UNIPAC
UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS
FACULDADE DE CIÊNCIA DA COMPUTAÇÃO E
COMUNICAÇÃO SOCIAL

CURSO DE CIÊNCIA DA COMPUTAÇÃO

Victor Tadeu Pereira de Araujo

SEGURANÇA EM REDES DE COMPUTADORES PARA SERVIDORES WINDOWS EM INTRANETS

BARBACENA
DEZEMBRO DE 2004

VICTOR TADEU PEREIRA DE ARAUJO

SEGURANÇA EM REDES DE COMPUTADORES PARA SERVIDORES WINDOWS EM INTRANETS

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação e ao Departamento da Faculdade de Ciência da Computação da UNIPAC – Universidade Presidente Antônio Carlos como requisito parcial para a obtenção do Titulo de Bacharel em Ciência da Computação.

Orientador
Prof. Luís Augusto Mattos Mendes

BARBACENA
DEZEMBRO DE 2004

VICTOR TADEU PEREIRA DE ARAUJO

SEGURANÇA EM REDES DE COMPUTADORES PARA SERVIDORES WINDOWS EM INTRANETS

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação e ao Departamento da Faculdade de Ciência da Computação da UNIPAC – Universidade Presidente Antônio Carlos como requisito parcial para a obtenção do Titulo de Bacharel em Ciência da Computação.

Aprovada em _____/_____/_____.

BANCA EXAMINADORA

_____
Prof. Luís Augusto Mattos Mendes – Orientador do Trabalho

_____
Prof. Ms. Gustavo Campos Menezes – Membro da Banca

_____
Prof. Eduardo Macedo Bhering – Membro da Banca

Agradeço primeiramente ao meu Orientador que com sua competência e paciência me ajudou a concluir este trabalho. Agradeço a Deus e aos meus pais que me deram muita força para chegar aonde cheguei, e agradeço também aos meus colegas que de certa forma me ajudaram neste trabalho.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Hoje em dia um dos principais problemas que estamos vivendo é a falta de segurança que afeta vários locais e áreas de todo o mundo, principalmente depois do avanço tecnológico das redes, fazendo com que a *Internet* se expandisse de forma que o mundo todo pudesse se interconectar.

Essa era da comunicação onde uma pessoa pode se comunicar facilmente com uma outra que está do outro lado do mundo, trouxe vários benefícios para a população mundial, mas também trouxe mais um meio de violação e crime que pode causar danos a empresas e pessoas. Com isso cuidar da segurança de sistemas em empresas ou até mesmo dentro da própria casa se torna algo essencial para que intrusos não tenham acesso a dados confidenciais em sistemas vulneráveis.

Através do sistema operacional Windows 2000 pode-se conseguir um bom nível de segurança para impedir que essas pessoas mal intencionadas consigam invadir uma rede interna que esteja conectada à *Internet*. O Windows 2000 traz vários novos recursos que se previamente forem bem configurados podem diminuir ou até mesmo sanar algumas vulnerabilidades do sistema. Mas para prover de um nível maior de segurança será necessário o auxílio de algumas ferramentas atualizadas assim como uma política de segurança bem estruturada.

Este estudo irá mostrar quais que são esses recursos que a versão 2000 do Windows traz em relação às versões anteriores, que fez com que ele se tornasse um sistema muito mais confiável e estável. Além de também falar sobre as ferramentas e a política de segurança. O trabalho trata no capítulo 2 das técnicas de ataque e invasão em redes Windows. Já no capítulo 3 serão abordados os recursos de segurança do Windows 2000. No capítulo 4, segurança em redes Windows, serão tratados os principais tipos de ferramentas de segurança que existem definindo uma política de segurança em cima de uma configuração básica do Windows 2000. No capitulo 5 será apresentado a conclusão deste estudo.

2 TÉCNICAS DE ATAQUES E INVASÕES EM REDES WINDOWS

Quando falamos de segurança em uma rede corporativa, estamos pensando nos cuidados que devemos tomar para impedir que intrusos consigam invadir e ter acesso a informações que são importantes para determinado ambiente corporativo.

Existem vários tipos de ataques a sistemas, e muitos modos de agrupá-los em categorias distintas. Um destes modos seria o de dividí-los em três grupos: intrusão, negação de serviços e roubo de informações. A intrusão é uma forma de ataque onde o atacante tem acesso não autorizado a dados ou serviços de um computador de outra pessoa como se fosse o usuário legítimo. O ataque de negação de serviços tem como objetivo interromper a utilização dos recursos computacionais da vítima. O roubo de informações é uma das técnicas utilizadas para se obter dados importantes sobre a rede ou *host* alvo.

2.1 Intrusão

A intrusão é a forma de ataque mais utilizada atualmente por ter o propósito principal de permitir ao atacante acesso não autorizado a dados ou serviços dos sistemas alvo. A utilização deste ataque pode ser usada para mesclar outros tipos deles, devido ao fato do intruso conseguir o controle do sistema podendo adquirir informações importantes sobre o usuário ou do próprio sistema.

Segundo Marques (2001, p.104) dependendo do grau de acesso obtido, o atacante pode ver-se em condições de alterar o conteúdo dos dados sem que isso seja percebido. Os efeitos dessa ameaça podem ter conseqüências piores do que uma simples quebra de confidencialidade dos dados. Para isso utilizam-se as técnicas de *Trojan Horses*, *Buffer overflow*, *Spoofing* e a exploração do relacionamento de confiança.

2.1.1 Trojan Horses

O *Trojan Horses*, ou mais comumente conhecido como cavalo de tróia são programas que demonstram um tipo de comportamento determinado, ou serve para realizar uma determinada tarefa, sem que o usuário saiba. Na maioria das vezes abrem o computador para invasões ou acessos remotos.

Existem vários métodos para se instalar *Trojans* em um sistema alvo. Os *Trojans* geralmente são ocultados em meio ao código de outro programa, podendo assim reproduzir alguns dos métodos de inserção ou "contágio" que são próprios do vírus de computador ou ainda são inseridos por meio de acesso não autorizado. Martins (2003, p.219) destaca que se o usuário que estiver "logado" no sistema tiver permissão de administrador, o *hacker* poderá fazer, através do *trojan*, qualquer coisa com o computador. É comum que *hackers* instalem *trojans* nos computadores das vítimas para, através deles, fazer ataques a outros sites, impossibilitando sua identificação.

Existem vários *Trojans* conhecidos como, por exemplo, o *Wincrash*, *NetBus*, *DeepThroat* e *SubSeven*, entre outros.

2.1.2 *Buffer overflow*

Segundo Marques (2001, p.107) esta denominação designa um conjunto de ações e métodos destinados a explorar uma classe de vulnerabilidades que afeta grande número de sistemas operacionais e aplicativos.

Em programas que não tratam a consistência dos dados de entrada, pode haver uma desestruturação do código em execução, permitindo que o código estranho seja enviado e executado. Por exemplo, um *buffer* de entrada de dados, que não possui consistência de dados e que seja configurado para receber 32 bytes, caso aconteça de alguém enviar mais do que esse limite de dados, normalmente causaria um estouro de *buffer* (*buffer overflow*) e, com isso, o que passar dos 32 bytes invadirá outras áreas de memória do sistema. Dependendo de que áreas sejam essas, é possível que esta "carga extra" seja executada, ocasionando a invasão.

As formas mais comuns de *buffer overflow* são encontradas em servidores *Web* e de FTP. Ao se submeterem uma URL muito grande (geralmente acima de 150 caracteres) o servidor para de responder. Vários servidores já foram vítimas de tais vulnerabilidades, como *Apache Web Server*, o *Internet Information Server*, *War FTP*, entre outros.

2.1.3 *Spoofing*

Marques (2001, p.104) afirma que o *Spoofing* é usado freqüentemente para explorar uma relação de confiança ou um mecanismo de autenticação baseado unicamente em endereço IP. De fato, existem vários serviços que concedem acesso a endereços IP especificados, como o NFS e o serviço de Proxy do MS Windows NT.

Vários sistemas usam relações de segurança entre determinadas estações ou redes baseado no endereço IP ou nome de uma máquina, assim um acesso pode ser obtido ou facilitado. Portanto, a personificação[1] de um terceiro por um invasor pode permitir ou facilitar o acesso a um determinado recurso.

O funcionamento deste ataque se dá quando um pacote for enviado com endereço de origem falso, a máquina irá responder para este mesmo endereço, devido ao roteamento na *Internet* ser baseado no endereço IP. Se o impostor tiver meios de interceptar o pacote, não encontrará problemas na personificação, no entanto tal situação não é comum.

Normalmente, o atacante tem que primeiro retirar a estação que deseja personificar de operação através de um ataque de DOS (*Denial of Service*, negação de serviço), de forma que o pacote de resposta da máquina atacada não chegue ao seu destino. Depois disto, o invasor tem que continuar a conversação sem conhecer as respostas da máquina vítima. O TCP dificulta esta técnica numerando os pacotes de forma a poder controlar a ordem dos datagramas durante uma conexão, por exemplo, se a máquina atacada envia o pacote 1025, ele espera receber o 1026 como resposta. A inicialização desta contagem “deveria ser” aleatória e fica a cargo da máquina vítima. Entendo o “deveria ser” ao fato de alguns sistemas utilizarem processos determinísticos para este fim, facilitando assim o ataque.

[1] Fazer a autenticação de uma máquina.

2.1.4 Exploração de relacionamentos de confiança

A idéia do relacionamento de confiança é de que um *host* ou domínio declarado/ configurado como confiável passa a ter acesso automático a recursos do domínio ou *host* confiante, normalmente sem que se faça autenticações ou validações adicionais. O Windows 2000/NT utiliza esse recurso através do relacionamento entre domínios, já em outros sistemas como o UNIX é possível estabelecer o relacionamento entre *hosts*.

Uma das técnicas usadas para a exploração desse recurso é o *Spoofing*, de modo que o atacante venha a personificar um *host* confiável para obter acesso não autorizado. Outra forma que também é utilizada é quando o atacante que consiga acesso a arquivos, que são usados para listar os *hosts* e usuários considerados confiáveis, possam incluir entradas de modo a atribuir o status de usuário confiável a si próprio, ou de *host* confiável à máquina que lhe for conveniente.

2.2 Negação de serviços

A técnica de negação de serviços, mais conhecida como DOS (*Denial of Service*) é um tipo de ataque que explora as vulnerabilidades do TCP/IP e da implementação do mesmo pelos sistemas operacionais, com o objetivo de tornar *hosts* ou serviços da rede inoperantes ou, pelo menos, diminuir o seu desempenho ao ponto que sua utilização torne-se inviável.

> *"A capacidade de processamento, largura de banda, e capacidade de armazenamento de dados são alguns dos recursos visados pelas técnicas de negação de serviços. Falhas de implementação, bugs e outras peculiaridades dos sistemas operacionais e dos aplicativos são também considerados no desenvolvimento dessas técnicas, na medida em que podem oferecer oportunidades para comprometer o funcionamento do sistema, a partir de sua incapacidade de tratar convenientemente erros ou eventos específicos" (MARQUES, 2001, p.96).*

Esse tipo de ataque é muito utilizado para facilitar que outras técnicas possam ser usadas em conjunto, podendo deixar um *host* fora do ar para que outro *host* assuma sua

identidade ou até interrompa o funcionamento de um sistema que execute funções de segurança e controle da rede, por exemplo, derrubar servidores *Web* e impedir que eles funcionem por algum tempo evitando que a empresa faça negócios, ou até mesmo um sistema de telefonia pode ser derrubado direcionando chamadas para o PABX da vítima.

Existem algumas técnicas de negação de serviços que são o *SYN Flood*, LAND, Ataques baseados em ICMP, DDOS.

2.2.1 *SYN Flood*

Este tipo de ataque explora uma limitação do sistema operacional na implementação do protocolo TCP, e tem como objetivo travar o *host* ou serviço alvo. O *SYN Flood* consiste no envio de uma grande seqüência de pacotes TCP SYN para *host* alvo. Estes pacotes são interpretados como solicitações de estabelecimento de conexão, onde cada um deles será registrado numa fila de conexões pendentes. Os pacotes TCP SYN/ACK que são enviados pelo alvo como resposta aos falsos pedidos de conexão não serão respondidos, pois geralmente as solicitações são geradas com um endereço IP falso no lugar do endereço da máquina do atacante. Então devido ao grande número de solicitações, ocorrerá o estouro do limite da fila de conexões e começará a descartar as novas solicitações fazendo com que o host alvo se torne indisponível para outros serviços.

Segundo Martins (2003, p.228) se este ataque for dirigido, consistentemente, contra um servidor *Web* o mesmo se tornará inacessível enquanto o atacante não parar de solicitar novas conexões. Existem alguns programas prontos, que podem ser encontrados facilmente para executar este tipo de ataque como o *Elite* e o *NT Hunter*.

2.2.2 LAND

O ataque é efetuado enviando-se um pacote TCP para qualquer porta do host alvo com a flag SYN habilitada. O pacote é montado de tal forma que os endereços de origem e

destino serão iguais. Alguns sistemas operacionais não conseguem processar este tipo de pacote produzindo um *loop* que pode esgotar os recursos da máquina alvo, causando uma queda de desempenho até o travamento do sistema.

De acordo com Marques (2001, p.98) as variações desta técnica prevêem alterações em outros campos no cabeçalho IP do datagrama inválido, como as portas ou bits de controle, por exemplo. Os datagramas inválidos são enviados pelo atacante mediante o uso de software específico que permite a geração do datagrama e a adulteração dos campos conforme sua necessidade. Geralmente este ataque é direcionado à porta 139 (NetBios) de computadores com o sistema operacional Windows.

2.2.3 Ataques baseados em ICMP

Este tipo de ataque reúne um conjunto de técnicas que se aproveita das funcionalidades do ICMP (*Internet Control Message Protocol*), para criar eventos que podem afetar o funcionamento de um alvo especifico. O ICMP serve para controlar e verificar a comunicação entre *hosts* e roteadores. Ele utiliza mensagens padronizadas para que, quando enviadas, possam saber a possibilidade de comunicar-se com o *host* de destino.

O utilitário *Ping* permite o envio de mensagens ICMP a um *host* especificado a fim de verificar se ele é alcançável, então as implementações padrão do TCP/IP irão reagir automaticamente às mensagens recebidas, executando as ações apropriadas a cada caso. Elas responderão a pedidos de ICMP_ECHO ou poderão encerrar conexões estabelecidas a partir do recebimento de mensagens do tipo *Destination Unreachable* ou *Time to Live Exceeded*. Um dos tipos mais simples deste ataque é o *PingFlood*, onde uma seqüência contínua de mensagens ICMP é enviada ao *host* alvo, que ocupa-se em responder a todas elas, consumindo desnecessariamente seus recursos.

Outro tipo de ataque desta categoria é o *SMURF*. Seu objetivo não é fazer com que apenas um *host* trave, mas sim fazer com que a rede inteira pare. A execução é feita enviando-se uma seqüência de pacotes ICMP (*Internet Control Message Protocol*) modificados, onde os endereços de origem e destino são iguais, para a rede vítima. O endereço utilizado é de *Broadcast*, fazendo com que os pacotes sejam enviados para todos os componentes da rede. Os

computadores irão responder enviando mensagens ICMP, com a opção ECHO_RESPONSE, para o suposto endereço de origem onde foi enviado o *Ping*. À medida que o atacante continuar enviando novos *Pings* o tráfego da rede aumenta exponencialmente, até toda a rede parar.

2.2.4 DDOS

O ataque do tipo DDOS (*Distributed Denial of Service*) consiste geralmente em enviar para uma única máquina ou rede, milhões de pacotes de rede ou requisições de serviços. A diferença é que o ataque é efetuado através de várias máquinas espalhadas por toda a Internet, enviando tráfego simultaneamente, para um mesmo servidor, estação ou rede. Assim, não importa o tamanho da conexão do serviço vítima, ele ficará potencialmente saturado.

Como este tipo de ataque deve ser previamente organizado, existem *softwares* específicos como o TFN, o Stacheldraht e o Trin00. Essas ferramentas são instaladas em alguns hosts, deixando-os em condições de atuar como servidores. Paralelamente, um grande número de outros *hosts* recebe também componentes de *software*, fazendo o papel de clientes. As distribuições dos módulos são feitas de forma não autorizada com os componentes embutidos em outros programas supostamente inofensivos ou aproveitando-se de conhecidas falhas de segurança do sistema operacional. Ao comando do atacante, os servidores comunicam-se com os clientes, determinando o início do ataque. Em resposta, os hosts que executam o módulo cliente lançam, a um só tempo, uma série de ataques contra o(s) alvo(s) especificados inicialmente.

O DDOS merece atenção não só pela sua eficácia, mas principalmente por estabelecer um novo modelo de ataque distribuído. Várias empresas já foram alvo de ataques do tipo DDOS como afirma Vigliazzi (2002, p.6). Este tipo de ataque chamado de *Negação de serviço distribuído* foi usado para tirar temporariamente do ar sites como o eBay, Amazon.com, Yahoo, CNN, Uol e muitos outros.

2.3 Roubo de informações

Essa categoria reúne as técnicas usadas para se obter informações importantes sobre a rede ou *host* alvo. A necessidade de um atacante adquirir essas informações é válida devido ao fato de que elas possam mostrar pontos de segurança de um sistema vítima ou também mostrar as vulnerabilidades que esse sistema possui, podendo assim ajudar ao atacante a resolver qual o tipo de ataque ele irá usar para que ele consiga efetuá-lo com sucesso. Nesta categoria as técnicas podem ser divididas como ativa ou passiva. Na maneira ativa o atacante pode fazer uma ligação para sua vítima, se fazendo passar por uma outra pessoa e solicitar as informações que deseja. De maneira passiva este atacante pode instalar um grampo no telefone alvo e utilizar o que é importante para ele. O mesmo ocorre na informática, onde um *hacker* invade um computador para roubar as informações ou capturar as mensagens que trafegam pela rede para obter os dados importantes que desejar.

Segundo Marques (2001, p.87) o acesso a dados comunicados pela rede ou armazenados em *hosts* conectados não constitui-se em seu objetivo prioritário, embora algumas delas possam fornecer isso, cumulativamente ou num segundo momento. Algumas das técnicas conhecidas dessa categoria são *Cracking* de senhas, Varredura de portas, *Sniffing* passivo.

2.3.1 *Cracking* de senhas

A quebra de senhas (*cracking*) consiste nas técnicas e métodos para se descobrir as senhas que os administradores usam em um sistema alvo a partir dos arquivos onde são registrados ou dos datagramas que as transportam pela rede para que com ela possam liberar o acesso a vários recursos e dados desse sistema.

As técnicas para a quebra de senhas são desenvolvidas a partir de dois métodos genéricos, que são chamados de método de força bruta e o método do dicionário. O método de força bruta consiste em um método de tentativa e erro, pois envolve o teste de todas as combinações possíveis dos caracteres que podem ser usados na senha, até chegar na combinação certa. Este método é pouco eficaz quando se usa senhas com número de caracteres muito grande

ou quando há uma grande variedade de caracteres alfabéticos, numéricos e especiais. O método do dicionário é usado utilizando uma lista previamente elaborada de combinações de caracteres ou palavras, que são testados um a um como possíveis senhas, até que uma dessas combinações produza um resultado positivo. Esse método reduz o número de tentativas possíveis consideravelmente, fazendo com que este método seja mais eficiente que o da força bruta, salvo nos casos onde as senhas são geradas aleatoriamente, não correspondendo palavras de uso comum ou outras combinações conhecidas. Um requisito importante para que esse método se torne mais eficiente é o fato do atacante ter que testar palavras ou combinações que sejam, por alguma razão, relacionadas com o usuário. Então é necessário que para elaborar a lista de tentativas o atacante conheça algumas informações importantes do usuário.

A maioria dos sistemas operacionais atuais usa mecanismos para dificultar bastante a entrada não autorizada em sistemas por tentativas exaustivas de nomes de usuários e senhas. Esses mecanismos podem apresentar níveis variados de sofisticação e eficiência, mas quase sempre envolvem criptografia em algum nível, controle sobre o tempo de validade da senha, bloqueio de acesso após tentativas de login frustradas e críticas e rejeição de senhas óbvias ou demasiadas curtas, chamadas senhas fracas. O mau uso desses recursos ou excessiva confiança neles podem ser considerados como as principais vulnerabilidades dos sistemas a essa técnica.

2.3.2 Varredura de portas

A varredura de portas (*port scanning*) é um método que consiste em testar as portas de um *host*, ou de um grupo de *hosts*, a fim de determinar quais dessas portas estão em condições de aceitar conexões. Geralmente, a varredura de portas é capaz de revelar outras informações importantes, tais como o sistema operacional que está sendo executado, a partir da análise de como o alvo reage aos eventos gerados na varredura.

A varredura de portas é feita através de *softwares* específicos, capazes de enviar pacotes com destino às portas do host alvo, monitorar as respostas emitidas pelo alvo e gerar relatórios de análise.

Essa técnica de ataque se aproveita do fato de que o TCP/IP gerencia as conexões de forma automatizada e com um nível de crítica muito elementar. Na maioria dos casos, um *host*

procura responder a toda e qualquer solicitação de abertura de conexão que é endereçada a suas portas, sem avaliar a origem do pedido. O uso dessas portas conhecidas associadas a serviços padrão é outra característica explorada por essa técnica.

2.3.3 *Sniffing* passivo

Essa técnica consiste na utilização de *Sniffers*, que são componentes de software capazes de capturar os pacotes que trafegam por uma rede. Os *Sniffers* ou farejadores ficam residentes na memória como um cavalo de tróia, analisando todo o tráfego que ali passa. Qualquer entrada ou saída de dados é capturada, seja um servidor FTP, uma página de chat ou um e-mail digitado. O *Sniffer* pega os pacotes recebidos em seu estado bruto e os transforma em texto puro para serem lidos.

A execução dessa técnica necessita de algum tipo de acesso a um host da rede local, para que o *sniffer* seja instalado. Devido a este fato, o *Sniffing* passivo é mais empregado por usuários internos da rede ou por usuários remotos após o prévio comprometimento de um *host* alvo. Apesar dessas dificuldades, essa técnica é muito eficaz e seu emprego pode representar uma ameaça considerável a confidencialidade de informações críticas, como por exemplo, senhas. O emprego de *Sniffers* traz um perigo maior do que uma simples obtenção de informações, fazendo com que os pacotes capturados possam vir a ser alterados e retransmitidos, num procedimento denominado de *Sniffing* ativo (*active sniffing*).

As ferramentas usadas nesta técnica são variadas e de fácil obtenção. A maioria é executada sobre o UNIX ou Windows NT. Boa parte delas são de uso comercial, formando módulos de *software* de gerenciamento ou de análise de tráfego de rede. O *Network Monitor* desenvolvido para o Windows NT, é um bom exemplo disso.

3 RECURSOS DE SEGURANÇA DO WINDOWS 2000

O Microsoft Windows 2000 foi um grande passo dado pela Microsoft na evolução dos seus produtos em relação às versões anteriores, proporcionando um apoio integrado para cliente/servidor e até mesmo para redes. A versão 2000 foi projetada para aumentar a confiança, prover níveis maiores de segurança do sistema e obter uma dimensionalidade de uma rede pequena para uma grande rede entre companhias.

Segundo Cardoso (2001, p.01) deu-se muita atenção a segurança, que agora está totalmente integrada à nova estrutura de diretório do *Active Directory*[2]. Em termos de flexibilidade e redimensionamento, o Windows 2000 foi projetado para ser redimensionado efetivamente do laptop – com suporte total do *Plug and Play*, ACPI (*Advanced Configuration and Power Interface*, interface de configuração avançada e energia) – até servidores e arquiteturas de rede, com suporte para equilíbrio de carga e organização de clusters de carga. Essas mudanças foram baseadas no sucesso do Windows NT, que foi um sistema operacional principalmente voltado para aplicações de *Internet*.

Dentre essas novas melhorias que foram implantadas ou aprimoradas e que vamos abordar estão o *Active Directory*, *Kerberos*, infra-estrutura de chave pública, objetos da diretiva de grupo, protocolo de segurança do protocolo de *Internet* e o sistema de criptografia de arquivos.

3.1 Revisão de segurança do Windows NT

O Windows NT apresenta recursos que facilitam a segurança da rede em vários níveis, permitindo ou não várias ações por partes dos usuários. Por isso a importância de comentarmos

[2] Recurso que fornece um serviço de diretório com uma hierarquia segura distribuída, escalonável e replicada.

sobre esses recursos para podermos entender porque a versão 2000 foi baseada nesta tecnologia NT.

Segurança da rede está sempre ligada a proteção de todos os componentes da *Intranet* contra acesso de usuários não-autenticados, além de garantir a integridade das informações do sistema. O modelo de segurança do Windows NT é formado por controladores de acesso de objetos, como por exemplo, arquivos e impressoras. Esses controladores são responsáveis por quais ações um usuário pode tomar em relação a um objeto.

3.1.1 O modelo de segurança do Windows NT

Uma das bases do modelo de segurança do Windows NT é a noção de contas, onde o sistema permite a criação de contas de usuário, permitindo que elas sejam divididas em quaisquer quantidades e tipos de grupos. Quando o usuário se identifica no sistema, efetua-se o *Login* e o NT cria uma ficha de acesso de segurança, incluindo um identificador de segurança exclusivo, identificadores de segurança para os grupos de usuários dos quais o usuário é membro, e uma lista de permissões destinadas a ele.

Existem alguns componentes básicos da arquitetura que formam o subsistema integral deste modelo de segurança, dentre eles estão:

- *Logon*: os processos de *logon* são componentes que aceitam as solicitações de conexões dos usuários. Um destes processos é o *logon* interativo inicial que exibe uma caixa de diálogo onde geralmente são requisitados o nome de usuário e senha, entretanto o Windows NT permite outros pacotes de identificação tais como *Scanner Retinal* (olhos), digital (dedos), ou até mesmo *Scanner Vocal* (voz);
- LSA (*Local Security Authority*): Componente do modelo de segurança que gera a ficha de acesso do usuário e fornece os serviços de autenticação do mesmo. Além de ser responsável pelo controle de auditoria.

- SRM (*Security Reference Monitor*): verifica os privilégios do usuário com relação a acesso de objetos e execução de qualquer ação do usuário. O SRM atua juntamente com o LSA com relação à validação de acesso e política de geração de auditoria.

3.1.2 Controle de acesso

O Windows NT Server permite o controle dos acessos concedidos ou não de recursos aos usuários e o controle de ações que o usuário pode ou não executar. Contas de usuários, direitos de usuários, grupos de usuários, *subjects* e permissões são os recursos que permitem ou não o acesso a outros recursos.

A conta de usuário é o recurso básico para uma pessoa participar de um domínio e conectar-se a rede utilizando os recursos do mesmo. Essa conta é criada por um administrador, atribuindo um nome de usuário a ela, contendo dados de identificação do usuário e seus privilégios dentro do sistema. Logo o sistema atribui a esta conta criada uma identificação de segurança, o SID (*Security Identifier*). Uma SID é única, ou seja, nunca será atribuída uma mesma SID a diferentes contas.

Os direitos do usuário são as regras impostas pelo administrador que determinam as ações permitidas a ele ou por questão de eficiência, são atribuídos geralmente a grupos. Grupos de usuários é o recurso utilizado para que os administradores agrupem os usuários de acordo com as necessidades dos trabalhos no acesso a rede. O uso deste recurso facilita a concessão de direitos e permissões a diversos usuários, pois quando um usuário é adicionado a um grupo, é concedido a ele automaticamente todos os direitos e permissões concedidos aos usuários do grupo.

Um *Subject* é a combinação da ficha de acesso de um usuário e de um programa que ele esteja executando, evitando que o programa tenha mais acesso a um objeto do que o próprio usuário. As permissões referem-se aos atributos de segurança de um objeto que fornece informações ao sistema, tais como, proprietário do objeto (um grupo ou um usuário), uma lista de acesso e uma lista de acesso para controle de mensagens de auditoria.

3.1.3 Auditoria

A auditoria é um recurso do Windows NT que possui funções básicas de segurança, como reunir informações sobre o uso do sistema, monitoramento de eventos de segurança, detecção de falhas de segurança e localização de danos no sistema.

O Windows NT é capaz de realizar a auditoria do próprio sistema e de eventos relativos a aplicações diversas. A auditoria de cada evento é identificada no seu próprio registro. Alguns dos eventos que podem ser auditados são o gerenciamento de usuários e grupos, processos, *logon* e *logoff*, acesso a arquivos e objetos, alterações na diretiva de segurança, uso de privilégios e o reinício e desligamento do sistema.

3.1.4 Estrutura de domínio

O domínio do Windows NT foi estruturado de maneira a manter uma rede segura para todos os computadores. Ele é definido como uma coleção de computadores com uma autoridade de segurança central, que é chamado de controlador de domínio primário (PDC – *Primary Domain Controller*). Assim, um domínio precisa consistir no mínimo em um PDC e zero ou mais estações de trabalhos ou servidores membros. Nesta estrutura ainda existe o controlador de domínio de *backup* (BDC – *Backup Domain Controller*) que serve para oferecer várias cópias idênticas para o banco de dados chamado de gerenciador de contas de segurança (SAM – *Security Accounts Manager*), que abrange todo o domínio para aumentar a disponibilidade e o serviço de autenticação distribuída a vários servidores.

Um domínio permite que um banco de dados comum de conta de usuário e uma diretiva comum de segurança sejam compartilhados eliminando a necessidade de que cada computador forneça seu próprio serviço de autenticação. Quando o usuário tiver sido autenticado em um domínio usando o serviço de autenticação do PDC ou de um BDC, esse usuário pode acessar os recursos de qualquer lugar dentro do domínio, contanto que tenha as permissões necessárias.

3.2 *Active Directory*

O *Active Directory* é o principal elemento de segurança do sistema, ele fornece um serviço de diretório com uma hierarquia segura distribuída, escalonável e replicada, estando totalmente integrado no Windows 2000. O *Active Directory* vem substituir a área do banco de dados do gerenciador de contas de segurança (SAM) do registro de controladores de domínio como principal repositório de informações do sistema inclusive contas, grupos e senhas de usuários. Este recurso armazena tanto as credenciais dos usuários para dar suporte a autenticação quanto as informações de controle de acesso para dar suporte à autorização para acessar os recursos do sistema.

Com a integração do conceito do DNS (*Domain Name System* – Sistema de nome de domínio) de um espaço de nome com os serviços de diretório do sistema operacional, o *Active Directory* pode ajudar a unificar e gerenciar vários espaços de nomes já existentes, fornecendo um único ponto de administração para todos os recursos. Assim como com o Windows NT, o domínio continua sendo a unidade primária de segurança e administração. No nível hierárquico mais alto, é possível conectar vários domínios a uma estrutura de árvore, enquanto nos níveis mais baixos, é possível estabelecer uma hierarquia de unidades organizacionais (OUs – *Organizational Units*) para refletir a estrutura interna da organização. A estrutura hierárquica resultante forma um espaço de nome servido pelo serviço localizador de DNS. De acordo com Cardoso (2001, p.05) a natureza hierárquica do *Active Directory* permite uma estrutura de diretório apurada que é ideal para a administração descentralizada sem comprometer a segurança, como mostra a Figura 1.

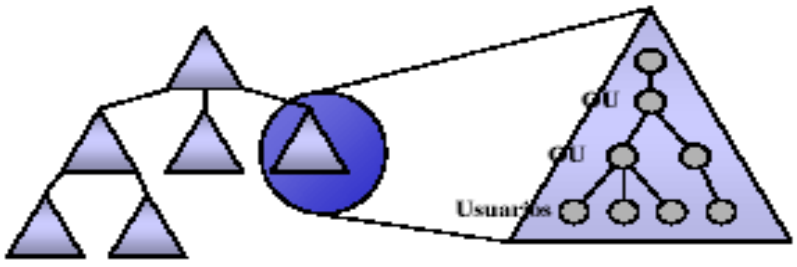

Figura 1: Estrutura hierárquica do *Active Directory*, (BADDINI, 1999).

Dentro do *Active directory* existem as listas de controle de acesso (ACL – *Access Control Lists*) que servem para proteger todos os objetos do mesmo modo que os arquivos e as pastas são protegidas quando se usa o NTFS[3]. As ACLs fazem parte do descritor de segurança do objeto, junto com as informações sobre o nível de auditoria necessário para eventos específicos de acesso de objeto. Uma ACL consiste no número de entradas de controle de acesso (ACEs – *Access Control Entries*). Cada ACE identifica o acesso de um usuário ou grupo em particular para um determinado objeto ou atributos de um objeto em particular.

O *Active Directory* é feito de um ou mais domínios, sendo que cada um deles constitui um limite administrativo e de segurança dentro da rede do Windows 2000. Um domínio pode se expandir além de uma localização física. Cada um deles tem suas próprias diretivas de segurança e configurações, incluindo diretórios administrativos e de usuários. Cada domínio pode vir a ter relações de segurança (confiança) com outros domínios. E, quando vários domínios estão conectados pelas relações de confiança e compartilham um esquema em comum, configuração e catálogo global estes se constituem em uma árvore de domínio.

Sendo assim, podemos dizer que uma árvore de domínio consiste em vários domínios que compartilham o mesmo esquema comum de configuração. Logo, todos os domínios dentro de uma árvore estão ligados pelas relações transitivas de confiança. Segundo Cardoso (2001, p.07) uma hierarquia de domínios permite um melhor tratamento administrativo sem comprometer a segurança.

Uma floresta é um conjunto de uma ou mais árvores que não formam um espaço de nome contíguo. Todas as árvores de uma floresta compartilham um esquema, uma configuração e um catálogo global comuns. Diferentemente de uma árvore, uma floresta não precisa de um nome diferenciado, pois uma organização pode incluir domínios do Windows 2000 com nomes de DNS separados.

Dentro da hierarquia do *Active Directory* existem as unidades organizacionais (OUs – *Organizational Units*), que são contêineres lógicos que existem abaixo do nível do domínio e dentro dos quais é possível colocar usuários, grupos, computadores e outras OUs. Cada domínio pode ter qualquer número de OUs que são organizadas em um espaço de nome hierárquico. Uma estrutura de OU bem definida simplificará em muito o gerenciamento de segurança e delegação

[3] Sistema de arquivos com suporte a criptografia e trabalha com o Windows 2000 utilizando as ACLs.

do controle administrativo, fazendo com que seja possível renomear facilmente as OUs dentro de uma árvore de domínio e também podendo movê-las para um local diferente.

3.2.1 Relacionamento de confiança de domínio

As relações de confiança entre domínios permitem que os usuários com contas definidas em um domínio sejam autenticados pelos servidores em um outro domínio. Diferentemente do Windows NT 4.0, a versão 2000 cria automaticamente a confiança transitiva bidirecional entre domínios à proporção que se adiciona cada domínio à árvore de domínios. Essa confiabilidade é definida com base em uma chave secreta compartilhada por ambos os domínios, que é atualizada regularmente. Quando se cria o primeiro controlador de domínio em um domínio, surge a opção de adicionar este domínio a uma árvore já existente, fazendo com que tal escolha resulte na criação automática de uma relação de confiança pai-filho com o domínio pai especificado. Dessa forma, todos os domínios aceitam implicitamente outros domínios da árvore. Essas relações de confiança são usadas pelo protocolo de autenticação *Kerberos v5* quando os clientes e servidores estão em domínios separados da floresta.

Todas as relações de confiança do Windows 2000, dentro de uma floresta, são por padrão bidirecionais e transitivas, ou seja, se o domínio A tem uma confiança bidirecional com o domínio B e o domínio B tem uma confiança bidirecional com o domínio C, isto significa que o domínio A confia no domínio C, e vice versa.

3.3 *Kerberos*

Kerberos é um protocolo de autenticação que define as interações de segurança entre um cliente, um recurso e um KDC (*Key Distribution Center* – centro de distribuição de chave). O domínio do Windows 2000 se torna equivalente a um reino *Kerberos*, usando o *Active Directory* como banco de dados de contas de usuários (principais) e grupos. O protocolo *Kerberos* está

totalmente integrado à arquitetura de *logon* única do *Winlogon* para fornecer controle de autenticação e acesso.

No Windows 2000, o *Kerberos v5* é o protocolo padrão ou o protocolo primário de autenticação. Esta versão do *Kerberos* é um protocolo padrão da *Internet* que fornece autenticação segura do usuário e de identidades do sistema. O fato de que ele utiliza mecanismos criptografados para decodificar as senhas faz com que ele possa ser usado em redes não-seguras para verificação de identidade das duas partes durante transações na rede. Nos domínios do Windows 2000, essas transações normalmente envolvem pedidos de utilização de serviços de rede pelos clientes, como compartilhamento de arquivos ou de impressão, e também envolve os serviços de rede autenticando esses clientes antes de conceder acesso a eles.

Como o *Kerberos v5* é baseado na implementação de referência *RFC 1510 Kerberos*, o Windows 2000 também opera com outros clientes e servidores do *Kerberos RFC 1510* entre si em alguns cenários e mesmo em equipamentos com sistemas operacionais diferentes do Windows 2000.

3.4 Infra-estrutura de chave pública

A Infra-estrutura de chave pública (PKI – *Public Key Infrastructure*) é um sistema que serve para distribuir e gerenciar as credenciais de usuário de modo seguro em uma organização. A PKI consiste em certificados digitais, ou seja, autorizações certificadas que verificam e autenticam a validade de cada parte envolvida em uma transação eletrônica através de criptografia de chave pública.

O Windows 2000 apresenta as ferramentas necessárias para construir uma PKI ampla baseada em padrões. No centro dessa infra-estrutura está o *Microsoft Certificate Services*, que permite a disposição de autorização de certificado (CAs – *Certificate Authorities*) empresariais para suportar as necessidades de uma organização. As CAs permitem que uma organização estabeleça e garanta a identidade dos portadores de certificados gerenciando a emissão e revogação dos certificados de chave pública X.509[4]. Os serviços de certificados estão integrados

[4] É um modelo de informação.

ao *Active Directory* de uma maneira que usa o serviço de diretório para publicar informações sobre os serviços de certificado, incluindo a localização de certificados de usuários e as listas de revogação de certificados.

É possível usar os GPOs (*Group Policy Objects* – Objetos de Diretiva de Grupo) do Windows 2000 para distribuir automaticamente os certificados em computadores, estabelecer listas de confiança de certificados e identificar autorizações de certificados comuns.

3.4.1 Comunicação segura na *Web*

Toda comunicação baseada na *Web* que utiliza HTTP, Telnet ou FTP através do TCP/IP não é segura porque todas as informações são enviadas como texto sem criptografia. As informações confidenciais ou sensíveis podem ser facilmente interceptadas e lidas. A falta de criptografia inerente é composta pela falta de autenticação do servidor da *Web* ao usar o HTTP padrão, abrindo caminho para a introdução de um servidor trapaceiro da *Web*. Um servidor desses poderia tentar obter de maneira passiva informações de um cliente ou introduzir de maneira ativa um *software* malicioso para o cliente.

Existem vários padrões de comunicação segura que utilizam as tecnologias de chave pública. Dois dos protocolos mais populares, o *Secure Sockets Layer 3.0* (SSL) e o protocolo aberto *Transport Layer Security* (baseado em SSL), são muito utilizados pelas empresas para fornecer canais seguros para comunicação confidenciais na *Web*. As limitações da intensidade da criptografia permitida para exportação são usadas durante a fase inicial de qualquer transação, quando o cliente e o servidor negociam com a força da criptografia que será usada. O servidor decide usar o nível mais forte de criptografia suportado tanto pelo cliente quanto pelo servidor, dessa forma, o nível mais alto de segurança está disponível somente quando o cliente e o servidor suportam a criptografia intensa de exportação controlada.

Para se prevenir contra a ameaça de vírus ou de outro código malicioso contido nos programas cujo *download* é feito através da *Internet*, a Microsoft desenvolveu a tecnologia *Authenticode*, que permite aos desenvolvedores assinarem digitalmente o *software* usando os certificados X.509. Quando o *software* tem assinatura, qualquer modificação invalida a assinatura

digital, já a presença de uma assinatura digital válida assegura que o usuário pode verificar a origem do *software* e se ele não foi alterado desde quando a assinatura foi feita.

As diretivas de grupo de chave pública do Windows 2000 podem ser configuradas para especificar as CAs (*Certificate Authorities*) confiáveis para a empresa na assinatura de código, a fim de que o *download* do *software* de fabricantes que usam os certificados fornecidos por essas CAs possam ser feitos automaticamente sem a consulta ao usuário. O administrador pode configurar o *Internet Explorer* para evitar que os usuários transfiram e excutem software sem assinatura.

3.5 Objetos da diretiva de grupo

No Windows 2000 as diretivas de grupo (*Group Policy*) são usadas principalmente para definir as configurações de sistema e aplicativos para grupos de usuários e computadores sendo definidas como uma propriedade do domínio ou de uma unidade organizacional usando a ferramenta de administração de usuários e computadores do *Active Directory*. A diretiva de grupo define as informações contidas em um GPO (objeto de diretiva de grupo) que está associado a um ou mais objetos do *Active Directory*, como, por exemplo, um *Site*, um domínio ou uma unidade organizacional, permitindo o gerenciamento centralizado ou descentralizado das opções de diretivas. Por padrão, um objeto de diretiva de grupo afetará todos os computadores e usuários no escopo ao qual é aplicado, entretanto, esse comportamento pode ser modificado pela aplicação de filtros, que são as listas de controle de acesso de sistema (SACLs – *System Access Control Lists*), com base na afiliação do usuário ou do computador em um *Security Group* do Windows 2000.

O Editor de diretivas de grupo e suas extensões permitem definir as opções de diretivas para as configurações gerenciadas da área de trabalho para computadores e usuários. Com ele, pode-se especificar as configurações para:

- Diretivas de *software*: é possível usar as diretivas de *software* para administrar as configurações da área de trabalho, incluindo as que afetam os componentes do sistema operacional e aplicativos;

- *Scripts*: possibilita controlar *scripts*, como a inicialização e o desligamento, o *logon* e o *logoff*, através da diretiva de grupo;
- Opções de gerenciamento de *software*: podem controlar quais aplicativos ficam disponíveis para os usuários e quais aparecem na área de trabalho. Os administradores podem instalar, atribuir, publicar, atualizar, reparar e remover o *software* para grupos de usuários e computadores através dessas opções;
- Documentos e configurações de usuários: podem adicionar arquivos, pastas e atalhos para pastas especiais que representam a área de trabalho do usuário. As pastas especiais ficam localizadas nos perfis na pasta *\Documents And Settings*. Essas configurações controlam a capacidade para redirigir a pasta *My Documents* do usuário para um local da rede;
- Configuração de segurança: é possível importar configurações de segurança de um modelo de segurança e aplicá-los automaticamente. O mesmo modelo pode ser usado pelo *Security Configuration Tool Set* para analisar a configuração atual de segurança de um sistema.

O objeto de diretiva de grupo de computadores é aplicado na inicialização do sistema. Já o que afeta os usuários é aplicado quando o usuário efetua o *logon*. A disposição dos aplicativos ocorre somente durante a inicialização do sistema ou quando o usuário efetua o *logon*.

3.6 Segurança de protocolo da *Internet*

O Windows 2000 tem uma implementação do IPSec (Protocolo de segurança da *Internet*) que serve para a segurança avançada de rede, incluindo a integridade, autenticação e confidencialidade dos dados da rede. O IPSec existe abaixo do nível de transporte e, por isso, seus serviços de segurança são transparentemente herdados pelos aplicativos. Esse protocolo é igualmente adequado para a proteção de dados sensíveis que viajam através de seções de uma rede interna, entre clientes e um servidor de aplicativos em particular, ou entre *hosts* (ou *sites*) individuais que formam uma VPN (*Virtual Private Network*, rede privada virtual) através de uma

rede insegura. O *IPSec Policy Agent Service* oferece recursos do IPSec e é responsável pelo gerenciamento da sua diretiva, e pela inicialização do *ISAKMP/Oakley* (IKE) e o *driver* do IPSec.

O Windows 2000 IPSec usa os algoritmos de criptografia e as técnicas de segurança padrão do setor. Segundo Cardoso (2001, p.16) várias empresas que trabalham com as implementações do IPSec testam a capacidade de interoperabilidade em comparação com o padrão para assegurar mais interoperabilidade, através de seus produtos comparados com as tecnologias já existentes de IP proprietário.

O IPSec usa um cabeçalho de identificação (*Authentication Header*) de IP e uma carga útil de segurança encapsulada (*Encapsulated Security Payload*). O cabeçalho de identificação fornece integridade, autenticação de código e função anti-reprodução repetida usando um algoritmo para computar um código de autenticação de mensagem com *Hashing*[5] para cada pacote de IP. A carga útil de segurança encapsulada fornece confidencialidade, além de autenticação e integridade, usando o algoritmo padrão de criptografia de dados (*Data Encryption Standard*) no algoritmo encadeamento de bloco cifrado (*Cipher Block Chaining*), o chamado DES-CBC. O Windows 2000 IPSec implementa o protocolo *Key Exchange* para gerenciar automaticamente as chaves de integridade e criptografia. Os administradores podem escolher entre o cabeçalho de identificação ou a carga útil de segurança encapsulada dependendo do grau de sensibilidade das informações que estão protegendo e a vulnerabilidade relativa da rede.

Uma diretiva IPSec é configurada usando *MMC Snap-In* do *IP Security Policy*. Com o *Snap-In*, é possível criar diretivas de IPSec de maneira centralizada e depois atribuí-las a computadores usando as unidades organizacionais do *Active Directory*. Essas diretivas são construídas em torno do conceito de diretivas de negociação e de filtros IP, e são elas que determinam os serviços de segurança que o administrador deseja incluir. É possível definir vários serviços de segurança para cada diretiva de negociação com o serviço *ISAKMP/Oakley* responsável pela negociação de uma diretiva que ambas as partes da associação de segurança podem aceitar. Os filtros IP determinam que ações sejam realizadas, com base em recursos individuais ou intervalos de recursos e endereço IP de destino, tipo de protocolo e se apropriado, portas de protocolo IP para datagramas IP individuais. Pode-se definir uma diretiva de IPSec para fornecer seus serviços a um datagrama, para que ele fique sem modificações, ou seja descartado.

[5] Mensagem dividida para cada pacote de IP.

3.7 Sistema de criptografia de arquivos

Ao fornecer criptografia de dados no disco usando a criptografia de chave pública, o EFS (*Encrypting File System* – sistema de arquivos com criptografia) incluído no Windows 2000, permite que arquivos e pastas em um sistema de usuários estejam protegidos contra acesso não-autorizado. Este nível de proteção é necessário para prevenir acesso a dados sensíveis quando o Windows 2000 não pode fornecer segurança usando as ACLs NTFS padrão. Esse seria o caso se um disco rígido fosse roubado e colocado em um outro sistema ou se o sistema original fosse inicializado em um disquete que contivesse um sistema operacional alternativo.

O EFS foi projetado para ser de uso simples, possibilitando que um usuário criptografe uma pasta (seu conteúdo atual e futuro) ou um arquivo individual selecionando a opção *Encrypt Contents To Secure Data* da opção propriedades avançadas da pasta ou dos arquivos do *Windows Explorer*.

> *"Se uma pasta ou arquivo estiver marcada como criptografada, todos os arquivos copiados para a pasta ou criados nela serão automaticamente criptografados. Além disso, os arquivos copiados de uma pasta criptografada permanecem criptografados, assim como acontece com os que são arquivados usando um programa de backup do Windows 2000. Os arquivos e pastas copiados para um disquete ou qualquer outro disco não-NTFS perderão a criptografia" (CARDOSO, 2001, p.17).*

A primeira versão do sistema de arquivos com criptografia não suporta o compartilhamento de arquivos entre usuários, mas essa estrutura foi projetada para facilitar essa função em uma versão posterior. Por isso, a versão atual é a melhor para fornecer proteção aos dados sensíveis em computadores móveis de mão, ou aos dados que só são necessários para um único usuário.

A proteção é obtida usando a criptografia de chave pública e aproveita a arquitetura do *CryptoAPI* do Windows 2000. Quando ativado, os arquivos são criptografados com um algoritmo de criptografia simétrica e rápida usando uma FEK (*File Encryption Key* – chave de criptografia de arquivo) gerada aleatoriamente. A versão inicial do sistema de arquivos com criptografia usa o DESX (*Data Encryption Standard* – padrão de criptografia de dados) como

algoritmo de criptografia. A própria chave de criptografia de arquivos gerada aleatoriamente é então criptografada com uma ou mais chaves de criptografia, inclusive a do usuário e a do agente de recuperação de Chave. Como a chave de criptografia de arquivos é totalmente dependente de um par de chaves pública/privada do usuário, o agente de recuperação pode descriptografar o conteúdo do arquivo sem comprometer a chave pública do usuário. O sistema de arquivos com criptografia suporta a criptografia e descriptografia de arquivos armazenados em unidades de disco locais assim como as armazenadas em servidores remotos de arquivos. Ele é bastante integrado com o NTFS, fornecendo um sistema de alto desempenho no qual os usuários não devem notar muita diferença entre a leitura de um arquivo criptografado ou descriptografado.

É possível definir a diretiva de recuperação do sistema de arquivos com criptografia no Windows 2000 aplicada em determinada rede na *Default Domain Policy* do *Active Directory* e definir a diretiva para todos os computadores do domínio, com isso, é possível também definir uma diretiva que cubra as unidades organizacionais individuais. Por padrão, o administrador de domínio controla a diretiva de recuperação do sistema de arquivos com criptografia, podendo delegar esse controle para os administradores de segurança encarregados. Isso fornece a essa rede um alto nível de controle e flexibilidade em relação a quem está autorizado para recuperar os dados criptografados.

4 SEGURANÇA EM REDES WINDOWS

Mesmo com uma melhora significativa da versão 2000 do Windows para as outras versões anteriores, quando se trata de segurança, não adianta um administrador de uma rede implantar este sistema operacional com todos os recursos de segurança bem configurados que com certeza esta rede não estará totalmente segura, com isso é necessário que o administrador da rede tenha conhecimento sobre algumas ferramentas e técnicas que auxiliam a diminuir as vulnerabilidades do sistema. Tendo em vista esta necessidade, trataremos algumas das ferramentas mais conhecidas para que seja definida uma política de segurança.

4.1 *Firewall*

Firewall é qualquer dispositivo utilizado como um mecanismo de controle de acesso de nível de rede para uma rede particular ou um conjunto de redes. Na maioria dos casos, os *firewalls* são utilizados para impedir que pessoas de fora acessem uma rede interna. O *firewall* nasceu como precursor dos roteadores, que são dispositivos de rede que atuam na camada três do modelo OSI, para fazer o encaminhamento de pacotes entre diferentes segmentos de rede. Sendo assim, ele funciona como um roteador que, antes de encaminhar um pacote, verifica uma lista de regras de controle de acesso para validar se o pacote pode ser encaminhado ou não. Segundo Martins (2003, p.235) no caso de conexões à *Internet*, o *firewall* geralmente é instalado atrás do roteador de borda, que protege o *firewall* de eventuais vulnerabilidades que ele possa ter, conforme mostra a Figura 2 o roteador também evita que ele receba um tráfego excessivo, encaminhando para o *firewall* os pacotes destinados à rede interna.

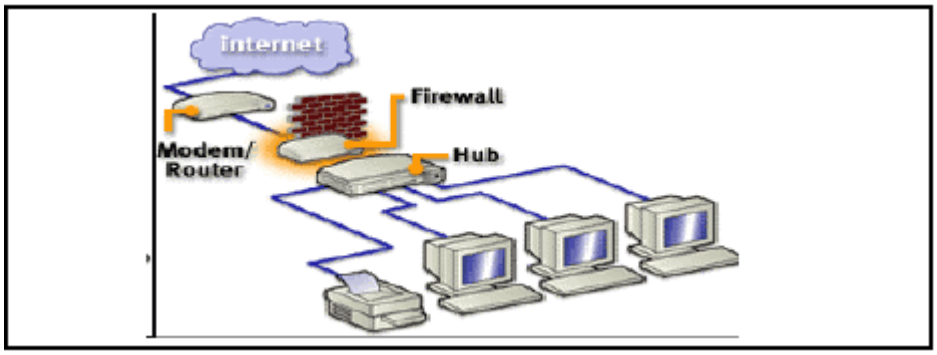

Figura 2: Esquema simplificado de um *firewall* (PELISSARI, 2002, p.27).

Os diversos tipos de *firewall* executam a análise e bloqueio de pacotes com base no modelo de camadas OSI. Quanto mais complexo for, maior será o número de camadas analisadas e, conseqüentemente, maior será o controle sobre o que entra e o que sai da rede. Existem várias técnicas usadas na implementação de *firewalls*, dentre elas estão:

- Filtragem de pacotes: é a técnica mais simples, mas é a menos segura. Simplesmente permite ou não o acesso baseado no endereço de origem/destino ou na porta origem/destino do protocolo de comunicação utilizado. Utiliza-se de uma relação de endereços confiáveis para permitir ou não o acesso. Por filtrar apenas os endereços, está sujeito a ataques *spoofing*. Trabalha na terceira camada do modelo OSI (IP);
- *Stateful Packet Inspection* (inspeção de estado de Pacotes): está técnica é um pouco mais complexa, com isso, possui uma melhor segurança. Permite ou não o acesso, analisando não apenas as informações utilizadas na filtragem de pacotes, mas também analisa o cabeçalho de cada pacote de informação que chega, verificando se pertence a uma conexão interna. Ou seja, se chegar ao *firewall* um pacote que não foi solicitado por algum terminal de dentro da área protegida, o pacote é bloqueado. Trabalha na quarta camada do modelo OSI (TCP);
- *Proxy Firewalls*: é a técnica mais segura, porém é a que mais diminui o desempenho da rede. Nesse tipo de implementação, toda a comunicação é direcionada ao *firewall*. Este, quando recebe uma solicitação de pacote para ser enviada a rede externa, examina suas políticas de segurança. Se o pacote

atendê-las, o *firewall* o envia para o destino, mas, com o seu próprio endereço IP, protegendo o verdadeiro endereço de origem da solicitação. Recebendo um pacote de respostas, ele examina o seu conteúdo e em seguida verifica se o pacote pertence a uma solicitação interna, em caso positivo, será repassado ao solicitante. O *Proxy Firewalls* trabalha na quinta camada do modelo OSI.

Geralmente o *firewall* é instalado entre a rede interna e a *Internet*, mas também pode ser utilizado entre segmentos da rede interna como, por exemplo, entre a rede do departamento financeiro e o resto da rede da empresa. Em ambientes simples somente um filtro já resolve o problema, mas em ambientes mais complexos talvez seja necessário, além de vários firewalls, também alguns servidores *proxy* e topologias de rede mais elaboradas, descritas adiante:

- Redes com DMZ (*Demilitarized Zone*, rede de periferia): é a topologia de rede mais simples, pois o segmento desta rede fica localizado entre a rede externa e a interna, e ficam conectadas através de um *firewall*. Os servidores que são acessados por usuários da rede externa devem ser instalados na DMZ, de modo que possam ser acessados por qualquer usuário interno ou externo. A DMZ pode ser montada de duas formas diferentes, entre dois *firewalls* ou entre o roteador de borda e um *firewall*;
- VPN (*Virtual Private Network*, rede virtual privada): o conceito de VPN é implementar uma rede privada usando a infra-estrutura disponível de uma outra rede não confiável, que geralmente é a *Internet*. Utiliza-se uma rede para transportar os pacotes IP de uma rede até a outra, da mesma forma que a *Ethernet* transporta os pacotes IP do TCP/IP. Este mecanismo é conhecido como tunelamento e os pacotes da rede VPN geralmente são criptografados para prover segurança contra a leitura não autorizada dos dados. Os padrões mais populares atualmente são o IPSec, o PPTP (*Point-to-Point Tunneling Protocol*) da Microsoft e o L2TP (*Layer 2 Tunneling Protocol*). Segundo Martins (2003, p.246) o *firewall* é o dispositivo de rede geralmente utilizado como terminal das conexões VPN e muitos fabricantes já fornecem suas ferramentas com esta capacidade. Na conexão de usuários remotos, é

estabelecido um circuito criptografado entre o computador do usuário remoto e o *firewall*, que fará a autenticação do usuário e permitirá que o mesmo acesse os dispositivos da rede interna, que forem permitidos pelas regras de segurança nele configuradas.

4.1.1 Ferramentas mais utilizadas

Vigliazzi (2002, p.25) afirma que algumas das ferramentas de *firewall* mais utilizadas comercialmente em sistemas operacionais Windows são, o *Firewall-1* (CheckPoint), PIX (CISCO), *Gauntlet* (NAI), *Raptor* (Axent/Symantec), *WatchGuard*, Altavista *Firewall* e o AKER (Nacional).

4.2 *Scanners*

Scanners são *softwares* utilizados para varrer as conexões de redes à procura de possíveis portas abertas ou vulnerabilidades. Estas ferramentas são de extrema utilidade, pois permitem identificar as passagens por onde a segurança de rede ficaria comprometida. Segundo Vigliazzi (2002, p.31) algumas dessas aplicações possibilitam até localizar compartilhamentos de impressoras, pastas, arquivos e unidades de disco com opção de tentativa de conexão.

Existem também os s*canners* de vulnerabilidades que permitem identificar e, muitas vezes, indicar a correção das vulnerabilidades do sistema tendo um papel importante no auxílio da segurança. Vigliazzi (2002, p.31) afirma que em sua utilização, ocorre a simulação de ataques que testam as falhas conhecidas e a reação dos sistemas, e assim, possibilita que as correções sejam efetuadas para melhorar as condições de segurança. Existem dois tipos básicos de *scanners* de vulnerabilidades:

- *Host Scanner*: é utilizado internamente em máquinas locais. Ele testa a máquina onde está sendo utilizado e, em geral, analisa as configurações do sistema operacional e de aplicações;
- *Network Scanner*: é utilizado para analisar máquinas remotas através da rede. Sua função é conectar as portas IP de equipamentos e, a partir do sucesso da conexão, localizar serviços vulneráveis que possam permitir algum tipo de problema de segurança, podendo analisar vários pontos da rede de uma vez.

As principais ferramentas *scanners* que são mais utilizadas no Windows são, o *Internet Security Scanner* (ISS), o *Security Shadow Scanner* e o Retina (e-eye).

4.3 IDS (*Intrusion Detection System*)

O IDS (sistema de detecção de intrusão) é uma ferramenta usada para detectar, notificar e, em alguns casos, prevenir acessos não autorizados a dispositivos de redes. O IDS funciona de forma similar ao *sniffer*[6], capturando e analisando os datagramas que estão trafegando na rede, e procurando identificar evidências de um ataque em andamento.

Algumas versões mais avançadas de IDS são capazes de trabalhar integradas ao *firewall*, atuando de forma ativa na proteção da rede. Com isso, os *firewalls* são capazes de criar regras dinamicamente sempre que notificados sobre um ataque em andamento, por exemplo, se o IDS perceber um ataque de negação de serviço em progresso, ele pode avisar o *firewall* para bloquear qualquer pacote proveniente da origem do ataque.

Existem dois tipos de IDS: o *host-based* (HIDS) e o *network-based* (NIDS). O *host-based* é um tipo de IDS que precisa ser instalado em cada computador da rede que precisar de proteção. Este tipo geralmente trabalha integrado ao sistema operacional, e pode detectar uma grande variedade de tipos de ataques. Já o *network-based* é implementado de forma similar a um analisador de protocolo de rede. Ele monitora todo o tráfego que passa pela rede, procurando identificar padrões conhecidos nos pacotes TCP/IP, ou seja, "assinaturas de ataques", para

[6] Ferramenta capaz de capturar os pacotes que trafegam pela rede.

identificar ataques em progresso. As “assinaturas de ataques” são compostas por seqüências de caracteres, certas características nos cabeçalhos dos datagramas e outras informações pertinentes aos diversos tipos de ataques conhecidos.

As ferramentas de IDS mais conhecidas são, o SNORT e o *RealSecure* (ISS).

4.4 Política de Segurança

Uma política de segurança é um conjunto de regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos. Ela é composta por um documento dividido em duas partes principais: uma com as diretrizes e regras de segurança na organização e outra detalhando como cada medida de segurança é implantada.

A implementação de uma política de segurança baseia-se na aplicação de regras que limitam o acesso a informações e recursos, com base na comparação do seu nível de autorização relativo a esses ativos. Assim, a política de segurança define o que é e o que não é permitido em termos de segurança durante operações de um sistema. É necessário adotar uma forte política de segurança em uma rede para evitar ocorrências de ataques, de modo a proteger as informações, considerando que elas constituem o maior patrimônio da corporação. Em um documento de política, alguns dados devem ser claramente explicados, como por exemplo:

- Relatar o que acontece quando programas e dados não homologados são detectados no ambiente operacional;
- Relacionar os recursos que se quer proteger e que *softwares* são permitidos rodar em quais locais.

4.4.1 Segurança física

A política de segurança física precisa considerar o planejamento das instalações, gerenciamento e procedimentos de recuperação de desastres. O objetivo é garantir a segurança da

infra-estrutura da empresa, deve contemplar a localização dos equipamentos, a construção e o controle de acesso às instalações e planos de contingência.

Devem ser tratados os seguintes aspectos na política de segurança física:

- Política de construção das instalações dos computadores e dos centros de comunicação, onde deve ser considerado como a instalação irá acessar os recursos redundantes e/ou os públicos, além de abordar também os aspectos ambientais;
- Política de controle de acesso às instalações, onde é tratado quem será o responsável por manter a lista de permissões e quem fará as auditorias. Nesta etapa o acesso de visitantes deve ser controlado;
- Política de proteção do lugar e dos equipamentos, onde deve se definir quem a gerência deve acionar nos casos de interrupções de serviços ou vazamento de informações;
- Política de manutenções preventivas, onde devem ser incluídas algumas normas para auditorias periódicas de sistemas e de configurações de rede, de modo a evitar que *hardwares* e *softwares* críticos criem riscos de segurança.

4.4.2 Autenticação e segurança de rede

Martins (2003, p.291) afirma que a segurança de rede diz respeito a qualquer acesso a informação através da rede. O controle básico de acesso é a autenticação, que é a porta da frente para qualquer sistema ou rede onde o solicitante de uma informação ganha direito de acesso com base em suas credenciais. Para definir esta parte da política de segurança é necessário considerar os seguintes aspectos:

- Arquitetura da rede, onde deve indicar o quanto de informação poderá fluir para fora da empresa. As políticas de endereçamento de rede devem

contemplar os tipos de endereços que serão utilizados, como estático ou dinâmico;

- Controle de acesso define como os elementos que permitem o acesso à rede devem ser inseridos nela, como roteadores e *firewalls*;
- *Login* com senhas, onde deve haver um padrão para criação de nomes de usuários, sendo conveniente que o nome identifique a pessoa e não o seu cargo. A política também deve definir o que deve ser feito com os usuários pré-cadastrados nos sistemas e pode usar o registro das tentativas frustradas e bem sucedidas de *login* como uma ferramenta de detecção de intrusão;
- Acesso remoto é um mecanismo que permite aos funcionários, ou a outras pessoas autorizadas, acessarem a rede da empresa. Podem ser definidas algumas políticas para controlar os tipos de equipamentos permitidos no ambiente de trabalho, e como os equipamentos são disponibilizados para os funcionários, além de dizer que o equipamento deve ser usado conforme configurado pela empresa, e o usuário não poderá alterar esta configuração.

4.5 Definindo uma política de segurança

Segundo Vigliazzi (2002, p.70) considerando uma configuração básica de segurança para um servidor Windows 2000 de uma rede *Intranet* será necessário abordar os seguintes pontos ao definir uma política de segurança:

- Verificar que todas as partições do disco estão formatadas com NTFS;
- Verificar se a conta Administrador (administrador) possui senha forte;
- Desativar serviços desnecessários;
- Desativar ou deletar contas desnecessárias;
- Proteger arquivos e diretórios;
- Certificar que a conta *Guest* (convidado) está desativada;
- Proteger o registro de acessos anônimos;

- Aplicar registros adequados às ACLs;
- Restringir o acesso público à informação *Local Security Autority* (LSA);
- Impor políticas de senhas mais fortes;
- Impor Política de bloqueio de contas;
- Configurar a conta Administrador (administrador);
- Remover todos compartilhamentos de arquivos desnecessários;
- Impor ACLs adequadas em todos compartilhamentos de arquivos.

4.5.1 Verificar que todas as partições do disco estão formatadas com NTFS

Partições NTFS oferecem controles de acesso e proteções que não estão disponíveis com os sistemas de arquivos FAT, FAT32 ou FAT32x. Certifique-se que todas as partições no seu servidor estão formatadas usando NTFS. Se necessário, use o utilitário *convert* (conversor) para conversão não destrutiva de suas partições FAT para NTFS.

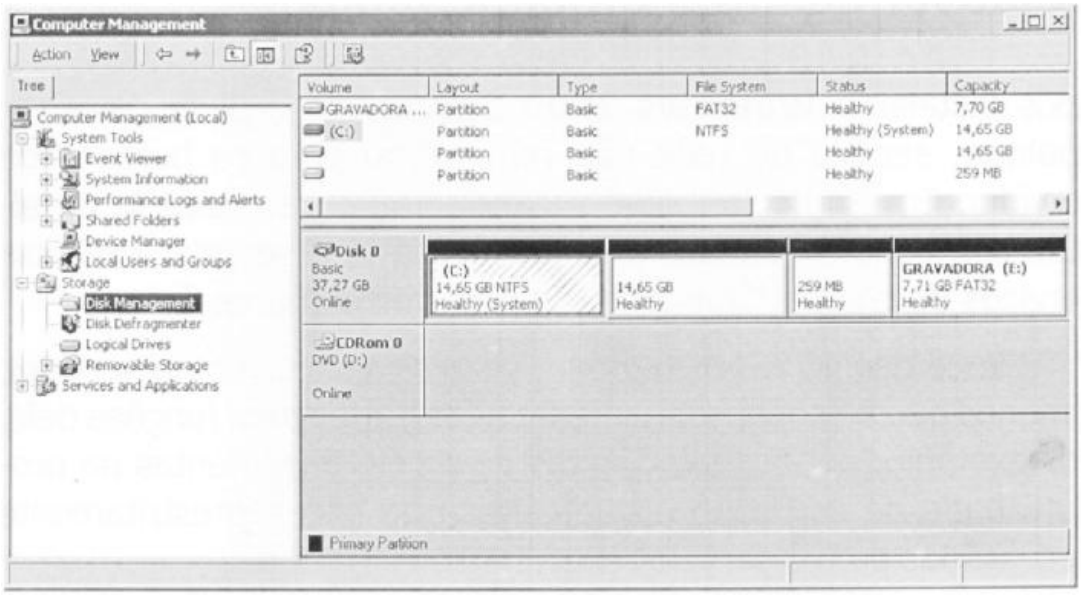

Figura 3: Verificação das partições de disco (VIGLIAZZI, 2002, p.71).

A Figura 3 mostra que através do caminho *Painel de controle\Ferramentas administrativas\Gerenciamento do computador*, selecionando o *Gerenciamento de disco* é possível verificar se as partições estão formatadas com NTFS.

4.5.2 Verificar se a conta Administrador (administrador) possui senha forte

O Windows 2000 permite senhas de até 127 caracteres. Em geral, senhas longas são mais fortes do que as curtas, e senhas com vários tipos de caracteres (letras, números, pontuação e caracteres não imprimíveis ASCII gerados pelo uso das teclas ALT e códigos de três dígitos no teclado numérico) são muito mais fortes do que os alfabéticos ou alfanuméricos apenas. Para a máxima proteção, certifique-se que a senha da conta do Administrador tem no mínimo nove caracteres e que inclui pelo menos um caractere de pontuação ou ASCII nos primeiros sete caracteres.

Em adição, a senha da conta Administrador não deve ser sincronizada através de múltiplos servidores. Senhas diferentes devem ser usadas em cada servidor para aumentar o nível de segurança em um *workgroup* (grupo de trabalho) ou domínio.

4.5.3 Desativar serviços desnecessários

Após instalar o Windows 2000 Server, deve-se desativar qualquer serviço de rede não requisitado. Em particular, deverá considerar a necessidade de algum servidor componente do IIS (*Internet Information Service*), e se é necessário o servidor executar serviços de compartilhamento de arquivos e impressão.

Deve-se também evitar instalar aplicativos no servidor, a menos que sejam absolutamente necessários para funções dele. Por exemplo, não instale clientes de *e-mail*, ferramentas de produtividade de escritório ou utilitários que são estritamente necessários para que o servidor execute suas tarefas.

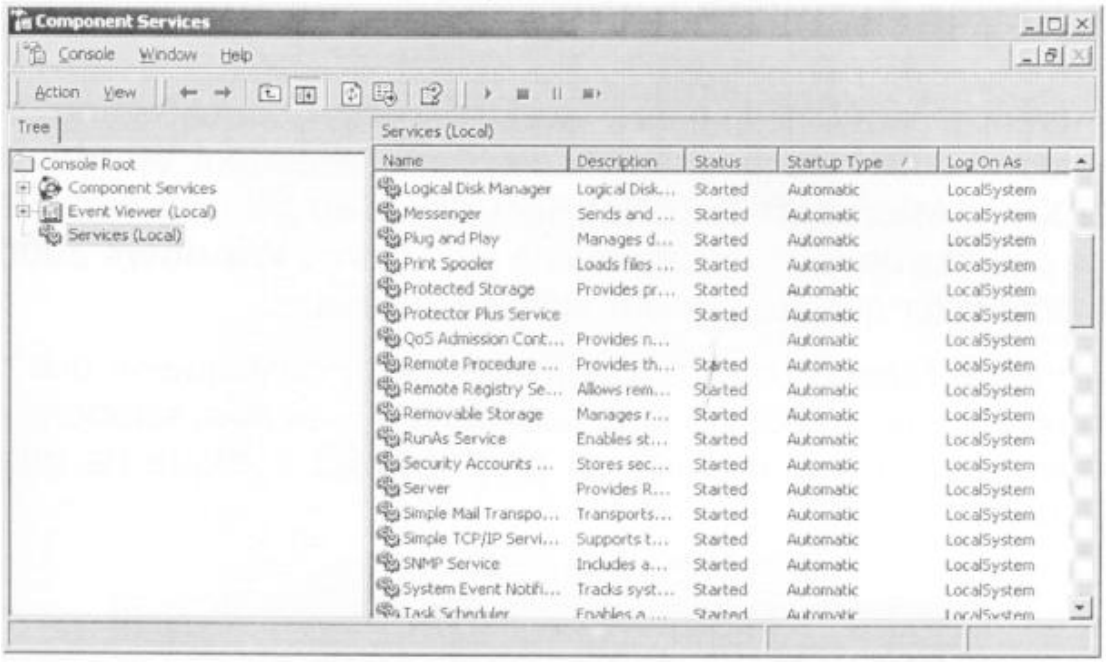

Figura 4: Visualizando serviços desnecessários (VIGLIAZZI, 2002, p.73).

Conforme mostra a Figura 4, através do caminho *Painel de controle\Ferramentas administrativas\Serviços de componente*, pode-se visualizar todos os serviços de rede instalados no sistema, e através dele é possível desativar os que forem desnecessários.

4.5.4 Desativar ou deletar contas desnecessárias

Nesta parte da configuração deve-se rever a lista de contas ativas no sistema através do *Computer Management snap-in*, desativar qualquer conta inativa e deletar contas que não são usadas por um longo tempo.

Figura 5: Desativando ou deletando as contas desnecessárias (VIGLIAZZI, 2002, p.73).

A Figura 5 mostra que através do *Painel de controle\Ferramentas administrativas\Active Directory usuários e computadores*, é possível ter acesso a uma das contas para que se possa fazer as modificações necessárias até mesmo desativá-la.

4.5.5 Proteger arquivos e diretórios

Para fazer a proteção, primeiramente, certifique-se que o arquivo ou pasta está em uma partição NTFS, depois, selecione a pasta ou arquivo, visualize as propriedades conforme mostrado na Figura 6 e clique na guia *Segurança* conforme mostra a Figura 7.

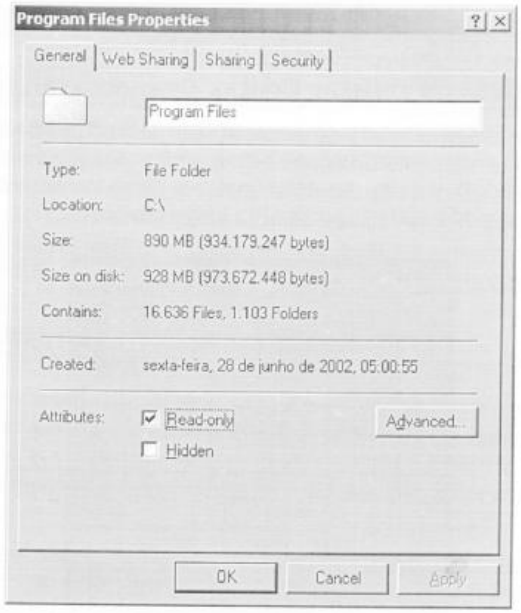

Figura 6: Propriedades de uma pasta ou arquivo (VIGLIAZZI, 2002, p.74).

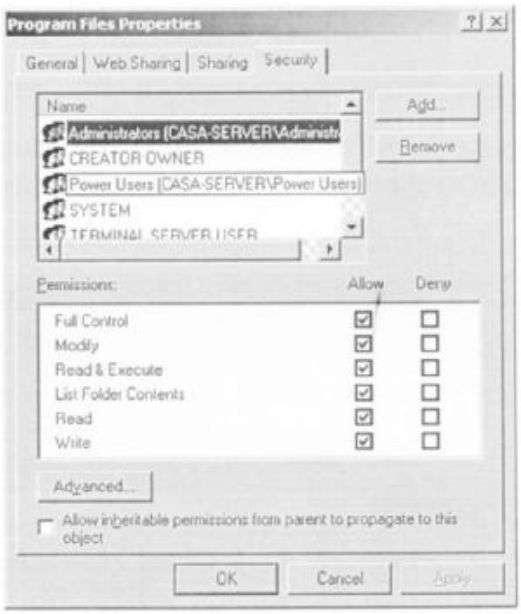

Figura 7: Guia *Security* das Propriedades (VIGLIAZZI, 2002, p.75).

De acordo com a Figura 7, clique em *Avançado* e atribua permissões necessárias aos usuários e grupos, como mostrado na Figura 8:

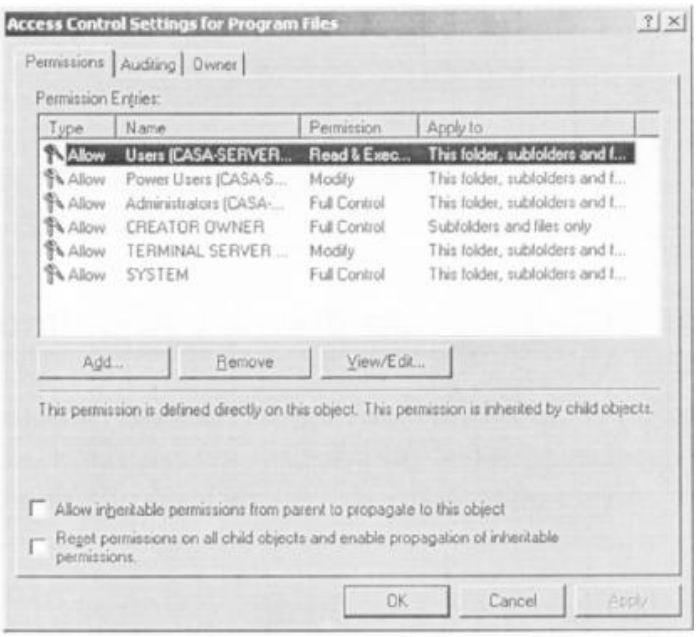

Figura 8: *Advanced* da guia *Security* (VIGLIAZZI, 2002, p.75).

Na seção seguinte trataremos como desativar a conta convidado.

4.5.6 Certificar que a conta *Guest* (convidado) está desativada

Por padrão, a conta *Guest* está desativada em sistemas executando Windows 2000 Server. Mas se caso a conta *Guest* estiver ativada, desative-a. Para isso siga os passos apresentados na seção 4.5.4.

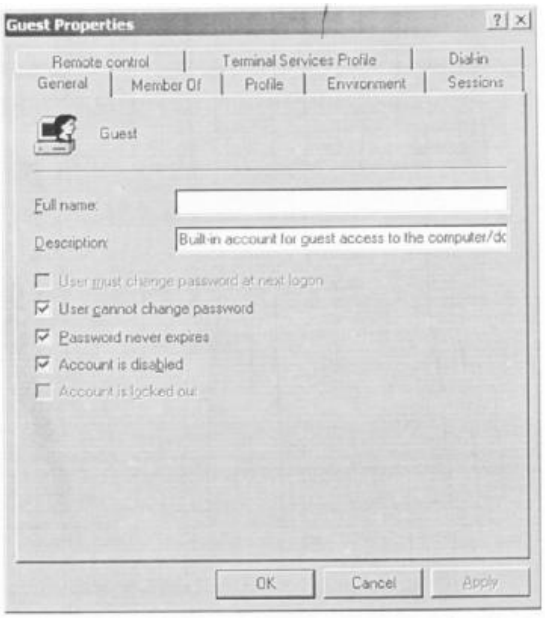

Figura 9: Propriedades *Guest* (VIGLIAZZI, 2002, p.76).

4.5.7 Proteger o registro de acessos anônimos

As permissões-padrão não restringem o acesso remoto ao registro, porém apenas administradores devem possuir tal acesso. Segundo Vigliazzi (2002, p.76) para restringir o acesso ao registro através da rede proceda da seguinte maneira:

1. Adicione a seguinte chave:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\SecurePipeServers
Value Name	\winreg

2. Selecione *winreg*, clique no menu *Segurança* e, então, clique *Permissões*.
3. Coloque a permissão do Administrador para *Full Control*, certifique-se de que nenhum outro usuário ou grupo é listado e, então, clique em *OK*.

A permissão de segurança (ACLs) aplicada nesta chave define quais usuários ou grupos podem se conectar remotamente ao registro do sistema. Em adição, a sub-chave

AllowedPaths contém a lista de todas as chaves para as quais os membros do grupo *Everyone* têm acesso, não constando as ACLs na chave do *winreg*. Isto permite funções específicas do sistema, como verificar o status da impressora.

4.5.8 Aplicar registros adequados às ACLs

Consulte "*Default Access Control Settings*" (ajustes do controle de acesso) da opção no documento original do Windows 2000 no *Web site* da *Microsoft TechNet Security* para detalhes no registro de ACLs e como fazer as modificações necessárias.

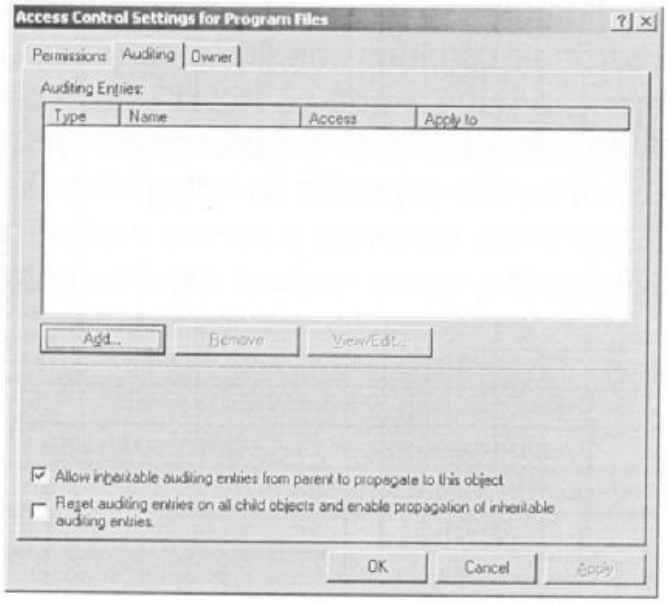

Figura 10: Ajustes do controle de acesso (VIGLIAZZI, 2002, p.77).

A Figura 10 mostra a guia *Auditoria* da guia *Segurança* das propriedades de alguma pasta ou arquivo.

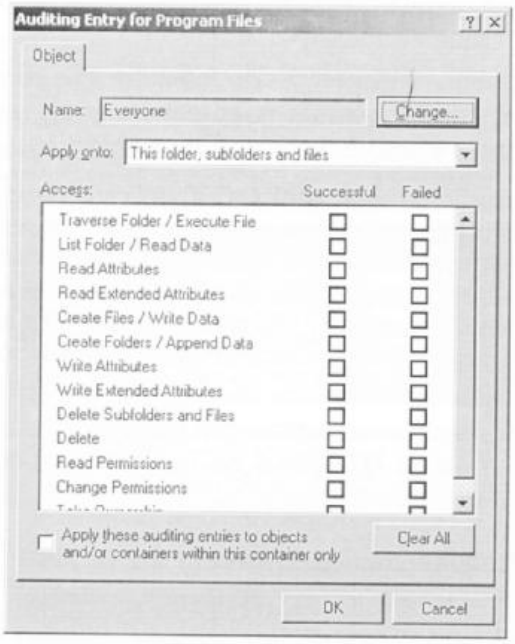

Figura 11: Modificando as ACLs (VIGLIAZZI, 2002, p.78).

A Figura 11 mostra que adicionando uma condição na tela anterior aparecerá a janela onde é feito as modificações para as ACLs.

4.5.9 Restringir o acesso público à informação *Local Security Autority* (LSA)

Nesta parte da configuração é necessário identificar todos os usuários do sistema, assim, deve-se restringir usuários anônimos de modo que a quantidade de informação pública que pode ser obtida de um componente de LSA do subsistema da segurança de Windows NT seja reduzida. O LSA mantém aspectos da administração da segurança no computador local, incluindo o acesso e as permissões. Para executar esta limitação, crie e ajuste a seguinte entrada do registro:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\LSA
Value Name	RestrictAnonymous
Type	REG_DWORD
Value	1

4.5.10 Impor políticas de senhas mais fortes

Trate a string utilizada em senhas com a política de segurança do domínio (ou a política local de segurança) *snap-in* para melhorar sua performance. Por isso faça as seguintes mudanças:

- Ajuste o comprimento mínimo da senha a oito caracteres;
- Ajuste uma idade mínima da senha apropriada à rede (tipicamente de um a sete dias);
- Ajuste uma idade máxima da senha apropriada à rede (tipicamente até de trinta dias);
- Ajuste uma manutenção do histórico da senha usando a opção *Remember passwords*, este histórico deve conter no mínimo seis senhas memorizadas.

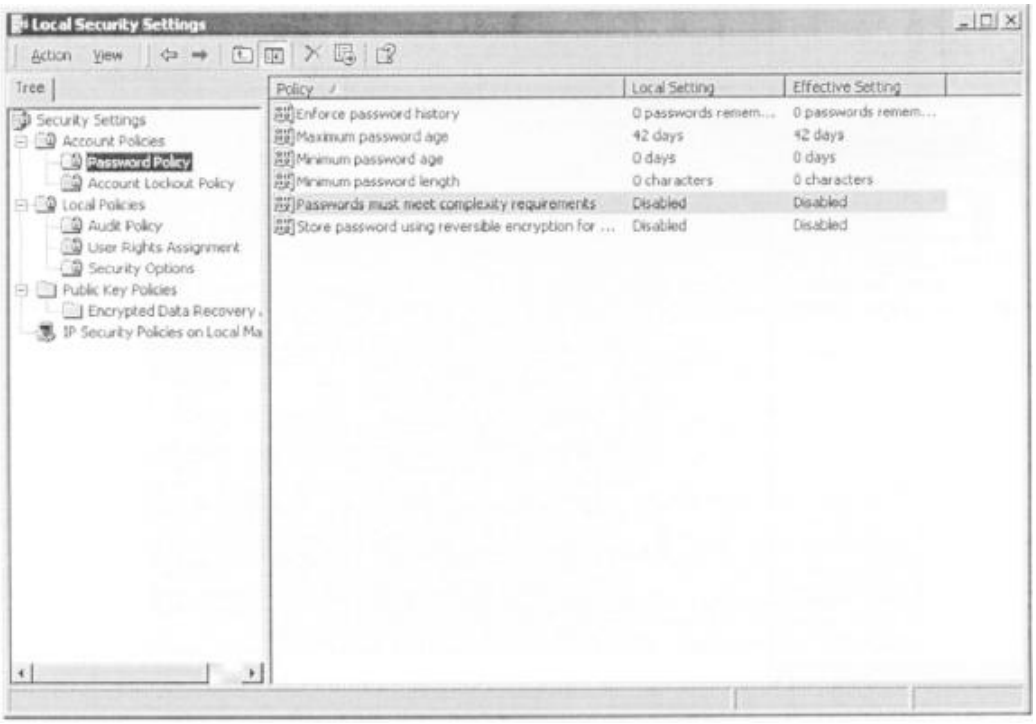

Figura 12: Impondo políticas de senhas fortes (VIGLIAZZI, 2002, p.79).

A Figura 12 mostra que através de *Painel de controle\Ferramentas administrativas\Diretiva de segurança local*, selecionando a ferramenta *Diretivas de senha* é possível tratar as configurações de senha.

4.5.11 Impor política de bloqueio de contas

O Windows 2000 possui um recurso que bloqueia a conta após um número, especificado pelo administrador, de falhas do *logon*. Para a máxima segurança, configure o bloqueio para três a cinco tentativas falhas, reiniciando a contagem após trinta minutos no mínimo, e ajuste a duração do bloqueio com a opção "para sempre (até que o *ADMIN* destrave)".

O Windows NT Server Resource Kit inclui uma ferramenta que permite o ajuste de algumas propriedades da conta que não são acessíveis através das ferramentas de gerência normais. Esta ferramenta, o *passprop.exe*, permite, por exemplo, que o administrador seja impedido de acessar remotamente o sistema:

- O *switch* do *adminlockout* permite que a conta do administrador seja travada para acesso externo.

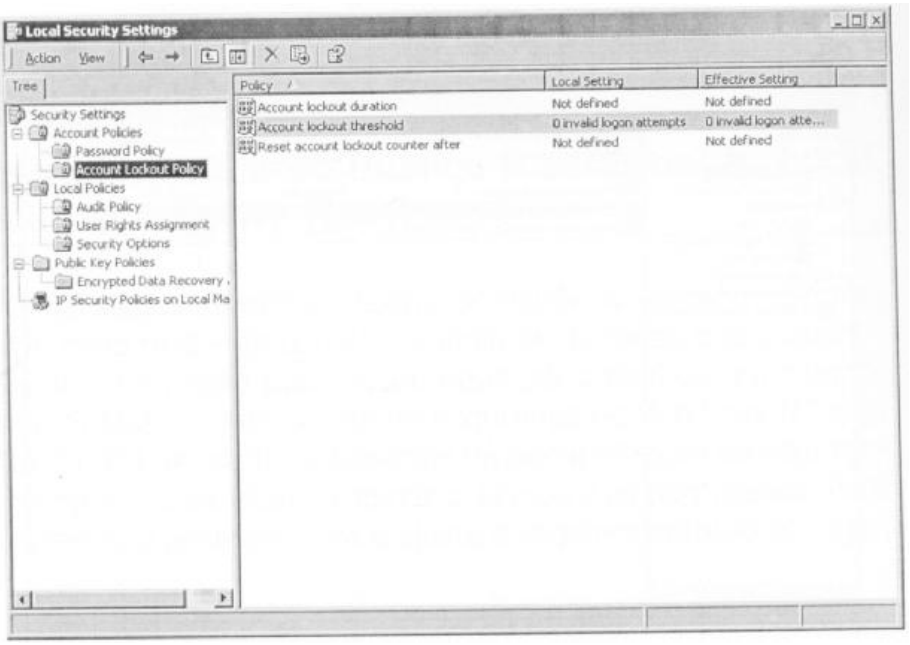

Figura 13: Impondo a política de bloqueio de contas (VIGLIAZZI, 2002, p.80).

A Figura 13 mostra que através do *Painel de controle\Ferramentas administrativas\Diretiva de segurança local*, selecionando a ferramenta *Diretiva de bloqueio de conta* pode-se fazer as configurações de bloqueio de conta.

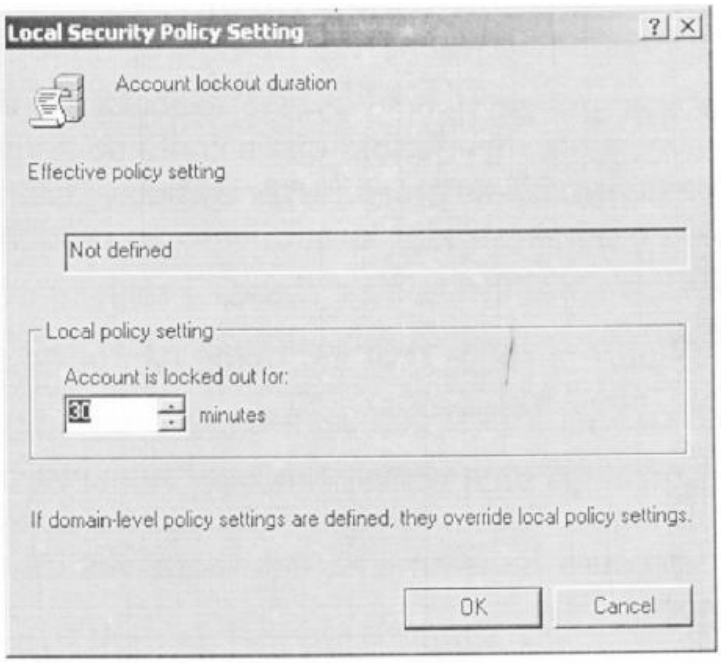

Figura 14: Duração de bloqueio (VIGLIAZZI, 2002, p.81).

A Figura 14 mostra a janela de propriedades do serviço de duração de bloqueio de conta, onde pode se definir o tempo que a conta estará desativada.

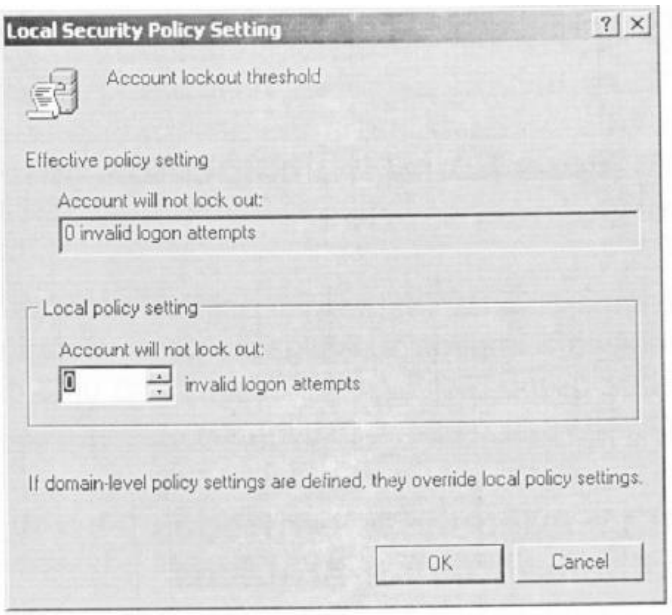

Figura 15: Tentativas de *logon* (VIGLIAZZI, 2002, p.81).

A Figura 15 mostra a janela de propriedades do número de tentativas de *logon*.

Na seção seguinte trataremos a configuração da conta Administrador.

4.5.12 Configurar a conta Administrador (administrador)

Quem vai atacar um servidor que está executando Windows 2000, provavelmente, deve saber que a conta do administrador foi construída dentro dele. Para dificultar o ataque, é necessário que, tanto para o administrador local quanto ao de domínio, façam o seguinte em cada servidor:

- Rebatize a conta com um nome não óbvio;
- Estabeleça uma conta nomeada *"Administrator"* sem privilégios. Faça a varredura do registro do evento que procura regularmente nas tentativas de usar este cliente;
- Permita o bloqueio das contas reais e do *Administrator* usando o utilitário do *passprop*;
- Desabilite a conta do administrador do computador local.

4.5.13 Remover todos compartilhamentos de arquivos desnecessários

Todos os compartilhamentos desnecessários no sistema devem ser removidos para impedir a divulgação possível da informação e também que usuários maliciosos usem como uma entrada ao sistema local.

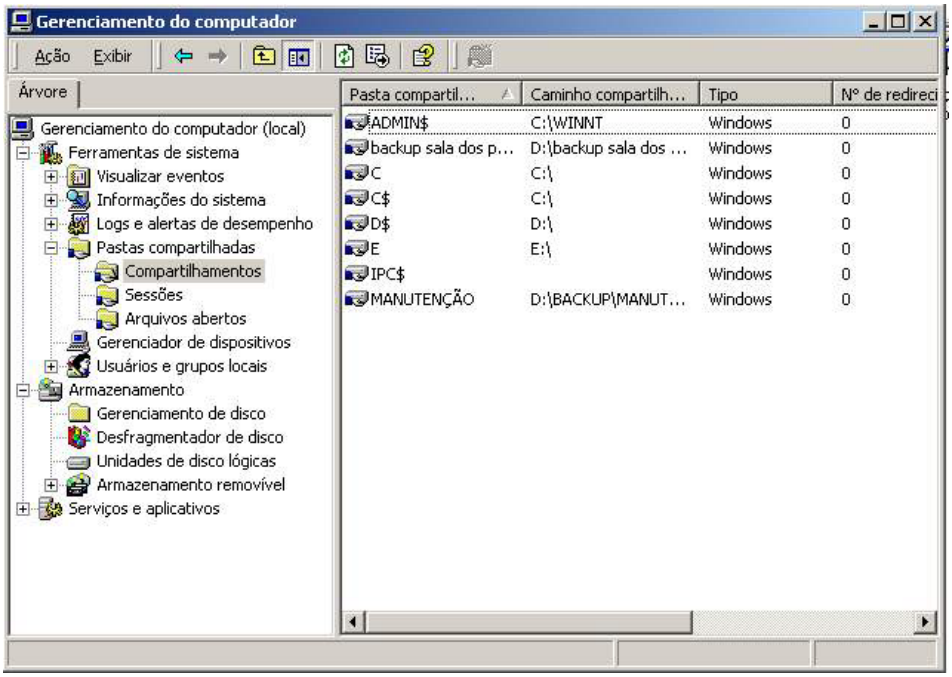

Figura 16: Visualizando os compartilhamentos

A Figura 16 mostra que através do caminho *Painel de controle\Ferramentas administrativas\Gerenciamento do computador*, selecionando a *Pastas compartilhadas\Compartilhamentos*, é possível visualizar todos compartilhamentos para poder desativá-los se não forem necessários.

4.5.14 Impor ACLs adequadas em todos compartilhamentos de arquivos

Pelo padrão, todos os usuários têm permissões *Full Control* em compartilhamentos recentemente criados. Todas as partes que são requeridas no sistema devem ser ACLs, tais que os

usuários têm o acesso em nível de compartilhamento apropriado. Saiba qual arquivo NTFS que deve ser usado para ajustar ACLs em arquivos individuais, além das permissões a nível de compartilhamento.

Além de todos esses passos de configuração existem mais três passos que são importantes para a manutenção da segurança do sistema:

- Instalar softwares antivírus e atualizações: como o Windows 2000 é muito vulnerável aos vários vírus de computadores que existem é necessário que seja instalado um *software* de antivírus e que esteja periodicamente atualizado nas assinaturas dos vírus em todos os sistemas *Internet* e *Intranet*;
- Instalar o último *Service Pack*: cada *Service Pack* para Windows inclui todos os reparos da segurança dos anteriores. É necessário que o sistema esteja atualizado nas liberações do *Service Pack* e que seja instalado corretamente nos servidores;
- Instalar os *Hotfixes* de segurança: a Microsoft emite boletins com seu serviço de notificação da segurança. Quando estes boletins recomendam a instalação de um *Hotfixes* da segurança, é necessário fazer imediatamente o *download* e a instalação correta nos servidores.

4.6 Configuração de uma ferramenta de segurança

Para aumentar o nível de segurança na política que foi definida é necessário instalar um firewall que esteja bem configurado além de outras ferramentas que possam auxiliar o sistema. Com isso será mostrado a configuração de uma ferramenta, que é muito usada em servidores Windows, chamada de *RealSecure Guard*.

O *RealSecure Guard* é uma ferramenta de detecção de intrusão, que auxilia muito para diminuir as vulnerabilidades do sistema. Essa ferramenta é implantada entre a conexão com a *Internet* e com a rede interna.

Quando os pacotes são enviados para qualquer máquina que compõe a rede, eles passam pelo RealSecure Guard, que analisa e verifica se há alguma tentativa de intrusão. Esta técnica é utilizada com o auxílio de um protocolo de tecnologia de análise chamado BlackICE que é instalado junto com a ferramenta.

O RealSecure Guard responde ao tráfego de três formas diferentes:

- Quando os pacotes que passam pelo RealSecure Guard estiverem seguros, são repassados para a rede normalmente até o endereço de destino de cada um;
- Se for detectado uma intrusão, mas que não seja uma ameaça imediata, são gerado *logs* de eventos que são enviados para o ICEcap manager. Depois o pacote é enviado para a rede.
- Se for detectado uma ameaça imediata em algum dos pacotes, o RealSecure Guard bloqueia tudo que for transmitido pelo intruso e deixa o resto do tráfego normal passar para a rede.

Com tudo isso que foi definido será mostrado uma configuração mínima sobre esta ferramenta.

4.6.1 Configurando a aba detecção de intrusão

A Figura 17 mostra a aba de detecção de intrusão a qual permite controlar que o endereço IP ou eventos do protocolo BlackICE seja confiável ou ignorado.

Figura 17: A aba Intrusion Detection

4.6.2 *Intrusion Detection Settings*

Setting	**Descrição**
Intruder IP	Lista os endereços que são confiados ou ignorados. Se um evento é ignorado para todos os sistemas é exibido na coluna "Tudo".
Intruder	Lista o nome da máquina do sistema ao endereço IP.
Event Name	Lista os eventos que são digitados para ignorar. Se algum endereço IP e completamente confiado, a coluna exibe "Tudo".
Event ID	Lista o número de identificação interna do BlackICE para os eventos ignorados.

4.6.3 Comandos

Comandos	**Descrição**
Add	Será exibido uma caixa de diálogo onde é possível adicionar novos endereços confiados ou pode ignorar eventos
Delete	Selecione uma entrada para ser removido e *click* Delete.

Modify	Selecione uma entrada para mudar e *click* Modify.

4.6.4 Excluindo da *Reporting Dialog Box*

Esta caixa de diálogo (Figura 18) aparece quando alguém clicar os botões *Add* ou *Modify* da aba *Intrusion Detection*. Use esta caixa para criar ou mudar um endereço confiado ou ignorado.

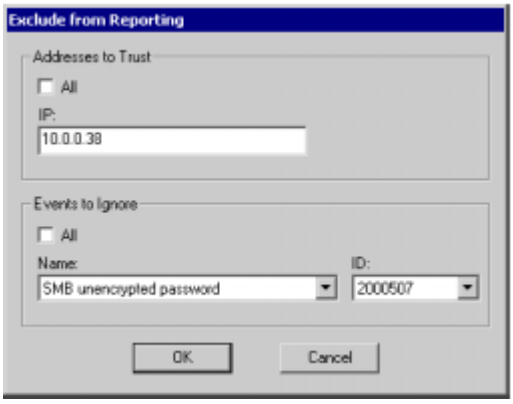

Figura 18: Excluindo da caixa de dialogo *Reporting.*

4.6.5 Endereços Confiáveis

Item	**Descrição**
All	Ignora um tipo de evento do endereço IP que é selecionado nessa mesma caixa. Quando a caixa é aberta é necessário selecionar o tipo de evento que será ignorado na caixa Nome. Não é recomendado deixar todos os endereços confiáveis, pois o sistema ficaria totalmente vulnerável.
IP	O IP tem que ser selecionado para que seja ignorado. Esta caixa é inválida se todos os endereços tiverem sido selecionados.
Add Firewall Entry	Selecione esta caixa no *Accept* para adicionar um IP que foi selecionado para BlackICE Firewall.

4.6.6 Eventos ignorados

Item	Descrição
All	Ignorar todos os ataques que se dirigem para um IP específico.
Name	Listar todas as assinaturas que o BlackICE pode identificar para ignorar um evento especifico.
ID	Esta caixa de seleção lista todas as assinaturas do BlackICE através da assinatura ID.

4.6.7 Como adicionar endereços confiados

1. Vá para *BlackICE Local Console Menu Bar*, selecione ferramentas, e depois *Edit BlackICE Settings*.
2. Selecione a aba *Detection* na janela *BlackICE Settings*.
3. Coloque o endereço confiado na nova lista, e clique *Add*. A caixa de diálogo *Exclude from Reporting* aparecerá conforme apresentado na Figura 19.

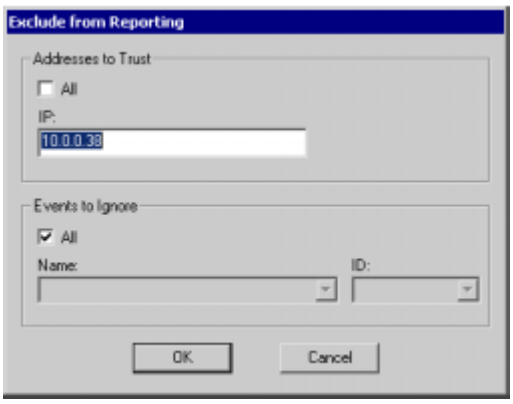

Figura 19: Use esta caixa de diálogo para adicionar endereços confiáveis ou ignorar assinaturas.

4. Entre com o IP que será dirigido para caixa de IP onde ele será confiado pelo sistema.
5. Adicione no *Accept* a entrada para que o IP se vá para o BlackICE Firewall, isto ensina o BlackICE a confiar neste IP permitindo todas as comunicações com o endereço selecionado.

6. Clique no *Add* para que o novo endereço confiado seja acrescentado na aba *Intrusion Detection*.

4.6.8 Como adicionar um evento ignorado

1. Vá para *BlackICE Local Console Menu Bar*, selecione ferramentas, e depois *Edit BlackICE Settings*.
2. Selecione a aba *Intrusion Detection* na janela *BlackICE Settings*.
3. Coloque uma assinatura ignorada na nova lista, e clique Add. A caixa de diálogo *Exclude from Reporting* aparecerá conforme apresentado na Figura 20.

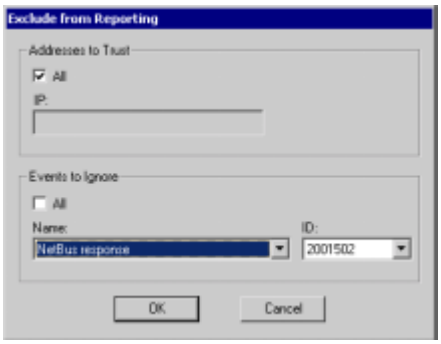

Figura 20: A janela *Exclude from Reporting*.

4. Ensinar o BlackICE a ignorar todos os eventos futuros da assinatura ignorada, siga esses passos:
    - Na seção dos endereços confiados, selecione *All* para ignorar um tipo de evento de um endereço IP;
    - Na caixa de seleção do Nome que lista todas assinaturas para que o BlackICE possa identificar, selecione o tipo de evento que será ignorado ou selecione o número ID na caixa de seleção.
5. Clique no *Add* para que o novo endereço confiado seja acrescentado na aba *Intrusion Detection*.

5 CONCLUSÃO

A criação do Windows 2000 foi uma melhora significativa dos produtos da Microsoft, pois essa versão se mostrou muito mais estável do que as outras, principalmente quando se trata da segurança em redes. Mesmo com muitas pessoas não acreditando que o Windows 2000 seja um sistema confiável, ele pode se tornar uma poderosa arma contra os ataques que ocorrem no mundo virtual, mas para isso ele tem que estar atualizado e bem configurado. Ainda é essencial evitar a ativação de serviços desprotegidos e desnecessários, para isso utilizando uma política de segurança que dita as regras e configurações do sistema tornando a rede menos vulnerável.

Existe ainda outro fator que é de extrema importância quando "falamos" em segurança, que é o homem. Devido ao fato do homem estar em constante interação com o computador, este pode provocar situações de insegurança em um sistema tido como seguro. Alem disso, é preciso conciliar a adequada configuração do sistema junto com a instalação de ferramentas que visam reduzir as vulnerabilidades do Windows 2000, sendo necessário manter as ferramentas de segurança e os *softwares* sempre atualizados buscando minimizar as vulnerabilidades existentes.

O trabalho teve como intuito mostrar os recursos que o Windows 2000 traz, possibilitando ao administrador da rede uma melhor confiabilidade no sistema. O mesmo apresenta ainda algumas ferramentas que auxiliam a prover a segurança de uma rede de computadores junto com uma política de segurança para ditar as regras do que é permitido e proibido dentro da rede.

6 BIBLIOGRAFIAS

BADDINI, Francisco. ***Considerações sobre o design e a implantação do Active Directory***. Disponível em <http://www.w2k.com.br/images/curso /implantacadoActiveDirectory/AD_Design.htm>. Acesso em 20 out. 2004.

CARDOSO, André L. ***Segurança para Microsoft Windows 2000*: O guia de referência técnica**. Rio de Janeiro: Campus, 2001.

MARQUES, Alexandre Fernandez. ***Segurança em redes IP***. Disponível por www em http://www.modulo.com.br.

MARTINS, José Carlos C. ***Gestão de projetos de segurança da informação***. Rio de Janeiro: Brasport, 2002.

PELISSARI, Fernando Antonio B. ***Segurança de redes e análise sobre a conscientização das empresas da cidade de Bauru (SP) quanto ao problema***. 112f. Monografia – Curso de Especialização em Informática, UNESP, Bauru, 2002.

DEERING, S.; HINDEN, R. ***Kerberos versão5***. Disponível em <http://www.ietf.org/rfc/rfc1510.txt?number=1510>. Acesso em 15 out. 2004.

VIGLIAZZI, Douglas. ***Soluções para segurança de redes Windows***. Florianópolis: Visual Books, 2002.