e o AP, para poder espionar e reproduzir pacotes que estejam sendo enviados na rede.

O sequestro de uma conexão TCP permite que os atacantes vejam e alterem informações privadas dos usuários que estão circulando na rede.

Exemplo de ataque:

O invasor usa um router WiFi como mecanismo para interceptar conversas de algum usuário o que pode se dar tanto através de um router corrompido quanto através de falhas na instalação de um equipamento. Numa situação comum o agressor configura seu laptop, ou outro dispositivo wireless, para atuar como ponto de WiFi e o nomea com um título comum em redes públicas . Então quando um usuário se conecta ao "router" e tenta navegar em sites delicados como de online banking ou comércio eletrônico o invasor rouba suas credenciais.

Num caso recente um hacker usou debilidades na implementação de um sistema criptográfico de uma rede WiFi real e a usou para capturar informações. Esta é a situação mais incomum, mas também a mais lucrativa. Se o invasor for persistente e acessar o equipamento hackeado por dias e horas

a fio terá a possibilidade de espiar as sessões de seus usuários silenciosamente fazendo com deixando as vítimas a vontade para usar informações delicadas durante a navegação.

Ataque de Inundação UDP

O UDP é um protocolo do tipo sem conexão, pois não precisa de qualquer procedimento para estabelecer uma conexão e começar a transferência de dados. O ataque de inundação UDP acontece quando o atacante enviar vários pacotes UDP para o sistema da vítima. O alvo recebe o pacote UDP, ele tenta descobrir qual é o aplicativo que pertence a esta solicitação. Se perceber que não há aplicativo destinado a receber estes pacotes, é criado um pacote de resposta ICMP de "destino não alcançado" e o envia para o endereço forjado. Se for enviado uma grande quantidade de pacotes UDP o sistema acaba abrindo as portas de acesso para o invasor. Pois o sistema ira liberar o acesso ou ficar ocupado processando as informações.

IP *Spoofing*

O IP *Spoofing* usa uma técnica para enganar o usuário comum. Isso porque ele simplesmente troca o IP (internet Protocolo, o "endereço" do internauta na Web) original por outro falso. Assim o cracker assume a "identidade" da vítima verdadeira. Este ataque pode criar centenas de usuários não existentes dentro de um sistema, isto causa aumento do consumo da largura de banda, uso inútil do processado com processos desnecessários e sobrecarga nos equipamentos.

De acordo com Roger. "O *cracker* usa o *spoofing* quando quer sequestrar alguma conexão entre o computador do cliente e o servidor, no caso do usuário doméstico, ele falsifica o IP da vítima e realiza o ataque via Web".

Roger afirma que "O criminoso usa um programa que procura saber quantos IP's estão conectados na Internet. A partir daí, utilizando softwares específicos, ele os falsifica".

Ponto de Acesso Falso

Este ataque é novo do tipo. Ele aproveita falhas nos sistemas operacionais e a falta de atenção do usuário. Utilizando um software para transformar a sua placa wireless em um ponto de acesso o

notebook se comporta como um AP assim é só ligar ele em uma rede cabeada para dar acesso à internet a vítima.

Isto é possível porque o invasor configura o notebook com o mesmo nome do ponto de acesso, sendo que o sinal do computador é mais forte que o sinal do AP verdadeiro. Como o Windows sempre se conecta com o sinal mais forte então acaba se conectando no ponto falso, o Windows irá mandar os dados como se fosse para o verdadeiro.

Deste jeito o invasor obteve acesso aos dados de acesso do verdadeiro ponto de acesso e outras informações importantes que estão sendo transferidas na rede.

Ataque de Engenharia Elétrica

A antena utilizada em uma rede wireless emite um sinal normalmente na frequência de 2.4 GHz (Frequência muito utilizada por outros produtos). É possível utilizar um *magnetron* de um forno micro-ondas para gerar uma interferência elétrica na antena Wireless ou comprar uma antena que gere ruídos em várias frequências. Se tiver ruídos na rede sem fio torna-se impossível estabelecer uma conexão com o AP, pois não pode fazer a sincronização.

MAC *Spoofing*

É uma técnica que simplesmente altera o endereço físico da sua placa sem fio ou placa de rede. O programa SMAC pode ajuda a fazer esta alteração do MAC *Address* no sistema operacional Windows.

A técnica de falsificação de endereços não é utilizada apenas para falsificação de endereços, mas serve também para evitar que o endereço real de um ataque seja reconhecido durante uma tentativa de invasão.

Ataque de Senhas

Para Cliff. “a utilização de senhas seguras é um dos pontos fundamentais para uma estratégia efetiva de segurança. As senhas garantem que somente as pessoas autorizadas terão acesso a um sistema ou à rede. As senhas geralmente são criadas e implementadas pelos próprios usuários que utilizam os sistemas ou a rede. Palavras, símbolos ou datas fazem com que as senhas tenham algum significado para os usuários, permitindo que possa ser lembrada.

Neste ponto é que existe o problema, pois muitos usuários priorizam a conveniência ao invés da segurança. Com o resultado, eles escolhem senhas que são relativamente simples. Com isso facilitam o trabalho de quebra dessas senhas por *hackers*. Invasores estão sempre testando as redes e sistemas em busca de falhas para entrar. O modo mais notório e fácil a ser explorado é a utilização de senhas inseguras".

Os profissionais de segurança da informação têm que educar os usuários que utiliza as senhas. Mostrar como usar a senha de modo seguro e fazer implementações no sistema para garantir que as senhas escolhidas pelos usuários tenham uma quantidade mínima de dígitos, números e letras.

Força bruta

Enquanto as listas de palavras, ou dicionários, dão maior velocidade no processo de quebra de senha, o segundo método de quebra de senhas simplesmente faz a repetição de todas as combinações possíveis. Este é um método muito bom para descobrir as senhas, no entanto é muito lento porque são nove verificadas todas as possibilidades existentes em uma determinada quantidade de dígitos.

Ataques *Sniffers*

São programas responsáveis por capturar os pacotes da rede. Os *sniffers* exploram o tráfego dos pacotes das aplicações TCP/IP, por não utilizar nenhum tipo de cifragem nos dados. Com esse programa, qualquer informação que não esteja criptografada é obtida.

Segundo Figueiredo a definição de *sniffers* é a seguinte: "São programas que permitem monitorar a atividade da rede, registrando nomes (username) e senhas sempre que estes acessam outros computadores da rede.

Estes programas ficam monitorando o tráfego da rede para capturar acessos a serviços de redes, tais como: serviço de e-mail remoto (IMAP, POP), acesso remoto (telnet, rlogin, etc), transferência de arquivos (FTP), etc., acessos feitos, pacotes capturados. Sempre com o objetivo de pegar a identificação de acesso e a conta do usuário".

O *Sniffer* funciona em conjunto com a placa ethernet ou placa WI-FI existente na máquina. O procedimento padrão das placas é descartar todos os pacotes da rede que não esteja endereçado para a placa. O *Sniffer* coloca as placas no modo promíscuo (monitor), que faz com que as placas recebam todos os pacotes transmitidos na rede e armazena para ser analisados posteriormente.

Existem diversos cenários e topologias nas quais o *sniffer* pode ser utilizado para capturar informações contidas em uma determinada rede cabeada ou sem fio.

Ataque usando o *Aireplay*

Faz-se quatro tipos de ataques pelo programa *Aireplay* tanto na versão Linux quanto Windows. O ataque dois é parecido com o ataque três não sendo muito relevante.

O primeiro ataque é chamado de ataque zero que faz a desautentificação do cliente junto ao AP utilizado, assim provoca uma reautenticação do cliente junto ao ponto de acesso possibilitando fazer a captura do pacote *handshake* do WPA.

Mas pode se usando para fazer a negação do serviço, já que permite mandar muitos pacotes de desautentificação, fazendo com que o PC do usuário fique tentando se conectar ao AP por um longo tempo sem sucesso na conexão.

O ataque um faz a autentificação falsa, para fazer este ataque precisar ter alguém usando o AP e trocar o endereço MAC da placa WI-FI que será usada neste ataque. Já o ataque dois permite eleger um dado pacote para reenviá-lo, às vezes proporciona resultados mais efetivos que o ataque três (reinjeção automática de ARP).

O ataque três é o mais utilizado, a reinjeção de requisição ARP. Este ataque faz a injeção dos pacotes no AP fazendo com que o mesmo gere mais pacotes IV's, utilizado para fazer a quebra da segurança WEP e WPA, quanto maior quantidade de pacotes mais rápidos e preciso será encontrada a chave de criptografia do AP.

***Denial of Service* (DoS)**

A frequência 2.4 GHz é usada por outros dispositivos sem fio como, por exemplo, telefones sem fios, dispositivos Bluetooth e equipamentos de monitoração de Bebês, etc. Por se uma frequência aberta todos os fabricantes de produtos adotam para não ter que adquirir uma licença na Anatel. Estes equipamentos um perto do outro em funcionamento causam degradação do sinal fazendo com que a capacidade e a qualidade diminuam. Um indivíduo com o equipamento apropriado pode enviar uma grande quantidade de sinais (*flood*) na mesma frequência fazendo fazer com que a rede pare de funcionar.

Outro problema relacionado à DoS é o conflito entre redes próximas. É comum o uso pelo fabricante do mesmo canal default para todos os equipamentos fabricados é a falta de configuração do usuário.

O principal tipo de ataque DoS é aquele que força o consumo total da largura de banda de uma rede específica. Normalmente este ataque ocorre em uma rede local, mas pode acontecer de maneira remota em todos os tipos de aparelhos eletrônicos.

Apesar de não causarem a perda ou roubo dos dados os ataques DoS são graves. Deixa a rede indisponível quando um usuário precisa utilizá-lo.

Exemplo de ataque DoS de uma forma figurada:

Imagine que você utiliza um ônibus regularmente para ir ao trabalho. Certo dia, no entanto, uma quantidade grande de pessoas "furou a fila" e entrou no veículo, deixando-o tão cheio que você e os demais passageiros regulares não conseguiram entrar. Ou então, imagine que você tenha conseguido entrar no ônibus, mas este ficou lotado ao ponto de não conseguir sair do lugar por excesso de peso. Este ônibus acabou negando o seu serviço - o de transportá-lo até um local -, pois recebeu mais solicitações - neste caso, passageiros - do que é capaz de suportar

Smurf

Explora erros de configurações em roteadores permitindo a passagem de pacotes ICMP *echo* a rede, a origem desses pacotes é falsificada como sendo o endereço da vítima, os pacotes chegam à rede, ele será multiplicado e, portanto, a vítima será inundada por muitos pacotes até que a rede pare de responder por causa da sobrecarga.

Exemplo de ataque:

Nos últimos seis meses a rede brasileira cuja configuração de roteadores permite este ataque tem sido utilizada com intensidade cada vez maior criando prejuízos tanto para as vítimas quanto para as redes 'amplificadoras'.

Inundação SYN:

Metodo de ataque DDoS de camada quatro que explora os recursos de conexão do servidor.

Em uma inundação de SYN, o ataque trabalha em cima do handshake (processo usado entre duas maquinas para se reconhecer e estabelecer uma comunicação entre as mesmas).

O primeiro programa emite um pacote do TCP SYN (sincronização), que seja seguido por um pacote do reconhecimento do TCP Syn-syn-ack (aplicação de recepção). Então, o primeiro programa responde com um ACK (reconhecimento). Uma vez que isto foi feito, as aplicações estão prontas para trabalhar.

Exemplo de ataque:

Durante um ataque de inundação SYN, um usuário do invasor envia várias mensagens SYN ao servidor-alvo. O servidor cria um registro em sua tabela de conexão para cada SYN recebido e responde a todos com uma mensagem SYN-ACK. O agressor pode não enviar uma mensagem ACK, mas muitas vezes falsifica o endereço IP do cliente nos pacotes SYN para que as respostas SYN-ACK do servidor-alvo nunca sejam recebidas. À medida que o agressor continua a enviar mensagens SYN, as tabelas de conexão do servidor-alvo ficam cheias, e o servidor não pode mais responder a nenhuma solicitação de conexão. Com todos seus recursos consumidos, o servidor-alvo não consegue se conectar com clientes legítimos, o que gera uma negação de serviço

Port Scanning

É o processo de verificação de quais serviços estão ativos em um determinado *host*, ou seja, é um processo para se conectar nas portas TCP e UDP do sistema alvo para determinar que serviço esteja em execução.

Segundo LIMA, "este processo é utilizado tanto por um administrador de redes para realizar uma auditoria eliminando assim quaisquer serviços que estejam rodando sem necessidades ou pode ser utilizado por um hacker para obter informações sobre as vulnerabilidades existentes no sistema".

Detectar atividades de varredura de portas é essencial para saber quando um ataque pode ocorrer e como ocorrera.

Falhas do WEP que Geram Ataquem de Pessoas Mal-Intencionadas

Jessé Walker, da Intel, foi um dos primeiros a mostrar que a chave WEP não é segura independentemente do tamanho da chave.

Também mostraram que é possível quebrar chaves de 128 bits e 256bits.

Uma das ferramentas usadas pelo Jessé Walker foi o AirSnort, uma ferramenta feita para ser usada no Linux, só funciona na placa wireless que tem o *chipset* Prism2. Após colocar a placa wireless em modo promiscuo (monitor) através de um *shell* script (dopromisc.sh), iniciando o modo de captura que serão armazenados e analisados depois. Assim que for capturado um número suficiente de pacotes para quebra o WEP, basta para a captura e começar a quebra da criptografia WEP.

De acordo com a documentação da ferramenta, são necessários aproximadamente 1500 pacotes "interessantes" para quebrar uma chave WEP de 128 bits, ou seja, precisa de 1500 IVs que são pacotes de inicialização.

Outra ferramenta disponível é o WEPCrack. O WEPCrack é composto por 4 scripts feitos em Perl que são usados para decodificar pacotes, identificar pacotes fracos e quebra a chave WEP. Mas o WEPCrack precisa de um sniffer para capturar os dados na rede, pois não tem um incluído.

Ataques ao ARP

O Ataque ARP *Spoofing* permite que o invasor intercepte quadros trafegados na rede, modificando-os e até podendo parar o tráfego, esse ataque só ocorre em segmentos da rede de área local.

Redireciona todo o tráfego via *spoofing* (falsificação) do endereço MAC da placa.

Outro ataque possível é o ARP *Poisoning*, este ataque é o mais hábil, pois permite que o invasor intercepte informações confidenciais ficando no meio de uma conexão de duas ou mais maquinas, atacante e a vítima estão no mesmo domínio de broadcast da rede. Esta técnica se aplica apenas em redes Ethernet.

Ataques a Smurf e DHCP

O *Smurf* é um ataque que gera uma grande quantidade de tráfego de pacotes ping (ICMP Echo) que é enviado para o endereço de IP de broadcast da rede. A vítima que teve o endereço falsificado recebe os pacotes de todas as máquinas da rede, causando lentidão na rede. Com o ataque DHCP *Spoofing*, colocar um servidor DHCP falso na rede, sendo assim, forçando uma configuração falsa das estações de trabalho da rede.

Bluetooth

É baseado em radiofrequência e com intuito de conexão de dispositivos de curta distância que permite a formação de redes pessoais sem fio. Disponível em muitos equipamentos, a quantidade de aplicações também é vasta, incluindo sincronismo de dados entre dispositivos, comunicação entre outros computadores, periféricos e transferência de arquivos.

Também tem seus riscos como em todo e qualquer tipo de redes em geral, como varredura, furto de dados, uso indevido de recursos, ataque de negação de serviço, interceptação de tráfego e ataque de força bruta.

Para Régio, os riscos a que as comunicações Bluetooth estão submetidos podem ser divididos basicamente em: captura de tráfego (escuta); negação de serviço; forja de identidade; configuração padrão e força bruta, acesso não autorizado, esses problemas podem causar violação de integridade, confidencialidade ou disponibilidade dos dados dos usuários conectados a ela.

Exemplo de ataque via Bluetooth

Uma recente polêmica em torno da falta de segurança dos dispositivos com Bluetooth aconteceu no Reino Unido, na cidade de Bath, onde através de scanners pela cidade, milhares de moradores tiveram suas atividades diárias sendo monitoradas.

Isso vai contra a quebra de sigilo e privacidade dos habitantes pois aconteceu sem qualquer autorização. Após os dados dos habitantes serem coletados para o projeto Cityware, ele era colocado na internet para download gratuito que poderia ser feito por qualquer um com acesso à internet, tudo após seus dados terem sido scaneados por bluetooth.

Conexão está ativo e acabam não se preocupando em tomar alguma atitude defensiva quanto a isto.

Cuidados a serem tomados:

Os cuidados a serem tomados em rede sem fio constituem em diferentes níveis de eficiência quando se trata de proteção das informações dos usuários. Neste quesito os principais assuntos a serem questionados estão relacionados á abrangência da rede, quantidade de hosts e as ferramentas necessárias para garantir um uso adequado das tecnologias, deste modo precisa de uma estratégia eficiente de segurança, deixando claro a diferença nas redes coorporativas e redes domésticas. Grande parte dessas técnicas de proteção a rede Wi-Fi são de simples realização e muitas vezes garantem a confiabilidade dos dados. (NAKAMURA; GEUS, 2007).

A seguir serão relatadas algumas recomendações para prevenção de possíveis ataques:

° Manter inativo a rede e ativar somente para uso.

° Mudar senha padrão de administrador do equipamento evita que senhas conhecidas sejam usadas em ataques.

° Usar padrão de criptografia apropriada, os equipamentos devem ser configurados conforme o ambiente onde estão inseridos.

° Manter a opção de visibilidade em culto ou invisível para não mostrar seu nome de usuário publicamente.

º Alterar o nome de usuário padrão e não usar dados pessoais.

° Sempre alterar a senha PIN padrão do dispositivo.

° Evitar fazer pareamento em locais públicos.

° Remover todas as relações de confiança já estabelecidas em caso de perda ou furto em um Bluetooth

° Ficar atento ao receber mensagens que solicitem autorização ou PIN, não responder.

° Execução de testes Periódicos de segurança avalia possíveis vulnerabilidades da rede.

Conclusão

Mediante o assunto exposto ao longo do trabalho, conclui que a segurança de rede WI-FI em diversos sistemas operacionais exige do usuário seja ele doméstico ou corporativo uma conscientização sobre qual a melhor forma de configurar o equipamento e os meios de maior eficácia da prevenção de possíveis ataques. Os usuários devem pesquisar softwares que possam ser utilizados como meio de auxílio à detecção de uma atual vulnerabilidade, mediante uma realização de testes para monitorar falhas na segurança, garantindo a confiabilidade da conexão.

É de suma importância a divulgação para o público em geral de informações sobre o processo de configuração correta da rede WI-FI, destacando importância de ferramentas que garantam a devida segurança da rede.

A falta de informação também faz que os profissionais da área tenham algumas dificuldades, em questão referente à segurança física. Partindo do ponto que fazem o uso desse tipo de conexão em rede de grande alcance, os profissionais tendem a trabalhar com altos números de estações associadas, tornando mais prejudicial uma possível invasão.

O Importante ressaltar que a utilização de alguns métodos de defesa pode ser ineficiente frente a certos tipos de ferramentas de ataque mais robustas, visando essa realidade o ideal é utilizar principalmente em redes de grande porte, métodos de defesa específicos para cada tipo de ameaça. Uma prevenção continua gera maior segurança e uma melhor preservação da confidencialidade de seus usuários.

Sugestão para estudos futuros

Este artigo buscou não apenas entender questões relativas sobre a segurança das redes e suas vulnerabilidades, como também levantar questões sobre como podemos melhorá-la posteriormente.

Portanto serão apresentadas em seguida, possíveis considerações para estudos posteriores.

RADIUS, porque usar?

O RADIUS tem diversas funcionalidades que o qualificam como um sistema eficiente de autenticação de redes, suas vantagens são:

- Modelo cliente/servidor: O RADIUS utiliza o modelo cliente/servidor que tem como cliente o NAS, responsável por enviar informações dos usuários que desejam acessar o serviço do NAS para o servidor RADIUS, que verificará a autenticidade do usuário e informará se é valido ou não, ou seja, todas as informações antes de chegarem ao servidor RADIUS, passam pelo NAS, até mesmo limites de acesso por usuário e tempos máximos de conexão.

- Segurança: A transferência de dados feita entre cliente e servidor são autenticadas através de um segredo compartilhado que nunca é enviado pela rede. É um segredo conhecido tanto do cliente quanto do servidor, serve para garantir a autenticidade de cada usuário para cada serviço requisitado. As senhas são altamente criptografadas.

- Flexibilidade e Adaptabilidade: O RADIUS pode permitir autenticação de muitos usuários ao mesmo tempo através do uso de seus servidores, utilizando proxy para servidores de maiores capacidades de processamento, isso ajuda para dispositivos de rede que não conseguem arcar com muitos números de usuários tentando se conectar.

- Protocolo extensível: O RADIUS permite que novos atributos sejam adicionados sem atrapalhar implementações previas do protocolo, também é possível estabelecer novos parâmetros e novos mecanismos de autenticação sem precisar alterar o formato do pacote.

- Compatibilidade: Servidores RADIUS podem verificar credenciais dos usuários em bancos de dados fora das próprias, dessa forma, a implementação de um servidor RADIUS pode ser realizada de forma a reaproveitar de usuários já existentes.

Referências

Alagoas, **Olho d'Água das Flores**. Disponível em: <http://www.ufal.edu.br/unidadeacademica/ic/graduacao/sistemas-de-informacao/arquivos-monografias/arquivos-2012/seguranca-em-redes-sem-fio>. Acesso em: 29 maio. 2017

ASSUNÇÃO, Marcos Flávio Araujo**. WIRELESS HACKING**: ataques e segurança de redes sem fio Wi-Fi. São Paulo: Visual Books, 2012

CARTILHA de segurança para internet. Disponível em :<https://cartilha.cert.br/redes/> Acesso em: 24.abr.2017

CLIFF, A. **Password Crackers – Ensuring the Security of Your Password,** 09 abr. 2001.Disponível em:<*http://www.securityfocus.com/*> Acesso em: 29.Maio.2017.

Disponível em:<http://cio.com.br/tecnologia/2016/08/31/fraudes-ss7-evite-que-falhas-na-rede-coloquem-suas-informacoes-em-risco/>Acesso em: 24.abr.2017

Disponível em:<http://exameinformatica.sapo.pt/noticias/software/2016-07-20-Descoberta-falha-que-permite-assumir-controlo-de-redes-moveis-inteiras> Acesso em: 24.abr.2017

DUARTE, Luiz Otavio. **Análise de vulnerabilidades e ataques inerentes a redes sem fio** 802.11x.2003. 53f.

FLEISHMAN, Glenn & ENGST, Adam. **Kit do iniciante em redes sem fio**. 2.ed. São Paulo: Makron Books, 2005.

IEEE Advancing Tchnology for Humanity. Disponível em:<http://www.ieee.org.br/organizacao/> Acesso em: 30. Maio.2017.

INFOWESTER. O que é Wi-Fi (IEEE 802.11). Disponível em:<https://www.infowester.com/wifi.php> Acesso em: 29.maio.2017.

Luiz Carlos da Silva. Furto de Sinal Wi-Fi. 2010. Disponível em:<www.teleco.com.br/tutoriais/tutorialwifiroubo/> Acesso em: 25 abr.2017

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos**. 1. ed. São Paulo: Novatec, 2007.

RUFINO, Nelson. **Segurança em Redes sem Fio: aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth**. 2. ed. São Paulo: Novatec, 2005.

RUFINO, Nelson. **Segurança em Redes sem Fio**. 3. ed. São Paulo: Novatec, 2011.

TECMUNDO. Disponível em:<www.tecmundo.com.br> Acesso em: 29 maio. 2017.

TEIXEIRA, Iêda Paula de Farias; SILVA, Maria das Graças Maciel. **Segurança em redes sem fio**. 2012. 56f. Trabalho de Conclusão de Curso (Sistemas de Informação) – Universidade Federal de