IMPLEMENTANDO SEGURANÇA NO WINDOWS NT 4.0

Fernando Antonio M. Cima, MCSE+Internet
Versão 1.0. Brasília, DF – 1998

1. Sumário

Com o seu enorme sucesso e o crescente uso, o Windows NT passou a ser utilizado nos mais diversos cenários e funções, incluindo a Internet, atraindo a atenção tanto de especialistas em segurança como de hackers. Como resultado, nos últimos meses diversos "furos" de segurança foram descobertos e várias redes baseadas em NT tiveram sua segurança comprometida.

Apesar disto, o Windows NT é um dos mais seguros sistemas operacionais de rede, quando configurado adequadamente. A intenção deste documento é mostrar alguns passos simples que, se seguidos, aumentam dramaticamente a segurança de uma rede Windows. Acredito que a adoção destas recomendações pode ser feita sem acarretar problemas na maioria dos ambientes, e de forma rápida e fácil de ser entendida.

Neste documento não serão colocados sugestões para permissões em arquivos e diretórios. Estas permissões variam enormemente em razão dos softwares instalados e das necessidades de segurança de cada sistema, e uma formula pronta acarretaria necessariamente problemas. A Microsoft fez uma recomendação de permissões em seu texto "Guidelines to Security a NT Installation"; no entanto esta recomendação causa problemas com diversos programas, notadamente o próprio Microsoft Office. Com as futuras normas ZAW no NT 5 uma estrutura coerente de permissões deverá ser possível.

1.1 Audiência

Este tutorial se destina a administradores e gerentes de rede, principalmente os que, mesmo já tendo experiência em ambientes Unix e Novell, estejam iniciando na administração de uma rede NT. No entanto, acredito que mesmo profissionais experientes podem tirar proveito dos tópicos abordados aqui.

2. Antes de começar, aplique as correções.

Não se pode pensar em segurança de um sistema se existem nele furos conhecidos de segurança que não foram corrigidos. Desta forma, é essencial que suas máquinas estejam utilizando a versão mais atualizada do sistema operacional.

A Microsoft divulga atualizações periódicas gratuitas do Windows NT, conhecidas como *Service Packs*. Estas atualizações são numeradas a medida em que são divulgadas (Service Pack 1, Service Pack 2, etc.), e contém correções de erros, melhoramentos e novas características do sistema. Os Service Packs são cumulativos, ou seja, o Service Pack 3 já incorpora todas as alterações dos Service Pack 1 e 2, por exemplo. A instalação do Service Pack mais recente é extremamente recomendável e item de segurança obrigatório em uma boa política de segurança para a rede.

No intervalo entre um Service Pack e outro, erros que porventura sejam descobertos são corrigidos pela Microsoft através de *hotfixes*. Estas correções não são tão exaustivamente testadas como os Service Packs e sua utilização é recomendada apenas onde o defeito seja realmente um problema, como nos casos onde haja ameaça a segurança do sistema.

➡ *Onde encontrar service packs e hotfixes?*

Os Service Packs e hotfixes podem ser obtidos no endereço ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes, ou através do PSS da Microsoft e também nas Microsoft Solution Providers (empresas associadas a Microsoft). Um pequeno guia sobre como deixar o seu sistema atualizado em relação às correções de segurança pode ser encontrado em http://www.aker.com.br/segnt/patch.htm.

3. Um pouco de teoria

Em 1985 a Microsoft lançou o seu primeiro software de rede. Chamado PC-LAN, permitia que usuários do MS-DOS compartilhassem diretórios e impressoras através de uma rede local, e pouca coisa além disso. A segurança fornecida (se é que pode se chamar assim) era uma senha única que podia opcionalmente ser colocada em cada compartilhamento. Talvez adequado para "micros", como eram chamados com certo desprezo na época, mas ainda longe do que era oferecido por sistemas operacionais mais avançados como o VMS e o Unix.

Apesar da precariedade, o PC-LAN teve um razoável sucesso e motivou mais investimentos da Microsoft na área. A cada novo produto lançado (OS/2 Lan Manager, Windows for Workgroups, Windows NT) novos recursos foram adicionados, tornando o que era um protocolo simples em um complexo conjunto de rotinas, que em sua maioria não eram documentadas até bem pouco tempo atrás. A este conjunto, que faz além do compartilhamento de recursos também autenticação de usuários, *browsing* e resolução de nomes, damos o nome genérico de "Rede Microsoft".

Desde o começo, a Microsoft adotou como padrão o NetBIOS como o protocolo de comunicação de todos os seus sistemas operacionais de rede. Desenvolvido pela IBM, o NetBIOS é uma interface de programação permite que dois programas em máquinas diferentes se comuniquem de forma confiável, independente do protocolo de transporte que esteja sendo utilizado. Todos os componentes da Rede Microsoft utilizam as rotinas do NetBIOS para trocar informação e proverem os seus serviços.

O NetBIOS pode rodar sobre três protocolos de transporte: NetBEUI, IPX/SPX ou TCP/IP.

O NetBEUI é basicamente o NetBIOS colocado diretamente no fio, apenas acrescentando a informação de controle do meio físico; é mais adequado em pequenas redes onde exista apenas um único segmento, onde fornece performance imbátivel. Com um número maior de máquinsa ou em uma topologia mais complexa, no entanto, ele fica insuportavelmente lento ou simplesmente não funciona. O NetBEUI não é necessário se você já estiver utilizando TCP/IP ou IPX/SPX.

O IPX/SPX, protocolo desenvolvido pela Novell, é utilizado primariamente para a comunicação com servidores Netware, mas também pode transportar o NetBIOS. Também não é necessário utilizar o IPX/SPX quando você já estiver utilizando o TCP/IP; muito pelo contrário, deve-se evitar a utilização de mais de um protocolo de transporte. Utilizar dois ou mais lhe darão uma avalanche de tráfego inútil em sua rede, além de algumas dores de cabeça por causa de alguns conflitos entre os redirecionadores. Caso você realmente precise utilizar o IPX/SPX como segundo protocolo por causa de algum servidor Novell em sua rede, desabilite a ligação do NetBIOS com o IPX para evitar estes problemas (veja como fazer isto mais a frente).

O TCP/IP é o protocolo utilizado na Internet, e que também pode servir de transporte para os serviços da Rede Microsoft. Utilizando o TCP/IP, por exemplo, você pode de sua casa, através da Internet, acessar um compartilhamento ou imprimir na impressora do seu escritório. O lado ruim é que isto abre uma porta para qualquer outra pessoa também possa, e esta é a causa da maioria dos incidentes de segurança envolvendo redes NT.

Além do compartilhamento de recursos, a Microsoft incorporou aos seus sistemas operacionais um mecanismo para que o usuário em uma máquina possam executar rotinas e programas em outras máquinas da rede. Este mecanismo, chamado RPC (*remote procedure call*), é utilizado por exemplo quando você gerencia a fila de impressão de um servidor remoto, ou utiliza o Server Manager para controlar as máquinas de um domínio. O funcionamento é similar ao RPC encontrado nos Unix, apesar de não serem o mesmo protocolo.

O que acontece quando eu tenho mais de um protocolo instalado no meu Windows? Há algum problema?

A Rede Microsoft irá utilizar todos os protocolos que estiverem instalados. A forma como isto vai ocorrer varia um pouco nestes casos, dependendo da versão. Até o NT 3.1 (e Windows 3.11), o Windows tenta cada um dos protocolos (NetBEUI, IPX/SPX e TCP/IP) na ordem de ligação, configurada no painel de controle. Se o primeiro protocolo na ordem não funcionar, é tentado o próximo, e assim por diante.

Devido a eventuais atrasos que este procedimento causava, o NT 3.5 e subsequentes trabalham de forma diferente: ele tenta todos os protocolos ao mesmo tempo, e quando um deles faz a conexão os demais são cancelados. A desvantagem é um significativo aumento do tráfego.

Além do problema de se ter uma enorme quantidade de tráfego absolutamente desnecessário, no dia a dia se observam alguns problemas em redes com vários protocolos, como compartilhamentos não acessíveis, ambiente de rede com máquinas ausentes e outros. Por estas razões, é altamente recomendável que se escolha qual será o protocolo de rede, que na grande maioria dos casos deverá ser o TCP/IP, e se retirem os outros que estiverem instalados.

4. Isolando a Rede Microsoft

Os serviços da Rede Microsoft foram desenhados originalmente para uma rede local, e é apenas na sua rede local que você provavelmente quer usá-los. O problema é que ao se conectar sua rede via TCP/IP a uma rede corporativa ou a Internet você estará também abrindo a porta para que pessoas de outras redes (ou de todo o mundo, no caso da Internet) tenham acesso aos seus recursos, e possa por exemplo compartilhar os seus diretórios via NetBIOS ou gerenciar suas máquinas e usuários por RPC.

De fato a enorme maioria das invasões e outros incidentes de segurança em NTs ligados a Internet utilizaram NetBIOS trafegando sobre TCP/IP como seu canal. Felizmente há um modo simples de evitar que isto aconteça: **impedindo a entrada de NetBIOS em sua rede.** Se você não precisa que pessoas externas utilizem os serviços da sua Rede Microsoft, impedi-los não lhe afetará em nada e aumentará exponencialmente a sua segurança. Hackers e outros não poderão mais acessar os recursos de sua Rede Microsoft, roubar senhas ou tentar derrubar os seus servidores com Winnuke.

Para impedir a entrada de NetBIOS, configure o seu roteador para filtrar (eliminar) os pacotes vindos de redes externas e destinados às seguintes portas de sua rede interna:

TCP porta 135 (utilizado pelo RPC).
UDP portas 137 e 138, TCP porta 139 (utilizado pelo NetBIOS).

Praticamente todos os roteadores (incluindo Cisco, Livingston, Cyclades, 3Com, Linux, NT R&RAS) permitem a implementação destes filtros. Consulte o manual do seu roteador sobre como configurá-lo desta forma.

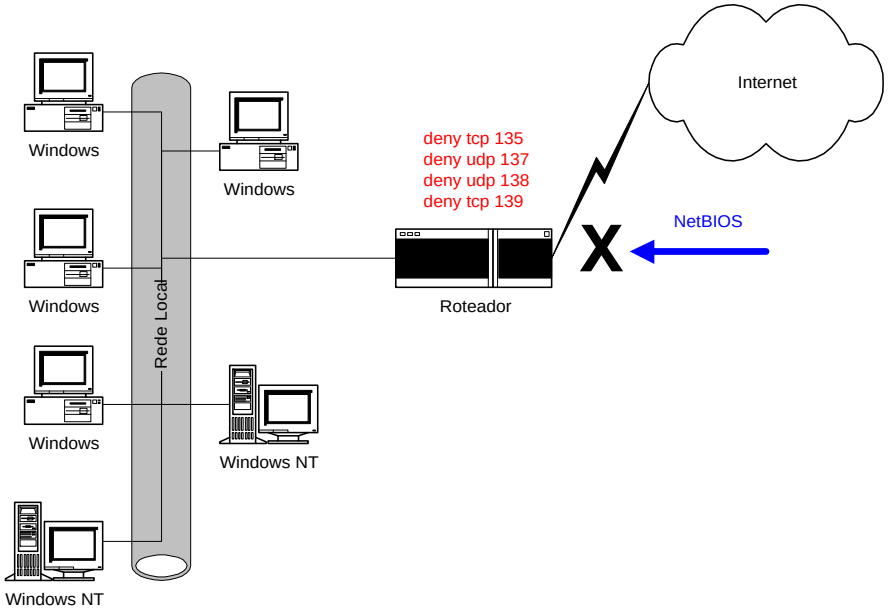

fig 1. Bloqueio da entrada de NetBIOS na rede local. .

5. Retirando ligações desnecessárias

Por ter uma arquitetura de rede extremamente modular, o NT permite que vários protocolos de transporte (NetBEUI, TCP/IP, IPX/SPX) utilizem ao mesmo tempo uma ou mais placas de rede, e que vários serviços de rede como o NetBIOS utilizem também simultaneamente diversos protocolos de transporte. A relação entre cada uma destas camadas é chamada de "ligação": quando o TCP/IP está trabalhando na placa de rede NE2000, dizemos que ele está "ligado" a esta interface. Quando o NetBIOS está utilizando o TCP/IP e o NetBEUI, dizemos que ele está "ligado" a estes protocolos.

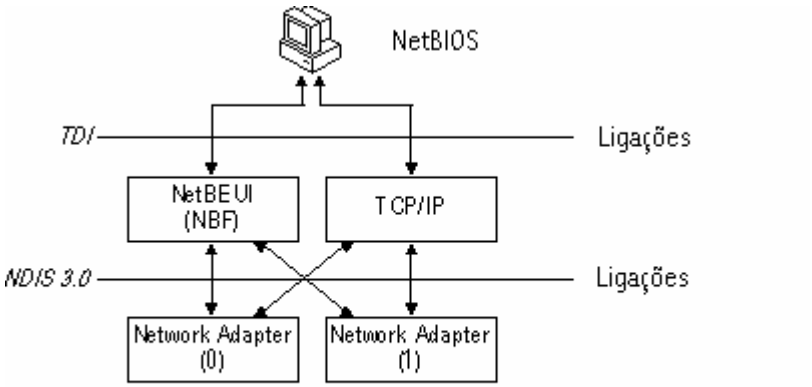

fig 2. Ligações (bindings)

Por default, o NetBIOS se liga a todos os protocolos de rede disponíveis. Ou seja, caso você esteja com NetBEUI e TCP/IP instalados, por exemplo, o NetBIOS (i.e. a rede Microsoft) estará se comunicando utilizando ambos os protocolos. Isto, como já vimos, além de piorar o tempo de conexão, aumenta sobremaneira o tráfego na rede.

Você como administrador pode controlar estas ligações, habilitando ou desabilitando-as conforme a sua necessidade. Por exemplo, suponha que você tenha uma rede rodando TCP/IP e precise instalar IPX/SPX para se comunicar com um servidor Novell Netware. Neste caso, você pode retirar a ligação do NetBIOS com o IPX/SPX, deixando que toda a comunicação da rede Microsoft seja feita pelo TCP/IP e evitando um aumento de tráfego desnecessário.

Em nosso caso, a razão pode ser por segurança. Em máquinas diretamente expostas a Internet ou a outras redes externas, onde não seja possível filtrar o tráfego NetBIOS dirigido à ela no roteador (por exemplo, quando a máquina é um servidor proxy), é recomendável retirar a ligação entre a Rede Microsoft e a placa de rede externa, que conecta a máquina a Internet ou a outras redes. Desta forma, hackers ou pessoas mal-intencionadas não conseguirão acessar compartilhamentos e recursos desta máquina, nem tentar obter senhas, utilizando a Rede Microsoft.

Para retirar a ligação, siga os seguintes passos:

1. Na máquina diretamente ligada a rede externa ou Internet, faça o login como administrador e abra o **Control Panel**. Dentro do painel de controle, selecione o ícone **Network** (Rede).
2. Em **Network**, selecione a guia **Bindings** (Ligações), a última a direita.
3. Em **Bindings**, você verá a opção *Show Bindings for* (Mostrar Ligações para). Selecione a *opção All Adapters* (Todos os Adaptadores).

A janela **Bindings** permite que o administrador ative ou desative ligações entre serviços, protocolos e placas de rede. Em *All Adapters* o NT lhe mostrará todos os adaptadores (interfaces ou placas de rede) presentes no sistema, e quais protocolos de rede estão ligados a eles.

4. Selecione a interface de rede que se liga à rede externa ou a Internet, clicando duas vezes. O NT mostrará quais protocolos de rede estão ligados a esta interface.
5. Selecione o protocolo WINS Client (que é na verdade o NetBIOS ou Rede Microsoft sobre TCP/IP) e clique no botão *Disable*. Um ícone vermelho deverá surgir ao lado do nome do protocolo, indicando que a ligação está desativada.
6. Reinicie a máquina.

A partir deste momento, a máquina não estará mais acessável via Rede Microsoft através da interface externa. Note que o roteamento deve estar desligado, de forma a também isolar outras máquinas e interfaces de rede do tráfego externo.

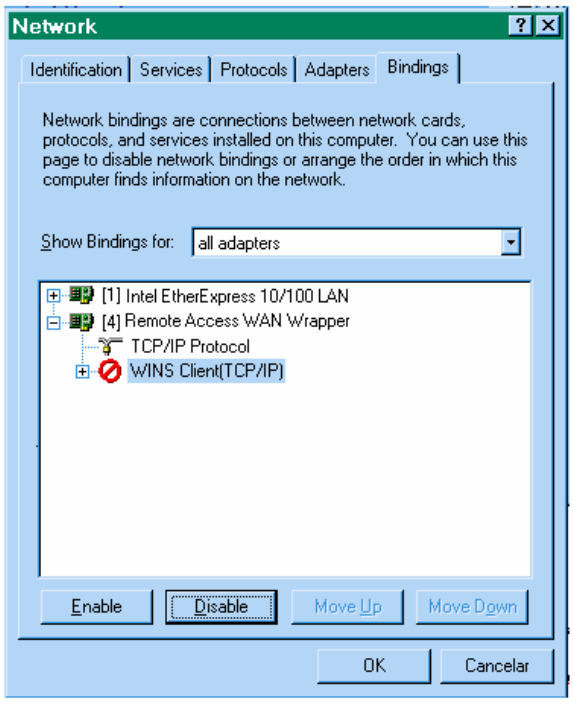

fig 3. Retirando ligação do NetBIOS

5. Controlando os privilégios de login

Em um sistema NT, se "logar" significa ser identificado pelo Windows NT, e a partir daí poder ter acesso os recursos da máquina. Para se logar o usuário deve informar a sua conta e a senha correspondente. Esta informação é checada no registro de usuários (SAM) local ou do domínio e se correta, o usuário é dito "autenticado". Ele recebe um *token* ("bastão") que o identifica como usuário e pode a partir deste momento ter acesso aos recursos da máquina ou do domínio.

Existem três tipos de login: **login local**, que ocorre quando o usuário está utilizando o console da máquina, fazendo o login digitando ctrl+alt+del e informando conta e senha; **login pela rede**, quando o usuário se autentica para acessar recursos da máquina pela rede; e **login como serviço**, quando um serviço (processo não-interativo, semelhante aos *daemons* do Unix) se identifica para executar com as permissões de um determinado usuário.

No Windows NT, os usuários são associados a uma série de privilégios, que permitem ou não a realização diversas ações no sistema. Entre os privilégios que um usuário pode ter estão, por exemplo, alterar a hora do sistema, realizar um shutdown ou incluir novas máquinas em um domínio. Os privilégios de um usuário estão contidos no *token* que ele recebe ao se logar. Você pode ver os privilégios do sistema e quem os possui utilizando o **User Manager**, clicando em **Policies** e a seguir em **User Rights**.

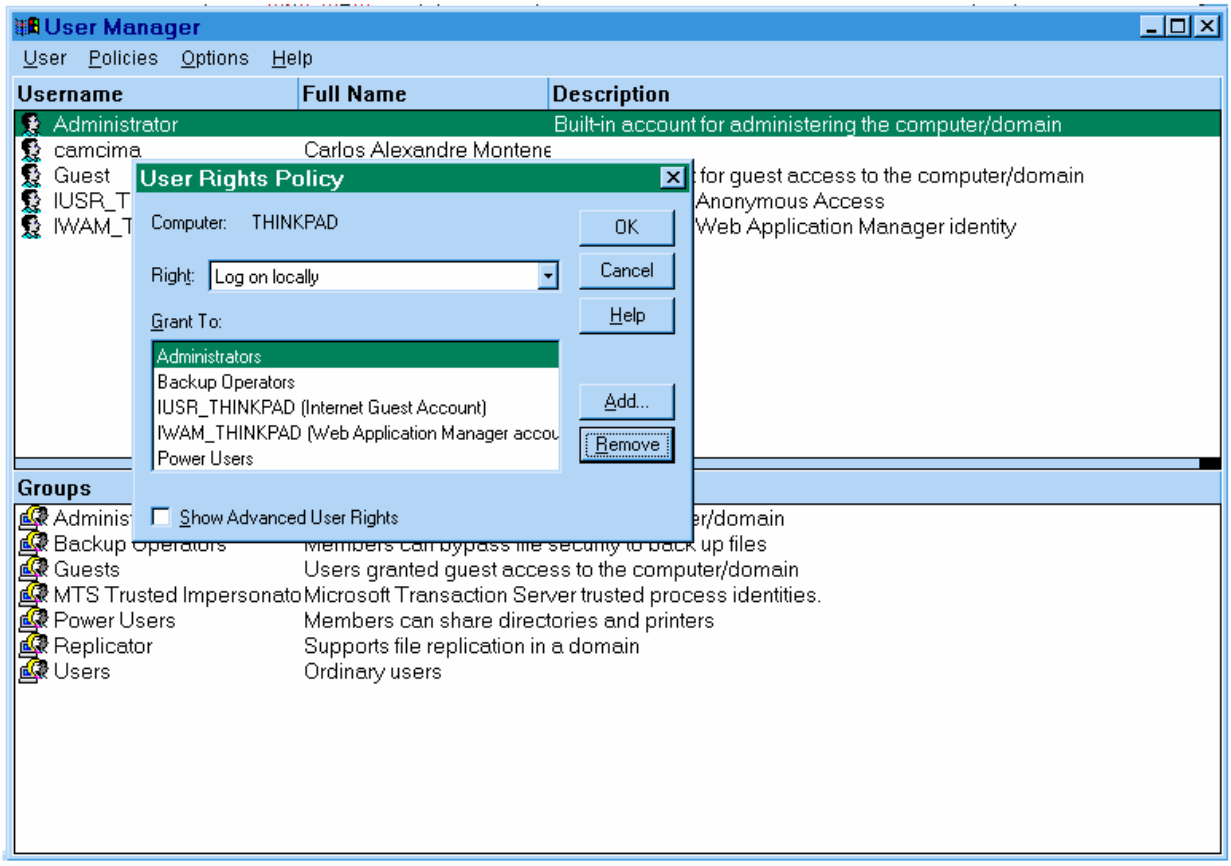

fig 4. Controlando privilégios de login

Login local, login pela rede e login como serviço também são privilégios. Apenas os usuários que possuam o privilégio de login local podem se utilizar a máquina no console, e da mesma forma só podem acessar recursos da máquina pela rede usuários que possuam o respectivo privilégio. É uma boa medida de segurança,

portanto, atribuir estes privilégios apenas a usuários que estejam autorizados a usar a máquina, negando o acesso aos demais.

Para restringir o login local, dê o privilégio de *Log on locally* apenas aos usuários que deverão utilizar localmente a console da máquina. Em um servidor, isto tipicamente inclui os grupos:

- Administrators
- Backup Operators
- Server Operators (ou Power Users)
- Algum outro grupo de pessoas que precise utilizar diretamente alguma aplicação no servidor, como DBAs ou Postmasters.
- Se o seu sistema possui o IIS (servidor web) instalado, o usuário IUSR_xxx que é utilizado pelo acesso anônimo também deve ter este privilégio, bem como qualquer usuário que queira acessar os serviços web de forma autenticada (isto é, tendo que informar conta e senha).

Em máquinas clientes, considere dar este privilégio apenas para os administradores de rede e para os usuários locais daquelas máquinas. Por exemplo, em um domínio departamental, permitir apenas aos usuários daquele departamento o uso local das máquinas, se esta for a política da empresa.

Já o privilégio de login pela rede, *Access this computer from network,* deve ser atribuído apenas para os usuários que deverão acessar recursos da máquina pela Rede Microsoft. Tipicamente ele é dado aos grupos:

- Administrators
- Domain Users (usuários do domínio)
- Users (usuários locais)
- Usuários de outros domínios que necessitem acessar pela rede recursos da máquina.

É importante se certificar de que os grupos Everyone e Guests não possuam nenhum destes dois privilégios, pois ambos abrem potencialmente portas para acessos não autorizados e invasão do sistema.

Esta configuração de privilégios vale apenas para a máquina local, a não ser em PDCs ou BDCs, onde vale para todos os controladores de domínio.

6. Implementando uma política de senhas

A maior parte das invasões acontecem devido a senhas fáceis de serem adivinhadas, seja por serem estupidamente óbvias (conta: joao senha: joao) ou por serem palavras de algum idioma, sujeitas a serem descobertas através de dicionários. Uma medida de segurança fundamental em uma rede é o estabelecimento de uma política de senhas, que diminua ao máximo o risco de um vazamento ou descoberta de senhas.

Alguns componentes de uma boa política de senhas são:

- Proibição de senhas que sejam facilmente quebradas, tais como a própria conta, palavras de dicionário, senhas em branco, senhas com poucos caracteres, etc. Deve-se recomendar o uso de senhas com letras maiúsculas e minúsculas, símbolos, números, de tal forma que fique virtualmente impossível a senha ser descoberta por tentativa e erro.
- Troca periódica de senhas, sem utilização das anteriores, minimizando o tempo de exposição no caso de uma senha haver vazado.
- Bloqueio de contas com um determinado número de tentativas de login sem sucesso, durante um determinado período ou até o desbloqueio pelo administrador.

A ferramenta utilizada para a definição da política de senhas de uma máquina ou domínio é o **User Manager**. Selecione no menu **Policies** a opção **Account Policy**. Aparecerá uma janela onde podem ser configurados os seguintes parâmetros de senha no sistema:

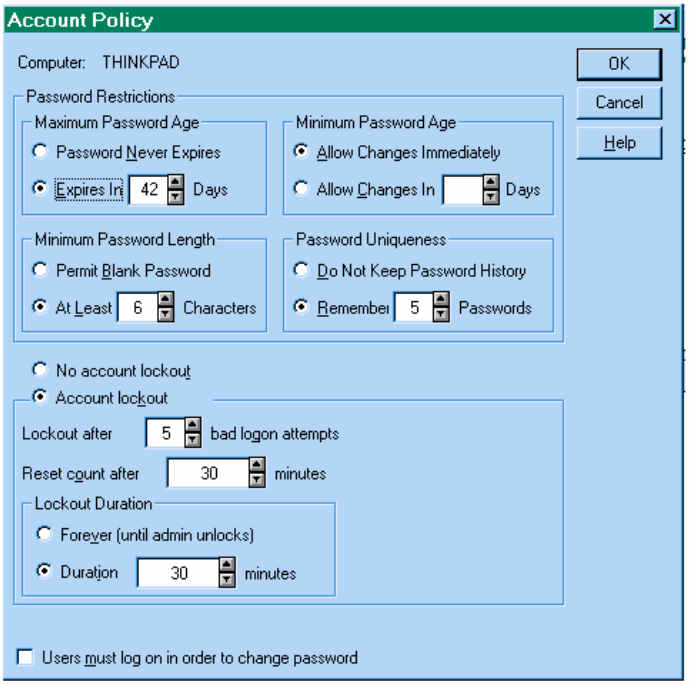

fig 5.Implementando política de senhas

- *Maximum Password Age* – Prazo máximo em que um usuário deverá trocar sua senha. Este valor normalmente é colocado ente 30 e 90 dias, dependendo das características do sistema.

- *Minimum Password Age* – Tempo mínimo que a senha deve permanecer antes de poder ser alterada. É utilizada para que a pessoa não troque rapidamente a senha várias vezes, de forma a burlar o controle de Password Uniqueness e utilize sempre a mesma senha. 1 dia de duração mínima da senha já deve ser o suficiente.

- *Minimum Password Length* – Tamanho mínimo emcaracteres da senha. Recomenda-se que as senhas do NT tenham entre 6 e 8 caracteres, devido a forma de criptografia utilizada (mais sobre isto a seguir no documento).

- *Password Uniqueness* – Número de senhas anteriores "se lembra", não permitindo que o usuário as utilize novamente. Isto garante que o usuário ficará sempre utilizando as mesmas senhas. Em geral usa-se um valor de 5 a 10.

- *Account Lockout* – Bloqueia a conta do usuário se a senha for informada incorretamente um determinado número de vezes. Esta conta pode ficar bloqueada por um período determinado ou indefinidamente até que o administrador a desbloqueie.

  É altamente recomendável a utilização de lockout de contas, devido entre outras coisas a uma deficiência grave na auditoria do NT: no caso de um login incorreto, ele não registra o endereço da máquina de onde foi feita a tentativa. Vários hackers se aproveitam da impossibilidade de serem rastreados para tentar continuamente o login pela rede, até adivinharem a senha.

Normalmente o bloqueio é feito após 3 a 5 tentativas, em um espaço de 30 minutos a uma hora. A duração do bloqueio ilimitada é mais segura, mas pode causar problemas no caso do administrador não estar disponível para reabilitar a conta para o legítimo usuário. 30 minutos de bloqueio são o suficientes para desencorajar um ataque e não prejudicar os usuários.

- Por fim, *Users must log on in order to change password* – Requer que o usuário esteja conectado para fazer uma troca de senhas, o que em outras palavras quer dizer que se uma senha expirar, o usuário deve procurar um administrador para colocar uma nova senha e desbloquear a conta. A não ser que você tenha requisitos muito exóticos de segurança, fuja desta opção.

Estas configurações valem para a máquina local, ou no caso de PDCs ou BDCs, para todos os controladores de domínio.

6.1 Utilizando senhas "fortes"

A partir do Service Pack 2 do NT 4.0 pode-se forçar os usuários a utilizar senhas "fortes", que sejam difíceis de serem adivinhadas. Este service pack vem com o arquivo PASSFILT.DLL, obriga as senhas a terem pelo menos um caractere de no mínimo três das quatro categorias abaixo:

- Letras maiúsculas.
- Letras minúsculas.
- Números.
- Caracteres especiais e pontuação.

Para habilitar este arquivo, edite a registry utilizando o **REGEDIT** ou **REGEDT32** e edite a chave **HKEY_LOCAL_MACHINE\SYSTEM**\CurrentControlSet\System\CurrentControlSet\Control\LSA. Crie o valor "Notification Packages" (sem as aspas), do tipo REG_MULTI_SZ, caso ele ainda não exista, e adicione ao seu conteúdo a string "PASSFILT".

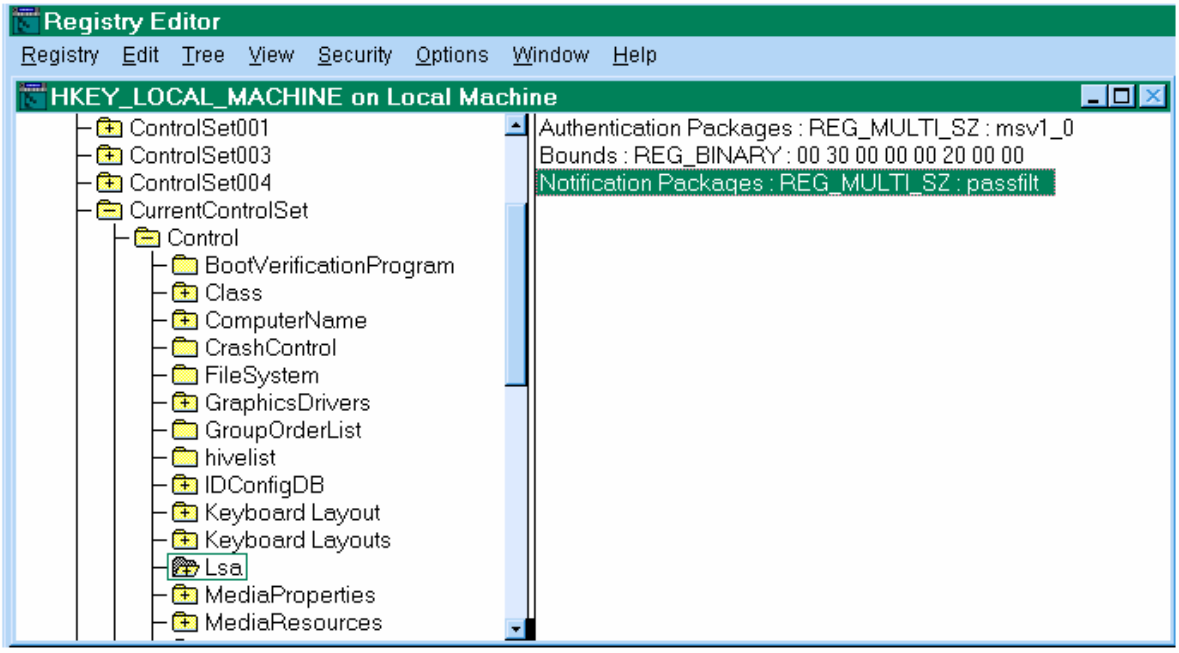

fig 6. Forçando o uso de senhas fortes

Esta DLL irá filtrar todas as alterações de senhas, checando se a a nova senha informada está de acordo com a norma acima. No caso de contas em um domínio, esta alteração na registry deverá ser feita em todos os controladores de domínio.

7. Auditoria

Por exigência da norma C2 de segurança do governo americano, no Windows NT todas as ações do sistema podem ser registradas e auditadas. Estas ações incluem, por exemplo, acesso a arquivos, login de usuários, execução de programas e impressão de arquivos. O registro destas ações é de fundamental importância tanto para diagnosticar defeitos e problemas, como também para verificar a integridade e a segurança do sistema. Boa parte dos ataques e violações podem ser identificadas através da auditoria do sistema.

Os registros gerados pela auditoria podem ser acessados pelo **Event Viewer** (Visualizador de Eventos). Eles são divididos em três tipos diferentes, *System, Security* e *Application*, dependendo se a origem do registro forem respectivamente serviços do sistema operacional, o subsistema de segurança ou aplicações sendo executadas na máquina.

A auditoria de segurança por default fica desligada, e nenhum evento do tipo *Security* é registrado. Ou seja, após a instalação do NT, o administrador não é informado se algum usuário se logou na máquina, se fez um shutdown ou se tentou acessar algum arquivo reservado no sistema. Para habilitar e configurar a auditoria, utilize no **User Manager**, dentro do menu **Policies** a opção **Audit**.

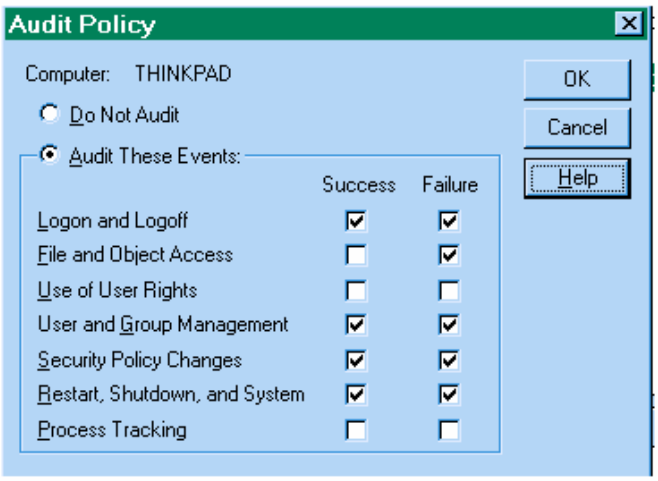

fig 7. Configurando auditoria de segurança

Como todas as ações podem ser registradas, a maior dificuldade em se configurar a auditoria em um sistema NT é evitar que seja gerada uma massa muito grande de registros, que impeça que uma boa análise dos dados seja feita. Nosso desafio é registrar apenas os eventos realmente significativos para serem auditados.

A janela de configuração **Audit Policy** oferece a possibilidade de registrar as seguintes ações, tanto no sucesso (o usuário estava autorizado a fazê-la) como em caso de falha:

- *Logon and Logoff* - Registra o sucesso ou falha na autenticação de um usuário durante o login, e também a sua saída do sistema. A ativação desta opção permite se saber quais usuários estavam usando o sistema

em um determinado momento, e se está havendo tentativa de se usar indevidademente a senha de um usuário.

- *File and Object Access* – Registra o acesso (ou tentativas de acesso) aos arquivos e outros objetos do sistema, como compartilhamentos, *pipes* e a registry. Após ativar esta opção, você terá que ir configurar no objeto quais eventos (leitura, gravação, deleção) devem ser registrados. A auditoria em arquivos exige que você esteja utilizando NTFS como sistema de arquivos.
- *Use of User Rights* – Ao ser acionado será registrado o uso de privilégios do sistema por parte dos usuários, como mudar a hora do sistema, acrescentar uma máquina no domínio ou tomar posse de arquivos. Este item não inclui o uso dos privilégios de login e shutdown, que são registrados separadamente.
- *User and Group Management* – Se refere a qualquer alteração na base de usuários do sistema, como inclusão e deleção de usuários, ou alteração de senhas.
- *Security Policy Changes* – Alterações nos privilégios dos usuários ou na política de auditoria do sistema.
- *Restart, Shutdown or System* – Registra reinicialização ou shutdown da máquina, bem como se o espaço para log de *Security* está cheio.
- *Process Tracking* – Informação sobre o controle de processos do NT, como início e termino, objetos acessados, e outros. Em geral é útil para debugação, mas não costuma ter aplicações com relação a segurança do sistema.

Ao ligar a auditoria dos itens *Process Tracking* e *Use of User Rights* você estará gerando uma enorme quantidade de registros em seu log de segurança, que não terão muita utilidade em ao se fazer uma auditoria de segurança. Portanto deixe-os desligados e ligue a auditoria para os demais, tanto sucesso como falha; esta informação pode ser crucial na detecção de um ataque ou de uma violação de segurança.

Altere também a configuração do seu log de eventos. Chamando o **Event Viewer** (Visualizador de Eventos), selecione no menu **Log** (Registro) a opção **Event Log Settings** (Configurações do Registro). Para o registro de segurança, aumente o tamanho máximo do log para um tamanho razoável, como 512k, e o configure para não sobrescrever eventos. Desta forma não se corre o risco de serem perdidas informações que sejam relevantes para a auditoria do sistema.