Segurança de Rede

- Segurança de rede e segurança de sistema (servidor individual) têm muito em comum
- Há redes onde o usuário faz login no domínio da rede para ter acesso aos recursos; em outras, se conecta a um servidor e deste tem acesso à rede
- Controle de acesso de usuários na rede
  - Criar uma conta (login) e definir uma senha é só o início para prover a um usuário acesso à rede
  - Existem vários aspectos no controle, permissões e limites de acesso a recursos e serviços de rede

Controle de Acesso em Rede

- Login concorrente
  - O mecanismo de autorização de acesso na rede deve, normalmente, restringir o acesso múltiplo (concorrente) aos usuários
  - Uma vez que o usuário se conectou à rede, ele deve primeiro finalizar sua conexão antes de poder se conectar a partir de outro lugar
  - Em ambiente de rede, bloquear login concorrente evita que o usuário deixe conexão em aberto em um computador e se conecte a partir de outro
  - Exceções em geral para administrador e suporte

Controle de Acesso em Rede

- Restrições a usuários
  - Espaço em disco: restringir o limite máximo de disco utilizado pelo usuário pode evitar descontrole no uso de espaço de armazenamento
    - pelo administrador da rede: backup, gerência de discos
    - pelo usuário: “faxina” em arquivos antigos, programas errados ou ataques que gerem dados excessivos
  - Estações restritas: controlar em quais estações um usuário pode conectar e em quais não
    - Facilita a setorização e organização no acesso
    - Também se aplica a definir um acesso restrito (em geral, apenas local via console) a um servidor da rede

Controle de Acesso em Rede

- Restrições a usuários
  - Restrição de tempo: limitar o tempo máximo de conexão e os horários/dias permitidos
    - Racionaliza a utilização dos recursos compartilhados
    - Desconexão por limite de tempo ajuda a contornar o problema de usuários que esquecem de desconectar
    - Restrição de horários e dias impede acessos indevidos e ataques em dias ou horários impróprios
  - Permissões de usuários e grupos de usuários
    - Mecanismo geral para controle de acesso a recursos e serviços, como arquivos e diretórios, impressoras etc.
    - Deve ser planejado cuidadosamente, de forma a dar sempre o mínimo de permissões necessárias às tarefas

Controle de Acesso em Rede

- Remoção de contas inativas
  - Revisar contas de usuários regularmente:
    - remover ou alterar senha das contas padrão do sistema (guest, root, administrator, postmaster, webmaster etc.)
    - remover contas que não são mais necessárias
    - bloquear contas de usuários temporariamente afastados ou que estejam há muito tempo sem acessar
- Single Sign-On (SSO)
  - Autenticação única ou centralizada de usuário com um único login/senha, evitando confusões
  - Sistemas SSO mapeam acesso a vários sistemas
  - Contra: roubo de senha dá acesso generalizado

Gerenciamento de Redes

- Gerenciamento de rede baseado em políticas
  - Abordagem com popularidade crescentemente em organizações com redes médias a grandes
  - Busca reduzir dificuldade de gerenciar redes com centenas ou mesmo milhares de nodos, distribuídos em vasta área geográfica
  - Gerenciamento baseado em políticas: processo de reunir propriedades de vários recursos de rede sob um controle administrativo central, visando:
    - Simplificar o processo de gerência de redes
    - Garantir segurança e integridade da rede através de um gerenciamento central de recursos distribuídos

Gerenciamento de Redes

- Gerenciamento de rede baseado em políticas
  - Também foca disponibilidade de recursos de rede
    - Políticas podem priorizar tráfego de rede, garantindo que serviços críticos recebam os recursos necessários, na distribuição de banda c/ sistemas menos prioritários
    - Ajuda a gerenciar objetivos de qualidade de serviço
  - Consolida informação de segurança dos recursos de rede: propriedade, ACLs (*Access Control List*), disponibilidade
  - Conceito principal do gerenciamento baseado em políticas: serviços de diretório

Gerenciamento de Redes

- Serviços de Diretório
  - Diretório: listagem abrangente de objetos, repositório de informações sobre objetos, como contas de usuário, localidades e coisas
  - Diretório de rede: contém informações de recursos como impressoras, aplicações, BDs, usuários, grupos, servidores, dispositivos, senhas
  - Função básica de serviços de diretório: localizar, nomear e controlar comunicações com recursos
  - Combinam métodos de acesso confiáveis
  - Desejável formatos intercomunicáveis (padrões)

Serviços de Diretório

- Formatos e Padrões
  - '80s: Protocolo de Acesso a Diretório (DAP) X.500
    - Especificação em esforço para criar e integrar um serviço de diretório universal
    - As implementações que surgiram não foram boas
  - LDAP: Lightweight Directory Access Protocol
    - Versão simplificada do DAP X.500
    - Focado somente nos protocolos que aplicações clientes devem usar para acessar o diretório, sem complicações do DAP original
    - LDAP vingou e é amplamente suportado
    - Hoje suporta recursos de segurança como TLS (SSL)

Serviços de Diretório

- Implementações de serviço diretório antigas
  - Sun Network Information Service (NIS)
  - IBM Distributed Computing Environment (DCE)
  - Banyan StreetTalk
- Implementações modernas (suportam LDAP)
  - Novell Directory Services (NDS)
    - Mais amadurecido e robusto
    - Versões Netware, Sun Solaris, Unix*, Linux, AS/400...
  - Microsoft Active Directory
    - Moderno e recente, surgiu com o Windows 2000
  - Netscape Directory Server

Serviços de Diretório

- Sistemas modernos suportam metadiretórios
  - Ferramentas para integrar hierarquicamente diretórios de rede existentes
  - Habilidade de compartilhar informação comum a todos os subdiretórios, independente de plataforma e arquitetura
  - Em geral, permitem propagar atualizações em um metadiretório por todos os diretórios componentes
- Exemplo típico
  - Cadastrar um novo usuário em um serviço de diretório cria contas e acessos nas diversas aplicações e recursos integrantes