
**UNIVERSIDADE ESTADUAL DA PARAÍBA**
**CENTRO DE CIÊNCIAS E TECNOLOGIA**
**DEPARTAMENTO DE COMPUTAÇÂO**
**CURSO DE LICENCIATURA EM COMPUTAÇÂO**

**TIAGO JOSÉ BANDEIRA LOURENÇO**

# VULNERABILIDADES EM REDES WINDOWS

**CAMPINA GRANDE**

**2013**

**TIAGO JOSÉ BANDEIRA LOURENÇO**

# VULNERABILIDADES EM REDES WINDOWS

Trabalho Acadêmico Orientado (TAO) apresentado ao Departamento de Computação da Universidade Estadual da Paraíba (UEPB), em cumprimento às exigências para obtenção do diploma de graduação em Licenciatura da Computação.

**ORIENTADOR**:

**Profº. Vladimir Costa de Alencar**
**Profº. Cleisson Christian Lima da Costa Ramos**

**CAMPINA GRANDE – PB**

**2013**

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL-UEPB

L892v Lourenço, Tiago José Bandeira.
Vulnerabilidades em Redes Windows [manuscrito] / Tiago José Bandeira Lourenço. – 2013.

**46 f. : il. color.**

Digitado

**Trabalho de Conclusão de Curso (Graduação em Computação) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2013.**

**"Orientador: Prof. Dr. Vladimir Costa de Alencar, Departamento de Computação".**

1. Segurança da Informação. 2. Hacker. 3. Sistemas operacionais. I. Título.

21. ed. CDD 005.8

**TIAGO JOSÉ BANDEIRA LOURENÇO**

**VULNERABILIDADES EM REDES WINDOWS**

**Aprovado em** 13 **de** 06 **de** 2013.

**BANCA EXAMINADORA**

Vladimir Costa de Alencar

Profº. Dr. Vladimir Costa De Alencar
Orientador

Profª. Dr. Misael Elias de Morais.

Profº. Dr. José Carlos Mota

## DEDICATÓRIA

Dedico esta monografia à minha família pela fé e confiança demonstrada. Pais, esposa e irmãs.

Aos meus amigos irmãos que sempre compartilharam de suas experiências e sempre me apoiaram em todas as conquistas da minha vida.

Aos professores pelo simples fato de estarem dispostos a ensinar.

Aos orientadores que participaram no decorrer deste trabalho.

Enfim, a todos que de alguma forma tornaram este caminho mais fácil de ser percorrido.

À minha mãe. DEDICO. Maria de Fátima Bandeira Lourenço.

## AGRADECIMENTO

A Deus pela oportunidade de estar realizando este trabalho, por ter me acompanhado a cada dia durante todo o período deste curso, pois sem Ele não sou nada.

A minha família, pelo incentivo e colaboração, principalmente nos momentos de dificuldade.

Ao meu pai heroi pelo incentivo durante toda minha vida e no decorrer deste trabalho.

A minha mãe guerreira pelo apoio de todas as horas, por ter estado sempre presente neste projeto.

A minha esposa pelo companheirismo por ter estado sempre ao meu lado.

Aos meus amigos de sala pela amizade e auxílio nos trabalhos e principalmente por estarem comigo nesta caminhada tornando-a mais fácil e agradável.

**RESUMO**

Esta pesquisa apresenta um estudo de caso sobre a segurança da informação que vem ganhando destaque em todo mundo e principalmente em empresas e instituições que vêm investindo em tecnologias e treinamentos de seus colaboradores com intuito de prevenção de seus dados. Pois, o número de vulnerabilidade representa o aumento de ameaça ao sistema. Entretanto, muitos deles ainda não compreenderam o uso e a elaboração eficaz dessa segurança e, até mesmo sem saber, muitos têm seus sistemas invadidos. O leitor poderá compreender também a utilização de programas para prevenção e de procura de falhas em sua rede, no qual abrangerá as vulnerabilidades atuais e formas de prevenção. Estarão presentes neste trabalho: Os motivos dos *hackers* realizarem as invasões para usufruir ou danificar os arquivos do alvo desejado; diferenciar vulnerabilidades de ameaças; modos de ataques e compreensão da importância dos pilares da segurança da informação (confidencialidade, integridade e disponibilidade). No estudo de caso, foi simulada uma rede local de uma instituição - dois cenários: um interno e outro fora da rede local - e analisada suas principais falhas e resolução das mesmas.

**Palavras-chaves:** Segurança da informação – Hacker – software – Proteção - vulnerabilidades

**ABSTRACT**

This research presents a case study on information security that has been gaining attention around the world and especially in companies and institutions that have been investing in technology and training of your employees in order to prevent your data. Therefore, the number of vulnerability representes increasing threat to the system. However, many still do not understand the use and the effective development of this security and, and, even unknowingly, many have their systems hacked. This research presents a case study on information security that has been getting attention around the world and especially in companies and institutions that have been investing in technology and training of yours employees in purpose of to prevent your data. The reader can also understand the use of programs for prevention and search of "flaws" in your network, which will cover the current vulnerabilities and prevention methods. Will be present in this work: The motives of the hackers carry out the raids to enjoy or damage the desired target files; differentiate vulnerabilities of threats; Modes attacks and understanding of the importance of the pillars of information security (confidentiality, integrity and availability). In the case study, we simulated a local network of an institution - two scenarios: one inside and one outside the local network - and analyzed their main faults and the resolutions of them.

**Keywords: Information Security - Hacker - Software - Protection - vulnerabilities**

# LISTA DE FIGURAS

# LISTA DE TABELA

**SUMÁRIO**

## INTRODUÇÃO

Há muito tempo vem se abordando o poder do hackerismo, onde se revela o fascínio, o risco e o prazer desses que os praticam. Os hackers, muitas vezes, são interpretados de forma maléfica e deturpada. No entanto, nem sempre fazem o mal. Esses podem usar dessa prática para combater desfalques em grandes corporações, mas também, podem usar da mesma prática para roubar dinheiro ou informações sigilosas, caracterizando então a atuação ilícita. Contudo, ainda temos a terceira opção que coloca o hacker como um pesquisador, buscando aprimorar os conhecimentos através da vulnerabilidade e do estudo de sistemas alheios. (VALLE, 2011)

Diante dos riscos mencionados, surgiu a necessidade de implementação de medidas de segurança da informação por parte das empresas, que não por acaso vem crescendo no intuito de arruinar a prática ilegal de hackerismo no mundo inteiro, onde o valor da informação se tornou mais expressivo para as empresas, que muitas vezes têm seu negócio e seu diferencial competitivo baseado unicamente em informações (JACQUES, 2003).

Neste tocante Sêmola (2003) considera estratégica a segurança que lidera as preocupações de grandes empresas em todo o mundo. Ou seja, estes processos de revisão e de avaliação de soluções dentro da segurança devem restringir cada vez mais as informações corporativas sem causar impacto na produtividade.

Assim, no mercado empresarial é relevante enfatizar a segurança e a vulnerabilidade dos sistemas ao se imaginar a possibilidade de ter suas informações expostas à atacantes da Internet, que tem seus números cada vez maiores e mais sofisticados para violar a privacidade e a segurança das informações. Desta forma as preocupações na proteção da informação tem se tornado um dos interesses primários dos administradores de sistemas, diminuindo sua vulnerabilidade, que é o interesse maior (LUIS MATOS, 2009).

Diante disso, Giordani (2005) postula que:

> *"[...] a segurança da Informação consiste na certeza de que as informações de uso restrito não devem ser acessadas, copiadas ou si quer lidas por pessoas não autorizadas, onde deve-se existir meios de evitar a sua vulnerabilidade."* (GIORDANI, 2005. p. 09)

WADLOW (2000) aponta que toda empresa de grande ou pequeno porte deve focar a Segurança da Informação que tem se tornado não só necessária, mas também obrigatória, pois

as vulnerabilidades existem, os ataques também existem e são crescentes a cada dia, tanto em quantidade quanto em qualidade tendo seus planejamentos e sua metodologia bem aplicados.

No que se refere a sistema seguro, os pilares devem seguir os seguintes parâmetros: Integridade, autenticação, logo após o não repúdio ou irrevogabilidade e por fim a disponibilidade, fazendo desse sistema mais seguro, porém não vulnerável (FONSECA, 2006).

Schneier (2001) ainda acrescenta que além dos pilares mencionados no parágrafo acima também deve ser respeitados os seguintes: Tecnologia, processos e pessoas, que postula que o maior perigo para uma empresa, em se falando de segurança, é o não conhecimento da vulnerabilidade. Pensando assim a vulnerabilidade é pior do que ameaças e ataques, pois como combatê-la se não a conhece? E desta forma cita:

> *"É perigoso ter a impressão de que não existem vulnerabilidades quando, na realidade, as brechas estão por todo lado e disponíveis aos fraudadores interessados. Por isso, a segurança precisa envolver Tecnologias, Processos e Pessoas num trabalho que deve ser cíclico, contínuo e persistente, com a consciência de que os resultados estarão consolidados em médio prazo*." (SCHNEIER, 2001, p. 47)

Com base na Segurança de Informações, essa revisão bibliográfica tem o objetivo de levar o conhecimento inerente à vulnerabilidade desta mesma segurança de informações ao mundo acadêmico, com o objetivo de verificar a Integridade, a autenticação, o não repúdio ou irrevogabilidade e por fim a disponibilidade desses sistemas de segurança. Este trabalho abordará vulnerabilidade de sistemas de informações ligada a área da computação já que a segurança é um tema muito amplo e poderia--se pecar devido a abordagem bibliográfica.

# 1. FUNDAMENTAÇÃO TEÓRICA

Os chamados hackers nem sempre são criminosos. Alguns iniciam a prática por acidentes, porém também existem aqueles que estudam apenas para invadir informações sigilosas alheias para através dessas informações, ou seja, diante da vulnerabilidade da Segurança da Informação, que é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade, faturar e expor a terceiros estes dados, e desta forma causar danos aos seus proprietários (BEAL, 2005).

Ao longo deste capítulo discutiremos estas afirmações.

## 1.1. O IMPÉRIO DOS HACKERS NO BRASIL

Por todo o mundo podemos observar a velocidade em que as mais diversas informações alcançam. Na era em que vivemos, os sons, as imagens e os textos são interativos. Pessoas conversam em tempo real mesmo estando a distâncias quilométricas, desenvolvendo comércio, pesquisas e até a saúde (MCLURE E SCAMBRAY, 2000).

Experiências magníficas e inovadoras têm sido compartilhadas por pesquisadores, administradores, médicos e outros. Juntamente com as novidades, vieram as indesejáveis consequências e práticas errôneas dos invasores de sistemas ou como mais conhecidos os "hackers", promovendo na maioria das vezes pirataria, delinquência e crimes. (STANTON, 2000)

No Brasil, onde as leis para prevenir os crimes digitais são ineficazes, torna-se o paraíso de hackers e de ataques na/pela internet. Portanto, este mesmo país cria laboratórios para este tipo de crime, de maneira que roubos, fraudes, pirataria e vandalismo online se tornam cada vez mais frequente. (BELHASSOF, 2009)

De acordo com Mi2g Intelligence Unit (empresa de Londres), o Brasil tem sido a maior base para os hackers da internet. Estes invasores atuam como sindicalistas de algumas organizações denominadas de "Quebrando seu sistema", "Inferno virtual" e "Observando sua administração" entre outros, diz a mesma fonte citada no parágrafo anterior.

Neste sentido, a segurança digital existe em um mundo obscuro entre seus profissionais, mostrando a necessidade (ou não) de ter conhecimentos sobre como os invasores entram no sistema. (LANDIM, 2011)

Assunção (2010) acrescenta que é preciso saber que "apesar de uma segurança digital estar em constante e rápida evolução, suas bases não mudam apenas se sofisticam". Ulbrich e Valle (2010) citam alguns conhecimentos hackerianos:

> "*Qualquer informação, por mínima que seja, é uma jóia rara. Cada novo sistema, linguagem de programação ou mecanismo de criptografia é um desafio a ser superado. Dependendo de suas ideias sociais e politicas, pode decidir inclusive que os conhecimentos encerrados em uma rede ou sistema autônomo devem ser abertos ao grande público, mesmo que seu sigilo esteja resguardado por leis- rebeldia e repúdio a leis imorais ou injustas são quase obrigatórias nesse meio*". (ULBRICH E VALLE, 2010, p. 16)

Estes hackers sempre estarão atentos a tudo e a todos que puderem alcançar, para buscar mais e melhores conhecimentos no intuito de invadir de segurança digital. (LANDIM, 2011)

Assim, a Bitolação é característica comum a todos os hackers. Eles são vidrados em computadores, programações, conectividade e tecnologia da informação. Os hackers chegam ao ponto de relaxar na aparência, deixam de se alimentar, de se higienizar e até de descansar e dormir por alguns dias para alcançar seu objetivo maior, seja ele produzir um programa importante ou até de invasão a sites famosos (ULBRICH E VALLE, 2010). Por isso, compartilhamento diz respeito aos usuários estarem trabalhando em terminais que possam interferir ou interagir intencionalmente nos programas de outros usuários.

Aqui para melhor entendimento citaremos Assunção (2010) quando este se refere a alguns termos utilizados no meio underground:

**Hacker**: termo original, utilizado desde a década de 1970 e servia para designar "fuçadores". No entanto, com o passar do tempo, foi utilizado pela mídia para nomear invasores de sistemas.

**Hacker White-Hat:** o "hacker do bem" também conhecido como "hacker chapéu branco". São pessoas que têm um vasto conhecimento, mas não usa-o de forma ilegal.

**Hacker Black-Hat:** o "hacker do mal' ou "chapéu negro", utiliza seus conhecimentos para roubar senhas, documentos e espionar indústrias.

**Cracker**: o mesmo que "hacker black-hat'.

**Engenheiro social**: este se utiliza de meios não-técnicos para obter informações privilegiadas.

**Scammer**: fraudador. Se utiliza de falhas de programas comuns, como o Internet Explorer.

**Script Kiddie**: invasor que não tem conhecimento profundo nem alvos definidos.

**Defacer**: um Script Kiddie. Preocupa-se em substituir a página principal de algum website.

**Lamer**: tem pouco conhecimento, se faz passar por um "guru da tecnologia".

Ainda segundo Assunção (2010) existem alguns termos irrelevantes como wannabes, gurus, backers, phreakers, etc.

No tocante aos ataques ou mesmo aos termos utilizados acima, pode-se afirmar que só será invadido aquele que tem seus recursos mal configurados. A maior falha surge com utilização de senha de acesso muito fácil. Mas não esqueçamos que todo software tem falha, desde a calculadora, passando pelo leitor de arquivos PDF, entre outros, o que os torna vulneráveis aos ataques e as empresas se tornam frágeis à invasões devido a falta de uma criptografia, ao um redirecionamento de tráfego, a um spoofing. Além disso, as proteções são ineficazes, a falta de atualizações e ao pior risco deles: o fator humano. (SÊMOLA, 2003)

## 1.2. FASES DO TESTE DE INVASÃO

### 1.2.1. Aquisição de informação

A aquisição de informação a fase mais importante do projeto, pois com ela o invasor saberá as falhas do alvo, ferramentas utilizadas, como e quando será executado o teste por completo. No estudo de caso falaremos um pouco sobre essa técnica que pode envolver a engenharia social.

### 1.2.2. Varredura

Após identificar os equipamentos e software que o alvo possui, é necessário a varredura das vulnerabilidades possíveis, relacionando as portas abertas ou programas maliciosos injetado na rede a ser atacada.

### 1.2.3. Ganhar acesso

Encontrado as vulnerabilidades, o invasor tenta o acesso por completo para obtenção do que deseja.

### 1.2.4. Manter acesso

Para o invasor, é cogente que esse acesso seja de forma continua, pois durante a invasão, o objetivo não pode ser completado por falta de energia, antivírus ou outro obstáculo que impeça a invasão, então se faz necessário essa conexão permanente.

### 1.2.5. Apagar rastros

Com todos os objetivos concluídos, o atacante deve limpar seus rastros com intuito de não ser rastreado, através de sites, porta ou programa que ele conseguiu invadir pode ser

rastreado logo depois do ataque, então para não ser identificado, ele realiza todos esses procedimentos.

## 1.3. PRINCIPAIS TIPOS DE INVASÃO

### 1.3.1. Varreduras de Portas (Port Scanners)

Para (RAMOS, 2012), essa varredura se dá com os escanners que buscam portas TCP abertas, no qual serão realizados os ataques. Essas varreduras são realizadas durante dias, semanas ou meses, de maneira aleatória com intuito de não ser identificado pela vitima.

### 1.3.2. Invasão TelNet

Segundo (Vieira, 2010), Telnet é um protocolo que já vem instalado no Windows que dá facilidade ao administrador do PC para acessar a máquina em locais diferentes, pedindo apenas a senha de acesso do administrador. Caso um invasor consiga essa senha, ele tem acesso a todo conteúdo do sistema.

### 1.3.3. Invasão por FTP

Método utilizado para o ataque de páginas da Web com alguns programas específicos, onde invasores procuram por senhas de transferências de dados para o servidor Web via FTP, caso consigam, terá acesso a todo site (Vieira, 2010).

### 1.3.4. Invasão por monitoração ou Sniffer

É utilizado para verificar e roubar pacotes na rede, esses pacotes contém dados de usuários, como senhas e arquivos pessoais (MATOS, 2010).

### 1.3.5. Invasão por Worms

Uns dos meios mais utilizado por invasores, consiste em infectar máquinas que acessam um determinado site que contenhas além de informações, um vírus Worms que contamina o PC da vítima com objetivo de não danificar o computador, mas sim de informar todas as senhas contidas nele (NOGUEIRA, 2008).

### 1.3.6. Invasão na Força Bruta

Consiste de tentativas de acesso a algum programa, onde o invasor oferece informações que podem estar contidas no acesso, no qual será preciso senhas com 8 dígitos. Essas informações podem demorar semanas ou meses com o computador ligado 24 horas por dia para que o software consiga finalizar o processo (BERBET, 2002).

### 1.3.7. Invasão por Spoofing

Nesta técnica, o invasor se passa por um computador da rede para obter acesso a um sistema, muitas vezes ele muda os cabeçalhos dos pacotes da rede para que pareçam vir de outra máquina.

Paulo Henrique Araújo Honório teoriza em seu TCC que existem várias formas de spoofing, citando-as:

> • *" Hardware adress: O endereço do hardware pode ser alterado numa fase posterior permitindo que o spoofing seja realizado no endereço de origem. Este ataque engana o destino quanto à proveniência da informação para que a garantia da segurança seja efetuada ao nível de aplicação. Em determinadas situações, o spoofing não é usado como fundamento para o funcionamento de um equipamento.*
> • *ARP(Adress Resolution Protocol): Permitem realizar uma equivalência entre os endereços de IP e os endereços de hardware. Quando um pacote encontra se num endereço de IP é necessário que ele seja enviado num endereço de hardware destino, podendo ocorrer as seguintes situações: O IP corresponde à rede local e o endereço de hardware de destino passa a ser a interface do destino. Caso contrário, o endereço de hardware de destino passa a ser o da interface do roteador (gateway) da rede local ou sub-rede.*
> • *Rotas IP: São mantidas pelos roteadores. Com base nas informações eles mantêm tabelas que permitem qual interface e para onde deve ser enviado um determinado pacote. O roteador usado para trocas de tabelas é o RIP (Routing Information Protocol). Se um roteador for um participante passivo do RIP, ou seja, recebe somente um broadcast e atualiza as tabelas dinâmicas, basta que qualquer computador as envie através da port 520. Existem algumas formas de evitar este tipo de ataque: Estabelecer, sempre que possível, as rotas estatísticas; Nunca utilizar RIP*

*passivo; Utilizar um daemon de roteamento e quando for possível, configurar os*
*endereços de IP para as origens confiáveis de RIP, se o gateway for um computador." (HONÓRIO,2005)*

### 1.3.8. Invasão por Exploit's

É uma das técnicas mais difíceis, porém uma das mais eficazes, pois com ela o "hacker" pode ter acesso completo da máquina-alvo, porém ele precisa utilizar scaneadores para encontrar os bug's e ter conhecimentos consistentes sobre programação para criar os exploit's específicos para ter acesso (Assunção, 2010)

### 1.3.9. Invasão Dos ou Denial of Service

Geralmente usado explorando uma falha em algum software. O hacker envia pacotes (maliciosos) para o usuário, onde vai recebendo os pacotes normalmente, mas com o número e a insistência dos pacotes, o host da vítima fica sobrecarregado de pacotes, chegando até travar, reinicia ou até mesmo não acontece nada. O motivo disto ocorrer varia, dependendo do tipo de DoS (ASSUNÇÃO, 2002).

### 1.3.10. Invasão por Trojans ou Cavalo de Tróia

Muito utilizados pelos iniciantes, funcionando com um programa camuflado em um arquivo que quando executado, permite que o invasor tenha o controle do PC ou informações via acesso remoto (ASSUNÇÃO, 2002).

### 1.3.11. Scanning de vulnerabilidades

São softwares que verificam toda a rede realizando testes em computadores, buscando por falhas de segurança, arquivos compartilhados( sem senha), protocolos, aplicativos e sistemas desatualizados (RAMOS, 2012).

## 1.4. ENGENHARIA SOCIAL

Segundo Kevin Mitnick, considerado um dos maiores engenheiros sociais e o mais famoso pirata digital, que saiu da prisão e agora ensina às empresas como se defender dos invasores cibernéticos, sobre a engenharia social, ele afirma:

*"É uma técnica usada por hackers para manipular e persuadir os funcionários nas empresas. Em vez de ficar se descabelando para encontrar uma falha no sistema, o hacker pode, por exemplo, largar um disquete no chão do*

> *banheiro com o logotipo da empresa e uma etiqueta bem sugestiva: 'Informações Confidenciais. Histórico Salarial 2003'. É bem provável que quem o encontre, o insira na máquina por curiosidade. O disquete pode ter sido preparado por um hacker para rodar na máquina da vítima e instalar um tipo de programa chamado Cavalo de Tróia, que dá acesso remoto à rede da empresa."*

### 1.5. INSIDERS

Muitas empresas não se preocupam com o treinamento de seus funcionários, principalmente alguém para tomar conta de seus dados. Por isto, os considerados Insiders, são denominados como empregados insatisfeitos, que com saída ou não da empresa, que realizam ataques internos na rede, tornado até mais fácil, uma vez que ela já está conectada na rede, faltando acessar os dados e danificar da empresa (PAULA, 2011).

### 1.6. PHISHING OU VISHING

São programas que utilizam mensagens ou pop-up para captura de senhas de bancos, cartão de crédito, número da segurança social, entre outras. Geralmente as mensagens vêm compostas de informações de "atualizações" ou de "validar" suas informações de conta. O usuário leigo acaba abrindo a mensagem e passando informações sigilosas para os hackers. (PAULA, 2011).

## 2. SEGURANÇA TECNOLÓGICA E SEUS PILARES

(FONSECA, 2006) afirma que a Segurança da Informação só será alcançada se a tríplice (Pessoas, Processos e Tecnologias) for aplicada a estratégia de segurança efetivamente, podendo ocorrer variações dentro de uma mesma empresa, porém, não pode apontar para o zero pois desta forma a estratégia seria falha.

Sêmola (2003) cita a tríplice, onde, a *Pessoa* é educação, é o que realiza treinamento, é como fazer e conscientizar e que é o elo mais frágil, pois a segurança começa e pode terminar nela. Nos *Processos* há flexibilidades, porém são metódicas, onde estão sempre na busca do equilíbrio para a perfeita segurança e funcionamento das informações da empresa. Já na Tecnologia, esta só poderá ser aplicada onde puder suportar a Política de Segurança das informações, pois reforça a pessoa citada acima.

Buscando investimentos, a Security Officer mede e faz funcionar a tríplice Pessoa, Processos e Tecnologia desmistificando e aprimorando aqueles que não estão de olhos vendados para a efetiva segurança tão almejada.

A revista fonte fala que a Segurança da Informação tem o objetivo de proteger, garantir, ser capaz de deslumbrar o inesperado e não deixar surpresas ruins acontecerem. A verdadeira Segurança da Informação armazena as informações de um determinado sistema computacional guardada e a mantém segura para que ninguém tenha acesso às mesmas sem a devida permissão. A empresa espera que suas informações esteja em local seguro para em sua necessidade poder acessá-la, com informações invioláveis.

Assim, o Módulo Security (2001) afirma que dentro dos princípios da segurança tecnológica pode-se destacar:

1. Confidencialidade ou privacidade, ou seja, deve-se proteger as informações de intrusos ou pessoas não autorizadas pelo seu proprietário, inclui-se aqui acesso restrito e criptografia.
2. Integridade, que nada mais é que evitar deletar e/ou alterar informações sem prévia autorização do proprietário.
3. Legalidade, que é a via legal a informação estando em concordância com os preceitos da legislação em vigor.
4. Disponibilidade, que sintetiza-se em garantir o serviço de informática e sua demanda sempre que o usuário necessitar.
5. Consistência, que se garante que o sistema abranja a expectativa do seu usuário.
6. Isolamento ou legítimo uso, sendo este a restrição ao acesso do sistema, ou seja, apenas o usuário autorizado pode ter acesso.
7. Auditoria, definindo-se quando se tem o intuito de identificar erros e ações que por ventura venha a ocorrer por parte de seus usuários autorizados, onde a auditoria ou *logs*, que registram o que, por que e quando foi acometido.
8. Confiabilidade, garantindo que o sistema funcione mesmo em adversidade.

Coltro (2002) cita quando atualizar a Segurança da Informação dentro do âmbito empresarial:

> *"[...] segurança de Informação é a conjugação de uma estratégia e de ferramentas específicas que atendam as necessidades corporativas para a manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança nunca está acabada e deve ser desenvolvida e*

> *atualizada durante toda a vida da empresa."* (COLTRO, 2002, p.26).

Alguns questionamentos devem ser observados para a implementação de um programa de segurança da informação, tais como: o que e contra o que proteger, qual a importância e ameaças possíveis, grau e tempo de objetivos a alcançar, e por fim quais expectativas e consequências para violação do sistema lesado. (BEAL, 2005)

Este mesmo autor define que uma política de Segurança é um conjunto de regras e práticas que regula como uma organização gerência pode proteger e distribuir suas informações. Essa Política da Informação define o que não é permitido na segurança em um certo período de tempo durante a operação de um dado sistema.

Giordani (2005) comenta que quando se detecta a ameaça, sabe-se logo que existiu a vulnerabilidade e consequentemente houve a perda da confidencialidade, integridade e disponibilidade. Podendo ser dividida em :

1. Ameaças naturais - Onde ocorre um fenômeno da natureza;
2. Ameaças involuntárias - Geralmente esta suscetível devido a falta de conhecimento ou mesmo acidentes e erros;
3. Ameaças voluntárias- Assemelha-se à engenharia social, pois é causada por *hacher,*ou seja, por disseminadores de vírus de computador.

Já Luis Matos (2009) postula sobre as vulnerabilidades como frutos de ameaças exploradas causando assim a segurança das informações que podem ser as seguintes:

1. Físicas – Salas de CPD mal planejadas e sem estrutura.
2. Naturais- Tempestades, incêndios, falta de energia no geral, poeira,etc... fazer a vulnerabilidade do sistema.
3. Hardware- Desgaste e má utilização do equipamento.
4. Software- Instalação incorreta, equipamento mal configurado,informação vazada.
5. Mídias- Disquetes, CDs danificados causam danos irreparáveis nas mídias.
6. Comunicação- Acesso não autorizado de pessoas invasoras.
7. Humanas- Falta de treinamento e conscientização e o não seguimento das políticas de segurança.

Ainda pode-se citar as duas vertentes da Política de Segurança. A primeira é a baseada em regras que utiliza-se de rótulos dos recursos e também dos processos que determinam o

tipo de acesso que pode ser efetuado. Já a segunda Política é baseada em segurança com o objetivo é permitir a implementação de um esquema de controle de acesso possibilitando especificar o que cada indivíduo pode fazer, leitura ou modificações nas funções na organização. (SCHNEIER, 2001)

A Segurança da Informação só será definida e completa se as questões anteriores forem alcançadas e dessa forma restringindo as ameaças e riscos possíveis e na busca da finalização administrativa dos sistemas é importante implantar uma gerência de segurança para o melhor funcionamento. (FONSECA, 2006)

## 3. POSSÍVEIS FERRAMENTAS DE SEGURANÇA

Desde tempos remotos, as pessoas comunicam-se das mais variadas formas, com gestos, com palavras e com escritas. Já nos dias atuais, esquece-se de olhar nos olhos. A transmissão das informações não é mais tão segura e pode ser invadida a qualquer momento, ou seja, transmitir é essencial, porém essas mudanças que facilitam a nossa vida diária, podem causar um dano irreparável dependendo do teor da informação como, a informação de uma empresa, que é o seu principal patrimônio. (CONCEITOS, 2002)

No tocante a Segurança da Informação o Código de Prática para a gestão da segurança da informação cita:

> *"A informação é um ativo que, como qualquer outro, importante para os negócios, tem um valor para a organização. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos ao negócio e maximizar o retorno dos investimentos e as oportunidades de negócios".* (NBR ISSO/IEC 17799:2001, pág.2).

Diante da citação referida acima, pode-se de forma ampla e clara definir informação e discernir os termos que antes eram confundidos ou assemelhados. Assim Conceito (2002) refere à diferenciação de dados, informação e conhecimento para melhor entendimento.

DADO: Observações simplificadas a respeito de um estado do mundo, bem estruturado, obtido rapidamente através de máquinas, geralmente quantificado e transferível.

INFORMAÇÂO: Grande relevância na unidade de análise e necessitando desta forma da mediação humana. Pode-se dizer que "Informação" é um conjunto de dados onde os seres humanos projetaram tornando-os úteis.

CONHECIMENTO: apreciação valorosa do ser humano com idealização, síntese e argumentação. Desta forma de difícil estruturação, captura em máquinas e difícil transferência. Sua definição pode ser um conjunto de ferramentas conceituais e categóricas utilizadas para criação, para colecionar, armazenar e compartilhamento de informações. Ao contrário dos dados, apenas a informação e o conhecimento têm condições de interferir ou modificar o comportamento de uma organização.

Davenport e Prusak (2000, p.18) acrescentam que em nossa sociedade contemporânea frequentemente referem-se a uma "economia ou a era da Informação". Simplificando, isso significa que a produção humana sempre estará ligada à informação mais que aos bens físicos.

Desta forma, a quantidade de acessos e a qualidade de seus usuários podem deixar o sistema vulnerável a ataques. Dentre o sistema mais utilizado estar o sistema Microsoft Windows, que é uma popular família de sistemas operacionais criados pela Microsoft, empresa fundada por Bill Gates e Paul Allen. Antes da versão NT, uma interface gráfica para o sistema operacional MS-DOS que é o mais acessado, cerca de noventa por cento das empresas e residências faz uso deste sistema, pois é inegável que seu desenvolvimento abrange desde expert até leigos em informática. A Microsoft Windows possui duas correntes diferentes de desenvolvimento, onde estão conservadas externamente (ULBRICH E VALLE, 2010).

Com Versão Profissional, a Microsoft iniciou o desenvolvimento de um sistema operativo de nome NT (New Tecnology), mantendo assim a interface gráfica de sucesso que por sua vez é compatível com os antecessores binário, lembrando que o seu interior é diferente, pois implementa os conceitos necessários a um sistema operativo seguro. Desta forma encontraremos duas famílias de Windows independentes. A primeira família diz respeito ao uso doméstico e pessoal com Windows 1.0, Windows 2.0, Windows 3.0, Windows 3.1, Windows 3.11, Windows 95, Windows 98 e Windows ME. No que se refere à segunda família temos o uso profissional que abrange Windows NT3.5x,WindowsNT4.0, Windows 2000 e por fim o WindowsXP (SCHNEIER, 2001).

Todo Windows possui característica própria de funcionamento interno. Deste modo Thomas (2000) cita alguns Monousuários x Multiusuários; Núcleos básicos; Modo real, protegido e virtual 8086; Memória virtual; Monotarefa; Multitarefa; Níveis de Privilégio; Componentes; Gerenciamento de Memória; Gerenciador de máquina virtual e também de VMN; Sistema de arquivos; Arquitetura de sistemas de 32 bits; Componentes da arquitetura e Registro.

O sistema operacional é considerado “Monousuário” quando permite que apenas um usuário trabalhe por vez no sistema, como é DOS, Windows 3.x, Windows ME, por exemplo. Assim, o sistema operacional é dito “Multiusuário” quando permite mais de um usuário trabalhando no sistema ao mesmo tempo, como exemplo do Windows NT, Windows 2000 e Windows XP.

Então, suscetibilidade a vulnerabilidade de sistemas faz Mitnick (2003) acrescentar que Vulnerabilidade é uma falha que deixa exposto todo o sistema sob algum aspecto da segurança, sendo desta forma um risco potencial. Sendo assim, as vulnerabilidades são as mais diversas, e dentre elas estão a Vulnerabilidade Humana, a falta de treinamento, o compartilhamento de informações confidenciais, a não execução de rotinas de segurança e a falta de comprometimento por parte dos funcionários.

Em meio às vulnerabilidades e a fim de manter o sistema operacional funcionando de forma mais segura, os processadores modernos possuem dois tipos de proteção denominados Modo Real e Modo Protegido. No Modo Real sua funcionalidade é semelhante a 8086, sendo com velocidade maior, no entanto pode-se alternar quando necessário para o modo protegido, pois a memória RAM pode ser instalada no sistema, além de incorporar recursos como a multitarefa e a memória virtual em disco e quando usamos a interface gráfica do Windows e rodamos seus aplicativos, também trazendo quatro novos recursos como memória virtual, multitarefa, proteção de memória e o modo virtual 8086. (MAIA, 2005)

Operando em Modo Real, o processador pode ser totalmente compatível com qualquer programa antigo o que seria inviável executar um aplicativo de Modo Real dentro do Windows 95 ou qualquer outro que faça uso do modo protegido. Desta forma, teria que fechar o Windows e fazer o processador voltar ao Modo Real. Pensando nisto, os pesquisadores da Intel desenvolveram o Modo Virtual 8086. Seu processador operando em modo protegido simula vários ambientes de Modo Real, cada um com 1MB de memória e total acesso ao hardware da máquina ou máquinas virtuais. (BEAL, 2005)

## 3.1. DIFERENÇA ENTRE AMEAÇAS E VULNERABILIDADES

Para entendermos a discussão sobre ameaças e vulnerabilidades precisamos saber as diferenças entre elas. Ameaças em sistemas podem ser falhas de hardware ou software, ações pessoais, invasão pelo terminal de acesso, roubo de dados, serviços e equipamentos, problemas elétricos, erros de usuários, mudanças nos programas ou problema de

telecomunicação. Podem se originar de fatores técnicos, organizacionais e ambientais, agravados por más decisões administrativas. (Laudone Laudon, 2004)

Também pode acontecer o ataque, que é o ato de tentar desviar dos controles de segurança de um sistema, de forma a quebrar os princípios da segurança. Os possíveis ataques são: Interceptação, interrupção, modificação, e personificação. O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes.

Porque os sistemas podem estar vulneráveis? O nível de complexidade depende do nível de proteção, ou seja, arranjos complexos de hardware, software, pessoas e organizacionais criam novas áreas e oportunidades para invasão e manipulação. As redes sem fio que utilizam tecnologias baseadas em rádio são ainda mais vulneráveis à invasão, porque é fácil fazer a varredura das faixas de radiofrequência. A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque. Todos os ambientes são vulneráveis, partindo do principio de que não existem ambientes totalmente seguros. A vulnerabilidade possibilita incidentes de segurança, afetando os negócios que impactam negativamente os clientes à imagem e o produto.

Neste contexto, a segurança na informática deve ser tomada como uma opção estratégica e não apenas tecnológica ou gerencial. Estando relacionada ao conjunto das medidas que visam dotar as redes de computadores com capacidade de inspeção, detecção, reação e reflexos aos potenciais de ataques, permitindo reduzir e limitar as vulnerabilidades e o impacto das ameaças quando estas se concretizam.

# 4. ESTUDO DE CASO: PROJETO

## 4.1. DESCRIÇÃO DO CENÁRIO

Através deste estudo, será apresentada uma rede, onde três são computadores, um deles servidor que contém um domínio, e as estações. Todas estas são conectadas com esse servidor obtendo algumas configurações do active directore(AD), dando algumas permissões e restrições para que não haja problemas de segurança em uma rede corporativa.

### 4.1.1. Objetivos da pesquisa

O objetivo desta rede é estabelecer uma conexão de uma escola de informática em que os professores tenham poder total sobre os alunos, e o administrador da rede tenha o controle completo de tráfico de dados, de permissões de internet e pastas, bloqueando não só

a estrutura lógica, mas também a estrutura física. Esse projeto é uma simulação de uma instituição técnica que tem cursos como manutenção e redes (Rede com um servidor e dois computadores), que foi desenvolvido com o objetivo de realizar estudos de vulnerabilidades, (brechas) na qual alunos ou pessoas mal intencionadas possam obter.

### 4.1.2. Coleta de dados

Foi realizado testes com um notebook conectado na rede e em um PC conectado na rede estudada para verificar algumas portas que possivelmente estejam abertas para ataques. O sistema operacional e alguns programas, todos eles atualizados e usando sempre versões gratuitas ou originais para evitar problemas, arriscou uma invasão a rede de dentro e fora, mostrando que os pilares de segurança(Confidencialidade, Disponibilidade, Integridade) podem ser quebrados.

Com este estudo foram submetidos a testes os seguintes mecanismos de segurança: controle de acesso, portas abertas, obtenção de IPs, nome da rede, identificação MAC, disponibilidades de arquivos e permissões, entre outros realizados no próprio ambiente da rede interna, tanto no local, residência com os quatro PCs, como em outro ambiente externo.

Os testes foram desenvolvidos em dois cenários diferentes e independentes:

CENÁRIO 1: Na própria rede local através do domínio, onde o invasor conheça toda rede e obtenha acesso alguma máquina nesse domínio. A rede contém um servidor para o professor e administrador mais algumas estações para os alunos que são conectados via domínio com o servidor.

CENÁRIO 2: O usuário está conectado na rede, mas não tem acesso ao domínio, porém obtém acesso por meio de um arquivo por engenharia social ou de programas citados abaixo para aquisição dos mesmos.

### 4.1.3. Especificação dos Equipamentos

Neste estudo de caso foram utilizados diversos equipamentos tanto para configuração da internet, quanto para análise da rede, conforme a Tabela 1.

| **Equipamentos** | **Sistemas** |
|---|---|
| *Desktop* | Windows XP |
| *Desktop* | Windows XP |
| *Notebook* | Linux Ubuntu e Windows 7 |
| *Servidor* | Windows server 2008 |
| Modem roteador wireless | |

TABELA 1 - ESPECIFICAÇÃO DOS EQUIPAMENTOS UTILIZADOS NO ESTUDO DE CASO.

### 4.1.4. A instalação do servidor

O servidor possui o Windows Server 2008 original onde está instalado por completo a versão entriprise 64 bits em um computador com um processador Core 2 duo 7400, 2 GB de memória RAM, HD de 320 GB, gravador de DVD, placa mãe phitronics, fonte de 550 wats, monitor de 22 polegadas, teclado e mouse. Após a instalação do Windows Server Entriprise, toda a configuração necessária foi instalada.

Toda configuração foi feita com bloqueio de instalação e alguns sites para os usuários não instalarem programas como foi realizado abaixo, onde na tentativa de instalação, exibiu mensagens de bloqueio para os usuários.

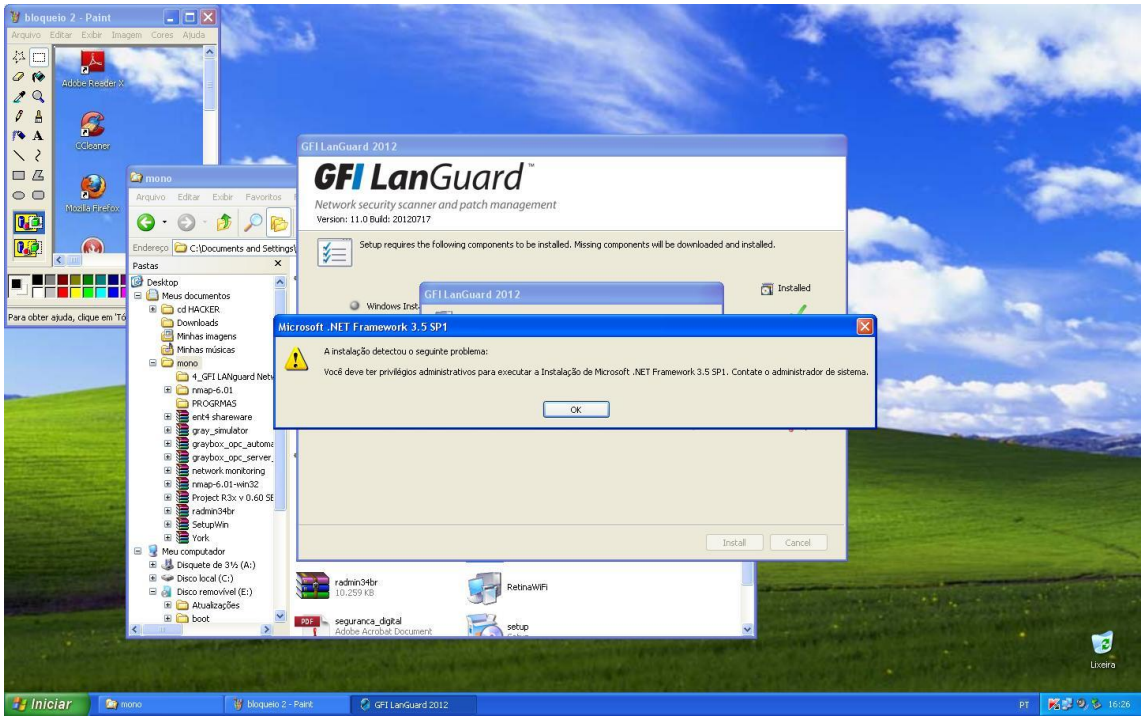


FIGURA 01 – Mensagem de bloqueio de instalação de programas na instalação do LanGuard.

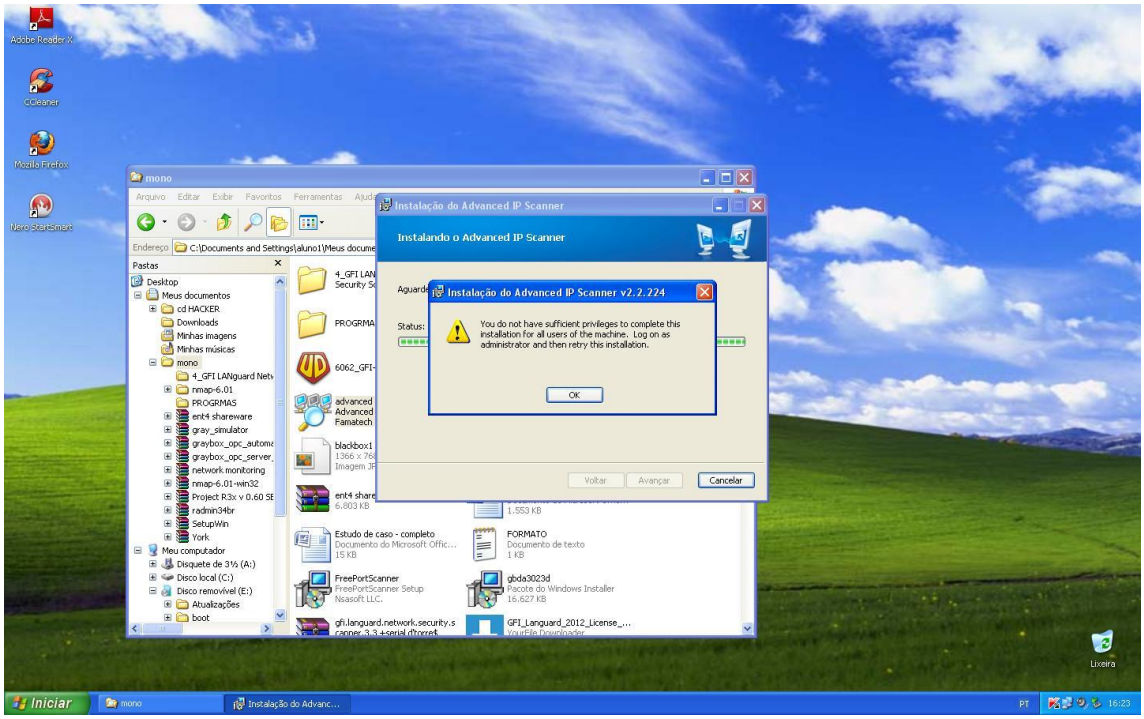


FIGURA 02 - Mensagem de bloqueio de instalação de programas

Para os usuários bem cadastrados no domínio, além dos bloqueios, caso eles queiram acesso a qualquer arquivo do servidor ou de uma estação, foi pedido uma senha para acessar a mesma.(figura 03 , figura 04 e figura 05 ).

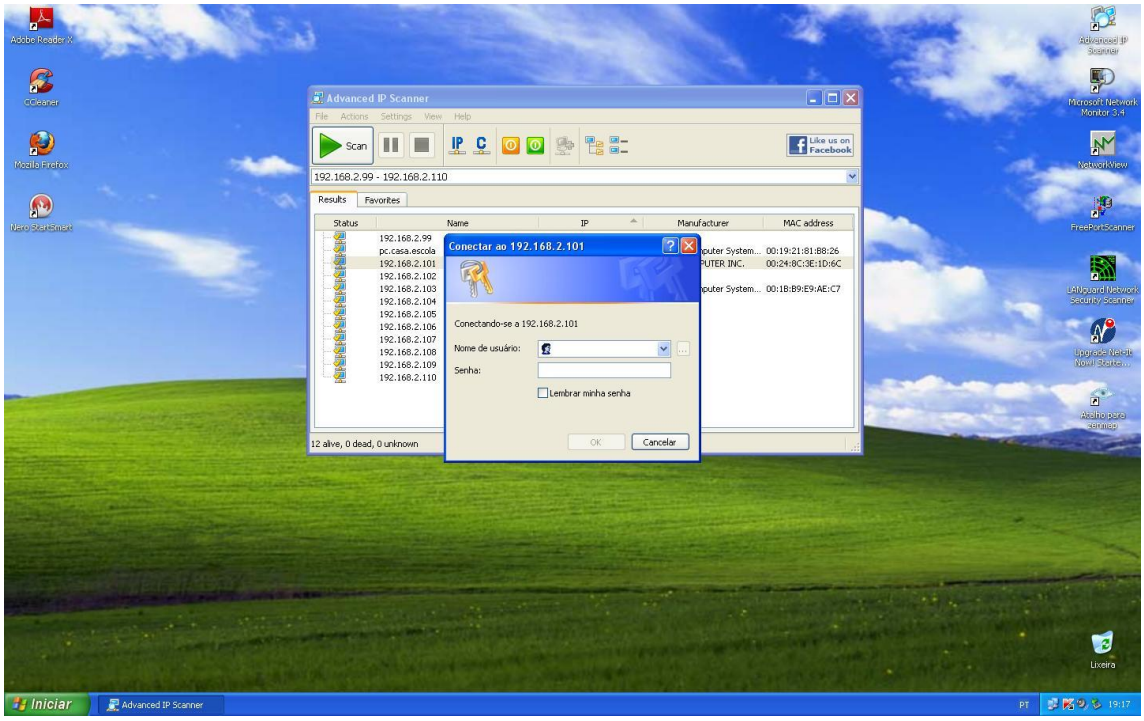


FIGURA 03 – Login de acesso ao servidor

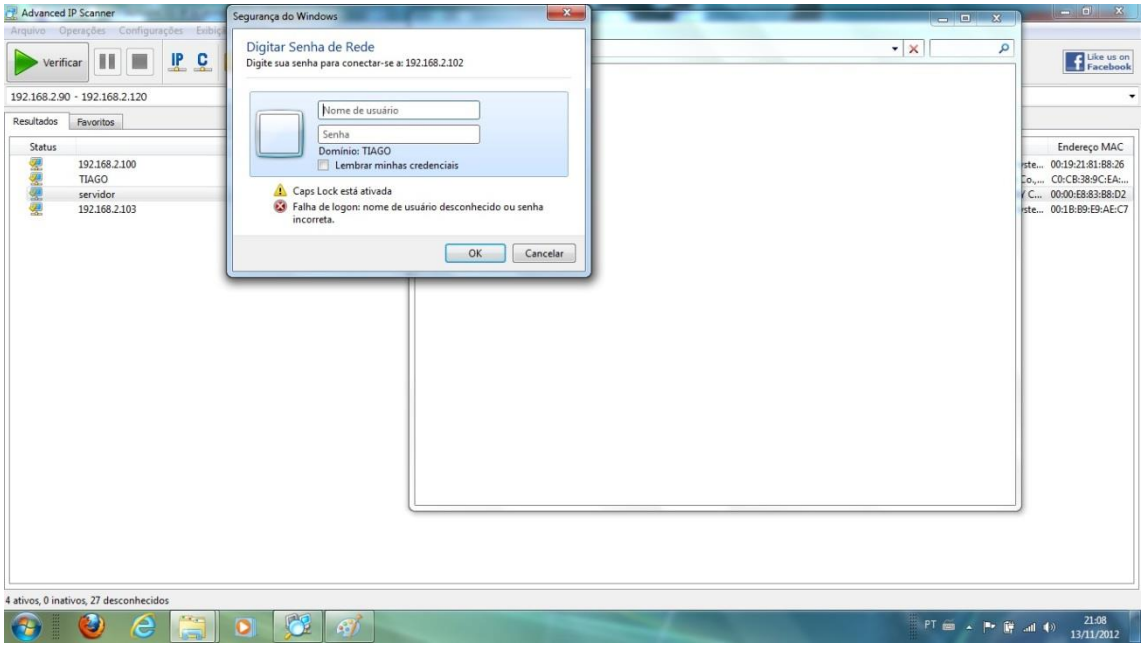


FIGURA 04 – Login de acesso ao servidor através do programa Advanced IP Scanner


FIGURA 05 – Login de acesso ao servidor

### 4.1.5. Planejamento

Para a rede, simulando uma escola técnica, o hacker iria conhecer informações da rede para execução do teste. Como vamos trabalhar de forma interna e externa, será apresentado apenas algumas maneiras de como ele pode conseguir essas informações, mas para isso, o livro "Segredos do Hacker ético" discursa sobre algumas perguntas que ele precisará responder para obtenção de uma invasão correta, as perguntas são:

- "Os funcionários e/ou clientes da empresa serão notificados do teste?
- Quão profundo será o teste? Apenas identificará falhas ou pode-se chegar às senhas dos diretores da empresa?
- Os testes serão realizados durante o expediente, após o horário de tratalho ou nos finais de semana?
- Quantos sistemas serão testados? Quais devem ser priorizados? Quais são considerados de missão crítica?
- O que a empresa faz? Quais suas principais atividades?
- Quais resultados estão sendo imaginados pela empresa?
- Com quem você deve falar caso algo dê errado?
- Qual o orçamento destinado?
- O que deverá ser entregue após o teste?"

(FLÁVIO, 2010)

(Flávio, 2010) fala que sempre é bom realizar um planejamento do ataque, cujo esse planejamento envolve fases para realização, para que a execução seja de forma eficiente é necessário seguir a tabela abaixo para evitar alguns erros. Lembrando que estaremos realizando um teste completo, não só visando um servidor ou uma maquia, mas sim qualquer vulnerabilidade que consta na rede.

| FASE | TEMPO MÉDIO |
|---|---|
| Planejamento | 2 a 4 semanas |
| Execução do Teste | 2 a 4 semanas |
| Fase Pós-teste | 2 a 4 semanas |
| Duração média total de 6 a 12 semanas | |

TABELA 2 – Tempo do planejamento da invasão

### 4.1.6. Verificando portas abertas na rede

Um dos principais testes de um Hacker ou Cracker se chama Penetration Test (Teste de Penetração), onde existe programas específicos para atacar/ tentar invadir um objetivo, sendo este um usuário, uma rede, sistema ou ambiente no qual se deseja detectar falhas (nosso caso).

Para (Flávio, 2010), existe três programas para realizar essa penetração. São eles:

- Black Box: Utilizado para simular ataques de invasores externos que não conheçam a estrutura da rede e sistema que estão varrendo.
- White Box: Utilizado com total conhecimento da rede ou sistema a ser atacado, onde já tem um objetivo especifico, são realizados para verificar vulnerabilidades no sistema.
- Gray Box: Utilizado quando há conhecimento parcial da estrutura a estudar.

Na nossa estrutura, usaremos o Black Box para simular um invasor que queira prejudicar a instituição sem saber como funciona o sistema e utilizaremos o White Box simulando um aluno que participe da rede e queira prejudicar a instituição de alguma maneira.

### 4.1.7. Softwares

Para uma análise da rede com o intuito de verificar quais portas estão abertas e quais computadores estão conectados a rede é preciso utilizar alguns programas e comandos para a identificação dos mesmos. Para análise da rede, temos os seguintes programas:

- Advanced IP Scanner

Programa para análise da rede com função de descobrir o status, nome, IP, nome NetBIOS, grupo NetBIOS, fabricante, com ele o administrador da rede obtém o controle total sobre os computadores de um local.

- Zenmap (Windows) e comando nmap para linux

O Nmap ou Network Mapper, tem como função essencial a detecção de computadores e serviços na rede, disponibilizando um "mapa" dos PCs na rede. Segundo (Simões, 2010) o nmap tem como funções mais importantes:

> • "Identificação dos computadores de uma rede, por exemplo, a lista dos computadores que respondem a pings, ou que tenham um determinado porto aberto;
> • Detecção de portos abertos em um ou mais computadores de destino;
> • Identificação dos serviços de rede em computadores remotos para determinar o nome da aplicação e o número da versão que estão a executar num computador de destino;
> • Detecção do sistema operativo e algumas características de hardware de dispositivos de rede."

| SINTAXE | FUNÇÃO |
|---|---|
| St | Conexão via TCP para a verificação de portas abertas |
| sS (SYN Scan) | Serve para descobrir portas TCP abertas sendo ligeiramente mais discreto. |
| sF (FIN Scan) | Também serve para descobrir portas TCP abertas sendo mais rápido que o sS, não roda se a maquina analisada estiver usando Windows. |
| sX (Árvore de Natal) | Manda os flags FIN, URG e PSH ligados para descobrir portas TCP abertas e ser mais discreto que o –sS. |
| sN (Null Scan) | Manda pacotes TCP sem nenhum flag ligado para descobrir portas abertas; dessa forma, também consegue se mais discreto que o –sS. |
| sU (UDP Scan) | Serve para descobrir portas UDP abertas. |

TABELA 3: SINTAXE DE ALGUMAS OPÇÕES DO NMAP COM AS POTENCIALIDADES OU FUNÇÕES DA FERRAMENTA. FONTE: SHEMA (2003). ELABORAÇÃO DO AUTOR.

- Languard

Programa para verificação de segurança de um PC. Traz as seguintes informações: Sistema operacional XP,WIN 9x, 7, Unix etc. Tipo de conexão, se Dial-up, Veloz ou GVT, nome do provedor a que pertence aquela faixa de IP, portas e serviços que estão rodando na máquina, nº MAC da placa de rede, vulnerabilidade CGI se existir.

- PCFinder 4.3

Serve para escanear o endereço IP para obter endereços de MAC e nomes de Host dos computadores na sua rede local. Possibilitando a verificação de dispositivos desatualizados na rede.

- Essential NetTools

O NetTools é uma ferramenta para o administrador ter diagnóstico da rede e monitorar conexões de rede do computador. É um poderoso software para todos os interessados em usar diariamente para sua rede ou obtenção de dados de uma rede a ser invadida. Essa ferramenta realiza a exploração da rede, da segurança, diagnosticando tipos de conexões na rede.

- Nessus

O Nessus é uma ferramenta de invasão remota de vulnerabilidades para sistemas Linux, BSD, Solaris e outros Unixes. O seu funcionamento é baseado em plugins, indicam as vulnerabilidades e os passos que devem ser seguidos para elimina-lás. Ele verifica o tipo de serviço que está rodando nas portas, verificando assim, as vulnerabilidades nos serviços em determinada porta, porém o mais importante desse programa é saber analisar de forma correta todas as instruções que ele apresenta para o praticante.

## 4.2. Execução do teste

Após identificar todos os tipos de problemas que podem vir a causar brechas de segurança no sistema montado, por exemplo, senhas fracas, programas piratas ou desatualizados, vírus, engenharia social etc. É interessante o invasor utilizar um notebook próprio para evitar utilizar computadores dos clientes, que contenha informações importantes e que possa lhe criminar de algo, o notebook deve conter ferramentas necessárias para o teste mostrado anteriormente.

### 4.2.1. Busca de vulnerabilidades

Primeiro, foi analisado que os computadores poderiam ter acesso como administrador, tornando assim alvo fácil para o praticante instalar os programas que serão mencionados abaixo, além do usuário ter acesso à conta de administrador, baseado no Curso EC-Council | Certified Ethical Hacker e alguns trechos encontrados na internet, existe, na geral quatro categorias de vulnerabilidades que podem ser encontradas:

- Os bugs específicos do sistema operativo, exploits, vulnerabilidades e buracos de segurança.
- As fraquezas no firewall e routers, entre diversas marcas.
- A exploração de scripts de web server.
- As partilhas e confianças exploráveis entre sistemas e pastas.

### 4.2.2. Hipótese, justificativa, metodologia e procedimentos

Esse projeto vem mostrar os aspectos referentes ao que hoje muita vezes é preocupação para empresas que é a segurança de seus dados. Muitas empresas não imaginam o perigo de seus arquivos confidenciais estarem desacobertados ou inseguros no seu sistema, correndo o risco da perca do mesmo, trazendo um prejuízo total financeiro, moral e ético.

No nosso caso, foi verificado a segurança da escola por completo, pois com a invasão de um computador, toda a rede se torna comprometida. Como justificativa, o trabalho teve como razão a busca de soluções para segurança, como a instalação de ferramentas, permissões de usuários, atualizações, integridade física das estações e o servidor, além de treinamento para usuários.

Para obtenção de soluções, foi analisado o ambiente, instalações de programas, verificações de permissões e analise de acesso de usuários. Com utilização de vários programas, identificou-se a falhas dos sistemas, principalmente o programa LanGuard que apresenta um resultado bastante completo como 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).

Em relação à vulnerabilidade humana, como sugestão ao gerente de rede, um treinamento para ele e os professores, para os alunos, se fez de forma de acesso ao servidor e até mesmo um treinamento para o bom funcionamento da rede. Verificado também por meio de engenharia social, sugeriu um mini-curso para fortalecer essa segurança. Lembrando que, esse trabalho não explica técnicas nem ferramentas para invasão, o mal uso dessas ferramentas podem danificar o bom funcionamento dos computadores e da rede.

## 4.3. Avaliação dos Resultados

O estudo comprovou a insegurança existente nos dois cenários, no primeiro, no qual apresenta um notebook ligado à rede mais não no domínio, foi executados os programas abaixo e encontrado algumas vulnerabilidades.

## 4.4. Testes realizados nos cenários dos pontos de acesso.

### 4.4.1. Advanced IP Scanner

Através deste programa ou do PROMPT DE COMANDO, conseguimos saber a qual IP cada máquina da rede pertencia; com o DOS, basta realizar pings através dos IPs referente à classe da rede correspondente, caso apresentasse respostas, representava uma máquina, porém, pelo Advanced IP Scanner, além de descrever IPs de toda a rede, concebia os nomes das máquinas representadas pelos IPs, a marca da placa mãe, MAC da placa de rede e nome de todos os computadores.

#### 4.4.1.1. Teste fora do domínio

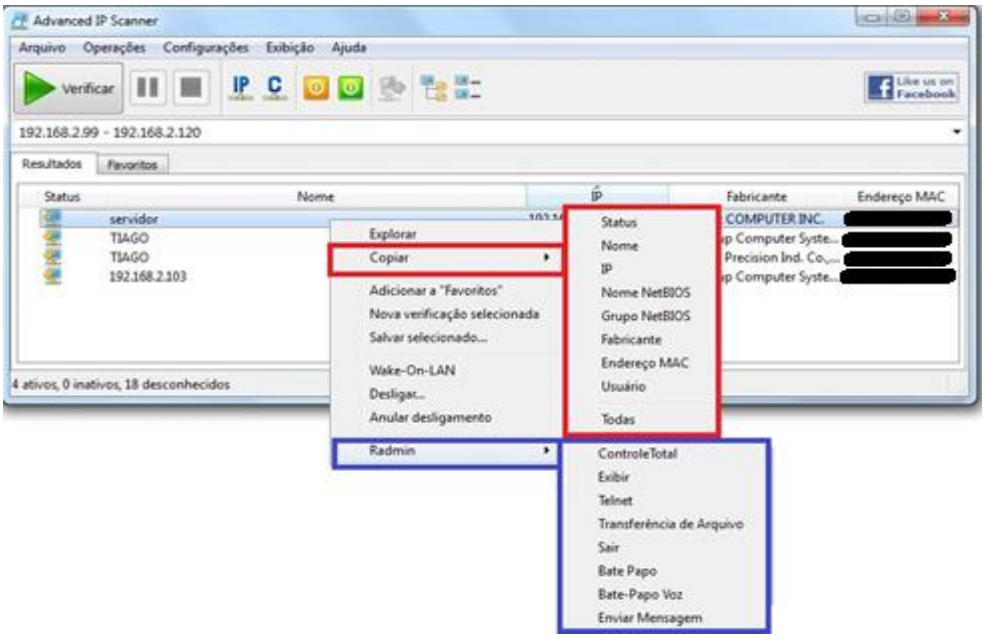


FIGURA 06 – Ferramentas do programa Advanced IP Scanner

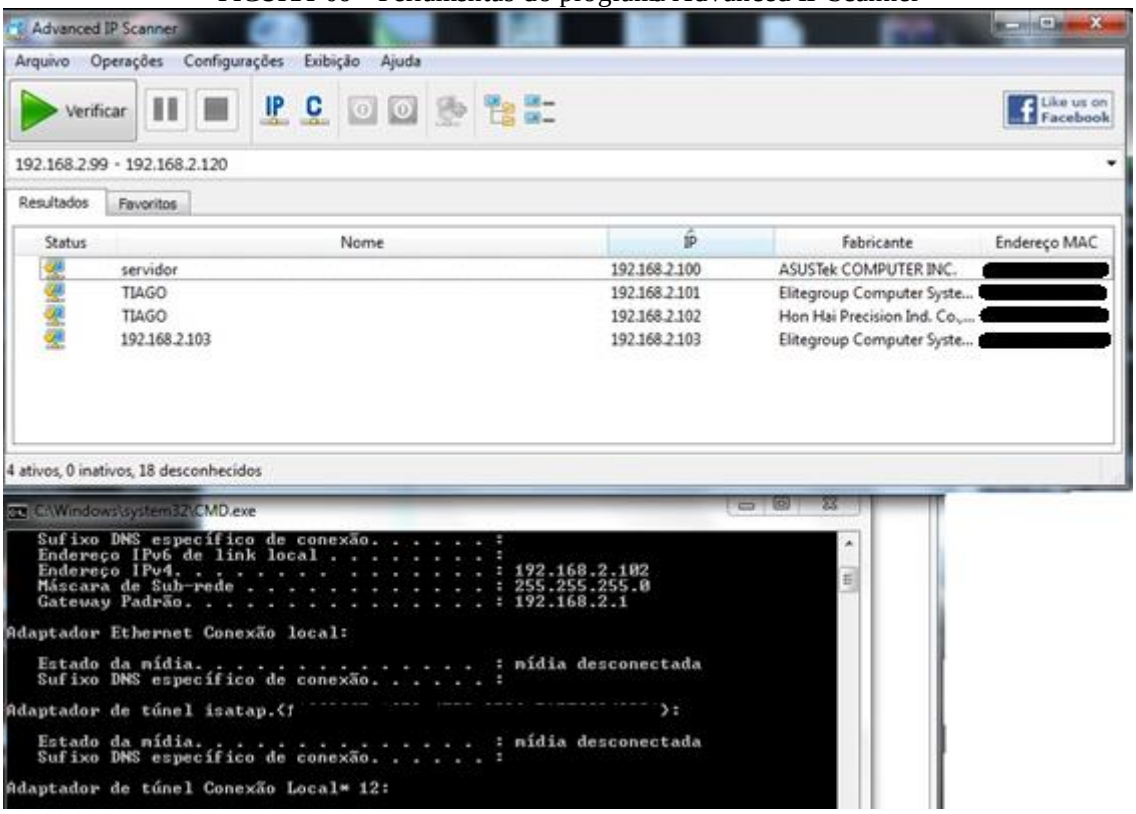


FIGURA 07 – Scanner de IP na rede local.

Na figura 07, temos o teste com Advanded IP Scanner e abaixo, o comando ipconfig para demonstrar o IP da máquina.

#### 4.4.1.2. Teste dentro do domínio

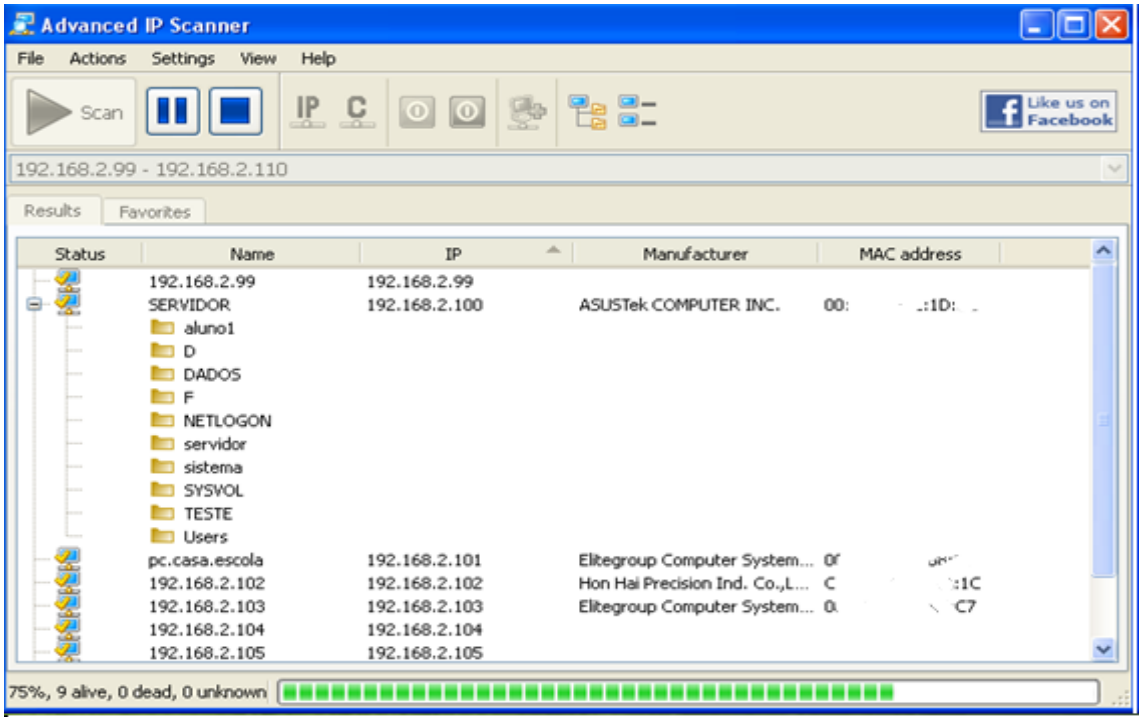


FIGURA 08 – Scanner de IPs e pastas compartilhadas na rede.

Com ele era possível verificar também as pasta e impressora compartilhadas de todos os computadores, tendo total acesso a elas, tornando assim uma vulnerabilidade dos arquivos de cada usuário.

### 4.4.2. PCFinder 4.3

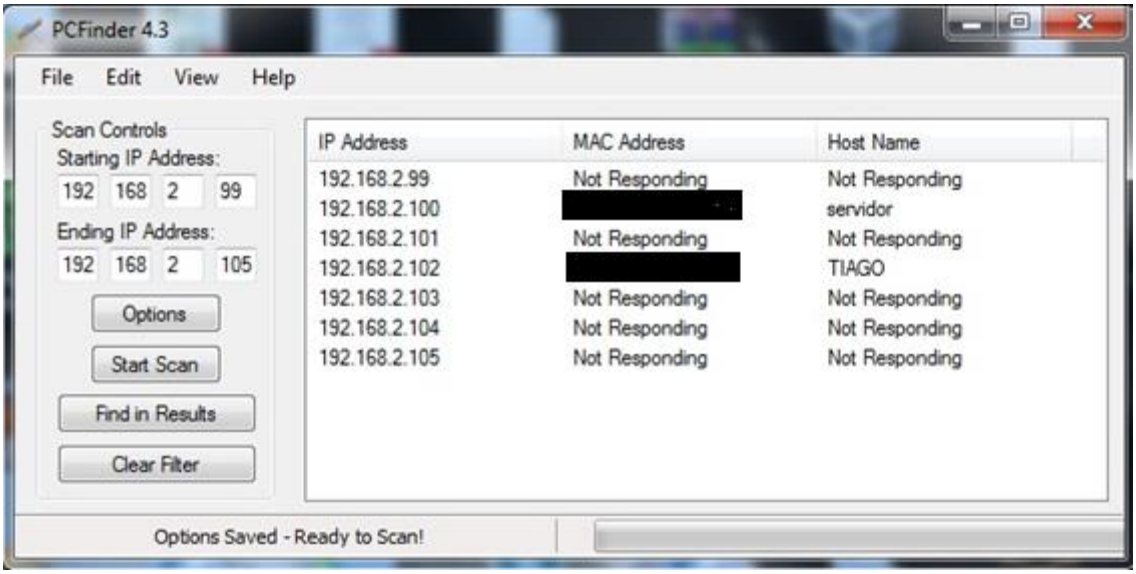


FIGURA 09 – Scanner de Rede pelo programa PCFinder 4.3

Outro programa para verificar os PCs de uma rede é o PCFinder, ele apresenta opções de realizar um escaneamento em uma determinada faixa de IP, reconhecendo assim, todos os computadores ligados com seus respectivos IP, MAC Address e Host Name.

### 4.4.3. Zenmap (Windows) e comando nmap para Linux

#### 4.4.3.1. Teste dentro ou fora do domínio

Após a detecção do IP da maquina a ser analisada, o nmap ou Zenmap(Windows), proporciona um teste fora ou dentro da rede para aquisição o nome, domínio, portas abertas, tipo de sistema operacional, MAC da placa de rede, entre outras. Informações que para um hacker, são muito valiosas para implementações de técnicas que detenha obtenção de dados. Representadas nas figuras abaixo.

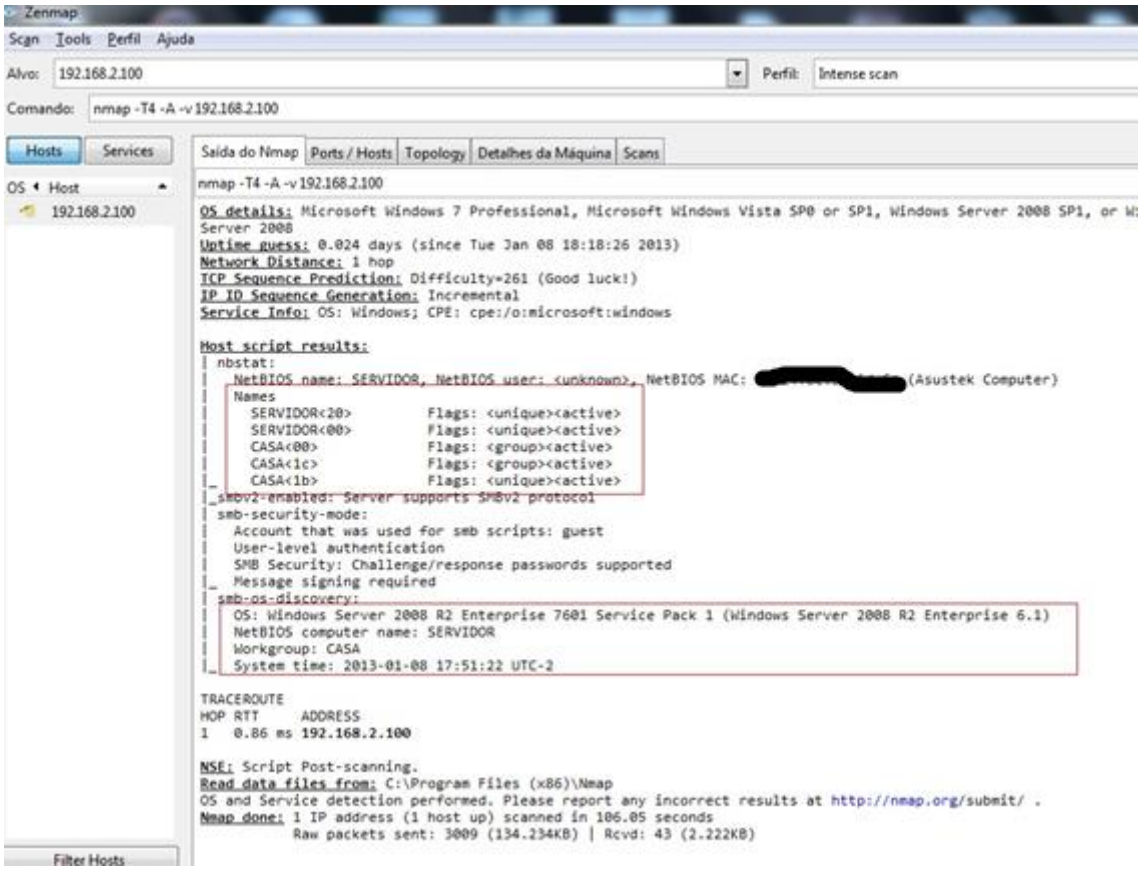


FIGURA 10 – Informações da máquina alvo pelo Zenmap.

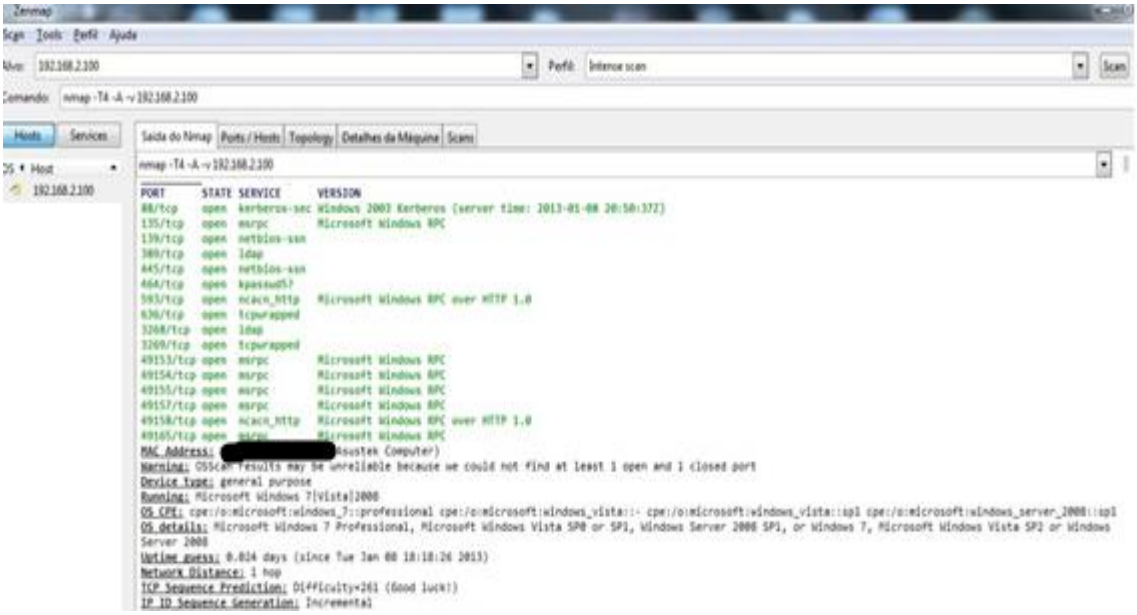


FIGURA 11 - Informações da máquina alvo pelo Zenmap.

### 4.4.4. IP Range - Angry IP Scanner

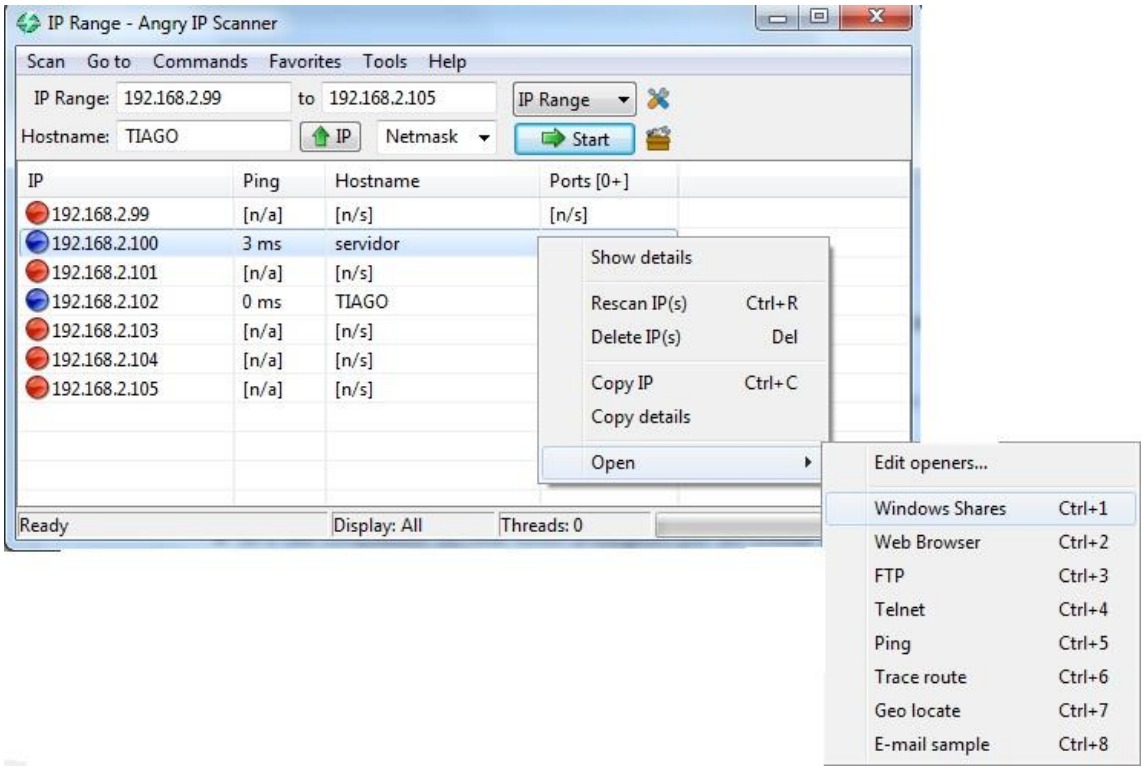


FIGURA 12 – Ferramentas do programa IP Range – Angry IP Scanner.

Já o IP Range, varre uma rede selecionada para mostrar todos os computadores representando os notada por uma bolinha azul e a não encontrada com uma bolinha vermelha, também com a função de explorar o PC alvo, teste de ping, trace route(traça toda rota do computador verificado até o computador correspondente), entre outros.

### 4.4.5. Keylogger

Outro programa bastante utilizado pelos invasores, são Keylogger instalados nas máquinas alvejadas para obtenção de todas as teclas digitadas no tecledo, onde eles podem obter todas senhas digitadas de qualquer site, principalmente de banco ou redes sociais. Um exemplo de um Keylogger é o Win spyMaster, representado na figura abaixo.

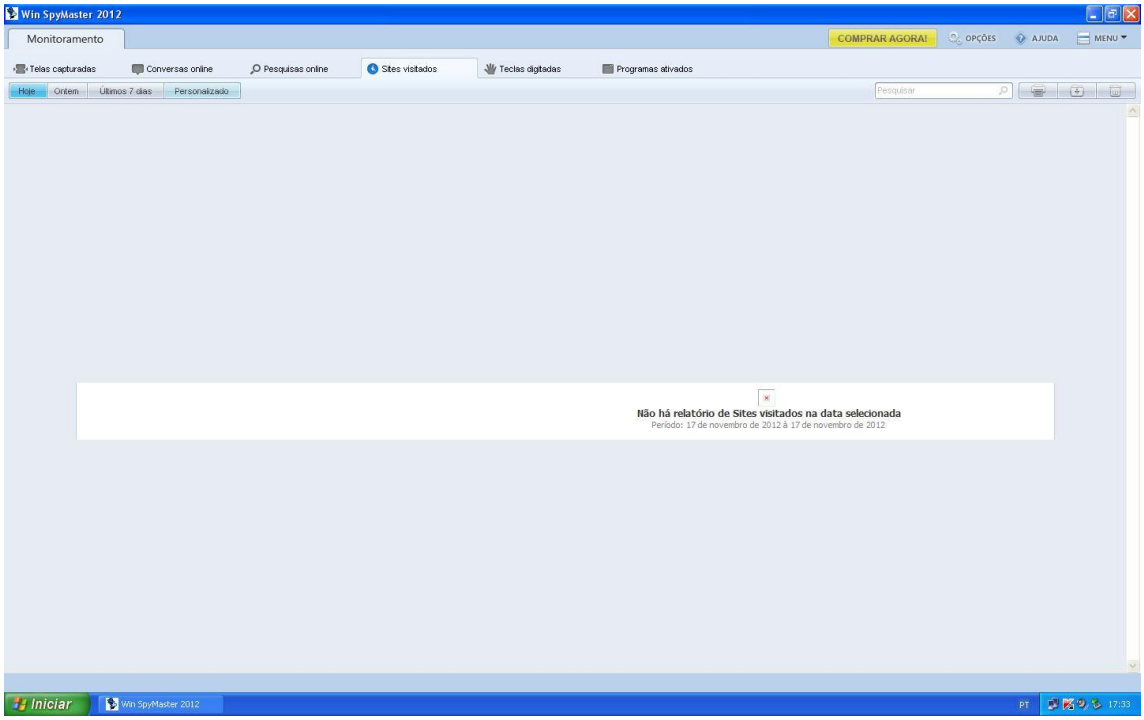


FIGURA 13 - Keylogger

## 5. CONSIDERAÇÕES FINAIS

O trabalho apresentou a importância da segurança da informação, pois não envolve só aspectos tecnológicos, como também outros ativos como processuais, legislativos, negócio e principalmente humano. Infelizmente, empresas não dão muita importância para os dados e a rede de sua instituição, muitas vezes, só acumulará do prejuízo, quando são alvos de ataques que por sorte, alguns venderam os dados roubados, no entanto alguns fazem a invasão só para prejudicar a mesma.

Com os testes, foi verificado várias vulnerabilidades em uma simples rede de computadores. Porém em uma rede com 20, 30 100 computadores, essas vulnerabilidades iriam aumentar muito mais. Por isso, é importante lembrar sempre que esse processo é contínuo, um investimento insignificativo que protege por completo. É válido lembrar-se

entretanto, que tem que se investir não só na tecnologia, mas principalmente no ser humano que por causa de sua fraqueza, acaba por cometer atos que todo invasor deseja.

### 5.1. FASE PÓS-TESTE

Realizado os testes e verificado as vulnerabilidades, realizou alguns procedimentos para evitar que aconteça alguma ameaça ou brecha na rede, tais procedimento foram:

- Utilização de senha no setup, onde através dele, todos podem desabilitar qualquer componente da placa mãe, dá boot para qualquer dispositivos para ter acesso a qualquer tipo de sistema para remover senhas, formatar, instalar programas, criar usuários, no Windows vista e 7 modificar o ícone de acessibilidade para o MS-DOS, entre outros.
- Apenas compartilhar as pastas necessárias no servidor e nas estações, aonde todos os usuários conseguia visualizar e modificar as pasta que fora denominado permissão.
- Desativar acesso de outra rede fora do domínico, com isso, o invasor poderá modificar, verificar, invadir o domínio.
- Desativar a permissão de pings nos IPs da rede, evitando assim que identifique assim quantos computadores estava ligado no momento, realizando apenas um teste de conectividade dos IPs.
- Desativar o DOS por completo, como também o comando traceroute, pois o mesmo conta os “hops” da rede, desde a máquina em que é executado até à máquina/sistema alvo.
- Realizar um treinamento humano, mostrando os perigos de acesso e de utilização.

### 5.2. PERSPECTIVAS FUTURAS

Realizado os estudos, as novas perspectivas são apresentar esse projeto com estas ferramentas mais outros softwares pagos, com intuito de mostrar o risco, como também a proteção necessária de obter em suas redes; apresentar para empresas e instituições que detêm dados a ser preservados, caso reflua às informações, a empresa venha a perder tudo, sendo essencial a segurança desse arquivos.

## 6. REFERÊNCIAS BIBLIOGRÁFICAS


ANA PAULA & DOUGLAS NASCIMENTO. voz sobre ip: estudo de vulnerabilidades e implantação de segurança. instituto federal do espírito santo - espírito santo - 2011.

ARAÚJO, Eduardo Edson de., **A vulnerabilidade humana na segurança da informação**. Trabalho de Conclusão de Curso em Sistema de Informação. Faculdade de Ciências Aplicadas de Minas, Uberlândia – MG, 2005

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do hacker ético**, 3 ed. Florianópolis:Visual Books, 2010

BEAL, Adriana - Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação das organizações. -São Paulo: Editora Atlas, 2005.

BELHASSOF, RONEY. Debate sobre o projeto de combate aos cibercrimes. Disponível em: http://www.clubedohardware.com.br/blog/251. Acesso em julho de 2012.

BERBERT, FÁBIO. O que é e como funciona um ataque de força bruta. Disponível em:http://www.vivaolinux.com.br/artigo/O-que-e-e-como-funciona-um-ataque-de-forca-bruta. Acesso em julho 2012.

CONCEITOS de segurança – TI. 2000. Disponível em: <http://www.ti.petrobras.com.br/gcom/seguranca/>. Acesso em: 25 jul. 2005

CONHEÇA a segurança da informação no governo federal brasileiro. Módulo Security Magazine, São Paulo, n. 328, 09 fev. 2004. Disponível em:<http://www.modulo.com.br/arquivoboletins/2k4/msnews_no328.htm>. Acesso em: 10 out. 2005.

DAVENPORT, T., PRUSAK, L. Conhecimento empresarial. Rio de Janeiro: Campus,

2000, 18p.

FONSECA, Paula F. **Gestão de Segurança da Informação**: O Fator Humano. 2009. 16 f. Monografia (Especialização)– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Acesso em: 24 ago. 2012.

GIORDANI RODRIGUES, InfoGuerra; Segurança e Privacidade (http://www.infoguerra.com.br). Acesso em 15 de julho 2012.

HONÓRIO, Paulo Henrique Araújo., **Hackers – Como se proteger**?. Trabalho de Conclusão de Curso em Ciências da Computação. Centro Universitário do Triângulo, Uberlândia – MG, 2003

Jacques D (2003) Ensino de pequenos grupos. In: Cantillon P, Hutchinson L, Wood D, eds. BMJ ABC de Ensino e Aprendizagem em Medicina. BMJ Publishing Group, London: 19-21p

LANDIM, WIKERSON. O lado obscuro da internet. Disponível em: http://www.tecmundo.com.br/internet/15619-deep-web-o-lado-obscuro-da-internet.htm . Acesso em julho de 2012.

LAUDON K. C. & LAUDON J. P. Sistemas de Informações Gerenciais. São Paulo: Prentice Hall, 2004

MAIA, Marco Aurélio. Engenharia social. Disponível em: <http://geocities.yahoo.com.br/jasonbs_1917/seguranca/leiamais_engsocial.html>. Acesso em: 10 maio 2012.

MATOS, ALEXANDRE. Tutorial Sniffing. Disponível em:http://invasaowirelles.blogspot.com.br/2010/01/tutorial-sniffing-definitivo.html. Acesso em setembro 2012.

MCLURE E SCAMBRAY, **Hackers Expostos Segredos e Solucoes para a Seguranca de Redes 2ª Edição, Editora Makron Books, 2001, 336p.**

MITNICK, KEVIN. O conhecimento que assusta. InformationWeek Brasil, [São Paulo], 2003. Entrevista. Disponível em: <http://www.informationweek.com.br/iw70/mitnick/>. Acesso em: 03 ago. 2012

MÓDULO Security Solutions S.A. 9ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro, 2003. Disponível em: <http://www.modulo.com.br/temp/9aPesquisaNacional_Modulo.zip>. Acesso em: 15 out. 2012.

NMAP. Disponível em <http://www.insecure.org/nmap/> Consultado em 12/11/2012.

NESSUS. Disponível em <http://www.nessus.org> Consultado em 12/11/2012.

NOGUEIRA, MARCIO. Worms e Vírus. Disponível em:http://www.invasao.com.br/2008/02/17/worms-e-virus/. Acesso em julho 2012.

RAMOS, CLEISSON. Vulnerabilidades e Uso do LTSP. Disponível em:http://www.iecom.org.br/encom_2012/ENCOM_2012_1.pdf. Acesso em setembro 2012.

Revista Fonte – Segurança da Informação. Minas Gerais: Ano 4 – Número 07: Julho / Dezembro, 2007, 86p

SCHNEIER, Bruce, Segurança.com – Segredos e mentiras sobre a proteção na vida digital. Editora Campus, 2001, 254p.

SECURITY OFFICER, DATA SECURITY, http://www.datasecurity.com.br/index.php/cursos/security-officer-foundation

SÊMOLA, Marcos. Gestão de segurança da informação: uma visão executiva. 8º ed. Rio de Janeiro, Editora Campus, 2003, 156p.

STANTON, Michael, A evolução das redes acadêmicas no Brasil: Parte 1 – da BITNET à internet. Boletim Trimestral da RNP, Vol. 2, n. 6. Rio de Janeiro: RNP, 1998. Disponível em <http://www.rnp.br/newsgen/9806/inter-br.html>. Acesso em 24 de agosto de 2009.

ULBRICH, H.C. **Universidade Hackers livros Exercícios.** São Paulo: Digerati Books, 2005. 65p, 77p, e 183p

VALLE – ULBRICH, DELLA. **Universidade H4CK3R - Desvende o submundo hacker**, CIDADE: Digerati Books, Vol 01, 2011

VIEIRA, LUIZ. Teste de invasão. Disponível em:http://segurancalinux.com/artigo/Teste-de-invasao-%28parte-1%29-Identificacao-de-banner/?pagina=1. Acesso em julho 2012.