Segurança e auditoria de sistemas

Professor Emiliano S. Monteiro

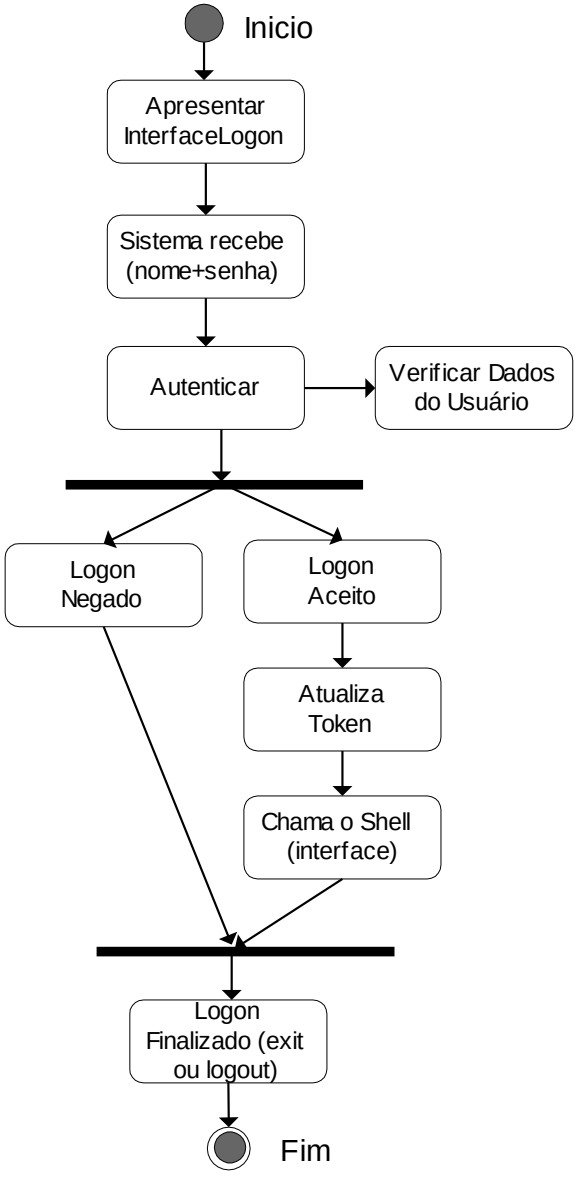
Autenticação

Prova ao sistema quem você realmente é, uma prova de identidade. Geralmente é implementada de forma a solicitar ao usuário Nome e Senha.
A maioria dos sistemas operacionais adota a autenticação padrão de NomeDeContaNoSistema+senha, porém quase todos permitem que isto seja personalizado e alterado. O que chamamos aqui de “NomeDeContaNoSistema” é a palavra que o sistema operaciona de rede e os serviços de rede usam para identificar um determinado usuário, por exemplo: “João Paulo II” poderia ter um nome para o sistema operacional como “santopadre”.
Contas de usuários (ID, nome, senha) em todos os sistemas estudados são armazenadas em bancos de dados tendo apenas a criptografia de senha com segurança deste banco de dados. Sistemas operacionais como o Linux armazenam as senhas em um arquivo /etc/passwd e os grupos de usuários em /etc/group. Estes são arquivos texto padrão e podem ser lidos com um editor de texto qualquer, porém o campo de senha foi criptografado e somente o root (super usuário do Linux) tem poder para ver o conteúdo destes arquivos.

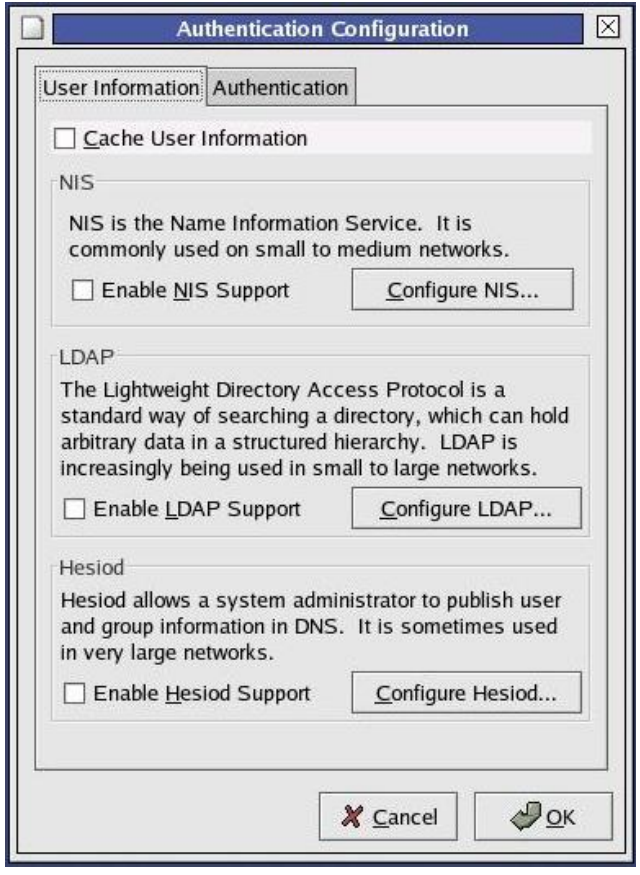
e-cac autenticação é via senha ou ecpf

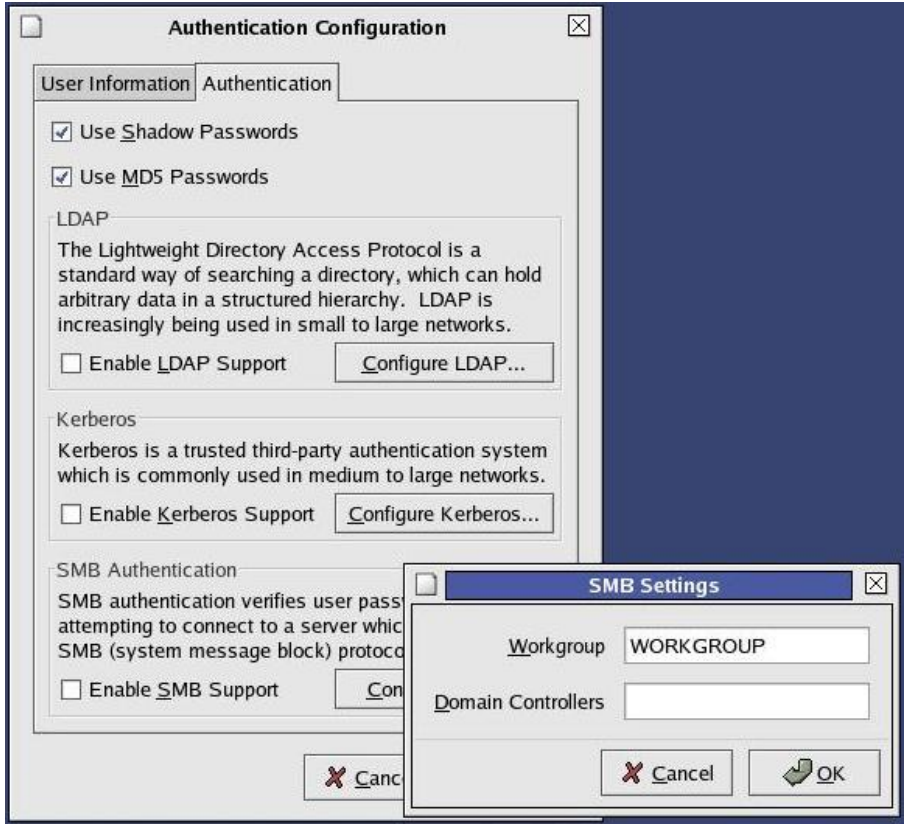
Autenticação

1. Nenhum processo lê a partir do teclado.
2. Não se armazena senhas no banco de contas.
3. Mecanismos de autenticação são substituíveis.
4. Se o usuário não vai mais trabalhar no shell ele só tem dois caminhos possíveis: a) desligar o computador ou b) voltar para o logon.
5. A cada login mal sucedido é imposto um retardo na próxima tela de login.
6. Um login com sucesso sempre chama o shell.
7. O security token contém os dados do usuário logado.
8. Token = crachá ! Na programação são variáveis do usuário logado.



Autenticação



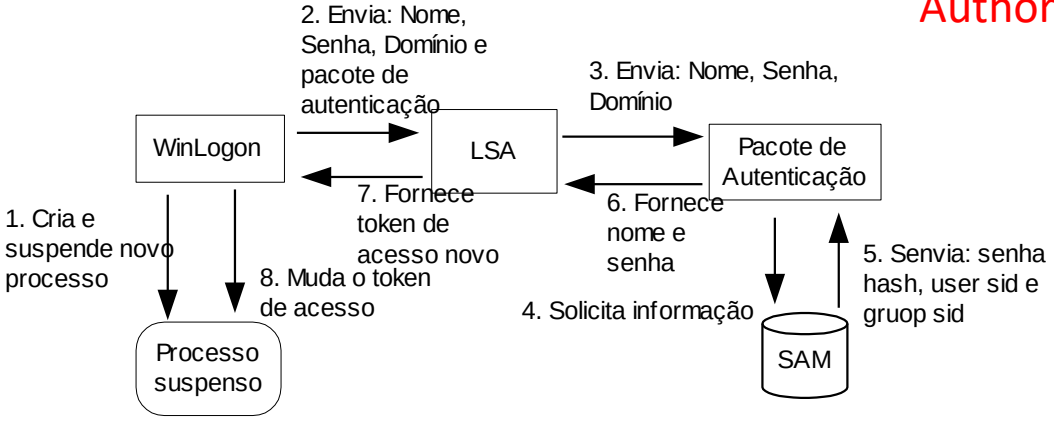


Autenticação

Quando o WinLogon receber os dados do usuário ele coleta o domínio do usuário, cria um SID e chama LSA. Antes da informação ser passada para o LSA, ela é criptografia. Uma vez que o LSA foi acionado ele chama o pacote de autenticação. O pacote de autenticação verifica o nome e senha (recuperando informações no banco de dados SAM). A autenticação é feita comparando-se as senhas hash fornecidas e armazenados no banco de dados. Se o usuário passar na autenticação é criado uma ACL para ser usada com o token do usuário . Um apontador para o primary token é passado ao WinLogon. Depois disto o WinLogon cria um Desktop (para que o usuário possa acessar o desktop).

SAM = Security Account Manager

LSA = Local Security Authority



GINA – Graphical Identification and Authentication

A identificação é implementada como um conjunto de DLLs (Dinamyc Link Library, Biblioteca de Ligação dinâmica), chamadas de GINA – Graphical Identification and Authentication. A DLL padrão é msgina.dll, que pode ser trocada por outra (implementado assim outros tipos de mecanismos de autenticação além dos tradicionais nome+senha). Outros tipos de DLLs para realizar autenticação podem ser adquiridos de outros fabricantes que não a Microsoft, para que o processo e autenticação possam receber outros dados como: voz, imagens, etc; na figura abaixo podemos ver o relacionamento destas DLL com os outros componentes do sistema de autenticação do Windows NT/2000.

GINA é responsável pelas seguintes operações: Reconhecimento de SAS (Security Authentication Sequence (CTRL+ALT+DEL) no processo de Logon; é responsável por mostrar a interface com o usuário que será usada para realizar a autenticação de Logon (tradicionalmente um dialog box para coletar o nome e senha digitado pelo usuário); Criação de Shell, associar o token de acesso do usuário a um processo shell, e iniciar o shell do usuário (explorer.exe) (userinit.exe, iniciar variáveis de ambiente entre outras coisas).

Token de acesso do windows

Os símbolos de acesso (ou símbolos de segurança) são criados pelo LSA e associados ao Shell do usuário e aos processos do usuário para identificá-lo quando for realizar um acesso a um objeto. São o equivalente no Unix a variáveis de ambiente que guardam o usuário, grupo, Shell, caminho, etc, do usuário. Tanto no Unix como no Windows, quando o usuário realiza um *logout* (ou *logoff*) estas variáveis (ou token no caso do Windows 2000) são liberadas. HAYDAY (2001) cita que um token pode contar as seguintes informações SID - Símbolo de segurança. Os tokens do usuário asseguram que os processos que o usuário deseja executar, não vão tentar acessar objetos cujas permissões sejam superiores as do usuário.

- SID do usuário
- SID do grupo
- SID de logon
- Privilégios de usuário ou de grupo
- SID de proprietário
- SID de grupo primário
- DACL
- A origem do símbolo de acesso
- Símbolo primário ou de imitação
- Lista opcional de SID restritivas
- Níveis de imitação

Arquivos de senhas do Linux

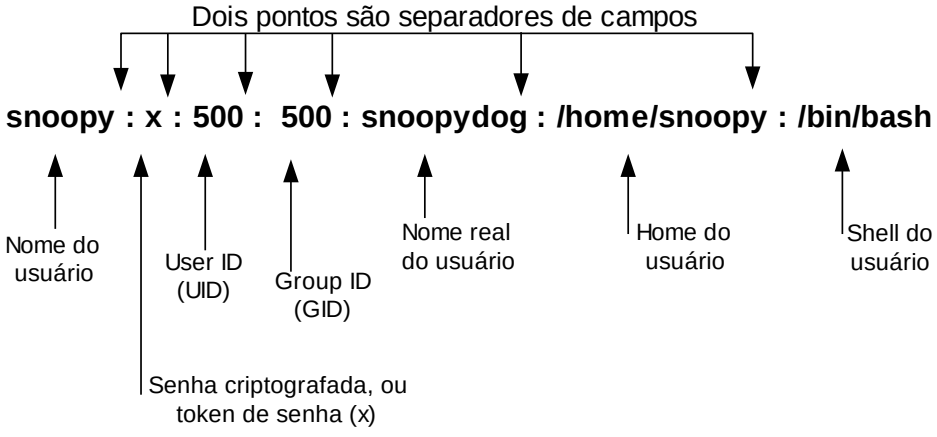
Para usuários e grupos, o Unix/Linux possue dois arquivos que ajudam o sistema a manter seus esquemas de segurança, são eles: passwd e group. Estão localizados no diretório /etc. O arquivo /etc/passwd, é mais que um local de armazenamento de senhas de usuários, ele contém informações sobre o usuário, telefone, shell, ID (Identifier) de usuário, ID de grupo, área no sistema, etc. O arquivo de grupo também está localizado em /etc.

São considerados dois bancos de dados sobre os usuários e grupos que usam o sistema. Antigamente a senha dos usuários era armazenada criptografada no arquivo /etc/passwd. Hoje muitos sistemas Unix/Linux usam senhas com sombra (shadow). Isto significa que as senhas ficam armazenadas em outro arquivo. Hoje as distribuições Linux estão entregando os sistemas com as senhas shadow como padrão, portanto é normal ter-se um arquivo /etc/passwd com um "x" no campo de senha, o que significa que o sistema usa shadow e as senhas ficam armazenadas em /etc/shadow de forma criptografada. A seguir tem-se um exemplo da estrutura de um arquivo passwd segundo Anonymous (2000). Um arquivo de senhas do Unix/Linux pode ter várias linhas similares. Número de Identificação único para cada usuário e grupo

Linux = ls, cd, cat	CMD = dir, cd, type

Arquivos de senhas do Linux

- Nome de usuário: é onde será colocado o nome de identificação do usuário para ser usado no sistema.
- Senha: local onde será armazenada a senha do usuário, antigamente a senha era armazenada neste campo de forma criptografada (ex: x1frt56m4d0AlB7), em sistemas novos a senha é deslocada para um arquivo sombra do passwd (/etc/shadow), onde a senha criptografada é armazenada, neste exemplo o “x” representa um apontador para o arquivo de sombra.
- UserID: número de identificação do usuário. É usado nos processos dos usuários, é único e pode ser um número qualquer entre 0 e 65534, 0 é usado para o root (superusuário), geralmente a numeração de usuários começa com 500.
- GroupID: armazena o identificador de grupo ao qual o usuário pertence, o usuário pode ou não participar de mais de um grupo Anonymous (2000), más para cada usuário novo criado no sistema deve existir um grupo para ele.



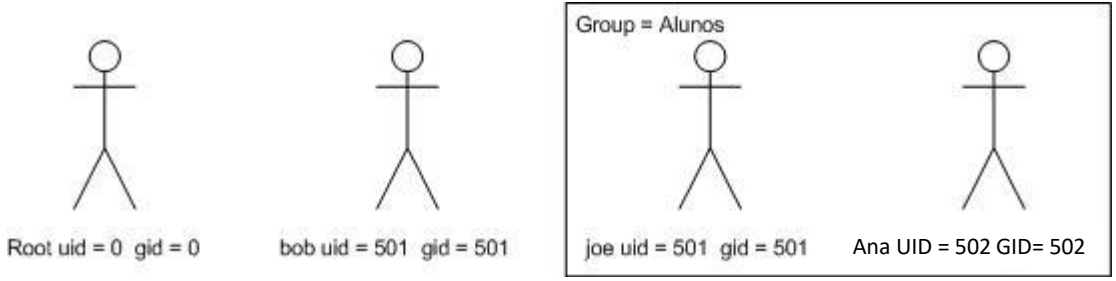
- Nome Real: também chamado de General Electric Comprehensive Operating System Field, Anonymous (2000), (GECOS), serve para armazenar diversos dados sobre o usuário, local de trabalho, fone, etc.
- User Home: diretório privado de trabalho do usuário, geralmente os diretórios padrão de usuários ficam dentro de /home
- User Shell: Shell padrão para o usuário, na maioria das distribuições Linux o Shell padrão é o Bash, localizado em /bin. Outros tipos de shell poderão ser colocados aqui como (ash, csh, ksh, etc).

Sistema de permissão do Unix/Linux

Os conceitos de grupos e usuários estão sempre juntos Unix e Linux. Quando criamos um usuário no Unix e Linux o sistema operacional automaticamente cria um grupo para este usuário. Por exemplo; se criarmos um usuário chamado Maria, o sistema irá criar um grupo chamado Maria e irá colocar Maria dentro de Maria (o usuário Maria dentro do grupo Maria). Depois o administrador poderá colocar o usuário Maria em qualquer outro grupo.

Na Figura 115, podemos observar o super usuário com número 0 e número de grupo 0 (uid = 0 e gid = 0); o usuário bob tem o número 501, em alguns sistemas (como o Red Hat ou Conectiva Linux) os novos usuários começam a receber seus números (de usuário e grupo) a partir de 500. Nesta figura esta presente um grupo chamado alunos com dois usuários.

Os comandos chmod e chown são usados para alterar as permissões de dono, grupo e outros, e alterar as permissões de proprietários respectivamente.



Sistema de permissão do Unix/Linux

Diretório	Descrição
/bin/	Binários essenciais
/boot/	Arquivos de Boot
/dev/	Arquivos de dispositivos
/etc/	Arquivos de parâmetros e configuração diversos
/home/	Pasta de usuários normais
/lib/	Bibliotecas básicas
/mnt/	Ponto de montagem de sistemas de arquivos
/media/	Ponto de montagem de CD/DVD
/opt/	Aplicações de usuários
/proc/	Sistema de arquivos em RAM com imagem do kernel e processos
/root/	Pasta do root
/sbin/	Binários de administração do SO
/tmp/	Pasta temp.
/srv/	Dados diversos para outros processos
/usr/	Arquivos compartilhados com outros processos
/var/	Pasta de arquivos variáveis, como o email e logs

Sistema de permissão do Unix/Linux

Arquivo	Descrição
/etc/passwd	Arquivo de senhas de usuários
/etc/group	Relação de grupos do sistema
/etc/inittab	Configura o processo init para carregar serviços e runlevels
/etc/rc.d/	Diversos scripts de inicialização
/etc/ppp	Opções de configuração do daemon ppp
/etc/http	Arquivos de configuração do servidor web (Apache)
/etc/init.d/inet e /etc/inetd	Script de inicialziação do daemon inetd
/etc/protocols	Identifica o número de cada protocolo
/etc/services	Identifica os números de portas
/etc/shells	Shells disponíveis para que os usuários possam realizar o login
/etc/host.equiv	Relação de host confiáveis
<Diretório do usuário>.rhosts	Controla acesso a uma conta de usuário individual
/etc/hosts	Tabela usada para transformar nomes em endereços
/etc/resolv.conf	Arquivo usado pelo resolvedor de nomes
/etc/named.conf	Arquivo usado pelo resolvedor de nomes – DNS (BIND)
/etc/host.conf	Define como o arquivo host é controlado e interage com o DNS
/etc/sysconfig/sendmail	Arquivo de configuração do sendmail
/etc/sendmail.cw e sendmail.cf	Arquivos de configuração do sendmail
/etc/httpd/apache/conf/httpd.conf	Arquivo de configuração do Apache
/etc/var/log/httpd/apache/	Localização dos arquivos de log do servidor
/home/httpd/html/	Localização das pastas que podem conter arquivos index.html
/etc/httpd/apache/conf/httpd.conf	Estipula controles de acesso ao servidor web

Sistema de permissão do Unix/Linux

Arquivo	Descrição
/etc/smb.conf	Arquivo de configuração do Samba
/etc/sysconfig/networks	Configurações genéricas de rede
/etc/gateway	Arquivo de configuração de daemon routed
/etc/gated.conf	Configura protocolos de roteamento de interior e exterior (como o bgp e ospf)
/etc/rc.d/init.d/dhcp.d	Inicializa serviço dhcp
/etc/dhcpd.conf	Ajusta diversas opções do dhcp
/etc/exports /etc/exportfs	Controla pastas que serão compartilhadas com NFS
/etc/fstab	Mostra a tabela de partições
/etc/hosts.allow e /etc/hosts.deny	Incluir hosts confiáveis ou não quando a máquina estiver recebendo ou enviando dados em uma conexão de rede
/etc/shadow	Arquivo que pode ser lido apenas pelo root, mantém uma sombra do arquivo /etc/passd com as senhas criptografadas
/etc/sshd/sshd_config	Arquivo de configuração do secure Shell
/etc/cron.daily/	Arquivos de agendamento de processos
/etc/var/spool/cron/root	Arquivos de logs agendamento do cron
/etc/ftpaccess	Configuração do acesso ftp

$su root
#cat /etc/fstab

Módulos Plugáveis de Autenticação - PAM

O PAM (Pluggable Authentication Modules) é outro sistema de segurança presente em muitas distribuições Linux/Unix de hoje. O PAM (Módulos Plugáveis de Autenticação), são módulos que gerenciam as autenticações dos programas e dos usuários. Isto surgiu para evitar que todo programador tivesse que alterar o código do programa login toda vez que um novo esquema de segurança era lançado. Na maioria das distribuições Linux modernas o PAM foi integrado ao processo Login (nem todas as distribuições existentes usam este processo de autenticação). O mesmo vale para qualquer programas que venha a requerer de seu usuário um algum tipo autenticação/identificação, é mais fácil para os programadores utilizarem as bibliotecas do PAM para que seus sistemas não tenham que ser re-escritos novamente porque algo mudou e afetou o processo de autenticação.. Hasenack (2001) cita que o PAM foi uma criação da SUN, mais tarde recebeu uma RFC (Request For Comments). Hasenack (2001) e TACKET (2000) também comenta que o PAM pode ser dividido em quatro grupos.

Módulos Plugáveis de Autenticação - PAM

1) auth: verifica a autenticação do usuário, pedindo senha ou outro mecanismo (biometria, por exemplo);

2) account: verifica se o usuário pode usar o serviços que está solicitando (se autenticando), “os módulos aqui podem checar por horário, dia da semana, origem do login, login simultâneo, etc” Hasenack (2001);

3) passwd: usado para mudança de senha, “podem ser colocados módulos que verificam se a senha é forte ou fraca”, Hasenack (2001);

4) session: cria o ambiente do usuário.

O uso de PAM simplifica o processo de login com mecanismos como Kerberos, Hagen (2001). Os arquivos de configuração de PAM são /etc/pam.conf e /etc/pam.d. PAM foi originalmente escrito para o Solaris, más teve seu momento de popularidade através de seu uso nas distribuições Linux

Controle de permissão