Advanced SUSE Linux Enterprise Server Administration (Course 3038)

Chapter 4

Secure a SLES 9 Server

Objectives

- Create a Security Concept
- Limit Physical Access to Server Systems
- Limit the Installed Software Packages
- Understand the Linux User Authentication
- Ensure File System Security

Objectives (continued)

- Use ACLs for Advanced Access Control
- Configure Security Settings with YaST
- Stay Informed About Security Issues
- Apply Security Updates

Create a Security Concept

- Objectives
  - Understand the Basics of a Security Concept
  - Perform a Communication Analysis
  - Analyze the Protection Requirements
  - Analyze the Current Situation and Necessary Enhancements

Understand the Basics of a Security Concept

- You must know what you are protecting your system from
- If users work on different computers and use common resources
  - Security concept pertaining to a network must be considered
- Formal method of creating a security concept
  - Helps to detect errors and sources of danger that are not obvious
  - Provides good documentation of the concept

Perform a Communication Analysis

- Creating a security concept
  - Begins with a communication analysis
- Answer the following questions
  - What information will be exchanged across which barriers and in which direction?
  - Which data packets will be transported with which protocols to which hosts in the network?
  - What resources are available to individual users and with which access rights?
  - Which resources must be available in each work area?

Perform a Communication Analysis (continued)

- Answer the following questions (continued)
  - Which data must users have access to and in which way?
  - Which external users have external access to company resources, what resources do they use, and how is access controlled?
  - Which external resources does the company provide?
  - Should users be charged for resources?
  - Which tasks must external service providers be involved in?
  - How do security restrictions affect users, and how open are users to these restrictions?

Perform a Communication Analysis (continued)

- Answer the following questions (continued)
  - Will you filter transmitted or stored information on gateways between networks or on computers?
  - How available do individual resources need to be?

Analyze the Protection Requirements

- Expense of securing individual resources
  - Determined by amount of potential damage
- Estimate frequency of occurrence of possible damage
  - To use in your calculations
- Questions
  - Which groups of people can access which information?
  - Where is protected data located?
  - Which zones exist and what security needs do they have?

Analyze the Protection Requirements (continued)

- Questions (continued)
  - What might happen to security zones if security barriers are breached?
  - Who are potential attackers?
  - What information is of special interest to others?
  - What are the remaining risks when the security concept is implemented?
- Important parts of the communication analysis
  - Can be represented in tables, also known as *access matrices*

Analyze the Protection Requirements (continued)

Table 4-1

	Proxy Server	Web Server	Mail Server
Workstation Office	8080		
Workstation Web Designer	8080	ssh	
Workstation Sysad	8080	ssh	ssh
Mail Server Intranet			smtp

Analyze the Current Situation and Necessary Enhancements

- Company-wide security policy should guarantee
  - Confidentiality, data integrity, availability, and transparency
- Security policy
  - Determines what security demands are required for specific data and resources
  - Should include the analysis of the remaining risk
  - Describes the current actual state of security
- Topics needed to be covered in the security policy
  - See Table 4-2

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-2

Security of network components	How the components and their physical storage areas are secured against unauthorized access
Actual state	The network cabinets are freely accessible so that each member of staff can patch his own network connections.
Target state	Technical rooms are locked, so only system administrators have access.
Task	The locks must be checked and keys assigned to system administrators.
Date	2007-02-02
Responsible Person	Jenny Doe, head of System Administration department.
Estimated expense	Approximately five days and $1200.
Done/checked	2007-03-01 Henry Boardman, Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

- Dial-up to and from the internal network
  - See Table 4-3
- Power failure measures
  - See Table 4-4
- Fire fighting measures
  - See Table 4-5

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-3

Security of network components	Do connections to other networks or dial-up possibilities to the internal network exist? How are these accesses protected?
Actual state	In the departments of the U.S. branches, there is an undefined number of Internet accesses through a local provider. It is not known if the computers used for the dial-up are connected to the internal network. A number of administrators are using Windows NT RAS access to administer from home. The NT RAS is operated using Chap and Callback. The situation at the other locations is not known.
Target state	There is no local Internet access. Members of staff who require Internet access can obtain this using the central firewall.
Task	All worldwide locations are connected by VPN to the headquarters in the U.S. in accordance with a board decision. A 2 MB Internet access is used in the headquarters, secured by a three-level firewall with an application level gateway. Local Internet access is removed.
Date	2007-03-30
Responsible Person	Jenny Doe, head of System Administration department. Management provides Ms. Doe with appropriate powers.
Estimated expense	Approximately 15 days and approximately $200,000.
Done/checked	2007-03-30 Henry Boardman, Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-4

Further Security Measures	How are the servers protected against power failure?
Actual state	In all technical rooms, a UPS is installed so servers automatically shut down in case of power failure. The UPS and server connecting cables are checked regularly.
Target state	All servers are connected to a functioning UPS. Actual state reflects target state.
Task	
Date	
Responsible Person	
Estimated expense	
Done/checked	2007-01-12 Henry Boardman, Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-5

Further Security Measures	What firefighting means are available?
Actual state	Suitable fire extinguishers are installed in front of all technical rooms. Suitable fire detectors are installed in all technical rooms. The large technical rooms at the U.S. headquarters are equipped with automatic fire extinguishing equipment.
Target state	Technical rooms are equipped with fire detectors and extinguishers outside the doors to the rooms. U.S. headquarters technical rooms have automatic sprinklers installed. Actual state reflects target state.
Task	
Date	
Responsible Person	
Estimated expense	
Done/checked	2007-01-14 Henry Boardman, Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

- Data storage issues
  - See Table 4-6
- Software security updates
  - See Table 4-7
- Virus protection of the IT systems
  - See Table 4-8

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-6

Further Security Measures	How is data security controlled? How are checks made to determine whether the data stored is usable?
Actual state	Important servers and workplace machines are equipped with tape drives. Backups take place daily. Responsibility for data backups lies with those members of staff in the technical departments who have been briefed for this.
Target state	At each location, backups are made on tape libraries by means of network backup software. The tapes are cloned, regularly recycled, and stored in fireproof safes.
Task	A data backup concept must be drawn up and implemented. An external consultant should be hired.
Date	2007-04-22
Responsible Person	Jenny Doe, head of System Administration department. Management provides Ms. Doe with appropriate powers.
Estimated expense	A cost estimate will be made by an external consultant.
Done/checked	2007-01-14 Florian Sailer, Co-Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-7

Further Security Measures	How can we guarantee that available software updates to close known security loopholes are tested and installed?
Actual state	Installing software updates is left to the judgment of the appropriate administrator, but this is discussed in detail with colleagues and suppliers or vendors.
Target state	Software updates will be recorded, tested, and released company-wide by two accountable members of staff. Security-relevant software updates will be installed especially on systems in the demilitarized zone. Only in exceptional cases, justified in writing, will software updates in the DMZ be delayed. In such cases, the head of System Administration must determine if other kinds of protective measures can be used.
Task	The head of the System Administration department will name two system administrators who will design a software update concept and who will then be responsible for software updates.
Date	2007-03-30
Responsible Person	Jenny Doe, head of System Administration department
Estimated expense	Approximately four days for designing the concept. The running costs will be included in the concept.
Done/Checked	2007-03-30 Henry Boardman, Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-8

Further Security Measures	How are the systems protected from malicious software viruses?
Actual state	Virus scanners are only installed on certain workplace computers.
Target state	Virus scanners with a frequent update service are installed on all file servers and workstations. Current virus signatures can be downloaded at any time from the Internet from the server of the virus scanner vendor. The virus scanners on workstations obtain the virus signatures from a central server, so new virus signatures only need to be installed once. To monitor the file servers, the product of a different vendor is used rather than the product monitoring the workstations. Overall, an efficient, two-level virus defense concept is implemented.
Task	The head of the System Administration department names two accountable persons who will design a virus defense concept and who will later on be responsible for the operation of the virus defense.
Date	2007-03-30
Responsible Person	Jenny Doe, head of System Administration department.
Estimated expense	Approximately ten days for the product evaluation and concept design. Operating costs will be included in the concept.
Done/checked	2007-03-30 Florian Sailer, Co-Assistant to the Board.

Analyze the Current Situation and Necessary Enhancements (continued)

- Documentation of the IT infrastructure
  - See Table 4-9

Analyze the Current Situation and Necessary Enhancements (continued)

Table 4-9

Further Security Measures	How Is the system configuration documented?
Actual state	Everyone who has configured a machine on the network writes down or remembers the configuration data.
Target state	All system configurations (hardware and software) are documented centrally in electronic form at the corresponding location. System administrators at the U.S. headquarters can access the documentation from all locations.
Task	The head of the System Administration department shall name two system administrators who will draw up documentation guidelines.
Date	2007-03-30
Responsible Person	Jenny Doe, head of System Administration department.
Estimated expense	Approximately 20 days to design a concept. The estimated cost of implementing this will be included in the concept.
Done/checked	2007-03-30 Henry Boardman, Assistant to the Board.

Limit Physical Access to Server Systems

- Objectives
  - Place the Server in a Separate, Locked Room
  - Secure the BIOS with a Password
  - Secure the GRUB Boot Loader with a Password

Place the Server in a Separate, Locked Room

- Best way to prevent physical access to a server
- Guidelines
  - Server room should be locked with a solid door
  - Only system administrators should have access
  - Room should be protected against fire
  - At the least, a separated locked room for all servers is recommended

Secure the BIOS with a Password

- For test systems or workstations that are not placed in a secure room
- BIOS represents the lowest level of software
  - Lies underneath the operating system
- Modern BIOS versions
  - Give you the option of protecting the boot process with a password
- You can also protect the BIOS settings
  - And prevent the system from booting from media

Secure the GRUB Boot Loader with a Password

- Another attack
  - Reboot system and pass additional parameters to the kernel
- GRUB can be configured to prompt for a password
  - Before any parameters can be entered
- Steps
  - Create encrypted password with the parameter:
    - grub-md5-crypt
  - Add password to GRUB configuration file as follows:
    - /boot/grub/menu.lst

Limit the Installed Software Packages

- Remove unnecessary software packages
  - From a production server
- A server should never offer any network services that are not needed
- Check which services are configured to start and their run levels
  - chkconfig -l
  - Command displays a line for every service installed
- Remove a service from its default run levels:
  - insserv -r *service_name*

Understand the Linux User Authentication

- Authentication on a Linux system
  - Based on Pluggable Authentication Modules (PAM)
- Objectives
  - How PAM Works
  - PAM Configuration
  - The Requirements for a Secure Password

How PAM Works

- Pluggable Authentication Modules (PAM)
  - Collection of software modules
    - Handles the authentication process
- User logs into a Linux system on a virtual terminal
  - Program called login is usually called
- Before PAM was introduced
  - Login and all other applications had to be extended to support a different authentication process
- PAM creates a software level
  - With clearly defined interfaces

How PAM Works (continued)

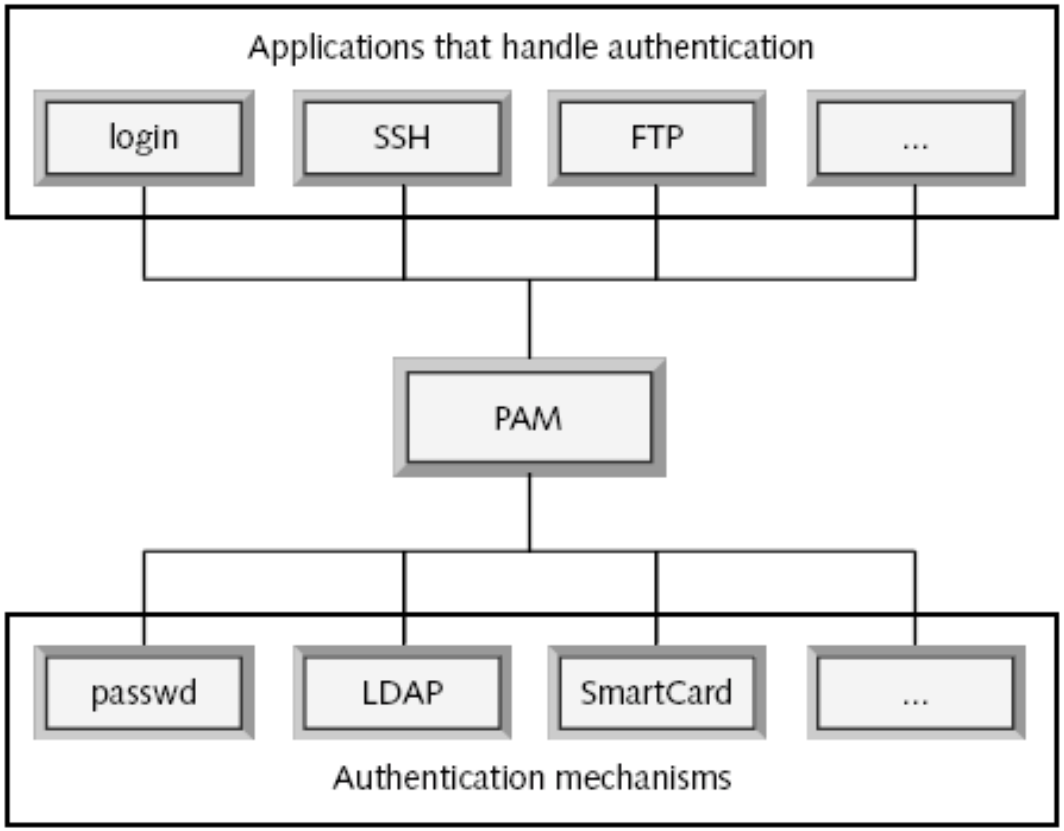

Figure 4-1

PAM Configuration

- PAM modules are located in directory /lib/security
  - Every filename starts with the prefix pam_.
- PAM configuration is done in directory /etc/pam.d/
  - Contains a configuration file for every application that uses PAM
- Configuration file entries structure
  - module-type
    - auth
    - account
    - session
    - password

PAM Configuration (continued)

- Configuration file entries structure (continued)
  - control-flag
    - required
    - requisite
    - sufficient
    - optional
  - module-path
  - args
  - auth requisite pam_unix2.so nullok
  - auth required pam_securetty.so

PAM Configuration (continued)

- Configuration file entries structure (continued)
  - auth required pam_nologin.so
  - auth required pam_env.so
  - auth required pam_mail.so
  - account required pam_unix2.so
  - password required pam_pwcheck.so nullok
  - password required pam_unix2.so nullok use_first_pass use_authtok
  - session required pam_unix2.so none
  - session required pam_limits.so

The Requirements for a Secure Password

- Even the best security setup for a system
  - Can be defeated if users choose easy to guess passwords
- Dictionary attacks
  - Password cracking program just tries one word after another from a dictionary file
- Enable a special PAM module pam_pwcheck.so
  - To test a password first before a user can set it
- Password check programs example
  - John the Ripper (www.openwall.com/john/)

Exercise 4-1 Change the PAM Configuration to Disable the Graphical Root Login

- In this exercise, you will modify the PAM configuration to disable the Graphical Root Login

Ensure File System Security

- Objectives
  - The Basic Rule for User Write Access
  - The Basic Rule for User Read Access
  - How Special File Permissions Affect the Security of the System

The Basic Rule for User Write Access

- File systems used in Linux
  - Structurally similar to UNIX file systems
  - Support the typical UNIX file access permissions (read, write, execute, sticky bit, SUID, SGID, etc.)
- Normal user should only have write access to
  - The home directory of the user
  - The /tmp directory to store temporary files
- Depending on the purpose of a computer
  - Other directories can be writable by users

The Basic Rule for User Read Access

- Some files should be protected from user read access
  - Especially files that store passwords
    - /etc/shadow
    - /etc/samba/smbpasswd
    - Files with Apache passwords
    - /etc/openldap/slapd.conf
    - /boot/grub/menu.lst
- Some password files can be readable for a nonroot account

How Special File Permissions Affect the Security of the System

- Three file system rights that influence the security in a special way
  - SUID bit
    - Set for an executable
    - Program is started under the user ID of the file owner
  - SGID bit
    - Lets program run under the GID of the group to which the executable file belongs
  - Sticky bit
    - Prevents users from deleting each others files

Use ACLs for Advanced Access Control

- Objectives
  - The Basics of ACLs
  - Important ACL Terms
  - ACL Types
  - How ACLs and Permission Bits Map to Each Other
  - How to Use the ACL Command-Line Tools
  - How to Configure a Directory With an Access ACL
  - How to Configure a Directory
  - The ACL Check Algorithm
  - How Applications Handle ACLs

The Basics of ACLs

- Set of permissions
  - read (r), write (w), execute (x)
- Types of users
  - File owner, group, and other users
- ACLs (Access Control Lists)
  - Assign permissions to individual users or groups
  - Supported by the ReiserFS, Ext2, Ext3, JFS, and XFS
- Useful when
  - Replacing Windows server with Linux server
    - Providing file and print services with Samba

Important ACL Terms

- user class
  - The owner, the owning group, and other users
- access ACL
  - User and group access permissions for all kinds of file system objects
- default ACL
  - Determine the permissions a file system object inherits from its parent directory
- ACL entry
  - Contains a type, a qualifier for the user or group to which the entry refers, and a set of permissions

ACL Types

- Two basic classes of ACLs
  - Minimum ACL
  - Extended ACL
- ACLs extend the classic Linux file permission
  - By the following permission types
    - named user
    - named group
    - mask
- Permissions defined in the entries owner and other are always effective

ACL Types (continued)

Table 4-10

Type	Text Form
owner	user::rwx
named user	user:name:rwx
owning group	group::rwx
named group	group:name:rwx
mask	mask::rwx
other	other::rwx

How ACLs and Permission Bits Map to Each Other

- Assigning an ACL to a file or directory
  - Permissions set in the ACL are mapped to the standard UNIX permissions

How ACLs and Permission Bits Map to Each Other (continued)

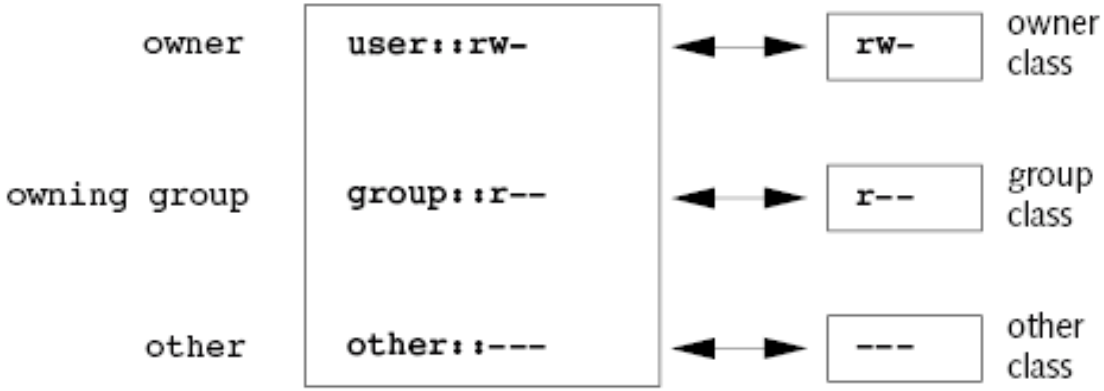

Figure 4-2

How ACLs and Permission Bits Map to Each Other (continued)

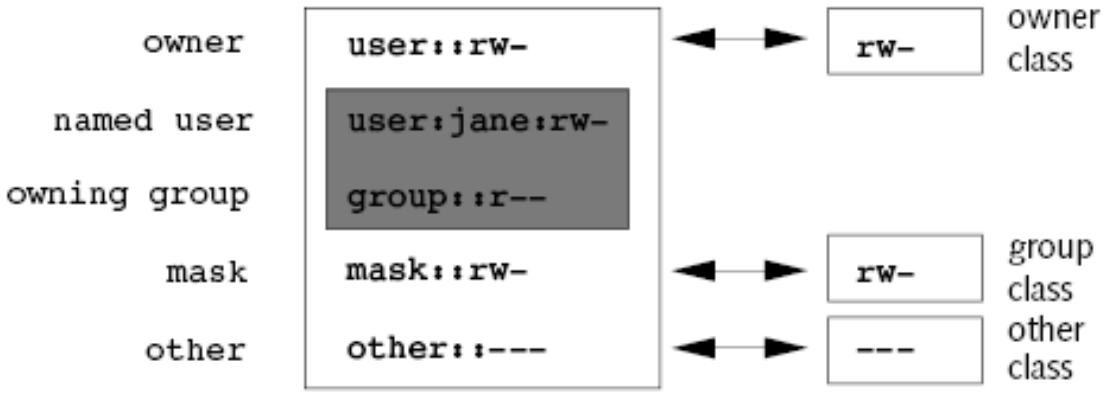

Figure 4-3

How to Use the ACL Command-Line Tools

- Command-line tools
  - getfacl
  - setfacl
- Examples
  - setfacl -m u:tux:rx my_file
  - setfacl -m g:accounting:rw my_file
  - setfacl -m m:rx

How to Use the ACL Command-Line Tools (continued)

Table 4-12

Option	Description
-m	Adds or modifies an ACL entry.
-x	Removes an ACL entry.
-d	Sets a default ACL.
-b	Removes all extended ACL entries.

How to Configure a Directory with an Access ACL

- Steps
  - Use the umask command to define access permissions to be masked
    - Each time a file object is created
  - Check initial state of the ACL by entering:
    - getfacl mydir
  - Modify the ACL
    - setfacl -m user:jane:rwx,group:jungle:rwx mydir
  - Take a look at the resulting ACL:
    - getfacl mydir
  - Add or remove permissions with chmod

How to Configure a Directory with a Default ACL

- Default ACL
  - Defines access permissions objects under the directory inherit when they are created
- Passing permissions of a directory's default ACL
  - Subdirectory inherits default ACL of parent directory
    - Both as its own default ACL and as an access ACL
  - File inherits default ACL as its own access ACL
- Parent directory does not have a default ACL
  - umask permission bits are subtracted from the mode parameter permissions

How to Configure a Directory with a Default ACL (continued)

- Parent directory has a default ACL
  - Permission bits correspond to overlapping portion of mode parameter permissions and default ACL
- Add a default ACL to the existing directory mydir
  - setfacl -d -m group:jungle:r-x mydir
- Create a subdirectory in mydir, which inherits the default ACL
  - mkdir mydir/mysubdir
  - getfacl mydir/mysubdir

The ACL Check Algorithm

- Applied before any process or application is granted access
  - To an ACL-protected file system object
- ACL entries are examined in the sequence:
  - owner, named user, owning group or named group, and other
  - Permissions do not accumulate
- Things are more complicated if
  - Process belongs to more than one group and belongs to several group entries

How Applications Handle ACLs

- Important applications still lack ACL support
  - There are no backup applications that guarantee full preservation of ACLs
- Basic file commands (cp, mv, ls, and so on) support ACLs
  - But many editors and file managers (such as Konqueror) do not

Exercise 4-2 Use ACLs

- In this exercise, you will do the following:
  - Part I: Configure the ACL of a Directory
  - Part II: Configure a Default ACL for a Directory
  - Part III: Delete an ACL

Configure Security Settings with YaST

- Open the YaST Control Center
  - Select Security and Users > Security settings
- You can change the following settings
  - The password settings
  - The boot behavior of the system
  - The login behavior
  - The user ID limitations
  - General file system security

Configure Security Settings with YaST (continued)

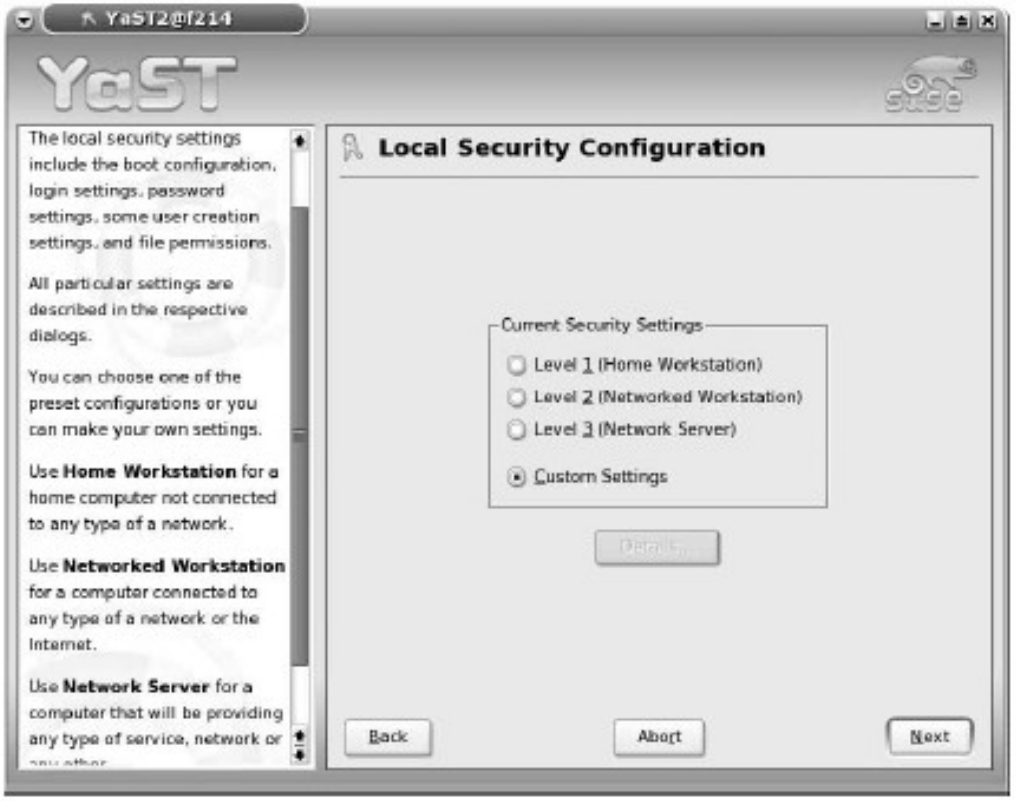

Figure 4-4

Configure Security Settings with YaST (continued)

- Levels of local security
  - See Table 4-13
- Change default password
  - See Figure 4-5
  - Password options (see Table 4-14)

Configure Security Settings with YaST (continued)

Table 4-13

Level	Description
Level 1 (Home Workstation)	This option represents the lowest level of local security. It should only be used on a home workstation that is not connected to any kind of network.
Level 2 (Networked Workstation)	This option provides an intermediate level of local security. It is suitable for workstations that are connected to a network.
Level 3 (Network Server)	This option enables a high level of local security. Systems that are used as a network server should be run with this setting.
Custom Settings	This option lets you create your own level of local security.

Configure Security Settings with YaST (continued)

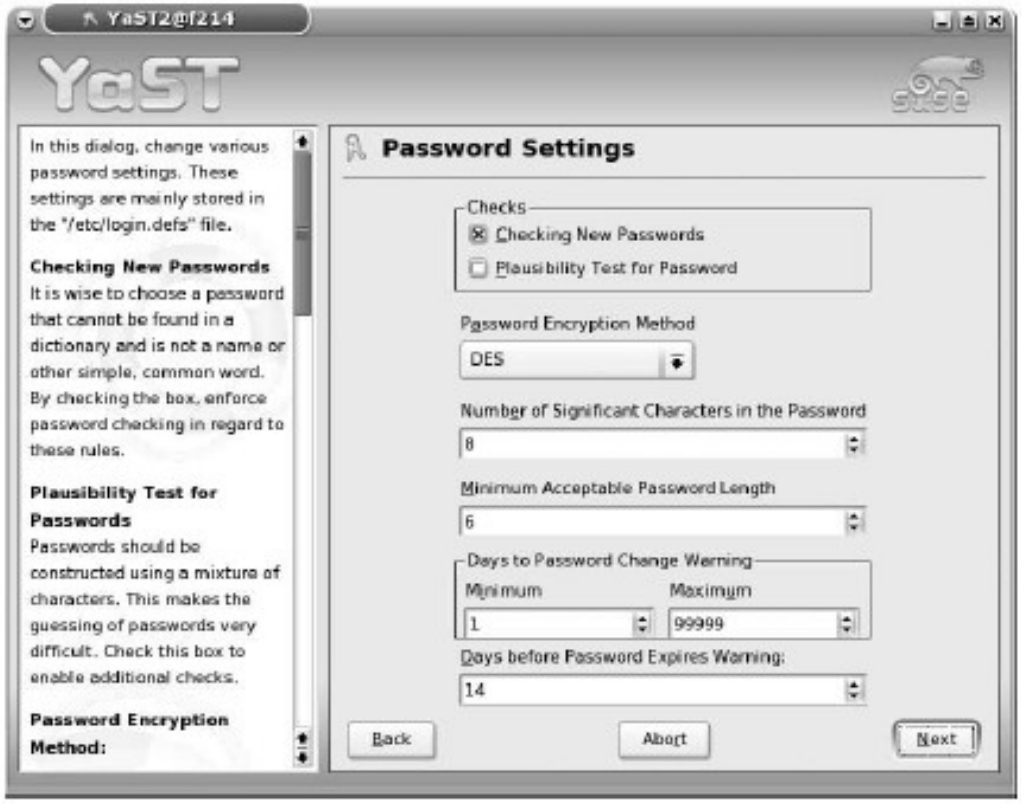

Figure 4-5

Configure Security Settings with YaST (continued)

Table 4-14

Option	Description
Checks	This option enables the checking of newly created passwords. The following two methods can be enabled: • **Checking New Passwords.** New passwords will be checked to see if they can be found in a dictionary. • **Plausibility Test For Passwords.** Passwords will be checked to see if they contain a mixture of different kind of characters (such as lowercase and uppercase characters). For a server system, you should at least enable Checking New Passwords.
Password Encryption Method	You can choose between different kinds of password encryption methods. This option sets the maximum length of the password. The default option DES supports only passwords with a length up to eight characters. MD5 and blowfish support longer passwords but are not well supported by older systems and applications. Unless your system does not need to meet very high security demands, you can stay with the default DES.
Number Of Significant Characters In The Password	This option corresponds to the previous one. You can only choose a value higher than eight if you have chosen a different encryption method than DES. For normal security demands, a value of eight is sufficient.
Minimum Acceptable Password Length	This value determines the minimum length of a password. The shorter a password is, the easier it is to crack it. A password should never be shorter than six characters.
Days To Password Change Warnings	The name of this option is a little bit misleading. There are two values to be set: • **Minimum.** The number of days after a user can change the password. • **Maximum.** The number of days after a user must change the password.
Days Before Password Expires Warning	This option determines how many days before a password has to be changed that a warning should be given to the user.

Configure Security Settings with YaST (continued)

- Configure how the system can be rebooted
  - See Figure 4-6
  - Configuration options (see Table 4-15)

Configure Security Settings with YaST (continued)

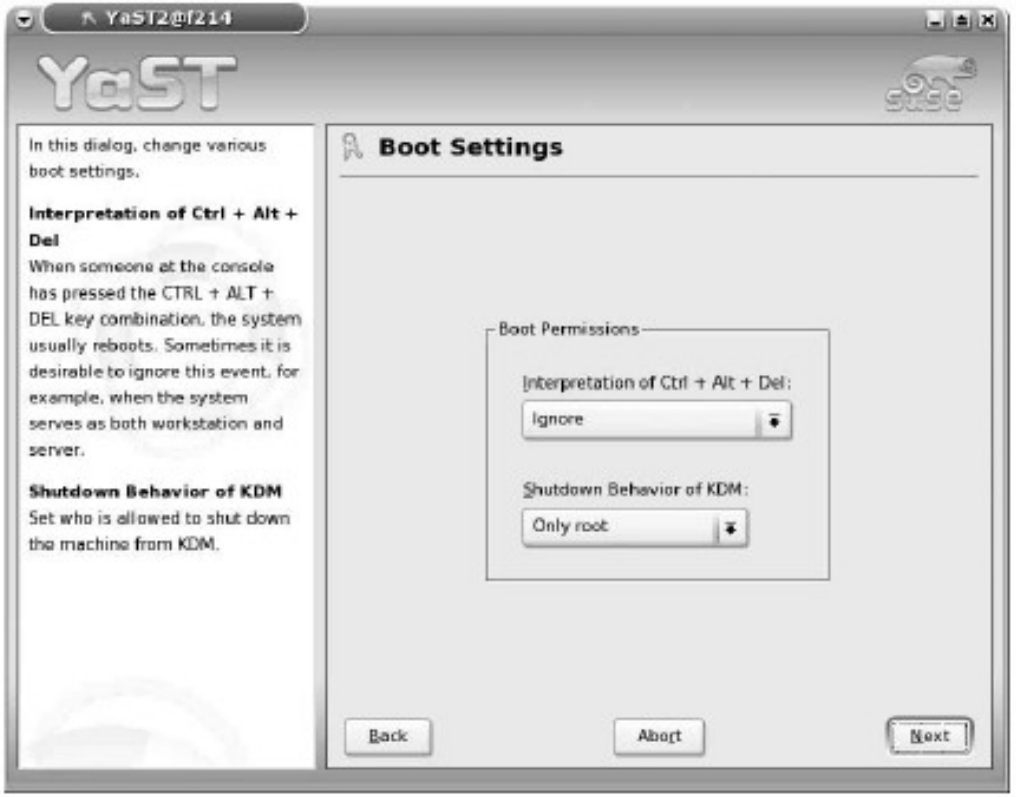

Figure 4-6

Configure Security Settings with YaST (continued)

Table 4-15

Option	Description
Interpretation Of Crtl+Alt+Del	This option determines how the Key Combination Crtl+Alt+Del is evaluated. You can choose between the following possibilities: • **Ignore.** The key combination is ignored; nothing happens. • **Reboot.** When the combination is pressed, the system reboots. • **Halt.** The system can be halted by pressing the key combination. On a server you should always choose Ignore because otherwise someone could halt or reboot the system even without being logged in.
Shutdown Behavior Of KDM	This option determines how the system can be halted with the graphical login manager KDM. You have the following choices: • **Only Root.** To halt the system, the root password has to be entered. • **All users.** Everyone, even remotely connected users, can halt the system using KDM. • **Nobody.** Nobody can halt the system with KDM. • **Local Users.** Only locally connected users can halt the system with KDM. • **Automatic.** The system is halted automatically after log out. For a server system you should use Only Root or Nobody to prevent normal or even remote users from halting the system.

Configure Security Settings with YaST (continued)

- Configure the login behavior of the system
  - See Figure 4-7
  - Configuration options (see Table 4-16)
- Adjust the Minimum and the Maximum value for User and Group IDs
  - See Figure 4-8

Configure Security Settings with YaST (continued)

Figure 4-7

Configure Security Settings with YaST (continued)

Table 4-16

Option	Description
Delay After Incorrect Login Attempts	The value of this option determines the number of seconds the next login try will be delayed after a failed login attempt. This is useful to prevent attackers from trying various passwords very quickly. The default value 3 is sufficient in most cases.
Record Failed Login Attempts	If this option is checked, failed login attempts are logged. This option should be enabled.
Record Successful Login Attempts	If this option is checked, successful login attempts are logged. This option should also be enabled.
Allow Remote Graphical Login.	The display manager KDM lets you log in remotely to the X-Window system. If this option is selected, remote login is allowed. For a server system, you should not enable this option unless it is needed for purpose of the server (for example, the system is a terminal server.)

Configure Security Settings with YaST (continued)

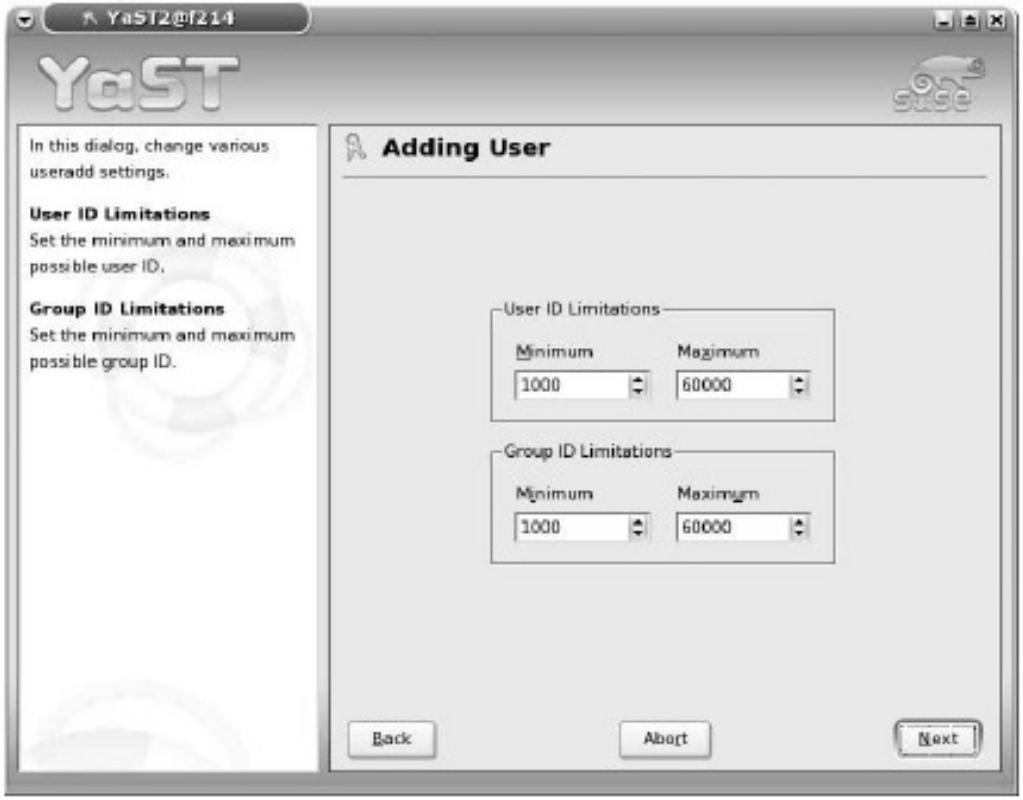

Figure 4-8

Configure Security Settings with YaST (continued)

- Configure miscellaneous settings
  - See Figure 4-9
  - Configuration options (see Table 4-17)

Configure Security Settings with YaST (continued)

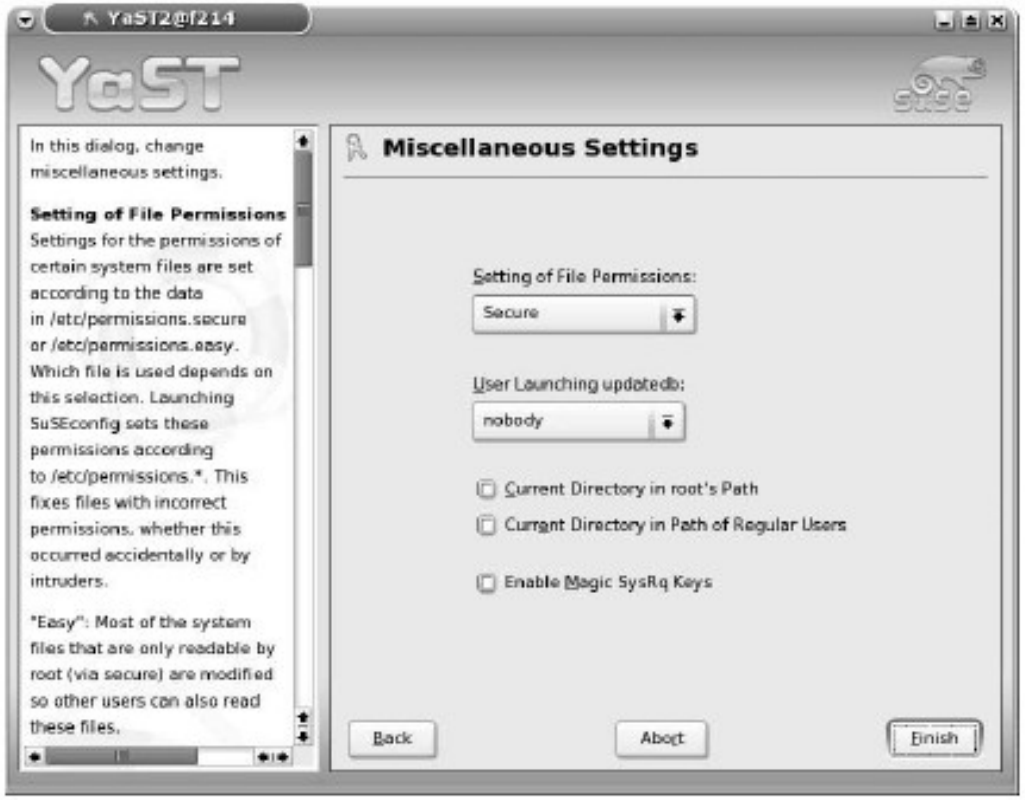

Figure 4-9

Configure Security Settings with YaST (continued)

Table 4-17

Option	Description
Setting Of File Permissions	From this menu, you can choose between three different presets for file system permissions. You have the following options: • **Easy.** Most configuration files are readable for normal users. • **Secure.** Certain system files (like /var/log/messages) can only be viewed by root. Some programs can only be launched by root or by daemons. • **Paranoid.** This is the preset with the highest level of file system security. Access rights are even more restricted than with the Secure setting. The security settings for every preset are read from configuration files following the naming scheme/etc/permissions.<level>. For example, the configuration for the Secure level is read from the file/etc/permissions.secure. Each file contains a description of the file syntax and purpose of the preset. You can also add your own rules to the file /etc/permissions.local.

Configure Security Settings with YaST (continued)

Table 4-17 (continued)

Option	Description
User Launching Updatedb	This option determines under which user ID the command updatedb is executed by cron. The updatedb program indexes all files in the file system. The generated database can be queried with the locate command. The choices of this option are: • **nobody.** The command is launched under the user ID of the system user nobody. This way only files that are accessible for the user nobody are indexed. • **root.** The command is executed under the user ID of the root user. This way all files in the file system can be indexed. For security reasons you should use the user nobody. This way no files are indexed that should not be accessible for normal users.
Current Directory In Root Path	If this option is selected, the current directory is added to the search path of root. This could lead to security problems if an attacker places an executable with a common name like ls into a directory. If root enters ls in that directory, the executable of the attacker could be launched instead of the normal ls command. Never select this option.
Current Directory In Path Of Regular Users	If this option is selected, the current directory is added to the search path of normal users. In a security sensitive environment, this option should not be enabled.
Enable Magic SysRq Keys	This option enables special key combinations that give you some control over the system even in the case of a system crash. This is useful for debugging purposes but should be disabled on production systems.

Stay Informed About Security Issues

- Resources
  - www.suse.de/en/business/security.html
  - www.suse.de/en/business/mailinglists.html
    - suse-security
    - suse-security-announce
  - www.securityfocus.com/

Exercise 4-3 Subscribe to the SUSE Security Announcements

- In this exercise, you will subscribe to the SUSE security mailing list

Apply Security Updates

- Objectives
  - Register Your Product
  - Use the YaST Online Update

Register Your Product

- Access the update packages
  - Need to enter a user name and a password
    - Create an account for the SUSE support portal
- SUSE support portal *http://portal.suse.com*
- Register your product in the portal
  - With registration code delivered with the SLES 9 DVD
- Registered products can be updated with the YOU module

Use the YaST Online Update

- Steps
  - Start the YOU module from the YaST Control Center
  - YOU asks you for your account at the SUSE support portal
  - YOU retrieves information about the available patches
  - Select packages to install
  - By selecting Accept, the selected updates are downloaded and installed

Use the YaST Online Update (continued)

Figure 4-10

Use the YaST Online Update (continued)

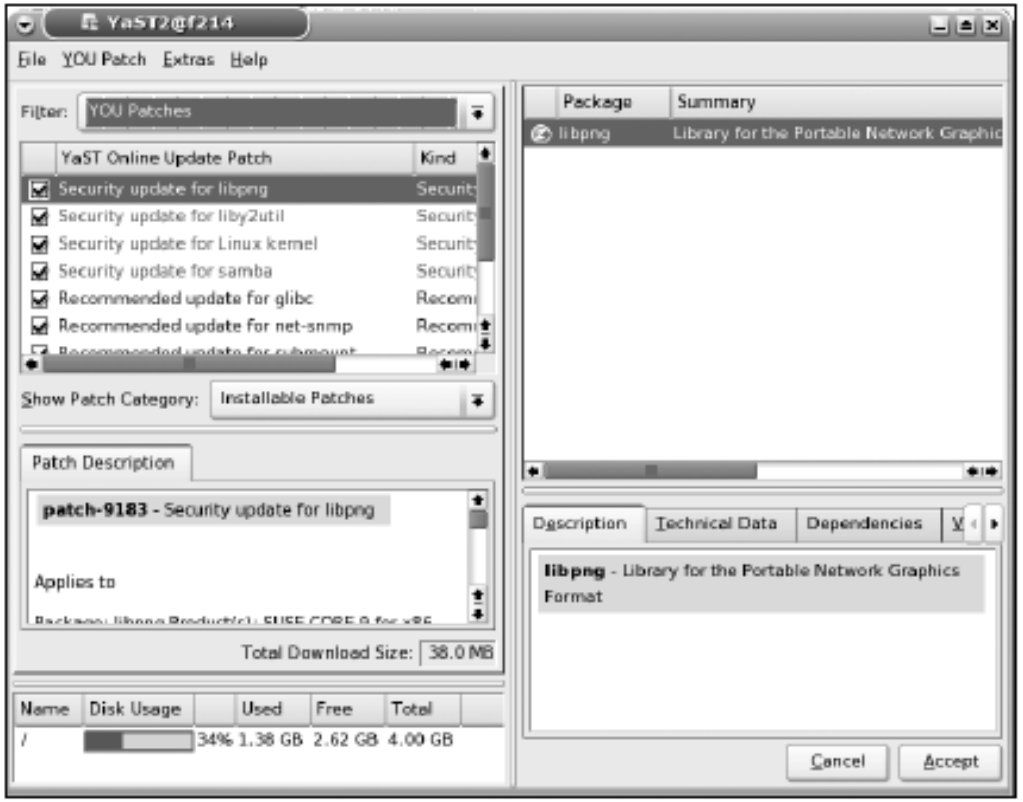

Figure 4-12

Use the YaST Online Update (continued)

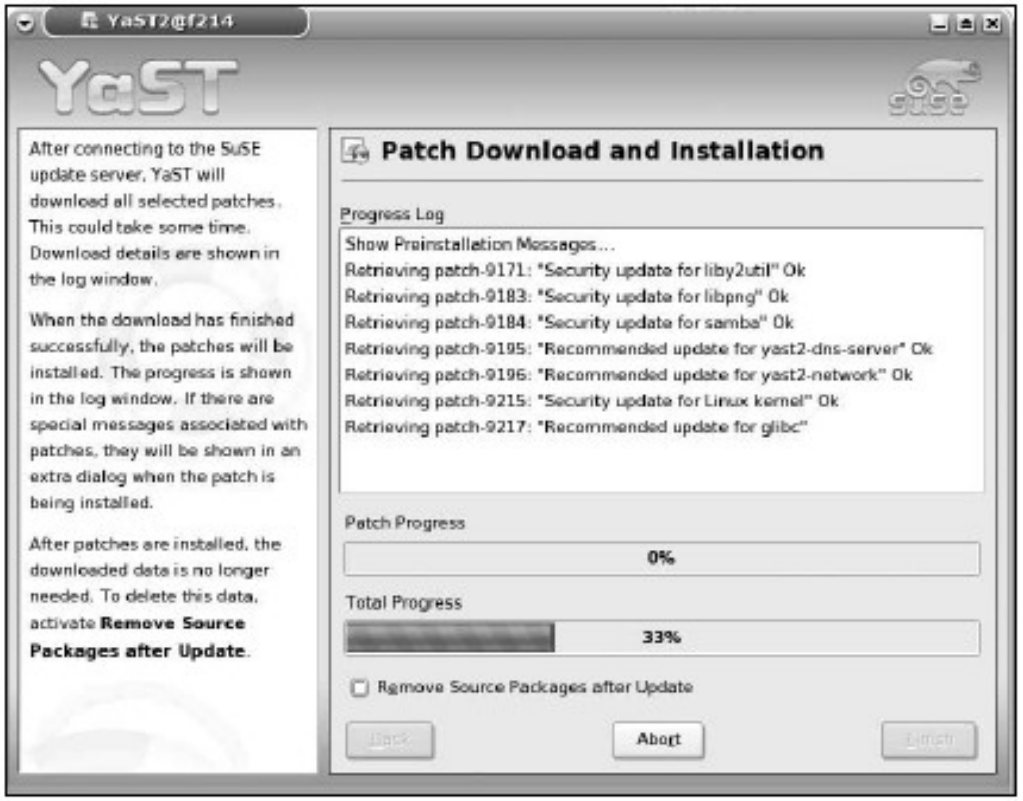

Figure 4-13

Summary

- Analyze network communication and protection requirements
- Protect your servers by storing them in a locked room
- PAM modules centralize authentication requests from applications
  - And add additional security to Linux systems
- Good security practice
  - Assign only the necessary permissions for system files and directories
- Write and read access rules

Summary (continued)

- Using the SUID and SGID permissions
  - Test your program thoroughly to ensure that no security loopholes exist during execution
- Use the sticky bit permission on public directories
  - To prevent data loss
- ACLs may be used to expand the assignment of traditional Linux permissions
- Default ACLs may be set on a directory
  - To modify the ACL on newly created files and subdirectories within

Summary (continued)

- Select an overall security level for your system using YaST
- There are many Web resources
  - That you can use to stay informed about current security issues
- YOU module
  - May be used to obtain important security-related patches
    - From the SUSE update servers