

FACULDADE LOURENÇO FILHO
CLAUDEMIR DA COSTA QUEIROZ

SEGURANÇA DIGITAL: UM ESTUDO DE
CASO

FORTALEZA

2007

FACULDADE LOURENÇO FILHO

CLAUDEMIR DA COSTA QUEIROZ

SEGURANÇA DIGITAL: UM ESTUDO DE CASO

Trabalho apresentado como exigência parcial para obtenção do grau de Bacharel em Ciência da Computação à comissão julgadora da Faculdade Lourenço Filho sob orientação do Prof. Msc. William de Araújo Sales.

Orientador: Prof. M.sc WILLIAM DE ARAÚJO SALES

**Fortaleza
2007**

MONOGRAFIA APRESENTADA À COORDENAÇÃO DO CURSO DE CIÊNCIA DA COMPUTAÇÃO DA FACULDADE LOURENÇO FILHO, INTITULADA, SEGURANÇA DIGITAL: UM ESTUDO DE CASO, COMO REQUISITO PARA OBTENÇÃO DO GRAU DE BACHAREL EM CURSO DE CIÊNCIA DA COMPUTAÇÃO.

POR: CLAUDEMIR DA COSTA QUEIROZ

APROVADA EM 26 / 02 /2007

BANCA EXAMINADORA CONSTITUÍDA DOS SEGUINTE PROFESSORES

Prof. Msc. William de Araújo Sales

ORIENTADOR

Prof. Msc. Valneide Cabral

Prof. Dr. Antônio Clécio Fontelles Thomaz

Aos meus pais José Aldemir e Osmira Vieira que sempre lutaram para me proporcionar o prazer de poder estudar. À minha esposa Janayna e à minha filha Karollyne que fazem parte imprescindível na minha vida.

AGRADECIMENTOS

A DEUS, que me deu de presente este curso de bacharelado.

À minha esposa Janayna que sempre e incondicionalmente me apoiou e acreditou em mim.

À minha filha, Karollyne, sempre minha maior motivação para viver, agradeço a compreensão, atenção e amor.

Ao meu orientador Prof. William Sales, por seu apoio contínuo que me conduziu ao término deste trabalho.

Aos Professores da graduação que estiveram presentes em minha vida acadêmica.

Ao Prof. José Maurício da Silva pelas inestimáveis contribuições e sugestões práticas durante a elaboração deste trabalho.

À Faculdade Lourenço Filho pelo apoio e, especialmente, aos colegas e amigos da graduação.

Resumo

Esta pesquisa é um estudo de caso que trata de problemas relacionados ao mundo da segurança em redes de computadores. Nele, o leitor pode encontrar além de outros, discussões sobre os mais importantes temas que englobam o assunto. A questão sobre os fundamentos da segurança intra-rede, os invasores e suas motivações, os objetivos da segurança de rede e dos sistemas, as vulnerabilidades a que um sistema pode estar submetido, os conceitos de vulnerabilidade, as diferenças entre ameaças e vulnerabilidade do sistema, os paradigmas de segurança em sistemas operacionais de uso corrente, itens específicos da linguagem da programação, diagnóstico de segurança do ambiente computacional, ferramentas de pesquisa a vulnerabilidades e por último o estudo de caso no qual é demonstrado que foram encontradas falhas no sistema de segurança da empresa testada como, por exemplo, a presença de um antivírus não atualizado e proposição de possíveis soluções para esse problema.

Palavras-chave: Ciência da Computação – Segurança digital – *hackers* – *cracker* – vulnerabilidades – *software* pirata.

Ora a fé é a certeza de cousas que se esperam, a convicção de fatos que se não vêem.

Hebreus 11.1.

Sumário

Lista de Ilustrações

Quadros, ix

Figuras, x

Resumo, xi

Abstract, xii

Introdução

1. ASPECTOS GERAIS SOBRE SEGURANÇA DA INFORMAÇÃO

1.1 Fundamentos de segurança, 16

1.1.1 Abrangência da segurança digital, 18

1.1.2 A contextualização, 20

1.1.3 Considerações sobre segurança digital, 21

1.1.4 Os invasores e motivações, 22

1.1.5 Consequências de invasões, 25

1.1.6 Objetivos da Segurança de redes e Sistemas, 27

2. ASPECTO SOBRE VULNERABILIDADES

2.1 Conceitos de vulnerabilidade, 29

2.2 Diferenciando entre ameaças e vulnerabilidades, 31

2.3 Vulnerabilidades em servidores *Web*, 32

2.4 Paradigmas de segurança em sistemas operacionais de uso corrente, 34

2.5 Vulnerabilidades em programação *Web*, 36

2.6 Itens específicos da Linguagem computacional, 37

3.FERRAMENTAS DE DETECÇÃO DAS VULNERABILIDADES

3.1 Diagnóstico de segurança do ambiente computacional, 40

3.2 Ferramentas de pesquisa a vulnerabilidades, 41

4. ESTUDO DE CASO

4.1 Passos da pesquisa, 50

4.2 Objetivos da pesquisa, 50

4.3 Hipótese, justificativa, metodologia e procedimentos, 51

4.4 Coleta de dados, 52

4.5 Instrumentos, 53

4.6 Testes, 56

4.7 Análise de dados da pesquisa, 56

4.8 Resultados da pesquisa e discussão das falhas encontradas, 68

Conclusão

Referências

Lista de Quadros

- 01 — Propriedades relacionadas à segurança do sistema no que respeita a informação e seu acesso pelos usuários, **17**
- 02 — Fatores que influem na importância da segurança, **21**
- 03 — Gerenciamento de pontos importantes para a segurança do sistema, **22**
- 04 — Pessoas, especificações e áreas de atuação no sistema dos tipos apresentados, **25**
- 05 — Condições de vulnerabilidades, **30**
- 06 — Ameaças que provocam perdas de confidencialidade, integridade e disponibilidade no sistema, **32**
- 07 — Breve lista de verificação das técnicas comuns já desenvolvidas, **37**
- 08 — Sintaxe de algumas opções do Nmap com as potencialidades ou funções da ferramenta, **42**
- 09 — Distribuição em quantidades dos doze dados considerados pela ferramenta LanGuard e as tipificações em real e virtual consideradas na pesquisa, **56**
- 10 — Passos para a atualização do sistema, **65**
- 11 — Falhas encontradas e possíveis soluções apresentadas, **70**

Lista de Figuras

- 01 — Ilustração da importância do programador e sua disciplina para com a segurança de uma aplicação,**38**
- 02 — *Nmap* versão para Windows,**43**
- 03 — Nmap versão para Linux,**44**
- 04 — Tela de relatório do Nessus, **45**
- 05 — Ilustração do comando do Netcat no console do Windows,**46**
- 06 — Tela de comando do Dsniff via console no Windows,**47**
- 07 — A tela inicial do Ethereal,**48**
- 08 — A tela inicial do LanGuard,**49**
- 09 — Tela principal de pesquisa do Google,**50**
- 10 — Tela inicial do LanGuard,**58**
- 11 — Máquinas ativas na rede,**61**
- 12 — Detalhamento da varredura feita pela ferramenta mostrando seu tempo de início e seu tempo de duração,**62**
- 13 — Alguns Patches desatualizados,**63**
- 14 — Informação de que 29 patches devem se atualizados,**64**
- 15 — Documentação para correções de erros em portas,**66**
- 16 — Portas Ativas e passivas a invasão,**67**
- 17 — Ilustração das pastas compartilhadas (shares),**68**
- .

ABSTRACT

This is a study case about problems security scan related with computer in intra-systems and in web system. In this work the reader can find out beside others, discussions about important themes which involve the information security. The questions about network security basis, invaders and their motivations, the net and systems security aims, vulnerabilities to it a system can be submitted, vulnerability concepts, the vulnerabilities and threat differences of the systems, the use of the security paradigm in operational systems, specific items of language programs, a security diagnosis of a computational environment, vulnerability research tools, and for the last the reader can find out the case study as it was researched about the identified failures in the enterprise security system studied as for example a non-updated antivirus and ideas for trying to give solution to the found matters.

Key-words: Computer Science, digital security, hackers, cracker, vulnerabilities, false programs.

Introdução

A segurança tem seu papel preponderante para o funcionamento adequado de qualquer ação dentro de um contexto geral ou particular, seja para uma empresa seja para uma pessoa. Na Ciência da Computação esse fato não é diferente. Ainda mais, é de suma importância devido ao grande desenvolvimento tecnológico e de situações de risco que o mundo real passou a estar submetido a partir das invasões e manipulações de dados particulares de pessoas e de empresas via elementos como *crackers*. São estes principalmente, que passeiam pelo mundo virtual deixando rastros catastróficos no mundo real como transferência de valores indevida, invasão e manipulação de informações de empresas e outros. Ao lado destes, também estão os *hackers*. Os *hackers* são elementos que embora aparentemente não ofereçam riscos a situação real de uma pessoa ou de uma empresa, desenvolvem constantemente maneiras de invadir sistemas de computacionais. A literatura atual descreve que o “*hacker*” faz isso apenas para se sobressair entre membros do mesmo grupo e dos demais invasores de sistemas. Isso acaba por causar danos ao tráfego de pacotes de informação que entram e saem de uma rede entre computadores porque enquanto os “*hackers*” desenvolvem novas formas de burlar a segurança virtual no tráfego desses pacotes apenas para demonstrarem que são inteligentes o suficiente para isso, *crackers* se aproveitam das novas maneiras e invadem sistemas para praticar crimes.

No mundo virtual, o tráfego de pacotes entrando e saindo de uma rede entre computadores dentro de uma empresa deve ser controlada de forma segura e abrangente. Dentro desse contexto, a literatura da área da Ciência da Computação tem demonstrado que a segurança da informação deve surgir como identificador que por sua vez deve ter como objetivo localizar os poucos pontos em que um controle seguro é realizado. Com isso, o controle deve ser feito de maneira a filtrar a permissão do tráfego de pacotes que por ele são autorizados à passagem de informações simultâneas com livre acesso ao sistema. Assim, a segurança da informação propõe que toda e qualquer informação, armazenada temporária ou permanentemente que trafegue por redes de computadores esteja protegida contra ameaças, isto é, a informação de maneira geral deve manter a sua confidencialidade, integridade e disponibilidade em situações

diferenciadas de acesso devido aos riscos e ameaças de invasão em relação à segurança e privacidade do sistema em geral. Quanto a isso, a teoria mais aceita sobre esse assunto é a de que há um estágio de consciência da capacidade de resolução de problemas que diz respeito ao tráfego de informações e das limitações na capacidade dessas resoluções quando o assunto é *hackerismo* e outros tipos de invasores e as novas formas de invasões a sistemas e redes de computadores.

Na Ciência da Computação, os riscos e as ameaças intencionais ou não-intencionais na segurança de maneira geral representam para redes e sistemas um fator de preocupação que tem sua importância quando se trata de vulnerabilidade a que está exposta pessoas e empresas. Portanto, há que se pensar em mecanismos de defesa de maneira clara e objetiva. Dessa forma, os mecanismos de defesa para a proteção do ambiente computacional devem ser planejados e realizados com base no conhecimento das ameaças e dos riscos existentes e nos que possam vir a existir como forma de prevenção e proteção ao sistema em que se está a trabalhar. Isso permite que vulnerabilidades possam ser exploradas em ataques após as identificações preventivas terem sido aplicadas ao sistema especificado. Conhecidos os riscos existentes e as ameaças iminentes que possam invadir o sistema, danificá-lo e comprometê-lo, a segurança intra-rede passa a controlar e eliminar as possibilidades de violação da informação. Entretanto, é preciso que se tenha em mente a não possibilidade de se proteger o sistema contra riscos e ameaças (ainda) não conhecidos. Nesse sentido, o presente trabalho é um estudo de caso que se propõe a estudar as soluções para os problemas de riscos e ameaças existentes na troca de dados em uma rede de computadores tendo como fator importante o seu gerenciamento.

Particularmente, são objetivos dessa pesquisa: discutir, avaliar, verificar e gerar relatório sobre a vulnerabilidade dentro de uma empresa a partir do ponto de vista da segurança da informação. E mais ainda, demonstrar que não é possível proteger o sistema contra riscos e ameaças que possuem características desconhecidas, também. Por outro lado, eliminar todos os riscos e ameaças já conhecidas facilita o controle de entrada de pacotes de informação que compromete o sistema e sua segurança. Em termos de cifras isso significa investimentos pesados na área. Mesmo assim, não se justifica investimentos mais altos do que o valor da própria informação. Assim, o

fundamental é que os riscos e as ameaças sejam gerenciados para que sejam acompanhados de maneira permanente com a finalidade de que eles sejam minimizados. E dessa forma possibilitar que riscos residuais sejam tolerados pela empresa, ou mesmo transferidos para terceiros. O que passa a ser tido como ponto de referência para a resolução de outros problemas relativos à segurança do sistema. Para tanto, este trabalho parte da hipótese de que as ameaças e riscos intencionais e não-intencionais podem representar prejuízos para a segurança de redes e sistemas da empresa quando os mecanismos de defesa para a proteção do ambiente computacional não forem planejados e realizados com base no conhecimento pré-existente dessas ameaças e dos riscos.

A pesquisa se inicia com a discussão e exploração sobre os aspectos gerais que englobam a segurança da informação. É o capítulo um (1). No capítulo dois (2), discute-se a questão de vulnerabilidade do sistema, conceitos, diferenças, paradigmas de segurança e itens específicos da linguagem utilizada pelo sistema. Esta parte vista, passa-se a discutir sobre as ferramentas para detecção de vulnerabilidades de *SNIFFERS* até *WARGOOGLE*. É o capítulo três (3). Para avaliação e verificação da hipótese o capítulo quatro (4) trás um estudo de caso. Parte principal do trabalho, o estudo de caso mostra problemas da vulnerabilidade, os objetivos do teste, a justificativa proposta, o ambiente computacional de teste, a execução do plano de teste em que aparecem os tópicos correspondentes a uma varredura na rede, a força da engenharia social e a execução de um mini-curso sobre segurança a partir do qual se gera um relatório em que são descritas falhas encontradas durante a pesquisa e propostas de soluções a serem realizadas. Finalizando a pesquisa, a conclusão faz uma revisão dos tópicos apresentados e discute os resultados obtidos pelo estudo proposto e situa o trabalho como sendo uma fonte para a comunidade interessada no assunto de segurança da informação e suas características peculiares dentro da computação.

1

Aspectos Gerais sobre Segurança da Informação

1.1 FUNDAMENTOS DE SEGURANÇA

A segurança de redes tem como principal objetivo proteger as informações que nela trafegam no sentido de garantir a sua confidencialidade, a sua integridade e a sua disponibilidade. De acordo com empresa Symantec (2006) define-se (1) confidencialidade como sendo uma propriedade cujo objetivo é o de responsabilizar-se por permitir acesso ao seu conteúdo somente a usuários que são autorizados; (2) a integridade se define como sendo uma propriedade que garante a chegada de uma informação ao seu destino em toda a sua totalidade, isto é sem restrições; (3) por último define-se disponibilidade como sendo uma propriedade que se caracteriza por assegurar ao usuário do sistema acesso à informação quando estes necessitam. O quadro um (01) ilustra cada uma dessas três propriedades situadas à esquerda e suas definições postas à direita de maneira resumida para melhor compreensão:

Quadro 01 - Propriedades relacionadas à segurança do sistema no que respeita a informação e seu acesso pelos usuários.

<i>Propriedades</i>	<i>Definição</i>
► <i>Confidencialidade</i>	É a propriedade que garante apenas aos usuários autorizados o acesso ao seu conteúdo.
► <i>Integridade</i>	É a propriedade que garante a chegada de uma informação ao seu destino de uma forma íntegra, ou seja, sem que tenha sofrido nenhuma mudança em seu conteúdo em qualquer momento de sua existência.
► Disponibilidade:	É a propriedade que garante a disponibilidade da informação para os usuários quando eles necessitam acessá-las.

Fonte: Curso de Segurança de Rede - RNP (2007.). **Elaboração do autor.**

Com as informações demonstradas no quadro um (01) pode-se inferir que a segurança de redes e de sistemas propõe para toda a informação, armazenada temporária ou permanentemente em um sistema, ou trafegando pela rede, proteção contra ameaças que podem comprometer a confidencialidade, a integridade e disponibilidade. Assim acontece porque as ameaças e riscos intencionais ou não-intencionais para a segurança de redes e sistemas, podem ser atingidos de forma comprometedora. Com isso, os mecanismos de defesa para a proteção do ambiente computacional devem ser planejados e realizados com base no conhecimento das ameaças e dos riscos já existentes. É exatamente nesse contexto que se pode fazer a identificação das vulnerabilidades que por sua vez possam se apresentar no sistema intra-rede. A partir da identificação feita, uma exploração em ataque pode ser utilizada para que as vulnerabilidades sejam controladas e suspensas as ações de caráter prejudicial ao sistema.

Como se pôde verificar na discussão anterior há um interesse que se necessita dar a devida importância quando o assunto é segurança do sistema computacional. Percebe-se que conhecer os riscos existentes se enquadra neste perfil. E mais, é preciso ter em mente que não é possível proteger a rede que está distribuída no sistema contra riscos

que não são ainda conhecidos. Entretanto, um passo importante em direção ao que já se conhece em termos de invasão de sistemas é o aprofundamento da questão. Com isso, a previsão dos riscos e ameaças pode significar para a segurança intra-rede uma questão a grosso modo econômica para que a empresa interessada leve em consideração os prejuízos causados por pacotes de informações infectados. Por outro lado, eliminar todos os riscos conhecidos pode ser bastante caro. O que em outras palavras não justifica investimentos mais altos do que o valor da própria informação. Assim, o fundamental é que os riscos sejam gerenciados, ou seja, eles devem ser minimizados, sendo possível que riscos residuais sejam tolerados pela empresa, ou mesmo transferidos para terceiros.

1.1.1 Abrangência da segurança digital

A segurança da informação engloba aspectos de defesa de redes e de sistemas de forma abrangente contra invasores de qualquer natureza. Ela envolve aspectos tecnológicos, humanos, processuais, legislativos, além dos aspectos de negócios. Isso significa que apenas com um conjunto de tecnologias de segurança a informação não pode ser considerada totalmente segura, já que ela pode ter a sua confidencialidade comprometida por outros meios. Por exemplo, um funcionário de uma empresa qualquer pode ser persuadido com uma boa conversa por uma pessoa de interesses estranhos para com a empresa em questão, e permitir acesso a informações confidenciais. Nesse caso, a engenharia social, invasão que explora características humanas como a boa vontade, a confiança ou a ingenuidade, faz com que a empresa sofra um incidente de segurança. O exemplo citado demonstra que a abrangência da segurança digital vai além de “*softwares*” e “*hardwares*”. Demonstra que esta pode envolver desde uma característica humana dentre outros que envolve as relações interpessoais, a empresa, seus funcionários e o sistema até a parte física do computador e seus programas. Assim, as tecnologias por si só não resolvem problemas de engenharia social, que requer um trabalho de conscientização dos usuários para evitar riscos envolvidos com ações dessa natureza.

Mesmo considerando apenas os aspectos tecnológicos, diversas camadas existem também e devem ser consideradas. A divisão desses aspectos facilita o entendimento dos problemas de segurança que existe intra-rede, além de tornar mais fácil a definição do mecanismo, técnica ou tecnologia para a proteção do ambiente contra a invasão do sistema. Por exemplo, a criptografia é usada principalmente para proteger a informação

contra acesso indevido, mantendo a sua confidencialidade. A integridade, como no caso da confidencialidade, também pode ser mantida pela criptografia¹, que por sua vez pode ser usada em protocolos de rede, protocolos do nível de aplicação ou em aplicações. Porém, a criptografia não é capaz de prover a disponibilidade, que exige o uso de outros mecanismos de segurança. Com isso, entender a abrangência da segurança é importante para que a falsa sensação de segurança – que é até mesmo mais perigosa do que os próprios riscos existentes – seja evitada. Além disso, alguns pontos-chaves devem ser definidos e implementados. É o entendimento desses pontos que dará o embasamento necessário para a segurança de redes e sistemas.

Os pontos-chaves referidos anteriormente estão divididos em: (1) motivação para ataques; (2) natureza dos ataques; (3) mecanismos de segurança; e (4) visão abrangente da segurança. O primeiro ponto diz respeito ao entendimento da motivação para a invasão ou ataques, a qual envolve a contextualização dos agentes e pacientes em um cenário que engloba interesses pessoais e de negócios. Isso porque em sua totalidade, os ataques representam ganhos para alguns e conseqüentes prejuízos para outros. O segundo ponto importante diz respeito à natureza dos ataques. Neste caso questionamentos em que estão inseridas possibilidades de soluções para o problema podem ser feitos a partir situações pré-existentes: O que, de fato, é explorado em ataques? Quais condições dão origem aos incidentes de segurança? Tais perguntas servem como elo entre os problemas que interferem no sistema. Designam assim, o conhecimento da causa que gera problemas de segurança, sendo dessa forma de fundamental importância para o sistema em que se está a operar.

O terceiro ponto a ser entendido diz respeito aos mecanismos de segurança. Mecanismos de segurança podem ser usados para que o ambiente inter-rede possa proteger-se da melhor maneira possível com o recurso nele disponibilizado. Muitas

¹ Consiste na ciência e na arte de se comunicar secretamente.

vezes, mais do que tecnologia, técnicas de defesa ou mecanismos de segurança são mais importantes para uma proteção efetiva do sistema. Esses mecanismos de segurança, em um contexto mais amplo, em que são considerados aspectos que vão além da tecnologia, são conhecidos como controles, ou seja, para que a proteção da informação seja eficaz no dia-a-dia da organização, os conceitos e os regulamentos de segurança devem ser compreendidos e seguidos por todos os usuários. O quarto ponto abrange todos os anteriores, ou seja, faz com que uma visão abrangente de segurança auxilie na definição da estratégia mais segura para o ambiente. A segurança passa, assim, a ser objeto de gestão, que por sua vez deve ser efetivada com uma base sólida nos conhecimentos sobre a natureza dos ataques, a motivação existente e a presença de mecanismos e técnicas de segurança. Nesse ínterim, os diferentes aspectos devem ser considerados e os controles para o gerenciamento dos riscos devem ser definidos e posto em prática de forma a prevenir os problemas de invasão da rede.

1.1.2 Contextualização

A constante evolução tecnológica permite grandes transformações mercadológicas em diversos níveis. Incluem-se nessa evolução desde a criação de novos negócios até a mudança na relação entre parceiros comerciais. A partir disso pode-se dizer que essa evolução resulta em grandes benefícios para a sociedade. Porém, como todo produto da tecnologia, trazem consigo problemas que devem ser conhecidos e tratados. Os problemas relacionados com a segurança da informação, por exemplo, são frutos dessa própria evolução tecnológica, que possibilitou a integração cada vez maior de ambientes e de redes diferentes, que se tornam cada vez mais complexas. Essa integração atinge a níveis cada vez mais fortes. E chega ao nível de interdependência entre diferentes redes e ambientes. Para ilustrar essa questão apresenta-se abaixo um conjunto de fatores que influem diretamente na importância cada vez maior da segurança intra-rede. Optou-se por pô-las no quadro que segue para destacá-las de maneira a facilitar a compreensão desses executores.

Quadro 02 - Fatores que influem na importância da segurança

Fonte: Curso de Segurança de Rede - RNP (2007.). Elaboração do autor

O conjunto de fatores que influi diretamente na importância da segurança

- A competitividade e a pressa no lançamento de novos produtos faz com que a falta de cuidados adequados no desenvolvimento provoque maior número de vulnerabilidades.
- O aumento da interação entre organizações, que aumenta o nível de conectividade e da conseqüente complexidade, o que, por sua vez, resulta no aumento de vulnerabilidades.
- O aumento do número de potenciais invasores, que encontram novas formas de obter vantagens, constituindo até mesmo uma nova forma de crime.
- O avanço tecnológico, que resulta em novas vulnerabilidades intrínsecas, como os riscos envolvidos com as redes sem fio padrão IEEE 802.11 (Wi-Fi).
- A integração entre diferentes tecnologias, que multiplica as vulnerabilidades.
- A era da Informação, em que o conhecimento é o maior valor, sendo, portanto, alvo de invasores.
- A segurança representando a habilitação de negócios, ou seja, o sucesso de novos negócios depende cada vez mais de aspectos de segurança, tanto de seus clientes quanto da própria empresa.

1.1.3 Considerações sobre a segurança do sistema

Diversos pontos devem ser considerados quando uma rede passa a constituir parte importante da organização. Aspectos como os perigos da falta de controle de acesso, o mal uso de senhas ou demais riscos precisam ser entendidos para que uma melhor segurança possa ser implementada. Alguns dos assuntos mais importantes a serem entendidos para o gerenciamento da segurança do sistema são os que estão relacionados com o tipo de informação que deve entrar e percorrer a rede, a definição do controle de acesso, a dificuldade de controle do administrador sobre os sistemas, a hostilidade do ambiente da internet, a sujeição das informações que trafegam pela rede, a conexão entre redes internas e pontos externos como meio de invasão à rede e por último a complexidade da segurança. A seguir o quadro três ilustra as considerações² sobre o gerenciamento da segurança do sistema:

Quadro nº 03: Gerenciamento de pontos importantes para a segurança do sistema.

Fonte: Curso de Segurança de Rede - RNP (2007.). Elaboração do autor.

Gerenciamento de pontos importantes para a segurança do sistema

² As considerações vistas no quadro três servem para demonstrar o quanto a segurança da informação é abrangente e multidisciplinar. Pode-se perceber que cuidado com alguns pontos e negligência para com outros pode comprometer totalmente a organização, pois os incidentes sempre ocorrem no 'elo mais fraco da corrente', ou seja, no ponto mais vulnerável do ambiente.

- A classificação das informações é fundamental para que recursos não sejam desperdiçados na proteção. A estratégia de segurança deve levar em consideração o valor relacionado com a informação. A análise e avaliação de riscos são importantes. Sem essa consideração, além dos riscos para a organização, o dimensionamento das perdas resultantes de um ataque fica comprometido.
- O controle de acesso mal definido faz com que os usuários autenticados no início da conexão tenham acesso irrestrito a quaisquer partes da rede interna. Esse acesso muitas vezes chega até mesmo a partes do sistema que não são necessárias para a realização de suas tarefas.
- A dificuldade de controle do administrador sobre todos os sistemas da rede faz com que eles não possam ser considerados confiáveis. Isso porque, além da falta de controle, os *bugs* nos sistemas operacionais ou nos softwares embarcados nos equipamentos representam grandes riscos.
- A internet deve ser considerada um ambiente hostil e, portanto, não confiável. Assim, todos os seus usuários devem se considerados não confiáveis e potenciais invasores.
- As informações que trafegam pela rede estão sujeitas a serem capturadas.
- Qualquer conexão entre a rede interna e qualquer outro ponto externo pode ser utilizada para invasores à rede interna.
- A segurança é complexa.

1.1.4 Invasores e Motivação

O tópico sobre invasores e motivação requer primeiramente que se fale sobre um ponto importante para a segurança do sistema e os riscos que este pode vir a ter. Trata-se do assunto “*Hacker*”. Em termos lingüísticos a palavra é formada a partir do verbo danificar ou cortar mais o morfema ‘er’ que por sua vez transforma um verbo em um nome (em inglês *to hack+er*). A forma “*hacker*” por sua vez é uma gíria utilizada para designar uma pessoa ou usuário de computadores que é hábil e entusiasta na área da computação. A mesma forma pode também ser utilizada para designar usuários de computadores que invadem sistemas de computadores e ilicitamente usam ou mudam informações do sistema computacional. Em computação, “*Hacker*” é um termo genérico para representar a pessoa que realiza uma invasão a um sistema computacional ou uma pessoa que desenvolve uma forma de burlar a segurança disposta no sistema. O que há em comum entre os dois tipos é a sua capacidade e conhecimento sobre computadores e seus programas. Essa generalização, porém, possui diversas ramificações na área da computação devido aos objetivos distintos para cada tipo de *hacker* e também ao grau de segurança dos alvos, que pode exigir maior capacidade do *hacker* em atacá-lo.

Os “*hackers*”, em sua definição original, como se pôde verificar são pessoas que utilizam seus conhecimentos em computação para invadir sistemas, não com o intuito

de causar danos às vítimas, mas sim como um desafio às suas habilidades. Segundo essa idéia, eles invadem os sistemas, capturam ou modificam arquivos para provar sua capacidade e depois compartilham suas proezas com seus colegas. Ainda de acordo com a definição em original, os “*hackers*” não têm a intenção de prejudicar, mas sim de apenas demonstrar que conhecimento é poder. Eles são exímios programadores e conhecedores dos segredos que envolvem as redes e os computadores. Atualmente, no entanto, devido ao crescimento da Internet e a conseqüente facilidade em se obter informações e ferramentas para ataques, a definição de *hacker* adquiriu um outro sentido. A própria imprensa nacional e internacional tratou de modificar seu conceito. Agora, qualquer incidente de segurança da informação é atribuído a *hackers*, em seu sentido genérico.

Isso gerou e ainda gera uma discussão calorosa, pois, segundo os próprios, existe uma diferença entre *hackers* e os invasores que não têm as mesmas características de um “*hacker*”. São por eles denominados de “*crackers*”.

De acordo com os *hackers*, *crackers*³ são elementos humanos que invadem sistemas para roubar informações deixando um rastro de danos que causam problemas reais às vítimas. O termo *cracker* também é uma denominação utilizada para aqueles que decifram códigos e destroem proteções de software. Existe ainda o *cracker* de senha. Este é um elemento que se utiliza de software avançado para descobrir senhas ou decifrar mensagens cifradas. Como forma de facilitar a compreensão de termos como o de *cracker* e *hacker* que estão ligados ao assunto segurança da informação, o quadro a seguir ao lado objetiva ilustrar e destacar alguns termos afins, de forma resumida. À esquerda as denominações de pessoas que atuam como invasores do sistema e um programa (*crack*) que por eles é utilizado. À direita, com exceção da especificação e áreas de acesso do programa *crack*, são descritas as especificações do papel de cada invasor e suas áreas de atuação nos sistemas de computação.

³ O termo *cracker* possui características formais idênticas ao termo *hacker* linguisticamente. Isto é, trata-se de uma palavra formada a partir do nome que nesse caso é um substantivo mais o morfema ‘er’ (elemento lingüístico mínimo dotado de significado). Literalmente ‘crack’ pode significar racha, estalo ou quebra ou ainda abertura, rompimento além de outras atribuições. No contexto da computação a palavra rompimento está bem próxima dos estragos causados por um *cracker* que consegue romper a segurança do sistema, penetrá-lo e danificá-lo. *Cracker* literalmente significa biscoito. No sentido da gíria em que *cracker* aparece como adjetivo seu significado é o de qualidade de pessoa ou coisa que tem atributos de inteligência especial. Informalmente, se se acrescentar um ‘s’ ao termo *cracker* (*crackers*) o adjetivo passa a significar que a pessoa qualificada como tal é um retardado mental, louco, estúpido.

Quadro n° 04: Pessoas, especificações e áreas de atuação no sistema dos tipos apresentados.

Fonte: Curso de Segurança de Rede - RNP (2007.). Elaboração do autor.

<i>Pessoas</i>	<i>Especificações e áreas de atuação no sistema</i>
<i>Hacker</i>	Pessoa com alto conhecimento em sistemas operacionais e linguagem de programação, com capacidade para modificar um sistema de acordo com sua vontade. <i>Linus Torvalds</i> é um hacker, por ter codificado e desenvolvido o <i>Linux</i> . <i>Theo de Raadt</i> , do <i>OpenBSD</i> é um hacker, por ajudar a manter, corrigir e melhorar o <i>OpenBSD</i> . O termo <i>hacker</i> também tem sua conotação negativa, como colocado.
<i>Cracker</i>	Pessoa cujo interesse é invadir sistemas alheios, para propósitos ilegais.
<i>Crack</i>	Programa utilizado para remover proteções de senhas/ <i>serial number</i> de <i>softwares</i> .
<i>Scriptkiddies</i>	Iniciantes, com nenhum ou pouquíssimo conhecimento, que se aproveitam da facilidade em se obter ferramentas de ataques utilizam ferramentas prontas para ataques, muitas vezes sem saber o que elas fazem (existem pacotes para o desenvolvimento de vírus/ <i>trojans</i> de fácil utilização).
<i>Insiders</i>	Funcionários insatisfeitos com a empresa a qual trabalha.
<i>White hat</i>	Profissionais de segurança contratados para averiguar as questões de segurança da empresa.

<i>Black hat</i>	Crackers ou bandidos da história passam o tempo tentando burlar a segurança de sistemas e redes.
<i>Gray hat</i>	Hackers que já foram black hat, mas que atuam como White hat.
Scammer	Pessoa que divulga spam dizendo-se ser um banco, agência de cartão de crédito ou afins, requisitando informações pessoais para o uso ilícito.

O quadro demonstra que não são apenas os “*hackers*” que causam problemas de segurança em sistemas. Os usuários, autorizados ou não, mesmo sem intenções malévolas, também podem causar danos ou negar serviços de redes, por meio de seus erros e de sua própria ignorância como é o caso dos *scriptkiddies*. Vê-se, com isso, que as motivações para uma invasão são diversas, variando de acordo com o tipo de invasor. Os “*scriptkiddies*”, por exemplo, são motivados pela curiosidade, pelo experimento, pela vontade de aprender, pela diversão ou pela simples necessidade de colocar a vítima em maus lençóis. Os “*scriptkiddies*” são os responsáveis, em alguns casos, pelas invasões mais simples, como a pichação de sites, também conhecida como “*web defacement*”.

1.1.5 Conseqüências de Invasões

Os sistemas podem sofrer acometimentos em seus serviços por intermédios de “*hackers*”, “*crackers*” e outros elementos do tipo. Isso significa que para a quebra desses serviços há sempre conseqüências que devem atingir a rede de computadores. Essas conseqüências de ataques podem ir desde a simples perda de produtividade para restauração de um serviço, até a privação de reputação e conseqüente perda de mercado. É interessante notar que os prejuízos dependem do valor da informação que está em jogo, porém devem ser considerados tanto os valores tangíveis quanto os valores intangíveis. Exemplos de valores tangíveis são as horas para recuperação de informações, perda de vendas no período de interrupção de serviços ou contratação de consultorias para implementação de segurança. Já os valores intangíveis são por natureza mais difícil de serem quantificados e estão relacionados à perda de mercado ou de reputação, e até a depredação e mancha no nome da empresa. Dessa forma, as

consequências de uma invasão bem-sucedida a uma empresa podem ser variadas, mas são sempre negativas. De acordo com [HORTON & MUGGE,2003], algumas delas são:

- ▶ Monitoramento não autorizado.
- ▶ Descoberta e vazamento de informações confidenciais.
- ▶ Modificação não autorizada de servidores e da base de dados da organização.
- ▶ Negação ou corrupção de serviços.
- ▶ Fraude ou perdas financeiras.
- ▶ Imagem prejudicada, perda de confiança e de reputação.
- ▶ Trabalho extra para a recuperação dos recursos.
- ▶ Perda de negócios, clientes e oportunidades. (2006)

Um ponto importante a ser considerado após a realização das invasões é que os hackers tentarão encobrir todos os procedimentos realizados por eles. Algumas técnicas para isso são bastante conhecidas como (1) a substituição ou remoção de arquivos de *logs*, (2) troca de arquivos importantes do sistema para o mascaramento de suas atividades ou formatação completa do sistema. Esses procedimentos fazem com que tecnologias como sistemas de detecção de intrusão (*Intrusion Detection System, IDS*) sejam importantes, bem como planos de resposta a incidentes e a forense computacional (o propósito do exame forense é a procura e extração de evidências relacionadas com o caso investigado, que permitam a formulação de conclusões acerca da infração.), busquem investigar a invasão e seus responsáveis.

1.1.6 Objetivos da Segurança de Redes e Sistemas

A complexidade e abrangência da segurança da informação como tem sido visto ao longo das discussões, envolve diferentes aspectos. Um desses aspectos refere-se à função tecnológica dada ao *firewall*⁴. Ele aparece como o melhor sistema de filtragem de dados. O que acontece a pacotes de informação vistoriados para que possam estar livres de riscos e ameaças ao sistema (CARTILHA DE SEGURANÇA PARA INTERNET) [5]. Os aspectos técnicos envolvem, por exemplo, um bom administrador de segurança. É ele o responsável por gerenciar as políticas de segurança envolvidas na empresa. De acordo com Kevin Mitnick [19], com relação aos aspectos sociais envolvidos entre a questão da segurança do sistema e a empresa situam-se funcionários inescrupulosos e funcionários leigos sobre o que ocorre ao sistema. No primeiro tipo de funcionário há uma caracterização peculiar em que aparece o aproveitamento da situação na qual eles roubam informações confidenciais da própria empresa. Já os funcionários leigos são os que por não conhecerem tecnicamente sobre o assunto invasão de segurança sofrem com esse aspecto da engenharia social, o que pode ser evitado se houver um treinamento desses funcionários sobre como se prevenir contra ataques de engenheiros sociais.

Embora haja todo esse aparato tecnológico, com toda sua abrangência na segurança da informação, o objetivo de proteger totalmente a empresa é impossível. Infere-se com isso que quando se fala em segurança da informação está-se a falar de um estado parcial de segurança. Isso é um fato. O motivo é porque sempre há algum aspecto esquecido, negligenciado ou desconhecido sobre o assunto. Portanto, afirmar que uma organização está cem por cento sob segurança total é, na realidade, um erro. O mais plausível é prover o sistema de máxima proteção possível, com os recursos disponíveis, já que simplesmente não existe um modelo de segurança à prova de *hackers*. Dessa forma, o objetivo da segurança de redes não é construir uma rede totalmente não vulnerável, mas sim um sistema altamente confiável. Um sistema que seja capaz de anular os ataques mais casuais de *hackers* e também tolerar problemas causados por acidentes como o esbarrar no cabo de energia elétrica de um servidor por uma faxineira na hora da limpeza do ambiente. Dessa forma, é importante lembrar que

⁴ É um sistema ou um conjunto de sistemas que implementam uma política de controle de acesso entre duas redes.

as empresas, portanto, podem definir o nível de segurança, de acordo com suas necessidades, já assumindo esses riscos⁵.

Pelo fato da rede nunca ser totalmente segura, devem-se procurar meios de torná-la, no mínimo, mais confiável. E isso pode ser feito a partir do manuseamento da confidencialidade, integridade e disponibilidade da informação. Neste caso, a segurança passa a ser uma questão de gerenciamento de riscos. Assim, deve-se ter em mente que a segurança se enquadra em um processo constante e evolutivo, uma luta do administrador de segurança que mantém os sistemas atualizados, suas políticas de segurança coerentes e seu plano de contenção abrangente em um ambiente hostil. Mesmo que esse ambiente se situe em uma rede que fique à mercê de “*hackers*” e usuários mal intencionados. Ou que comprometam a segurança e até mesmo ludibriem o administrador com a engenharia social. Junte-se a isso a segurança de perímetro e a abordagem em camadas como pontos importantes. Eles também representam tipos de proteção nos quais vários mecanismos de segurança são adotados de forma encadeada. A função de cada uma das camadas é a de ser transposta pelo hacker para que este tenha acesso à informação. Quanto maior o número de camadas, maior a dificuldade de invasão ao recurso.

⁵ Isso faz com que o plano de contingência seja um dos pontos essenciais dentro da estratégia de segurança de uma empresa.

2

Aspectos sobre Vulnerabilidades

2.1 CONCEITOS DE VULNERABILIDADES

Uma vulnerabilidade corresponde a um ponto fraco que possui características inerentes ou falhas que estão associadas a um bem material ou a seu ambiente. O que pode permitir um comprometimento ao ambiente ou a um dado bem. As vulnerabilidades são desencadeadas ou atacadas de forma intencional ou por acontecimento fortuito. Uma vulnerabilidade pode ser uma simples fraqueza ou uma série de pontos fracos que acabam permitindo uma ou várias ameaças. Uma ameaça usa uma ou mais vulnerabilidades para afetar a confidencialidade, a integridade e/ou a disponibilidade de um bem. Optou-se neste trabalho por listar no quadro 04, de acordo com Mike Shema e Yen-Mling Chen [26] as seguintes condições propostas em que às vulnerabilidades se dão:

Condições em que as vulnerabilidades ocorrem

- *Controles inadequados.*
- *Controles e configurações funcionais incorretamente ajustados.*
- *Falta de atualizações ou de patches⁶ de software.*
- *Má administração ou procedimentos operacionais indevidos.*

Quadro nº 05: Condições de vulnerabilidades

Fonte: Mike Shema & Yen-Ming Chen – Segurança na Web Série Hack Notes(2003.). Elaboração do autor.

⁶ Procedimentos de atualizações que precisam ser realizados para que os softwares permaneçam atualizados.

2.2 DIFERENCIANDO AMEAÇAS DE VULNERABILIDADES

Para dar início ao assunto deste tópico um pergunta se faz necessária: Qual é a diferença entre ameaças e vulnerabilidades? Para responder a essa questão é importante conseguir entender melhor sobre tal diferença. O primeiro passo é imaginar o seguinte: Quando uma pessoa se sente ameaçada seja por qualquer tipo de fator ou circunstância, esta pessoa não se sente vulnerável necessariamente. Ela se sente intimidada. O que a transforma em alvo passivo. Esta é uma característica peculiar à pessoa que pode se sentir ameaçada. Sentir-se vulnerável, isto é, ser paciente de poder ser atacada em seus pontos mais fracos tanto em termos físicos quanto em termos psicológicos é uma característica de quem é vulnerável. Entretanto, a sua condição de paciente se torna indireta, pois aquele (a) que espera atingi-lo (a) não o faz por força de ameaça. Ele simplesmente ataca sem sobreaviso. Para o caso de uma pessoa se sentir ou se considerar vulnerável a situações ou momentos externos, ela instintivamente se denomina e/ou se acha ameaçada. O que transforma a ameaça em uma consequência. Por isso mesmo ela pode se autocontrolar e se preparar para as ações concretas que foram planejadas e injetadas pela ameaça em termos de contexto físico e psicológico.

Trazendo as considerações feitas acima para o contexto de segurança de sistema percebe-se a proximidade de significação de ameaça e vulnerabilidade na questão de ataques a uma rede de computadores em particular. Isto não é uma regra, entretanto vale principalmente no contexto do que se diz respeito às informações de acordo com *Symantec* (2006). Como foi possível ver com a discussão apresentada no parágrafo anterior, as ameaças podem surgir enquanto consequências das vulnerabilidades existentes. Com isso, como resultado dessa transformação há a provocação de perdas de confidencialidade, integridade e disponibilidade. Essas perdas podem ser divididas como mostra o quadro demonstrativo a seguir:

Ameaças que provocam perdas no sistema

1) Ameaças naturais: fenômenos da natureza.

2) Ameaças involuntárias: ocorrem devido o desconhecimento, ou acidentes, erros dentre outros.

3) Ameaças voluntárias: as que mais se relacionam com a Engenharia Social, causadas por hacker, invasões, espiões, disseminadores de vírus de computador. São ameaças propositais, de ocorrência humana.

Quadro nº 06: Ameaças que provocam perdas de confidencialidade, integridade e disponibilidade no sistema.

Fonte: Curso de Segurança de Rede - RNP (2007.). Elaboração do autor.

2.3 VULNERABILIDADES EM SERVIDORES WEB

Uma plataforma fortalecida contribui para a segurança da aplicação *Web* tanto quanto um código seguro. Um servidor *Web* instalado com segurança deve estar fortalecido para proteger a aplicação de várias situações de ataques. Muitas investidas de aplicação que acessam arquivos arbitrários ou executam comandos arbitrários podem ser bloqueadas por uma configuração de servidor rígida que limita o acesso do servidor a áreas suscetíveis de vulnerabilidades no sistema operacional (GARFINKEL and SPAFFORD, 1996: 971). Outra atitude fundamental que pode ser tomada para a segurança do servidor *Web* é a remoção de capacidades desnecessárias. Nesse caso, as únicas funções que devem estar habilitadas devem ser aqueles que realmente são utilizados pela aplicação. Como o servidor *Web* é a porta de entrada para qualquer aplicação, uma programação segura pode ser colocada a perder por um servidor mal configurado que divulga código-fonte. Além disso, as configurações do Apache e IIS[VEIGA, 2004][MIKE SHEMA & YEN-MING CHEN,2003] podem ser acessadas e modificadas com ferramentas de linha de comando, o que aumenta bastante a sua capacidade de criar *scripts* personalizados e ferramentas de bloqueio automatizado. Qualquer servidor *Web* deve oferecer a capacidade para a configuração segura.

De acordo com Ontreus e Lord [23] ao ser acessado, qualquer site possui um servidor por trás daquele endereço eletrônico responsável por disponibilizar as páginas e todos os demais recursos que uma pessoa pode acessar. Assim, quando o usuário envia um *e-mail* via formulário, coloca uma mensagem em um fórum de discussão, faz uma compra *on-line* etc., um servidor *Web* (ou um conjunto de servidores) é responsável por processar todas essas informações. Um servidor *Web* é um computador que processa solicitações HTTP (*Hyper-Text Transfer Protocol*), o protocolo padrão da *Web*. Quando o usuário usa um navegador de *internet* para acessar um site, este faz as solicitações devidas ao servidor *Web* do site via protocolo HTTP e então recebe o conteúdo correspondente. No caso do Apache, além de executar o HTTP, ele executa também outros protocolos tais como o HTTPS (HTTP combinado com a camada de segurança SSL - *Secure Socket Layer*), o FTP (*File Transfer Protocol*), entre outros. Como servidor *Web*, o Apache⁷ é o mais conhecido e usado (GARFINKEL and SPAFFORD, 1996:961). De acordo com Veiga [33], em se tratando do IIS (Internet Information Server) sabe-se que ele é um conjunto integrado de serviços de rede para a plataforma Windows de 32 *bits* (principalmente o Windows NT/2000 Server) que permite publicar conteúdo e disponibilizar arquivos e aplicações em um ambiente *Internet/Intranet*. Totalmente integrado ao sistema operacional e dotado de uma interface administrativa gráfica, o IIS pode ser uma das melhores opções disponíveis para hospedagem de *web sites*, site FTP e grupos de notícias, bem como para o desenvolvimento de aplicações. Entretanto não há apenas vantagens no que se refere ao IIS. Há também desvantagens em seu uso no sistema. Quanto às desvantagens que o IIS é possuidor, está a impossibilidade de este poder citar a integração da segurança do servidor com a autenticação do Windows 2000. Neste programa, tudo funciona a partir da mesma base de dados de usuários. Isso ocorre de forma que a Conta Guest⁸ precisa estar habilitada no *Windows 2000* para que outros usuários tenham permissão para acessar seu *site Web*. Este recurso é muito interessante para quem já está acostumado a

⁷ Os motivos para esse reconhecimento incluem seu excelente desempenho, segurança, compatibilidade com diversas plataformas e todos os seus recursos. Embora sua reputação quanto à segurança possa parecer arranhada pela descoberta de vulnerabilidades, a configurabilidade e as opções de segurança disponíveis para administradores ainda fazem dele uma excelente escolha.

⁸ No Sistema operacional Windows 2000/2003 Server, existem algumas contas como: de usuário, administrador e a conta convidado é chamada de ContaGuest.

administrar redes *Windows 2000*, mas é muito complicado para pessoas que não estão habituadas com este sistema operacional⁹ (TANENBAUM) [30].

2.4 PARADIGMAS DE SEGURANÇA EM SISTEMAS OPERACIONAIS DE USO CORRENTE

Tanenbaum e Woodhull [30] citam dois paradigmas¹⁰ de segurança em sistemas operacionais de uso corrente: o paradigma de segurança que consiste na concentração e isolamento dos direitos privilegiados do computador e o paradigma de segurança presente nesses sistemas que consiste do usuário como limitador de segurança. O primeiro paradigma de segurança presente nesses sistemas trata-se do próprio usuário que os opera. Enquanto paradigma de segurança age como limitador da entrada de elementos estranhos que possam burlar a segurança e atingir o sistema da rede de computadores. Para que a limitação ocorra, ele cria arquivos e aplicações de segurança intra-rede na qual se associa uma linguagem, isto é, o usuário, ao criar esses arquivos e aplicações, associa a estes permissões referentes à leitura, escrita e execução dos programas. Em alguns casos, essas permissões são expandidas a um conjunto maior de situações em que aparecem ações mais específicas para si próprio, para usuários do mesmo grupo e para os demais usuários do sistema (TANENBAUM, 2005: 1120). Segundo o autor, a esse conjunto de permissões associados aos arquivos denomina-se domínio. Dessa forma, fica sob a responsabilidade do usuário restringir os arquivos/recursos que julgar relevante.

⁹ Por sistema operacional de uso corrente, estão sendo englobados os sistemas mais difundidos em organizações e computadores pessoais. Neste grupo, são enquadrados os derivados do Unix (Linux, BSD e suas várias distribuições), o Windows (com destaque ao NT, 2000 e XP) e o MacOS. Esses sistemas são derivados dos [sistemas operacionais de terceira geração](#), em especial o Unix. Nele as preocupações de segurança se restringiam aos poucos usuários que tinham acesso ao computador, diretamente via terminal, ou pela rede interna isolada a qual pertencia a máquina e o [DOS](#) no qual preocupações de segurança de recursos não existiam.

¹⁰ Paradigmas nesse contexto têm o mesmo significado de modelos no sentido pleno. Isso porque existem paradigmas defectivos, e que, portanto não têm sentido pleno, utilizados no uso da língua em relação às ações das pessoas. Paradigmas defectivos na linguagem humana possuem falhas na forma. Por exemplo, formas de verbo defectivo em português. O que se quer alcançar com essa pequena descrição é que não se generalize o conceito de paradigma como algo ou alguém livre de falhas e defeitos. Aliás, os paradigmas são constantemente postos à prova e muitos deles são quebrados.

De forma similar, ao ser executada uma aplicação, esta passa a ter acesso ao domínio do usuário, podendo interagir com aplicações e/ou arquivos de maneira idêntica ao que faz o usuário de quem foi obtido o domínio e suas informações. Adicionalmente, existem situações em que se deseja permitir que um usuário, por intermédio de uma aplicação apropriada, possa interagir com o sistema operacional como se fosse outro usuário. Nestes casos são associadas *flags* ao sistema que permitam o chaveamento de direitos. No Linux, por exemplo, existe o *bit* SetUID associado às aplicações. Quando ativas, as aplicações passam a ser executadas no domínio do seu proprietário, e não no do usuário que comandou a execução (GARFINKEL ; SPAFFORD) [11].

O segundo paradigma de segurança a ser discutido, como foi visto, consiste na concentração e isolamento dos direitos privilegiados do computador. Esse paradigma serve como uma barreira de proteção de informações que não podem ser acessadas por pessoas não autorizadas mesmo que estas possuam tráfego livre pelos sistemas operacionais. Ou seja, os sistemas operacionais possuem um usuário o qual é denominado superusuário ou administrador. Ele, por sua vez, tem acesso a todos os recursos da máquina. Entretanto esse acesso não é irrestrito. Embora a primeira impressão a esse respeito seja a de que a sua função seja ilimitado, o superusuário na verdade tem que obedecer a restrições aplicadas a todas as operações privilegiadas. Mesmo assim, é importante ressaltar que o domínio do superusuário compreende acesso irrestrito a todos os recursos do computador, inclusive acesso aos arquivos e aplicações pertencentes aos demais usuários. Isso ocorre porque a importância de um administrador não se define como a de usuários comuns. No caso de usuários comuns e suas respectivas aplicações só é permitido a estes o acesso a um subconjunto de operações privilegiadas, e ainda assim limitado¹¹ pelas decisões do núcleo do sistema operacional.

¹¹ Essa limitação se dá a partir de uma interface bem definida com o sistema operacional, também conhecida como *API – Application Programming Interface*. Dessa forma, garante-se que os usuários comuns não possam causar alguma falha de operação ao sistema operacional, seja acidentalmente, seja intencionalmente. Assim, como pode ser observado, o acesso às operações privilegiadas é total ou nenhum, já que a *API* é responsável por controlar o acesso indireto realizado pelas aplicações. Nesse contexto, existem aplicações que por necessitarem de acesso a alguma operação privilegiada não provida pela *API* acabam tendo que usar o domínio do super-usuário. O que lhe dá permissão de acesso irrestrito a todas as operações privilegiadas como dizem.

2.5 VULNERABILIDADES EM PROGRAMAÇÃO WEB

De acordo com Mike Shema e Yen-Ming Chen [26] conceitos de codificação segura que são proibidas e estão em determinadas linguagens como, por exemplo, o conceito da codificação que está fora da linguagem JAVA. É possível que esses conceitos sejam possuidores de aspectos mais importantes e menos usados e, que por isso estejam ausentes em linguagens cujas características não estejam de acordo com especificações e comentários completos no código-fonte e código reutilizável. Certas partes do código-fonte se ‘autodocumentam’ caso as suas variáveis sigam convenções de nomeação padrão e as funções dessas variáveis sejam descritas. Por outro lado, os comentários completos são necessários a partir do momento em que são descritas as suposições a que uma função faz parte quando ao receber e retornar valores. O código reutilizável pode melhorar a capacidade de manutenção de uma aplicação *Web*. Por exemplo, deve ser necessário escrever uma única biblioteca de rotinas de validação de entrada. A aplicação só precisa fazer chamada a essa biblioteca básica via dados fornecidos pelo usuário. Depois, se algum filtro¹² de validação de entrada for julgado insuficiente, será necessário fazer mudanças somente em um arquivo – não em vários arquivos espalhados por toda a aplicação.

Infere-se, portanto, a partir dos dados acima, que o melhor lugar para combater ataques de aplicações *Web* é no próprio código-fonte. Os desenvolvedores de código-fonte podem frustrar a maioria dos tipos de ataques seguindo bons padrões de codificação, como por exemplo, um tratamento de erros adequado e uma validação de entrada robusta para todos os dados fornecidos pelo usuário. Com isso, os desenvolvedores podem empregar uma verificação das técnicas comuns para melhorar a segurança de sua aplicação. O quadro nº 7 a seguir ilustra uma breve lista de verificação das técnicas comuns já desenvolvidas:

¹² Já se sabe que a *Open Web Application Security Project* (www.owasp.org), já trabalha em uma coleção de filtros de validação de entrada de fonte aberta, bem como em recomendações comuns para codificadores.

Quadro nº 07: Breve lista de verificação das técnicas comuns já desenvolvidas.

Fonte: Shema (2003). Elaboração do autor.

Lista de verificação das técnicas comuns

- Código-fonte
 - ✓ Os comentários do desenvolvedor são incluídos entre delimitadores de linguagem e não aparecem no código-fonte HTML recebido pelo navegador. Delimitadores de linguagem comuns: `<% %>` `<? ?>`;
 - ✓ Os comentários fornecem uma descrição suficiente para cada função e variável;
 - ✓ De algum código foram retirados os comentários? Por quê? Ele precisa ser removido ou corrigido?
 - ✓ Os comentários refletem o código real? Ou como o programador deseja que o código funcione?

Podem-se aqui também ser citadas outras formas seguras no código-fonte como: Autenticação, Manipulação de sessão, Tratamento de erros, Manipulação de banco de dados, Manipulação de arquivos, Eventos de auditoria de aplicação e validação de entrada.

- Autenticação: O nome do usuário não é baseado no Social Security Number (SSN). O SSN é uma informação confidencial do usuário e deve ser tratado como tal – não deve ser usado como um identificador arbitrário.
- Manipulação de Sessão: O token de sessão é criado com segurança. Ele implementa um selo de tempo (timestamp) para minimizar os ataques de repetição.
- Tratamento de Erros: Os erros http 500 são capturados sempre que possível. Uma página padrão é retornada ao usuário. Essa página não contém qualquer informação de estado interna como nomes de variável, nomes de arquivos ou consulta de dados.
- Manipulação de Banco de Dados: Credenciais de conexão são armazenadas de uma maneira segura. Se o nome de usuário e a senha do *db* precisar ser armazenada em texto claro dentro de um arquivo, as permissões de leitura desse arquivo são restritas. Adicionalmente, o arquivo não é armazenado dentro da raiz de documento Web.
- Manipulação de Arquivos: As referências de arquivos removem todos os caracteres de mudança de diretório.
- Eventos de Auditoria de Aplicação: O ID de usuário e o endereço IP de origem são registrados para sucesso e falha de autenticação.
- Validação de Entrada: Antes de os filtros de entrada serem aplicados, os dados são normalizados para um conjunto de caracteres padrão. Todos os caracteres codificados para URL são interpretados.

2.6 ITENS ESPECÍFICOS DA LINGUAGEM COMPUTACIONAL

A segurança de uma aplicação se deve à disciplina dos programadores, não à linguagem usada para codificar a aplicação. Entretanto, há certos métodos e cuidados exclusivos a algumas linguagens comuns usadas em aplicações Web. A figura nº1 ilustra os tipos de linguagens utilizadas e a sua relação com a disciplina do programador. Tendo em vista a segurança de uma aplicação, o programador se insere no

centro e as linguagens usadas para codificação e aplicação estão subordinadas. A ordem não foi considerada:

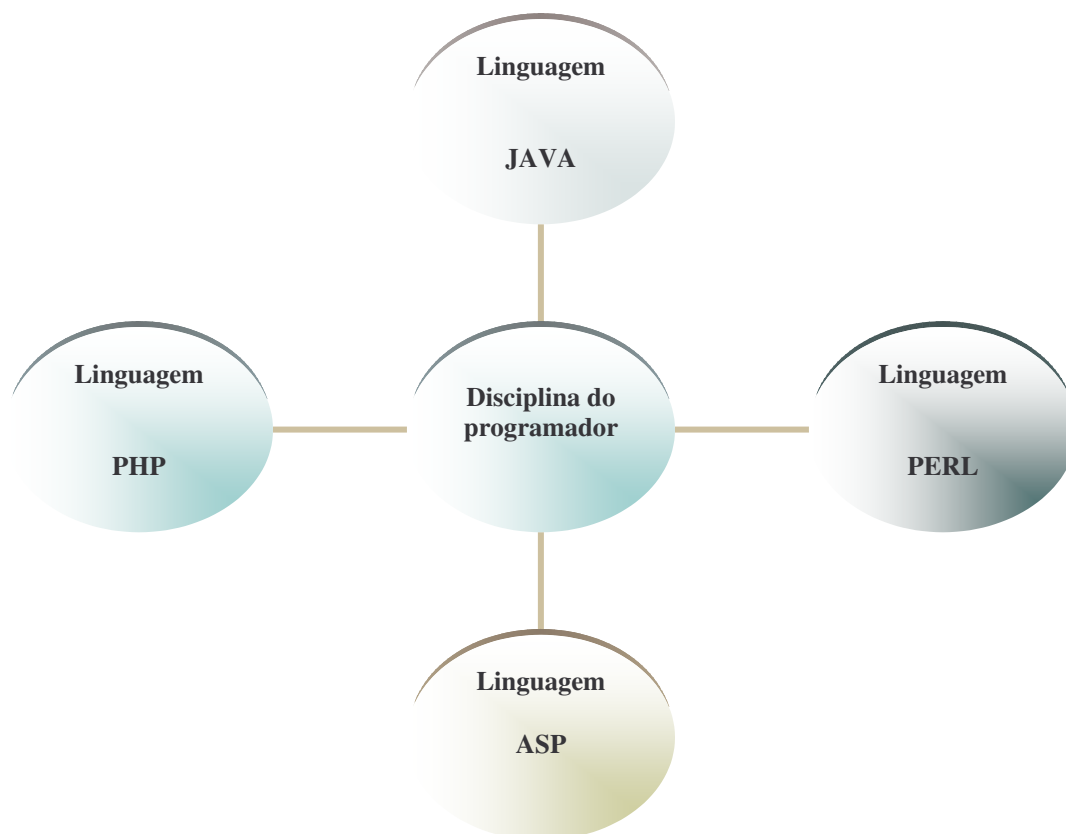


Figura nº 01: Ilustração da importância do programador e sua disciplina para com a segurança de uma aplicação.

Fonte: Horton (2003). Elaboração do autor.

De acordo com Mike Shema e Yen-Ming Chen [26] pode observar na figura 01 há quatro tipos de linguagens distribuídas em linguagem JAVA, a linguagem PERL, a linguagem ASP e por último a linguagem PHP. Todas ligadas à disciplina do programador. Agora, pode-se discutir e descrever cada uma dessas linguagens. Na linguagem JAVA as aplicações aí baseadas apresentam um problema peculiar para os desenvolvedores de aplicação. O código de byte do Java é projetado para rodar em qualquer plataforma. Conseqüentemente, é muito fácil converter um arquivo Java compilado em seu código-fonte original. Esse *não* é o caso das linguagens compiladas, como C ou C++. Contudo, a maioria das aplicações que empregam Java intensamente usa execução de Java do lado servidor. Ou seja, o código é interpretado por uma JVM

(Máquina Virtual Java) no servidor e o resultado é apresentado no navegador Web do usuário. Em alguns casos, a aplicação pode ter um applet Java que se destina a ser baixado e executado no navegador do usuário. Em qualquer caso, se um usuário puder obter os arquivos *.class originais, então, é possível obter, através da engenharia reversa informações úteis. Algumas credenciais para a descoberta são as credenciais de banco de dados, construção de consultas SQL, rotinas de criptografia personalizadas e *stream* de programa.

Na linguagem ASP um dos maiores erros nas aplicações é o mau uso dos arquivos *include*. Quando esses arquivos contêm a lógica básica da aplicação, é muito importante conter seu conteúdo protegido da visão. A primeira atitude é nomear qualquer extensão .inc para .asp de modo que um servidor IIS analise o arquivo *include* e mantenha privado tudo o que estiver entre as tags `<% %>`. Em relação à linguagem PERL, sua maior vantagem é seu mecanismo de expressão regular. Regexes(sintaxe de expressão regular na linguagem Perl) corretos para validação de entrada podem levar a uma aplicação bastante segura. Por outro lado, ela não possui tipos variáveis. Assim, “\$foo” pode conter “var”, “12345”, “(*&\$^#\$(&*” ou quaisquer caractere estranho, mesmo caracteres *NULL* múltiplos. Quanto à linguagem PHP, o que se tem a dizer é que esta se tornou rapidamente uma das linguagens preferidas dos desenvolvedores *Web*. Ela tem as mesmas capacidades de segurança da PERL. Parece semelhante, o que facilita a migração mental para a codificação PHP. Por outro lado, o mecanismo PHP teve algumas falhas de segurança graves no passado. Por exemplo, vinha habilitado o *allow_url_fopen* no *php.ini*, abrindo assim oportunidades de ataques do tipo *cross-site scripting*(este método de ataque aparece em páginas que oferecem serviços de *blogs* e fóruns que são acedidos pelo público em geral). Qualquer empresa que permite aos seus empregados ter acesso a páginas web que são sociais e interativos, por exemplo *blogs* e fóruns podem ser afetados, porque os visitantes destas páginas podem não estar seguros da legitimidade da empresa que hospeda a página. *Hackers* hospedam este tipo de conteúdo malicioso para obter acesso a dados do utilizador como *passwords*(senhas) e dados privados através de manipulação de tags embutido em código HTML.) ou de execução de comando arbitrário.

3

Ferramentas para detecção de vulnerabilidades (*Sniffers*)

3.1 DIAGNÓSTICO DE SEGURANÇA DO AMBIENTE COMPUTACIONAL

Realizar um diagnóstico de segurança do ambiente é o primeiro passo para a definição da melhor estratégia de proteção para qualquer empresa. Além do conhecimento sobre a natureza de ataques e sobre diferentes aspectos envolvidos com a segurança (tecnologias, processos, pessoas), o diagnóstico envolve também o conhecimento sobre diferentes técnicas e o uso de ferramentas. Conhecer a situação de segurança das empresas, portanto, é importante para que eventuais vulnerabilidades sejam corrigidas antes que elas sejam exploradas por *hackers*. Nesse contexto, realizar um diagnóstico seguro envolve além de conhecimentos sobre a natureza dos ataques, conhecimentos sobre vulnerabilidades existentes e sobre métodos de verificação de resultados gerados pelas ferramentas. A análise, que envolve diagnóstico de segurança do ambiente e a verificação de vulnerabilidades, é o início para um ambiente de rede mais seguro. Com a análise de segurança é possível identificar as vulnerabilidades que devem ser corrigidas. Assim, surgem novas características do profissional de segurança:

O trabalho do profissional de segurança envolve o exame de segurança, as correções das vulnerabilidades encontradas, o planejamento dos controles para minimizar os riscos encontrados, e a realização dos controles definidos.

3.2. Ferramentas de pesquisa a vulnerabilidades

Com novas características, o Profissional de segurança possui em mãos ferramentas de apoio que vão facilitar o seu trabalho. Para tanto, estão dispostas para uso nesse contexto os sete seguintes instrumentos: *Nmap*, *Nessus*, *Netcat*, *Dsniff*, *Ethereal*, *Languard* e *Wargoogle*. A partir de agora cada uma dessas ferramentas será apreciada seguindo a ordem a partir de *Nmap*. Uma das principais ferramentas de pesquisa da vulnerabilidade, o *Nmap* ou *Network Mapper*, pode ser encontrado em <<http://www.insecure.org/nmap>>. O *Nmap* pode ser utilizado tanto em Sistemas operacionais Linux quanto pelo Windows, possuindo assim alguns *front-ends* gráficos, o que facilita seu manuseio. Ele realiza mapeamento do ambiente em busca de *hosts* ativos, sendo capaz ainda de identificar o sistema operacional de cada um deles (os *Fingersprinting*) e, principalmente, saber qual o tipo de serviço que está rodando e que está sendo provido pelo *host*. A seguir, o quadro oito mostra a sintaxe de algumas opções do Nmap com as potencialidades ou funções da ferramenta. Logo após, a figura dois ilustra a ferramenta de console no Windows. Na figura, o Nmap para Windows¹³ mostra os detalhes e os tipos de *scanners* detalhando o resultado de uma varredura feita em uma rede *ethernet*. Em seguida, a figura três ilustra o comando `nmap -sS -n -O` sendo executado no console do Linux¹⁴ em que o Nmap é usado na versão deste programa para este Sistema operacional.

¹³ Comando no console do Windows: `c: \> nmap [tipo de scan] [opções] < numero. ip.da.vitima >`

¹⁴ Comando no console do Linux `[root@host] # nmap [tipo de scan] [opções] < numero.ip.da.vitima >`

<i>Sintaxe</i>	<i>Função</i>
<i>sT</i>	Faz a conexão TCP completa para descobrir portas TCP abertas.
<i>sS (SYN Scan)</i>	Serve para descobrir portas TCP abertas sendo ligeiramente mais discreto.
<i>sF (FIN Scan)</i>	Para descobrir portas TCP abertas e ser ainda mais discreto que o <i>-sS</i> . Não funciona se a máquina sob teste estiver rodando Windows.
<i>sX (Árvore de Natal)</i>	Manda os flags FIN, URG e PSH ligados para descobrir portas TCP abertas e ser mais discreto que o <i>-sS</i> . Não funciona se a máquina sob teste estiver rodando Windows.
<i>sN (Null Scan)</i>	Manda pacotes TCP sem nenhum <i>flag</i> ligado para descobrir portas abertas; dessa forma, também consegue ser mais discreto que o <i>-sS</i> . Não funciona se a máquina sob teste estiver rodando Windows.
<i>sU (UDP Scan)</i>	Serve para descobrir portas UDP abertas. Como não há conexão no protocolo UDP (a comunicação fica com problemas), é mais difícil detectar um <i>portscan</i> em suas portas.

Quadro nº 08: Sintaxe de algumas opções do Nmap com as potencialidades ou funções da ferramenta
 Fonte: Shema (2003). Elaboração do autor.

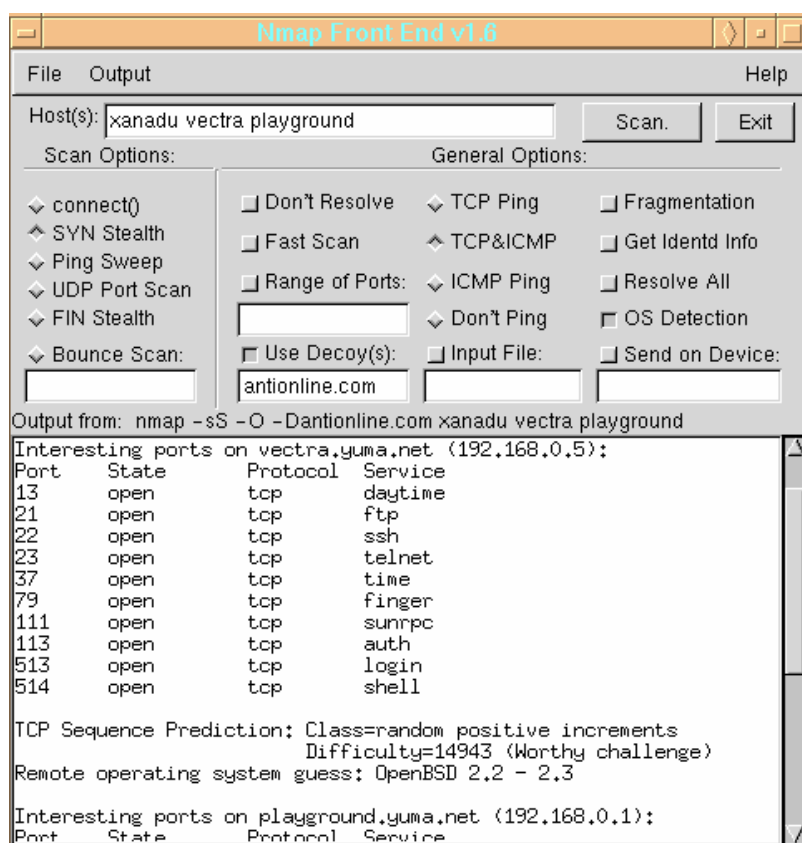


Figura 02 - Nmap versão para Windows.

Fonte: Universidade Hacker (2005).

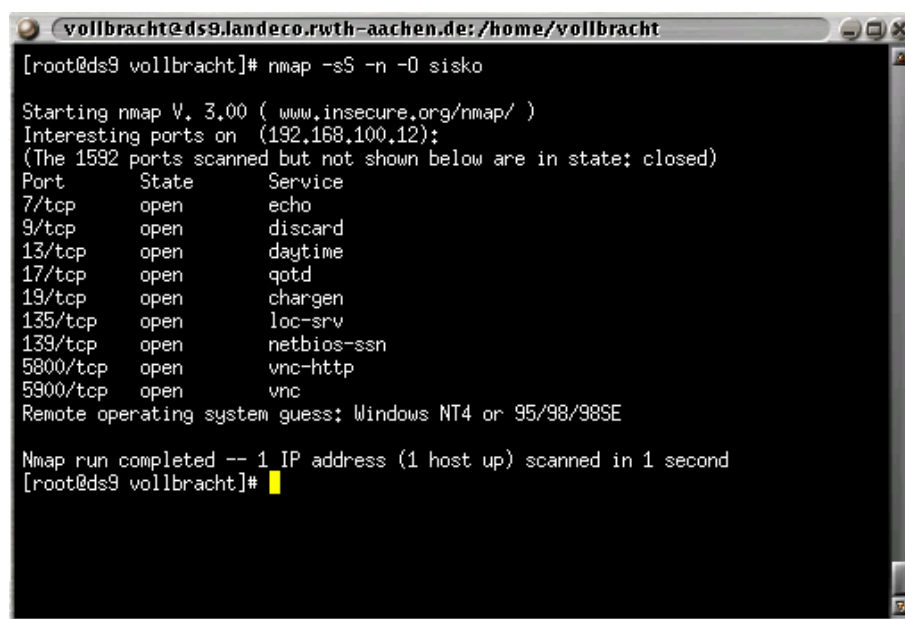


Figura nº 03: Nmap versão para Linux

Fonte: Universidade Hacker (2005)

Utilizado em conjunto com o Nmap, há uma outra ferramenta importante. É a ferramenta Nessus. Ela forma um conjunto poderoso capaz de realizar o diagnóstico preliminar da segurança de qualquer ambiente ou servidor específico. Ao contrário de outros *scanners* de vulnerabilidade, o Nessus não confia nas portas-padrão para determinar o tipo de serviço oferecido por cada uma delas. Por exemplo, se o Nessus notar um serviço rodando na porta 80, não vai informar, sem comprovação, que aquele é um servidor Web. Pelo contrário, vai aplicar todos os testes que conhece para saber qual o serviço e se está ou não vulnerável. Saber usá-lo é fundamental, porém o mais importante é saber analisar de forma correta os resultados oferecidos por esta ferramenta. A seguir a figura quatro ilustra a tela de relatório linguagem Nessus.

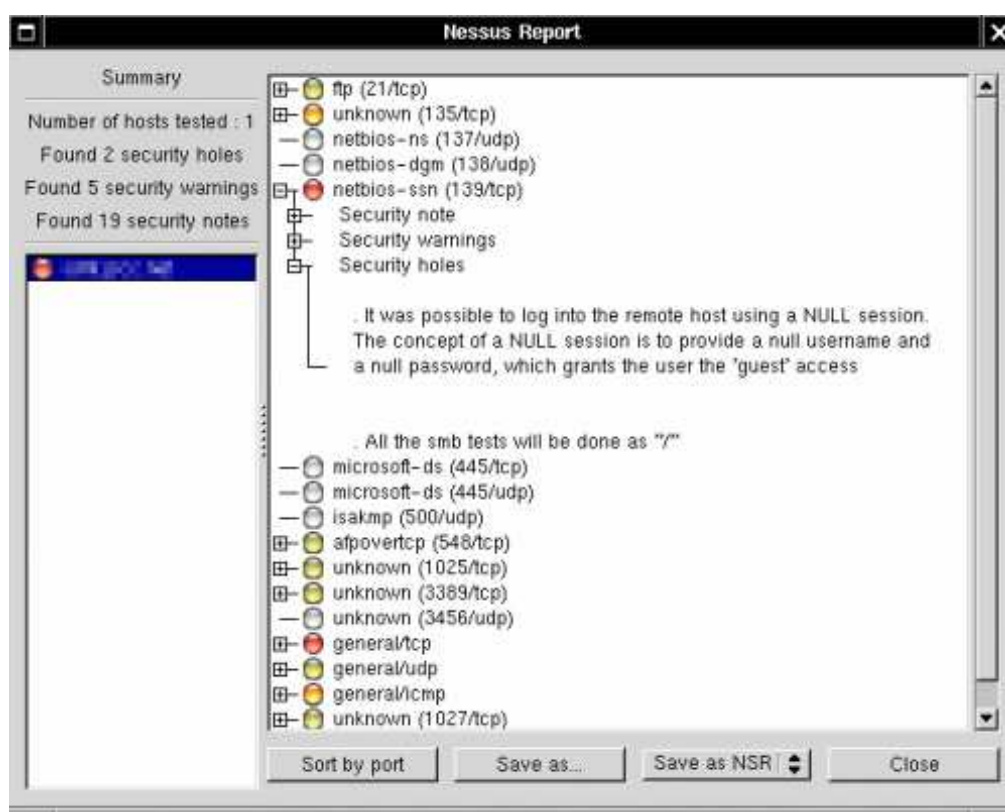


Figura nº 04: Tela de relatório do Nessus
Fonte: Bravo Tecnologia (2006)

A terceira ferramenta a ser apreciada agora é a Netcat. Ela foi desenvolvida em 1996. É considerada um “canivete suíço” da rede, devido à sua versatilidade. Sua

principal característica é a capacidade de ler e escrever dados em conexões de rede, usando o protocolo TCP ou UDP. Essa característica faz com que o instrumento atue como “*back-end*”, ou seja, para ser integrado com programas e scripts. Assim, ele pode funcionar também como um servidor, aguardando conexões em uma porta arbitrária, como se fosse um *Telnet*. Seu uso é simples, porém exige um conhecimento sobre protocolos, já que envolve o envio de mensagens da especificação para que tarefas efetivas possam ser realizadas. A figura cinco ilustra o comando do Netcat no console do Windows:

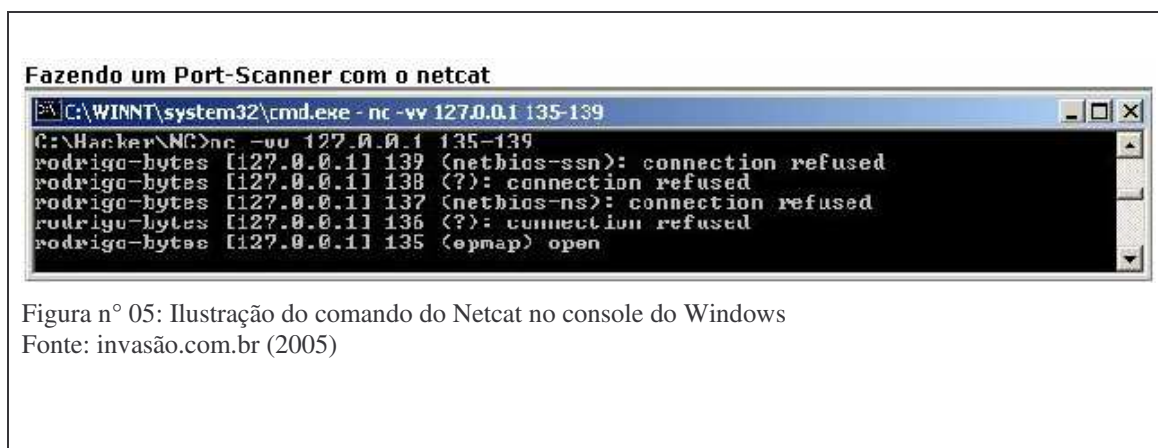
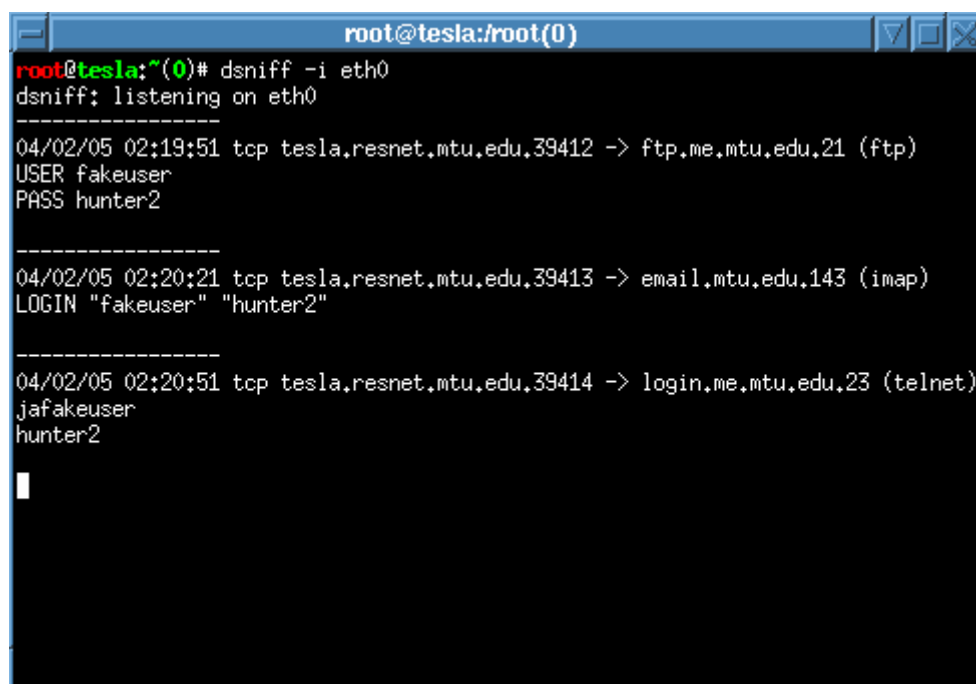


Figura nº 05: Ilustração do comando do Netcat no console do Windows
 Fonte: invasão.com.br (2005)

A quarta ferramenta a ser apreciada é a *Dniff*. Esse instrumento é composto por um conjunto de ferramentas capaz de realizar auditoria de segurança na rede. As ferramentas presentes nesse grupo mostram algumas capacidades que são importantes para análises de segurança, porém, elas podem ser usadas para fins maléficos, o que exige muita responsabilidade e ética da pessoa que tem acesso sobre as mesmas. As ferramentas são capazes de monitorar passivamente a rede em busca de pacotes específicos (*dsniff*, *filesnarf*, *msgsnarf*, *urlsnarf*, *webspy*), de interceptar o tráfego (*arp spoof*, *dnsspoof*, *macof*) e de realizar ataques *man-in-the-middle* (*sshmitm* e *webmitm*). A figura seis ilustra e demonstra a tela de comando *Dsniff* via console no Windows.



```
root@tesla:/root(0)
root@tesla:~(0)# dsniff -i eth0
dsniff: listening on eth0
-----
04/02/05 02:19:51 tcp tesla.resnet.mtu.edu,39412 -> ftp.me.mtu.edu,21 (ftp)
USER fakeuser
PASS hunter2
-----
04/02/05 02:20:21 tcp tesla.resnet.mtu.edu,39413 -> email.mtu.edu,143 (imap)
LOGIN "fakeuser" "hunter2"
-----
04/02/05 02:20:51 tcp tesla.resnet.mtu.edu,39414 -> login.me.mtu.edu,23 (telnet)
jafakeuser
hunter2
```

Figura nº 06: Tela de comando do Dsniff via console no Windows.
Fonte: invasão.com.br (2005).

A quinta ferramenta trata-se do *Ethereal*. Este instrumento se caracteriza por ser muito simples de se trabalhar¹⁵. Possui *menu* bem intuitivo, cujas principais funções estão relacionadas com a barra de ferramentas que por sua vez pode servir como atalho para o sistema. A ferramenta em questão possui uma coleção de filtros para a sua captura de pacotes, trabalhando com mais de 300 protocolos de comunicação diferentes, desde os mais simples (TCP, Telnet etc.) até os mais específicos (AIM, IMAP etc.). Sua

¹⁵ Ao observar o *Ethereal* com olhos de analista de segurança, sugere-se a todos os administradores de redes a adotá-lo como uma ferramenta de monitoramento dos pacotes que trafegam em sua rede. Muitas vezes, algumas ferramentas que os Hackers utilizam para invadir, servem também como *anti-hackers*. Um outro forte motivo para adquiri-lo seria a facilidade que se tem de controlar e saber o que seus usuários (internos da empresa) estão conversando com o mundo externo ou enviando dados sigilosos da empresa.

interatividade se dá por captura de dados, o que acontece via visualização, com informações ricas, incluindo filtros específicos e a habilidade para visualizar flags de cabeçalho dos pacotes receptados. Assim, ele pode capturar dados de dispositivos ethernet, token-ring, FDDI, LAN wireless (802.11), conexões ATM e uma série mais de dispositivos de redes. A seguir a figura sete mostra a tela inicial da ferramenta Ethereal.

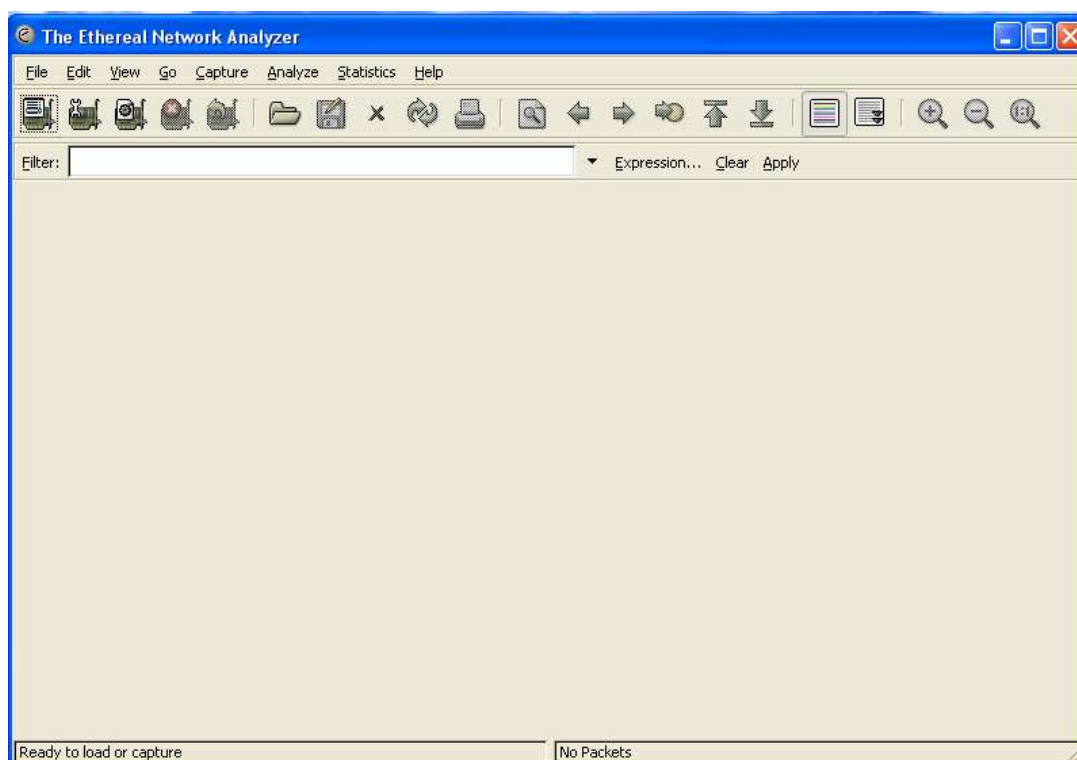


Figura nº 07: A tela inicial do Ethereal
Fonte: Universidade Hacker (2005)

A sexta ferramenta a ser apresentada é o *LanGuard*. Ela se encontra na categoria dos *scanners* ‘híbridos’. Possui por isso características de detecção de portas e vulnerabilidades. Essa é uma espécie de integração que a torna muito simples de operar. Além de facilitar a interpretação dos resultados, apesar de deixá-lo com menor poder e pouca flexibilidade. É boa como ferramenta para ser usada no dia-a-dia, para o administrador de redes¹⁶, embora os *crackers* e consultores de segurança da informação

¹⁶ Principalmente redes Microsoft.

usem scanners mais poderosos. A seguir, a figura oito representa a tela inicial da ferramenta LanGuard.

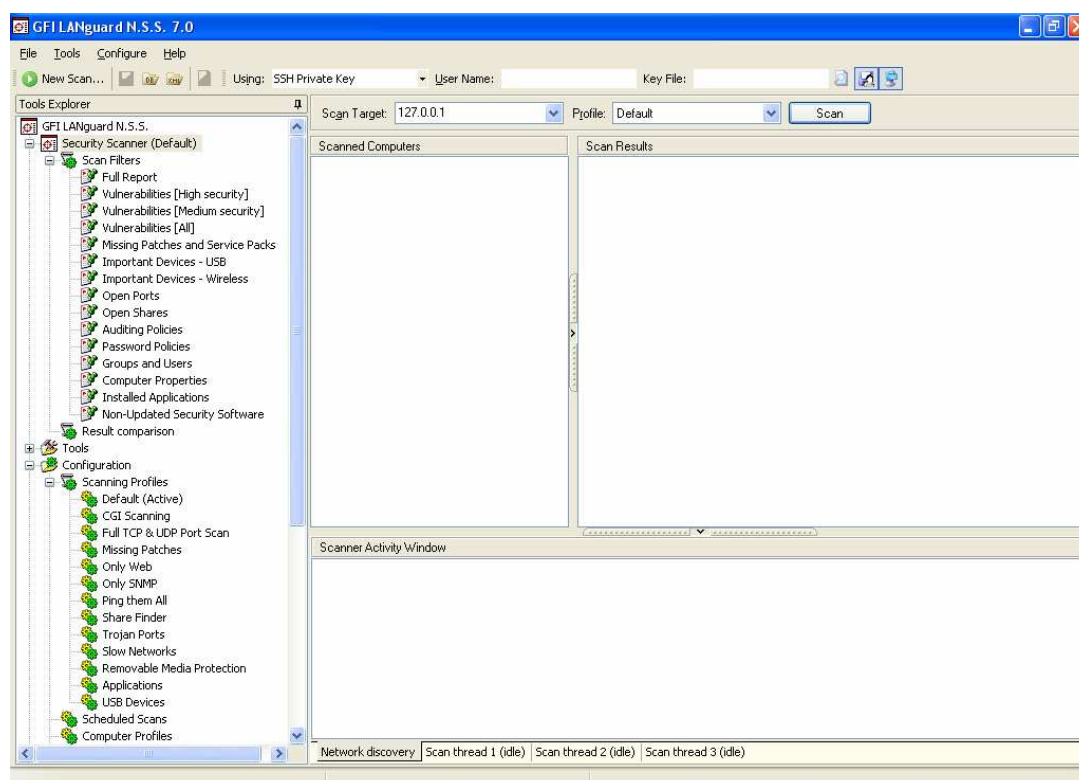


Figura nº 08: A tela inicial do LanGuard.

Fonte: GFI.org (2005)

A última ferramenta da lista mostrada no início dessa discussão trata-se do *Google*. Este instrumento é considerado de alta importância por ser uma ferramenta altamente qualificada para enfrentar as tentativas de invasões. Porém, o que vale ser mencionado aqui é o que na literatura se costuma chamar de Engenharia do Conhecimento. Com ela, consegue-se ter acesso a variedades de comandos que se pode executar para um ataque a partir do portal *google*.

Enfim, para manuseá-la, basta apenas que seu usuário possua conhecimentos em comandos específicos para tal. A seguir a figura nove representa a tela principal de pesquisa google.



Figura nº 09: Tela principal de pesquisa do Google.
Fonte: GFI.org (2005)

4

Estudo de Caso

4.1 Passos da pesquisa

Esse tópico da pesquisa dá acesso ao estudo de caso proposto sobre a segurança digital. Para tanto o trabalho se inicia com a apresentação dos objetivos da pesquisa que vão desde o geral aos específicos, sua hipótese, a coleta de dados e os teste aplicado. Em seguida trabalha-se a análise de dados e os resultados obtidos.

4.1 Objetivos da pesquisa

O presente estudo teve como objetivo geral identificar as falhas de segurança em que uma empresa denominada Teste invasão possui. Nesta pesquisa optou-se por se trabalhar com objetivos específicos direcionados para a discussão do assunto. Trabalhou-se também com os objetivos específicos de discutir e descrever os aspectos gerais sobre segurança da informação como, por exemplo, os fundamentos que perfazem a abrangência do problema, sua contextualização, considerações, a questão dos tipos de invasores e os motivos a que estão ligados, as conseqüências dessas invasões e os principais alvos da segurança de redes e sistema. Um outro objetivo específico foi a verificação da questão das vulnerabilidades em que apareceram os conceitos para o assunto tendo como tópicos as diferenças entre ameaças e vulnerabilidades, a vulnerabilidade em serviços da *web*, os paradigmas de segurança em

sistemas operacionais de uso corrente, as vulnerabilidades em programas *web* e os itens específicos das linguagens utilizadas por sistemas de computadores.

Foram considerados na pesquisa mais três objetivos específicos: apreciar as ferramentas usadas para detecção de vulnerabilidades e manutenção no sistema como forma de facilitar o diagnóstico de segurança do ambiente computacional. Gerar relatório de pesquisa sobre a segurança do sistema durante o estudo e após o seu término. Propor soluções a serem postas em prática a partir da identificação das falhas encontradas.

4.2 Hipótese, justificativa, metodologia e procedimentos

Para o presente estudo trabalhou-se com a hipótese de que as ameaças e riscos intencionais e não-intencionais poderiam representar prejuízos para a segurança de redes e sistemas da empresa Teste invasão caso os mecanismos de defesa para a proteção do ambiente computacional não fossem planejados e realizados com base no conhecimento pré-existente dessas ameaças e dos riscos. Como justificativa, o trabalho teve sua razão de ser na busca de soluções como a implantação de ferramentas para prevenir problemas reais de caráter de segurança de informações de dados, econômicas, integridade física das estações e servidores conseqüentes de ações virtuais em sistemas computacionais. Para alcançar as soluções desejadas e propostas após o resultado da identificação das falhas foi utilizado como metodologia a aplicação de teste via LanGuard instrumento utilizado para a obtenção dos resultados. Nesse sentido, as variáveis utilizadas para o teste na pesquisa foram as falhas encontradas pela ferramenta após a varredura. São elas: Antivírus desatualizados, *Softwares* piratas (*MSOffice* & Sistemas Operacionais *Windows*), senhas fracas, ausência de conhecimento em segurança em TI, serviços desnecessários em execução, pastas compartilhadas sem senhas, falta de IDS (Sistema de Detecção de Intrusos).

Para a obtenção dos resultados referentes ao que foi considerado como falhas humanas, utilizou-se da Engenharia Social. Em termos de proposições aplicou-se um minicurso sobre segurança da informação como iniciativa da diretoria da empresa em melhorar seus aspectos de segurança do sistema contra possíveis ataques. Quanto aos procedimentos de coleta de dados e participantes observou-se o levantamento da

categoria de dados e participantes da pesquisa apresentados como reais e virtuais o quadro nove (9) à frente após o tópico quatro-ponto-três (4.3) e os tipos de dados e participantes levantados. A partir desse levantamento deu-se início o experimento no ambiente computacional e fora dele. Em relação ao perfil da empresa participante é importante observar após os testes terem sido realizados, optou-se por seguir um código de ética em que se tem a certeza de resguardar a identidade da empresa aqui mencionada utilizando-se para isso um nome fictício, por precauções de ordem jurídicas, pois se trata de dados confidenciais da empresa. Lembrando que, não é pretensão aqui apresentar e ensinar, técnicas em ferramentas aqui mencionadas e usadas para testes, onde o uso indevido das mesmas acaba comprometendo o bom funcionamento da rede de uma empresa.

4.3 Coleta de dados

Foram considerados dados para a pesquisa os itens pertencentes ao ambiente computacional da empresa Testeinvásio¹⁷ que forneceu seu ambiente computacional para o levantamento dos dados presentes na pesquisa. Para a coleta de dados utilizou-se nessa pesquisa a ferramenta Languard¹⁸, que teve por objetivo neste trabalho, fazer uma varredura¹⁹ na rede de testes, e foi considerada como parâmetro para a análise dos riscos e ameaças intencionais e não-intencionais para a segurança do sistema em questão. Durante o levantamento foi identificado no ambiente um total de doze variáveis analisadas nesse estudo. A partir disso obteve-se uma quantidade de dados como ocorrência durante a varredura feita pela ferramenta. Dessa forma os dados foram tipificados em reais e virtuais a partir de sua existência dentro e fora do sistema. O quadro nove (09) ilustra o levantamento de dados da pesquisa num total de doze, a distribuição em termos de quantidade para cada dado obtido e a tipificação em ocorrência real e virtual. Para este último caso, considerou-se real a parte física do material posto em teste e virtual a parte de programas manipulados não - fisicamente durante a pesquisa.

¹⁷ Foi preciso fazer essa experiência com a substituição do nome da empresa participante de forma a protegê-la para o não abuso de terceiros no que diz respeito ao seu nome e os interesses da mesma.

¹⁸ De propriedade da empresa GFI Software Ltd, é um scanner de redes com algumas características de detecção de vulnerabilidade.

¹⁹ Jargão usado para explicar que o procedimento adotado é de pesquisar toda a rede que foi selecionada para o teste em questão.

Quadro nº 09: Distribuição em quantidades dos doze dados considerados pela ferramenta LanGuard e as tipificações em real e virtual consideradas na pesquisa.

Fonte: GFI Software LTDA (2006). Elaboração do autor.

<i>1</i>	TestedeInvasão	<i>Real e virtual</i>
<i>1</i>	Servidor – Windows server.	Real e virtual
<i>10</i>	Estações entre Linux e Windows.	Real e virtual
<i>1</i>	Switch	Real
<i>1</i>	Hub	Real
<i>1</i>	Internet Banda Larga.	Virtual
<i>1</i>	Estação com o software VNC, para dar suporte a clientes e simulações de erros na Capital e interior.	Real e virtual
<i>10</i>	Funcionários.	Real
<i>2</i>	Funcionários que dão suporte a cliente tanto interno como externo	Real
<i>1</i>	Sistemas Web – plataforma Delphi/web.	Virtual
<i>30</i>	clientes	Real
<i>1</i>	Recepcionista.	Real
Número de participantes e de dados da pesquisa	Participantes e tipos de dados	Características dos dados e participantes

4.4 Instrumentos

Foram utilizados como instrumentos, um *notebook* para interagir com o sistema da empresa, aparelho telefônico fixo para manter o contato pesquisador-recepcionista a fim de tentar burlar a segurança pessoal de seus dados como senha e *login* registrados na empresa, o programa LanGuard, o ambiente computacional e a engenharia social com a apresentação de um documentário sobre segurança digital. Coletados os dados durante a pesquisa preparou-se um teste de varredura a partir do ambiente computacional dando início a uma verificação na rede da empresa TesteInvasão.com.br²⁰ supostamente

²⁰ O nome e os dados de registros reais da empresa que emprestou seu ambiente para a pesquisa foram ocultados com o uso de tinta preta como forma de proteção e pedido do proprietário. Embora se tenha

invadida. O teste levou em consideração todos os dados obtidos após o seu levantamento tendo em mente a sua ocorrência no mundo real e no mundo virtual observando a questão da segurança digital. Para este estudo de caso foi utilizado como ferramenta de coleta de informações sobre falhas em uma rede que interliga os computadores da empresa pesquisada o programa Languard. Optou-se por usá-lo por se tratar de uma ferramenta de maior uso nesse tipo de teste de vulnerabilidade. Para validação da pesquisa optou-se por seguir as orientações da linha seguida pela GFI Software Ltda que é a responsável pela criação do LanGuard e a Teoria da Engenharia Social aplicada como forma de mostrar que a parte humana da empresa pode estar à mercê de invasores que trafegam pela rede. A seguir, a figura dez (10) ilustra a tela inicial da ferramenta LanGuard utilizada para captar as falhas e os dados por ele pesquisados durante o estudo:

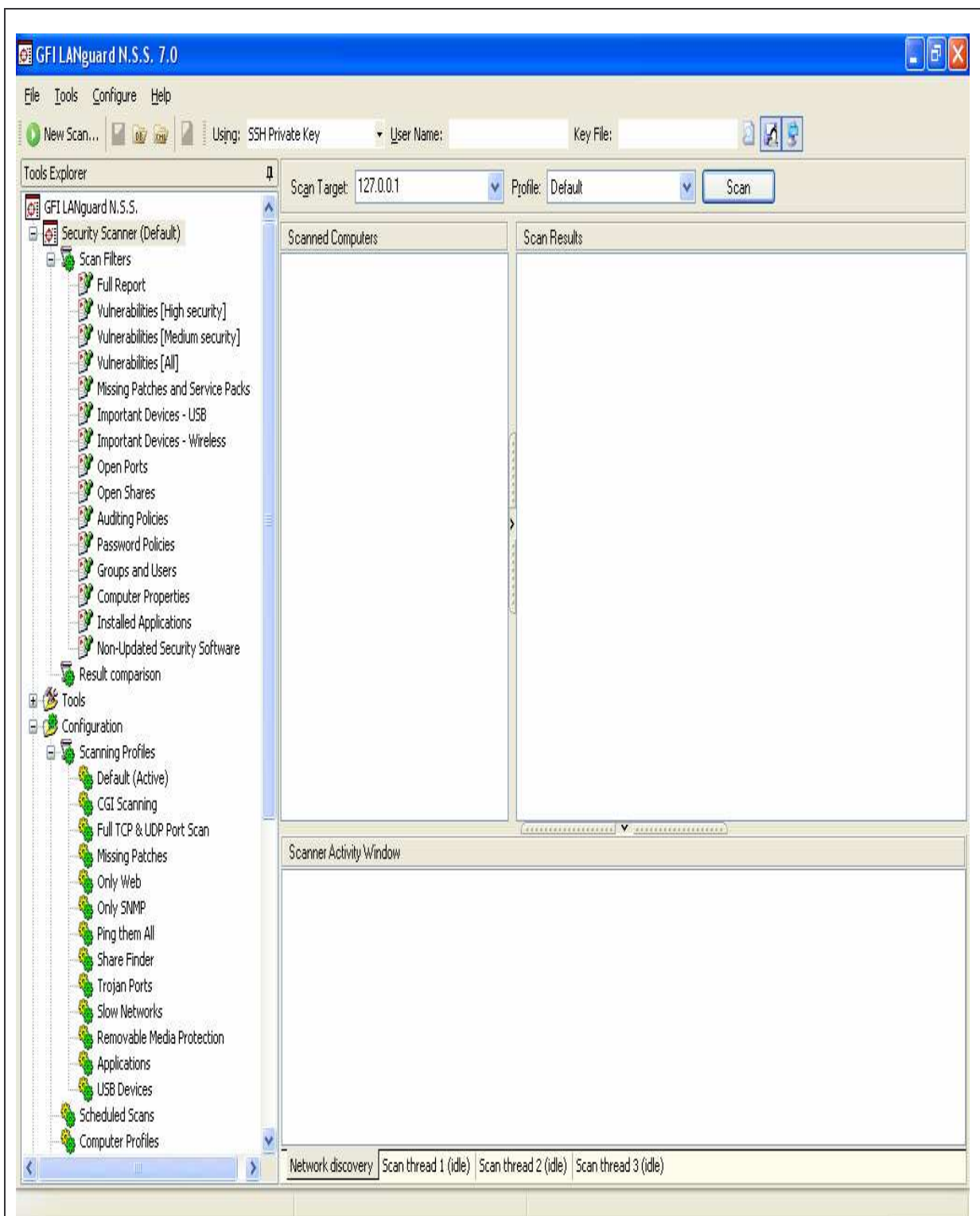


Figura n° 10: Tela inicial do LanGuard.
 Fonte: GFI Software Ltda (2006)

4.5 Testes

Os testes utilizados na pesquisa foram aplicados no ambiente computacional da empresa TesteInvasão . O total de testes aplicados foi dois, a saber: Um teste com uso da ferramenta LanGuard e um teste com uso da Engenharia Social. No segundo teste via telefone simulou-se uma conversa na qual se tentou persuadir a funcionária a revelar sua senha e seu *Login* de acesso a dados importantes da empresa. Foi preciso fazer esse procedimento para demonstrar que a parte humana que dá os comandos para o computador e se utiliza da rede para trafegar e fazer trafegar informações sigilosas da empresa, enviar mensagens importantes referentes a negócios importantes da empresa etc., pode se tornar instrumento de uso dos invasores de sistema e de redes de computadores.

4.6 Análise de dados da pesquisa

Para dar início a varredura, digitou-se em *ScanTarget*²¹, o número IP (ou endereço) da empresa em teste: numero.do.ip.da.empresa, e em seguida clicou-se em *Scan*, com LanGuard instalado em um notebook do suposto invasor (consultor de vulnerabilidade) e conectado a mesma rede *ethernet*. A figura onze (11) ilustra duas máquinas ativas na rede em questão que foram detectadas pelo LanGuard. Na figura elas foram denominadas como cobaia e cobaia um (01). A mancha em destaque sobre a identificação real da empresa testada foi usada como forma de proteção ao seu sistema. Depois de feito o scan pela ferramenta em tempos distintos, como se pode ver na parte que diz duração da varredura²², a seta em destaque do lado da cobaia um (1) e a cor vermelha em destaque no texto informativo inferior indica que uma das cobaias está infectada. Note-se também que os tempos de ambas são diferenciados. Enquanto a cobaia não infectada ou invadida foi varrida em dois minutos e quinze segundos (2 minutos e 15 segundos), a cobaia infectada ou invadida foi varrida em mais tempo com a duração de três minutos e quinze segundos (3 minutos e 15 segundos), o que deu uma diferença de dez minutos para que a LanGuard pudesse encontrar algum problema no sistema.

²¹ Uma opção no Software LanGuard onde se define uma faixa de IP válido para se fazer uma varredura na rede.

²² Scan duration

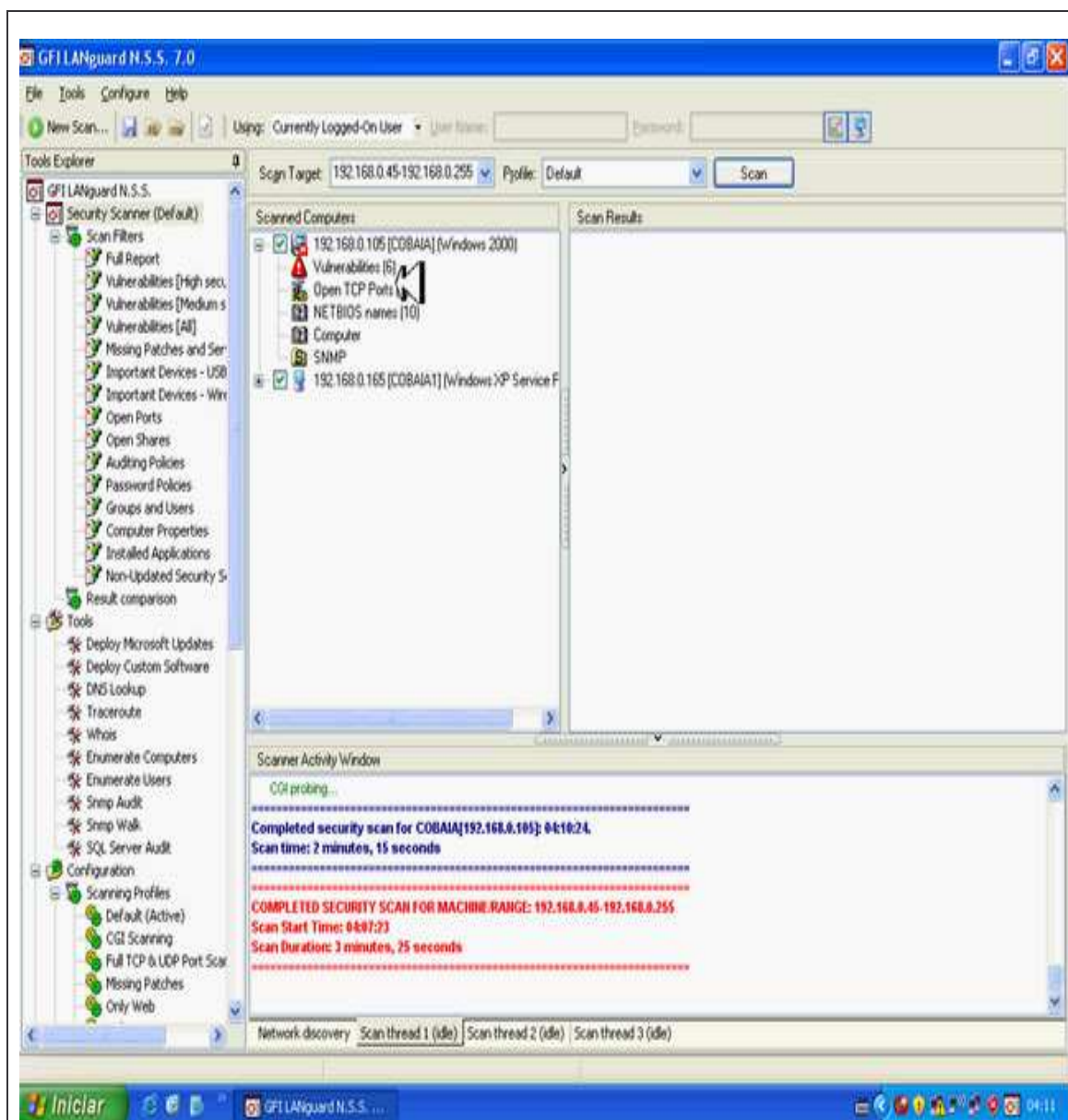


Figura nº 11: Máquinas ativas na rede
 Fonte: GFI Software Ltda (2006)

Com o quadro anterior verificou-se que o LanGuard conseguiu detectar as duas máquinas ativas na rede como já foi mencionado. Esse foi o primeiro teste para

identificar possíveis ameaças e riscos intencionais e não-intencionais que poderiam representar prejuízos para a segurança de rede e sistema da empresa Teste invasão. Isso significa dizer que com esse desempenho a ferramenta até o presente momento confirmou as suspeitas de possíveis vulnerabilidades apresentadas pela ferramenta utilizada. Mais detalhadamente, ao final do primeiro teste, o programa mostra na janela *Scanner Activity*, uma mensagem indicando o final da operação em que aparece o título da operação que se trata de um detalhamento completo de segurança por máquina e oscilação, o tempo em que se iniciou o esquadrinhamento e o tempo levado para a execução do detalhamento ou pesquisa:

```

.....
COMPLETED SECURITY SCAN FOR MACHINE/RANGE23: XYZ.XYZ.X.Z.
Scan Start Time24: 04:07:23
Scan Duration25: 3 minutes, 25 seconds
.....

```

Figura nº 12: Detalhamento da varredura feita pela ferramenta mostrando seu tempo de início e seu tempo de duração.

Fonte: GFI Software Ltda (2007)

Dando seqüência a uma nova tentativa de varredura utilizando-se do *LanGuard* foi possível constatar que não houve o cuidado por parte do administrador de redes em observar e comprovar se o servidor da empresa estava com *firmware*²⁶, sistema operacional e programas sempre atualizados. Foi possível observar que, a janela *Scanned Computers* mostra uma lista com várias categorias de possíveis (ou reais) falhas encontradas no sistema da empresa, i.e., trinta e seis (36) vulnerabilidades detectadas, dentre elas três (3) em potenciais. De início o LanGuard dá uma informação muito importante, que é o sistema operacional ao qual o micro rastreado está utilizando. A figura onze (11) ilustra e mostra que em *Scan Results*, há vários arquivos desatualizados indicados por letras xis (x) na cor vermelha. Essas letras em destaque indicam o nome, crítica e a data da última atualização feita.

²³ Detalhamento completo de segurança por máquina e oscilação.

²⁴ Tempo de início da varredura.

²⁵ Duração da varredura.

²⁶ Qualquer Software armazenado sob a forma de memória de leitura, ROM, EPROM, EEPROM, e que, portanto, preserva seu conteúdo mesmo quando a eletricidade é desligada, não volátil.

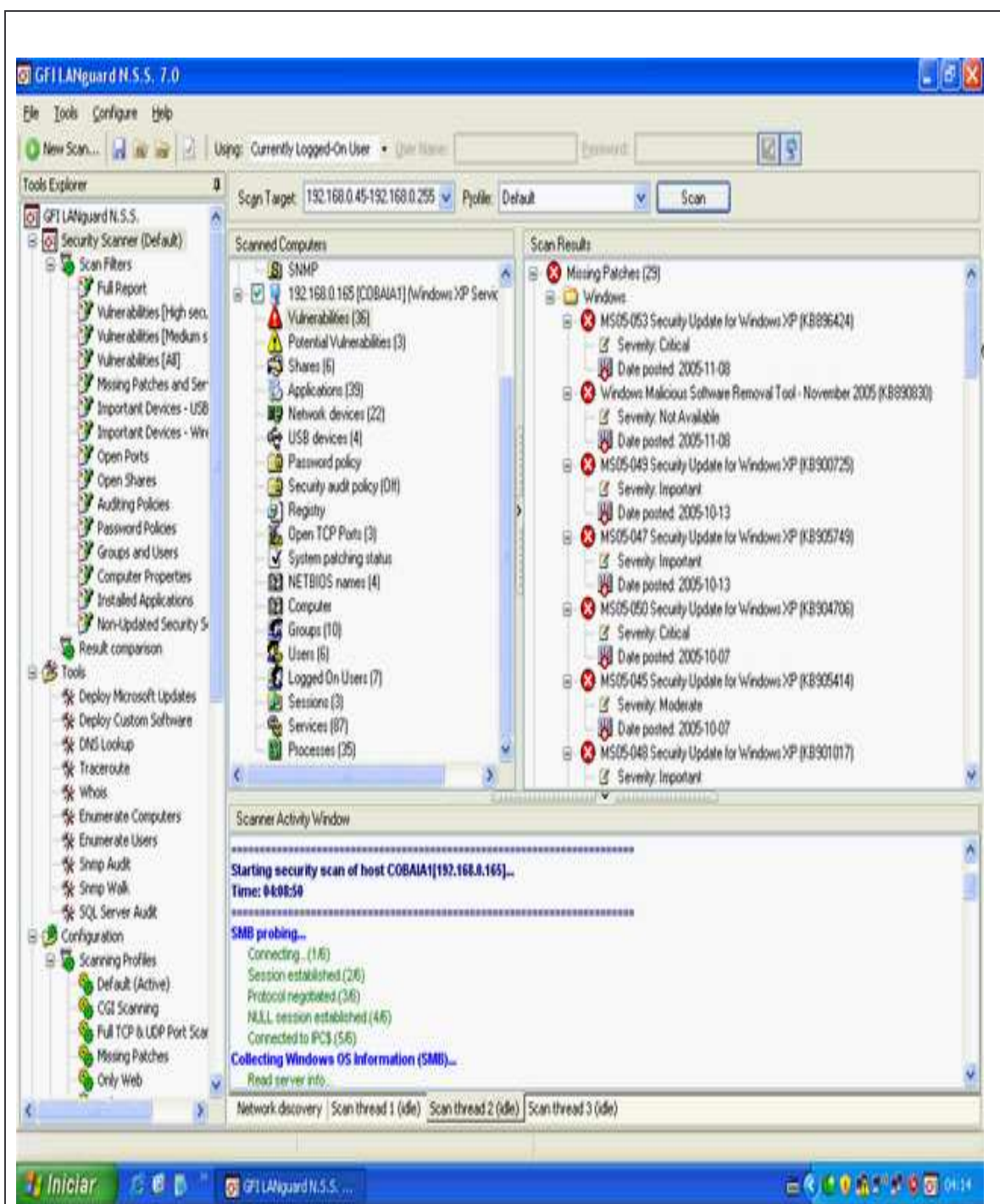


Figura n° 13: Alguns Patches desatualizados.
 Fonte: GFI Software Ltda (2007)

Ao ser clicado em uma dessas categorias, puderam ser examinadas em detalhes as vulnerabilidades provocadas e os *patches* que as corrige. Observaram-se os detalhes de

vinte e nove (29) ausências de *patches*²⁷ apresentadas no lado direito da janela do LanGuard. Isso significa que se tem na máquina afetada vinte e nove (29) arquivos desatualizados. A figura doze (12) ilustra e mostra o número total de patches ausentes no sistema como o primeiro tópico a ser observado:



Figura nº 14: Informação de que 29 patches devem se atualizados.
Fonte: GFI Software Ltda (2007)

Verificada a presença de vinte e nove não atualizações a partir da ferramenta LanGuard, foi proposta para a empresa uma forma de correção dos erros de programas desatualizados que foram apresentados pelas informações obtidas a partir da ferramenta. Nesse sentido, foram importantes para esse procedimento duas situações: o primeiro procedimento foi que os *softwares* que foram atualizados tiveram que possuir a qualidade de ser originais. O outro procedimento a ser tomado foi quanto ao host, no caso a máquina teve que estar conectada a *Internet*. Já conectado, primeiramente o *host* mostrou o nome do arquivo que precisava ser atualizado, em seguida, exibiu o *link* específico para aquele tipo de arquivo. Em seguida ao se clicar neste *link*, basta executá-

²⁷ Missing Patches

lo para que o mesmo venha a ser atualizado automaticamente²⁸. Com a apresentação da figura doze (12) se pode observar que há *link* para o *exploits* que são programas criados para explorarem falhas de segurança. Cada exploit corresponde a uma falha específica, e geralmente vêm em código-fonte (C-F), *Perl* e alguns poucos em executáveis comuns, ou para a atualização que corrige a falha especificada.

Como forma de corrigir a não atualização do programa pediu-se que fossem seguidos os passos para o *Deploy*(seus objetivos estão ligados a automatização de processo de construção de algo, testes e distribuição). Os passos aparecem ilustrados no quadro oito (08), em que são apresentados os pedidos direcionados para o melhor funcionamento do sistema. Logo após, a figura treze (13) ilustra a documentação para correções de erros em portas TCP e UDP.

Quadro n° 10: Passos para a atualização do sistema.

Fonte: GFI Software Ltda (2007)

Passos para o Deploy

1. Execute uma varredura em sua rede;
2. Selecione o host para aplicar o deploy;
3. Selecione os *patches* para o deploy;
4. Dê um *download*²⁹ nos *patches* e pacotes de serviços;
5. Aplique o *Update*³⁰ nos *deploys*³¹

²⁸ Vale à pena ressaltar que, o LanGuard ao detectar não originalidade do *software* ou do arquivo, o administrador da rede ou o analista de segurança tem que estar ciente de que seu servidor, pode sofrer um ataque a qualquer momento.

²⁹ Baixar ou descarregar.

³⁰ Atualização

³¹ Desdobramentos

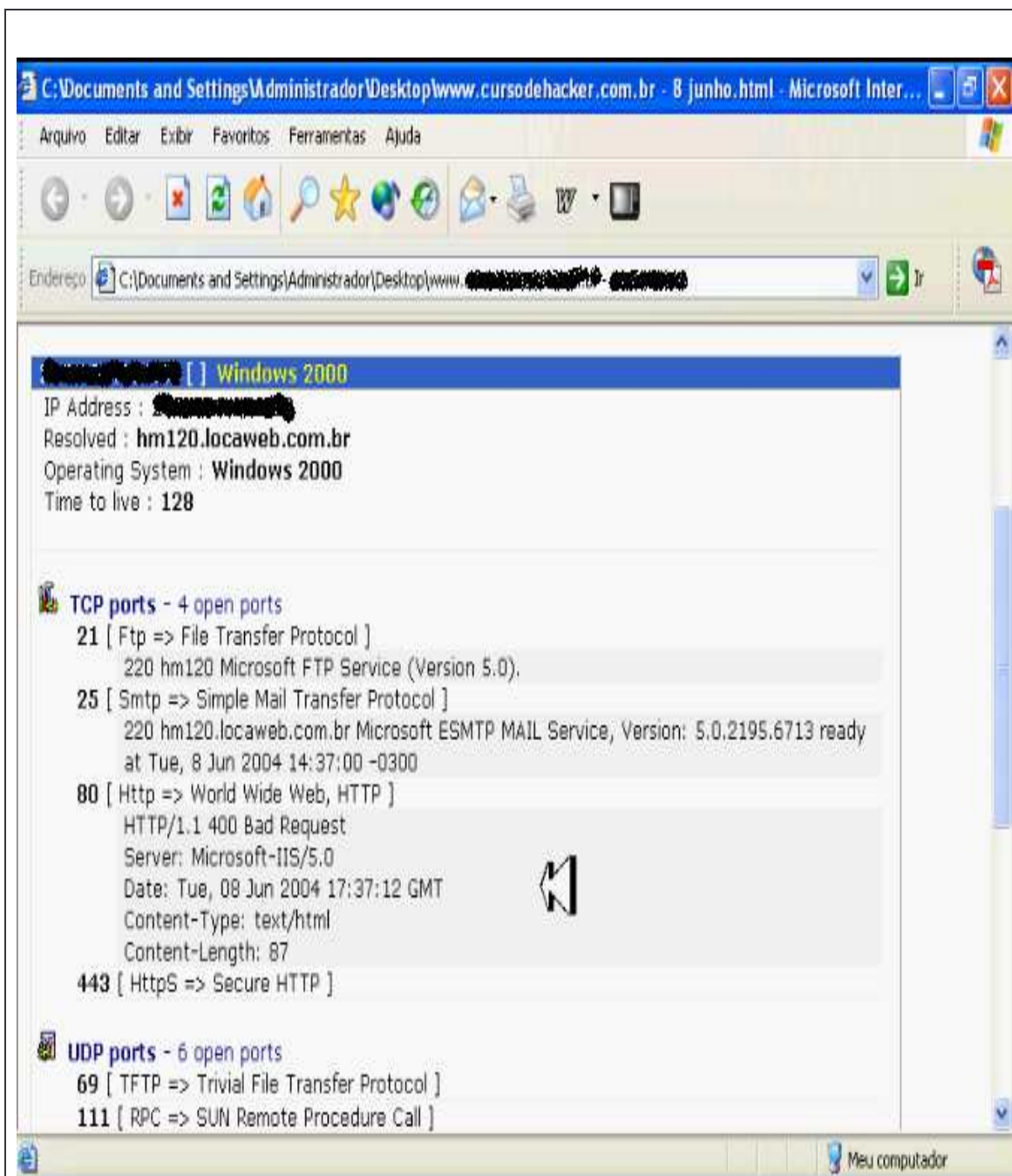


Figura nº15: Documentação para correções de erros em portas.
Fonte: GFI Software Ltda (2007)

Vista a figura que ilustra a documentação para correções de erros em porta de entrada e saída, o próximo passo foi aplicar uma nova varredura feita pelo LanGuard, nas portas TCP e UDP, e tipos de serviços ativos. Com isso, tentou-se verificar o que ocorreria ao sistema caso um invasor explorasse cada um desses serviços. Verificou-se também se o invasor ganharia acesso à máquina por completo, desde que as precauções estivessem sido tomadas antes da tentativa de invasão. O objetivo dessa experiência foi testar uma forma de como fazer para que o invasor não tivesse sucesso em sua investida neste caso. Durante o experimento cogitou-se que primeiramente o responsável pela segurança digital teria que fechar todas as portas desnecessárias às aplicações e serviços que não são oferecidos pelo servidor. Levou-se em consideração que em todo sistema operacional Windows, as portas 135 (serviço RPC), 139 (Serviço da sessão NetBIOS) e 445 (serviço SMB) estão sempre abertas. Caso o LanGuard mostrasse alguma porta com a cor avermelhada, significaria que se tratava de uma entrada fortemente passível a ataques do tipo *trojans*. A figura catorze (14) ilustra as portas ativas e passivas no sistema em operação ao final do detalhamento sem a saliência vermelha.

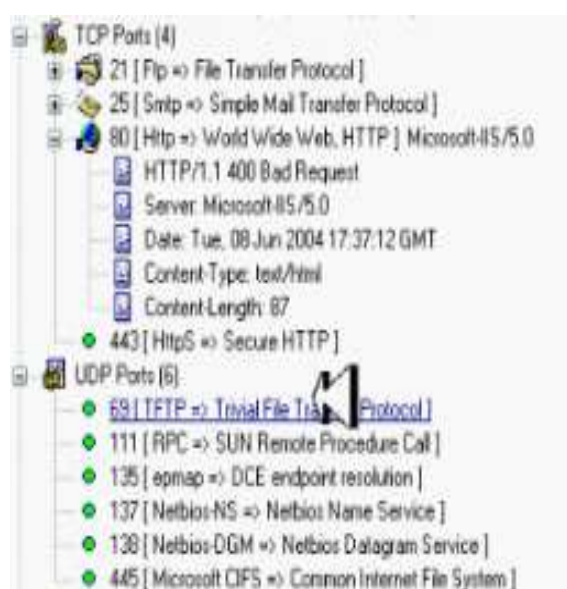


Figura nº 16: Portas Ativas e passivas a invasão.
Fonte: GFI Software Ltda (2007)

Em se encontrado que as portas desnecessárias para o sistema estavam abertas, todo o sistema e a rede estão passíveis de serem invadidas a qualquer momento. Esta foi outra falha encontrada: a não atualização do sistema usado. Como solução para o

problema foi proposto como forma de evitar esse tipo de vulnerabilidade as seguintes ações: Atualização dos arquivos (*patches*) de configurações do sistema operacional, atualização das políticas de segurança dos firewalls, auditoria em cada *log* de usuário para saber se aquele usuário realmente pertence àquela rede, e caso pertença, observar o seu nível de acesso quanto aos serviços oferecidos como forma de prevenir ataques, inclusive problemas de compartilhamento de diretórios. Os compartilhamentos de diretórios (*shares*) são os principais responsáveis por invasões e disseminação de vírus. Há vírus que se aproveitam dos compartilhamentos nos computadores das empresas e se espalham via rede, criando cópias suas em todos os *shares* que possam alcançar. Em compartilhamentos abertos também são bem vistas a implantação por “hackers” de coisas estranhas nos computadores, como cavalo de tróia, programas ou arquivos não autorizados. A figura quinze (15) ilustra pastas compartilhadas vistas durante a varredura.

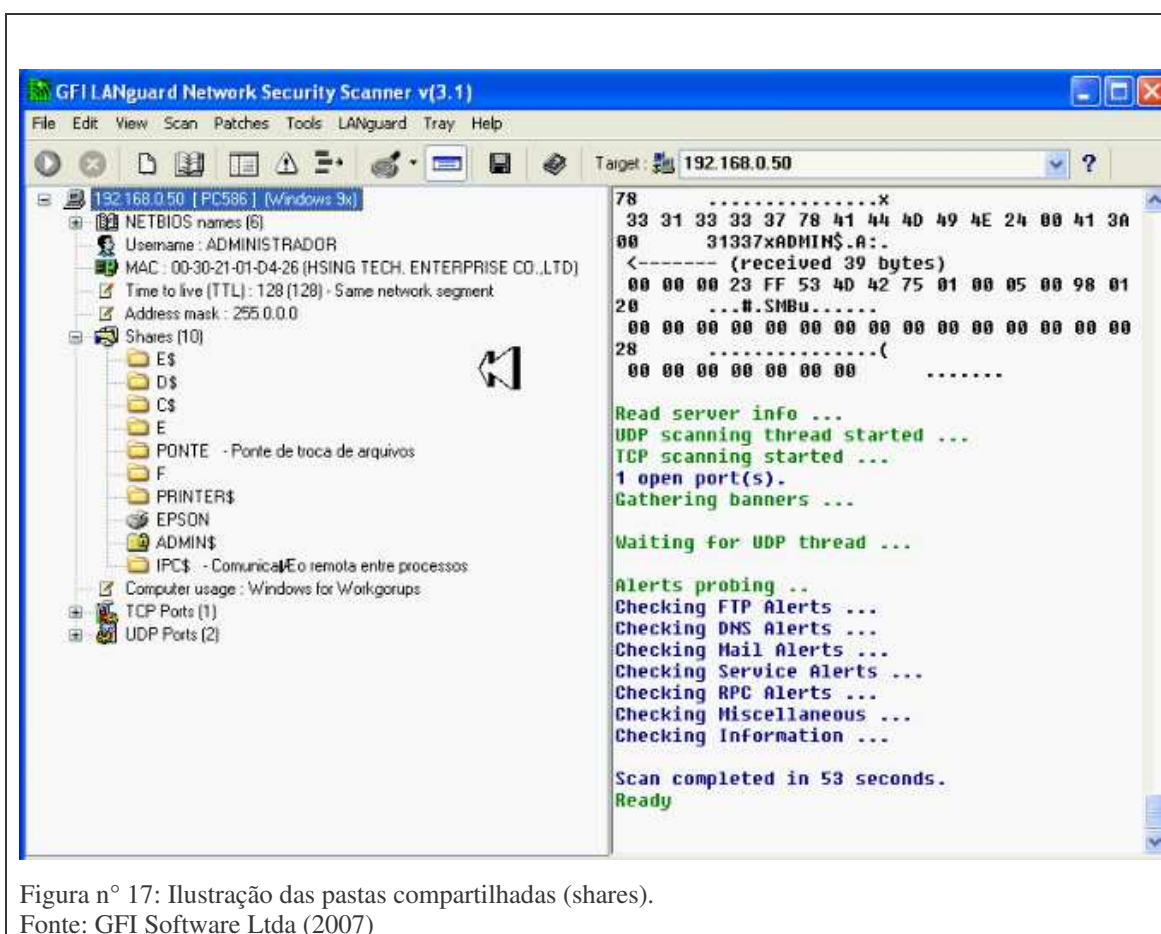


Figura nº 17: Ilustração das pastas compartilhadas (shares).

Fonte: GFI Software Ltda (2007)

4.7 Resultados da pesquisa e discussão das falhas encontradas

Como resultado da pesquisa observou-se que havia falhas no sistema do ambiente computacional em que se aplicou a varredura. As falhas encontradas foram enumeradas perfazendo um total de sete não sendo considerada a ordem em que estas apareceram. São elas: Antivírus desatualizados, softwares piratas (msoffice & sistemas operacionais windows), senhas fracas, ausência de conhecimento em segurança em TI, serviços desnecessários em execução, pastas compartilhadas sem senhas e falta de IDS (Sistema de Detecção de Intrusos). Para o combate a estas falhas, foram propostas soluções para esse problema específico dessa empresa. Listou-se, assim, um total de onze (11) possíveis ações que apontam para as soluções das falhas encontradas no sistema pesquisado. As ações foram distribuídas levando em conta a ordem em que aparecem as falhas. São elas: Implantação de softwares originais, antivírus atualizados, treinamento em segurança digital com funcionários, senhas em pastas compartilhadas, instalação de *ids* (sistema de detecção de intrusos), contratação de profissionais qualificados para dedicação exclusiva a segurança digital, plano de contingência contra riscos, modificação de senhas padrão de roteadores, *switchs*, instalação de *honeypot*, desabilitar alguns serviços do sistema operacional *windows* server., fazer auditoria constantemente os registros de logs. A seguir o quadro nove (09) ilustra as falhas encontradas e as possíveis soluções:

Quadro nº 11: Falhas encontradas e possíveis soluções apresentadas.

Fonte: Resultado da pesquisa. Elaboração do autor.

<i>Falhas encontradas</i>	<i>Possíveis soluções</i>
○ <i>Antivírus desatualizados.</i>	○ Antivírus atualizados.
○ <i>Softwares piratas (MSOffice & Sistemas Operacionais Windows).</i>	○ Instalação de HoneyPot.
○ <i>Senhas fracas.</i>	○ Implantação de softwares originais.
○ <i>Ausência de conhecimento em segurança em TI.</i>	○ Desabilitar alguns serviços do Sistema Operacional Windows Server.
○ <i>Serviços desnecessários em execução.</i>	○ Modificação de senhas padrão de Roteadores, Switchs.
○ <i>Pastas compartilhadas sem senhas.</i>	○ Senhas em pastas compartilhadas.
○ <i>Falta de IDS (Sistema de Detecção de Intrusos).</i>	○ Treinamento em segurança digital com funcionários.
	○ Plano de contingência contra riscos.
	○ Instalação de IDS (Sistema de Detecção de Intrusos).
	○ Contratação de profissionais qualificados para dedicação exclusiva a segurança digital.
	○ Fazer auditoria constantemente nos registros de logs.

Com a apresentação do resultado à empresa real, esta por iniciativa e intermédio da sua diretoria buscou melhorar seus aspectos quanto à segurança da informação. Para tanto, foi requisitado uma palestra em que vários assuntos seriam abordados, como: conhecer os possíveis inimigos, considere os fatores humanos, conheça seus pontos fracos, a tática da engenharia social e como cuidar do patrimônio da empresa em relação aos seus dados. Nesta oportunidade foi apresentado um documentário sobre segurança da informação em empresas americanas, e o quanto que eles investem nesse tipo de consultoria. Após a explanação sobre os aspectos quanto à segurança, os colaboradores chegaram à conclusão de que estavam completamente vulneráveis a todo e qualquer tipo de ataque. No entanto o que mais surpreendeu, foi que o pessoal de TI, tinha certo conhecimento do que seria segurança da informação, entretanto, chegaram a uma triste realidade: todos estavam fazendo a coisa errada, ou seja, tinha a certeza de que um

firewall instalado o sistema estaria imune a esse tipo de ataque. Quanto à parte negativa, foi constatado inúmeras irregularidades no que tange a segurança dos dados da empresa. A parte positiva de tudo que foi realizado, é que agora a empresa já sabe como proteger seu bem maior que são suas informações.

Durante o minicurso foi possível destacar que a inobservância do preceito de segurança digital aparentemente corriqueiro pode custar milhões em prejuízos a partir da perda ou vazamento de dados, indisponibilidade de serviços e mesmo risco de vida (ou do emprego do responsável pela segurança). No caso de sistemas operacionais modernos como Windows ou *Debian GNU/Linux*, não há pretextos para que o responsável pela segurança digital da empresa não faça a atualização correta e freqüente de todos os computadores sob sua responsabilidade. Afinal de contas, o *Windows Update* não é tão difícil de usar. É aqui que se encontra a utilidade de um recurso do *LanGuard* chamada de *Missing Patches*. Trata-se de um tipo de *scan* que permite procurar por computadores ainda não atualizados na sua rede interna. O programa procura, nas máquinas sob teste, indícios de (falta de) atualização, bem como pontos vulneráveis provocados pela não aplicação do procedimento. Isso é um grande desafio para qualquer analista de segurança da informação, caso contrário, seu sistema operacional fica muito desguarnecido ao ataque de um invasor.

Conclusão

Neste trabalho foi possível apreciar, descrever, verificar e gerar relatório sobre a segurança digital e vulnerabilidade de uma rede entre computadores dentro de uma empresa a partir do ponto de vista da segurança da informação. As duas formas aqui aplicadas, como; teste de invasão e a tática da engenharia social, mostram que cada vez mais estamos vulneráveis tecnologicamente. Foi também possível verificar que a segurança da informação, que engloba a segurança de redes e de sistemas, é abrangente e que envolve aspectos não só tecnológicos, mais também humanos, processuais, legislativos, além é claro dos aspectos de negócios.

Após o término da varredura e do estudo feito, identificou-se um número de sete falhas presentes que foram detectadas pelo LanGuard no sistema da empresa confirmando a hipótese de que as ameaças e riscos intencionais e não-intencionais poderiam representar prejuízos financeiro em alta escala. Com isso, gostaríamos de lembrar que segurança da informação é um processo contínuo. As empresas não podem se acomodar com investimentos esporádicos sem um plano estruturado e viver sempre a mercê de futuros ataques a sua rede.

Ainda nesse contexto, deve-se ressaltar que preliminarmente à própria validação dos dados coletados para análise, a ferramenta LanGuard se apresentou como instrumento auxiliar na percepção e entendimento do tráfego de uma rede de computadores já que, também, pode ser usada como um sniffer e até mesmo como um capturador de dados, de tráfego, para posterior submissão aos futuros patches.

Referências Bibliográficas

1. BANCO DO BRASIL. Disponível em <<http://www.bb.com.br>>, Consultado em 19/11/2006.
2. Bravotecnologia. Disponível em
<<http://www.bravotecnologia.com.br/landesK/index.htm>> Consultado em 19/11/2006.
3. BREDARIOL, A., Aspectos de segurança em redes de computadores: IPSecurity e email Monografia – Universidade São Francisco – Itatiba, Novembro 2001, p.6
4. CARVALHO, D.B. **Segurança de Dados com Criptografia Métodos e Algoritmos**. 2ª ed. Rio de Janeiro: EBook Express, 2001. 194 p.
5. CARTILHA DE SEGURANÇA PARA A INTERNET. Disponível em
<<http://cartilha.cert.br>> Consultado em 20/11/2006.
6. CURSO DE TECNOLOGIA ANTI-HACKER. Disponível em
<<http://www.invasao.com.br>> CD-Room 2006
7. DSNIFF. Disponível em <<http://navaghty.monkey.org/~dugsong/dsniff/>> Consultado em 25/01/2007.
8. DIOGO, D.K.; G.P.L., Paradigmas de segurança em sistemas operacionais, UECG, Laboratório de Administração e Segurança de Sistemas, 2004.
9. ETHEREAL. Disponível em <<http://www.ethereal.org>> Consultado em 28/11/2006.
10. EDUARDO, E.A., A Vulnerabilidade Humana na Segurança da Informação, Monografia – Faculdade de Ciências Aplicadas de Minas, Uberlândia – MG, 2005.
11. GARFINKEL, S.; SPAFFORD, G. (1996). **Practical Unix & Internet Security**. O'Reilly & Associates, Inc., USA, 2nd edition. p.971
12. GARFINKEL, S. and Spafford, G. (1999). **Web Security & Commerce**. O'Reilly & Associates, Inc., USA, 1nd edition. 255 p.
13. HORTON, M & MUGGE, C. **Hack notes: Segurança de redes, referência rápida**. Rio de Janeiro: Campus, 2003. 250 p.
14. KLEIN, A. ; ORRIN, S. **Um novo tipo de ataque http splitting**. In Revista Digerati, Ano III, nº 17. 2006-11-30

15. KUROSE, J.F. ; ROSS, K.W. **Redes de computadores e a Internet, uma abordagem top-down**. 3.ed. São Paulo: Pearson, 2006. 634 p.
16. LANGUARD. Disponível em <<http://www.gfi.com/languard>> Consultado em 28/11/2006.
17. FREIRE, A., Machado. **Como Blindar seu PC: aprenda a transformar seu computador**. Rio de Janeiro: Campus, 2006. 181 p.
18. MICROSOFT. disponível em
<<http://www.microsoft.com/brasil/security/guidance/riscos/srsgc03.map#top,>>
Consultado em 18/11/2006.
19. MITNICK, K.D. ; SIMON, W. L. **A arte de invadir**. São Paulo: Person Prentice Hall, 2005. 236 p.
20. NMAP. Disponível em <<http://www.insecure.org/nmap/>> Consultado em 25/01/2006.
21. NESSUS. Disponível em <<http://www.nessus.org>> Consultado em 11/12/2006.
22. NETCAT. Disponível em
<http://www.atstake.com/research/tools/network_utilities/nc110.txt> Consultado em 10/01/2007
23. ONTREUS, DARK_FOX ; LORD_V1RU5, **Dossiê V1RU5**, São Paulo : Digeraty, p.43-131.
24. RNP. Disponível em <<http://www.rnp.br/newsgem/9907ipsec3.html>>, Consultado em 21/11/2006.
25. RNP. **Curso de Segurança em Redes e Sistemas** , UFC / NPD – janeiro 2007.
26. SHEMA, m. **Hack notes: Segurança na Web: referência rápida**. Rio de Janeiro: Campus, 2003. 182 p.
27. STALLINGS, w. **Network Security Essentials: applications and standards**. EUA: Makron Books, 2003. 436 p.
28. SYMANTEC. Disponível em
<<http://www.symantec.com/region/br/avcenter/reference/Securitypor.rtf>>
Consultado em 24/11/2006.
29. SERVIDOR APACHE, Disponível em
<<http://www.infowester.com/servapach.php>> Consultado em 28/11/2006
30. TANENBAUN, A. S. **Redes de computadores: soluções dos problemas**. São Paulo: Editora Campus, 2005, 1120 p.
31. TEXTOS CIENTÍFICOS. Disponível em

<<http://www.textoscientificos.com/imagenses/criptografia/chave-privada.gif>>

Consultado em 20/11/2006.

- 32.ULBRICH, H.C. **Universidade Hackers livros Exercícios**. São Paulo: Digerati Books, 2005. 381 p.
- 33.VEIGA, R. G. A. **IIS V.5**. São Paulo: Novatec, 2001. 96p.