Configuração de Segurança em Servidores IIS

Guia do Administrador

SCUA Information Security Ltda.

SCUA Information Security Ltda.
Rua Líbero Badaró, 158 – 3º andar
São Paulo, SP, 01008-904
Telefone : +55 11 3292-6255
Fax: +55 11 3105-4769
webmaster@scua.com.br
www.scua.com.br

Sumário

Capítulo 1

Introdução

O Internet Information Server fornece serviços essenciais de Internet. A versão 4.0 inclui os seguintes serviços fundamentais: World Wide Web, FTP e Gopher. Já a versão 5.0 que acompanha o Windows 2000 fornece os serviços de World Wide Web, FTP, SMTP e NNTP. Além de prover esses serviços, ele também possibilita administrar remotamente o próprio IIS e o sistema operacional através do navegador web.

A instalação do IIS deve ser feita apenas depois de um cuidadoso planejamento e preparação. Além disso, o IIS deve ser instalado apenas em uma máquina dedicada e nunca em um controlador de domínio. A seguir estão relacionadas as configurações do IIS recomendadas para fornecer um nível de segurança adequado a um servidor Web.

O objetivo deste curso é fornecer aos alunos o conhecimento e as habilidades de que necessitam para configurar servidores web rodando as versões 4.0 e 5.0 do Internet Information Server de forma segura.

Pré-requisitos

Este curso requer que os alunos tenham a seguinte base para compreender os conceitos e tarefas apresentados:

- Conhecimento dos componentes básicos de hardware, incluindo memória de computador, discos rígidos, unidade central de processamento (CPU, Central Process Unit), portas de comunicação e de impressão, adaptadores de vídeo e dispositivos apontadores.
- Conhecimento dos principais conceitos de rede, incluindo cliente, servidor, rede local (LAN, Local Area Network), placa de adaptador de rede, driver, protocolo e sistema operacional de rede.
- Conhecimento do funcionamento da interface Windows NT 4.0 ou Windows 2000;
- Experiência na administração e suporte a servidores Windows NT 4.0 ou Windows 2000;
- Noções de instalação e administração do Internet Information Server 4.0 e 5.0.

Recomendações de Segurança

A segurança da informação é feita através de políticas e sistemas de controle. As políticas de segurança devem ser definadas e documentadas antes que os sistemas possam ser configurados de modo que se possa alcançar a melhor segurança possível.

Política de Segurança Corporativa

Uma política de segurança corporativa não só encorpora as necessidades de segurança da corporação, mas também define a forma como a corporação trata e reage a ataques aos seus recursos. Baseado nesta política, é preciso responder a várias perguntas, tais como:

Como reagir a uma invasão?

Onde os backups estão armazenados?

Quem tem permissão de acessar o servidor?

Boas fontes de informação sobre política de segurança podem ser encontradas em SANS Institute (http://www.sans.org) e Baseline Software, Inc. (http://www.baselinesoft.com).

O capítulo sobre segurança do Resource Kit do IIS aborda muitos aspectos de segurança do Windows NT/2000 e do IIS.

Serviço de Notificação de Segurança da Microsoft

O “Security Notification Service” é um serviço de notificação de e-mail gratuito que a Microsoft usa para enviar aos assinantes informações sobre a segurança dos produtos Microsoft.

O objetivo deste serviço é fornecer aos clientes informações precisas que eles possam usar para se informar e se proteger de ataques maliciosos. A equipe de segurança da Microsoft investiga os assuntos informados diretamente a ela, como também assuntos discutidos em certos newsgroups de segurança populares. Quando os boletins são publicados, eles contém informações sobre qual é o assunto, que produtos são afetados, como se proteger, o que a Microsoft planeja fazer para resolver o problema, e faz referência a outras fontes de informação sobre o assunto.

Para receber essas informações da Microsoft via e-mail, acesse http://www.microsoft.com/technet/security/bulletin/notify.asp.

Capítulo 2

Técnicas de Ataque: Conceitos

Existem vários sites de empresas de segurança que divulgam de forma aberta detalhes sobre técnicas de invasão e ataques. Alguns profissionais de segurança criticam tais sites, pois entendem que os mesmos estão divulgando informações que acabam ajudando os hackers. Os divulgadores destas informações, por sua vez, argumentam que para um profissional de segurança aprender a se defender precisa conhecer em detalhes como o ataque é feito, e é por isto que a informação deve ser divulgada. Além disso, argumentam eles, a comunidade hacker já dispõem destas informações e muitas outras. Portanto, divulgar ataques já conhecidos não irá agregar nenhum conhecimento para os hackers, e não aumentará o risco de invasões.

Apesar desta lógica fazer sentido, a NetSec não se sente à vontade em divulgar "detalhes" de como são feitos os ataques (full disclosure). Portanto, neste site você não encontrará nenhuma receita de bolo para invadir ou atacar sites via Internet.

Prefirimos utilizar o nosso espaço de tecnologia para apresentar os conceitos que servem de base para os ataques. Ou seja, quais são as fragilidades que os ataques exploram? Porque isto acontece?

Desta forma esperamos poder ajudar os responsáveis pela segurança internet a compreender melhor as ameaças, e assim poder defender melhor as suas empresas.

Buffer OverFlow

Falha de programação que faz com que haja um “transbordamento” da área de memória de uma determinada variável sobre a área reservada para outras variáveis, ou sobre a área de memória que contém código executável.

Conseqüência: Softwares podem ser derrubados ou forçados a executar outras funções (código arbitrário).

Abrangência: Atinge todos os tipos de software, sistemas operacionais, Serviços (ex: Web Servers), aplicativos (scripts CGI).

Como os hackers exploram esta vulnerabilidade: Hackers técnicos desenvolvem programas para explorar um buffer overflow (exploits) em um determinado software/versão.

Estes programas são extremamente sofisticados, exigindo que se "mescle" em tempo de execução dois códigos de máquina. Uma vez desenvolvido estes exploits e divulgados na internet, qualquer hacker pode se utilizar dos mesmos para fazer um ataque contra um servidor que utilize o software com problema de buffer overflow.

Cracking de Senhas

Fazer "crack" de um senha significa descobrir qual é a senha para uma determinada conta. Os métodos empregados são:

Advinhação: Este é um método bastante primitivo, contudo eficiente. Trata-se de utilizar o bom senso junto com algumas informações sobre a conta atacada. Muitos usuários utilizam senhas fáceis (times de futebol, conta acrescido de um digito, datas especiais, nomes de familiares) que são faceis de serem adivinhadas.
Um outra possibilidade de adivinhação está relacionada com softwares que vem com "senhas de fábrica". Por exemplo, quando um banco de dados é instalado o mesmo vem com alguns contas de administração padrão, as quais possuem algumas senhas padrões. Se estas senhas não forem alteradas pelo administrador, fica-se vulnerável a qualquer hacker que tenha uma lista de senhas padrões. Este problema ocorre para roteadores, sistemas operacionais, softwares básicos (ex: backup), etc.

Programas de Cracking: Este método consistem em empregar programas que "descobrem" as senhas utilizando tentativa e erro. Para isto, os programas utilizam dicionários de senhas básica, aplicando variações, ou então utilizam força bruta (tentam todas as senhas possíveis).
Este processo normalmente é efetuado após o hacker ter conseguido obter um arquivo contendo o hash code das senhas. Este arquivo contém uma representação das senhas, não as senhas propriamente ditas. O programa de cracking tenta começa então a gerar senhas, e quando uma senha gerada produzir o mesmo hash code ele terá encontrado a senha.
Uma vez que é muito simples obter via internet um bom programa de cracking, esta técnica de ataque será muito efetiva caso o arquivo de hash da sua empresa caia nas mãos dos hackers.

Denial of Sevice (DoS)

Ataques de denial of service tem como objetivo paralisar (derrubar) um serviço em um servidor, ou então tornar os serviços tão lentos que o usuário legitimo não consegue acessá-los. As vulnerabilidades exploradas por ataques de DoS são as seguintes:

Falhas em softwares: Softwares que possuem falhas de buffer overflow podem ser paralisados (derrubados) caso recebem um string que ultrapasse a capacidade de seu buffer. Isto causa um denial of service com paralisação do serviço que foi derrubado, exigindo um restart neste serviço. Outras falhas de software que causem o seu cancelamento e

possam ser induzidas externamente também produzem o efeito de denial of service.

Falhas de Protocolo: Alguns sistemas operacionais se desestabilizam quando recebem pacote TCP/IP mal formados. Isto pode levar a uma queda completa do host, exigindo um shutdown.

Esgotamento de recursos: Todo máquina tem um conjunto de recursos limitado (CPU, memória, banda de comunicação). Se estes recursos forem esgotados, o servidor fica extremamente lento, ou pode cair. Este é o princípio utilizado pelos ataques de denial of service do tipo distribuido.

Os tipos de ataques denial of service são:

Denial of Service comum (DoS): Neste ataque, uma máquina ataca a outra. Normalmente exploram as vulnerabilidade de "Falha de Softwares" e "Falhas de Protocolo".

Distributed Denial of Service (DDoS): Este ataque utiliza várias máquinas para atacar uma máquina alvo. O objetivo do ataque é esgotar algum recurso da máquina alvo.

Como ocorre um ataque DoS

Um hacker técnico desenvolve um sistema para explorar alguma vulnerabilidade dos protocolos TCP/IP. Este sistema é composto por dois programas: Master e Zumbi.

Para um hacker vândalo disparar um ataque é necessário primeiro "plantar" os programas zumbis nos computadores atacantes. Para isto o hacker vândalo invade computadores que tenha uma boa largura de banda e uma segurança fraca. Neste computadores eles instalam o programa zumbi.

Quando o hacker vândalo já tem uma quantidade suficiente de computadores comprometidos com o programa zumbi, ele dispara o ataca. Para isto ele utiliza o programa Master, o qual é capaz de se comunicar de forma direta (e normalmente criptografada) com os Zumbis. Através deste programa Master o hacker identifica o alvo do ataque, e como será feito o ataque.

Uma vez recebido o comando de ataque, todos os computadores Zumbis começam simultaneamente a atacar o computador alvo.

Normalmente os programa DDoS utilizam IP Spoofing. Desta forma a equipe responsável pela administração do Site que está sendo atacado não tem como saber quais os IPs fazem parte do ataque, pois os IPs são falsos. Isto dificulda as tentativas de filtragem. A única saída é tentar descobrir alguma característica nos pacotes recebidos que possa permitir separar os pacotes de ataque dos pacotes de acesso legítimo. Isto não é fácil, e exige que a equipe responsável pela segurança esteja bem treinada e preparada para este tipo de ataque.

IP Spoofing

Cada máquina que está se comunicando na internet tem um identificador único: o endereço IP. Contudo, este endereço pode ser forjado, permitindo que uma máquina utilize o endereço de uma outra máquina. Esta técnica é denominda IP spoofing.

As conseqüências de um ataque IP spoofing:

Atacante anônimo: Utilizando o IP Spoofing o atacante pode esconder a sua verdadeira identidade (IP de origem).

Sobrecarregar servidores/roteadores: O IP spoofing faz com que os roteadores/servidores fiquem sobrecarregados ao ter de responder mensagens com endereços IPs falsos. Se isto for aplicado em grande escala, possibilita ataques de denial of service.

Como são elaborados programas com o IP Spoofing

Para construir um programa com IP spoofing, o hacker ignora a camada de protocolo IP do sistema operacional e gera os seus próprios pacotes (modo RAW). Esta técnica dá ao hacker um controle total sobre os pacotes IP.

Quando este programa com IP Spoofing for executado, permitirá a escolha dos endereços IP de origem. O programa pode permitir ao usuário especificar um endereço IP, um grupo de endereços IP, ou ainda solicitar ao programa que gere endereços IP aleatoriamente.

O que acontece quando se utiliza o IP Spoofing

Quando um servidor/roteador tenta responder a um pacote com endereço spoofado (endereço falso), poderá acontecer duas coisas:

Se existir uma máquina ativa com o endereço IP indicado, esta máquina responderá que não está interessada em receber dados deste servidor, uma vez que ela não solicitou nenhuma comunicação com este host. Isto é feito através de um pacote com flag RST.

Se não existir nenhuma máquina com o endereço IP indicado, o servidor/roteador acabará recebendo da rede uma mensagem de "Host Unreacheable".

Tanto um caso quanto o outro fazem com que haja um consumo de CPU e de banda neste servidor. Este é um dos artifícios empregados nos ataques de denial of service. Neste ataques o servidor recebe milhares de pacotes com IP Spoofing e o resultado do tratamento a estes pacotes gera uma sobrecarga no host, ocasionando um denial of service.

Sniffer

Computadores em uma rede local (Ethernet) compartilham um meio físico. Normalmente, uma placa de rede "le" os pacotes destinados a ela, e descarta os demais. Um programa Sniffer coloca a placa de rede em modo promiscuo, possibilitando que um computador receba todos os pacotes que circulam no segmento de rede (dominio de colisão) a que

pertence. Isto possibilita ao hacker obter informações privilegiadas (ex: senhas que circulam sem criptografia) que facilitem um ataque.

Trojan (Cavalo de Tróia)

Trojan é um programa que finge realizar uma certa tarefa, e secretamente realiza uma outra tarefa maliciosa. Suas características técnicas são:

Não detectáveis: Trojans sob medida (feitos específicamente para atacar uma certa empresa) não são detectados por antivirus, uma vez que não possuem uma assinatura que os identifique como virus.

Executam de forma camuflada: Trojans normalmente se instalam como serviços, ou se instalam no startup com um programa sem janela. Os trojans se comunicam com o mundo exterior através de TCP ou UDP, empregando portas que estão abertas no firewall. Os Trojans mais sofisticados criptografam toda a sua comunicação para evitar que seja compreendia.

Backdoors: Uma das principais finalidades dos trojans é criar uma backdoor, permitindo ao hacker controlar a máquina comprometida, e poder assumir uma posição interna na rede. Isto abre novas possibilidades de ataque.

Existe uma tendência de aumentar a utilização de Trojans em invasões de ambientes complexos, pois:

Elo Fraco: Exploram um elo fraco (curiosidade humana), permitindo uma instalação com muita facilidade. A grande maioria dos usuários atualmente considera seguro abrir um arquivo que recebeu em anexo em e-mails. Tais usuários acreditam que o sistema de antivirus irá bloquear qualquer arquivo nocivo.

Facilidade de invasão pelo lado de dentro: Na maioria dos casos é mais fácil romper um sistema de segurança partindo de um ponto interno. A maioria das empresas reforça sua segurança na parte periférica da sua rede, e imagina que os usuários internos são "bem comportados".

Customização: Trojans podem ser customizados para invasões específicas. Eles podem por exemplo ser programados para executar algum comando que enfraqueça momentaneamente o sistema de segurança, permitindo ao hacker invadir a rede enfraquecida pelo lado externo.

Como é feito um ataque com Trojan

O hacker tem dificuldade em atacar a rede alvo pelo lado de fora, mas percebe que o sistema de segurança talvez seja fácil de desarmar por dentro.

O hacker desenvolve um trojan com a função oculta de enfraqueçer o sistema de segurança, ou instalar uma backdoor para permitir ao hacker analisar a rede por dentro.

Este trojan é enviado para os usuários da rede alvo, como um arquivo que atraia a curiosidade (imagem, piada). Para isto, o hacker pode inclusive forjar o seu endereço de e-mail, passando-se por um colega da empresa.

Os usuários inocentemente executam o trojan. O Trojan dá uma mensagem de despiste (arquivo corrompido), ou executa uma função de disfarçe, e simultaneamente se instala na máquina de um forma camuflada (serviço).

Secretamente o Trojan passa a executar funções de ataque contra o sistema de segurança, ou então permite ao hacker começar a vasculhar a rede interna como se estivesse localizado numa máquina interna (backdoor).

Engenharia Social

O hacker se passa por outras pessoas, enganando os funcionários da empresa. Para poder fazer um "teatro" convincente, o hacker utiliza informações (nomes de usuários, administrador, etc) coletadas previamente. Com isto o hacker consegue obter informações privilegiadas (ex: senhas), ou então induzir funcionários a executar ações que enfraqueçam a segurança (ex: executar um trojan, induzir uma reinicialização de senha).

Alguns exemplos de ataque de Engenharia Social são:

Usuário recebe um e-mail do "administrador" (que é o hacker disfaraçado) solicitando para que a sua senha seja alterada para x. Se o usuário proceder conforme solicitado, o hacker saberá qual sua senha, e poderá passar a utilizar a conta deste usuário.

Administrador da rede recebe um e-mail/telefonema de um "usuário" (que é o hacker disfaraçado), solicitando a reinicialização da sua senha. Isto permite ao hacker logar com a senha deste usuário.

Administrador iniciante recebe um e-mail/telefonema de um administrador de uma outra empresa" (que é o hacker disfaraçado), alegando que está recebendo ataques da sua empresa e solicitando a execução de um comando para se certificar. Este comando pode ser um trojan.

Consolidação do Poder

Após o hacker ter conseguido invadir o computador alvo, ele procurará se certificar que seja possível voltar a invadir novamente em outra ocasião, de uma forma simples, sem perder tempo. Além disso, ele deve garantir que os rastros da sua invasão sejam apagados, para não correr o risco de ter seu acesso bloqueado. A este conjunto de atividades pós-invasão inicial, damos o nome genérico de consolidação do poder.

Etapas na consolidação do poder:

Promoção para Administrador: Caso o hacker tenha feito a sua invasão através de uma conta com poucos privilégios (conta de usuário), ele tentará se promover a administrador. Para isto, existe uma série de técnicas diferentes para cada sistema operacional.

Remoção de pistas: Após ter obtido privilégios para manipular os logs do sistema, o hacker eliminará os rastros de sua invasão, de forma a não chamar a atenção.

Instalar backdoors: Para poder retornar facilmente à maquina invadida, o hacker procurará instalar backdoors, ou então fará alguma modificação no sistema de segurança para deixá-lo mais aberto. A instalação de backdoors é preferida pelos hackers, pois chama menos atenção. Os programas que implementam a backdoor são normalmente difíceis de serem localizados, pois instalam-se de forma camuflada.

Técnicas de Ataque utilizadas na "Simulação de Ataque Hacker"

Abaixo listamos de forma resumida as principais técnicas de ataque utilizadas na "Simulação de Ataque Hacker". A separação por nível (técnicas básicas, médias, avançadas) tem como objetivo dar uma idéia da complexidade das técnicas, e mostrar quais técnicas serão aplicadas na simulação de ataque hacker em função do nível de simulação selecionado pelo cliente.

Técnicas Básicas	Descrição
Coletar Informações sobre alvo	Esta é a primeira fase de um ataque. Consiste na coleta de informações que possibilitarão ao hacker fazer uma análise do seu ambiente computacional, e decidir qual a estratégia de ataque será utilizada.
Cracking de senhas	Crackear uma senha significa descobrir qual é a senha através de "adivinhação" ou utilizando programas de cracking. Existem programas prontos para fazer isto, tornando esta tarefa bastante simples. Na maioria dos casos a parte difícil é obter o arquivo de senhas (usuário x hash da senha), sobre o qual programa vai rodar.
Explorar vulnerabilidades conhecidas e documentadas	Diversos softwares tem vulnerabilidades conhecidas e documentadas. Um dos principais causadores deste tipo de vulnerabilidade são os erros de buffer overflow, os quais muitas vezes vezes permitem ao hacker executar um código arbitrário (definido pelo hacker) no seu servidor. Estas falhas podem ocorrem em qualquer tipo de software: softwares básico (ex: WebServer, FTP Server), scripts (CGI), etc. Escrever programas para explorar buffer overflow é uma técnica avançada. Porém, utilizar programas prontos (que existem em grande número) é básico.
Denial of Service por falhas em software	Existem ataques de denial of service que tem como objetivo paralisar o seu servidor explorando falhas de sofwares (ex: buffer overflow), ou então deficiências no tratatamento de protocolos. Existem programa prontos para explorar estas falhas, e portanto é uma técnica básica.
Denial of Service por falta de recurso	Existem ataques que tem como objetivo paralisar o seu servidor, através do consumo dos recursos da máquina (ex: SYN FLOOD, ping Amplifying). Existem programa prontos, mas requer um bom conhecimento de protocolos para tornar o ataque efetivo.

Técnicas de Nível Médio	Descrição
“Sniffar”	“Sniffar” significa instalar um programa (sniffer) para monitorar todo o tráfego de rede em em determinado segmento de colisão. É um técnica de nível médio, pois requer uma invasão prévia para instalar o sniffer (tem de ser plantado internamente na rede, ou em um server que está na rota), e é necessário saber fazer um triagem seletiva nos dados coletados pelo sniffer.
Promover um usuário para Administrador	Uma vez obtida uma conta de usuário normal (normalmente através de cracking de senha), existem técnicas para se promover esta conta para ter os direitos do administrador do host (ex: Administrator no NT, root nos Unix). Este é um dos objetivos principais dos hackers que desejam ter controle total sobre a sua instalação.
Instalar Backdoors	Instalar uma backdoor é preparar um outra forma mais simples de se entrar na sua rede. Isto é feito após o hacker ter conseguido efetuar uma primeira invasão. Para instalar uma backdoor é necessário um bom conhecimento de como está configurado o sistema de segurança, principalmente o firewall.
Plantar Trojans	Trojan são programas que parecer fazer uma coisa (benigna) e fazem outra (maligna). Os trojans são usados em invasão para enfraquecer os sistemas de segurança pelo lado de dentro, ou para instalar backdoors.
Limpeza de Log	Limpar os logs, ou alterá-los para encobrir pistas é o artifício que os hackers utilizam para esconder a ocorrência de invasão.

Técnicas Avançadas	Descrição
Trojans sob medida	Desenvolver trojans específicos para atingir a sua organização é uma técnica avançada empregada pelos hackers. Trojans específicos não são detectados por antivirus.
Engenharia Social	A Engenharia social tem como objetivo fazer com que pessoas da sua organização entreguem ao hacker informações ou executem ações que facilitem a invasão. Para isto o hacker irá se passar por outras pessoas da sua organização, e utilizará ligações telefônicas ou e-mails forjados. Fazer isto de forma a obter informações úteis e não levantar suspeitas é uma técnica avançada.
Hacker Interno	Um hacker interno tem o conhecimento de um hacker e os privilégios de usuário interno. Isto torná-o muito mais perigoso de que um hacker acessando sua rede externamente. Isto acontece quando um hacker é "plantado" na sua organização passando-se por um funcionário; ou então quando o hacker efetua uma invasão "física", assumindo o controle de um computador interno.
Trashing	Procurar por informações que possibilitem um ataque explorando o "lixo" do alvo. Esta técnica é considerada avançada pois "reconhecer e recuperar" uma informação útil no meio de um estrutura totalmente desorganizada (lixo) requer uma abordagem bastante metódica.

Interceptação de Sessão	O sequestro de uma sessão consiste no hacker interceptar uma conexão na internet, conseguir ler todos os dados que estão trafegando, e se for o caso conseguir forjar uma das pontas transmitindo dados falsos. Para isto ser possível, o hacker deve ter dominado algum ponto próximo da sua conexão com a internet (normalmente os computadores do provedor de acesso).
Denial of Service por sobrecarga de banda	Este ataque consiste em sobrecarregar a banda de entrada da sua conexão internet. Normalmente são executados através de DDoS (Distribuido). Apesar de existirem ferramentas prontas no mundo hacker, dispor estas ferrramentas de forma estratégica em máquinas que vão gerar um ataque efetivo requer conhecimento.

Capítulo 3

Configuração de Segurança do Sistema Operacional

Os sistemas operacionais Windows NT e Windows 2000 fornecem uma grande variedade de características de segurança. Entretanto, a configuração padrão do produto é altamente insegura.

Este capítulo descreve várias configurações de segurança relacionadas a estes sistemas operacionais para criar um ambiente altamente seguro. Tais configurações são descritas na forma de um “checklist” conforme podemos observar a seguir:

Instalação
Colocar o servidor em um local fisicamente seguro
Definir o tipo de controlador de domínio
Formatar disco rígido com NTFS
Aplicar o Service Pack e os Hot-fixes mais recentes
Remover o servidor da rede ou deixar apenas na rede interna, antes de completar as configurações
Definir o tempo de inicialização do sistema para zero segundos

Rede
Desativar os serviços de Internet desnecessários
Remover os subsistemas OS/2 e POSIX
Remover todos os compartilhamentos de rede
Restringir o acesso anônimo via rede
Remover todos os protocolos com exceção do TCP/IP
Remover a ligação do NetBIOS com TCP/IP
Desabilitar o Roteamento de IP
Configurar a filtragem de TCP/IP
Remover as fontes de dados ODBC/OLE-DB não utilizadas
Desabilitar o suporte a RDS
Desabilitar endereço IP em Content-Location
Desabilitar a chamada do shell de comando com #exec

Autenticação
Esconder o nome do último usuário no logon
Exibir uma notificação legal antes do logon
Definir tamanho de senha
Remover o botão “Desligar” da tela de logon
Executar o utilitário SYSKEY
Definir uma senha bem difícil para conta de Administrador
Impedir o acesso não autenticado ao Registro
Remover o diretório virtual IISADMPWD

Contas de Usuário
Renomear a conta de Administrador
Permitir o bloqueio da conta de Administrador através da rede
Verificar as contas de usuários, associação de grupos e privilégios

Permissões de Acesso
Desativar a criação de nomes de arquivo do tipo 8.3
Definir as permissões do NTFS
Mover e definir permissões para os arquivos críticos
Definir permissões e auditoria para chaves críticas do Registro
Proteger os diretórios virtuais e aplicações Web
Modificar as permissões ou mover o Metabase
Proteger o Microsoft Certificate Server

Auditoria
Auditar sucesso e falha de Logon/Logoff
Definir o intervalo de sobrescrita para o arquivo de log
Sincronizar data e hora

Instalação

A seguir descrevemos as configurações de segurança recomendadas para a utilização do Windows NT/2000 como servidor web que estão relacionadas à instalação do sistema operacional.

Colocar o servidor em um local fisicamente seguro

Os controles de segurança física devem ser aplicados a todas as áreas que processem informações sensíveis à organização, não necessariamente só a recursos informatizados, mas também qualquer recurso que processe, ou receba informações que se divulgadas ou utilizadas indevidamente possam causar danos ou prejuízos a organização ou a seus parceiros, como por exemplo fax, impressão de documentos, etc.

Na implantação de controles de segurança física, o CPD deve receber atenção especial, devido a criticidade das informações processadas nele. Devem ser observadas desde a sua localização até o controle das pessoas que o acessam.

A seguir descrevemos os principais ítens de segurança física que devem ser observados em um CPD:

- Localização
- Controle de acesso
- Acesso de prestadores de serviços
- Monitoramento
- Cabeamento
- Portas e janelas
- Controles ambientais
- No Break
- Backup

Definir o tipo de controlador de domínio

Os controladores de domínio servem a dois propósitos no ambiente Windows NT/2000: autenticar usuários e fornecer-lhes acesso a outros recursos disponíveis na rede, de acordo com os direitos e permissões definidos.

Os controladores de domínio, por via de regra, não devem executar nenhum outro software pois eles contêm informações de usuários extermamente sensíveis que são usadas para autenticação.

Preferencialmente, deve-se configurar o servidor IIS para ser um servidor “stand alone” para minimizar uma possível exposição das contas de usuários do domínio.

Formatar disco rígido com NTFS

O sistema de arquivos FAT nunca deve ser usado. O NTFS é o mais seguro dos dois sistemas de arquivos. Servidores de rede devem utilizar NTFS para aproveitar as características de segurança do Windows NT/2000. O NTFS também fornece maior capacidade de auditoria, permite o uso de vários atributos extendidos e compressão.

Vale a pena lembrar que alguns programas permitem que outros sistemas operacionais acessem um volume NTFS. Por exemplo, se você tiver acesso físico a um servidor, você pode inicializá-lo através de um disquete e executar o programa NTFS Pro (http://www.winternals.com). Este programa montará um volume NTFS e o tornará acessível. Para previnir-se contra esse tipo de problema, todos os servidores críticos devem ser protegidos fisicamente.

Depois que o sistema operacional for instalado e os drives foram formatados, você pode converter de FAT para NTFS usando o utilitário CONVERT.EXE. Entretanto, esta conversão acontece em mão única, ou seja, quando um volume é convertido para NTFS, é impossível convertê-lo para FAT.

Aplicar o Service Pack e os Hot-fixes mais recentes

Atualmente, o Service Pack 6a e o Service Pack 2 são as mais recentes atualizações para o Windows NT 4.0 e Windows 2000 respectivamente. Revise todos os Boletins de Segurança da Microsoft e então procure pelos hot-fixes:

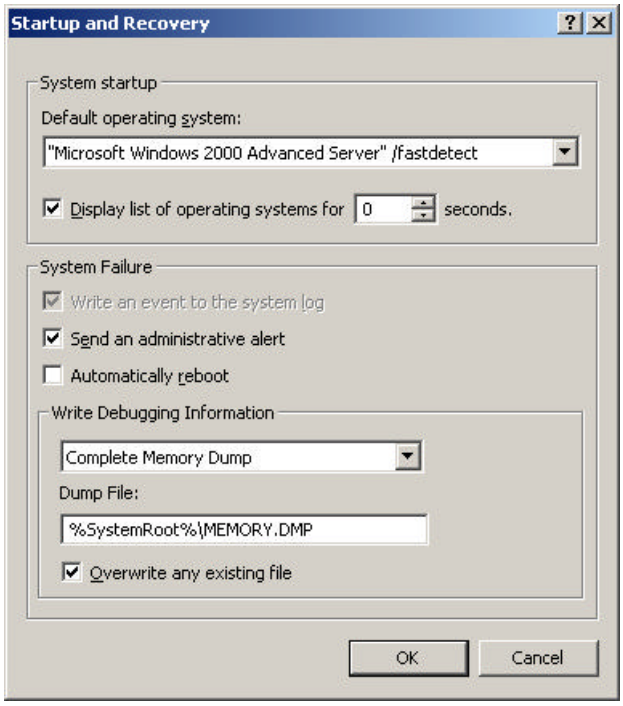
Produto	**URL**
Windows NT/2000	http://www.microsoft.com/technet/itsolutions/security/current.asp?productID=51
IIS	http://www.microsoft.com/technet/security/itsolutions/current.asp?productID=14
Certificate Server	ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/certserv/
Web site “Microsoft Security”	http://www.microsoft.com/technet/itsolutions/security/default.asp
Microsoft Security Advisor	http://www.microsoft.com/security/

Remover o servidor da rede ou deixar apenas na rede interna, antes de completar as configurações

Se é necessário acessar o servidor IIS através da Internet, recomendamos instalá-lo inicialmente com tráfego de entrada bloqueado no roteador ou no firewall. Depois de terminada a configuração, podemos permitir o tráfego de entrada. Esta recomendação é feita pois uma vez finalizada a instalação principal do IIS, os serviços são ativados e conexões podem ocorrer. Isto pode provocar o comprometimento do sistema antes que haja tempo para configurar a segurança do(s) web site(s).

Definir o tempo de inicialização do sistema para zero segundos

Entre em Control Panel | System | Startup/Shutdown (para o Windows NT 4.0) ou Control Panel | System | … (para o Windows 2000). Em seguida, defina “Show list for” para zero.



Rede

A seguir descrevemos as configurações de segurança recomendadas para a utilização do Windows NT/2000 como servidor web que estão relacionadas ao ambiente de rede.

Desativar os serviços de Internet desnecessários

Geralmente é recomendável reduzir o número de pontos de entrada em um servidor, o que para o Windows NT/2000 significa reduzir o número de serviços. É necessário parar e desabilitar os serviços desnecessários usando o Service Configuration Manager. Apenas os seguintes serviços devem estar rodando para permitir o funcionamento do IIS:

Log de eventos

Serviço de Auditoria de Licenças

Windows NTLM Security Support Provider

Serviço de Remote Procedure Call (RPC)

Windows NT/2000 Server ou Windows NT/2000 Workstation

Serviço IIS Admin

MSDTC

Serviço de Publicação na World Wide Web

Armazenamento protegido

Remover os subsistemas OS/2 e POSIX

Remova estes subsistemas realizando as seguintes mudanças no registro:

Registry	HKEY_LOCAL_MACHINE
Chave	SOFTWARE\Microsoft\OS/2 Subsystem for NT
Ação	Apague todas as subchaves

Registry	HKEY_LOCAL_MACHINE
Chave	SYSTEM\CurrentControlSet\Control\Session Manager\Environment
Nome	Os2LibPath
Ação	Apague a chave Os2LibPath

Registry	HKEY_LOCAL_MACHINE
Chave	SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
Ação	Apague as chaves Optional, Posix e OS/2

Em seguida apague o diretório de \winnt\system32\os2 e todos os subdiretórios. As mudanças entrarão em vigor na próxima reinicialização.

NOTA: As subchaves "Microsoft\OS/2 Subsystem for NT" e "Os2LibPath" serão recriadas depois que o sistema reiniciar, mas contanto que a chave "Optional" continue vazia, o subsistema OS/2 estará removido.

Remover todos os compartilhamentos de rede

O Windows NT/2000 cria compartilhamentos ocultos (também chamados compartilhamentos administrativos) para todas as unidades de disco rígido. Estes compartilhamentos são acessíveis (sem uma senha) somente para o Administrador a partir da máquina na qual ele efetuou o logon. Os outros usuários podem ter acesso usando a senha correta e digitando no nome do compartilhamento (\\MACHINE1\C$, por exemplo) para mapear tais unidades de rede.

Só os membros do grupo global Admins de Domínio ou do grupo local Administradores têm acesso aos compartilhamentos ocultos. Se qualquer outro usuário está em sessão no sistema, não é necessário efetuar o logoff do mesmo, mas será preciso se conectar ao compartilhamento como um administrador e fornecer a senha correta.

Depois que a senha correta for fornecida, o diretório raiz e todos o subdiretórios e arquivos estarão acessíveis até mesmo se eles não foram compartilhados do modo normal.

Execute “NET SHARE /D” a partir da linha de comando e certifique-se que você removeu todos compartilhamentos de rede. Também é recomendável impedir a criação dos compartilhamentos administrativos (C$, D$, ADMIN$) através da seguinte configuração de Registro:

Registry	HKEY_LOCAL_MACHINE
Chave	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Nome	AutoShareServer
Tipo	REG_DWORD
Valor	0

Restringir o acesso anônimo via rede

Windows NT/2000 tem uma característica que permite a usuários não autenticados enumerar os usuários de um domínio Windows NT/2000. Se você não necessita desta funcionalidade, faça a seguinte configuração no Registro:

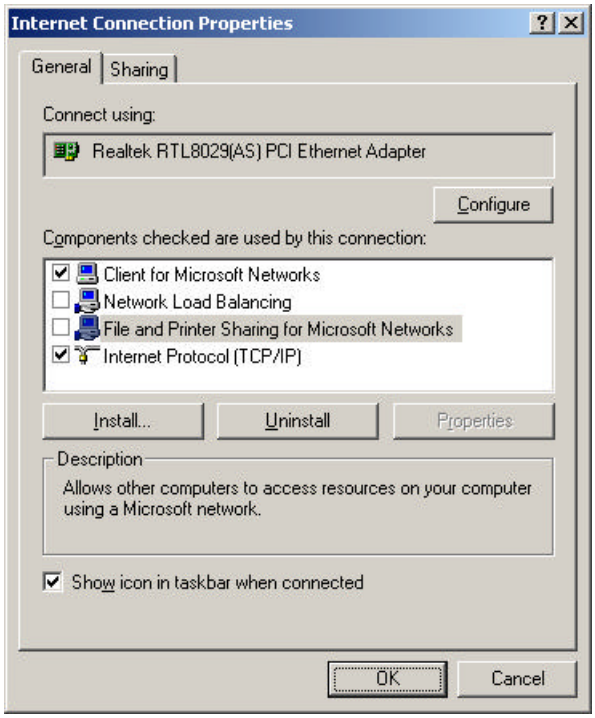
Registry	**HKEY_LOCAL_MACHINE**
Chave	SYSTEM\CurrentControlSet\Control\LSA
Nome	RestrictAnonymous
Tipo	REG_DWORD
Valor	1

Remover todos os protocolos com exceção do TCP/IP

O Windows NT/2000 suporta vários protocolos de redes. Devido ao fato de estarmos focalizando em segurança, analisaremos aqueles protocolos que têm implicações de segurança, independentemente da implementação do Windows NT/2000.

O NWLink, a implementação da Microsoft para o protocolo Internetwork Packet Exchange (IPX), permite conectividade entre os ambientes Windows NT/2000 e Novell NetWare. A menos que a rede em questão seja uma mistura dos ambientes Windows NT/2000 e NetWare, recomendamos que este protocolo não seja usado e nem mesmo instalado.

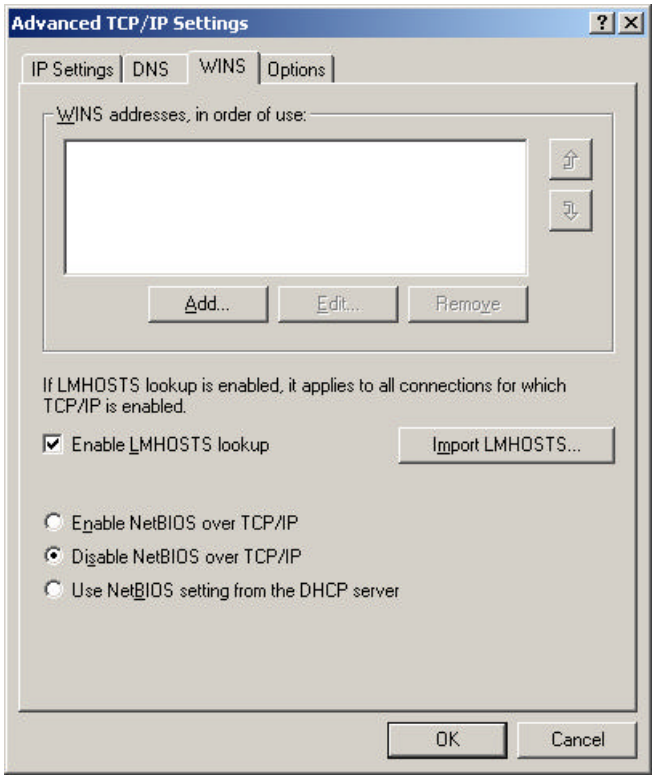
O NetBEUI, um protocolo de rede da Microsoft, suporta comunicação em um ambiente Microsoft quando a rede é pequena e composta de um único segmento de rede. O NetBEUI é um protocolo não roteável - quer dizer, seus pacotes não contêm nenhuma informação de roteamento e não podem atravessar roteadores em outros segmentos de rede. Entretanto, quando usado em uma rede Token Ring, o NetBEUI é roteável - quer dizer, usa uma fonte de roteamento.



Remover a ligação do NetBIOS com TCP/IP

A rede Microsoft requer o uso do protocolo NetBIOS junto com um protocolo de transporte padrão para completar o endereçamento de um pacote. O NetBIOS pode ser roteado para outros segmentos de rede quando combinado com os protocolos TCP/IP ou NWLink em uma forma conhecida como um protocolo encapsulado. Todos serviços de compartilhamento de arquivos e impressoras do Windows NT/2000 usam NetBIOS para carregar suas informações. Seu uso pode reprensentar sérios riscos à segurança, por isso os serviços de NetBIOS devem ser desativados em um servidor web.

Ao remover o serviço de NetBIOS sobre TCP/IP impede-se que um usuário acesse informações de máquina usando ferramentas como NBTSTAT. Essa ferramenta mostra o conteúdo da tabela de nomes do NetBIOS de um computador remoto. As informações listadas nessa tabela podem ser usadas para determinar o nome do domínio ou grupo de trabalho onde a máquina está e os usuários conectados. As informações também podem ser utilizadas para descobrir a conta de administrador, devido ao fato de que os SIDs também são mostrados.



Desabilitar o Roteamento de IP

Se o roteamento estiver habilitado, existe o risco de que os dados passem entre a intranet e a Internet. Para desabilitar o roteamento, abra o Control Panel | Network | Protocols | TCP/IP Protocol | Properties | Routing e desative a opção “Enable IP Forwarding”.

Configurar a filtragem de TCP/IP

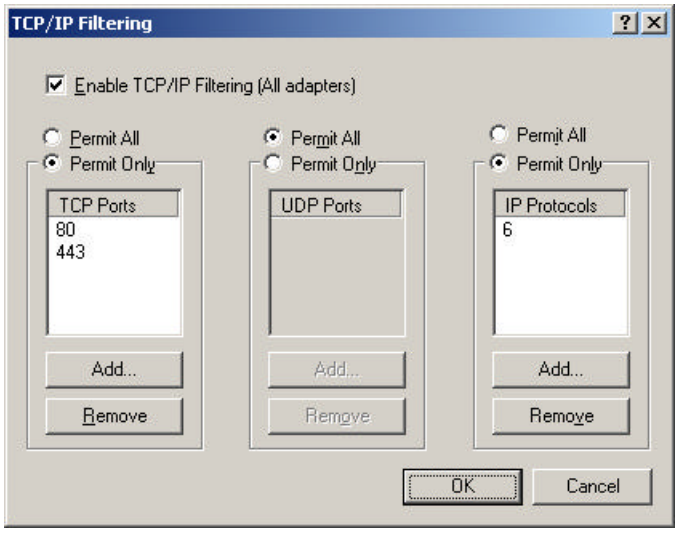
O Windows NT/2000 permite que o protocolo TCP/IP seja filtrado e restrito. Esta filtragem pode ser utilizada para aumentar a segurança do sistema operacional em qualquer configuração. A filtragem pode ser aplicada tanto no nível das portas quanto do protocolo, para cada adaptador de rede instalado no sistema.

A configuração da filtragem de TCP/IP é feita especificando-se quais são as portas permitidas em cada uma das placas de rede. Abra o Painel de Controle | Network | Protocols | TCP/IP | Advanced | Enable Security | Configure. Agora defina as seguintes opções:

Permitir as portas TCP 80 e 443 (caso utilize SSL)

Não permitir nenhuma porta UDP

Permitir apenas IP Protocol 6 (TCP)



IMPORTANTE: A filtragem de pacotes no Windows NT/2000 não é uma proteção suficientemente forte quando implementada por si só. Este controle deve ser implementado em conjunto com a filtragem de pacotes nos roteadores e firewalls.

Remover as fontes de dados ODBC/OLE-DB não utilizadas

Alguns aplicações instalam fontes de dados ODBC para bancos de dados de exemplo, enquanto outras podem instalar novos drivers de banco de dados ODBC/OLE-DB. É recomendável remover qualquer fonte de dados e driver não desejado que usam a ferramenta ODBC Data Source Administrator.

Desabilitar o suporte a RDS

Devido à configuração padrão do RDS Datafactory (componente do RDS) permitir, de forma implícita, que sejam feitas requisições remotas de acesso a dados, é possível explorar esta característica para permitir que clientes de Internet sem autorização acessem fontes de dados OLE DB disponíveis para o servidor.

Ao conectar-se ao IIS com RDS (Remote Data Services) instalado, um usuário malicioso pode ganhar acesso a dados ODBC tais como informações contidas no Microsoft SQL Server ou Microsoft Access.

Se você não utiliza esta funcionalidade, recomendamos desativá-la ou restringir seu uso através de permissões. Para desativar totalmente a funcionalidade de RDS, é nescessário remover as seguintes entradas de registro do servidor IIS:

Registry	**HKEY_LOCAL_MACHINE**
Chave	SYSTEM\CurrentControlSet\Services \W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
Ação	Apague a chave e eventuais sub chaves

Registry	HKEY_LOCAL_MACHINE
Chave	SYSTEM\CurrentControlSet\Services \W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
Ação	Apague a chave e eventuais sub chaves

Registry	HKEY_LOCAL_MACHINE
Chave	SYSTEM\CurrentControlSet\Services W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls
Ação	Apague a chave e eventuais sub chaves

Active Server Pages (ASP) que só dependem de ADO para conectar-se ao banco de dados continuarão funcionando. Entretanto, a seção de benefícios do site de exemplo do IIS, chamada Exploration Air, pode não funcionar corretamente depois desta mudança.

Confira também o log do IIS regularmente em busca de sinais de ataque. A assinatura a se procurar é algo como:

```
1999-10-24 20:38:12 - POST /MSADC/MSADCS.DLL ...
```

É possível automatizar o processo de busca usando o seguinte commando:

```
find /i "msadcs" logfile.log
```

Para obter maiores informações sobre as implicações de segurança do RDS, dois excelentes artigos da rain.forest.puppy (r.f.p.) podem ser encontrados em RFP9901 (http://www.wiretrip.net/rfp/p/doc.asp?id=3&iface=2) and RFP9902 (http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=2).

Desabilitar endereço IP em Content-Location

Quando você usa que páginas HTML estáticas (Default.htm, por exemplo), um cabeçalho de Content-Location é acrescentado à resposta. Como padrão, no IIS, o Content-Location referencia o endereço IP do servidor ao invés do nome do servidor ou FQDN (Full Qualified Domain Name). Veja o exemplo a seguir:

```
HTTP/1.1 200 OK

Server: Microsoft-IIS/4.0

Content-Location: http://10.1.1.1/Default.htm

Date: Thu, 18 Feb 1999 14:03:52 GMT

Content-Type: text/html

Accept-Ranges: bytes

Last-Modified: Wed, 06 Jan 1999 18:56:06 GMT

ETag: "067d136a639be1:15b6"

Content-Length: 4325
```

Este cabeçalho pode expor endereços IP internos que estão normalmente ocultos ou mascarados atrás de NAT (Network Address Translation) fornecida por um firewall ou servidor proxy.

No exemplo anterior, o Content-Location especifica o endereço interno do servidor IIS dentro do cabeçalho. Este cabeçalho permanece inalterado quando atravessar o firewall ou servidor proxy. Então, a segurança da rede interna pode ser comprometida expondo os endereços de rede que estão sendo usados.

Há um valor que pode ser modificado no metabase do IIS para mudar o comportamento padrão de expor endereço IP para, ao invés disso, enviar o FQDN. Isto permite que o endereço IP seja mascarado pelo nome do domínio. Para isso, realize o seguinte procedimento:

Abra um “Prompt de Comando”;

Vá para o diretório \WINNT\SYSTEM32\INETSRV\ADMINSAMPLES (IIS 4.0) ou INETPUB\ADMINSCRIPTS (IIS 5.0);

Digite o seguinte comando:

```
adsutil set w3svc/UseHostName True
```

Recomendamos reiniciar o serviço Inetinfo após feita a modificação. Para parar o processo Inetinfo, digite o seguinte comando:

```
net stop iisadmin /y
```

Em seguida, digite o seguinte comando para iniciar o serviço novamente:

```
net start w3svc
```

Desabilitar a chamada do shell de comando com #exec

O comando #exec pode ser utilizado para chamar comandos arbitrários no servidor de Web a partir de uma página HTML. Como padrão, o IIS desativa esta opção, mas é possível confirmar seu estado atual através da seguinte chave do Registro:

Registry	**HKEY_LOCAL_MACHINE**
Chave	SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
Nome	SSIEnableCmdDirective
Tipo	REG_DWORD
Valor	0

Autenticação

A seguir relacionamos as configurações recomendadas para aumentar o nível de segurança na autenticação dos usuários no Windows NT/2000 quando utilizado como servidor web.

Esconder o nome do último usuário no logon

Como padrão, o Windows NT/2000 coloca o nome do último usuário que efetuou logon no computador no campo “Nome” da tela de Logon. Para ajudar a manter os nomes de usuário em segredo, pode-se impedir que o sistema operacional mostre o nome de usuário do último que efetuou o logon. Para tanto, faça a seguinte configuração no Registro:

Registry	**HKEY_LOCAL_MACHINE**
Chave	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Nome	DontDisplayLastUserName
Tipo	REG_SZ
Valor	1

Exibir uma notificação legal antes do logon

Faça a seguinte configuração no Registro para exibir informações legais sobre o uso do computador:

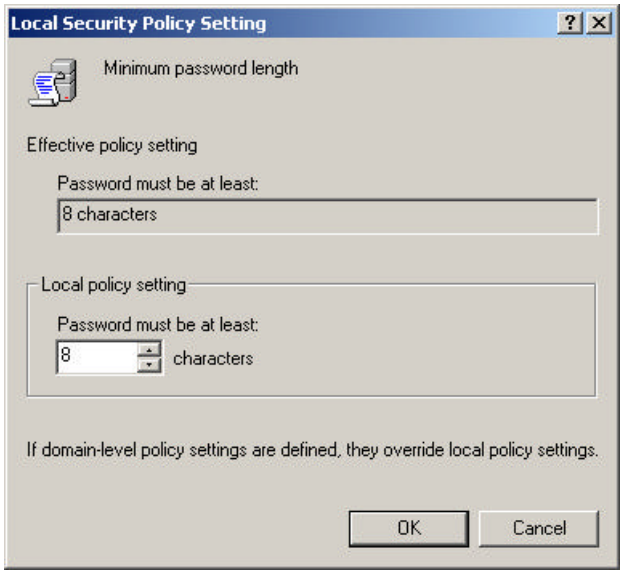
Registry	**HKEY_LOCAL_MACHINE**
Chave	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Nome	LegalNoticeCaption
Tipo	REG_SZ
Valor	O título que você quiser que apareça na mensagem

Registry	**HKEY_LOCAL_MACHINE**
Chave	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Nome	LegalNoticeText
Tipo	REG_SZ
Valor	O texto que você quiser que apareça na mensagem

Uma excelente fonte de informação para formular uma mensagem de logon pode ser encontrada no web-site CIAC (http://www.ciac.org/ciac/bulletins/j-043.shtml).

Definir tamanho de senha

Configure o tamanho da senha para, no mínimo, nove caracteres. Isto faz com que ela seja muito mais difícil adivinhar que com oito ou menos caracteres devido ao modo o Windows NT/2000 cria o “hash” da senha. Também, use pontuação e outros caracteres não-alfabéticos nos primeiros 7 caracteres.



Remover o botão "Desligar" da tela de logon

Os servidores ficam freqüentemente com a sessão fechada pois podem compartilhar arquivos, executar serviços e autenticar usuários enquanto exibem a tela de autenticação. Se o servidor web não estiver em um local fisicamente seguro e alguém o desliga acidental ou propositalmente, nenhum usuário poderá acessar qualquer recurso do mesmo.

Faça a seguinte configuração no Registro para remover a opção de desligar o computador sem efetuar logon:

Registry	**HKEY_LOCAL_MACHINE**
Chave	SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
Nome	ShutdownWithoutLogon
Tipo	REG_SZ
Valor	0

Executar o utilitário SYSKEY

O SYSKEY é uma ferramenta que foi introduzida ao Windows NT 4.0 no Service Pack 3 e a capacidade de usar técnicas de criptografia forte para aumentar a proteção das informações de senha das contas armazenadas no registro através do Gerenciador de Contas de Segurança (SAM). O Windows NT/2000 armazena informações das contas de usuário, inclusive uma derivação da senha da conta de cada usuário, em uma parte segura do Registro protegida por controle de acesso e uma função de ofuscação.

As informações de conta no Registro só são acessíveis aos membros do grupo Administradores. O Windows NT/2000, como outros sistemas operacionais, permite a usuários privilegiados que são administradores, o acesso a todos os recursos do sistema. Para instalações que desejam aumentar a segurança, a criptografia forte das informações derivadas da senha de conta fornece um nível adicional de segurança para impedir os

Administradores de acessar, intencionalmente ou sem querer, as derivações de senha usando as interfaces de programação do Registro.

Para ativar essa criptografia forte, basta executar o utilitário Syskey.exe localizado no diretório \WINNT\SYSTEM32 da unidade local e escolher a opção “Encryption Enabled” conforme mostra a figura acima.

Para obter detalhes adicionais sobre esta funcionalidade, recorra ao documento Q143475 (http://support.microsoft.com/support/kb/articles/q143/4/75.asp) .

Definir uma senha bem difícil para conta de Administrador

Certifique-se que a conta de administrador tenha uma senha muito difícil adivinhar e seja mudada freqüentemente.

Impedir o acesso não autenticado ao Registro

Todas as informações de inicialização e configuração usadas pelo Windows NT/2000 são armazenadas no Registro. Normalmente, as chaves no Registro são alteradas indiretamente, através de ferramentas administrativas como o Painel de Controle. Este método é recomendado.

Entretanto, o Registro também pode ser alterado diretamente, com o Editor de Registro, que possibilita acesso remoto ao registro de Windows NT/2000. Para restringir o acesso via rede ao registro, use o Editor de Registro para criar a seguinte chave:

Registry	**HKEY_LOCAL_MACHINE**
Chave	SYSTEM\CurrentControlSet\Control\SecurePipeServers
Nome	\winreg

As permissões de segurança (ACLs) definidas para esta chave definem quais usuários ou grupos podem se conectar ao sistema para ter acesso remoto ao registro.

Remover o diretório virtual IISADMPWD

O IIS permite que os usuários do Windows NT/2000 alterem suas senhas e notifica os usuários que suas senhas estão prestes a expirar. Isto é feito usando o diretório virtual IISADMPWD que é instalado como parte do Web site padrão.

Esta característica é implementada como um conjunto de arquivos .HTR localizados no diretório \WINNT\SYSTEM32\INETSRV\IISADMPWD e uma extensão ISAPI chamada ISM.DLL. Este diretório deve ser removido se esta característica não for necessária ou se o servidor estiver na Internet. Para mais obter maiores informações sobre esta funcionalidade, recorra ao documento Q184619 (http://support.microsoft.com/support/kb/articles/q184/6/19.asp).

Contas de Usuário

O Windows NT/2000 fornece várias funções que permitem aos administradores proteger e controlar contas de usuário. Os tipos de senhas que os usuários escolhem podem ser controlados, assim como os direitos e privilégios que os usuários têm no sistema.

A seguir descrevemos as configurações recomendadas para essas funções em um servidor web.

Renomear a conta de Administrador

A conta de Administrador tem total controle sobre a operação e segurança de todo o sistema operacional. Qualquer um que efetue logon como um administrador tem controle até mesmo sobre os arquivos de outros usuários. Este é o principal motivo porque a conta Administrador e seus equivalentes devem ser completamente confiáveis.

Como padrão, a conta de Administrador é definida com uma senha que nunca expira. A preocupação principal com esta conta é que ela é muito poderosa e todo mundo sabe que ela existe. Devido ao fato de ser comum a todo sistema operacional e todo mundo sabe que é, a conta é um alvo muito suscetível a ataques. Deste modo, os controles de segurança para protegê-la devem ser estritos.

Recomendamos adicionar um “falso” administrador para ajudar na deteção de ataques à conta. Além disso, não dar nenhum direito a este 'Administrator' e examinar cuidadosamente seu uso.

NOTA: nbtstat -a ou nbtstat -A pode ser usado para determinar a conta de administrador real se ele estiver atualmente conectado.

Permitir o bloqueio da conta de Administrador através da rede

Normalmente, a conta de Administrador não pode ser bloqueada se um hacker tentar adivinhar a senha. Porém, há uma ferramenta do Resource Kit do Windows NT/2000 chamada PASSPROP que fornece esta opção. Se você executa o seguinte comando, a conta de Administrador será bloqueada caso um hacker tente utilizar um ataque de força bruta ou de dicionário, mas o administrador ainda pode efetuar logon localmente ao servidor:

```
passprop /adminlockout
```

Verificar as contas de usuários, associação de grupos e privilégios

Minimize o número de usuários e grupos no servidor e mantenha apenas uma pequena associação de grupos. Apenas as contas mais confiáveis devem ser listadas nos grupos Administradores e Admins. de Domínio.

Através dos direitos é possível autorizar um usuário a realizar certas tarefas no sistema operacional e afetam recursos específicos. Tais direitos são divididos em duas categorias: direitos padrão e direitos avançados. Existem 10 direitos padrão que são normalmente atribuídos a usuários e 17 direitos avançados que normalmente não são atribuídos a um usuário.

Para manter a segurança em um domínio, todos os direitos de usuários devem ser restritos a apenas aqueles indivíduos que necessitam de tal acesso. Apesar dos administradores serem poderosos e terem mais direitos que qualquer outro grupo, eles não tevem possuir todos os direitos.

É difícil recomendar a melhor configuração de segurança dos direitos de usuário devido a grande variedade de ambientes. A seguir descrevemos alguns direitos que são particularmente poderososos, verifique todas as contas que possuem tais direitos abrindo o Gerenciador de Usuários | Políticas | Direitos de Usuário:

Debug programs: este direito permite aos usuários depurar objetos de baixo nível tais como processos e “threads”. Devido ao poder que este direito dá, ele deve ser atribuído apenas a desenvolvedores em máquinas de desenvolvimento.

Act as part of operating system: é um dos direitos mais poderosos do Windows NT/2000. Permite que as contas ajam como uma parte confiável do sistemas operacional e, portanto possam fazer qualquer coisa independentemente de outros direitos. Como padrão, apenas algumas partes do subsistema do Windows NT/2000 possuem esse direito. Este direito não deve ser dado a nenhum usuário.

Back up files and directories: este direito permite que as contas realizem o back up de arquivos e diretórios independentemente de suas permissões. Usuários com tais direitos podem evitar as ACLs nos objetos do Windows NT/2000. Por essa razão, este direito representa um risco de segurança extremamente alto.

Existem ainda algumas recomendações especiais para a conta IUSR_*Computername.* Esta é uma conta padrão, criada durante a instalação do IIS, com privilégios de logon anônimo para acessar serviços de Internet tais como FTP, WWW, e Gopher. Esta conta precisa ser protegida o acesso de usuários anônimos ao servidor. A seguir descrevemos as configurações de segurança recomendadas para esta conta:

Através do Gerenciador de Usuários, dê um duplo clique sobre a conta IUSR_*Computername*, selecione as opções “User connot change password” e “Password Never Expires” e pressione OK;

Agora através da opção “User Rights” no menu “Policies” adicione o direito “Log on locally” ao usuário e remova os direitos “Log on as a batchservice” e “Access this computer from network”

Selecione "Access this computer from the network", remova o grupo Everyone da lista e acrescente Authenticated Users. Esta configuração fará com que somente os usuários que têm uma conta no domínio ou na máquina possam acessar compartilhamentos no servidor.

NOTA: Se caso o servidor web não for aceitar acesso anônimo, desabilite a conta IUSR_*Computername*.

Permissões de Acesso

O Controle de acesso a arquivos e diretórios é um elemento crítico na proteção de um servidor web. Configurando os objetos com as permissões apropriadas, asseguramos a confidencialidade dos dados, negando o acesso dos usuários aos objetos que não estão relacionados às responsabilidades de sua função. A seguir descrevemos como implementar as permissões do Windows NT/2000 como controles de segurança no sistema.

Desativar a criação de nomes de arquivo do tipo 8.3

O NTFS pode gerar automaticamente nomes de arquivo do tipo 8.3 para manter a compatibilidade com aplicações de 16 bits. Como aplicações de 16 bits não devem ser utilizadas em um servidor web seguro, a criação de nomes de arquivo do tipo 8.3 pode ser desativada seguramente. Além disso, há um benefício de desempenho ao desativar esta funcionalidade. Para desativar a criação de nomes de arquivo do tipo 8.3 configure a seguinte entrada de registro:

Registry	**HKEY_LOCAL_MACHINE**
Chave	\SYSTEM\CurrentControlSet\Control\FileSystem
Nome	NtfsDisable8dot3NameCreation
Tipo	REG_DWORD
Valor	1

Definir as permissões do NTFS

Permissões de arquivos e diretórios são a base do controle de segurança do Windows NT/2000 e são definidas através do menu Segurança no Windows Explorer. A seguir descrevemos as permissões recomendadas para construir um servidor web seguro:

Criar uma nova rota para o diretório INETPUB em um drive separado da partição do Sistema Operacional e outros programas, usando um outro nome diferente de INETPUB para amenizar os ataques;

Remover todas as permissões NTFS do diretório INETPUB, adicionando apenas os grupos de acesso e contas necessárias (por exemplo, remova o grupo Todos e adicione WebUser, WebAdmin etc.);

Estabelecer uma estrutura lógica de diretórios (não misturar arquivos executáveis com HTML, ASP, scripts etc.);

Definir as permissões NTFS nas estruturas de diretórios conforme necessário (para maiores detalhes, ver o próximo capítulo);

Apagar ou mover todos os diretórios de exemplos e scripts que executem exemplos.

Há muitas referências sobre quais são as permissões apropriadas para serem aplicados, como o Resource Kit do IIS e o documento “Windows NT Security Guidelines – a study for NSA Research” desenvolvido pela Trusted Systems Services, Inc. e disponível em http://www.trustedsystems.com/tss_nsa_guide.htm.

Mover e definir permissões para os arquivos críticos

Recomendamos que todas as ferramentas administrativas, que são usadas freqüentemente, sejam colocadas em um diretório especial fora do %systemroot% e definir permissões para elas de forma que só os administradores tenham acesso total a estes arquivos. Por exemplo, crie um diretório chamado \CommonTools e coloque lá os seguintes arquivos:

xcopy.exe	wscript.exe	cscript.exe	net.exe	ftp.exe
arp.exe	edlin.exe	ping.exe	route.exe	at.exe
posix.exe	rsh.exe	atsvc.exe	qbasic.exe	runonce.exe
cacls.exe	ipconfig.exe	rcp.exe	secfixup.exe	nbtstat.exe
debug.exe	regedt32.exe	regedit.exe	edit.com	netstat.exe
telnet.exe	finger.exe	syskey.exe	rdisk.exe	tracert.exe
nslookup.exe	rexec.exe	cmd.exe		

Definir permissões e auditoria para chaves críticas do Registro

Devemos monitorar e aplicar permissões bastante restritivas às seguintes entradas de registro, pois elas podem ser usados para executar programas “trojan”:

Chave de Registry	**ACL**
HKEY_LOCAL_MACHINE\SOFTWARE Microsoft\Windows\CurrentVersion\Run	Administrators (Full Control) SYSTEM (Full Control) Creator Owner (Full Control) Everyone (Read)
HKEY_LOCAL_MACHINE\SOFTWARE Microsoft\Windows\CurrentVersion\RunOnce	Administrators (Full Control) SYSTEM (Full Control) Creator Owner (Full Control) Everyone (Read)
HKEY_LOCAL_MACHINE\SOFTWARE	Administrators (Full Control)

Microsoft\Windows\CurrentVersion\RunOnceEx	SYSTEM (Full Control) Creator Owner (Full Control) Everyone (Read)
HKEY_LOCAL_MACHINE\SOFTWARE Microsoft\Windows NT\CurrentVersion\AeDebug	Administrators (Full Control) SYSTEM (Full Control) Creator Owner (Full Control) Everyone (Read)
HKEY_LOCAL_MACHINE\SOFTWARE Microsoft\Windows NT\CurrentVersion\WinLogon	Administrators (Full Control) SYSTEM (Full Control) Creator Owner (Full Control) Everyone (Read)

Proteger os diretórios virtuais e aplicações Web

É preciso definir as permissões apropriadas para os diretórios virtuais e aplicações Web. Esta configuração depende de cada aplicação, mas as seguintes regras básicas se aplicam:

Tipo de arquivo	**ACL**
CGI etc. (.EXE, .DLL, .CMD, .PL)	Todos (RX) Administradores (Controle Total) Sistema (Controle Total)
Arquivos de Script (.ASP etc)	Todos (RX) Administradores (Controle Total) Sistema (Controle Total)
Arquivos de Include (.INC, .SHTML, .SHTM)	Todos (RX) Administradores (Controle Total) Sistema (Controle Total)
Conteúdo estático (.HTML, .GIF, .JPEG)	Todos (R) Administradores (Controle Total) Sistema (Controle Total)

Ao invés de definir as permissões para cada arquivo, é melhor definir novos diretórios para cada tipo de arquivo e definir as permissões no próprio diretório e permitir que os arquivos as herdem. Como exemplo, uma estrutura de diretório pode se parecer com a seguinte:

c:\inetpub\wwwroot\myserver\static **(.html)**

c:\inetpub\wwwroot\myserver\include **(.inc)**

c:\inetpub\wwwroot\myserver\script **(.asp)**

c:\inetpub\wwwroot\myserver\executable **(.dll)**

c:\inetpub\wwwroot\myserver\images **(.gif, .jpeg)**

A herança de permissões é uma característica do Windows NT 4.0 com Service Pack 4 e com o Security Config Editor instalado.

Modificar as permissões ou mover o Metabase

O metabase é o repositório para a maioria das informações de configuração do IIS. Os valores das chaves do metabase são armazenados em um arquivo em disco chamado Metabase.bin.

O metabase é carregado a partir do disco quando o IIS inicia, armazenado no disco quando o IIS fecha, e salvo periodicamente enquanto o IIS está rodando. É importante proteger este arquivo de acessos não autorizados. Recomendamos que o arquivo Metabase.bin seja armazenado em uma partição NTFS, utilizando as permissões do Windows para protegê-lo.

O arquivo Metabase.bin é armazenado no diretório INETSRV. É possível mover ou renomear o arquivo e alterar a configuração do registro do Windows que fixa informa ao IIS onde encontrar o arquivo durante a inicialização. Para mover ou renomear o arquivo de metabase, é necessário parar o IIS, mover ou renomear o arquivo e alterar o a chave LOCAL_MACHINE\SOFTWARE\Microsoft\INetMgr\Parameters no registro. Adicione um valor REG_SZ com o nome MetadataFile nesta chave. O valor de MetadataFile especifica o caminho completo do novo arquivo de metabase, incluindo a letra do drive e o nome de arquivo.

Proteger o Microsoft Certificate Server

Como padrão, as páginas ASP instaladas para o Certificate Server não são protegidas. É recomendável remover as páginas ou definir permissões bastante restritivas a essas páginas. Elas ficam situadas no diretório %systemroot%/certsrv. Você deve configurar as seguintes permissões:

Administrators (Controle Total)

Certificate Issuers (Controle Total)

SYSTEM (Controle Total)

Em seguida, inclua os operadores de certificado confiáveis ao grupo Certificate Issuers.

Auditoria

A auditoria é um controle de segurança importante que precisa ser planejado cuidadosamente. As recomendações feitas aqui podem não se encaixar em qualquer ambiente, mas podem ser utilizadas como base para as demais configurações.

Auditar sucesso e falha de Logon/Logoff

A auditoria indica ações que podem representar um risco de segurança e também identificar as contas de usuário responsáveis por tais ações auditadas. A auditoria só informa quais contas de usuário foram usadas para os eventos auditados. Se as senhas estão protegidas adequadamente, podemos chegar até o usuário que tentou realizar os eventos auditados. Porém, se uma senha foi roubada ou se as ações foram realizadas enquanto um usuário estava em sessão, mas longe do computador, a ação poderia ter sido iniciada por alguém diferente da pessoa a quem pertence a conta de usuário.

Aqui estão algumas ameaças de segurança comuns e o tipo de auditoria que pode ajudar a localizá-las:

Ação	Ameaça

Entrada de Hacker usando senhas randômicas	Ativar a auditoria de falha para eventos de logon e logoff.
Entrada usando senha roubada	Ativar a auditoria de sucesso para eventos de logon e logoff. As entradas do log não distinguirão entre os usuários reais e os falsos. O que você estará procurando aqui são atividades incomuns em contas de usuário, como logon em horas estranhas ou em dias quando você não esperaria nenhuma atividade.

Definir o intervalo de sobrescrita para o arquivo de log

Abra o Event Viewer | Log | Log Settings, e defina um tamanho máximo e "Overwrite Events Older Than" para todos os três tipos de log. Se o sistema vai sobrescrever os registros de log depois de apenas alguns dias e o tamanho máximo do arquivo de log é muito pequeno, é necessário conferir os registros de log mais freqüentemente.

Sincronizar data e hora

A precisão da hora do sistema é um pré-requisito para uma trilha de auditoria, porque o conhecimento de quem estava acessando recursos a uma hora específica poderia implicar um usuário. Toda a auditoria, monitoração de eventos e sistema de log está baseado na hora e, conseqüentemente, esta não deve ser alterada.

No caso de múltiplos servidores Web, devemos nos certificar que a data e hora dos mesmos estejam sempre sincronizadas. O modo mais simples de fazer isso, é utilizar o comando NET TIME e definir um servidor como base.

Segurança específica para o Windows 2000

A Microsoft fornece um conjunto de modelos que se aplicam a vários cenários de segurança comuns. Tais modelos de segurança podem ser divididos em duas categorias distintas: Padrão e Incremental. Os modelos padrão ou básicos são aplicados pelo sistema operacional quando é feita uma instalação “limpa”. Caso seja feita atualização, eles não são aplicados. Os modelos incrementais devem ser aplicados depois dos modelos básicos de segurança. Existem quatro tipos de modelos incrementais: Compatível, Seguro, Altamente Seguro e Controlador de Domínio Dedicado.

Como um ponto de partida aplicável à maioria dos servidores Web, recomendamos realizar a importação do modelo de segurança chamado HISECWEB.INF. Este modelo configura automaticamente algumas das diretivas de segurança discutidas neste capítulo. Para obter o modelo HISECWEB.INF, acesse: http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe

Para instalar e utilizar o modelo, realize os seguintes passos:

Copie o modelo para a pasta: \WINNT\SECURITY\TEMPLATES;

Execute o Microsoft Management Console (MMC);

Abra a ferramenta “Security Templates” para ver as configurações deste modelo;

Abra a ferramenta “Security Configuration and Analysis” e carregue o modelo (clicando com o botão direito e escolhendo a opção “Import Template”);

Clique novamente com o botão direito do mouse em “Security Configuration and Analysis” e selecione a opção “Analyze Computer Now”;

Revise os resultados e atualize o modelo se necessário;

Quando você estiver satisfeito com o modelo, clique com o botão direito do mouse em “Security Configuration and Analysis” e selecione a opção “Configure Computer Now”.

Capítulo 4

Serviço de WWW

O serviço de WWW é aquele que permite a navegação de uma página para outra, recebendo as informações disponíveis, através de textos, sons, imagens e animações.

Configuração Geral

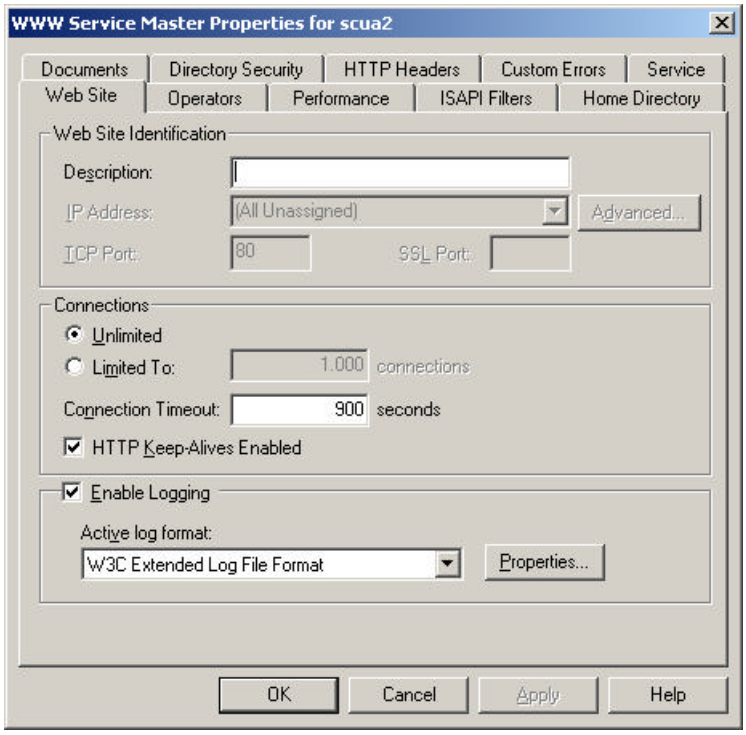
A tela de “Master Properties” é usada para definir os valores padrão usados por todos os sites atuais ou novos de cada servidor. Para acessar esta tela realize o seguinte procedimento:

Clique com o botão direito do mouse sobre o nome do servidor dentro do utilitário ISM (Internet Service Manager);

Selecione a opção “Properties” dentro do menu “Action”;

Selecione o serviço de WWW na lista e pressione o botão “Edit” para configurar as propriedades do servidor selecionado.

Guia "Web Site"



A auditoria é o único item relacionado à segurança disponível nesta tela, mas é fundamental para tentar descobrir se um servidor está sendo atacado. Deste modo, devemos ativar a auditoria de sucesso e falha para as opções "Write", "Delete", "Change Permission" e "Take Ownership".

Recomendamos utilizar o formato W3C Extended Log, selecionando a opção Enable Logging (W3C Extended Log) e definindo as seguintes propriedades:

Client IP Address

User Name

Method

URI Stem

HTTP Status

User Agent

Server IP Address

Server Port

Também é necessário proteger os arquivos de log do IIS. Para isso, recomendamos definir as seguintes as permissões para os arquivos de log gerados pelo IIS (%systemroot%\system32\LogFiles):

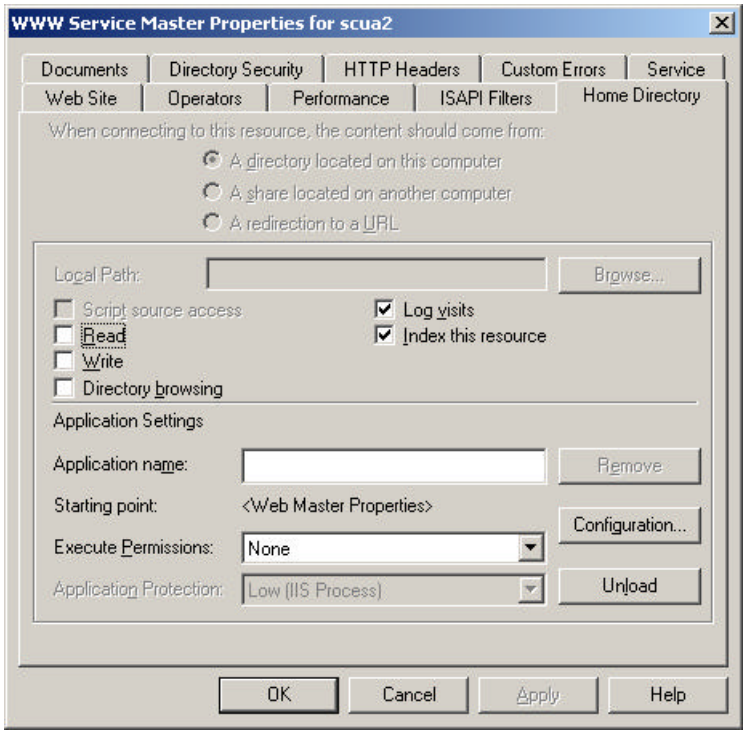
Administradores (Controle Total)

Sistema (Controle Total)

Todos (RWC)

O motivo desta configuração é evitar que usuários maliciosos apaguem os arquivos para cobrir seus rastos.

Guia "Home Directory"



Este é o melhor lugar para se ativar a opção "Log visits" para todos os sites. Isso vai assegurar que todos os sites, mesmo aqueles que forem criados posteriormente, tenham esta opção ativa.

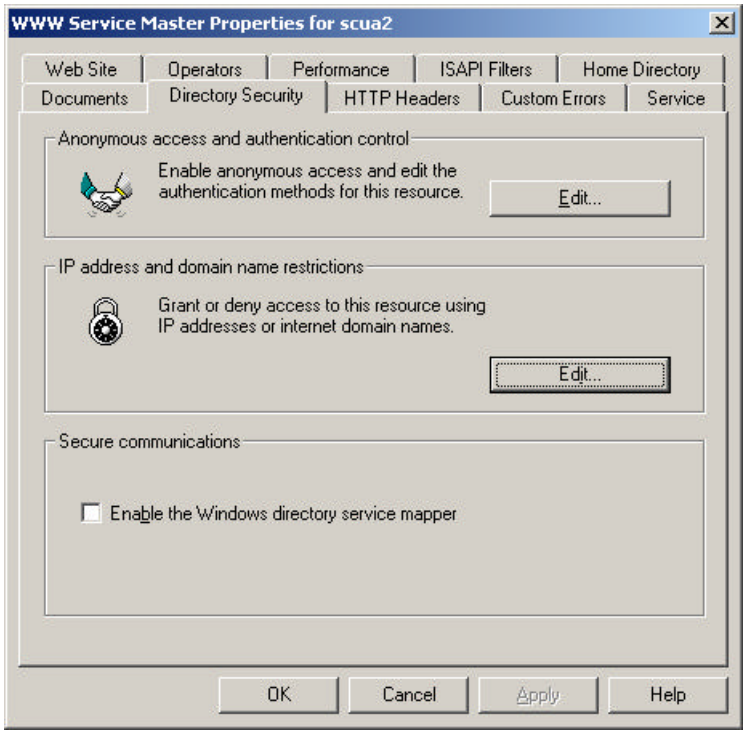
As opções "Read", "Write" e "Directory browsing" devem ser mantidas desativadas, sendo que para cada site criado elas podem ser selecionadas de acordo com a necessidade.

A configuração recomendada para a opção "Execute Permissions" é "None", pois impede que os usuários sejam capazes de rodar "scripts" ou executávies. Esta configuração pode ser alterada, caso necessário, para cada site individualmente.

O IIS é pré-configurado para suportar extensões de arquivos comuns como .ASP e .SHTM. Quando o IIS recebe um pedido para um destes tipos de arquivo, a chamada é processada por uma DLL. Se não estiver utilizando algumas destas extensões ou funcionalidades, você deve remover as seguintes associações através do botão "Configuration":

Se você não usa	**Remova esta entrada**
Troca de senha através da Web	.htr
Internet Database Connector (novos Web sites não usam isto, eles usam ADO de Active Server Pages)	.idc
Server-side includes	.shtm, .stm, .shtml
Impressão via Internet	.printer
Index Server	.htw, .ida e .idq

Guia "Directory Security"



Os métodos de autenticação usados no web site são muito importantes para a identificação dos usuários e controle de acesso a arquivos, diretórios e scripts ou executáveis. A configuração do método de autenticação depende da aplicação, mas é preciso certificar-se que o método de autenticação utilizado seja "forte o bastante" para a aplicação.

Para acessar a tela de configuração dos métodos de autenticação, selecione o botão "Edit" na área "Anonymous access and authentications control" desta tela. A lista a seguir mostra os esquemas de autenticação suportados pelo IIS:

Método de Autenticação	**Nível de Segurança**	**Requisitos do Servidor**	**Requisitos do Cliente**	**Comentários**
Anonymous	Nenhum	IUSR_computername ou conta similar	Qualquer navegador	Usado para áreas públicas em sites Internet
Basic	Baixo	Contas válidas no servidor	Informar nome e senha	Transmite a senha em texto claro
Digest	Alto	Cópia em texto claro de todas as senhas; Contas válidas.	Qualquer navegador que suporte HTTP 1.1	Utilizável através de servidores proxy e firewalls
Integrated Windows	Alto	Contas válidas	Suporte do navegador	Satisfatório para áreas privadas em

				intranets
Certificate	Alto	Obter certificados para o servidor e configurar a lista de certificados confiáveis (apenas para uso inicial)	Suporte do navegador	Largamente utilizado para transações seguras através da Internet
FTP Anonymous	Nenhum	IUSR_computername ou conta similar	Nenhum	Utilizado para áreas públicas em sites FTP
FTP Basic	Baixo	Contas válidas no servidor	Informar nome e senha	Transmite a senha em texto claro

Guia "Server Extensions"

Esta tela permite a configuração das capacidades de desenvolvimento remoto dos sites do IIS. Esta característica está relacionada ao produto FrontPage e permite que o desenvolvedor faça alterações nas páginas e publique-as no servidor remotamente. As recomendações a seguir se aplicam às opções da sessão "Permissions" desta tela:

Selecione a opção "Log authoring actions" para gerar eventos de auditoria quando alguém publicar novas páginas no web site.

Selecione a opção "Manage permissions manually" para desativar as funções de configuração de segurança das ferramentas administrativas do FrontPage Server Extensions, de modo que as ferramentas não possam ser utilizadas para alterar as configurações de segurança do web site.

Selecione a opção "Require SSL for authoring" para forçar a criptografia na comunicação com o servidor.

Desative a opção "Allow authors to upload executable" para evitar que o administrador ou um possível invasor adicione scripts ou executáveis no servidor.

Configuração Específica

A seguir descrevemos as telas de propriedade usadas para configurar o servidor de WWW com segurança. Para acessar esta tela, realize o seguinte procedimento:

Execute o ISM;

Clique com o botão direito do mouse sobre o web site que você deseja configurar, e;

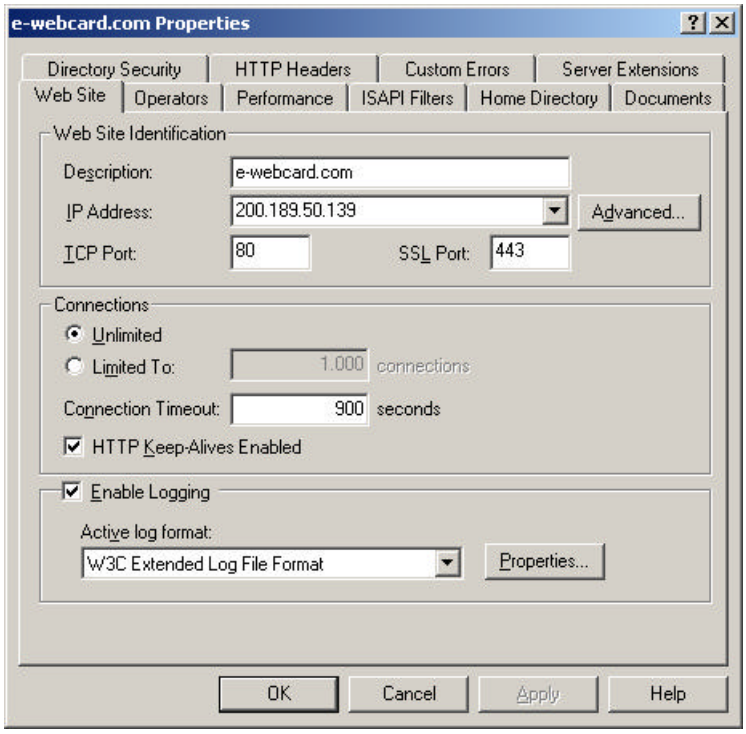
Selecione a opção "Properties".

As aplicações podem ser configuradas com maiores detalhes através do botão "Configuration" na guia "Home Directory". Uma tela separada é mostrada com as seguintes opções: "App Mappings", "App Options", "Process Options" e "App Debugging".

Recomendamos desabilitar ou remover todas as aplicações de exemplo, incluindo a documentação (o documentos do SDK incluem código de exemplo), o site de exemplo Air Exploration entre outros. Alguns exemplos são instalados de modo que possam ser acessados somente por http://localhost ou 127.0.0.1, entretanto também devem ser removidos. A tabela a seguir descreve os locais padrão para alguns dos exemplos:

Tecnologia	Localização
IIS	c:\inetpub\iissamples
SDK do IIS	c:\inetpub\iissamples\sdk
Documentação do IIS	c:\winnt\help\iishelp
Admin Scripts	c:\inetpub\AdminScripts
Acesso a dados	c:\Program Files\Common Files\System\msadc\Samples

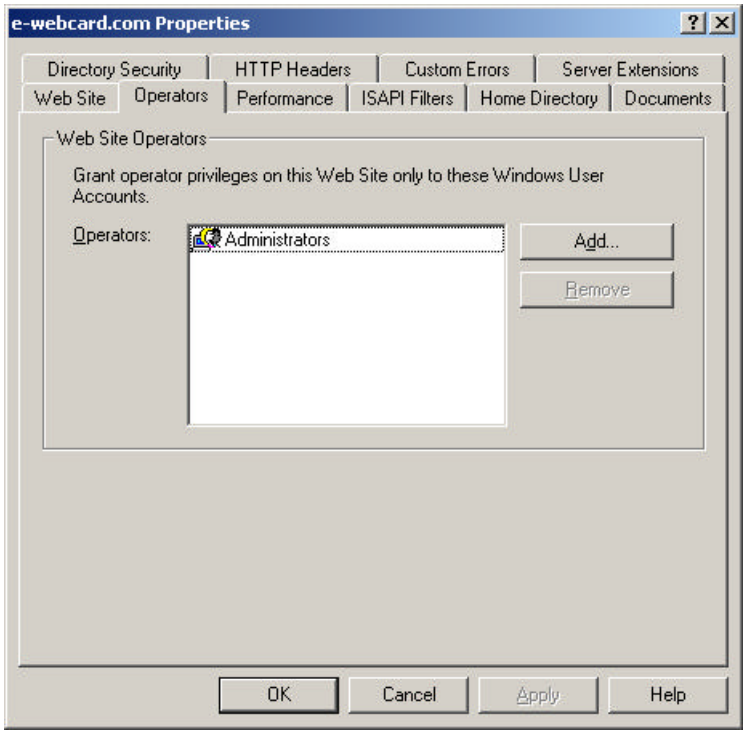
Guia "Web Site"



Ative a opção "Enable Logging" e certifique-se de que a auditoria está configurada conforme definido anteriormente no item "Configuração Geral".

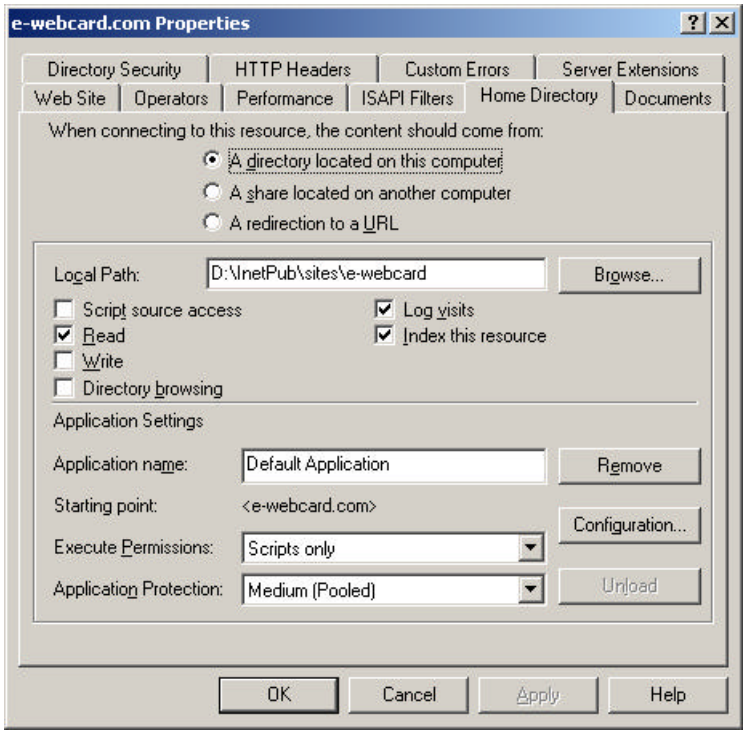
Defina um valor para o "timeout" de conexão para previnir-se de um possível ataque de DoS (Denial of Service).

Guia "Operators"



Nesta tela é possível definir quais são as contas de usuários e/ou grupos do sistema operacional que podem administrar o web site. Recomendamos utililizar um grupo (se servidor pertencer a um domínio) e as contas associadas não necessitam necessariamente de permissões administrativas no sistema operacional. Os operadores podem trabalhar apenas com as propriedades que afetam o web site para o qual foram criados. Devemos impedir o acesso deles às propriedades que controlam a configuração global do IIS, o sistema operacional do servidor que contém o IIS ou a rede onde o sistema roda.

Guia "Home Directory"



Esta tela nos permite visualizar e alterar as configurações que controlam a apresentação do conteúdo do site, as permissões de acesso e a configuração e depuração de código ASP (Active Server Pages). As recomendações a seguir se aplicam à opção "A directory located on this computer" desta tela:

Configure as permissões NTFS conforme descrito no capítulo 3. Por exemplo, HTML e ASP devem ter apenas permissão de leitura, scripts e executáveis devem não devem ter permissão de leitura e devem ser colocados em diretórios separados.

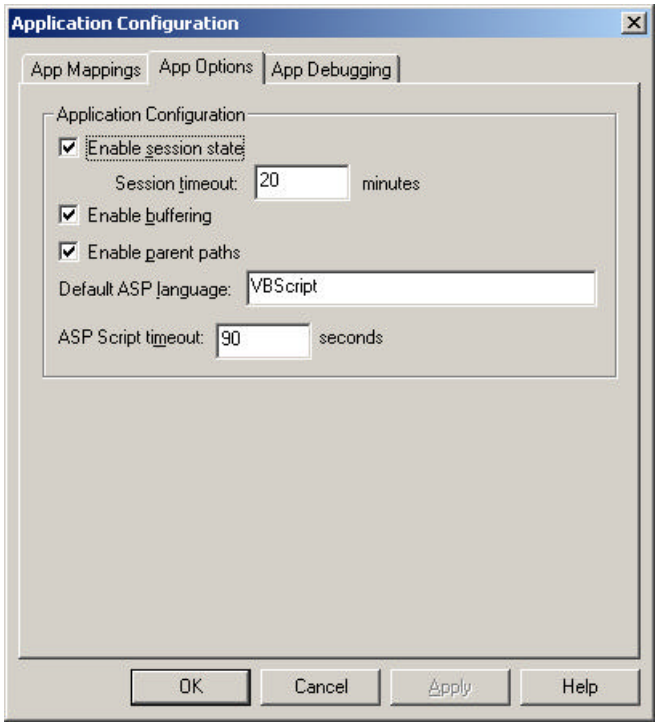
Desativar a opção "Directory Browsing", pois caso nenhum documento padrão seja enviado para o cliente quando o site é acessado, não é possível obter a listagem do diretório.

Desabilitar a opção "Script Source Access" para evitar que os usuários acessem os arquivos fonte.

Recomendamos ativar a opção "Log visits" para assegurar que todos os acessos a este diretório sejam monitorados.

A opção "Execute Permissions" controla a execução de aplicações localizadas no diretório. Para evitar a execução de programas e scripts, ative a opção "None".

Guia "App Options"



Estas opções podem ser configuradas nos níveis de web site, diretório virtual e diretório. As recomendações são:

Ativar as opções "Session state" e "Session timeout" para que seja criada uma nova sessão para cada usuário que acesse uma aplicação ASP.

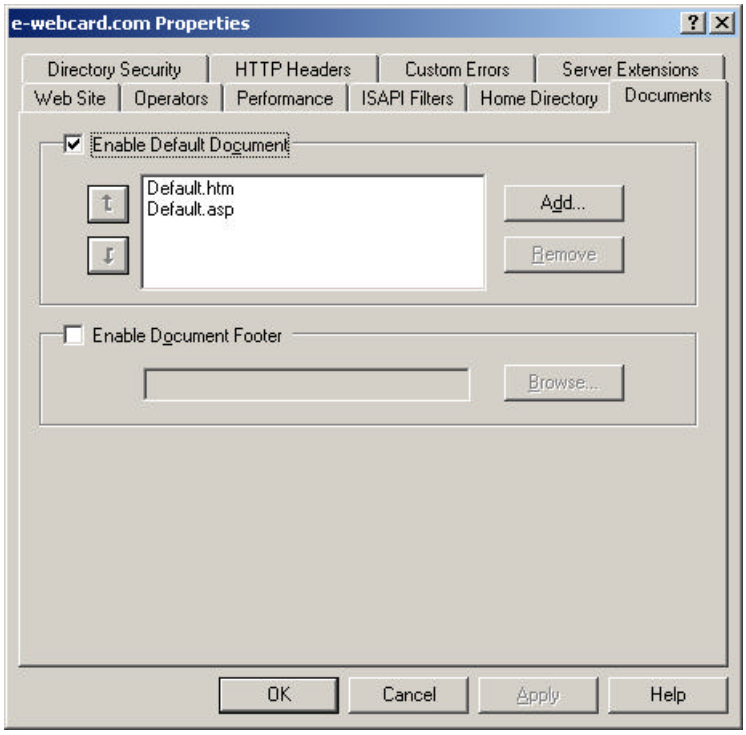
Definir um valor para a opção "ASP script timeout", pois caso um script não complete a execução dentro do tempo definido, um registro de log será gerado e a execução do script será finalizada. Isso ajuda a previnir um ataque de DoS.

É recomendável desabilitar a opção "Parent Paths", pois esta opção é habilitada como padrão e através dela é possível utilizar '..' em chamadas de MapPath e outras do mesmo gênero.

Guia "Process Options"

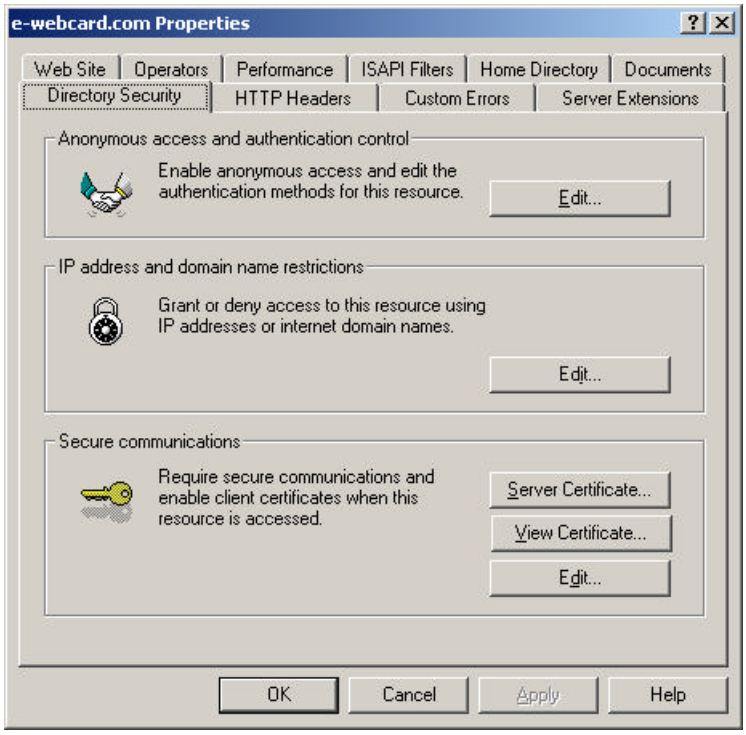
Nesta tela, ative a opção "Write unsuccessful client requests to event log". Entretanto, esta opção estará disponível somente se estiver configurada Alta proteção de aplicação.

Guia "Documents"



Recomendamos sempre fornecer um documento padrão que todos os usuários verão ao acessar o site. Esta configuração ajuda a evitar que a estrutura de diretórios do site seja exibida a um usuário.

Guia "Directory Security"



As propriedades de segurança podem ser definidas nos níveis de web site, diretório, diretório virtual e arquivo. Portanto, o método de autenticação pode ser configurado conforme definido anteriormente no item “Configuração Geral”.

Para definir quem pode acessar o site WWW baseado no endereço IP, configure as restrições de endereço IP / endereço DNS. Note que se você fornece os nomes DNS então o IIS tem que fazer uma busca que pode consumir tempo.

A opção “Secure Communications” é utilizada para configurar as características de SSL/TLS (Secure Sockets Layer) disponíveis no servidor web. O SSL/TLS pode ser usado para proteger os dados no momento em que é transferido do cliente para o servidor Web. O SSL/TLS é usado principalmente quando senhas ou cartões de crédito serão transferidos pela Internet. Porém, o uso do SSL/TLS torna a transferência mais lenta, especialmente durante a negociação inicial do protocolo. Portanto, é recomendável minimizar o conteúdo e a quantidade de páginas que usam SSL/TLS.

Guia “Server Extensions”

O IIS permite publicação remota, ou seja, fazer alterações em uma página web e publicar uma nova página no servidor através dos produtos FrontPage e Visual Interdev. Recomendamos fortemente que a opção “Enable authoring” seja desativada para cada web site no servidor.

Caso exista a necessidade de permitir a publicação remota, configure as seguintes opções:

- Ativar a opção “Version control” para manter um registro de quem esta modificando o conteúdo do web site, identificar alterações e evitar que as alterações de um desenvolvedor remova as de outro.
- Ativar a opção “Don’t inherit security settings”, e definir “Log authoring actions”, “Require SSL for authoring” e “Manage permission manually”, pois apesar de estarem selecionadas no item Configuração Geral, é recomendável definí-las novamente.

Recomendações para desenvolvedores

Muitos sites usam entradas do usuário para chamar outro código ou construir declarações SQL diretamente. Em outras palavras, eles tratam as entradas como válidas, bem formadas e nao maliciosas. Isto não deveria ser assim, pois existem vários ataques, mais frequentemente em Unix onde as entradas do usuário são tratadas incorretamente como entradas válidas e o usuário pode ganhar acesso ao servidor ou causar danos. É recomendável conferir todas as entradas de usuário <FORM> antes de repassá-las para outro processo ou as chamadas de métodos que podem usar um recurso externo como o sistema de arquivos ou um banco de dados.

A verificação do texto pode ser feita através das funcionalidades do JScript e do VBScript. O exemplo de código a seguir remove todos os caracteres inválidos (qualquer um exceto 0-9, a-z, A-Z e _) de uma string:

```
Set Reg = New RegExp
```

```
reg.Pattern = "\W+" ' Um ou mais caracteres que não
sejam 0-9 a-z A-Z ou '_'

strUnTainted = reg.Replace(strTainted, "")
```

O exemplo a seguir remove todo o texto depois de um operador '|':

```
Set Reg = New RegExp

reg.Pattern = "^(.+)\|(.+)" ' Qualquer caracter
desde o começo da string até um '|'

strUnTainted = reg.Replace(strTainted, "$1")
```

Também é preciso ter cuidado caso a abertura ou criação de arquivos estiver sendo feita usando o Scripting File System Object, onde o nome do arquivo está baseado em entradas do usuário, o usuário pode tentar abrir uma porta serial ou impressora. O seguinte código JScript remove nomes de arquivos inválidos:

```
var strOut =
strIn.replace(/(AUX|PRN|NUL|COM\d|LPT\d)+\s*$/i,"")
;
```

Capítulo 5

Serviço de FTP

O FTP (File Transfer Protocol) é um protocolo de comunicação utilizado para:

- promover o compartilhamento de arquivos (programas de computador ou dados);
- encorajar o uso indireto ou implícito (via programas) de computadores remotos;
- transferir dados de maneira confiável e eficaz.

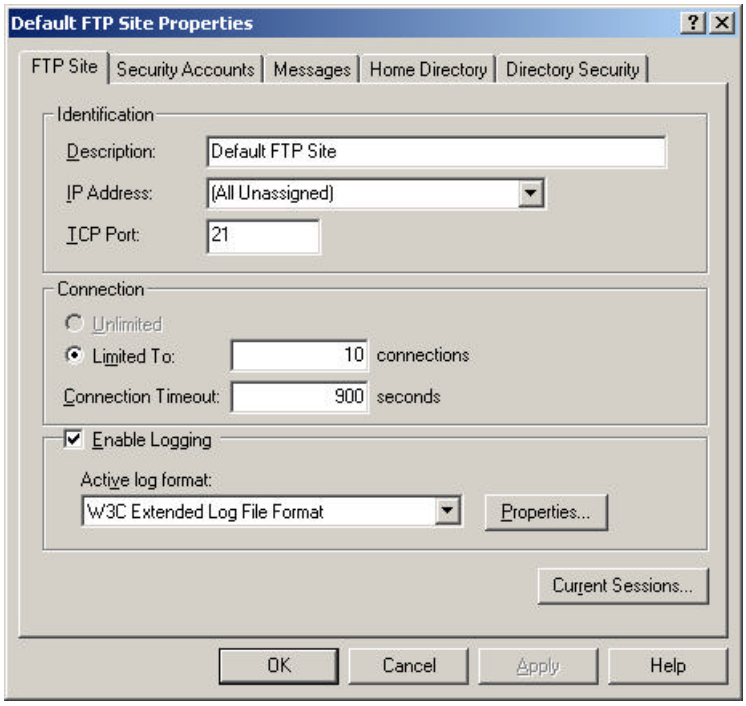
Embora seja possível utilizar o FTP diretamente através de um terminal, o protocolo foi projetado principalmente para uso através de programas.

O FTP utiliza a porta 21 (TCP) e está definido na RFC 959 (http://www.freesoft.org/CIE/RFC/959/index.htm).

Configuração Geral

A tela de configuração das propriedades gerais do serviço de FTP tem menos opções disponíveis do que para o serviço de WWW. Para acessar tais propriedades, basta acessar a tela de propriedades do servidor IIS, selecionar FTP Service e clicar no botão Edit.

Guia "FTP Site"



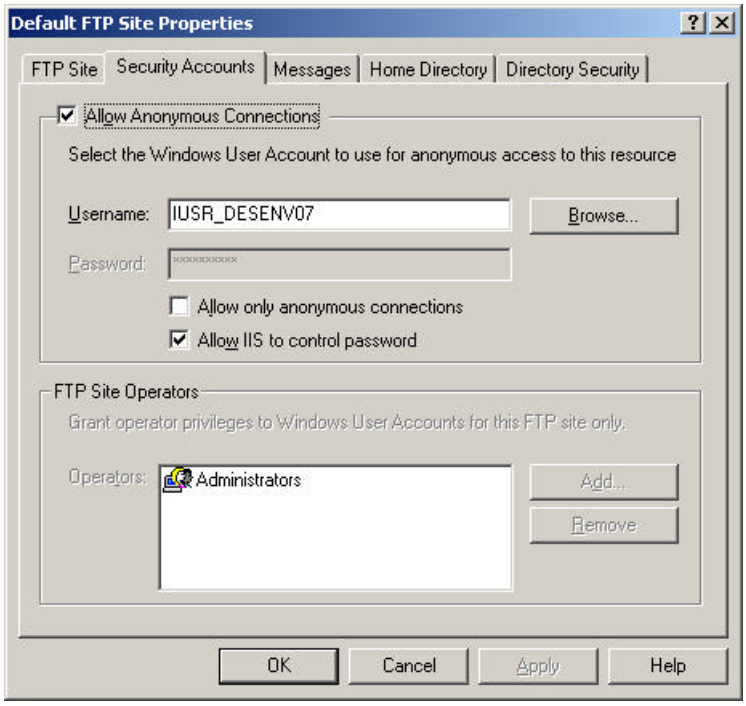
Recomendamos definir as seguintes opções:

Configurar o número máximo de conexões de acordo com a quantidade esperada de usuários.

Configurar um valor máximo para o limite de duração da conexão para permitir um melhor controle sobre ataques de DoS e consumo de recursos do servidor.

Ativar "Enable Logging" conforme visto anteriormente no capítulo 4 para assegurar que esta opção não seja esquecida conforme os sites são adicionados.

Guia "Security Accounts"

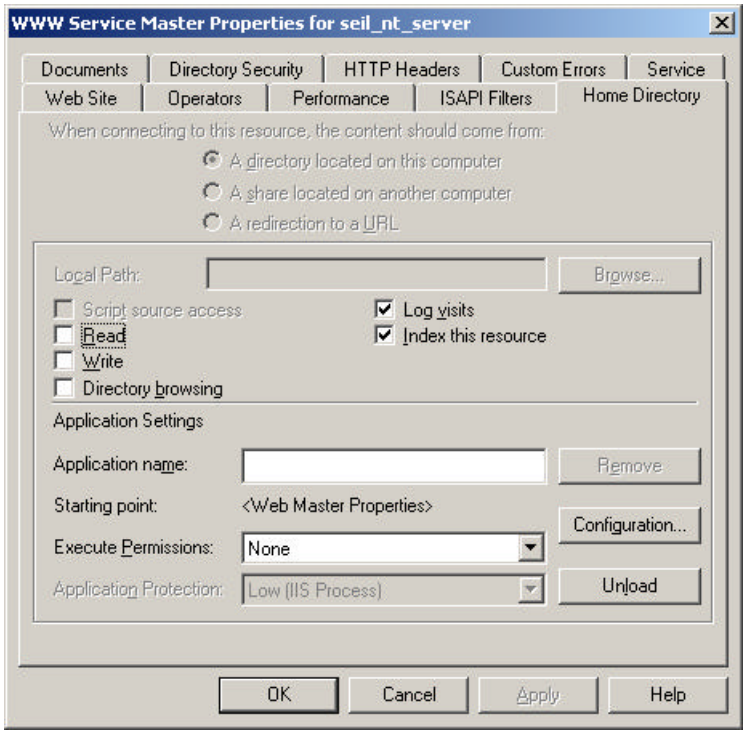


De forma similar à tela de propriedades do serviço de WWW, o acesso anônimo ao servidor de FTP pode ser configurado aqui. Se o servidor de FTP estiver disponível na Internet e o acesso anônimo for permitido, recomendamos a seguinte configuração:

Selecione as opções "Allow Anonymous Connections" e "Allow only anonymous connections" para impedir que os usuários efetuem logon através de nome e senha válidos, que são enviados abertamente, evitando possíveis ataques usando a conta de um administrador

Selecione a opção "Allow IIS to control password" no IIS 5.0 e "Enable automatic password synchronization" no IIS 4.0 para associar o nome e a senha do usuário anômimo de FTP (geralmente IUSR_Computername) com a conta criada no sistema operacional.

Guia "Home Directory"



Esta tela tem apenas uma opção relacionada com segurança: "Log visits". Diferente de algumas outras opções que dependem da implementação do servidor, esta opção deve estar sempre ativada do ponto de vista da segurança.

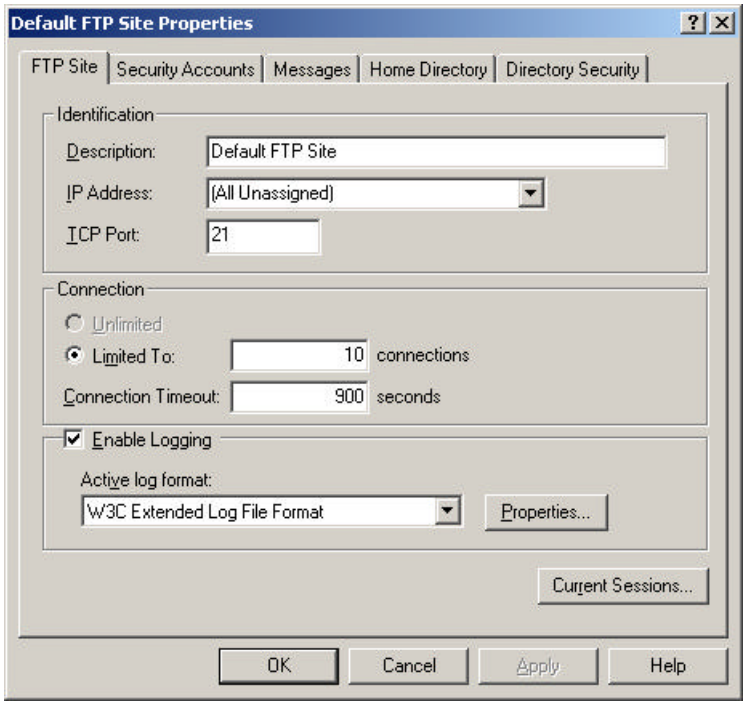
Configuração Específica

O diretório c:\inetpub\ftproot precisa de atenção especial, pois possui permissão de controle total para o grupo Todos e deve ser configurado com maior restrição dependendo do nível de funcionalidade desejado. Coloque a pasta em um volume diferente do servidor IIS se você for dar permissão de escrita para o grupo Todos.

Recomendamos ainda que os diretórios de FTP sejam organizados para os usuários. Para os downloads via FTP, os nomes dos diretórios devem refletir o seu conteúdo e ter apenas permissão de leitura.

A seguir mostramos as telas disponíveis para configurar as propriedades do FTP. Acesse as telas clicando sobre o site de FTP no Internet Service Manager e selecionando as propriedades no menu Action.

Guia "FTP Site"



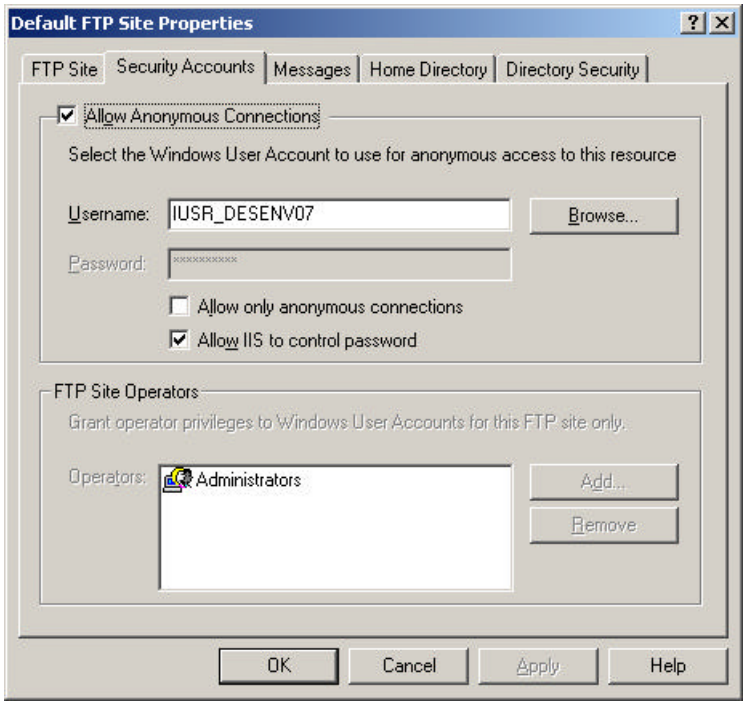
Esta tela contém as mesmas propriedades que a guia a "Web Site", mas que aplicam-se especificamente ao serviço de FTP. Recomendamos definir as seguintes opções:

Configurar o número máximo de conexões de acordo com a quantidade esperada de usuários.

Configurar um valor máximo para o limite de duração da conexão para 600 segundos.

Ativar a opção "Enable Logging" conforme visto anteriormente no capítulo 4.

Guia "Security Accounts"

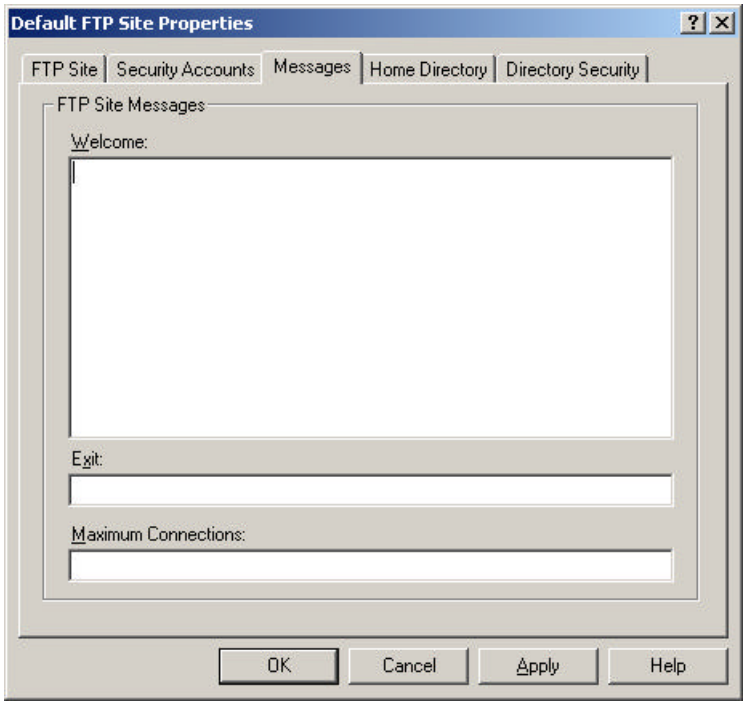


Esta tela é usada para configurar o acesso anônimo e os operadores locais do FTP. Recomendamos definir as seguintes opções:

Selecione as opções "Allow Anonymous Connections" e "Allow only anonymous connections" para impedir que os usuários efetuem logon através de nome e senha válidos, que são enviados abertamente, evitando possíveis ataques usando a conta de um administrador

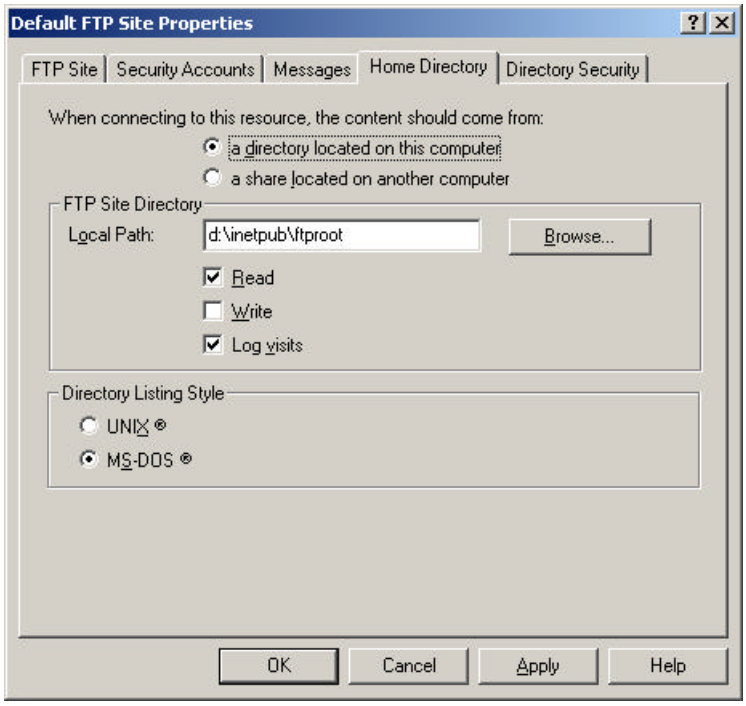
Selecione a opção "Allow IIS to control password" no IIS 5.0 e "Enable automatic password synchronization" no IIS 4.0 para associar o nome e a senha do usuário anômimo de FTP (geralmente IUSR_Computername) com a conta criada no sistema operacional.

Guia "Messages"



Há três tipos de mensagens que podem ser exibidas para os usuários: "Welcome", "Exit" e "Maximum Connections". Recomendamos que a mensagem de "Welcome" seja feita na forma de uma Notificação de Segurança e exibida a qualquer usuário que se conecta no servidor de FTP.

Guia "Home Directory"

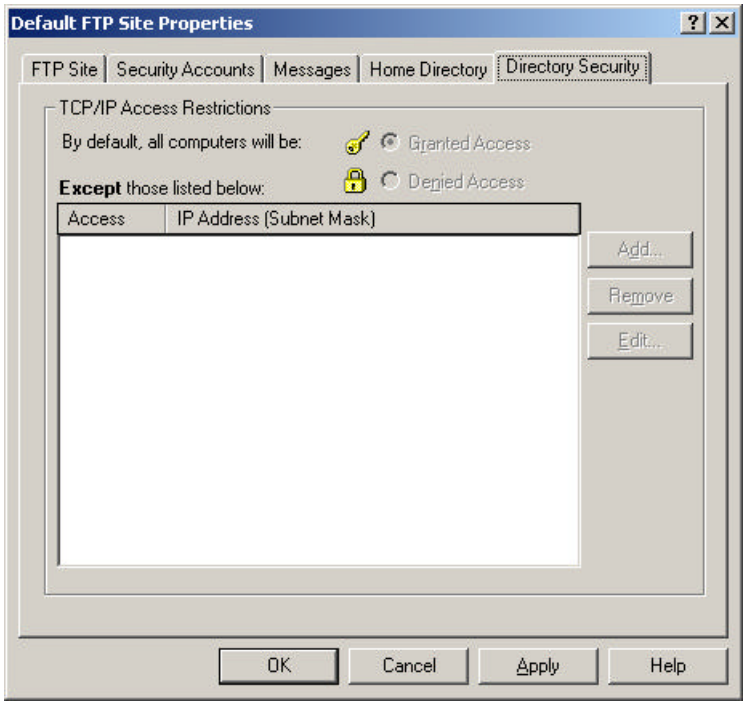


Esta tela é usada para especificar de onde vem o conteúdo (de um diretório localizado no computador ou de um compartilhamento de rede localizada em outro computador). Também é possível configurar o caminho local para o diretório, as permissões de acesso e o estilo de listagem de diretórios que o IIS envia ao cliente. Recomendamos definir as seguintes opções:

Certifique-se de que a opção “Log Visits” esteja selecionada.

Certifique-se de que o diretório FTPROOT tenha apenas pesmissão de leitura.

Guia “Directory Security”



Esta tela permite a especificação de quem pode acessar o site de FTP baseado no endereço de IP.

Capítulo 6

Serviço de SMTP

O SMTP (Simple Mail Transfer Protocol) é um protocolo que permite enviar, receber e armazenar mensagens (correio eletrônico).

Um usuário, ao desejar enviar uma mensagem, utiliza uma interface para compor a mensagem e solicita ao sistema de correio eletrônico que a entregue ao destinatário. Quando recebe a mensagem do usuário, o sistema de correio eletrônico armazena uma copia da mensagem junto com o horário do armazenamento e a identificação do remetente e do destinatário. O processo de transferencia de mensagens mapeia o nome da maquina de destino baseado em seu endereço IP, e tenta estabelecer uma conexão TCP com o servidor de correio eletrônico da maquina de destino.

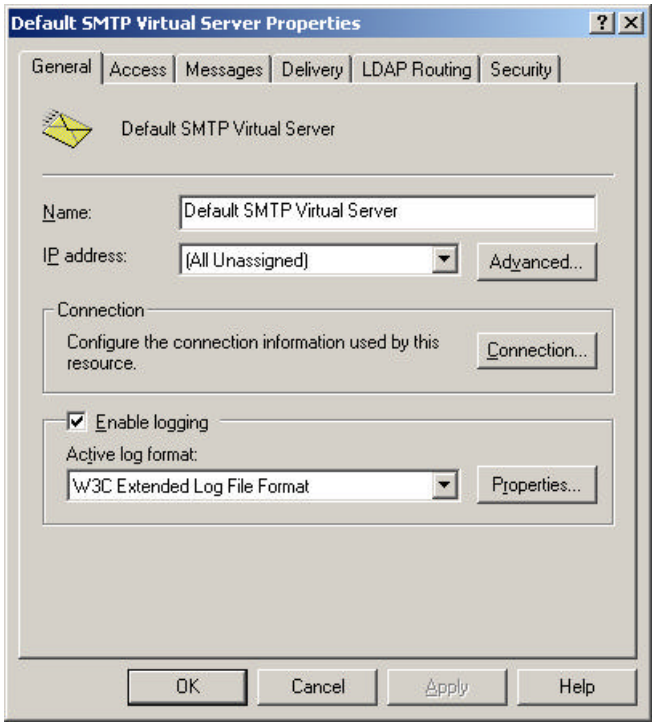
O SMTP utiliza a porta 25 (TCP) e está definido na RFC 821 (http://www.freesoft.org/CIE/RFC/821/index.htm).

Configuração

O diretório c:\inetpub\mailroot precisa de atenção especial, pois possui permissão de controle total para o grupo Todos e deve ser configurado com maior restrição dependendo do nível de funcionalidade desejado. Coloque a pasta em um volume diferente do servidor IIS se você for dar permissão de escrita para o grupo Todos.

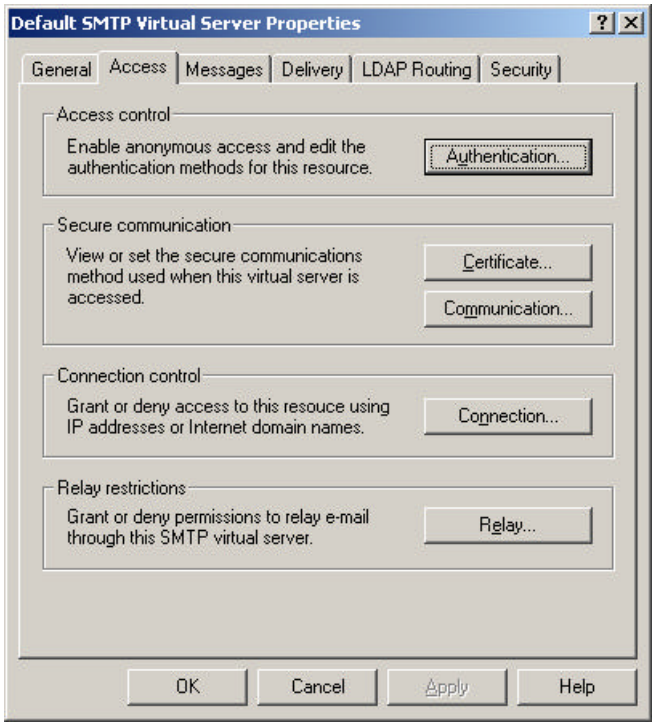
A seguir mostramos as telas disponíveis para configurar as propriedades do SMTP. Acesse as telas clicando sobre o site de SMTP no Internet Service Manager e selecionando propriedades no menu Action.

Guia "General"



Esta tela permite que o administrador controle várias opções gerais do servidor de SMTP. Recomendamos ativar a opção "Enable Logging" conforme visto anteriormente no capítulo 4.

Guia "Access"



Através desta tela é possível configurar as seguintes características:

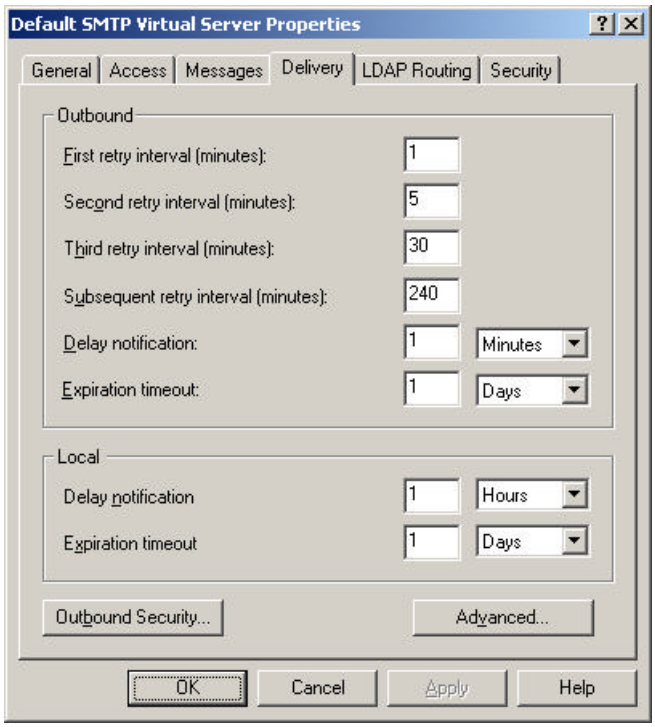
Autenticação: as opções de autenticação são similares àquelas já mencionadas nos outros serviços. Dependendo do uso do servidor, diferentes recomendações são necessárias.

Comunicação: Se selecionarmos a opção “Require TLS encryption” todas as mensagens que chegam são criptografadas. Então, selecione as opções “Required secure channel” e “Required 128 bits encryption” para maximizar a proteção dos dados que trafegam entre os clientes e o servidor contra acesso não autorizado.

Conexão: funciona da mesma forma que da mesma forma que o bloqueio de domínios dos serviços de WWW, FTP. Defina aqui as restrições de endereços IP e Domínios.

Relay: o conceito desta opção é similar à configuração das restrições de endereço IP e domínios. Selecione a opção “Only the List Below” para definir os computadores que poderão enviar e-mail através deste servidor. Desative a opção “Allow all computers which successfully authenticate to relay, regardless of the list above” para impedir que o servidor seja utilizado para “spam”.

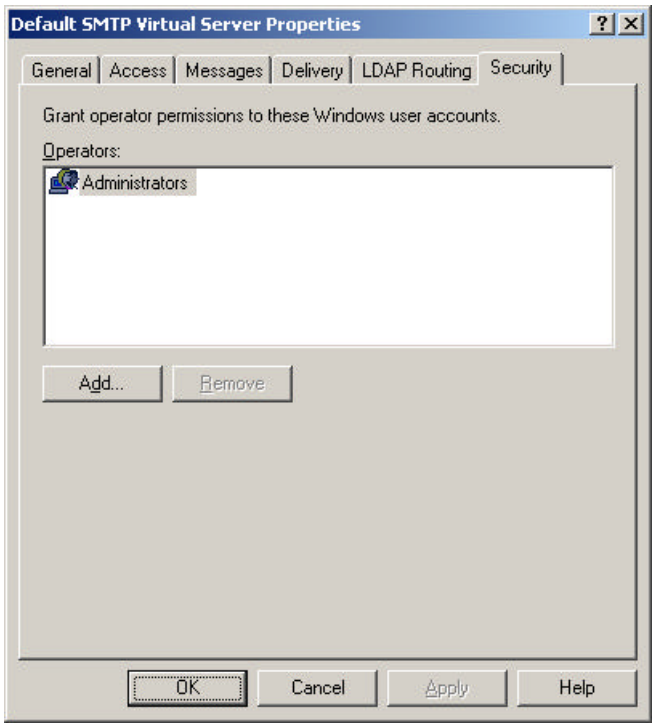
Guia “Delivery”



Esta tela define o tipo de autenticação para o envio de e-mail. A escolha do tipo de autenticação/criptografia deve ser compatível com o servidor do outro lado da conexão, o que torna impraticável qualquer configuração de segurança no envio de mensagens se o servidor estiver enviando mensagens para um ambiente heterogêneo como a Internet.

Se o servidor estiver operando em uma Intranet e estiver enviando informações confidenciais, recomendamos o uso de, no mínimo “Basic Athentication”, incluindo criptografia TLS se possível.

Guia "Security"



Esta tela nos permite definir o usuário ou grupo de usuários responsável pela administração do serviço. Ao contrário dos serviços de WWW e FTP, existe a possibilidade de criar grupos locais para administrar as contas de usuário. Recomendamos o seguinte procedimento:

Adicionar um grupo local chanado *SMTPAdmin* com privilégios de operador.

Capítulo 7

Serviço de NNTP

O NNTP (Network News Transport Protocol) é um protocolo que permite a distribuição, solicitação, recuperação e publicação de notícias usando uma transmissão segura entre a comunidade de Internet.

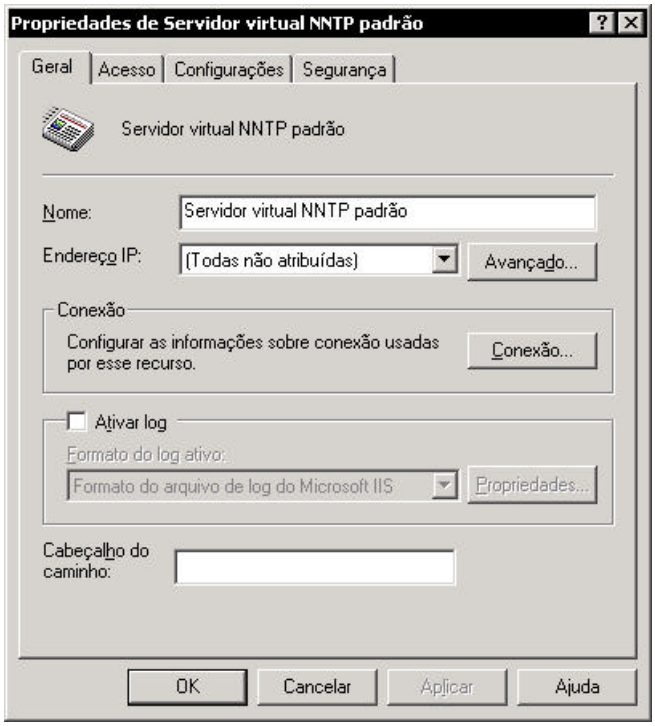
O NNTP foi projetado de forma que as notícias são armazenados em um banco de dados central que permite a um assinante selecionar somente os itens que deseja ler. Também são fornecidas funções de indexação, referência cruzada e expiração de mensagens antigas.

O NNTP utiliza a porta 119 (TCP) e está definido na RFC 977 (http://www.freesoft.org/CIE/RFC/977/index.htm).

Configuração

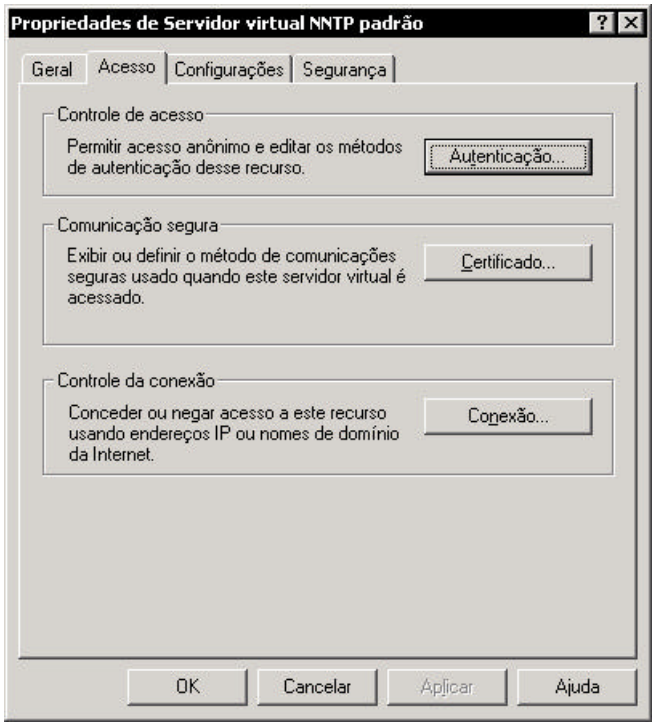
A seguir mostramos as telas disponíveis para configurar as propriedades do NNTP. Acesse as telas clicando sobre o site de NNTP no Internet Service Manager e selecionando propriedades no menu Action.

Guia "General"



Recomendamos ativar a opção "Enable Logging" conforme visto anteriormente no capítulo 4.

Guia "Access"

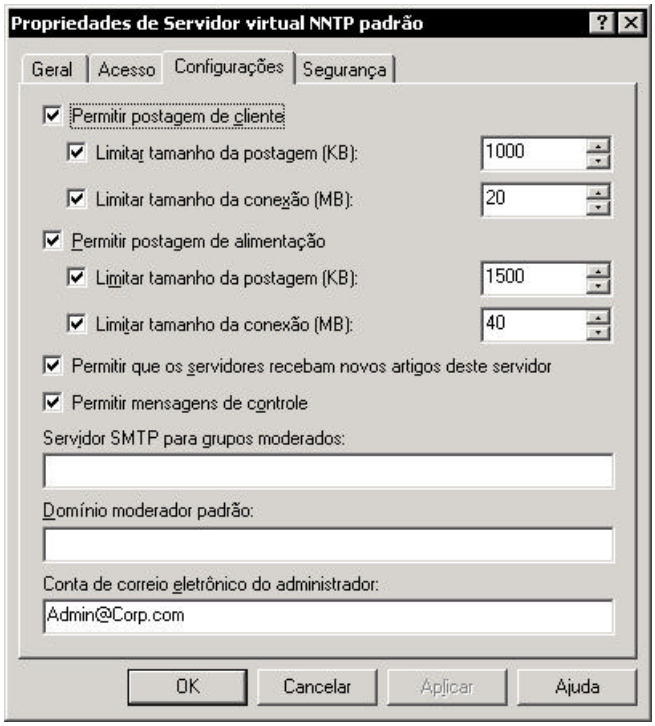


Através desta tela é possível configurar as seguintes características:

Autenticação: define o método de autenticação utilizado pelos usuários para se conectar ao servidor de notícias. Se um firewall estiver sendo utilizado para proteger a entrada, recomendamos desabilitar a opção “Allow Anonymous”. Procure utilizar SSL, especialmente com “Basic Authentication” (requer certificado).

Conexão: funciona da mesma forma que da mesma forma que o bloqueio de domínios dos serviços de WWW, FTP e SMTP. Defina aqui as restrições de endereços IP e Domínios.

Guia “Settings”

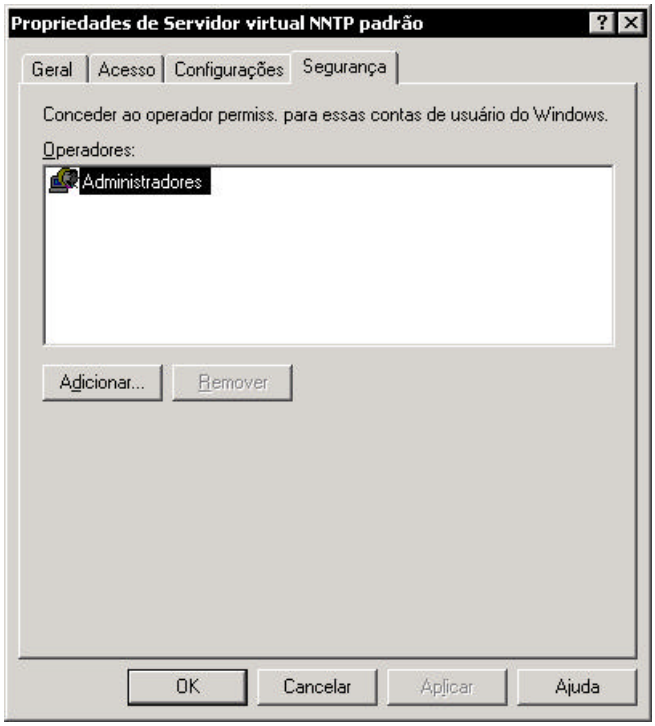


Nesta tela existem várias funcionalidades que podem ser personalizadas, tais como o tamanho das mensagens, quem pode postá-las, servidor de SMTP e informações do moderador. Há duas opções nesta tela que devem ser configuradas:

Desabilitar a opção “Allow servers to pull news articles” para evitar que as mensagens postadas no servidor sejam propagadas para todos os servidores NNTP do mundo.

Desabilitar a opção “Allow control messages” para evitar que usuários maliciosos removam mensagens ou grupos de notícias.

Guia "Security"



Esta tela nos permite definir o usuário ou grupo de usuários responsável pela administração do serviço. Ao contrário dos serviços de WWW e FTP, existe a possibilidade de criar grupos locais para administrar as contas de usuário. Recomendamos o seguinte procedimento:

Adicionar um grupo local chanado *NNTPAdmin* com privilégios de operador.