1. INTRODUÇÃO

Os grandes problemas de segurança nas empresas no contexto técnico e de negócio dos dias de hoje, as diversas tecnologias de segurança que não são mais válidas, e a falha de reconhecer profundamente essas alterações impede com que soluções mais eficazes sejam adotadas para lidar com novos problemas relacionados à segurança de sistemas.

Nas seções seguintes são apresentados alguns conceitos relacionados a estrutura deste trabalho de pesquisa.

1.1. CONTEXTO DO TRABALHO

O conceito de *Sobrevivência* (*Survivability* no original em inglês) dá uma nova perspectiva técnica e de negócios no que diz respeito à segurança. Além disso, expande a idéia de que a segurança não é apenas trabalhada por peritos e técnicos de segurança, mas também envolve a participação de toda a organização para proteger os sistemas críticos contra ataques, acidentes ou falhas.

Sobrevivência pode ser definida como a capacidade que um sistema tem para cumprir sua missão em um espaço de tempo adequado mesmo na presença de ataques, falhas ou acidentes [EFL99]. Neste trabalho estaremos usando os termos *survivability* e *sobrevivência* de maneira análoga para descrever o mesmo conceito. Utilizando-se do Método de Cálculo da Vulnerabilidade Potencial e com o auxílio da ferramenta de simulação EASEL, estaremos criando cenários de aplicações baseadas em redes sem fio, mostrando as diversas formas de ataques a essas redes, e sugerindo melhorias na segurança visando à sobrevivência do negócio.

1.2. OBJETIVOS DO TRABALHO

O trabalho proposto tem por objetivo *a análise de uma metodologia* para estudos de segurança de sistemas, concentrando-se na capacidade de sobrevivência de uma empresa sob a perspectiva de falhas de segurança e ataques aos seus sistemas de informação. Diante de um cenário empregando o uso de redes sem fio, estaremos estudando as diversas vulnerabilidades conhecidas e simulando possíveis combinações de segurança visando um ambiente seguro e estável. Entende-se por seguro e estável um sistema que com alta probabilidade de executar suas tarefas de missão crítica. A metodologia a ser empregada baseia-se em uma linguagem de simulação especificamente desenvolvida para esse fim, chamada EASEL. Esta permite a modelagem de sistemas complexos constituídos por um número muito grande de elementos interagindo entre si.

A ferramenta EASEL, desenvolvida e apoiada o seu uso pelo CERT® , órgão de pesquisas na área de segurança de redes e Internet ligada à Universidade Carnegie Mellon, já desenvolveu diversas pesquisas com a ferramenta e muitos trabalhos acadêmicos. O mecanismo de simulação do Easel fornece em um ambiente simulado composto por atores fracamente acoplados interagindo sem controle central ou visibilidade global segundo Fischer. [FISHER99B]

1.3. JUSTIFICATIVAS DO TRABALHO

As principais justificativas para a implementação deste trabalho são as seguintes:

- A necessidade do desenvolvimento de novas metodologias para tratar e trabalhar os problemas relacionados à segurança da informação.
- Analisar os problemas relacionados com a segurança de sistemas baseados em redes de computadores utilizando-se de um enfoque global, e não somente aquele tradicionalmente centrado em

problemas específicos. Espera-se assim obter uma análise mais consistente e confiável sob o ponto de vista estratégico da empresa.

- Realizar estudo de alguns dos principais problemas e soluções específicas na área de segurança de redes de computadores, levando-se em conta as diversas interações entre eles que determinam o comportamento global do sistema.
- Mostrar que o uso de redes sem fio apesar das diversas vulnerabilidades caso sejam configuradas corretamente e reforçadas com mecanismos de segurança e políticas adequadas, ainda são um grande atrativo para as empresas que necessitam desse tipo de redes de computadores.

1.4. RESULTADOS E CONTRIBUIÇÕES ESPERADAS

Como resultados deste trabalho esperam-se:

- Disponibilizar as conclusões sobre o uso de uma metodologia para o tratamento de problemas de segurança em redes de computadores sem fio e sistemas.
- Dominar o uso e avaliar a eficiência da ferramenta de simulação EASEL na análise de problemas de segurança de redes de computadores e principalmente em redes de computadores sem fio.
- Disponibilizar o uso de uma metodologia para o tratamento de problemas de segurança em redes de computadores e sistemas.
- Apesar de estar sendo proposto como um estudo de caso, o surgimento e a integração de recursos com suporte à conexões *sem fio* resultam em sérias implicações de segurança em um ambiente que já possui outros problemas dessa natureza. Pretende-se analisar com profundidade problemas e soluções nesse contexto.

1.5. ESTRUTURA DA DISSERTAÇÃO

A proposta descrita por este documento encontra-se organizada da seguinte forma:

- O capítulo 1 apresenta o contexto da pesquisa, os objetivos, a importância e as justificativas, os resultados e as contribuições.
- O capítulo 2 oferece uma visão geral sobre sistemas de informações, conceitos e tipos de redes de computadores, especialmente tecnologias para ambientes sem fio.
- O capítulo 3 discorre sobre segurança de redes e sistema de informação, demonstrando as formas de ataques e prevenções às redes de computadores, com especial atenção para redes sem fio.
- O capítulo 4 aborda o conceito de Sobrevivência e do Método do Cálculo da Vulnerabilidade Potencial que com a ferramenta de simulação EASEL, formam a base do trabalho a ser desenvolvido.
- O capítulo 5 descreve a *aplicação do Método do Cálculo da Vulnerabilidade Potencial* em cenários e situações hipotéticas, apresentando conclusões sobre a aplicação do Método, seus valores e a eficácia dos mecanismos de segurança adotados em cada caso.
- Finalmente, no capítulo 6 são apresentadas as conclusões deste trabalho, com atenção especial para a adequação e eficácia desta metodologia no estudo de segurança de sistemas baseados em redes sem fio.

2. SISTEMAS DE INFORMAÇÕES E REDES

A Tecnologia da Informação representa o mais importante instrumento de transformação para os processos de negócios das empresas, visando aprimorá-los. O foco, porém não pode concentrar-se exclusivamente em T.I. Estudos nos anos 80 mostraram que o nível de produtividade por funcionário nas organizações americanas e européias nesse período aumentou apenas 1%; com esse resultado foi colocada em dúvida à eficácia da tecnologia na empresa.

O prêmio Nobel dos laboratórios Bell, Dr. Arno Penzias, afirma que há de fato, uma perda real em níveis de produtividade quando profissionais precisam trabalhar individualmente, isolados de seus colegas, por exemplo, utilizando microcomputadores não conectados a uma rede de computadores.

Constatou se que a raiz do problema de baixos níveis de produtividade dava se não pelos equipamentos e programas de computadores, mas sim em seu uso inadequado, impedindo todo o potencial dos benefícios que a empresa poderia ter.

Podemos perceber a rápida evolução no campo da informação, tecnologia, telecomunicações e somos a cada dia mais dependente desses recursos seja em casa ou na empresa. No clima de negócios altamente competitivo, hoje uma empresa que não esta informatizada praticamente está desperdiçando tempo e deixando de faturar mais que o esperado. Os principais serviços computacionais que as empresas utilizam ainda hoje são os sistemas empresariais integrados, conhecidos como Pacotes de ERP, o uso de correio eletrônico e a rede mundial de computadores, a Internet.

A facilidade que a informática trouxe para as empresas atualmente, permitiu expandir seus negócios, aumentar a produção e principalmente permitir a troca de informações entre suas filiais, fornecedores e clientes no tempo ideal. É possível ter o processo de armazenamento e transporte dessas informações

on-line, tornando as mais competitivas e permitindo que essas empresas cuidem basicamente de seus negócios.

A indústria de informática teve um progresso considerável em um curto período de tempo. Para ter uma diminuição nos custos operacionais, de uma melhor produtividade e de tornar-se competitiva, as empresas estão implantando ambientes de serviços baseados em Redes de Computadores.

Como afirma o professor Michael Porter, da Universidade de Harvard, [FERNANDES01] declarou o seguinte a respeito: “A importância da revolução pela informação não é devida à disputa que se impõe. A questão não é se a Tecnologia da Informação vai impactar de maneira marcante a posição de mercado de uma empresa; a questão é como podemos tirar vantagem da oportunidade? As organizações que anteciparem a força da Tecnologia da Informação terão os eventos sob controle, e aquelas que não o fizerem estarão fadadas a uma severa desvantagem competitiva”.

Nas seções seguintes são apresentados alguns conceitos básicos relacionados com a tecnologia de redes de computadores e normalmente utilizada no projeto e implementação de sistemas de informação corporativos.

2.1. REDES DE COMPUTADORES

A rede de computadores com o propósito de trocar informações e economizar recursos dá lugar a um novo ambiente muito mais complexo. A importância da Internet nos negócios e a globalização resultam em trocas de informações técnicas, comerciais e financeiras por meio de redes integradas entre empresas matrizes, filiais, fornecedores e parceiros comerciais [NAKAMURA02].

As informações agora são primordiais para o sucesso das negociações. Com isso o grau de proteção e preocupação com estas informações cresceu consideravelmente dentro deste ambiente integrado. Medidas e cuidados de segurança devem ser tomados e sempre verificados. A informática deixa de ser

uma ferramenta para se tornar um dos elementos principais na organização e na metodologia dos negócios, definindo modelos e características de organizações, fluxo e segurança de informações e tecnologias aplicáveis na gestão dos negócios.

A plataforma de *hardware* dominante antigamente baseava-se em *mainframes* (computadores de grande porte). As mudanças no ambiente de negócio têm forçado as empresas a buscar por mudanças correspondentes na plataforma da Tecnologia da Informação. Ocorreu-se bastante substituição dos mainframes por serviços de redes.

As redes prevêem a descentralização dos recursos, evitando a total dependência de componentes centralizados, reforçando a confiabilidade e a tolerância à falhas, adaptando as aplicações aos seus ambientes mais apropriados de *software, hardware* e necessidades pessoais.

Gerenciamento de redes centralizadas tem mostrado inadequado para o gerenciamento eficiente de grandes redes heterogêneas. Como conseqüência, diversas abordagens distribuídas tem sido adaptada para superar o problema segundo [KAHANI]. Segundo [ZHANG], uma rede para sobreviver, deve ser heterogênea já que uma rede homogênea é vulnerável a ataques maliciosos que exploram uma fraqueza em comum para todos os componentes.

Na década 80 era utilizado o famoso “terminal burro”, as redes ganharam popularidade a partir da década 90 onde os computadores pessoais passaram a oferecer uma grande vantagem competitiva de preço/desempenho em relação aos mainframes. O que grandes pensadores viam como a possibilidade interessante de um dia a rede oferecer, hoje pode dizer que esses serviços estão disponíveis para um usuário em sua casa. Emprega-se o uso em:

- Instituições Financeiras;
- Jornais, Revistas e Diversas Publicações digitais;
- Uso de Correio Eletrônico;

- Acesso à internet, WWW.
- Realização de Videoconferência;
- Newsgroups Mundiais;
- Outros.

Pode se considerar que praticamente todas as empresas utilizam um ou mais computadores e a grande maioria destas empresas necessitam compartilhar recursos, seja uma impressora, troca de arquivos, uso de uma aplicação web, uso de um sistema, uso de Internet, enfim, estamos dizendo que essas empresas possuem redes de computadores. As redes de computadores permitem:

- Aumentar a confiabilidade do sistema, pois Existem fontes alternativas de fornecimento – Redundância;
- Investimento reduzido em relação ao grande porte. O custo inicial de um projeto de redes depende muito do tipo de rede e o que espera dela. Um projeto simples de grande porte é várias vezes mais caro que a arquitetura utilizada hoje;
- Escalabilidade possibilita de acordo com as necessidades do desempenho do sistema, adicionar recursos sem a necessidade de substituir toda a linha estrutura existente.

A SUN Microsystems foi uma das primeiras empresas engajadas na divulgação e viabilização das funcionalidades oferecidas no contexto dos serviços baseados em redes de computadores, provando que o emprego correta da tecnologia pode alterar a natureza da concorrência de modo inesperado.

Uma arquitetura de rede padronizada e eficiente é fundamental para ter um serviço de rede com qualidade. O número de usuários e as complexidades das aplicações são fundamentais para a determinação do nível de funcionalidade e também do custo de implementação da infra-estrutura de suporte para uma rede.

2.2. TIPOS DE REDES

Existem diversos tipos de redes de computadores, mas a que a torna uma rede diferente da outra não esta simplesmente no tamanho e nem na quantidade de micros nela, mas sim em suas características. Hoje podemos citar que existem 4 tipos de redes e que apesar de classificação diferenciada, trabalham para ter o mesmo objetivo e resultado, o de compartilhar recursos e permitir a troca de informações entre os computadores configurados para nesse ambiente. A importância dessas classificações reside no fato de que o tamanho de uma rede influencia decisivamente na tecnologia de sua implementação, uma vez que os dados levam para se propagar de uma ponta a outra da rede é um dos fatores-chave a ser considerados.

2.2.1. REDE LOCAL

As conhecidas Redes Locais (Local Área Networks - LAN) surgiram dos ambientes de institutos de pesquisa e universidades. E graças as mudanças do enfoque dos sistemas de computação que levaram em direção à distribuição do poder computacional, as Redes Locais surgiram, assim, para viabilizar a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software) preservando a independência das várias estações de processamento e permitindo a integração em ambientes de trabalho cooperativo.

Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região e essas redes são em geral de propriedade privada.

As LANs aceitam diversas topologias, as mais utilizadas são Barramento, Anel e Estrela. Para gerenciar o envio e o recebimento dos pacotes de informações entre os computadores as LANs utilizam o padrão IEEE 802.3 conhecido como Ethernet.

2.2.2. REDE METROPOLITANA

A MAN (Metropolitan Area Network) é uma rede baseada em qualquer uma das novas tecnologias de rede, que opera em altas velocidades (até vários Gbps) e que se estende por distancias grandes o bastante para envolver uma região metropolitana. Exemplo de uma empresa que possui duas unidades na mesma cidade. Esses tipos de rede são capazes de transportarem dados e voz e utilizam o padrão IEEE 802.6

2.2.3. REDE DE LONGA DISTÂNCIA

WAN (Wide Area Network) Utiliza qualquer tecnologia de rede física capaz de se espalhar por grandes distâncias, abrange uma área geográfica maior, muito utilizada entre países e ou continente.

Um aspecto interessante, ligado à história do desenvolvimento das redes, é que o termo “rede geograficamente distribuída” não foi usado para caracterizar as primeiras redes implementadas, pois não havia redes de outros tamanhos. Nessa época os computadores eram muitos raros e caros, e não havia necessidade de se pensar em conectar computadores em rede locais – só havia um computador por área. Somente quando os computadores começaram a proliferar surgiu a necessidade das LANs, e o termo WAN foi então introduzido para descrever as redes muitos grandes que ligavam computadores geograficamente distantes.

2.2.4. REDES SEM FIO

Quando se fala em redes sem fio, inúmeras tecnologias estão incluídas nessa categoria de redes de computadores. A ênfase deste trabalho recairá sempre relacionada ao padrão 802.11, conhecido genericamente como Wi-Fi e aos diversos padrões de uso em redes sem fio definidos pelo Institute of Electrical and Electronics Engineers (IEEE).

Em 1990 o IEEE criou um grupo para desenvolver o protocolo 802.11. O objetivo era criar um padrão para redes sem fio locais (WLAN)., também conhecida como **Wi-Fi,** o padrão estava especificado para operar na freqüência de 2.4GHz.

As Redes Locais Sem Fio (Wireless Local Area Networks -WLANs) já são populares nos dias de hoje. A pesquisa de mercado do IDC de novembro de 2001, mostra que são fabricados 3 milhões de componentes para WLANs por trimestre. Para o Yankee Group, as WLANs substituirão as redes com fio que temos hoje, por causa de sua flexibilidade e o Retorno de Investimento que oferecem, através da redução de custos de implementação e suporte, além do ganho de produtividade. Conforme o relatório publicado em julho de 2003, o número de implementações de redes sem fio nos Estados Unidos duplicou nos últimos 12 meses e estão atualmente em uso cerca de 1.000.000 de Access Points em 700.000 empresas nos EUA. De acordo com o Gartner Group, em 2005 existia cerca de 137 milhões de usuários de redes sem fio, a maioria em empresas. [MMARTINS03].

São uma boa solução para várias ambientes e diversas situações, destacam-se o escritório portátil. Exemplo, Um prédio onde não é permitida a passagem de cabeamento. Não é necessário o uso de cabeamento para essa rede, isso torna a principal vantagem da sem fio. A desvantagem esta na taxa de transferência que é de 11 Mbps e 54 Mbps.

O uso de Redes Sem fio permitiu a expansão de assuntos envolvidos com a mesma. Exemplo de Segurança, Novos Equipamentos, Criptografia, etc. Muito utilizado em muitos lugares, mas existe pelo menos uma pessoa que tem uma opinião contrária da funcionalidade dessa rede, Bob Metcalfe, o inventor da Ethernet disse: “Os computadores sem fio móveis são como banheiros móveis sem tubulação – verdadeiros penicos portáteis. Eles serão cada vez mais comuns em veículos, construções e em shows de Rock. Para mim, as pessoas devem instalar a fiação necessária em suas casas e ficarem lá”.

As WLANs oferecem as organizações uma maior produtividade por empregado, oferecendo conectividade permanente às redes tradicionais, em locais onde antes não havia disponibilidade.

Não há nada de novo no conceito de comunicação sem fio digital. Em 1901, o físico italiano Guglielmo Marconi demonstrou como funcionava um telegrafo sem fio que transmitia informações de um navio para o litoral por meio de código Morse. Os modernos sistemas de sem fio digitais têm um desempenho melhor, mas a idéia básica é a mesma.

Fatores externos ocasionam muito mais interferência nas redes sem fio que as redes convencionais. Tal situação acontece, obviamente, por não existir proteção em relação ao meio por onde as informações trafegam. A informação não dispõe de nenhuma proteção física, mas por outro lado, pode atingir, sem muito esforço, locais de difícil acesso para redes cabeadas.

Os principais fundamentos de redes sem fio são:

- **Freqüências**
    - Sinais de radiofreqüência são utilizados pelos mais variados tipos de serviços, que vão desde as infra-estruturas comerciais (estações de rádio e TVs, operadoras de telefonia móvel e etc). Porém a maioria das faixas destinadas a cada um desses serviços não é padronizada internacionalmente. Quando falamos de freqüências de rádio, temos em mente que um sinal será propagado no espaço por alguns centímetros ou por vários quilômetros. À distância percorrida está diretamente ligada às freqüências do sinal. Em tese, quanto mais alta a freqüência, menor será a distância alcançada.
- **Canais**
    - O espectro de radiofreqüência é dividido em faixas, que são intervalos reservados, normalmente, para um determinado tipo

de serviço, definido por convenções internacionais e ou agências reguladoras. Uma faixa é, em geral, subdividida em freqüências menores, para permitir a transmissão em paralelo de sinais diferentes em cada uma delas. Essas freqüências menores são chamadas de canais.

- **Spread Spectrum**
    - Essa tecnologia, originalmente desenvolvida para uso militar, distribui o sinal através de toda a faixa de freqüência de maneira uniforme. Consome mais banda, porém garante maior integridade ao trafego das informações e está muito menos sujeita a ruídos e interferências que outras tecnologias que utilizam freqüência fixa predeterminada, já que um ruído em uma determinada freqüência ira afetar apenas a transmissão nessa freqüência e não na faixa inteira. Esse é o padrão de comunicação para todos os tipos de redes sem fio atuais.
- **Frequency-Hopping Spread-Spectrum (FHSS)**
    - Neste modelo, a banda 2,4 GHz é dividida em 75 canais, e a informação é enviada utilizando todos esses canais numa seqüência pseudo-aleatória, em que a freqüência de transmissão dentro da faixa vai sendo alterada em saltos. Essa seqüência segue um padrão conhecido pelo transmissor e pelo receptor, que uma vez sincronizados, estabelecem um canal lógico. O sinal é recebido por quem conhece a seqüência de saltos e aparece como ruído para outros possíveis receptores. Com essa técnica, limita-se a velocidade de transmissão a 2 Mbps, já que todo o espectro é utilizado e as mudanças de canais constantes causam grande retardo na transmissão do sinal.

- **Direct Sequence Spread Spectrum (DSSS)**
    - Utiliza uma técnica denominada code chips, que consiste em separar cada bit de dados em 11 subbits, que são enviados de forma redundante por um mesmo canal em diferentes freqüências e a banda 2,4 GHz é dividida em três canais.
- **Orthogonal Frequency Division Multiplexing/Modulation (OFDM)**
    - Trata-se de outro tipo de modo de transmissão (mais eficiente) utilizado não somente por equipamentos sem fio, mas também por redes cabeadas, como ADSL, cujas características do sinal e isolamento de interferências podem também ser bem aproveitadas. A maioria dos padrões atuais de redes sem fio adota esse modo de transmissão, principalmente por sua capacidade de identificar interferências e ruídos, permitindo troca ou isolamento de uma faixa de freqüência, ou mudar a velocidade de transmissão.
- **Bandas de radiofreqüência públicas**
    - Seguindo-se convenções internacionais há pelo menos três diferentes segmentos de radiofreqüência que podem ser usados sem a necessidade de obter licença da agência reguladora governamental (Anatel). Esses segmentos foram reservados a uso industrial, cientifico e médico, portanto podem ser utilizados de maneira irrestrita por qualquer aplicação que se adapte a uma dessas categorias. As freqüências disponíveis em cada uma das três faixas são:
        - 902 – 928 MHz;
        - 2.4 – 2,485 GHz (2,4 a 2,5 GHz no Brasil);
        - 5,150 – 5,825 GHz.

- **Freqüência 2,4 GHz**
    - Faixa de freqüência utilizada por uma vasta quantidade de equipamentos e serviços, por isso se diz que é poluída ou suja, por ser usadas por telefone sem fio, Bluetooth, forno de microondas e pelos padrões 802.11b e 802.11g.
- **Freqüência 5 GHz**
    - No Brasil a a faixa de 5,725 – 5,825 GHz está alocada para uso militar, o que atualmente restringe a comercialização de produtos que se utilizam dela.
- **Freqüências licenciadas**
    - Algumas soluções de redes sem fio optam por utilizar faixas de radiofreqüências menos sujeitas à interferência e, principalmente, que tenham maior alcance. Para utilizar essas aplicações, o fornecedor da solução deve requerer da agência reguladora autorização e normalmente, pagar uma taxa de atualização. O padrão 802.16a (WiMax), por exemplo, utiliza a faixa de 2 a 11 GHz e pode atingir 50 km a uma velocidade de 10 a 70 Mb.

Alguns conceitos são restritos às redes sem fio, e outros são adaptados das redes convencionais cabeadas. Essas redes relacionam-se às camadas mais próximas do hardware, ou seja, 2 e 3 no modelo de referencia OSI.

Numa rede baseada em contenção não existe uma ordem de acesso e nada impede que dois ou mais nós transmitam simultaneamente provocando uma colisão, o que acarretará, geralmente, a perda das mensagens. A estratégia de controle de contenção vai depender da habilidade que uma estação tem para a detecção de colisão e retransmissão da mensagem. Se assumirmos que o tráfego da rede consome apenas uma pequena porcentagem da vazão

máxima, o número de colisões e retransmissões será pequeno e o protocolo, bastante eficiente.

E as principais características de alguns conceitos às redes sem fio, muitas vezes adaptadas das redes convencionais cabeadas e outros próprios das redes sem fio são:

- **Carrier Sense Multiple Access (CSMA)** – Como a Slotted-Aloha, está técnica vai também sincronizar os quadros em colisão fazendo com que se superponham desde o início, mas não o fará pela divisão do tempo em intervalos. Além disso, e principalmente, esse método de acesso vai tentar ao máximo evitar a colisão e em algumas de suas variantes, detectarem quadros colididos em tempo de transmissão abortando-a, fazendo com que os quadros colidam durante o menor tempo possível, aumentando assim a eficiência na utilização da capacidade do canal. Quando deseja transmitir, a estação "ouve" antes o meio para saber se existe alguma transmissão em progresso. Se na escuta ninguém controla o meio, a estação pode transmitir, em caso contrário, a estação espera por um período de tempo e tenta novamente.

- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –** Depois de cada transmissão com ou sem colisão, a rede entra em um modo onde as estações só podem começar a transmitir em intervalos de tempo a elas pré-alocados. Ao findar uma transmissão, a estação alocada ao primeiro intervalo tem o direito de transmitir sem probabilidade de colisão. Se não o faz, o direito passa à estação alocada ao segundo intervalo e assim sucessivamente até que ocorra uma transmissão, quando todo o processo se reinicia. Se todos os intervalos não são utilizados, a rede entra então no estado onde um método CSMA comum é utilizado para acesso, podendo ocorrer colisões.

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD) –** Um dos motivos da ineficiência das técnicas Aloha e

CSMAs anteriores é o fato de um quadro inteiro ser transmitido mesmo que tenha colidido com um outro. Para quadros de grande tamanho, comparado com o tempo de propagação de ida e volta, a ineficiência na utilização da capacidade do meio é considerável. Nesse método a detecção de colisão é realizada durante a transmissão. Ao transmitir, um nó fica o tempo todo escutando o meio e, notando uma colisão, aborta a transmissão. Detectada a colisão, a estação espera por um tempo para tentar a retransmissão. Devido ao fato de o tempo de propagação no meio ser finito, para que possa haver a detecção de colisão por todas as estações transmissoras, um quadro vai ter de possuir um tamanho mínimo.

- **Extended Service Set Identifier (ESSID)** – Apresentado o método de acesso anteriormente, nas redes sem fio temos o ESSID, também conhecido como o "nome da rede", é a cadeia que deve ser conhecida tanto pelo concentrador, ou grupo de concentradores, como pelos clientes que desejam conexão. Em geral, o concentrador envia sinais com ESSID, que é detectado pelos equipamentos na região de abrangência, fazendo com que estes enviem um pedido de conexão. Quando os concentradores não enviam seu ESSID de forma gratuita, os clientes devem conhecer os ESSIDs dos concentradores e informar manualmente, para requer a conexão.

- **BEACON** – Concentradores que enviam sinais informando sobre sua existência, para que clientes que estejam procurando por uma rede por detectarem a percebem "farejam" sua presença e estabeleçam corretamente conexão com um determinado concentrador. Entretanto essas características podem não existir em alguns concentradores, já que é facilmente configurável e em alguns casos de segurança que veremos no próximo capítulo, é recomendado ser desabilitado.

- **Meio compartilhado** – Na rede sem fio o meio é compartilhado entre todas as estações conectadas a um mesmo concentrador. Ou seja, quanto maior o número de usuários, menor será a banda disponível para cada um deles, fazendo com que o tráfego fique visível para

todas as interfaces participantes. Portanto, de forma similar às redes cabeadas, uma estação pode capturar o trafego não originado em si ou que lhe é destinado. Um atacante não precisa estar presente fisicamente ou ter acesso a um equipamento da rede alvo. Como o meio de transporte é o próprio ar, basta que um atacante esteja na área de abrangência do sinal. A tecnologia mais difundida para redes sem fio é o padrão *Spread Spectrum*, desenvolvido para uso militar, tendo como características de projeto a segurança e o uso em comunicações em situações adversas. O uso de rádio transmissão faz com que o equipamento receptor tenha que conhecer a exata freqüência da unidade transmissora para que a comunicação seja estabelecida corretamente. O padrão 802.11 define modos distintos de operação, estudaremos o Ad-Hoc e o modo de Infra-estrutura.

2.2.4.1. AD-HOC

Funciona na forma de abstração de um ponto central de conexão. Também conhecida como “Configuração de um serviço básico independente” (IBSS). Os equipamentos conectam-se diretamente uns aos outros sem a necessidade de utilização de um Access Point (AP) conforme representa a Figura 1. Este é o padrão da maioria dos cartões sem fio. Devemos enfatizar que a ausência do concentrador cria vários problemas de segurança, administração e gerência de rede. Contudo, pode resolver questões pontuais, como acesso momentâneo para troca de arquivos ou permitir a comunicação rápida entre os equipamentos de sem fio.

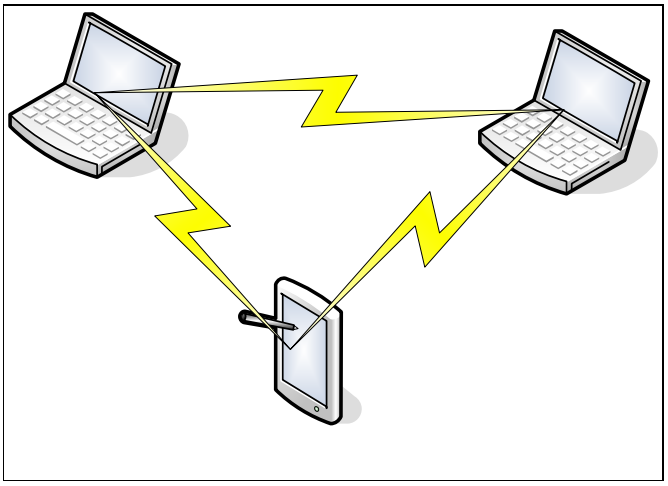

FIGURA 1: TOPOLOGIA DE REDE NO MODELO AD-HOC

2.2.4.2. INFRA-ESTRUTURA

O concentrador é o equipamento central de uma rede que se utiliza dessa topologia. Apenas o Ponto de Acesso ou um roteador será rodeado de diversos clientes, (ilustrado pela Figura 2) e fazendo com que toda as configurações de seguranças sejam concentradas e aplicadas aos clientes, possibilitando um melhor controle de todos os itens (autorização, autenticação, controle de banda, filtros de pacote, criptografia etc.). As conexões são iniciadas enviando um identificador (SSID). Na Infra-estrutura as chaves secretas são manualmente configuradas no AP (Access Point) e nos clientes de rede sem fio (não é escalável).

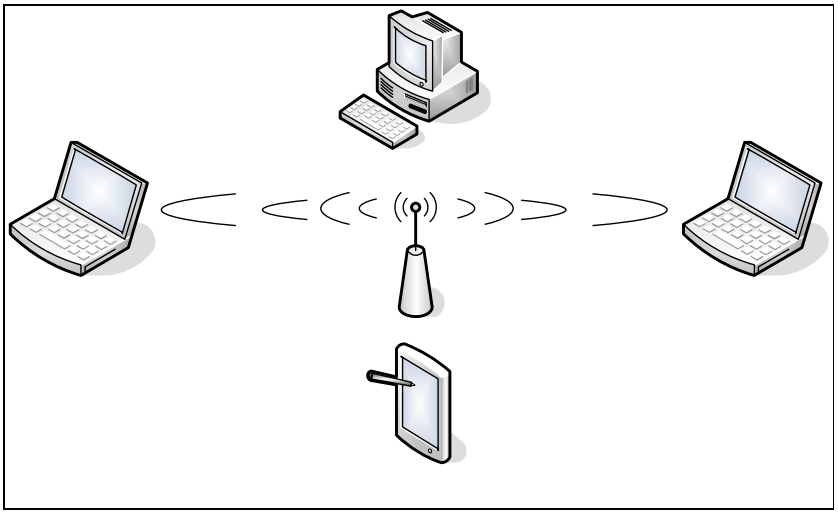

FIGURA 2: TOPOLOGIA DE REDE NO MODELO INFRA-ESTRUTURA.

As WLANs estão classificadas pelo comitê de acordo com uma nomenclatura e a sua funcionalidade. A diversos padrões de redes sem fio, entre eles:

- 802.11 – O padrão original WLAN. Suporte de 1 à 2 Mbps;
- 802.11a – WLAN de alta velocidade padronizado para operar na faixa de 5 GHz e taxa de dados de 54 Mbps;
- 802.11b – WLAN padrão para faixa de 2.4GHz e suporte para taxa de dados de 11 Mbps;
- 802.11c - Especificação para operar com IEEE 802.11 MAC's.
- 802.11d - Especificação para Telecomunicações e troca de informações entre dois sistemas.
- 802.11e - Suporte para aplicações que precisam de QoS.
- 802.11f - Recomendação para redes ponto a ponto sob protocolo IAP (Inter Access Point).
- 802.11g - Padrão para tráfego na taxa de 54 Mbps em freqüência de 2.4 GHz.

- 802.11h - Gerenciamento do espectro na faixa de 5 GHz usado na Europa e Ásia. Requer equipamentos para verificar as freqüências utilizadas na transmissão.
- 802.11i – Este padrão abrange 802.1X, TKIP e protocolos AES. Melhoria na segurança para protocolos de autenticação e segurança. Trabalhando para troca do padrão WEP.
- 802.1X (não 802.11X) – Melhoria na segurança do padrão 802.11, definindo o modo que os usuários irão se autenticar em redes locais sem fio (WLAN).

Entre os diversos padrões 802.11 para tecnologia de LAN sem fio, destacam-se os, 802.11b, 802.11a e 802.11g. Os três padrões 802.11 compartilham muitas características, ou seja, todos usam o mesmo protocolo de acesso ao meio, CSMA/CA; também usam a mesma estrutura de quadro para seus quadros de camada de enlace; todos têm a capacidade de reduzir sua taxa de transmissão para alcançar distâncias maiores e operam em modo “modo de infra-estrutura” e “modo ad hoc”.

Nesse trabalho pode ser aplicado no padrão 802.11b e 802.11g e a seguir são apresentados detalhes desses padrões.

2.2.4.3. PADRÃO 802.11B

O primeiro sub padrão a ser definido permite 11 Mbps de velocidade de transmissão máxima, porém pode comunicar-se a velocidades mais baixas, como 5,5,2 ou mesmo 1 Mbps. Opera na freqüência de 2,4 GHz e usa somente DSSS. Permite um número máximo de 32 clientes conectados. Foi ratificado em 1999 e definiu padrões de interoperabilidade bastante semelhante aos da rede Ethernet. Essa especificação afeta somente a camada física, adicionando altas taxas de dados e conectividade mais robusta. [3Com00]

Também conhecida como Wi-Fi, ou para a tecnologia da Apple, AirPort o padrão 802.11b foi tremendamente bem-sucedido e empresas venderam milhões de dispositivos que o suportavam. [ENGST05]

Há limitação em termos de utilização de canais, e possui a desvantagem da velocidade de transmissão máxima que no 802.11g, é de 54 Mbps, mas ainda hoje é o padrão mais popular e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis.

2.2.4.4. PADRÃO 802.11G

O padrão IEEE 802.11g é baseado na tecnologia *Direct Sequence Spread Spect rum (DSSS)* que usa transmissão aberta (broadcast) de rádio e opera na freqüência de 2.4 a 2.485 GHz com uma capacidade de transferência de até 54 Mbps, em ambientes abertos (~ 450 metros) ou fechados (~ 50 metros). Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no quais as ondas estão se propagando (paredes, interferências, etc). Por ser uma transmissão aberta, qualquer pessoa com um receptor operando na mesma freqüência pode captar as ondas.

O padrão 802.11g originalmente suporta apenas dois tipos de autenticação do cliente de sem fio: *"open authentication"* e "*shared-key authentication"*. No primeiro modo o cliente necessita apenas fornecer o SSID *(Service Set Identifier)* correto para juntar-se à rede. No modo *"shared-key authentication"* é preciso o conhecimento de uma chave WEP *(Wired Equivalent Privacy)* para que isso ocorra. É importante notar que essa autenticação é do dispositivo da sem fio, e não dos usuários da rede. Estaremos tratando especificamente de WEP no capitulo de Segurança.

O padrão 802.11 define o protocolo WEP como mecanismo para cifrar o tráfego entre os APs e os clientes da sem fio. Essa cifragem ocorre na camada de enlace e exige que todos os participantes compartilhem a mesma chave WEP estática.

Este padrão é mais recente que os padrões 802.11b e 802.11a e pelo fato de o 802.11g operar na mesma faixa (2,4GHz) permite que os equipamentos de ambos os padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática do parque instalado.

3. SEGURANÇA DE SISTEMAS DE MISSÃO CRÍTICA

A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou organização.

Segundo [PUTTINI00], uma solução de segurança adequada deve satisfazer os seguintes princípios:

Confiabilidade: significa proteger informações contra sua revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.

Autenticidade: O controle de autenticidade está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos.

Integridade: A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo armazenada em discos ou fitas de backup. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada de mensagens (ex. tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade).

Disponibilidade: consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

Através da correta aplicação desses princípios, a segurança da informação pode trazer benefícios como: aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e, finalmente garantir a funcionalidade das aplicações críticas da empresa.

3.1. SEGURANÇA DE REDES SEM FIO

Devido à facilidade com que uma sem fio pode ser utilizada por pessoas não autorizadas e à facilidade com que se pode capturar o tráfego, é extremamente importante o uso de criptografia e de mecanismos de autenticação numa rede sem fio. Existem diversas formas de tentativa de invasão e de ataque. Este trabalho foi estruturado e serão apresentadas as formas de ataques e os principais métodos para prevenção e correção.

3.1.1. MECANISMOS DE SEGURANÇA

Estarão sendo apresentados e estudados separadamente alguns mecanismos de segurança disponíveis em redes sem fio. Existem diversas soluções proprietárias contendo funcionalidades que, em alguns casos, trarão um grau maior de segurança e confiança se forem aplicadas isoladamente em relação às soluções aqui descritas, entretanto não serão abordados nesse trabalho por não poderem ser aplicadas em ambientes heterogêneos, o que limita seu campo de atuação, inviabiliza soluções onde não se tem controle do ambiente completo (como quando o cliente usa o próprio equipamento, por exemplo) e pode comprometer o crescimento e ou a evolução do parque instalado, por depender de um único fabricante ou fornecedor.

3.1.1.1. ENDEREÇAMENTO MAC

Para um perfeito funcionamento de uma rede padrão Ethernet ou rede sem fio, cada equipamento necessita de uma placa de rede *(NIC)* que deverá ter um número único de identificação definido pelo fabricante *(MAC Address)* e controlado pelo *Institute of Eletrical and Eletronics Engineers (IEEE).* Esse número permite, teoricamente, identificar de forma inequívoca um equipamento em relação a qualquer outro fabricado mundialmente.

Uma das formas encontradas para restringir o acesso a uma determinada rede sem fio é mediante o cadastramento prévio dos dispositivos participantes. Como o endereço MAC identifica de forma única cada interface de rede, apenas os dispositivos cadastrados previamente terão acesso permitido. Esse mecanismo exigirá sempre alguma manutenção, que será maior ou menor, de acordo com o fluxo de usuários e interfaces que entra e sai do cadastro, pórem não deixa de ser uma boa solução para pequenas redes e ambientes com poucas mudanças. Lembrando que esse tipo de autenticação permite a identificação do equipamento e não do usuário.

No entanto, alguns modelos de placas antigas permitiam usar um software fornecido pelo fabricante que permitia cadastrar um MAC e ainda, hoje existem técnicas e ferramentas para se apropriar de um endereço MAC de outra placa

ou simplesmente fazer uso de outro que não o original de fábrica. Estaremos apresentando algumas destas ferramentas nesse trabalho.

O endereço MAC é facilmente obtido na maior parte dos equipamentos com a interface de rede. Em sistemas Windows NT, 2000, XP ou 2003, poderia usar o comando ***ipconfig*** conforme apresentado na Figura 3. Onde a linha Physical Address indica o endereço MAC dessa interface e em sistemas Linux, pode ser usado o comando ***ifconfig*** para a mesma função..

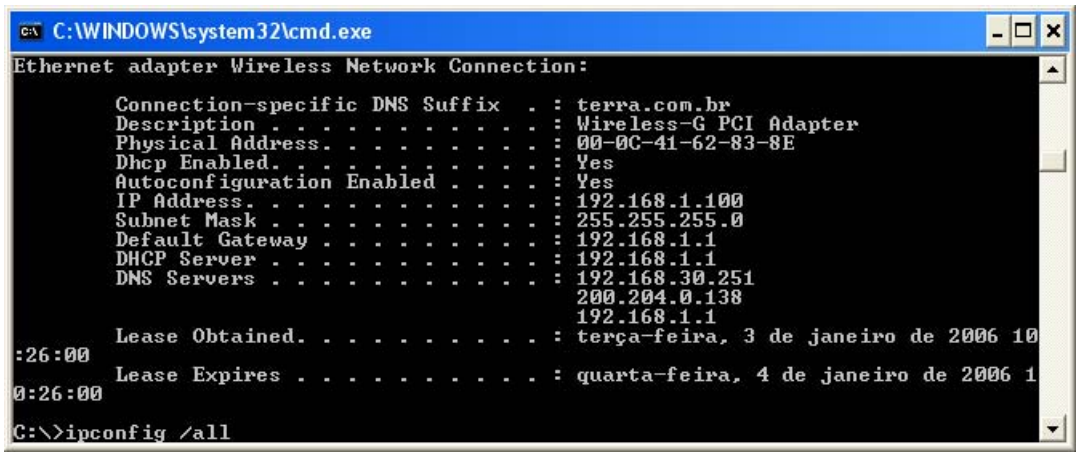

FIGURA 3: INTERFACE DO PROMPT DO COMANDO DO MS-DOS

3.1.1.2. WIRED EQUIVALENT PRIVACY (WEP)

Devido à facilidade com que uma rede sem fio pode ser utilizada por pessoas não autorizadas e à facilidade com que se pode capturar o tráfego, é extremamente importante o uso de criptografia e de mecanismos de autenticação numa rede sem fio.

O padrão 802.11 define o protocolo WEP como mecanismo para cifrar o tráfego entre os APs e os clientes sem fios. Essa cifragem ocorre na camada de enlace e exige que todos os participantes compartilhem a mesma chave WEP estática.

A segurança do WEP é composta de dois elementos básicos: uma chave estática, que deve ser a mesma em todos os equipamentos da rede, e um componente dinâmico, que eles juntos irão formar a chave usada para cifrar o

trafego. O protocolo não definiu a forma que essa chave deverá ser distribuída, a maneira convencional é também a mais trabalhosa, é a de cadastrar manualmente a chave em todos os equipamentos.

Após o estabelecimento de conexão, essa chave estática sofre uma operação matemática para gerar quatro novas chaves: uma destas será escolhida para cifrar as informações em transito. Essa chave será fixa e somente trocada se a chave estática original mudar.

Para aumentar a segurança de sua rede sem fio deve-se escolher o maior tamanho de chave WEP possível, sendo essencial trocar as chaves WEP que venham nas configurações padrão dos equipamentos. O uso de criptografia nas aplicações, como SSH e SSL, também são recomendáveis para minimizar os riscos de escuta não autorizada. Além disso, também deve ser considerado o uso de criptografia no próprio TCP/IP, como IPsec e o uso de VPNs em geral.

O WEP possui diversas fragilidades, mas apesar disso seu uso é recomendável e deve ser encarado como uma camada adicional de segurança.

Salvo algumas extensões implementadas por alguns fabricantes, o protocolo 802.11 original apresenta alguns problemas:

- Fragilidade do protocolo WEP;
- Problemas de gerenciamento das chaves WEP, que devem ser trocadas manualmente;
- Falta de autenticação dos usuários da rede.

Existem várias iniciativas para a criação de novos padrões que aperfeiçoem a segurança do protocolo, sendo recomendável que sejam utilizados assim que estiverem disponíveis. Entre eles, pode-se citar:

- IEEE 802.1x, que suporta autenticação e distribuição de chaves através da consulta a um servidor de autenticação;

- WAP (Wi-Fi Protected Access), desenvolvido em conjunto pela Wi-Fi Alliance e IEEE, que provê algumas melhorias criptográficas, como o uso do protocolo TKIP (Temporal Key Integrity Protocol). Também provê suporte para autenticação de usuários via 802.1x e EAP (Extensible Authentication Protocol);

- IEEE 802.11i, sendo desenvolvido pelo IEEE 802.11 Task Group i (TGi), que inclui uma nova versão de WEP utilizando AES (Advanced Encryption Standard), além da definição de um framework de distribuição de chaves.

Na Figura 4 é o exemplo de uma tela de configuração do WEP em um Ponto de Acesso. No Ponto de Acesso foi definida a palavra ***Chave*** como a frase e conforme o cálculo matemático presente no protocolo, gerou-se as 4 chaves. Após isso é só digitar esse valor da chave gerado nas estações que tentarem se conectar a está sem fio quando for solicitada.

O protocolo sugerido, o WEP, que hoje está presente em todos os produtos e que está em conformidade com o padrão **Wi-Fi.**

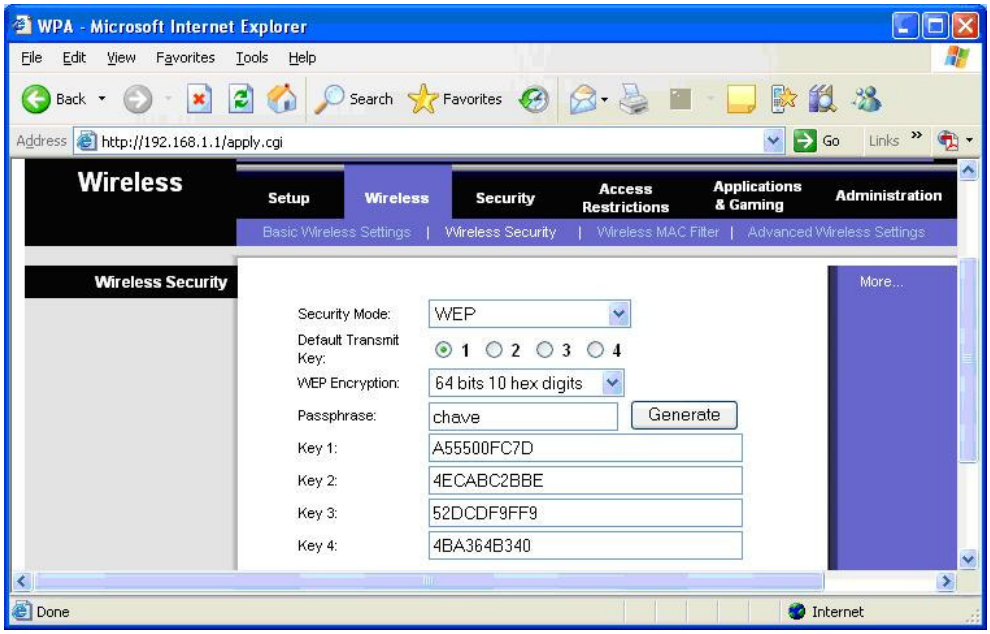

FIGURA 4:INTERFACE DE CONFIGURAÇÃO DO WEP DE UM ROTEADOR SEM FIO

3.1.1.3. WI-FI PROTECTED ACCESS (WPA)

Após as vulnerabilidades e fragilidades descobertas no WEP, o Wi-Fi Alliance adiantou a parte de autenticação e cifração do trabalho que estava sendo feito para o fechamento do padrão 802.11i e liberou o protocolo WPA. Foram diversos mudanças e avanços incorporados a esse protocolo, porem a maior parte das mudanças necessita a inclusão de outros elementos à infra-estrutura e ainda deve trabalhar combinados com outros protocolos, como o 802.1x. Esses mecanismos de proteção introduzidos no protocolo WAP não estão disponíveis para suportar conexões Ad-Hoc.

Atuando em duas áreas distintas: a primeira, que visa substituir completamente o WEP, trata da cifração dos dados objetivando garantir a privacidade das informações trafegadas, e a segunda, foca a autenticação do usuário (área não coberta efetivamente pelo padrão WEP) utiliza, para isso, padrões 802.1x e *EAP (Extensible Authentication Protocol).*

Todos esses itens abordados surgem devido a grande parte do problema de sigilo existente no WEP referente aos mecanismos de criptografia utilizados, destacando se: na forma de criptografia dos protocolos usados para cifrar as informações onde utilizam uma chave compartilhada previamente, a *Pre-shared Key ou WPA-PSK*, que pode trabalhar com o protocolo *TKIP (Temporal Key Integrity Protocol)* que é responsável por gerenciar as chaves temporárias usadas pelos equipamentos em comunicação e na **infra-estrutura** que exigirá um servidor de autenticação (RADIUS). Para finalizar, o EAP que permite integrar soluções de autenticação já conhecidas e testadas incluindo a possibilidade de certificação digital. Na Figura 5, um exemplo de configuração de Ponto de Acesso configurado com WPA e permitindo escolher entre TKIP ou AES.

FIGURA 5: CONFIGURAÇÃO DO WPA EM UM PONTO DE ACESSO

3.1.2. RISCOS E AMEAÇAS

Quais são os riscos e ameaças que as redes sem fio estão sujeitas? A seguir, listamos os principais riscos e ameaças encontradas nos dias de hoje.

3.1.2.1. PROBLEMAS DE SEGURANÇA FÍSICA

Administradores preocupam-se muito mais com a segurança lógica do que com a segurança física, porém se a segurança física é um importante componente de risco quando se trata de rede cabeadas, em redes sem fio esse aspecto é ainda mais relevante, visto que a área de abrangência "física" aumenta substancialmente. Aspectos antes irrelevantes (sob o aspecto de vista de performance e segurança), como posicionamento de determinados componentes de rede, agora devem ser cuidadosamente estudados, sob o risco de comprometer o bom funcionamento da rede e, principalmente, facilitar o acesso não autorizado e outros tipos de ataques.

Não se deve esquecer que antenas ou interfaces mais potentes ampliam a distância de recepção. Portanto, para garantir que o sinal não vai ser capturado a uma determinada distância, não é suficiente percorrer os limites da instalação para verificar até onde o sinal chega já que um atacante munido de uma interface de maior potência, ou de uma antena que lhe permita estar a uma distância tão grande deste limite quanto for à qualidade e potência da antena ou interface por ele utilizada, poderá receber sinal a uma distância não prevista pelos testes.

3.1.2.2. CONFIGURAÇÕES DE FÁBRICA (DEFAULT)

Os equipamentos possuem vários e diversos mecanismos de segurança, mas eles não vêm habilitados de fábrica e quando vêm com alguma configuração, essa configuração é padrão para todos os equipamentos de um mesmo fabricante conforme exemplo da Figura 6. Diante dessa padronização, esses equipamentos serão alvos fáceis de ataques se um administrador sem experiência em segurança de redes sem fio não alterar essa configuração ou instalar esse equipamento sem o mínimo de requisitos necessários para dificultar a invasão de exploração de Análise de Tráfego, uma invasão muito típica nessas redes.

Praticamente todos os equipamentos saem de fábrica com senhas de administração e endereço IP padrão. Caso não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede alvo e tenha condições de identificar todas as configurações feitas, podendo até mesma modificá-las. E não adianta o equipamento possuir suporte a WEP e se estes equipamentos venham com as chaves WEP configuradas e estas não sejam mudadas pelo administrador. Roteadores sem fio da Linksys modelo WRT54G, por exemplo, saem de fábrica com as seguintes configurações:

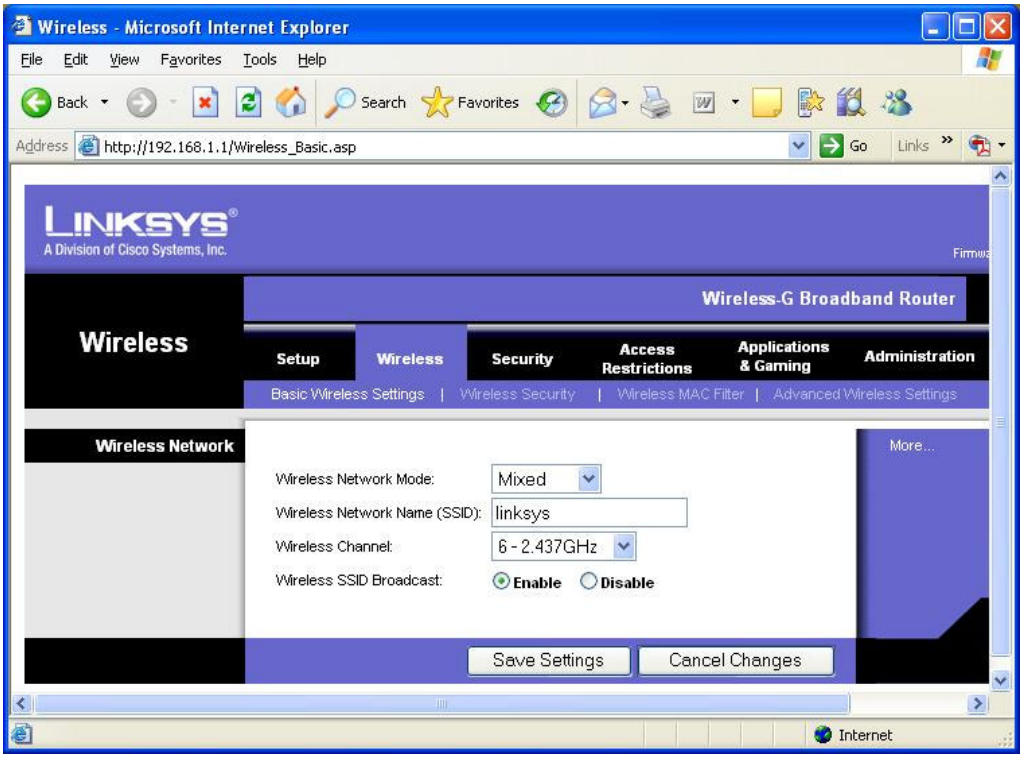

FIGURA 6: CONFIGURAÇÃO DO SSID EM UM PONTO DE ACESSO

3.1.2.3. ENVIO E RECEPÇÃO DE SINAL

Diferentemente das redes cabeadas, o posicionamento dos componentes pode ser determinante na qualidade da rede e na sua segurança. Essa característica é fácil de ser percebida quando se sabe que o sinal é enviado em varias direções, portanto um Ponto de Acesso colocado em uma parede enviará sinal tanto para dentro do ambiente quanto para fora deste, o que pode não ser o desejado pelo administrador. E quanto mais ao centro estiver o Ponto de Acesso melhor será o aproveitamento, pelas estações, do sinal irradiado por ele, conforme o exemplo da disposição dos equipamentos na Figura 7.

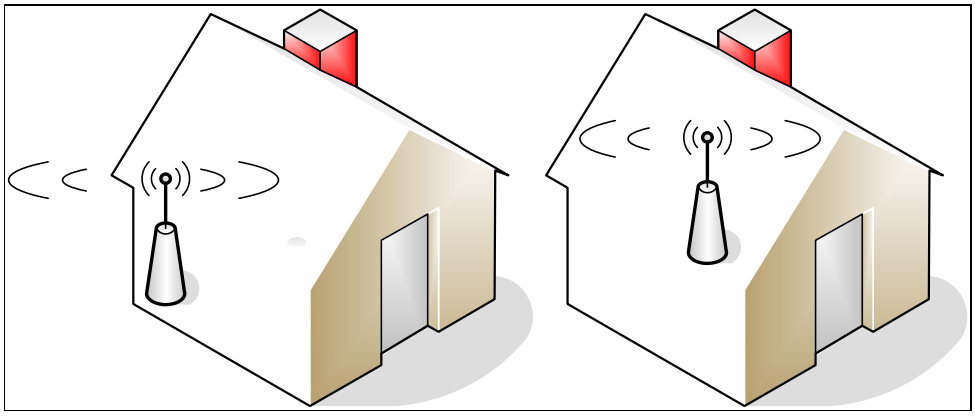

FIGURA 7: ILUSTRAÇÃO DO ALCANCE DE UM PONTO DE ACESSO

3.1.2.4. NEGAÇÃO DE SERVIÇO (DENIAL OF SERVICE DOS)

Ataque em que o atacante explora uma fraqueza ou limitação de design de um serviço de rede para sobrecarregar ou interromper o serviço, de modo que ele não fique disponível para uso. Geralmente, esse tipo de ataque é iniciado para impedir que outras pessoas usem um serviço de rede, como um servidor Web ou de arquivos.

Trata-se de um tipo de ataque que não necessita de acesso ou invasão à rede alvo, mas pode acarretar sérios transtornos dependendo da importância do ambiente envolvido. Verificou-se que dispositivos Bluetooth próximos a concentradores Wi-Fi, causam grande interferência, posteriormente essa constatação foi anunciada nos boletins de segurança divulgados pelo Grupo Cert identificando problemas dessa mesma natureza em rede 802.11b e 802.g em baixa velocidade (menos de 20 Mb). Essa característica de coexistência entre os padrões 802.11g e 802.11b abre uma possibilidade de ataque combinando ações, pois basta existir um dispositivo 802.11b em uma rede 802.11g para uma queda geral de performance (velocidade), o que permite a um atacante maliciosamente associar um dispositivo 802.11b em uma rede 802.11g para facilitar um ataque de negação de serviço.

3.1.2.5. MAPEAMENTO DO AMBIENTE

Uma das primeiras etapas realizadas pelo invasor é sem duvida elaborar um mapeamento do ambiente. Esse procedimento possibilita obter o maior numero de informações sobre uma terminada rede, permitindo conhecer detalhes que lhe permitam lançar ataques de forma mais precisa e com menos riscos de ser identificado. Tal ação pode ter maior ou menor grau de êxito, dependendo dos mecanismos de proteção existentes na rede.

A técnica “Wardriving” consiste em utilizar um equipamento portátil com a suporte a redes sem fio, e sair andando pela cidade em busca de Access Points. “Wardriving” surgiu da técnica “Wardialing” que consistia em discar um determinado grupo de números de telefone para ver qual deles respondia com um modem.

Especialistas usam o “Wardriving Kit” para descobrir quais as empresa que mantêm as suas redes abertas (sem segurança). Esses kits são bem simples e fácil de adquirir. Com estes equipamentos é possível detectar redes sem fio, capturar tráfego e até mesmo quebrar a criptografia WEP, obtendo acesso não autorizado aos dados transmitidos na WLAN. A Figura 8 mostra o “Phôphet Wardriving Kit” usado na décima Deefcon, durante a conferência sobre redes sem fio.

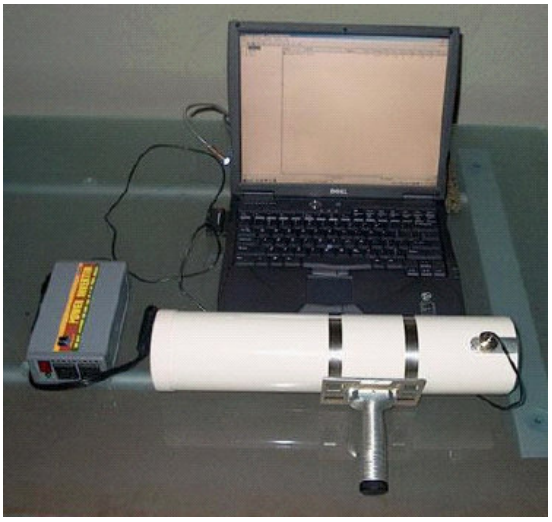

FIGURA 8: “PRÔPHET WARDRIVING KIT” FONTE: MODULO SECURITY

Com base nesses “passeios”, criou-se o hábito de registrar no prédio ou na calçada com o uso de giz o lugar onde é possível conseguir acesso sem fio. Esta prática recebeu o nome “Warchalking” (chalk significa giz), e é originária da língua dos “hobos” (vagabundos, na gíria inglesa) que, durante a grande depressão americana de 1929, buscavam lugares onde pudessem ser acolhidos e com marcas de giz, informavam os companheiros sobre as condições do lugar. A Figura 9 ilustra um exemplo de um local por onde passou esses especialistas e registrou o status da rede.

FIGURA 9: O RESULTADO DO “WARCHALKING” RISCADO NO CHÃO. .

Os símbolos vistos na figura acima, possuem significados diferentes. Com esses símbolos, fica visível e fácil de saber o status da segurança de uma rede de computadores sem fio de uma empresa. Todos esses dados estão a partir desse momento disponíveis para a comunidade de hacker para um futuro ataque. Veremos a seguir na Figura 10 a explicação para cada símbolo e como essas informações são difundidas de um hacker a outro.

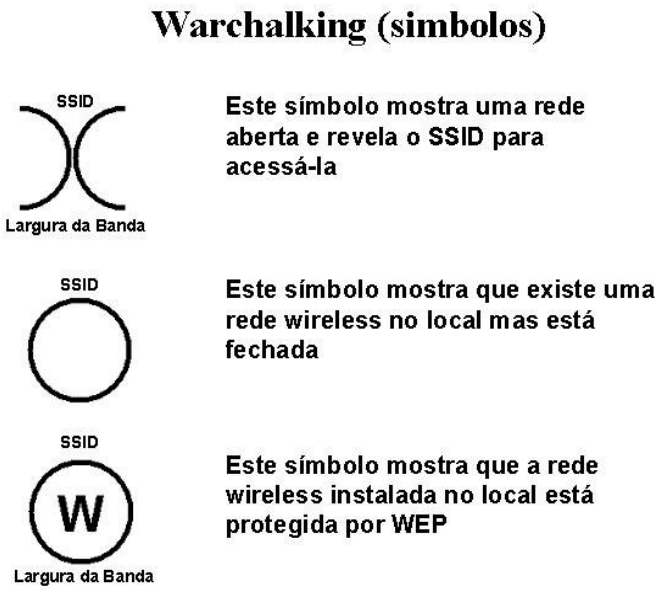

FIGURA 10: A SIMBOLOGIA.

Os hacker começaram a mapear todos os APs que foram descobertos sem segurança. O site http://mapserver.zhrodague.net oferece um serviço de mapeamento de APs em todo o mundo com o uso de GPS. Usuários que tem as informações no formato NetStumbler podem fazer upload. Existe outro mapa, feito no Microsoft MapPoint 2002 (Exemplo na Figura 11) que com o auxilio da ferramenta StumbVerter, disponível no endereço http://www.sonar-security.com, que importa os dados capturados pelo NetStumbler. O sinal vermelho na parte inferior da pirâmide significa WEP habilitado. [MMARTINS03].

FIGURA 11: PONTOS DE ACESSO DETECTADO NA REGIÃO DA CALIFÓRNIA.

3.1.2.6. CAPTURA DE TRÁFEGO

As ondas de radiofreqüência se propagam pelo ar e são passíveis de captura. Caso essas informações não estejam devidamente criptografadas, não somente o tráfego como seu conteúdo pode ser conhecido. Para isso basta que o invasor esteja na área de alcance com um computador ou laptop com ferramenta de captura de tráfego. Ferramentas tradicionais para escuta de tráfego em redes cabeadas podem ser utilizadas com poucas restrições, pois quase todas se utilizam de qualquer interface de rede, independentemente de serem para rede cabeadas ou sem fio.

Existem várias razões para que um invasor queira acessar a uma determinada rede, por outro lado há também possíveis vulnerabilidades a que um ambiente de rede pode estar exposto e permitir acessos não autorizados. Entre as formas de acessar, o invasor poderá encontrar um ambiente com a Configuração Aberta onde o Ponto de Acesso aceita conexão de qualquer dispositivo, portanto basta o invasor dispor de um equipamento e conectar-se no ambiente alvo, conseguindo muitas vezes o ip através da configuração

habilitada por meio de um servidor DHCP ou se não for possível obter automaticamente ele poderá utilizar escutas de tráfegos por meio de ferramentas tradicionais como o ***Tcpdump*** e ou ***Kismet***. Ou com a Configuração Fechada onde o SSID (Service Set IDentifier) não é enviado pelo Ponto de Acesso, portanto o invasor terá que promover uma escuta do tráfego para determinar o SSID correto para então, conectar-se ao Ponto de Acesso da sem fio. Ferramentas especificas para redes sem fio, como o Airsnort, Kismet ou BSD AirTools, permitem capturar os sinais e identificar o SSID dessas redes.

3.1.2.7. VULNERABILIDADE NOS PROTOCOLOS WEP E WPA

Existem problemas administrativos e técnicos em relação ao protocolo WEP. Em relação ao padrão original, os principais relacionam-se ao fato de usar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes de uma determinada rede. Portanto, caso seja necessária à troca da chave, o processo pode ser trabalhoso e, em alguns casos, inviável.

Sendo a única opção para aumento da segurança, o WEP caiu em descrédito quando foram publicadas maneiras de quebrar seu algoritmo. Outro problema é a dificuldade de distribuir as chaves e o seu armazenamento no cliente.

A despeito de o WPA ter características de segurança superiores às do WEP, ainda assim apresenta algumas vulnerabilidades já reportadas e que devem ser conhecidas para que o seu impacto possa ser minimizado. Entre essas vulnerabilidades destacam-se: O Uso de senhas pequenas ou de fácil adivinhação e o uso de diversas ferramentas como o WPA Crack, que de posse de um tráfego já capturado, permite ataques combinados usando um dicionário e técnicas de força bruta.

3.1.2.8. EQUIPAMENTOS SEM FIO EM AMBIENTES CABEADOS

Um grande risco é encontrado nesses equipamentos sem fio que podem permitir facilmente acesso externo de um segundo invasor, bastando apenas

habilitar a placa Wi-Fi para o modo Ad-Hoc e permitir o roteamento com a rede cabeada. O invasor pode ser tão sofisticado e utilizar de mecanismos com *NAT (Network Address Translation)*, escuta de pacotes (sniffer) e etc.

3.2. TÉCNICAS E FERRAMENTAS DE ATAQUE

Todas essas vulnerabilidades ou falta de conhecimento apresentadas podem ser facilmente exploradas com o auxílio de ferramentas e métodos que detalharemos a seguir. Portanto, para ter a completa dimensão dos desafios a serem encarados para criar e manter um ambiente sem fio seguro é fundamental decidir qual o equipamento ou ferramenta utilizar para uma varredura ou levantamento de sinal de uma área extensa.

3.2.1. FERRAMENTAS UTILIZADAS

Grande parte do mapeamento, captura de pacotes e ataques a redes sem fio podem ser realizados com ferramentas conhecidas em redes cabeadas, porém esses mesmos dados podem ser obtidos mais facilmente com ferramentas especializadas. Outras informações mais específicas como qualidade do sinal e demais características exclusivas de redes sem fio, só podem, obviamente, ser colhidas com ferramentas proprietárias.

A seguir serão descritas várias ferramentas para redes sem fio e as suas principais características para auxiliar no trabalho de detecção e invasão.

3.2.1.1. AIRTRAF

Airtaf permite coletar uma vasta quantidade de informações sobre as redes identificadas, tais como clientes conectados, serviços utilizados e várias totalizações, tudo em tempo real. Esses detalhes podem ser úteis a um invasor que procure, por endereço IPs da rede e endereço MAC de clientes conectados por exemplo. A figura 12 mostra a interface da ferramenta.

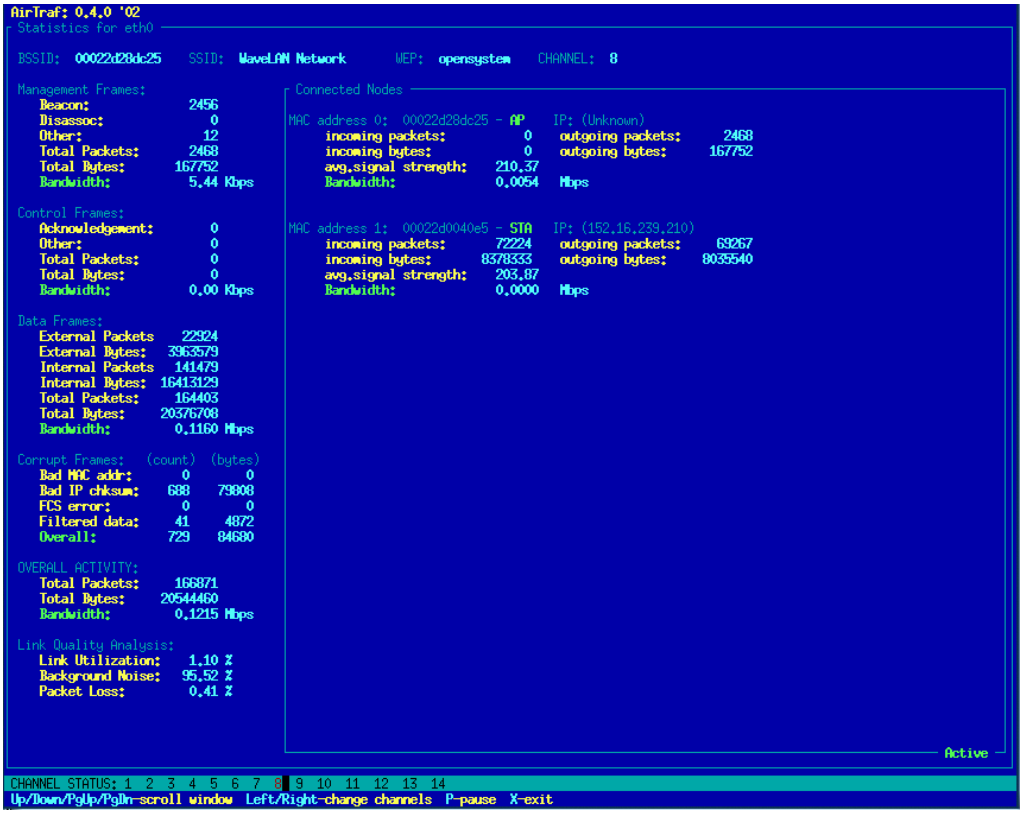

FIGURA 12: AIRTRAF NA TELA DE MONITORAMENTO DO PONTO DE ACESSO

3.2.1.2. AIRSNORT

Uma ferramenta antiga, mas muito utilizada, principalmente após a divulgação de algumas falhas no protocolo WEP. O Airsnort possibilita à captura do trafego e a quebra da chave WEP. Desta maneira, a quantidade de pacotes coletados não precisa ser previamente definida, como ocorre com outras ferramentas, nas quais primeiro é feita a captura dos pacotes e, em seguida, o processamento visando à quebra da chave.

3.2.1.3. NETSTUMBLER

O Netstumbler foi uma das primeiras ferramentas disponíveis para mapeamento e identificação de redes sem fio em ambiente Windows. Quando o objetivo é apenas de levantar informações, é uma das ferramentas mais rápidas e precisas. É possível identificar as redes, seus nomes, endereços

MAC e outras informações tais como nível de sinal de propagação de cada rede detectada. Entre as suas características, a principal é permitir a integração com equipamentos GPS e desta maneira, obter um mapa preciso de pontos de acesso identificados. A grande vantagem desta ferramenta é estar atualizada em relações aos padrões de mercado, antes limitada ao padrão 802.11b, atualmente aceita todos os outros padrões comerciais (802.11/a/b/g). Sua desvantagem está em não permitir a captura de tráfego e não possuir métodos para quebra de chaves WEP. A Figura 13 mostra a interface do software em execução.

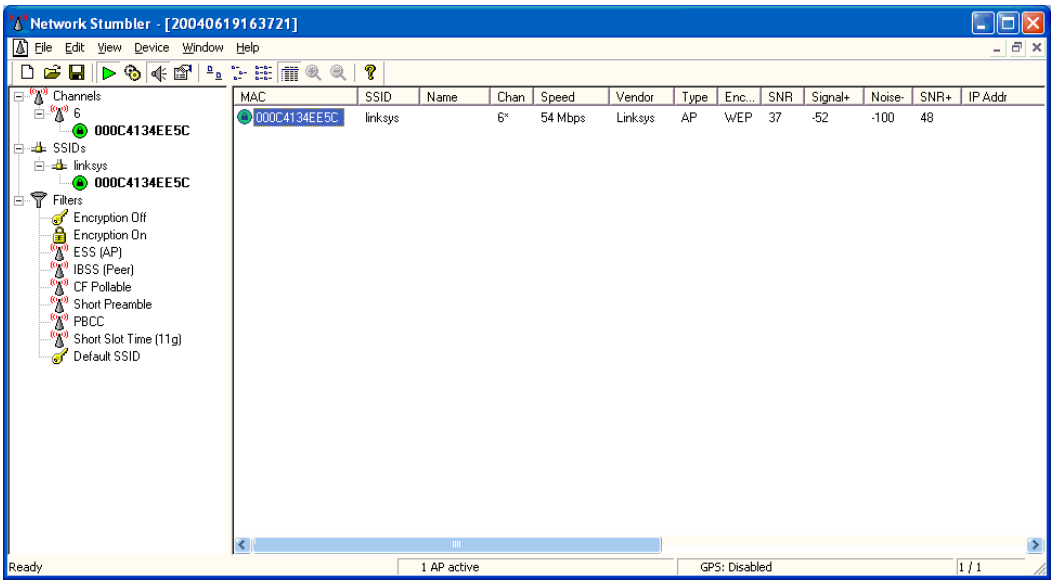

FIGURA13: INTERFACE DO SOFTWARE NETWORK NETSTUMBLER

3.2.1.4. KISMET

O Kismet5 apesar de não suportar ambiente gráfico (plataforma Linux), é um scanner e sniffeer de redes sem fio. Além de ele procurar os sinais de um Ponto de Acesso, os pacotes capturados podem ser armazenados para uma analise posterior, com o uso de programas específicos que quebrem a chave WEP. Como o arquivo com o conteúdo do tráfego é gerado no formato *pcap* ou *dump*, recomenda-se o uso da ferramenta para análise de tráfego **Ethereal** para sistemas operacionais Windows e **TcpDump** para sistemas operacionais

Linux. Esses resultados podem ser salvos em arquivos Html gerados pelo Kismet log viewer e visualizados pelo Internet Explorer. A Figura 14 e Figura 15 exibem a interface do software Kismet em execução e a Figura 16 mostra a tela inicial do software Ethereal em execução.

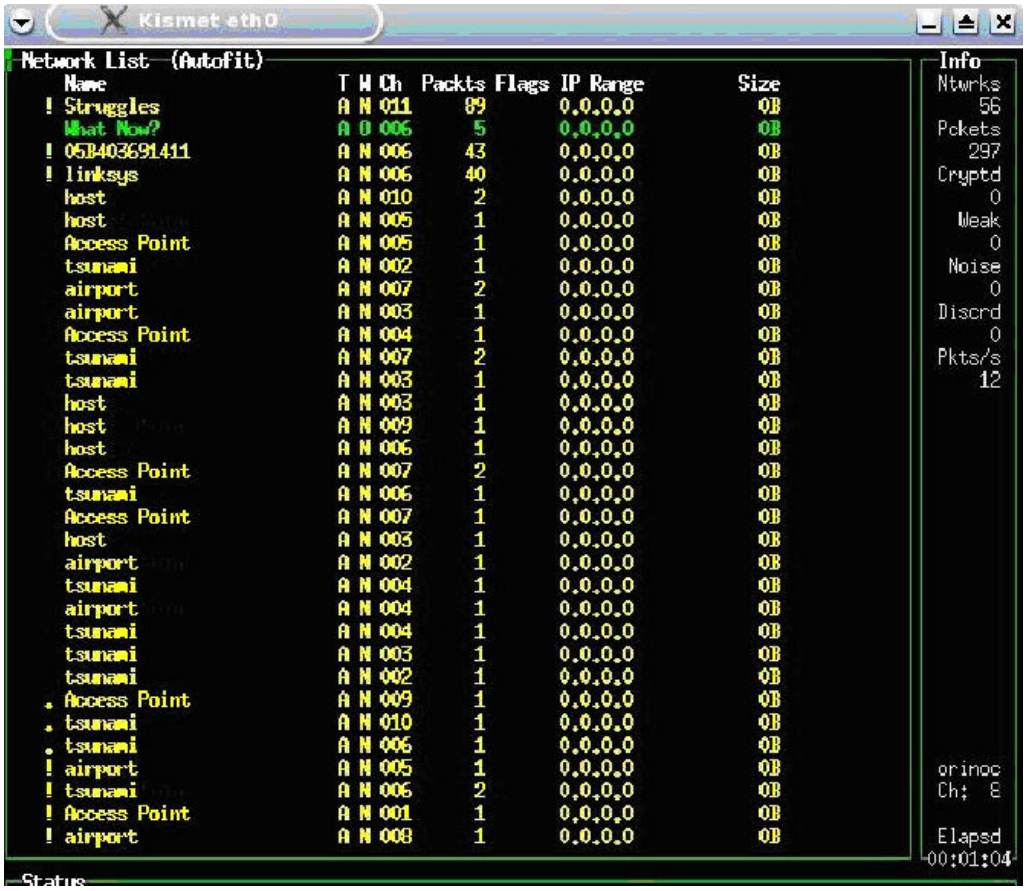

FIGURA 14: INTERFACE DO SOFTWARE KISMET

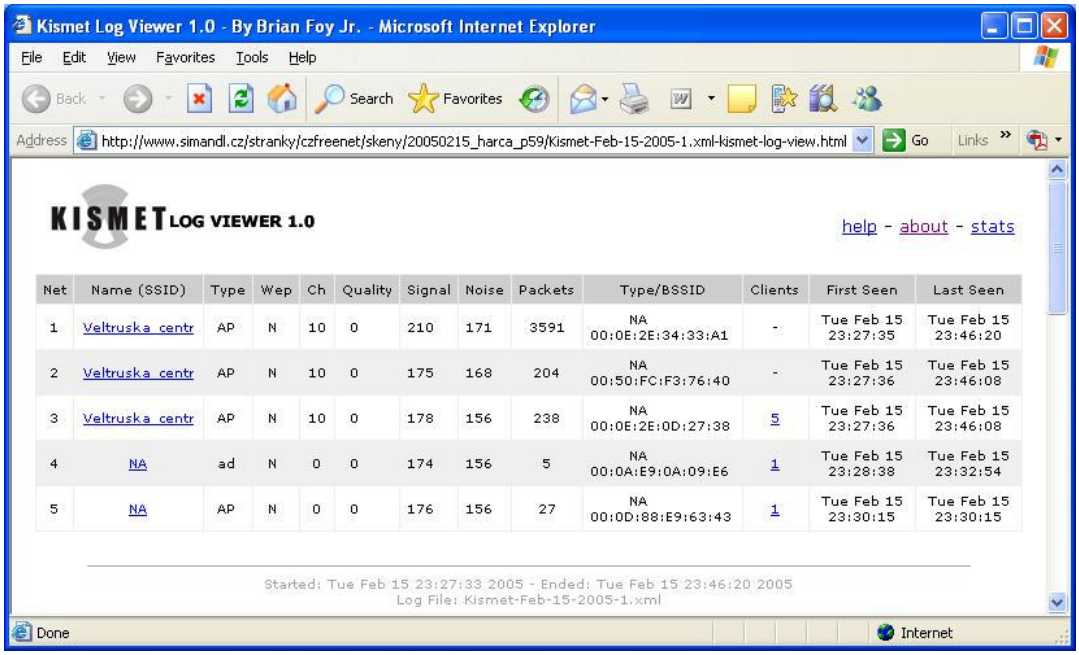

FIGURA 15: KISMET LOG VIEWER

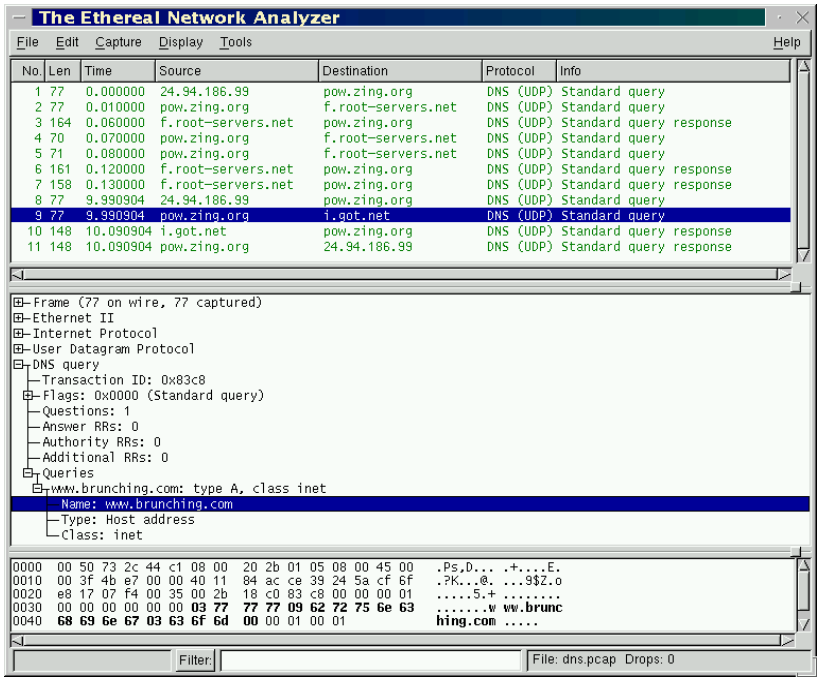

FIGURA 16: INTERFACE DO SOFTWARE ETHEREAL

3.2.1.5. FAKEAP

Uma das grandes dificuldades dos clientes de redes sem fio está em identificar de forma inequívoca o Ponto de Acesso ao qual ele está conectado. Há situações em que o invasor poderá se passar por esse ponto de acesso com o objetivo de capturar senhas e informações que por aí transitam. O FakeAp é uma ferramenta que permite essa tarefa como parte de uma “honeypot” ou como instrumento de segurança para confundir invasores que utilizam de ferramentas como Wardrivers, NetStumblers entre outros. A Figura 17 é a interface da ferramenta em execução.

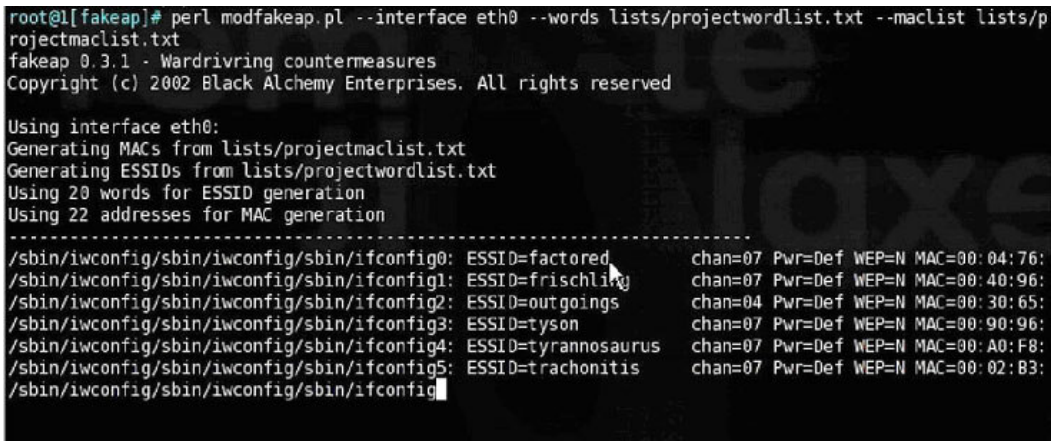

FIGURA 17: O EXEMPLO DO SCRIPT DO FAKEAP

3.2.2. VULNERABILIDADE DO ENDEREÇO MAC

Algumas medidas de segurança fazem uso do prévio cadastramento dos endereços MAC, de equipamentos que poderão ser utilizados em uma determinada rede sem fio. Porém, na prática, esta solução pode ser burlada facilmente por uma estação clandestina, que identifique o tráfego e perceba quando a estação cessar a comunicação, para então alterar seu próprio endereço MAC para se fazer passar pela estação legítima. Em ambiente Windows, a informação sobre o endereço MAC fica armazenada em uma entrada na base do registro, podendo ser modificada com o utilitário **Etherchange,** conforme mostrado na Figura 18.

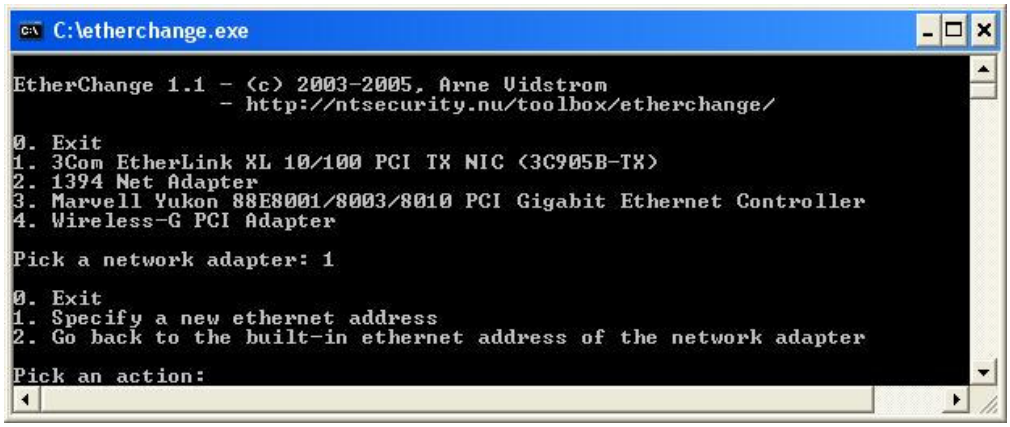

FIGURA 18: INTERFACE DO UTILITÁRIO ETHERCHANGE

3.2.3. QUEBRA DE CHAVES WEP

Existem várias ferramentas desenvolvidas para descobrir chaves WEP. Utilizam em geral uma combinação de força bruta, ataques baseados em dicionário e exploração de vulnerabilidades conhecidas. Entre as diversas ferramentas podemos destacam-se o **AirCrack, WepCrack, WepAttack, Wep_Tools e Weplab.**

3.2.4. VULNERABILIDADES DE VPN (VIRTUAL PRIVATE NETWORK)

O objetivo deste trabalho não é tratar de segurança em VPN como uma "parte" essencial, porém considerando exemplos de segurança forte. As VPNs têm sido a solução preferida para garantir acesso a ambientes remotos por meios inseguros. Contudo, existem modelos e implementações sob a designação genérica de VPN, podendo várias ser eficientes em redes cabeadas, mas não apresentam a mesma robustez em ambientes de redes sem fio. Tal situação ocorre porque vários deles confiam em camadas de redes mais baixas, como endereço MAC, e em autenticações unilaterais. Em outros casos os próprios protocolos utilizados possuem fragilidades e devem ser usados com alguma reserva exemplo do *Point-to-Point Tunneling Protocol (PPTP) e MS-CHAPv1* (Microsoft CHAP versão 1).

3.2.5. NEGAÇÃO DE SERVIÇO (DOS)

Ataques de negação de serviço em rede convencional, em geral, necessitam de grandes quantidades de banda para atingir o seu objetivo, o que se consegue mediante a combinação de várias máquinas subjugadas e o envio de pacotes ininterruptamente para uma única rede ou equipamento.

Em redes sem fio, podem ser atacada usando os métodos como associação, autenticação ou dissociação em massa com o auxílio de algumas ferramentas específicas, por exemplo, o **Void11**, mostrado na Figura 19.

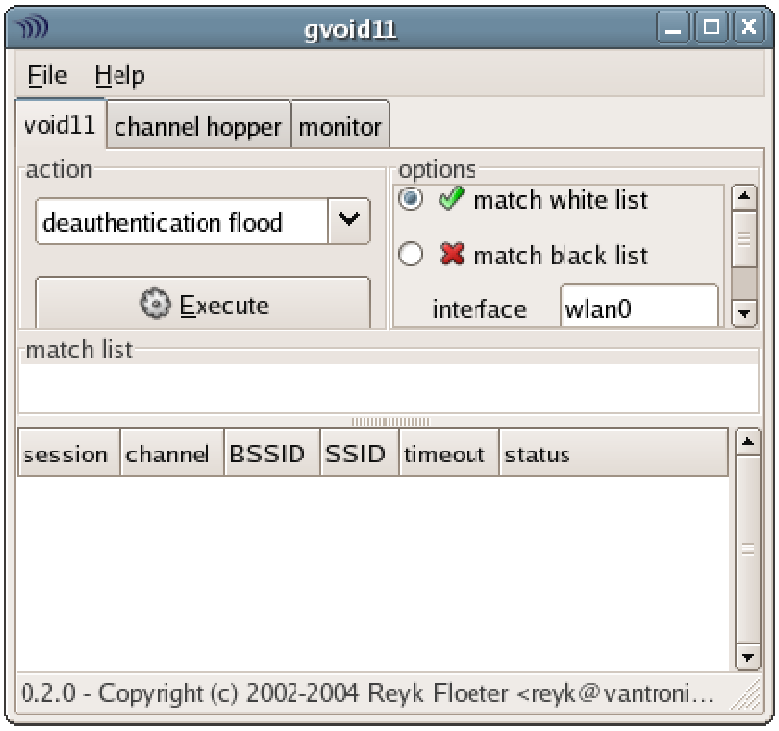

FIGURA 19: INTERFACE GRÁFICA DO GVOID11

3.2.6. ROOT KIT

Root Kit são poderosas ferramentas usadas para violar os sistemas de computadores sem serem detectados e basicamente servem para garantir que, uma vez obtido o acesso do usuário privilegiado no equipamento invadido, este acesso será mantido. Esses ataques podem começar e permanecer por muito tempo sem nenhum administrador perceber. Muito usado para descrever mecanismos e técnicas por meio de softwares malware, incluindo vírus, spyware e trojans, que tentam se esconder perante bloqueadores de spyware, antivírus, e utilitários de gerenciamento de sistemas. São classificados de diversos tipos e podem executar em modo usuário ou modo kernel.

3.3. MÉTODOS DE DEFESA

Os métodos estudados foram baseados em soluções portáveis entre os sistemas operacionais mais populares que permitam aplicar técnicas de proteção e configurações que aumentem a segurança nas redes sem fio. Várias das soluções aplicadas isoladamente não proporcionam um nível se segurança adequado, portanto devem ser combinadas para que se tornem efetivas.

3.3.1. CONFIGURAÇÕES NO PONTO DE ACESSO/ROTEADOR

O acesso ao Ponto de Acesso é um ponto crítico da infra-estrutura de um ambiente de rede e é fácil perceber por que um acesso não autorizado a este equipamento pode pôr em risco a segurança da rede.

Deve-se pensar em segurança da infra-estrutura, mas também deve ser pensada no sentido de garantir a segurança e privacidade dos clientes e proteger toda a rede contra acesso indevido e demais tipos de ataque.

Em todos os procedimentos de boas práticas de segurança em redes sem fio, é recomendado desabilitar a difusão do envio de ESSID, pois essa configuração dificulta ações maliciosas escondendo o nome da rede mostrado na Figura 20.

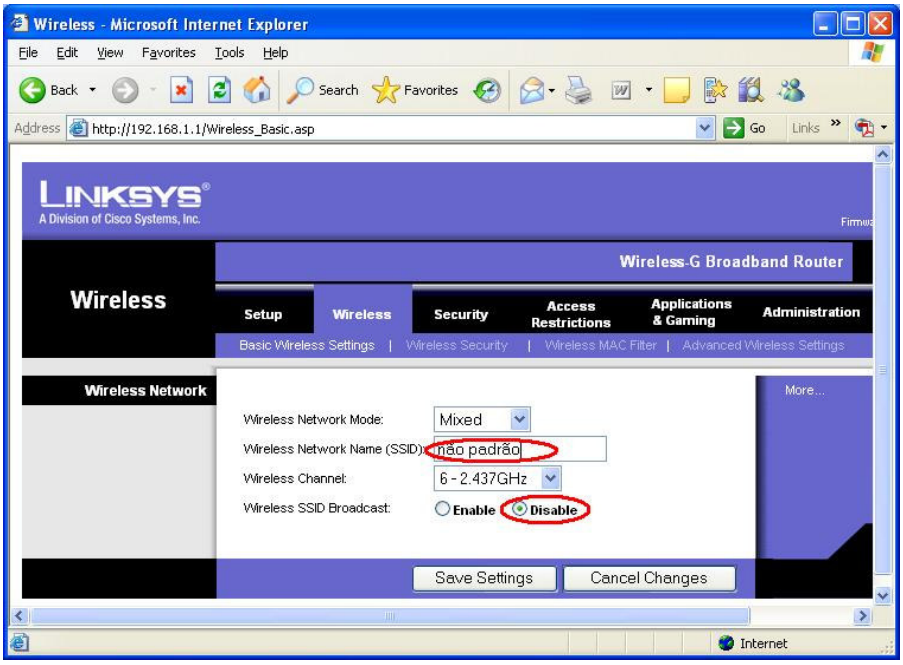

FIGURA 20: INTERFACE DE CONFIGURAÇÃO DO SSID

Outro procedimento também tende a ser categorizado como “segurança por obscuridade” e é recomendada à substituição do nome padrão do SSID para ao menos retardar um possível ataque, podendo representar o tempo necessário para o administrador detectá-lo e promover as contramedidas necessárias.

Evite a utilização dos recursos de gerenciamento e administração do ponto de acesso remotamente em redes sem fio, pois a grande maioria permite configuração via HTTP e também TELNET, mas como não há criptografia e garantia na troca das informações, desabilite conforme mostra a Figura 21.

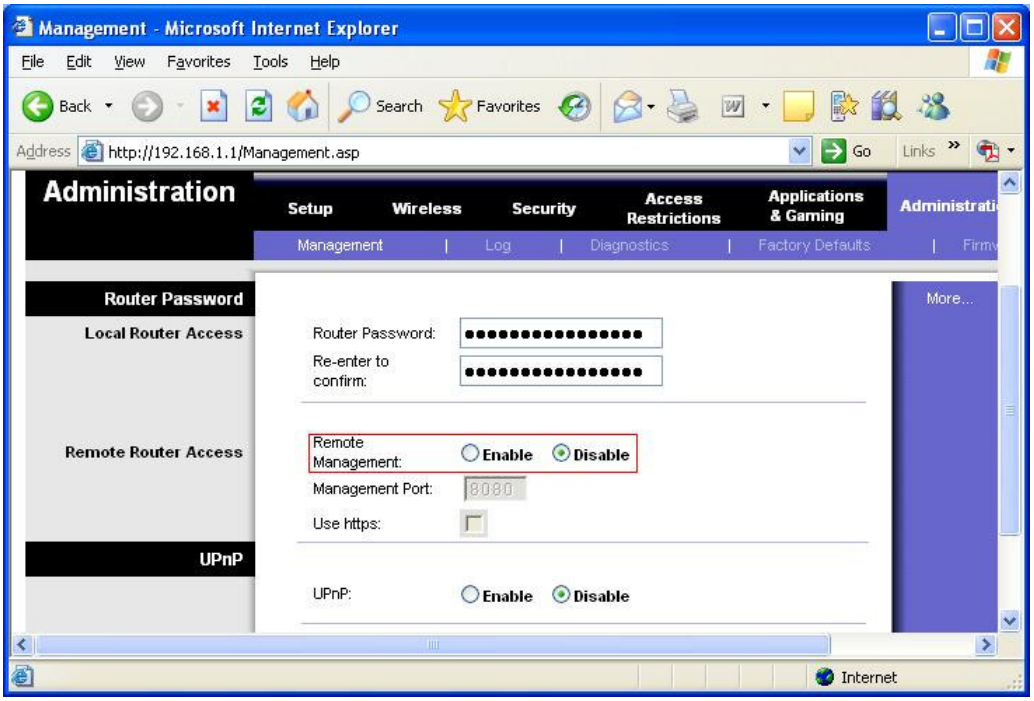

FIGURA 21: INTERFACE DE CONFIGURAÇÃO DO GERENCIAMENTO REMOTO

A Geração de chaves WEP é ponto que merece muito cuidado e atenção. Evite usar palavras conhecidas para facilitar a lembrança no momento que for gerar as chaves WEP. O administrador deverá combinar maiúsculas, e minúsculas com algarismos e caracteres especiais, entre outras recomendações.

Recomenda-se gerar a chave WEP com 128 bits e 26 dígitos hexadecimal, conforme ilustrado na Figura 22. A chave WEP é usada automaticamente, portanto não precisa ser algo que, em geral, o usuário deva ou necessite conhecer, assim sendo deve-se utilizar a de maior complexidade e com o maior tamanho, em bits, possível.

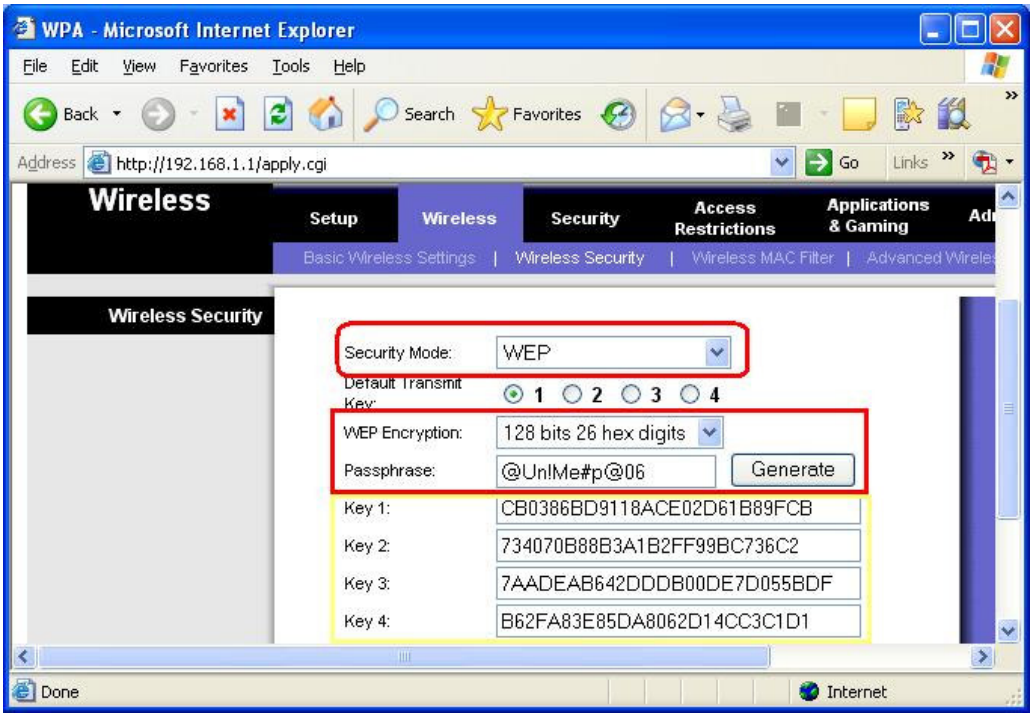

FIGURA 22: INTERFACE DE CONFIGURAÇÃO DA CHAVE WEP

3.3.2. CONFIGURAÇÃO DOS CLIENTES

A defesa dos clientes tem duas principais preocupações a serem consideradas, a inviolabilidade de comunicação, dados e equipamento do usuário e quanto ao acesso indevido às configurações de segurança da rede, ou seja, evitar que um ataque bem sucedido ao equipamento do usuário revele chaves e outras informações que possibilitem ao invasor acessar a rede com as credenciais obtidas.

Uma possibilidade interessante para aumentar as garantias de que a conexão será feita com o Ponto de Acesso (PA) correto é forçar a associação do IP com o endereço MAC do concentrador. Desta maneira será possível evitar ataques em que haja concentrador clone.

3.3.2.1. PADRÃO 802.1X E RADIUS

O padrão 802.1x define métodos de autenticação baseados no protocolo *RADIUS (Remote Authentication Dial-in User Service)* e a autenticação é um componente importante para aumentar o nível de segurança de um ambiente de sem fio.

É o método mais usado, visto que pode ser integrado a LDAP e bancos de dados convencionais. Desta forma, o usuário solicita acesso, informa usuário e senha, o concentrador valida essa informação em um servidor RADIUS e permite ou não o acesso do cliente em função da resposta dada pelo servidor.

3.3.2.2. WEP

Apesar de toda a crença na adoção do WEP, de que se trata de solução de alta segurança, a utilização do WEP permite sair da completa insegurança para um ambiente seguro sob certas limitações.

Considerar WEP robusto e por causa disso não se preocupar em implementar mais nenhuma proteção e não proceder a um correto monitoramento do ambiente pode ser um erro tão grande quanto deixar de utilizá-lo pelo simples fato de ter lido sobre suas vulnerabilidades, sem fazer uma avaliação do seu ambiente e das possibilidades que os seus recursos computacionais oferecem.

3.3.2.3. EAP_TLS

A autenticação no modelo **TLS (Transport Layer Security)** é realizada mediante troca inicial de certificados digitais entre o cliente e o servidor de autenticação RADIUS, por intermédio do concentrador. No caso mais simples, a autenticação mútua é o único elemento adicional, ou seja, baseia-se apenas na comprovação de autenticidade dos certificados apresentados. Quando o RADIUS aceita as credenciais, ele informa ao concentrador que está permitindo o acesso à rede ao equipamento.

3.3.2.4. EAP_TTLS

O estabelecimento de uma sessão que utilize este método é muito semelhante ao utilizado no **EAP_TLS**, principalmente no lado servidor, porém o cliente não necessita possuir um certificado digital para estabelecimento da conexão e fechamento do túnel, já que a autenticação será feita informando uma identificação (login) uma senha. Portanto este modelo serve apenas para estabelecer o túnel criptográfico. Após o túnel ser criado, requer-se então outro método que fará efetivamente a autenticação.

3.3.2.5. WPA

Quando necessita de segurança mais robusta, o WPA pode ser utilizado de diferentes maneiras, incluindo-se apenas os recursos de segurança nativos e também os que podem trabalhar de forma integrada a outras tecnologias, tais como 802.1x e certificados digitais.

A maneira mais simples de utilizar os recursos nativos do WPA é por meio de chaves compartilhadas, pois assim se estabelece negociação entre o cliente e o concentrador, que ao usar uma chave preestabelecida, faz com que a chave de seção seja trocado periodicamente de forma configurável.

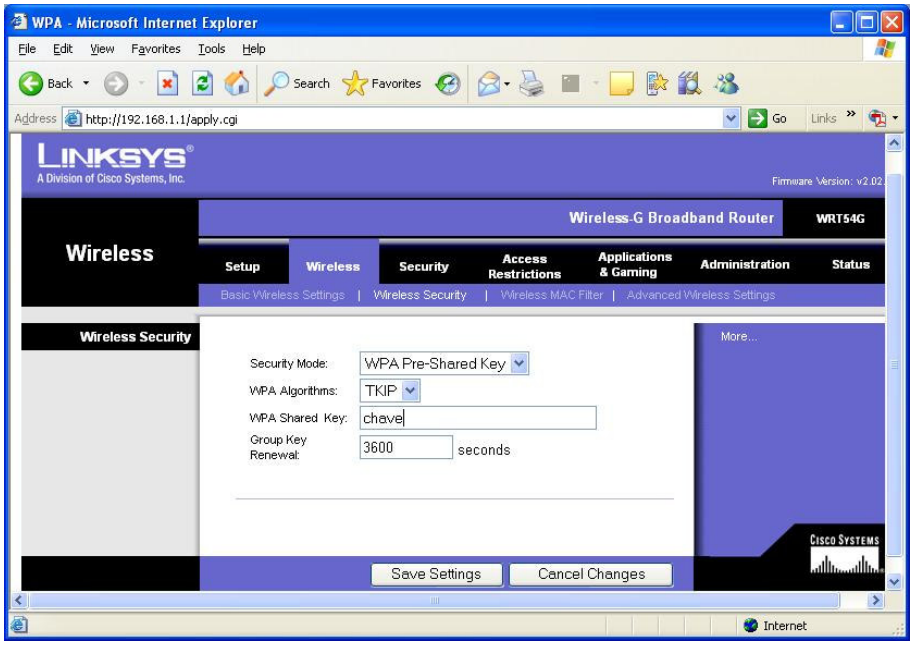

FIGURA 23: INTERFACE DE CONFIGURAÇÃO DO WPA

Em ambiente Windows é necessário que o sistema operacional suporte nativamente essa funcionalidade, como é o exemplo na Figura 24 da Propriedade da Conexão de Rede do Windows XP ou poderá ser configurada por meio de uma ferramenta específica, disponibilizada pelo fornecedor da placa de rede.

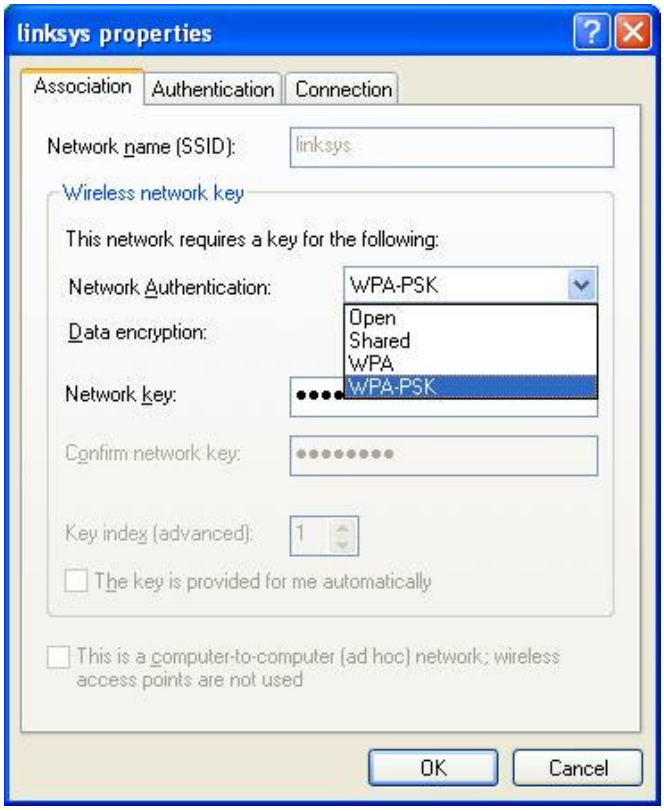

FIGURA 24: ESCOLHA DO MÉTODO DE AUTENTICAÇÃO NO WINDOWS XP

3.3.2.6. WPA-PSK

O protocolo não define mecanismos para distribuição da chave-mestra, a forma usual para executar esse procedimento é por meio do cadastro manual o que torna muito mais conveniente para redes pequenas.

O objetivo do formato WPA-PSK (também conhecido como WPA pessoal) é ser muito simples de usar e, simultaneamente, permitir um bom nível de segurança. A configuração tanto do lado do concentrador quando do lado cliente resume-se a habilitar o uso do recurso (WPA-PSK) e escolher uma chave-mestre difícil de ser descoberta.

3.3.2.7. CRIPTOGRAFIA

Independentemente do que a infra-estrutura de rede sem fio local prover, o usuário em algum momento poderá encontrar-se em um ambiente completamente aberto e sujeito aos mais variados tipos de ataque. Surge a necessidade de proteger o acesso ao equipamento e ao conteúdo das informações que trafegam pela rede de computadores.

Neste caso, devemos pensar em proteger o equipamento com tecnologias de firewall, antivírus, antíspyware etc para prover, ao usuário, mecanismos de autenticação baseados em senhas descartáveis, tokens e cartões processados (smartcards), ou ainda, fazer uso de dispositivos biométricos, que podem ou não ser combinados com token e cartões.

A proteção do equipamento varia em função do sistema operacional utilizado pelo usuário e das necessidades de sigilo das informações.

As soluções para proteger informações existem há algum tempo e vêm sendo muito utilizadas em segurança do trafego de e-mail com PGP/GPG, S-MIME etc., para acesso remoto, transferência de arquivos e VPNs simples com o uso de SSL, ou ainda, acesso e autenticação para http, principalmente com SHTTP (http + SSL). Porém, todas essas soluções apresentam pontos fracos no que diz respeito ao armazenamento das informações em áreas que podem ser lidas por um possível invasor ou por programas plantados no equipamento do usuário, da mesma forma que um programa pode também capturar as teclas digitadas pelo usuário quando este informa suas senhas.

3.3.2.8. CERTIFICADOS DIGITAIS

Um dos métodos de autenticação mais seguro aparece como a solução de segurança definitiva que não pode ser resolvida com apenas uma tecnologia, visto que, por melhor que seja, deve proporcionar com outros elementos combinados, a segurança de um determinado ambiente.

Os objetos e a cadeia que os une, em ordem crescente de hierarquia, têm: a chave privada (private key) do usuário, sua chave pública (public key) e o seu certificado, a chave pública e a certificadora AC ou AR (autoridade de registro) que assinou o certificado do usuário e, finalizando, a chave pública e o certificado da AC raiz, que por sua vez, assinou o certificado da AC/AR intermediária. Desta maneira, procura-se manter uma relação de confiança a partir da autoridade raiz.

A garantia entre as partes envolvidas é assegurada por um terceiro elemento confiável, a autoridade certificadora, que certificaremos ambas ou, ao menos, uma das partes. Na comunicação existe uma troca inicial de certificados assinados pela mesma AC ou entre as ACs que devem ter uma relação mútua de confiança e chaves públicas. As informações, então, passam a ser cifradas com a chave pública do destinatário, que usará a própria chave privada para decifrar os dados transmitidos. Neste momento negocia-se uma chave simétrica, que requer muito menos esforço computacional para agilizar a comunicação que será usada até o final da sessão ora estabelecida. A Figura 25 mostra as propriedades de configuração de um cliente permitindo a forma de autenticação.

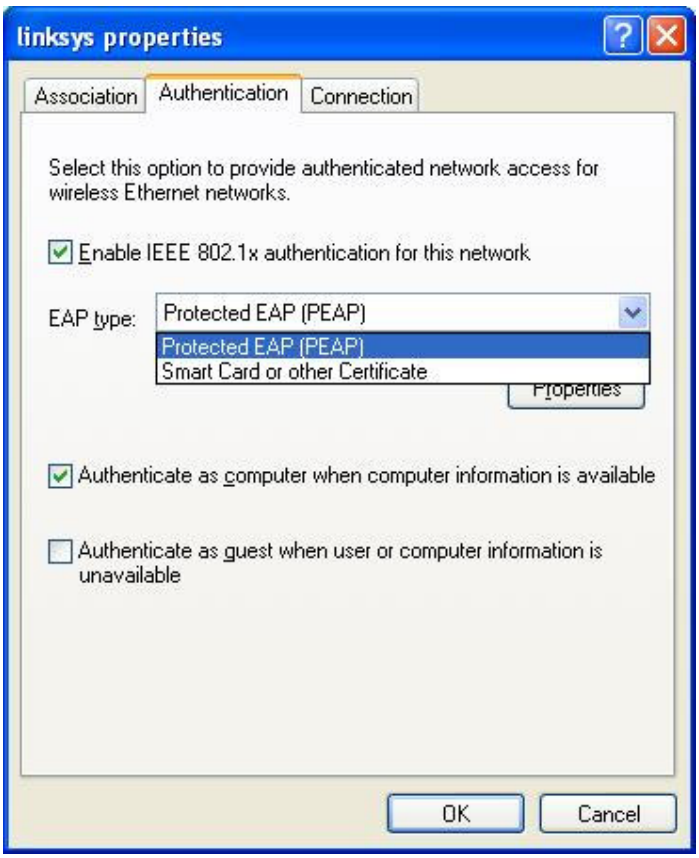

FIGURA 25: CONFIGURAÇÃO NO CLIENTE PARA PERMITIR A AUTENTICAÇÃO

3.3.2.9. FIREWALL

Combinação de hardware e software que fornece um sistema de segurança, geralmente para impedir acesso externo não autorizado a uma rede interna ou intranet. Um *firewall* impede a comunicação direta entre a rede e os computadores externos ao rotear as comunicações através de um servidor proxy fora da rede. O servidor *proxy* determina se é seguro deixar um arquivo passar pela rede. Também chamada de *gateway* de segurança.

Com o *Firewall* poderemos bloquear as portas de comunicação dos equipamentos que não estão sendo utilizadas e criar um controle sobre a comunicação dos aplicativos instalados, restringindo e garantindo certos acessos.

4. AVALIAÇÃO DA CAPACIDADE DE SOBREVIVÊNCIA DE UM SISTEMA

A segurança da informação é o problema de maior interesse, pois está relacionada com a disponibilidade da informação e a continuidade dos serviços. Em termos gerais a *viabilidade* comercial de uma empresa depende de sua habilidade de produzir e entregar produtos e serviços em um prazo ótimo, ou na pior das hipóteses aceitável. Assim podemos definir esses como sendo os objetivos e *missão crítica* de uma empresa a serem preservados para que ela consiga *sobrevier* na presença de falhas de segurança na rede ou em seus sistemas de informação. Abordamos o problema focado em última instância na sobrevivência da empresa, e não na simples prevenção e respostas aos ataques ou falhas das mais variadas formas. No enfoque da Sobrevivência, nenhum componente *individual* do sistema é imune a ataques ou falhas, mas a soma desses componentes deverá no mínimo, possibilitar a sobrevivência dos procedimentos de missão crítica, e como conseqüência da própria empresa.

As empresas em geral confiam em software comercial com vulnerabilidades conhecidas e de um único fornecedor, o que facilita a vida de elementos mal intencionados. Além disso, basicamente confia apenas em um Firewall para a proteção e manutenção da sobrevivência do sistema de informação da empresa, o que é inadequado.

A diferença entre Sobrevivência e a segurança tradicional esta nas características que são os objetivos, contexto técnico e de negócios, e ainda suposições básicas para tecnologia aplicável. Como exemplo tem-se que na segurança tradicional assume-se que um F*irewall* de última geração protegerá o sistema contra tudo e todos. Porém, do ponto de vista da Sobrevivência isso não é verdade, já que como componente *individual* o Firewall é passível de falhas.

Enquanto a segurança tradicional tem focado na confidencialidade da informação, a preocupação dos problemas hoje é relacionada à disponibilidade da informação e continuidade dos serviços. Preocupação com a continuidade

de serviços críticos entre fornecedores de infra-estrutura, seus clientes e agências de governo têm conduzido para o novo campo de garantia da infra-estrutura. A viabilidade comercial das companhias depende de suas habilidade para produzir e entregar seus produtos e serviços na maneira oportuna. Estes objetivos vão além de missões que devem conseqüentemente estender o escopo da segurança tradicional [LIPSON99].

Tratar os eventos adversos, sem esperar uma determinação definitiva da causa é o paradigma central da sobrevivência. Os efeitos são de uma importância mais imediata do que as causas, porque você terá que disponibilizar o mais rápido possível o seu sistema (ambiente). O plano de contingência requer decisões dos gerentes de riscos e da gerencia executiva, além é claro de profissionais das mais diversas áreas técnicas. A Sobrevivência depende assim de um planejamento adequado envolvendo todos esses atores.

Ocorreram muitas transformações e mudanças dramáticas dentro da natureza e estrutura de sistemas de informação. Soluções tradicionais de segurança não são suficientes para lidar com modernos problemas de segurança associados com sistemas de missão critica. Sobrevivência é uma disciplina emergente que mistura segurança de computador com administração de risco de negócio para o propósito de proteger informações altamente distribuídas, serviços e ativos. Uma suposição fundamental é que o sistema não é totalmente imune a ataques, acidentes, ou fracassos. Então, o foco desta nova disciplina não é só para evitar os intrusos de computador, mas também assegurar que a missão critica e os serviços contínuos e essenciais serão efetuados mesmo na presença de cyber-ataques, fracassos, e acidentes.

Conforme argumentado anteriormente, o estudo da segurança de redes sob o ponto de vista da sobrevivência do sistema é uma abordagem nova, e como conseqüência ainda não possui um conjunto de métodos e ferramentas bem estabelecidos. Uma alternativa recentemente proposta é o uso de uma ferramenta de simulação especificamente desenvolvida para esse fim (EASEL), a qual se encontra descrita na próxima seção.

4.1. CONCEITOS DE MISSÃO CRÍTICA

Pode se afirmar que modelos de negócios altamente dependentes da utilização de redes de computadores e de redes sem fio têm a sua sobrevivência condicionada à sobrevivência da própria rede de computadores e a rede sem fio, ou seja, ela própria pode ser considerada como sendo de missão crítica. Nesse contexto, capacidade de sobrevivência é definida como sendo a capacidade que um sistema possui para cumprir sua missão de maneira correta e com tempo de resposta aceitável, mesmo na presença de falhas ou ataques maliciosos ao sistema.

O foco da pesquisa de sobrevivência está na entrega de serviços essenciais e na preservação de recursos essenciais mesmo durante um ataque ou violação, além de recuperar oportunamente todos os serviços e recursos após o ataque. Defini-se recursos e serviços essenciais àqueles sistemas que são críticos para o cumprimento das missões de uma organização. Sobrevivência na presença de ataques depende de três capacidades essenciais que o sistema deve ter as estratégias de: resistência, reconhecimento e recuperação conhecidos como “3Rs”. [ELLISON99].

Sobrevivência, sendo uma disciplina emergente, apóia-se em disciplinas existentes incluindo segurança, tolerância à falhas e confiabilidade, introduzindo também novos conceitos e princípios.

Dessa forma, conclui-se que aspectos ligados à segurança de redes são críticos para a capacidade de sobrevivência do negócio da empresa. Em linhas gerais este trabalho pretende identificar os aspectos técnicos e funcionais que são relevantes para a sobrevivência das redes sem fio e serão analisados os possíveis cenários de ataques, invasões e finalmente proposto medidas de prevenção e correção que garantam a manutenção da atividade de missão crítica da empresa.

4.2. MÉTODO SNA

Neste trabalho está sendo empregada a metodologia proposta pelo CERT (instituto ligado à *Universidade Carnegie Mellon*), usado na análise de aspectos relevantes, que busca entender os riscos para um sistema ou ambiente e tem os objetivos de identificar os serviços essenciais que devem sobreviver às intrusões, identificarem os efeitos da intrusão na missão e Identificar os processos; exigências ou melhorias na arquitetura que podem melhorar as chances do sistema sobreviver com a ferramenta para realizar a simulação, o *Easel.*

O Método de Análise de Segurança de Rede sob o enfoque da sobrevivência *(Survivable Network Analysis - SNA)* é dividida em quatro etapas, conforme mostrado na Figura 26. No primeiro passo preocupa-se com as definições do sistema que é dividido em: definição das exigências do sistema; definição da arquitetura e descrição do sistema.

No segundo passo, identificam-se os serviços essenciais e recursos, baseados no objetivo da missão e a conseqüência das falhas. Para isso, usam-se cenários para caracterizar serviços essenciais e uso dos recursos. A definição essencial da potencialidade é dividida em: serviços essenciais/eleição dos recursos/cenário; identificação de componentes essenciais.

No passo três foram escolhidos os cenários de intrusão baseados no ambiente do sistema e uma avaliação de risco e potencialidades de intruso. A definição da potencialidade de comprometer. É avaliada em: seleção do cenário de intrusão e identificação dos componentes comprometidos, que o intruso pode entrar ou danificar.

No passo quatro foi identificado à arquitetura dos componentes de ponto de vulnerabilidade com os componentes que são essenciais e comprometidos, baseados nos passos 2 e 3. Analisando então os pontos de vulnerabilidade dos componentes e suas arquiteturas que suportam as propriedades chaves da sobrevivência que são: estratégias de resistência, reconhecimento e recuperação, também conhecidas como “3Rs”.

A análise dos três Rs é mostrada em um mapa da sobrevivência. Este mapa é uma matriz que mostra, para cada cenário de intrusão e seus efeitos correspondentes aos pontos de vulnerabilidade, uma tarefa que já é feita e uma recomendação para as três estratégias de resistência, reconhecimento e recuperação.

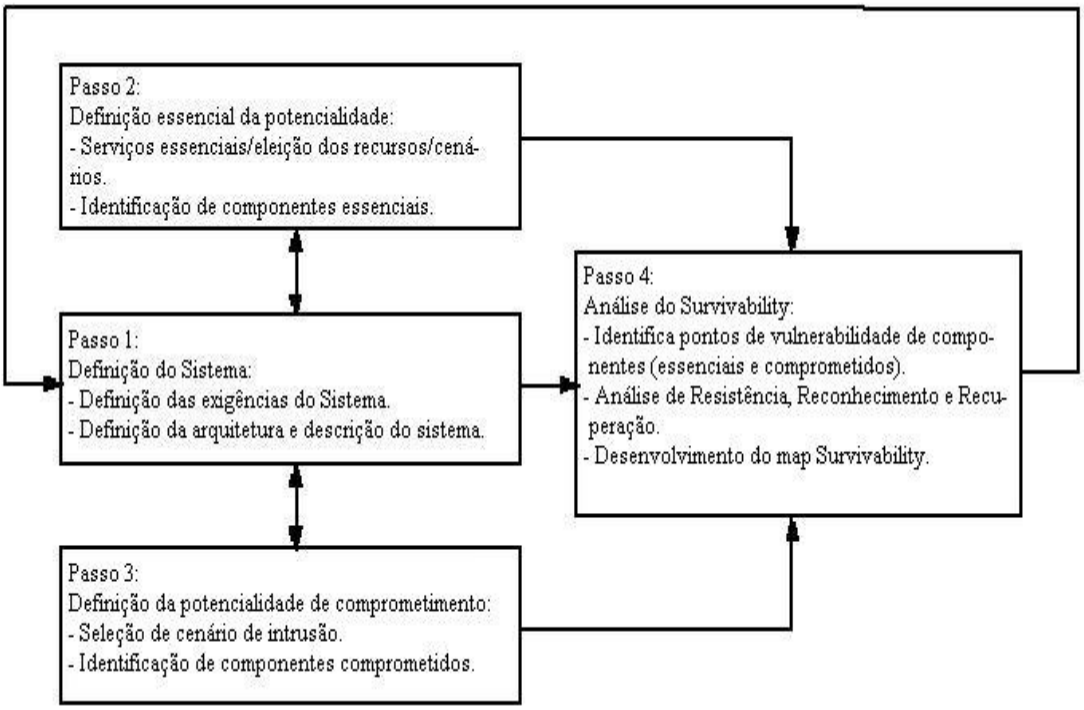

FIGURA 26: MÉTODO DE ANÁLISE DE REDE PELA SOBREVIVÊNCIA

Easel é uma ferramenta de desenvolvimento para pesquisa de segurança e sobrevivência em sistema *"não delimitado".* Segundo [CHRISTIE02], um sistema "não delimitado" é qualquer sistema nos quais os participantes (humano ou computadorizado) têm somente informações incompletas ou imprecisas sobre o sistema inteiro. Eles incluem participação humana e também de componente automatizados. Seus limites não são conhecidos precisamente. A interconexão entre os participantes no sistema "não delimitado" altera-se constantemente. E, além disso, a confiabilidade e freqüentemente a identidade dos participantes é desconhecida. O controle administrativo centralizado não pode ser inteiramente eficaz em tais sistemas.

A exigência de pontos chaves que incluem uma semântica consistente de execução com redes *"não delimitada"* e diversos tipos de configurações permitem a simulação de aplicativos e também a monitoração, levantamento de dados e a analise de simulações.

Esta ferramenta permite a modelagem de sistemas complexos constituídos por um número muito grande de elementos interagindo entre si. Facilitando ao usuário visualizar propriedades emergentes, algoritmos e alguns recursos únicos para segurança e sobrevivência, que possuem diversas características importantes, e que podemos destacar – seu código é móvel (no sentido de mobilidade), protocolos definíveis do usuário da interação e a habilidade de compartilhar o nó do usuário arbitrário em combinações especificadas.

Os algoritmos e protocolos podem ser simulados em diferentes níveis de situações, a tempo de a linguagem abstrair o processo de descrição dos atores com o nível de precisão esperado.

Empresas altamente dependente de processos de software devem ser capazes de lidar com condições dinamicamente mutáveis, incluindo o mercado, colaboradores internos e externos, e esses mesmos processos computacionais. Todavia, as conseqüências dessas mudanças são de difícil previsão, principalmente quando são levadas em conta as *interações* entre os diversos atores de um modelo complexo. Em geral um ator interage com outros atores localmente, não tendo acesso a todo o conjunto de informações relevantes à suas ações, mas apenas a um subconjunto delas. Características como essas definem um sistema como sendo "*não delimitado"*, ou seja, um no qual atores individuais possuem uma visão restrita da informação do sistema completo. Assim, decisões tomadas por atores individuais podem parecer apropriadas no contexto local, porém inadequadas para o sistema global. As propriedades do sistema resultantes dessas decisões são ditas *emergentes*, sendo de difícil previsão.

Propriedades emergentes podem ser vistas como análogas àquelas de sistemas sociais ou biológicas, onde cada ator possui um comportamento relativamente simples e local, interagindo com alguns outros, porém sem um

completo conhecimento sobre outros atores participando ou interagindo no sistema. Esse tipo de comportamento local forma a base para os chamados algoritmos emergentes, definidos como uma computação que alcança efeitos globais previsíveis através da comunicação com um número limitado de vizinhos imediatos e sem a presença de controle centralizado ou visão global. Exemplos de algoritmos emergentes em sistemas *não-delimitados* incluem a cultura do povo de uma determinada região, a economia de um país, ou ainda processos de negócios altamente dependentes de sistemas baseados em software.

É fácil perceber a dificuldade encontrada na previsão dos efeitos globais sofridos por um sistema de informações baseado em uma rede aberta, sujeito a ações individuais – genuínas ou maliciosas – das mais diversas espécies. Igualmente obvio é a relação que isso possui com a necessidade de garantia de sobrevivência do sistema na eventualidade de falhas ou ataques. Como resultado estabelece-se a necessidade de um sistema ou ferramenta com a qual algoritmos emergentes possam ser descritos analisados, testados e monitorados no contexto de redes de computadores não-restritas.

Nesse contexto, EASEL tem sido desenvolvido como uma *ferramenta de simulação* para pesquisas em segurança e sobrevivência de redes não-restritas, que inclui identificar tendências e analisar o alto impacto das ameaças e vulnerabilidade, como tais ataques difundidos na infra-estrutura da rede ou ataques automatizados que envolvem novas vulnerabilidades, técnicas ou ferramentas.

Alguns dos requisitos indispensáveis que EASEL preenche incluem uma semântica de execução consistente com o modelo de rede não-restrita, um conjunto de dados rico o suficiente para suportar uma larga gama de aplicações simuladas, e ainda recursos para o monitoramento e análise de dados estatísticos. EASEL permite a simulação de um ambiente composta por atores fracamente acoplados, interagindo entre si sem qualquer controle centralizado ou visibilidade global.

Alguns exemplos de simulação do Easel constam no site do CERT e em [CHEN99], onde podemos visualizar os seus códigos e entender os seus propósitos. São eles:

- Simulação de Ataque na Rede, À rede consiste de 4 tipos de nós que são: Vermelho é o atacante, Azul o defensor, Verde é o host descomprometido e Preto é o *host* comprometido. Existe a comunicação entre eles.

- Simulação de Reação de emergência simula a resposta de ambulâncias para um desastre. Ambulâncias são associadas com hospitais e notificadas inicialmente do desastre, correm no cenário onde pegam suas vitima a qualquer hora e transportam para os hospitais.

- Simulação de Simples roteamento. A simulação ilustra um simples algoritmo para roteamento de redes, seleciona randomicamente os destinos.

4.3. METODOLOGIA PROPOSTA

Conforme apresentado na seção anterior, o *SNA* é o método usado na análise de aspectos relevantes, que busca entender os riscos para um sistema ou ambiente e tem os objetivos de identificar os serviços essenciais que devem sobreviver às intrusões, identificarem os efeitos da intrusão na missão e Identificar os processos; exigências ou melhorias na arquitetura que podem melhorar as chances do sistema sobreviver.

A metodologia proposta é uma simplificação do método SNA, visando facilitar a sua aplicação juntamente com o auxílio da ferramenta *Easel* para realizar as simulações sugeridas em Cenários de Uso que poderão ser modificados, visando obter resultados desejáveis de Sobrevivência através do Cálculo da Vulnerabilidade Potencial.

A proposta do Cálculo da Vulnerabilidade Potencial (VP) contém quatro passos, são eles:

Passo 1. Definição do Sistema

Onde serão definidas as exigências do sistema, a definição da arquitetura e as descrições do sistema.

Passo 2. Definição de Serviços e Componentes de Missão Critica

Identificar os serviços e recursos essenciais baseados nos objetivos da missão e das conseqüências das falhas.

Passo 3. Definição de Potencialidade de Intrusão

Selecionar cenários de intrusão baseados nos ambientes do sistema e a identificação dos componentes comprometidos, que o intruso poderá acessar e ou danificar.

Passo 4. Cálculo da Vulnerabilidade Potencial

Diferentemente do método SNA, que analisa os pontos de vulnerabilidade dos componentes e das suas arquiteturas que apóiam os elementos chaves da sobrevivência dos “3Rs” (Estratégias de Resistência, Reconhecimento e Recuperação), o Cálculo da Vulnerabilidade Potencial dispensa a análise dos “3Rs” e calcula através das simulações o valor do parâmetro “Vulnerabilidade Potencial”, que é a porcentagem de intrusões bem sucedidas para determinados cenários.

O Método do Cálculo do Valor da Vulnerabilidade Potencial é dividida em quatro etapas, conforme mostrado na Figura 27.

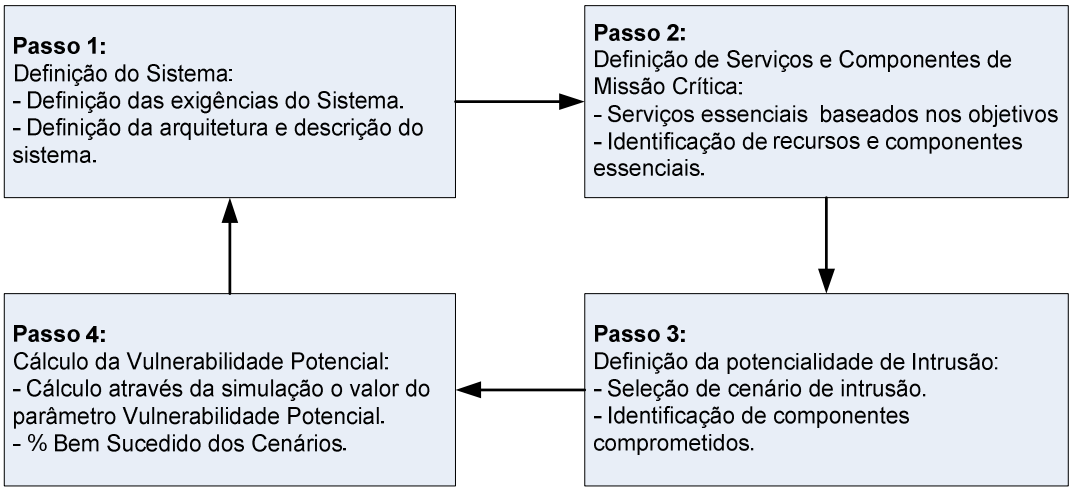

FIGURA 27: MÉTODO DE CÁLCULO DO VALOR DE VULNERABILIDADE POTENCIAL

Em termos de interação entre esses componentes, é circular, ou seja, de 1→ 2 → 3 → 4 → 1 que retorna para 1 para redefinir novas configurações do sistema, caso o resultado não seja aceitável, em decisão gerencial/técnica.

Com isso, podemos identificar claramente os "possíveis" riscos e melhorar as configurações de segurança em partes dos componentes ou em todo o Cenário, modificando os parâmetros assumidos e realizando novas simulações com o auxílio da ferramenta Easel.

Por exemplo, para um Cenário ocorreram 165 ataques do tipo Mal-Sucedidos e 22 ataques do tipo Bem-Sucedidos. Aplicando o Cálculo da Vulnerabilidade Potencial que é representada pela equação ilustrada na Figura 28, o valor da Vulnerabilidade Potencial é 0.12.

$$VP = \frac{BS}{(MS + BS)}$$

FIGURA 28: EQUAÇÃO DO CÁLCULO DA VULNERABILIDADE POTENCIAL

Onde *VP* é o valor da Vulnerabilidade Potencial, *BS* é a quantidade de ataques Bem Sucedido e *MS* é a quantidade de Ataques Mal Sucedido.

Utilizando a ferramenta Easel, espera-se poderem simular os diversos ambientes propostos nos estudos de casos e que permitam as interações dos diferentes atores para se obter as diferentes formas de configuração corretas dos equipamentos e situações de uso que foram inseridos na simulação.

Com a Linguagem Easel será possível simular os ataques que tiveram sucessos e falhas, quais os atores que proporcionaram o ataque, o tipo de ataque, em qual equipamento da sem fio sofreu essa invasão e o tipo de risco que estará sujeito à rede de computadores e os seus sistemas existentes.

4.4. RESULTADOS ESPERADOS

Como resultado final, espera-se compreender melhor os problemas e as dificuldades para manter a sobrevivência de um sistema, que está fortemente dependente da utilização de redes sem fio e o potencial desta metodologia para lidar com essas dificuldades.

5. APLICAÇÃO DA METODOLOGIA EM CENÁRIOS HIPOTÉTICOS

Entre diversas aplicações, ambientes de negócios e tecnologias é possível acompanhar a evolução da utilização de redes sem fio em empresas que não medem esforços para acompanhar o ritmo do mercado, e ao mesmo tempo destacar suas tecnologias empregadas no desenvolvimento do seu produto.

Diante desses e de outros fatores, podemos afirmar que muitas empresas adotam e instalam estrutura de rede sem fio para suportar o seu negócio sem a segurança necessária. Muitas vezes desconhecem as medidas necessárias ou ignoram certas recomendações para “ganhar tempo” no processo de implementação e esquecem de analisar os riscos que podem trazer aos seus negócios. Apesar de poder ser enquadrado em um contexto mais genérico, este trabalho de pesquisa utiliza uma rede sem fio hipotética, utilizada por uma empresa de fabricação de bens de consumo eletrônicos, como impressoras, telefones celulares, etc. Esta empresa pode ser vista como um fabricante terceirizado, que recebe pedidos de outras empresas responsáveis pelo projeto e a comercialização dos produtos. Um processo bastante interessante ocorre entre os computadores clientes que estão alocados nas linhas de produção e que controlam todas as fases de produção dos bens. Os dados coletados no processo de fabricação pelos softwares de chão de fábrica são armazenados nos servidores localmente e que estão trabalhando em redes sem fio, conforme apresentado na Figura 29 ilustrando a planta da fábrica.

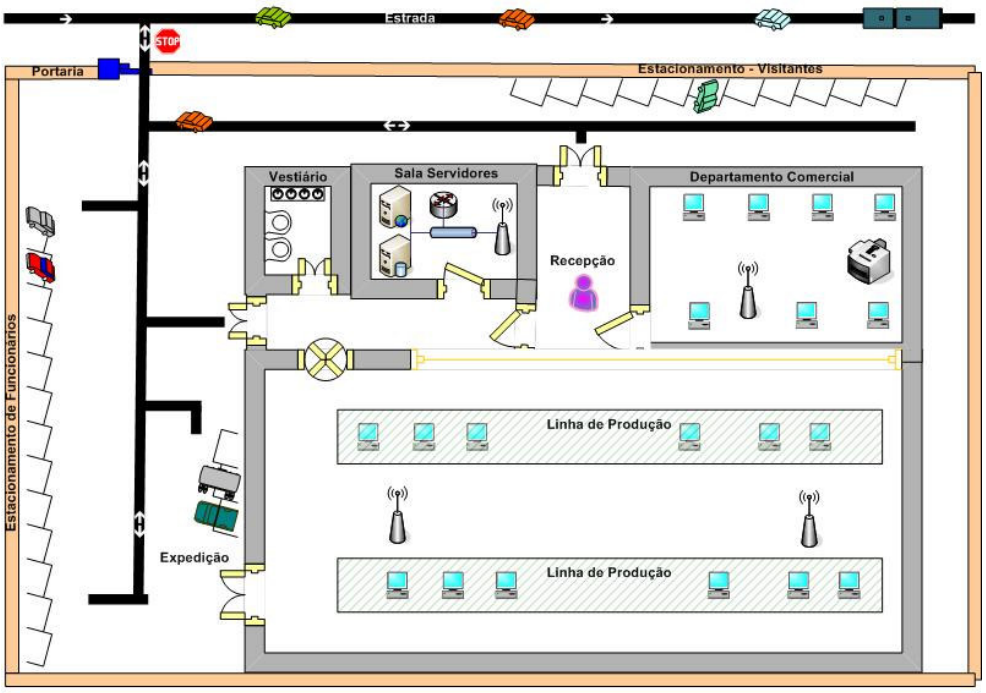

Figura 29: Planta da distribuição dos equipamentos na linha de produção.

Essa Planta foi criado com o auxílio do software Microsoft Office Visio 2003 baseado em uma planta de uma empresa do mesmo segmento fabril proposto, esse arquivo gerado pelo Microsoft Office Visio 2003 foi convertido para a extensão ***tif*** e então importado para o equipamento Macintosh no diretório do software de simulação Easel.

Dessa forma, fica clara a importância do funcionamento correto da rede sem fio e dos servidores relacionados para a manutenção das atividades de missão critica da empresa de manufatura.

Foram simuladas 03 configurações diferentes de segurança dos equipamentos de Ponto de Acesso (PA) de uma rede de computadores sem fio de uma empresa hipotética.

As simulações foram definidas e executadas na Ferramenta Easel que roda somente em equipamentos Macintosh. O hardware utilizado para desenvolver esse trabalho é um computador MAC G3 com Processador de 500 MHz e de

256 MB de Memória, conforme a Figura 30 que exibe essas informações obtidas do equipamento.

FIGURA 30: TELA DE CONFIGURAÇÃO DO MACINTOSH

5.1. DELIMITAÇÃO DO PROBLEMA

O trabalho proposto deverá estudar a capacidade de sobrevivência de uma empresa sob a perspectiva de falhas de segurança e ataques aos seus sistemas de informação. O método proposto a ser empregado, o Cálculo da Vulnerabilidade Potencial baseia-se na ferramenta de simulação EASEL conforme apresentado na seção 4.2.

Adotando a configuração padrão nos equipamentos da rede sem fio, ou seja, definida sem a mínima segurança, poderemos simular os acessos de usuários válidos; a invasão de usuários não autorizados e a invasão de *hackers* na rede sem fio. Através dessa simulação, teremos o Cálculo da Vulnerabilidade Potencial que permitirá visualizar os riscos que a empresa está sujeita e concluiremos a fragilidade da infra-estrutura que comprometer-se com a

missão crítica da empresa. Alternativamente, será considerado o uso de alguns procedimentos de segurança, verificando-se o grau de eficácia dos mesmos.

Foi adotada a interação de 30 atores, que são os personagens criados para a simulação e que estão sendo classificados de 3 maneiras nesta simulação: **Usuário,** o **Usuário Mal intencionado** e o **Hacker**. Através do monitoramento da atividade desses atores, espera-se compreender melhor e prever o impacto de usuários reais acessando a rede sem fio da empresa.

5.2. DESCRIÇÃO E NECESSIDADES DE UMA EMPRESA HIPOTÉTICA

A empresa **Capricórnio Computer International** é líder na produção de seus computadores no mercado de Taiwan. Realizado um estudo com seus diretores, chegou à decisão de que teriam um melhor custo-benefício se os equipamentos fossem produzidos no Brasil para atender aos pedidos de compras dos países da América do Sul.

O serviço de montagem e logística dos microcomputadores no Brasil foi terceirizado para a empresa de médio porte **Toffee Informática e Engenharia Ltda**. A Toffee Informática e Engenharia possui em sua fábrica um prédio dividido em administrativo e área de produção, onde possuem 2 linhas de produção para atender aos pedidos de produtos de diversos clientes. Inicialmente estará sendo produzido o microcomputador modelo **XM2007**.

Para esta Descrição e Necessidades de Uma Empresa Hipotética estaremos aplicando o Passo 1 da Metodologia Proposta, através do Método de Cálculo da Vulnerabilidade Potencial.

5.2.1. ASPECTOS CONSIDERADOS DE MISSÃO CRÍTICA PARA A EMPRESA

A empresa cliente, a Capricórnio precisa acompanhar semanalmente pela Internet toda a operação de produção e logística de seus equipamentos produzidos pela empresa terceirizada, a Toffee Informática e Engenharia Ltda.

Usando a Internet o cliente conecta ao servidor WEB e realiza os downloads dos *logs* de produção e faz os ajustes nos sistemas quando necessário.

Todos os equipamentos computacionais deverão estar configurados com o padrão recomendado de segurança e os servidores e a infra-estrutura adotada na empresa contratada, necessitará possuir uma política de segurança que satisfaça os órgãos responsáveis evitando o roubo ou o vazamento de informações sigilosas dos negócios.

Esses servidores que armazenam os planejamentos e os registros de produção devem estar fortemente configurados para receber os registros e ao mesmo tempo aceitar somente as conexões remotas do cliente e proprietário dos dados que é a Capricórnio Computer International.

A Toffee Informática e Engenharia Ltda é obrigada a armazenar por um período de 5 anos todos os registros de todos os equipamentos que venha a ser produzidos para a empresa Capricórnio. (Histórico dos equipamentos para auditoria anual da Capricórnio Computer International). É fundamental e necessária a utilização dos recursos computacionais de forma racional e que garantam a segurança exigida para reduzir o melhor equipamento com a qualidade e o comprometimento que foi vendido ao cliente num curto prazo de tempo do processo de produção à logística. (Distribuição ao cliente do cliente).

Portanto, para este cenário, a Missão Crítica envolve toda a disponibilidade dos servidores de aplicação e armazenamento, o funcionamento da rede sem fio com as devidas configurações, a segurança na utilização dessa infra-estrutura, as permissões e direitos atribuídos aos usuários que deverão ser monitorados e principalmente, a garantia de armazenamento e integridade dos dados produzidos.

Estaremos aplicando o Passo 2 da Metodologia Proposta, através do Método de Cálculo da Vulnerabilidade Potencial serão identificados os componentes essenciais.

A Figura 31 apresenta a infra-estrutura adotada para suportar esse negócio e na seção seguinte detalhes dos recursos tecnológicos empregado.

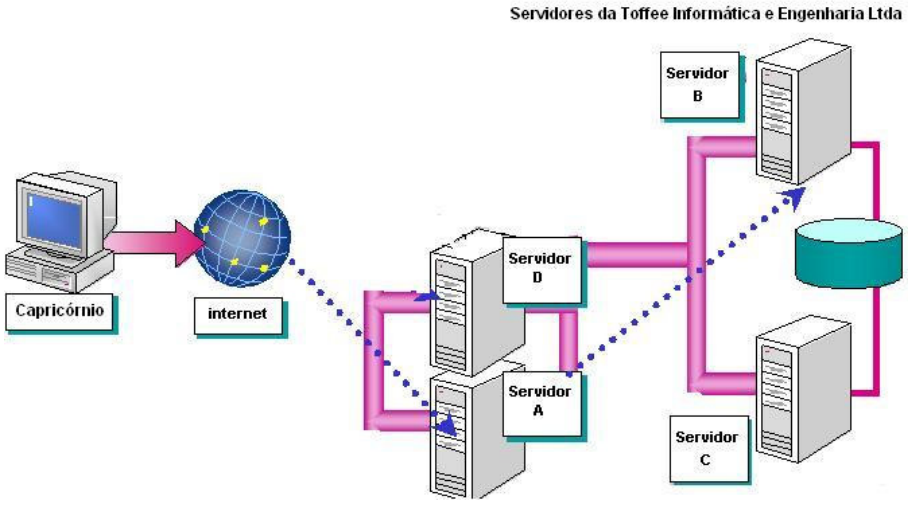

FIGURA 31: AMBIENTE COMPUTACIONAL DA TOFFEE ENGENHARIA LTDA.

5.3. MODELAGEM DA EMPRESA ANALISADA

Nesta seção descrevemos o modelo analisado, considerando os equipamentos, softwares, formas de ataque e de defesa.

Esse sistema hipotético é inspirado em sistemas reais de produção de grandes empresas e marcas conhecidas. Tal escolha justifica-se pelo complexo cenário de infra-estrutura e na sobrevivência da missão crítica em situações de riscos.

5.3.1. EQUIPAMENTOS E SOFTWARES

A Toffee Informática e Engenharia Ltda dispõe de recursos para servidores e para suas estações de trabalho. A seguir a descrição completa de cada recurso.

O sistema de produção foi desenvolvido baseado na tecnologia Web. Os servidores de aplicação Web e de Banco de dados devem estar funcionando no sistema 24 x 7, com parada preventiva pré-agendada para o terceiro domingo do mês, no intervalo das 06h:00 às 14h:00.

Na linha de produção há microcomputadores com leitores de código de barras e impressoras de etiqueta que em determinadas etapas da produção o operador necessita para registrar o código dos produtos utilizados e gerar o número de série do produto final. Todo esse controle é necessário devido ao controle de qualidade do produto e a logística do mesmo. As estações de trabalhos rodam o sistema operacional Windows XP Professional e o Internet Explorer 6.0 como o navegador para abrir o sistema.

Desenvolvido para rodar em plataforma WEB, o sistema de chão de fábrica, **TRACK** é o responsável por gerenciar todos os processos de produção dos microcomputadores da Capricórnio Computers International.

Utiliza-se do banco de dados SQL 2000 da Microsoft como armazenamento dos dados gerados.

5.3.2. EQUIPAMENTO DO CLIENTE

Os equipamentos da linha de produção são todos do modelo e com os periféricos:

- Micro Pentium 4 1.8 GHz de processador, com 256 MB Ram e HD de 80 GB.
- Leitor Óptico de mão.
- Impressora de Etiqueta
- Sistema Operacional Windows 2000 Professional com Internet Explorer 6.0 que o usuário necessita para rodar a aplicação de chão de fabrica.

5.3.3. SERVIDORES

Na estrutura de servidores, podemos dizer que a empresa possui bons equipamentos para suportar a aplicação do cliente. Falamos de performance. A seguir a descrição do que cada servidor roda:

Servidor A – Roda o sistema operacional Windows 2003 Server e o Internet Information Server que gerencia toda a aplicação TRACK e os serviços de WEB. Ele é apenas o meio de comunicação entre o cliente e a base de dados onde é feito o armazenamento.

Servidor B e C – Roda o sistema operacional Windows 2003 Advanced Server, com o serviço de Cluster ativo (quando uma maquina parar a outra assume) e o banco de dados SQL 2000 Advanced Server armazenado em uma storage. Este hardware é o responsável por gerenciar e armazenar as informações de todos os equipamentos e periféricos criados.

Servidor D – Roda o sistema operacional Microsoft Windows 2003 Server, é o responsável pelas contas de usuários (login na rede), pelo gerenciamento das impressoras e pelos dados gerados pelo departamento administrativo.

Todos os equipamentos estão em redes, utilizam placas de redes configuradas a 100 MBps. A Figura 32 ilustra o layout dos equipamentos que a Toffee Informática e Engenharia possuem.

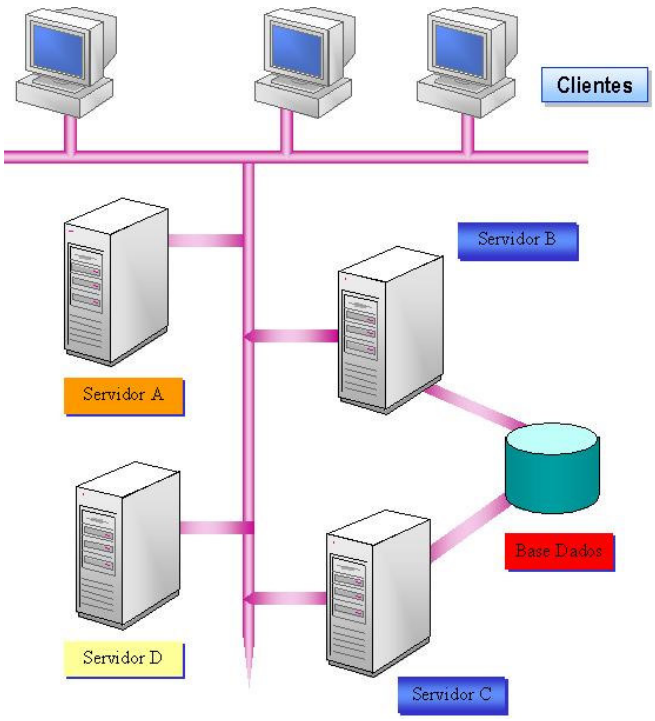

FIGURA 32: ILUSTRAÇÃO DOS SERVIÇOS E SERVIDORES DA TOFFEE INFORMÁTICA

5.3.4. IDENTIFICAÇÃO DE POSSÍVEIS FALHAS OU ATAQUES NO CENÁRIO ASSUMIDO

Conforme visto no Capítulo 3, existem diversas maneiras e ações que podem ocorrer e comprometer o funcionamento do sistema que atende a linha de produção da empresa hipotética descrita. Nas simulações a serem feitas, serão consideradas as seguintes vulnerabilidades:

- Descoberta do nome da rede sem fio, o SSID e a invasão.
- Ausência das chaves WEP para prover criptografia.
- Configuração do Firewall.
- Problemas de segurança nos softwares utilizados.

Para esses Cenários Assumidos, aplicando o Passo 3 da Metodologia Proposta, através do Método de Cálculo da Vulnerabilidade Potencial serão identificados os componentes comprometidos.

5.4. MODELAGEM DOS ATAQUES

Nesta etapa realizou-se uma representação através de um modelo de simulação que reflita os aspectos relevantes dos sistemas na utilização de redes sem fio e a sua interação com os servidores em toda a fábrica. Entenda-se por relevantes aos aspectos que podem influenciar a segurança e sobrevivência do sistema, ou seja, a segurança da rede é crítica para a capacidade de sobrevivência do negócio da empresa o que inclui segurança dos componentes de hardware, acessos e falhas ou vulnerabilidades encontradas. Estes últimos servirão como base para a simulação de ataques, falhas e procedimentos corretivos.

Utilizando de uma planta da fábrica, torna-se fácil compreendermos a topologia existente e a utilização dos **PAs** (Pontos de Acesso) espalhados. Para determinarmos a área de alcance do PA, foram utilizados dados do fabricante desses PA's, sendo considerados outros itens próximos aos PAs como por exemplo: proximidade de janelas, aquários, equipamentos que utilizam da mesma freqüência da rede e para melhorar nosso entendimento e o desenvolvimento adotamos o valor de 1 metro correspondente a 1 pixel representado na Figura 28 que ilustra a Planta da Fábrica.

Foram criados os atores **User, BadUser** e **Hacker**, que são simbolizados pelas figuras identificados na Tabela 1, juntamente das cores escolhidas para representar o Sucesso ou a Falha de um determinado tipo de ataque.

Inicialmente foram escolhidas as três principais formas de invasões, que são: **Análise de Tráfego, Acesso Não Autorizado** e o **ataque de DoS** os quais foram abordados na seção 3.1 e 3.2. Além disso, um ataque DoS bem sucedido pode originar-se em um quarto tipo de ataque muito perigoso conhecido como **Root Kit**, que são poderosas ferramentas que uma vez utilizada, explora as vulnerabilidade do sistema operacional, violando o sistema do computador sem ser detectado. Para as redes de computadores sem fio, podemos implementar as seguranças recomendadas visando a redução da

possibilidade de ataques, e permitindo estudos na simulação que poderá ter a inclusão de quantos outros componentes (ataques e segurança recomendada) para serem simulados e analisados, conforme a necessidade.

Previamente configurados a quantidade desses atores na simulação, ao começar a simulação, o BadUser e o Hacker começam a caminhar aleatoriamente na área determinada da planta da fábrica em busca de um sinal de um Ponto de Acesso para tentar se conectar. Inicialmente tentarão a invasão por Análise de Tráfego. Se não conseguirem, tentarão por Acesso Não Autorizado. Caso ainda não consigam sucesso, tentarão o ataque de DoS e se conseguir o ataque DoS, podemos afirmar que as configurações do Firewall foram vencidas com sucesso, possibilitando uma ataque do tipo Root Kit aos servidores, o que pode comprometer a missão crítica da empresa. Não conseguindo a invasão, o ator recomeçará as tentativas. Obtendo o sucesso em qualquer situação, esse ator ficará "parado" na cor que representa o sucesso do ataque, registrando o Tipo de Ataque, Tipo de Ator, o tempo que ele conseguiu o sucesso, a porcentagem que foi gerada da chance de sucesso do ator e em qual Ponto de Acesso ocorreu o ataque. Todas essas atividades e resultados correspondentes são registrados no relatório da simulação gerado pela ferramenta EASEL.

ATOR	FIGURA	ANÁLISE TRÁFEGO	SUCESSO	ACESSO NÃO AUTORIZADO	SUCESSO	DOS	SUCESSO	ROOT KIT
USER	○	VERDE	VERDE ESCURO	AMARELO	LARANJA	ROSA	VERMELHO	PRETO
BAD USER	⬭	VERDE	VERDE ESCURO	AMARELO	LARANJA	ROSA	VERMELHO	PRETO
HACKER	□	VERDE	VERDE ESCURO	AMARELO	LARANJA	ROSA	VERMELHO	PRETO

TABELA 1: TIPOS DE ATORES E DE ATAQUES

5.4.1. CONFIGURAÇÃO DO TEMPO DE SIMULAÇÃO

Em cada execução de simulação desejada, o tempo de simulação da mesma, deverá ser informado (configurado) individualmente no código do programa que a linguagem irá interpretar. Esse tempo é o tempo real de execução da simulação e deverá ser informado na função, ***TempoReal :: number := 60;.***

Para os Estudos de Casos apresentados nesse trabalho, foram realizadas as simulações de 10 minutos de atividades, simulando cada configuração.

5.4.2. CONFIGURAÇÃO DA PROPORÇÃO DE TEMPO ENTRE A SIMULAÇÃO E O TEMPO REAL DE EXECUÇÃO

Para poder trabalhar com os tempos de simulação foi necessário, seguindo a documentação da ferramenta Easel, definir a proporção do Tempo Real de Execução e da Simulação.

O Tempo de Simulação é a simulação real que um Administrador de Redes possa querer simular algum componente, neste trabalho, por exemplo, querer simular 30 minutos de tentativas de invasão a seus Pontos de Acesso configurados de alguma forma. E o Tempo de Execução é o tempo de Processamento da Simulação pelo Easel, ou seja, não é necessário esperar por 30 minutos para obter os resultados. Através da função ***speed*** eu consigo ajustar seus valores da proporção de tempo real e conseguindo reduzir esse tempo de acordo com o padrão adotado na ferramenta.

A sintaxe da função é:

(s.skdr).speed:= 10.0; onde representa:

s: É a variável de simulação;

s.skdr: Na variável simulação, utiliza a variável speed.

speed: Variável que define o tempo de simulação.

A Proporção adotada no Easel para ser informada na função ***(s.skdr).speed:=*** da execução da simulação são:

- **5.0 = 0,5** – Dar 1 Tempo Real para metade do Tempo de Simulação interna do Easel;
- **10.0 = 1** – Dar 1 Tempo Real para 1 Tempo de Simulação interna do Easel;
- **20.0 = 2** – Dar 1 Tempo Real para 2 Tempos de Simulação interna do Easel;
- **40.0 = 2** – Dar 1 Tempo Real para 4 Tempos de Simulação interna do Easel;

Lembrando que esses valores deverão ser utilizados em um bom equipamento, e o Easel ter a prioridade de processamento para permitir uma perfeita simulação, sem a redução de desempenho.

Após a escolha do Tempo de Simulação, podemos calcular o Tempo de Execução com a Proporção necessária utilizando a equação ilustrada na Figura 33.

$$Execucao \times \left(\frac{\mathrm{Pr}\, oporcao}{10} \right) = Simulacao$$

FIGURA 33: EQUAÇÃO DO TEMPO DE EXECUÇÃO E PROPORÇÃO

Para a equação acima, por exemplo, se adotarmos 30 minutos de simulação, e o parâmetro do **speed** for 20.0, a ferramenta rodará por 15 minutos ou menos, que estará simulando os 30 minutos. Para este trabalho, definimos a proporção de 10.0, ou seja, 1 minuto de simulação equivale a 1 minuto de execução.

5.4.3. IMPLEMENTAÇÃO DA CONFIGURAÇÃO DE SEGURANÇA

Na simulação criada para ilustrar as possíveis falhas ou ataques em Pontos de Acesso (PA) de uma rede sem fio inserimos 4 Pontos de Acesso, representados por **PA 1, PA 2, PA 3** e **PA 4**, onde esses PAs podem ser configurados com o nível de segurança desejado para cada simulação, permitindo ao final de cada simulação obter os resultados separados e classificados por PA ou de todo o conjunto.

Com os PAs inseridos na Planta, foi calculado a área de atuação de cada PA para determinar e conhecer quando um ator se movimentar pela planta se este está dentro do raio de atuação do sinal da rede sem fio ou não. Para encontrarmos e inserirmos estes valores na simulação, através do Plano Cartesiano, pode calcular o raio utilizando a equação da circunferência e o Teorema de Pitágoras conforme a ilustração da equação apresentada na Figura 34 a seguir.

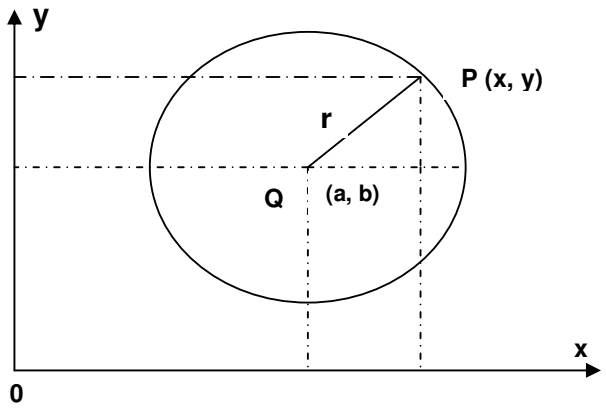

FIGURA 34: ILUSTRAÇÃO DA CIRCUNFERÊNCIA

Seja, então, uma circunferência com centro no ponto Q (a, b) e raio r conforme a Figura 34, Um dado ponto P (x, y) está contido na circunferência se, e somente se a seguinte condição for verdadeira da Figura 35.

$$(x-a)^2 + (y-b)^2 <= r^2$$

FIGURA 35: EQUAÇÃO DA CIRCUNFERÊNCIA

Considerando a função matemática acima adotada, conseguimos identificar e definir a localização exata da área de atuação da rede sem fio (o raio) e podemos apontar essas coordenadas dos Pontos de Acessos individualmente no código da simulação e trabalhar com esses parâmetros para conseguirmos simular a interação dos atores quanto à segurança física e lógica da rede.

Após o conhecimento desses valores, podemos com o auxílio do Easel, implementar no código da simulação de acordo com a sintaxe exigida a real localização dos Pontos de Acessos permitindo uma simulação mais precisa.

No código da simulação desenvolvida nesse trabalho, a localização dos 04 PA's na sintaxe é representada pelos seguintes parâmetros:

null new (s,TAcessPoint(410,184,100, false, false, false, false, 1, 9,9.5,9,8));

null new (s,TAcessPoint(611,235,100, false, false,false, false, 2, 9,9.5,9,8));

null new (s,TAcessPoint(325,420,100, false, false, false, false, 3, 9,9.5,9,8));

null new (s,TAcessPoint(660,423,135, false, false, false, false, 4, 9,9.5,9,8));

Onde temos a localização dos PAs, (com a Posição X, Posição Y e Raio), a opção *false* (que permite a exploração das vulnerabilidade, ou seja a Efetividade de Defesa) SSID, Wep, Firewall, Rootkit, Id (identificação do PA), ChanceSSID, ChanceWep, ChanceDos, ChanceRootKit (e os valores que são as porcentagens da Efetividade de Ataque).

A Figura 36 ilustra a localização física dos Pontos de Acessos de acordo com as coordenadas na planta da fábrica.

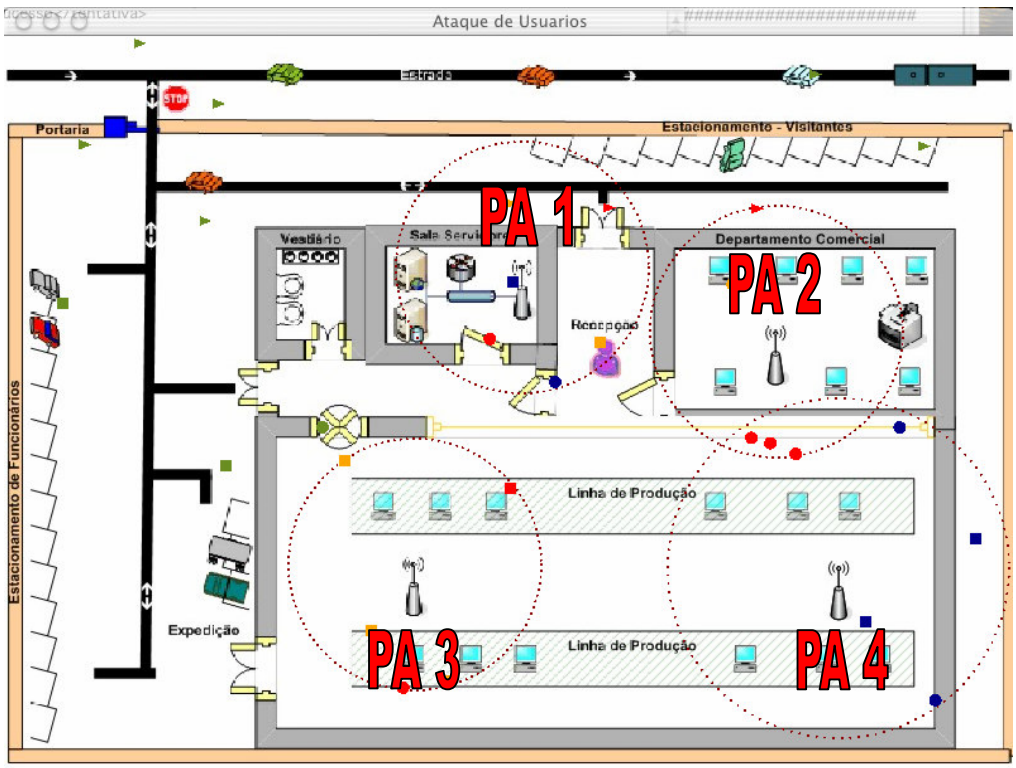

FIGURA 36: LOCALIZAÇÃO DOS PA´S

Para eleger os tipos de ataques e as recomendações necessárias para a prevenção dos mesmos, poderemos adotar valores e métodos apresentados por institutos de segurança que trabalham especificamente com segurança.

Para este trabalho foram escolhidos os principais problemas de segurança que são; **Análise de Tráfego, Acesso não autorizado, DoS e Root Kit** (este último ocorre somente quando o ataque ao DoS ocorrer com sucesso) e as soluções adotadas para a prevenção e redução desses ataques são, **Alterar o SSID e desabilitando o envio de sinal automaticamente, a implementação de Chaves Wep 128 bits, a adoção de um Firewall fechando todas as portas desnecessárias e Instalando todos os corretivos dos sistemas operacionais tornando o mais seguro e vulneráveis a exploração de falhas.**

Devemos configurar individualmente cada opção de segurança recomendada ou todas habilitando ou desabilitando de acordo com a segurança recomendada para a simulação desejada e aqui proposta.

RECOMENDADO PARA A SEGURANÇA	***ATAQUE***
SSID DISABLED	*TRAFFIC ANALYSIS*
WEP/WPA	*UNAUTHORIZED ACCESS*
FIREWALL	*DOS*
SEGURANÇA DO S.O.	*ROOT KIT*

TABELA 2: TIPOS DE ATAQUES E RECOMENDAÇÕES PARA SEGURANÇA

5.4.4. QUANTIDADE DE ATORES

Depois de configurado os PAs, é necessário informar a quantidade de atores que serão simulados, lembrando que temos os atores, User, BadUser e Hacker. Para adicionar a quantidade, é necessária apenas a alteração na variável *quantidade*, representada no Easel: ***quantidade := 10;*** *#10 tipos de cada*

5.5. CENÁRIO HIPOTÉTICO 1

Para este Estudo, foi utilizado o cenário da Fábrica adotando-se os 4 Pontos de Acesso com os mesmos valores que representam os equipamentos com as configurações padrões dos fabricantes, ou seja, sem a segurança recomendada e sujeito aos principais ataques. Essas configurações adotadas inicialmente pelos fabricantes, visam à inexperiência dos clientes e a facilidade

de uso, porém esquecem a segurança recomendada e que com certeza trará grandes problemas aos usuários.

Adotou-se a quantidade de 10 atores (User, BadUser e Hacker) de cada tipo e simulando por 10 minutos, onde os atores exploraram e fizeram os ataques por procura de sinais (pacotes) na rede pelo SSID, por captura de pacotes não criptografados (Ausência de WEP) e por ataques de DoS que se sujeita devido a ausência de Firewall e este ataque quando for executado com sucesso, foi gerado o ataque de Root Kit explorando vulnerabilidades das configurações e do sistema operacional.

Ilustraremos a quantidade e quais foram os ataques sofridos por esses equipamentos com esses parâmetros.

5.5.1. PARÂMETROS DE CONFIGURAÇÃO ASSUMIDOS

Assumiu-se que os equipamentos da rede sem fio, ou seja, os Pontos de Acesso estão com as seguintes configurações:

- Nome da rede sem fio, o SSID padrão, neste exemplo de equipamento da marca Linksys® [LINKSYS], o SSID é ***Linksys*** e habilitado o envio do SSID por sinal sem fio.
- O Modo de Segurança da rede sem fio Desabilitado, ou seja, não implementado o WEP.
- E sem a Proteção do Firewall

Assumindo-se essas configurações na simulação, foi adotada em cada item de segurança, a **Opção de Falso**, opção que permite o ataque ao componente e torna-se necessário informar a porcentagem mínima (valor) que um ator deverá possuir para conseguir o sucesso no ataque. Esse valor atribuído ao ator é dado aleatoriamente no momento da simulação que pode ser baseada em chances e probabilidade de ataques segundo estudos de organizações credenciadas. Quanto mais recursos de segurança implementados, menores serão as chances de sucesso na invasão, logo, eu devo aumentar a

porcentagem dos recursos que são os atributos que determinam se um ator conseguirá ou não o sucesso. Por exemplo, se na simulação um ator estiver com o valor 30, e o recurso estiver configurado para permitir o sucesso com porcentagens acima de 40%, portanto esse ator não conseguirá sucesso na sua invasão. A Tabela 3 descreve os componentes e a porcentagem mínima para ocorrer o sucesso no ataque.

Dispositivo	SSID	WEP	Firewall	Root Kit
Ponto de Acesso 1	Falso = 20%	Falso = 0,1%	Falso = 0,1%	Falso = 30%
Ponto de Acesso 2	Falso = 20%	Falso = 0,1%	Falso = 0,1%	Falso = 30%
Ponto de Acesso 3	Falso = 20%	Falso = 0,1%	Falso = 0,1%	Falso = 30%
Ponto de Acesso 4	Falso = 20%	Falso = 0,1%	Falso = 0,1%	Falso = 30%

FALSO: *EFETIVIDADE DE DEFESA (ED).*

% *: INDICADOR DE EFETIVIDADE DE DEFESA DE UM RECURSO.*

TABELA 3: CONFIGURAÇÃO DOS PA´S NO CENÁRIO HIPOTÉTICO 1.

5.5.2. RESULTADOS OBTIDOS DA SIMULAÇÃO

No intervalo de tempo monitorado, ocorreram 19 ataques sendo 18 ataques com êxito. As suas tentativas de exploração na falta de configuração e implementação dos recursos de segurança e apenas 1 ataque que não satisfazia os valores definidos para o sucesso.

Uma classificação sobre os tipos de ataques e as quantidades correspondentes encontram-se nos gráficos abaixo.

Na Figura 37 temos o gráfico que ilustra as quantidades de ataques sofridos do Cenário 1.

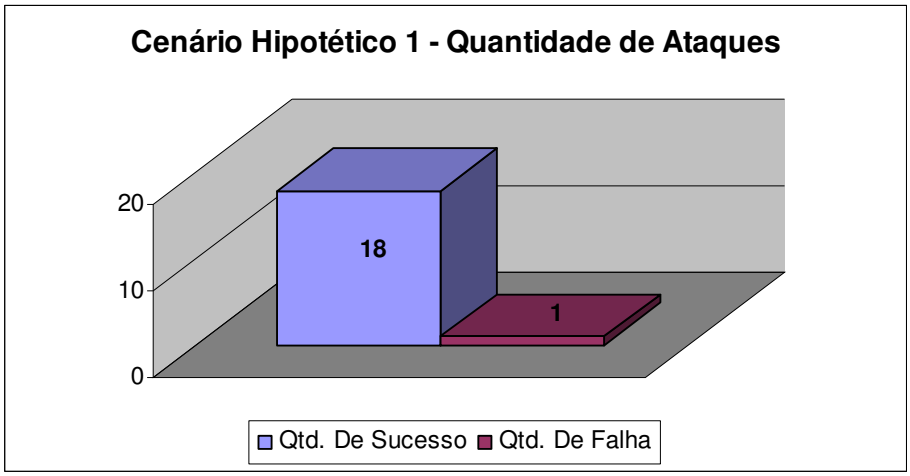

Figura 37: Quantidade de Ataques no Cenário Hipotético 1

Na Figura 38 temos o gráfico que ilustra as quantidades e os tipos de ataques sofridos do Cenário 1.

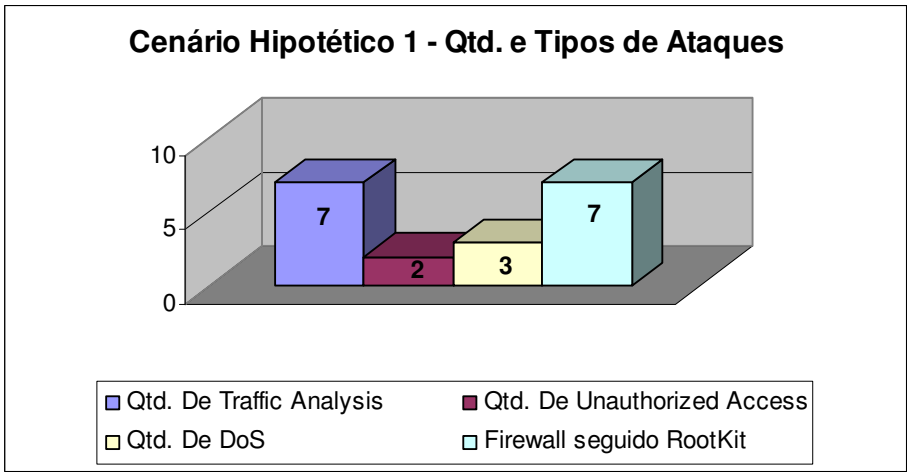

Figura 38: Quantidade e Tipos de Ataques no Cenário Hipotético 1

5.5.3. CÁLCULO DA VULNERABILIDADE POTENCIAL

Para este Cenário 1, conforme seção 4.3 e aplicando o Passo 4 da Metodologia proposta, o valor da Vulnerabilidade Potencial é **0,95**; onde o Valor da Vulnerabilidade Potencial ideal é 0,0 (Seguro); concluímos um Cenário vulnerável e principalmente, incapaz de manter a missão crítica.

A Figura 39 ilustra a planta da fábrica após essas invasões no período de tempo monitorado. Conforme a Tabela 1, os pontos coloridos na Figura 39, representa os variados tipos de atores em execução e ilustram os ataques ocorridos com sucessos e os ataques com falhas neste Cenário 1.

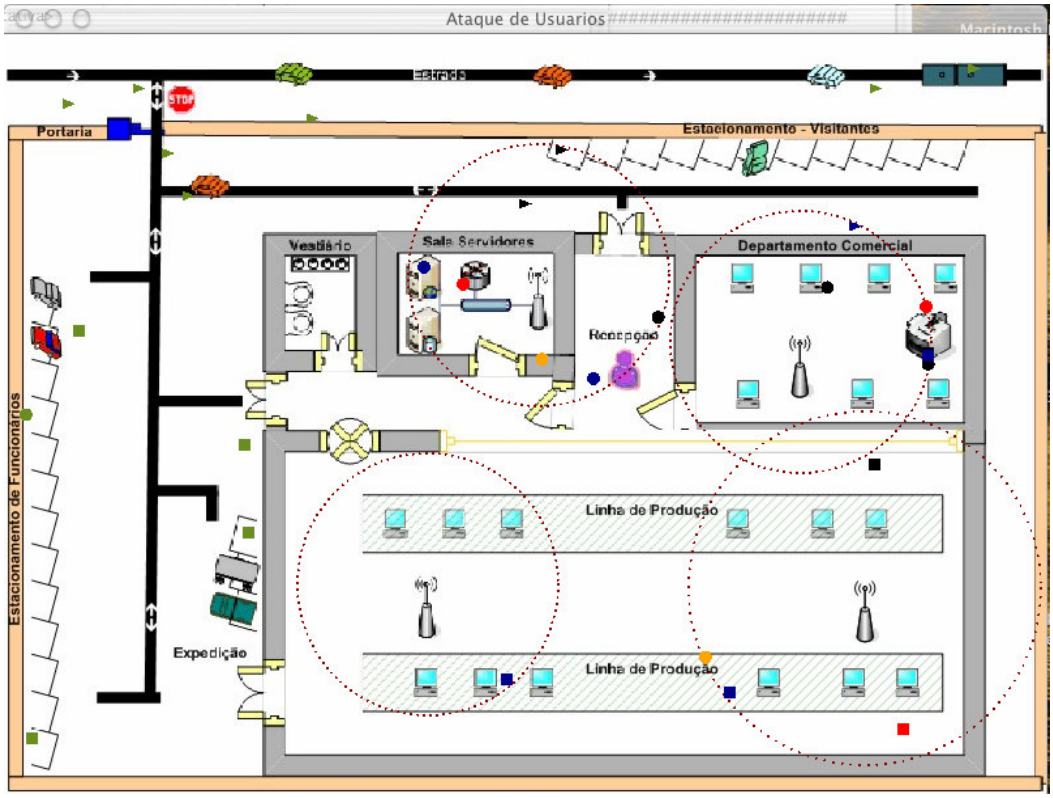

FIGURA 39: INVASÕES SOFRIDAS NO CENÁRIO HIPOTÉTICO 1

Fica claro pela quantidade de invasões sofridas nos equipamentos sem a devida configuração, que independente do ataque, o acesso à rede sem fio possibilita o comprometimento da sobrevivência do sistema, e, por conseguinte a missão crítica, da empresa.

5.6. CENÁRIO HIPOTÉTICO 2

Para este Estudo, foi utilizado o cenário da fábrica adotando-se os 4 Pontos de Acesso com os mesmos valores que representam os equipamentos com as configurações básicas de segurança implementada e recomendada para um usuário com conhecimentos limitados. Essas configurações adotadas foram recomendas e proporcionam uma segurança básica aos equipamentos e a sobrevivência da sem fio.

Adotou-se a quantidade de 10 atores (User, BadUser e Hacker) de cada tipo e simulando por 10 minutos, onde os atores exploraram e fizeram os ataques por procura de sinais (pacotes) na rede pelo SSID porém com o SSID alterado, por captura de pacotes não criptografados por WEP definidas com chaves de 64 bits e por ataques de DoS que se sujeita devido a fraca configuração do Firewall e este ataque quando foi executado com sucesso, foi gerado o ataque de Root Kit explorando vulnerabilidades das configurações e do sistema operacional. Ilustraremos a quantidade e quais foram os ataques sofridos por esses equipamentos com esses parâmetros.

5.6.1. PARÂMETROS DE CONFIGURAÇÃO ASSUMIDOS

Assumiu-se que os equipamentos da rede sem fio, ou seja, os Pontos de Acesso estão com as seguintes configurações:

- Nome da rede sem fio, o SSID foi alterado e implementado um nome de difícil descoberta que combina caracteres, números e caracteres especiais que dificultam a descoberta e habilitado o envio do SSID por sinal sem fio. Para se conectar a esta rede sem fio, basta ligar a conexão de rede que automaticamente o sistema operacional detectará o sinal da rede sem fio.

- O Modo de Segurança da rede sem fio foi configurado para permitir chaves WEP de 64 bits. Por exemplo, a palavra ***UNIMEP*** gera a chave ***17D08A1CD1***.

- E com a utilização de um Firewall com as configurações básicas, ou seja, as principais portas configuradas.

Assumindo-se essas configurações na simulação, foi adotada em cada item de segurança, a **Opção de Falso**, opção que permite o ataque ao componente e torna-se necessário informar a porcentagem mínima (valor) que um ator deverá possuir para conseguir o sucesso no ataque. Esse valor atribuído ao ator é dado aleatoriamente no momento da simulação que pode ser baseada em chances e probabilidade de ataques segundo estudos de organizações credenciadas. Quanto mais recursos de segurança implementados, menores serão as chances de sucesso na invasão, logo, eu devo aumentar a porcentagem dos recursos que são os atributos que determinam se um ator conseguirá ou não o sucesso. Por exemplo, se na simulação um ator estiver com o valor 30, e o recurso estiver configurado para permitir o sucesso com porcentagens acima de 40%, portanto esse ator não conseguirá sucesso na sua invasão. A Tabela 4 descreve os componentes e a porcentagem mínima para ocorrer o sucesso no ataque.

Dispositivo	SSID	WEP	Firewall	Root Kit
Ponto de Acesso 1	Falso = 60%	Falso = 80%	Falso = 50%	Falso = 30%
Ponto de Acesso 2	Falso = 60%	Falso = 80%	Falso = 50%	Falso = 30%
Ponto de Acesso 3	Falso = 60%	Falso = 80%	Falso = 50%	Falso = 30%
Ponto de Acesso 4	Falso = 60%	Falso = 80%	Falso = 50%	Falso = 30%

FALSO: *EFETIVIDADE DE DEFESA (ED).*

% *: INDICADOR DE EFETIVIDADE DE DEFESA DE UM RECURSO.*

TABELA 4: CONFIGURAÇÃO DOS PA´S NO CENÁRIO HIPOTÉTICO 2.

5.6.2. RESULTADOS OBTIDOS DA SIMULAÇÃO

No intervalo de tempo monitorado, ocorreram 30 ataques sendo 11 ataques com êxito em suas tentativas de exploração na falta de configuração e implementação dos recursos de segurança.

Uma classificação sobre os tipos de ataques e as quantidades correspondentes encontram-se nos gráficos abaixo.

Na Figura 40 temos o gráfico que ilustra as quantidades de ataques sofridos do Cenário 2.

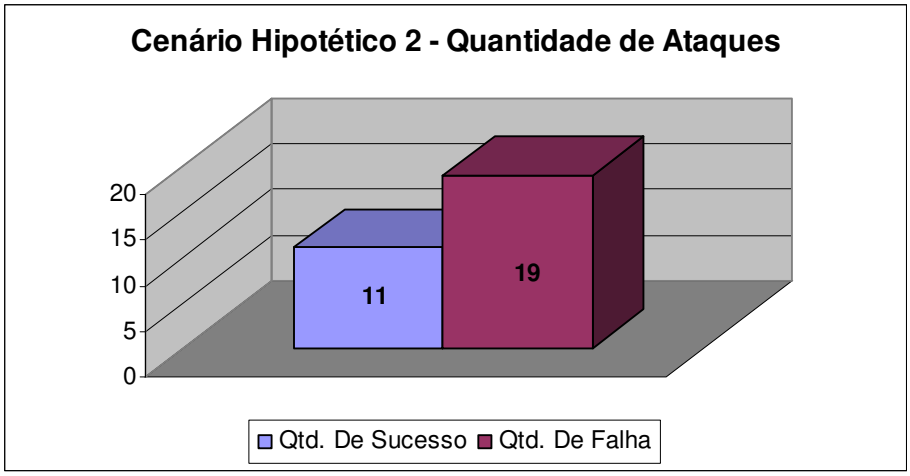

Figura 40: Quantidade de Ataques no Cenário de Uso Hipotético 2

Na Figura 41 temos o gráfico que ilustra as quantidades e os tipos de ataques sofridos do Cenário 2.

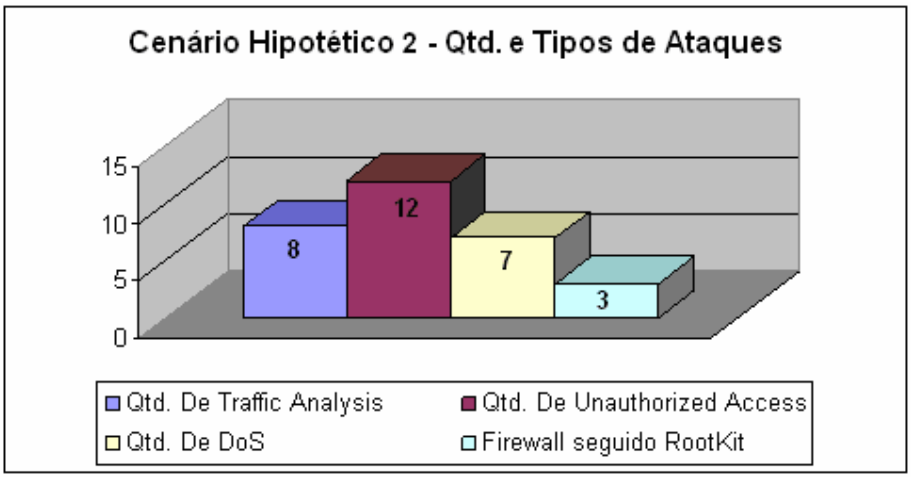

Figura 41: Quantidade e Tipos de Ataques no Cenário de Uso Hipotético 2

5.6.3. CÁLCULO DA VULNERABILIDADE POTENCIAL

Para este Cenário 2, conforme seção 4.3 e aplicando o Passo 4 da Metodologia proposta, o valor da Vulnerabilidade Potencial é **0,37**; onde o Valor da Vulnerabilidade Potencial ideal é 0,0 (Seguro); concluímos um Cenário um pouco vulnerável e principalmente, capaz de manter parte da missão crítica.

A Figura 42 ilustra a planta da fábrica após essas invasões no período de tempo monitorado. Conforme a Tabela 1, os pontos coloridos na Figura 42, representa os variados tipos de atores em execução e ilustram os ataques bem sucedidos e os ataques mal sucedidos ocorridos neste Cenário 2.

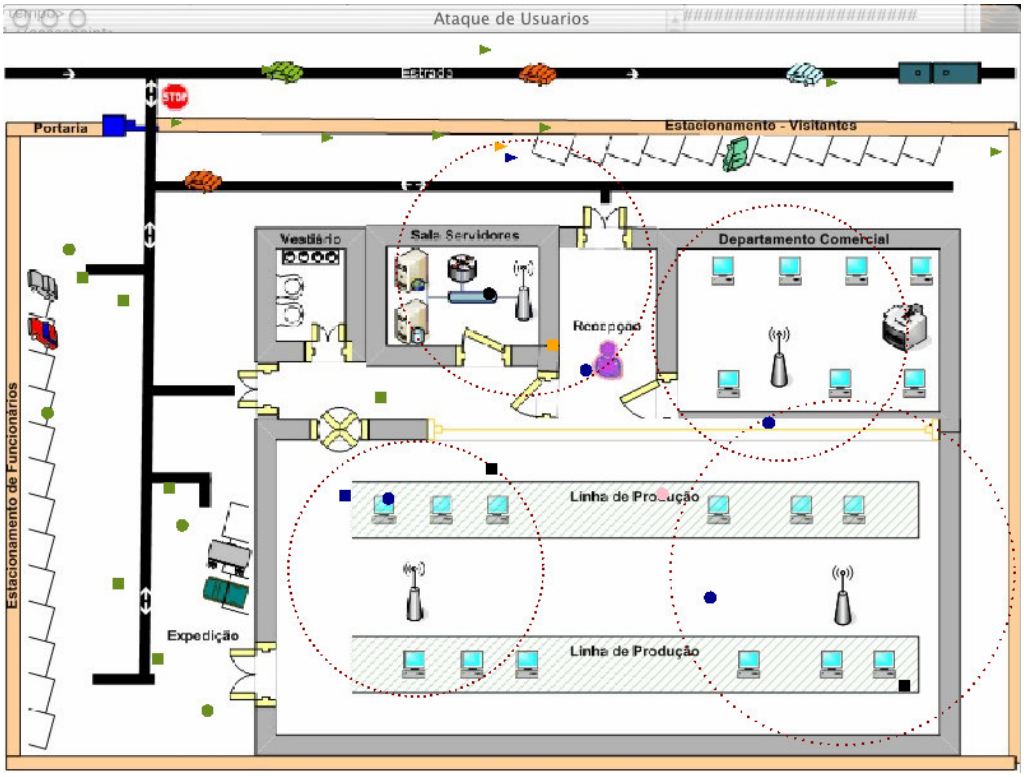

FIGURA 42: INVASÕES SOFRIDAS NO CENÁRIO HIPOTÉTICO 2

Com as medidas de segurança adotada, a quantidade de invasões sofridas foi consideravelmente reduzida. Basicamente foram adotadas medidas de segurança básica, que podem ser implementadas por um usuário responsável. Ocorreram ainda diversos tipos de invasões, mas fica bem visível à diferença entre nenhuma configuração de segurança, e a adoção da configuração básica. Porém, apesar do serviço de rede sem fio continuar ativo, ele permitiu que os servidores fossem "invadidos" por alguns usuários. Portanto, a Missão Crítica do Sistema ainda pode ser comprometida mesmo com estas configurações, indicando que medidas adicionais ainda são necessárias para bloquear possíveis invasões.

5.7. CENÁRIO HIPOTÉTICO 3

Para este Estudo, foi utilizado o cenário da Fábrica adotando-se os 4 Pontos de Acesso com os mesmos valores que representam os equipamentos com as

altas configurações de segurança implementada e recomendada para um administrador de redes. Essas configurações adotadas foram recomendas e proporcionam uma segurança adequada aos equipamentos e a sobrevivência da sem fio.

Lembrando que o surgimento de novas falhas ou problemas é previsível e cabe aos administradores o seu prévio conhecimento e a sua rápida atualização na configuração.

Adotou-se a quantidade de 10 atores (User, BadUser e Hacker) de cada tipo e simulando por 10 minutos, onde os atores exploraram e fizeram os ataques por procura de sinais (pacotes) na rede pelo SSID porém com o SSID alterado, por captura de pacotes não criptografados por WEP definidas com chaves de 128 bits e por ataques de DoS que tentaram passar pelo Firewall que foi bloqueado as portas desnecessária e implementados configurações avançadas. Este ataque de DoS quando foi executado com sucesso, foi gerado o ataque de Root Kit explorando vulnerabilidades das configurações e do sistema operacional. Ilustraremos a quantidade e quais foram os ataques sofridos por esses equipamentos com esses parâmetros.

5.7.1. PARÂMETROS DE CONFIGURAÇÃO ASSUMIDOS

Adotamos que os equipamentos da rede sem fio, ou seja, os Pontos de Acesso estão com as seguintes configurações:

- Nome da rede sem fio, o SSID foi alterado e implementado um nome de difícil descoberta que combina caracteres, números e caracteres especiais que dificultam a descoberta e desabilitado o envio do SSID por sinal sem fio. Para se conectar a esta sem fio será necessário inserir manualmente na estação do usuário o nome do SSID.

- O Modo de Segurança da sem fio foi configurado para permitir chaves WEP de 128 bits. Por exemplo, a palavra ***UNIMEP*** gera a chave ***D315932ABC72C405173C62F396***

- E com a utilização de um Firewall com as portas desnecessárias bloqueadas.

Assumindo-se essas configurações na simulação, foi adotada em cada item de segurança, a **Opção de Falso**, opção que permite o ataque ao componente e torna-se necessário informar a porcentagem mínima (valor) que um ator deverá possuir para conseguir o sucesso no ataque. Esse valor atribuído ao ator é dado aleatoriamente no momento da simulação que pode ser baseada em chances e probabilidade de ataques segundo estudos de organizações credenciadas. Quanto mais recursos de segurança implementados, menores serão as chances de sucesso na invasão, logo, eu devo aumentar a porcentagem dos recursos que são os atributos que determinam se um ator conseguirá ou não o sucesso. Por exemplo, se na simulação um ator estiver com o valor 30, e o recurso estiver configurado para permitir o sucesso com porcentagens acima de 40%, portanto esse ator não conseguirá sucesso na sua invasão. A Tabela 5 descreve os componentes e a porcentagem mínima para ocorrer o sucesso no ataque.

Dispositivo	SSID	WEP	Firewall	Root Kit
Ponto de Acesso 1	Falso = 90%	Falso = 95%	Falso = 90%	Falso = 80%
Ponto de Acesso 2	Falso = 90%	Falso = 95%	Falso = 90%	Falso = 80%
Ponto de Acesso 3	Falso = 90%	Falso = 95%	Falso = 90%	Falso = 80%
Ponto de Acesso 4	Falso = 90%	Falso = 95%	Falso = 90%	Falso = 80%

FALSO: *EFETIVIDADE DE DEFESA (ED).*

% *: INDICADOR DE EFETIVIDADE DE DEFESA DE UM RECURSO.*

TABELA 5: CONFIGURAÇÃO DOS PA´S NO CENÁRIO HIPOTÉTICO 3

5.7.2. RESULTADOS OBTIDOS DA SIMULAÇÃO

No intervalo de tempo monitorado, ocorreram 189 ataques sendo 23 ataques com êxito as suas tentativas de exploração na falta de configuração e implementação dos recursos de segurança.

Uma classificação sobre os tipos de ataques e as quantidades correspondentes encontram-se nos gráficos abaixo.

Na Figura 43 temos o gráfico que ilustra as quantidades de ataques sofridos do Cenário 3.

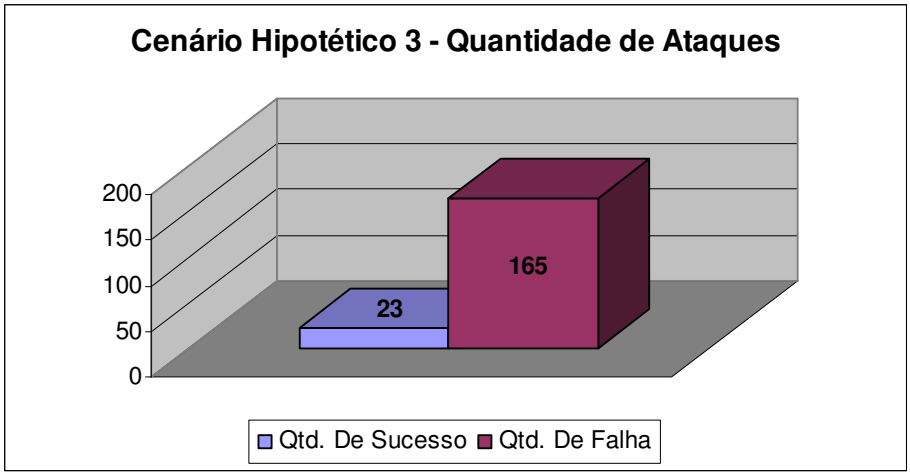

FIGURA 43: QUANTIDADE DE ATAQUES NO CENÁRIO HIPOTÉTICO 3

Na Figura 44 temos o gráfico que ilustra as quantidades e os Tipos de Ataques sofridos do Cenário 3.

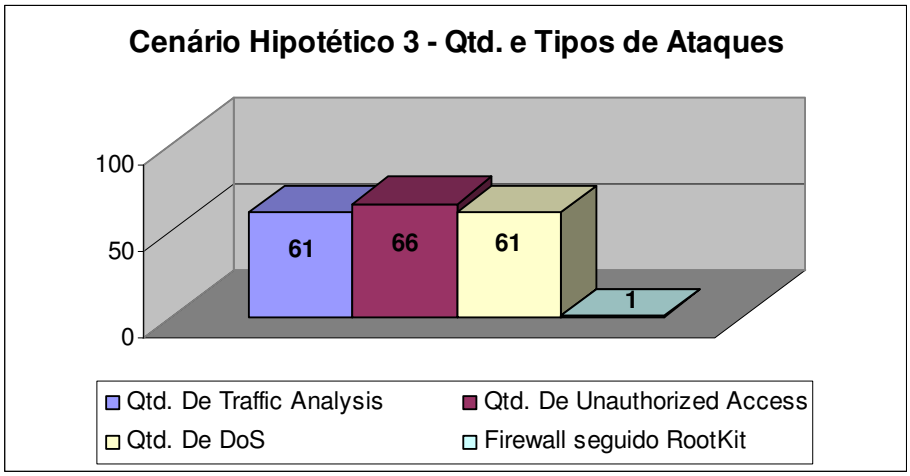

FIGURA 44: QUANTIDADE E TIPOS DE ATAQUES NO CENÁRIO HIPOTÉTICO 3

5.7.3. CÁLCULO DA VULNERABILIDADE POTENCIAL

Para este Cenário 3, conforme seção 4.3 e aplicando o Passo 4 da Metodologia Proposta, o valor da Vulnerabilidade Potencial é **0,12**; onde o Valor da Vulnerabilidade Potencial ideal é 0,0 (Seguro); concluímos um Cenário vulnerável e principalmente, incapaz de manter a missão crítica.

A Figura 45 ilustra a planta da fábrica após essas invasões no período de tempo monitorado. Conforme a Tabela 1, os pontos coloridos na Figura 45, representa os variados tipos de atores em execução e ilustram os ataques bem sucedidos e os ataques mal sucedidos ocorridos neste Cenário 3.

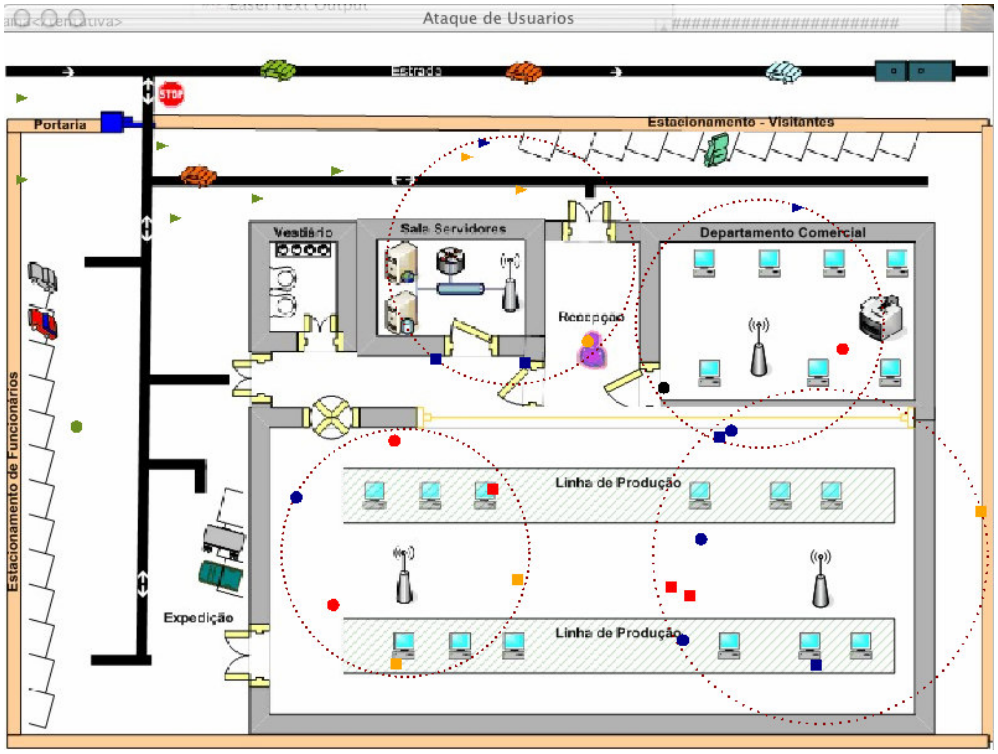

FIGURA 45: INVASÕES SOFRIDAS NO CENÁRIO HIPOTÉTICO 3

Apesar configurações adotadas serem efetivas na grande maioria dos casos, ainda existem vulnerabilidades passíveis de serem explorados. No caso, 1% pode ser ou não um número elevado para os padrões de segurança da empresa. A decisão sobre implementar medidas adicionais passa a depender mais de decisões gerenciais da empresa, e não apenas técnicas.

Com essas configurações conseguimos simular o quão seguro o sistema estará em face a ataques à sem fio. Pode-se ainda inferir que um dado nível de segurança possui um custo correspondente e proporcional. Porém, esses custos podem torna-se muitos maiores e elevados caso uma invasão seja bem sucedida.

6. CONCLUSÕES

Este trabalho apresentou uma metodologia para a simulação de ambientes computacionais utilizando redes sem fio. Foram abordados aspectos de segurança que apesar de conhecidos, são muitas vezes ignorados. Apesar disso, muitas vezes são vitais para a sobrevivência de sistemas de missão crítica da empresa. O Método do Cálculo da Vulnerabilidade Potencial adotado é baseada na ferramenta EASEL, que possui uma linguagem de simulação particularmente apropriada para análise de problemas dessa natureza.

Constatou-se a adequação da metodologia como elemento auxiliar para administradores de redes e gerentes de negócios responsáveis pela sobrevivência de sistemas de missão critica da empresa. De certa forma a metodologia apresentada permite que se quantifiquem previsões subjetivas no que diz respeito à segurança de um sistema.

A principal vantagem da metodologia está no seu poder de simular a interação entre diversos recursos e atores de modelos complexos. Os modelos empregados muitas vezes, refletem a quase impossibilidade de se adotar uma solução analítica para o problema. Uma vantagem adicional é o uso de uma interface visual para o acompanhamento da simulação. Isso pode facilitar a comunicação entre técnicos, usuários e gerentes, que geralmente não estão acostumados a analisar situações de riscos em ambientes computacionais, pelo simples fato de acharem seus ambientes seguros devido às medidas convencionais adotadas. Além disso, a metodologia empregada neste trabalho pode ser utilizada em outras aplicações que apresentem as mesmas características definidas anteriormente.

Entretanto encontramos algumas limitações na aplicação da metodologia. Dentre elas, podemos destacar as seguintes:

- A falta de estudos e dados sobre tipos de ataques, e porcentagens reais de invasão. Esses são parâmetros fundamentais para a obtenção de resultados confiáveis.

- A necessidade do conhecimento do modelo e recursos de simulação disponibilizados pela ferramenta. Isto pode inibir o seu uso por parte de administradores e gerentes de sistemas.

- A pouca documentação e pequeno número de exemplos disponíveis.

- A necessidade do uso de um computador Macintosh para executar a ferramenta EASEL.

Como trabalho futuro, seria de grande interesse, o desenvolvimento de um questionário visando esclarecer sobre os diferentes usos de redes sem fio adotadas por empresas, bem como problemas referentes a segurança das mesmas. Isso possibilitaria a aplicação mais precisa desta metodologia para quantificar, e possivelmente melhorar o nível de segurança de seus ambientes computacionais.

Seria interesse também o desenvolvimento de uma interface gráfica que facilitasse a modelagem dos sistemas a serem simulados. Exemplificando, poderia ser disponibilizado algum recurso para a importação de modelos para formas de invasão diversas, métodos de detecção, e custos associados. Isso poderia ser aplicado a quaisquer cenários usuários com poucos conhecimentos da ferramenta, permitindo ao mesmo simular determinados cenários, com a conseqüente geração de relatórios para análise técnica e gerencial.

Finalmente, seria bastante útil implementar a ferramenta de simulação para o ambiente PC-Linux, já que equipamentos Macintosh ainda são relativamente incomuns e caros.

Referências Bibliográficas

[3COM00] Technical Paper, IEEE 802.11b Wireless LANs Wireless Freedom at Ethernet Speeds, 2000.

[CHEN99] Yen-Ming, “Study of the interdependencies within the banking and finance infrastructure for survivability research”, Submitted to the Information Networking Institute in Partial Fulfillment of the Requirements for the degree Master of Science in Onformation Networking, Pittsburgh, Pennsylvania, 1999.

[CHRISTIE02] Alan M. C., “Network Survivability Analysis Using Easel”, Technical Report CMU/SEI-2002-TR-039 e ESC-TR-2002-039, Networked Systems Survivability Program, December 2002.

[EFL99] R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T.A. Longstaff, N.R. Mead, “Survivable Network Systems: An Emerging Discipline,” Proceedings of the 11th Canadian Information Technology Security Symposium (CITSS), Ottawa, Ontário Canada, May 10-14, 1999, Communications Security Establishment, 1999.

[ELDER98] Matthew E. Elder, “Major Security Attacks on Critical Infrastructure Systems”, Topics in Survivable Systems, Computer Science Report No. CS-98-22, University of Virginia, August 1998.

[ELLISON99] Robert J. Ellison, Richard C. Linger, Thomas Longstaff, and Nancy R. Mead, “Technical Report: Survivable Network System Analysis: A Case Study”, (condensed version of SEI Technical Report CMU/SEI-98-TR-014, ESC-TR-98-014) published in July/August 1999 issue of IEEE Software.

[ENGST05] Adam e Glenn Fleishman, “Kit do Iniciante em Redes Sem Fio – O guia prático sobre redes Wi-fi para Windows e Macintosh”, 2ª Edição, Editora Pearson Makron Books, 2005.

[FERNANDES01] Fernandes, Almir, “Administração Inteligente”, Editora Futura, São Paulo, 2001.

[FISHER99B] D. Fisher, “Design and Implementation of EASEL- A Language for Simulating Highly Distributed Systems”, Proceedings of MacHack 14, the 14th Annual Conference for Leading Edge Developers. Deerborn, MI, USA, 1999.

[FISHER99] D. Fisher, H. Lipson, “Emergent Algorithms – A New Method for Enhancing Survivability in Umbounded Systems”, Proceedings of the Hawaii International Conference on System Sciences. Maui, HI, USA, 1999.

[KAHANI] Mohsen Kahani, H.W. Peter Beadle, Artigo “Decentralised Approaches for Network Management”, The Institute for Telecommunication Research (TITR)

[LINKSYS] A Division of Cisco Systems, Inc. – Empresa do hardware utilizado.

[LIPSON99] H. Lipson, D. Fisher, “Survivability- A New Technical and Business Perspective on Security”, Proceedings of the 1999 New Security Paradigms Workshop. Caledon Hill, ON, USA, 1999.

[NAKAMURA02] E. T. e GEUS, P. L., “Segurança de Redes em Ambientes Cooperativos”, Berkeley, 2002.

[MMARTINS03] M., “Protegendo Redes Wireless 802.11b”, Módulo Security, 2003.

[PUTTINI00], Ricardo S.; SOUZA, Rafael T. de. Principais Aspectos da Segurança, acessado em http://webserver.redes.unb.br/security/introducao/aspectos.html - Acessado em 17/03/2006.

[ZHANG] Yongguang Zhang Harrick Vin Lorenzo Alvisi, Wenke Lee e Son K. Dão, “Heterogeneous Networking: A New Survivability Paradigm”.

Bibliografia

Nikita Borisov; Goldberg, I.; Wagner, D. “Security of the WEP algorithm”, UC Berkeley.

White Paper “Strong Wireless LAN Security: A Reality Today”, INTEL, 2004.

James F. Kurose e Keith W. Ross, “Redes de Computadores e a Internet – Uma abordagem top-dow”, 3ª edição, Editora Pearson Addison Wesley, 2006.

D. Molta, “WLAN Security On The Rise” www.networkcomputing.com

8ª Pesquisa Nacional sobre Segurança da Informação, Módulo, 2001.

F. A. B. Pelissari, “Segurança de Redes e Analise sobre a conscientização das empresas da cidade de Bauru (SP) quanto ao problema”, no site www.modulo.com.br/index.jsp, UNESP, 2002.

Nelson M. Rufino O., “Segurança em Redes sem Fio” Novatec Editora, 2005.

F. Simão, Apresentação sobre Segurança Wireless no Congresso Regional de Auditoria de Sistemas e Segurança da Informação realizada na cidade do Rio de Janeiro nos dias 31/03 e 01/04/2003, CNASI 2003.

STANG, D. J. e MOON, S., “Segredos de Segurança em Redes”, IDG Books, 1994.

Andrew S. Tanenbaum, “Redes de Computadores”, 3ª edição , Campus, 1997.

J.H. Teixeira, J.P. Suave, J. A B. Moura, S. Q. R. Teixeira “Redes de Computadores”., Makron Books.

J. Walker, “Unsafe at any key size; An Analysis of the WEP encapsulation”

http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

802.11 Wireless Networks: The Definitive Guide. Matthew Gast. O'Reilly, 2002.

LISTA DE WEB SITES RELACIONADOS

http://www.sei.cmu.edu/community/easel/examples.html - Índice de Recursos do processo de simulação do Easel – Acessado em 27/03/2006.

http://www.sei.cmu.edu/community/easel - Easel Survivability Simulation – Acessado em 26/03/2006.

http://airtraf.sourceforge.net - Ferramenta AirTraf - Acessado em 05/01/2006.

http://sourceforge.net/projects/airsnort - Ferramenta Airsnort - Acessado em 05/01/2006.

http://www.kismetwireless.net - Ferramenta Kismet – Acessado em 05/01/2006.

http://ntsecurity.nu/toolbox/etherchange - Ferramenta para alterar o MAC - Acessado em 05/01/2006.

http://www.wlsec.net/void11 - Ferramenta de Negação de Serviço – Acessado em 05/01/2006.

http://www.contingencia.com.br – Empresa de Consultoria em Continuidade dos Negócios conforme a ISO 17799. – Acessado em 17/03/2006.

http://www.drii.org – Disaster Recovery Institute – Acessado em 17/03/2006.

http://www.nist.gov – National Institute of Standards and Technology – Acessado em 17/03/2006.

http://www.defcon.org – Evento de Hacker – Acessado em 17/03/2006.

http:// www.netstumbler.org – Ferramenta para capturar sinal SSID – Acessado em 17/03/2006.

http://www.kismetwireless.net – Ferramenta para quebrar chave WEP. – Acessado em 17/03/2006.

http:// www.worldpath.net/~minstrel/hobosign.htm - Sinais Hobo - Acessado em 17/03/2006.

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html - Informações adicionais da quebra da chave Wep. – Acessado em 17/03/2006.
http://sourceforge.net/projects/wepcrack - Ferramenta para cracks Wep 802.11 – Acessado em 17/03/2006.

http://www.ethereal.com/ - Ferramenta de análise e gerenciamento de redes – Acessado em 17/03/2006.

http://ee.lbl.gov/ - Página da Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL) in Berkeley, California – Acessado em 17/03/2006.

http://www.antivirus.com – Página do Fabricante de Antivírus da Trend – Acessado em 17/03/2006.

http://www.professorglobal.com.br/texto.php?id_texto=175 – Explicação da Fórmula da Circunferência - Acessado em 22/03/2006.

http://www.cert.org/annual_rpts/cert_rpt_02.html - CERT® Coordination Center 2002 Annual Report – Acessado em 26/03/06.

http://www.sysinternals.com/Utilities/RootkitRevealer.html - RootkitRevealer é um avançado utilitário para detector rootkit.

http://www.rootkit.com - The Online Rootkit Magazine – Acessado em 26/03/2006.

http://br-linux.org/artigos/segur_intro.htm - Revista do Linux – Acessado em 26/03/2006.

http://www.cert.org/research/papers.html#emergent – Artigos do CERT.

APÊNDICE 1 – O CÓDIGO E A INTERFACE DA SIMULAÇÃO DESENVOLVIDA

```
# ####################################################################

include "::libraries:physical.easel";

# ####################################################################

TSimulacao : simulation type is

      vw::view :=?;

      ListUser::list := new list any;

      ListAcessPoint::list :=new list any;

      nTotAt::number := 0;
      nTotSuc::number := 0;
      nTotErr::number := 0;
      totAp1::number := 0;
      totAp2::number := 0;
      totAp3::number := 0;
      totAp4::number := 0;
# ####################################################################

TAcessPoint(xPA:int, yPA:int, rPA:int, bolSsid:boolean,
bolWep:boolean, bolFirewall:boolean,
bolRootKit:boolean,idAcessPoint:int, chanceTrafAnal:number,
chanceUnAcess:number, chanceDos:number, chanceRootKit:number ) : actor
type is

      dblx::number := ?;

      dbly::number := ?;

      dbli::number := 0;

      iTotal::number := 2*pi;

      push (sim.ListAcessPoint,self);

      for every dbli <= iTotal do

            dblx := rPA * cos dbli;

            dbly := rPA * sin dbli;

            depict(sim.vw,var offset_by(paint(circle(0.0,0.0,2.0),
darkred), var dblx+xPA, var dbly+yPA));

            dbli := dbli + 0.05;

      wait 1.0;

# ####################################################################

TypeUser : type is enum (tuCommonUser, tuBadUser, tuHacker);
```

```
# ######################################################################

TypeAttack : type is enum (taTrafAnalysis, taUnAccess, taDos);

# ######################################################################

TUser2(t:TypeUser,x1:int, y1:int, x2:int, y2:int) : actor type is

      n::number :=1;

      posicao::number := ?;
      xOld::number := ?;
      yOld::number := ?;
      myColor:: pattern := olivedrab;
      bolSucesso::boolean := false;
      tUsuario::number := ?;
      xCurrent::number := random (uniform,x1,x2);

      yCurrent::number := random (uniform,y1,y2);

      ta::TypeAttack := taDos;
      AtaqueOk::number := 0;
      simTime::number :=0.0;
      push (sim.ListUser,self);

      if t = tuBadUser then
            tUsuario := 1;
            depict(sim.vw,var offset_by(paint(rectangle(-4.5,4.5,4.5,-
4.5), var myColor),var xCurrent, var yCurrent));

      else
            if t = tuHacker then
                  tUsuario := 2;
                  depict(sim.vw,var
offset_by(paint(polygon(0.0,4.0,10.0,0.0,0.0,-4.0), var myColor),var
xCurrent, var yCurrent));
            else
                  tUsuario := 3;
                  depict(sim.vw,var
offset_by(paint(circle(0.0,0.0,10.0), var myColor),var xCurrent, var
yCurrent));
      wait 1.0;
      for every true do
            xOld := xCurrent;
            yOld := yCurrent;
            if !bolSucesso then
                  changePosition(self);
            for p : each sim.ListAcessPoint do

                  posicao := sqrt((p.xPA - xCurrent)^2 + (p.yPA -
yCurrent)^2);

                  if ( posicao <= p.rPA ) then
                        if !bolSucesso then
                              randomicAttack(self);
                              AtaqueOk:=AttackValidation(self,p);
                  else
                        AtaqueOk := 0;
                  wait 3.0;
```

```
# ######################################################################

AttackValidation(u: TUser2, p: TAcessPoint) : action is
      nChance::number := ?;
      nChanceNovo::number := ?;
      bolOk::number := 0;
      nTipo::number := 0;
      nPor::number := 0;
      tempo::number := 0;
      nChance := random(uniform, 1.0, 10.0);
      nChanceNovo := random(uniform, 1.0, 10.0);
      if u.ta=taTrafAnalysis then
            if (!p.bolSsid & nChance>p.chanceTrafAnal) then      # se
nao tiver a protecao SSID...
                  u.bolSucesso := true;
                  u.myColor := darkblue;                    # consegue
atacar...
                  bolOk := 1;
                  nTipo := 1;
                  calculoAttack(u,p,u.bolSucesso);

            else
                  nTipo := 1;
                  u.myColor := blue;                        # nao tem
sucesso
                  calculoAttack(u,p,u.bolSucesso);
      if u.ta=taUnAccess then
            if (!p.bolWep & nChance>p.chanceUnAcess) then        # se
tiver a protecao Wep...
                  u.bolSucesso := true;
                  u.myColor := orange;                      # consegue
atacar...
                  bolOk := 1;
                  nTipo := 2;
                  calculoAttack(u,p,u.bolSucesso);
            else
                  nTipo := 2;
                  u.myColor := yellow;                      # nao tem
sucesso
                  calculoAttack(u,p,u.bolSucesso);
      if u.ta=taDos then
            if (!p.bolFirewall & nChance>p.chanceDos) then # se tiver
a protecao Firewall..
                  if (!p.bolRootKit & nChanceNovo>p.chanceRootKit) then
                        u.bolSucesso := true;
                        u.myColor := black;
                        bolOk := 1;
                        nTipo := 4;
                        calculoAttack(u,p,u.bolSucesso);
                  else
                        u.bolSucesso := true;
                        u.myColor := red;                       #
consegue atacar...
                        bolOk := 1;
                        nTipo := 3;
                        calculoAttack(u,p,u.bolSucesso);
            else
                  nTipo := 3;
                  u.myColor := pink;                        # nao tem
sucesso
```

```
                  calculoAttack(u,p,u.bolSucesso);
      output("<ataque>\cr");
      nPor := round(nChance * 10);
      sim.nTotAt := sim.nTotAt + 1;
      tempo := ceil(u.simTime / 10);
      output("<porcetagem>",nPor,"%</porcetagem>\cr");
      output("<tempo>",tempo,"</tempo>\cr");
      output("<acesspoint>",p.idAcessPoint,"</acesspoint>\cr");
      if nTipo = 1 then
            output("<tipo>Traffic Analysis</tipo>\cr");
      if nTipo = 2 then
            output("<tipo>Unauthorized Access</tipo>\cr");
      if nTipo = 3 then
            output("<tipo>DoS</tipo>\cr");
      if nTipo = 4 then
            output("<tipo>Firewall seguido RootKit</tipo>\cr");
      if u.tUsuario = 1 then
            output("<usuario>Bad User</usuario>\cr");
      if u.tUsuario = 2 then
            output("<usuario>Hacker</usuario>\cr");
      if u.tUsuario = 3 then
            output("<usuario>Common User</usuario>\cr");
      if u.bolSucesso then
            output("<tentativa>sucesso</tentativa>\cr");
      else
            output("<tentativa>falha</tentativa>\cr");
      output("</ataque>\cr");
      return bolOk;
# ######################################################################
changePosition(p: TUser2) : action is
      xTime::number := ?;

      yTime::number := ?;

      xPass::number := ?;

      yPass::number := ?;

      xNew ::number := ?;

      yNew ::number := ?;

      xTime := random (uniform,0.0,1.0);

      yTime := random (uniform,0.0,1.0);

      if xTime >= 0.5 then

            xPass := 5;

      else

            xPass := -5;
      if yTime >= 0.5 then

            yPass := 5;
      else

            yPass := -5;
      xNew := p.xCurrent+xPass;
```

```
      yNew := p.yCurrent+yPass;

      if xNew>=p.x1 & xNew<p.x2 & yNew>=p.y1 & yNew<p.y2 then

            p.xCurrent := xNew;

            p.yCurrent := yNew;

# ######################################################################
randomicAttack(p: TUser2) : action is
      num::number :=?;
      num := rand(1, 3);
      if num=1 then
            p.ta := taTrafAnalysis;
      else
            if num=2 then
                  p.ta := taUnAccess;
            else
                  p.ta := taDos;

      p.simTime := clock();
# ######################################################################
calculoAttack(u: TUser2, p: TAcessPoint, bolTentativa: boolean) :
action is
      total::int := 0;
      if (p.idAcessPoint == 1) then
            total := sim.totAp1;
            total := total + 1;
            sim.totAp1 := total;
      if (p.idAcessPoint == 2) then
            total := sim.totAp2;
            total := total + 1;
            sim.totAp2 := total;
      if (p.idAcessPoint == 3) then
            total := sim.totAp3;
            total := total + 1;
            sim.totAp3 := total;
      if (p.idAcessPoint == 4) then
            total := sim.totAp4;
            total := total + 1;
            sim.totAp4 := total;
# ######################################################################
drawSim(s:TSimulacao) : action is
      s.vw:=new view (s, "Ataque de Usuarios",(silver),nil);
      null make_window(s.vw,vector(100,100,900,700));
      depict(s.vw, picture("::Graphics:PlantaFabrica.pct"));

# ######################################################################

simulate(): action is
      n::number := 1;
      tempo::number := 0;
      tempos::number := 0;
      quantidade::number := 0;
      TempoReal :: number := 600; # Tempo real que vai ser a simulacao
(relogio)
      # QuantosSegundosReaisValeASimulacao :: number := 5.0;
      output("<?xml version='1.0' encoding='ISO-8859-1'?>\cr");
      output("<easel>\cr");
```

```
      output("<cabecalho>\cr");
      output("<titulo> </titulo>\cr");
      output("<descricao>Simulacao de ataque a uma rede Wireless
</descricao>\cr");
      output("<contact>Ricardo Slavov </contact>\cr");
      output("</cabecalho>\cr");
      output("<tipos>\cr");
      output("<metodo>\cr<nome>Traffic
Analysis</nome>\cr<descricao>Ataque aonde o usuario procura por sinais
(pacotes) na rede, pelo SSID padrao</descricao>\cr</metodo>\cr");
      output("<metodo>\cr<nome>Unauthorized
Access</nome>\cr<descricao>Ataque aonde o usuario captura pacotes nao
criptografados (wep)</descricao>\cr</metodo>\cr");
      output("<metodo>\cr<nome>DoS</nome>\cr<descricao>Ataque aonde o
usuario explora a ausencia de firewall</descricao>\cr</metodo>\cr");
      output("</tipos>\cr");
      output("<simulacao>\cr");
      s::TSimulacao := new TSimulacao;

      (s.skdr).speed := 10.0; # Proporcao de tempo entre a simulacao e
o tempo real
      # 10.0 equivale a proporcionalmente 1:1 (um real para um da
simulacao)
      # 5.0 equivale a proporcionalmente 1:0.5 (um real para metade de
um na simulacao - dois reais para 1 de simulacao)
      null new (s,TAcessPoint(410,184,100, false, false, false, false,
1, 9,9.5,9,8));   # Sequencia de Parametros: PosicaoX, PosicaoY, Raio,
ssId, Wep, Firewall, Rootkit, Id, ChanceSSID, ChanceWep, ChanceDos,
ChanceRootKit
      null new (s,TAcessPoint(611,235,100, false, false,false, false,
2, 9,9.5,9,8));
      null new (s,TAcessPoint(325,420,100, false, false, false, false,
3, 9,9.5,9,8));
      null new (s,TAcessPoint(660,423,135, false, false, false, false,
4, 9,9.5,9,8));
# Na criacao dos access points acima, se o for "false", o ataque eh
permitido, se for "true" o ataque eh bloqueada.
            # Quantidade de Usuarios, ...random ( uniform, X.0, Y.0) do
      # X: Quantidade minima de usuarios
      # Y: Quantidade maxima de usuarios
      # ps: ele sempre cria 1 usuario, para cada "usuario"
especificado

      quantidade := 10; # Quantidade de usuarios criados, para 1
definido, ele criacao 1 CommonUser, 1 BadUser e um Hacker.

      for every n <= quantidade do
            null new (s,TUser2(tuHacker,5,5,790,150));
            null new (s,TUser2(tuCommonUser,15,160,790,550));
            null new (s,TUser2(tuBadUser,15,160,790,550));
            n := n + 1;

      # Funcao para desenhar fundo, e criar a janela para simulacao

      drawSim(s);

      wait TempoReal;
      pause();
      tempo := ceil((s.skdr).clock / 10);
      tempos := ceil(rtc());
```

```
output("</simulacao>\cr");
output("<resultado>\cr");
output("<tempodesimulacao>",tempo,"</tempodesimulacao>\cr");
output("<tempodeexecucao>",tempos,"</tempodeexecucao>\cr");
output("<acesspoint1>\cr");
output("<totalataques>",s.totAp1,"</totalataques>\cr");
output("</acesspoint1>\cr");
output("<acesspoint2>\cr");
output("<totalataques>",s.totAp2,"</totalataques>\cr");
output("</acesspoint2>\cr");
output("<acesspoint3>\cr");
output("<totalataques>",s.totAp3,"</totalataques>\cr");
output("</acesspoint3>\cr");
output("<acesspoint4>\cr");
output("<totalataques>",s.totAp4,"</totalataques>\cr");
output("</acesspoint4>\cr");
output("</resultado>\cr");
output("</easel>\cr");
simulate();
#Final
```

A Figura 41 ilustra a ferramenta Easel em execução, gerando o Log e salvando as posições da movimentação dos atores pela planta da fábrica.

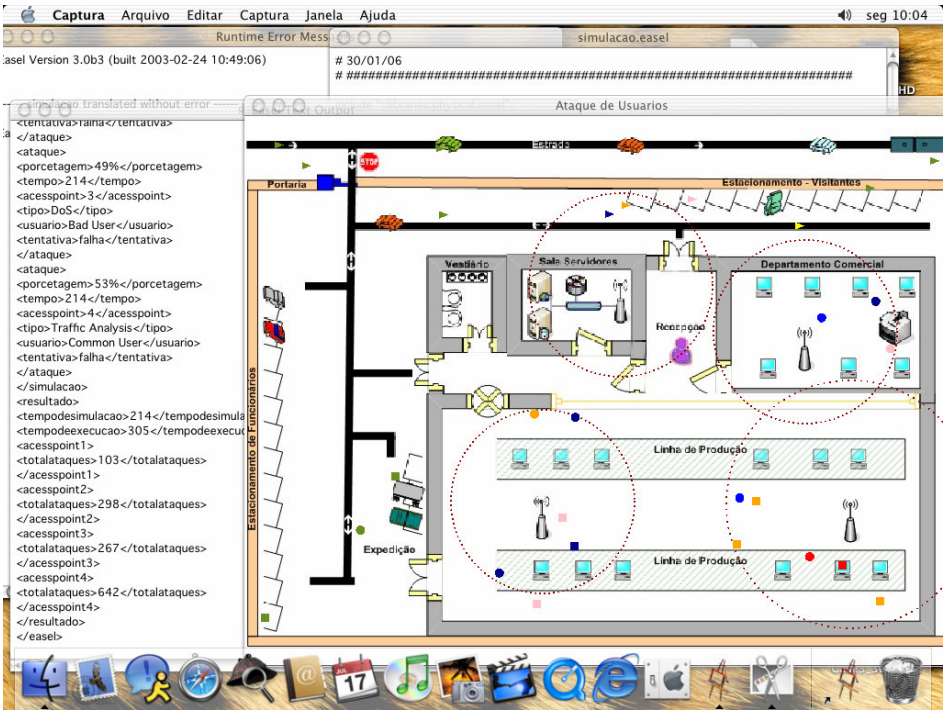

FIGURA 46: INTERFACE DO EASEL SENDO EXECUTADA NO MACINTOSH